Zone Labs セキュリティ ソフトウェア

バージョン 6.5

ZONE LABS
A Check Point COMPANY
Smarter Security™

(c) 2006 Zone Labs, LLC. All rights reserved.
(c) 2006 Check Point Software Technologies Ltd. All rights reserved.

Check Point、Application Intelligence、Check Point Express、Check Point ロゴ、AlertAdvisor、ClusterXL、Cooperative Enforcement、ConnectControl、Connectra、CoSa、Cooperative Security Alliance、FireWall-1、FireWall-1 GX、FireWall-1 SecureServer、FloodGate-1、Hacker ID、IMsecure、INSPECT、INSPECT XL、Integrity、InterSpect、IQ Engine、Open Security Extension、OPSEC、Policy Lifecycle Management、Provider-1、Safe@Home、Safe@Office、SecureClient、SecureKnowledge、SecurePlatform、SecurRemote、SecurServer、SecureUpdate、SecureXL、SiteManager-1、SmartCenter、SmartCenter Pro、Smarter Security、SmartDashboard、SmartDefense、SmartLSM、SmartMap、SmartUpdate、SmartView、SmartView Monitor、SmartView Reporter、SmartView Status、SmartViewTracker、SofaWare、SSL Network Extender、TrueVector、UAM、User-to-Address Mapping、UserAuthority、VPN-1、VPN-1 Accelerator Card、VPN-1 Edge、VPN-1 Pro、VPN-1 SecureClient、VPN-1 SecuRemote、VPN-1 SecureServer、VPN-1 VSX、Web Intelligence、ZoneAlarm、Zone Alarm Pro、Zone Labs、および Zone Labs ロゴは、Check Point Software Technologies Ltd. またはその提携会社の商標または登録商標です。ここで言及されている他のすべての製品名は、各所有者の商標または登録商標です。本文書に記載されている製品は、U.S. Patent No. 5,606,668、5,835,726、および 6,496,935 で保護されており、米国のその他の特許またはその他の国の特許で保護されている場合や、特許を出願中のアプリケーションの場合があります。

Zone Labs, LLC.
A Checkpoint Company
475 Brannan, Suite 300
San Francisco, CA 94107

ZLD 1-0422-0650-2006-06-03

コンテンツ

表 ix

図 xi

はじめに xiii

バージョン情報 Zone Labs セキュリティ ソフトウェア xiv

リリース 6.0 の新機能 xv

このガイドについて xvi
規則 xvi
Zone Labs ユーザ フォーラム xvi

第 1 章 インストールとセットアップ 1

システム要件とサポートされるソフトウェア 2
メール保護がサポートしているプロトコル 2
サポートされているブラウザ ソフトウェア 2
サポートされている IM クライアント 3

Zone Labs セキュリティ ソフトウェアのインストール 4
ZoneAlarm のインストール 4
Zone Labs セキュリティ ソフトウェアのインストール 5

旧バージョンからのアップグレード 6
アップグレードと Windows XP SP2 ファイアウォール 6
アップグレードおよび IMsecure myVault 設定 6
アップグレードおよび MailFrontier 設定 6

基本オプションの選択 7
プログラムのアクセス許可の設定 7
DefenseNet コミュニティへの参加 7

Zone Labs セキュリティ ソフトウェアのアンインストール 9

第 2 章 Zone Labs セキュリティ ソフトウェアの基本 . 11

Zone Labs セキュリティ ソフトウェアコントロール センタの概要 . . . 12
コントロール センタの使用法 12
ダッシュボードの使用 13
システム トレイ アイコン 15
ショートカットメニュー 15
［状況］タブの使用 16

ゾーンの概念 18
ファイアウォール セキュリティを管理するゾーン 18
プログラム コントロールを提供するゾーン 19

警告への対応 20
新しいプログラム警告. 20
新しいネットワークおよび VPN 警告 21

製品設定の指定 22
アップデート オプションの設定. 22
パスワードの設定. 22
セキュリティ設定のバックアップとリストア 23
全般的な製品設定の指定 24
連絡設定の指定 25
製品表示とプロキシ サーバのオプションの設定. 26
オンライン詐称保護プロファイルの作成 26

ライセンス、登録、およびサポート 28
製品ライセンスのアップデート 28
Zone Labs セキュリティ ソフトウェアの登録 28
テクニカル サポートへのアクセス 29

第 3 章 Zone Labs セキュリティ ソフトウェア を使ったネットワーキング 31

新しいネットワーク接続の設定 32
ネットワーク設定ウィザードの使用 32
ネットワーク設定ウィザードの無効化. 33
ワイヤレス ネットワーク設定ウィザードの使用. 33
ワイヤレス ネットワーク設定ウィザードの無効化 34

ネットワーク サービスとの統合 35
ファイルおよびプリンタの共有の有効化 35
ネットワーク メール サーバへの接続. 35
インターネット接続共有（ICS）の有効化 36

VPN 接続の設定 37
サポートされている VPN プロトコル 37
VPN 接続の自動設定 37
VPN 接続の手動設定 38
VPN ゲートウェイとその他のリソースのトラスト ゾーンへの追加 39
ブロックされた IP 範囲またはサブネットからの VPN ゲートウェイの削除 39
VPN プロトコルの許可. 40
VNP ソフトウェアのアクセス許可. 40

第 4 章 ファイアウォール保護 43

ファイアウォール保護の概念. 44

セキュリティ レベルの選択. 45
ゾーンのセキュリティ レベルの設定 45

アドバンス セキュリティ オプションの設定. 47
ゲートウェイ セキュリティ オプションの設定. 47
ICS（インターネット接続共有）オプションの設定 47
全般的セキュリティ オプションの設定 48
ネットワーク セキュリティ オプションの設定. 49
ワイヤレス ネットワーク セキュリティ オプションの設定 50

通信ソースの管理 52
通信ソースの一覧の表示 52

通信ソースの変更 52
トラスト ゾーンへの追加 53
ブロック ゾーンへの追加 54
ログに記録されたファイアウォール イベントの表示 54

ポートのブロックおよびブロック解除 56
デフォルトのポート許可設定 56
カスタム ポートの追加 57

エキスパート ファイアウォール ルールの概念 59
エキスパート ファイアウォール ルールの施行方法 59
エキスパート ファイアウォール ルールの適用ランク 60

エキスパート ファイアウォール ルールの作成 62

グループの作成 65
場所グループの作成 65
プロトコル グループの作成 66
曜日 / 時間グループの作成 68

エキスパート ファイアウォール ルールの管理 70
エキスパート ルールの一覧の表示 70
ルールの編集とランク変更 71

第 5 章 プログラム コントロール 73

プログラム コントロールの概念 74
自動によるプログラム許可の設定 74
手動によるプログラム許可の設定 75

全般的プログラム コントロール オプションの設定 77
プログラム コントロール レベルの設定 77
SmartDefense Advisor のレベルの設定 79
自動ロックの有効化 79
ログに記録されたプログラム イベントの表示 81
記録された OSFirewall イベントの表示 82

アドバンス プログラム設定の指定 83
グローバルなプログラム プロパティの設定 83
新しいプログラムのアクセス許可の設定 83

特定プログラムの許可の設定 85
プログラム一覧の使用 85
プログラム一覧へのプログラムの追加 89
プログラムのインターネット アクセスの許可 89
プログラムのサーバ動作の許可 90
プログラムへのメール送信許可の付与 90

特定プログラムの許可の設定 91
アドバンス プログラム コントロール オプションの設定 91
プログラムのアウトバウンド メール保護の無効化 91
プログラムのフィルタ オプションの設定 92
認証オプションの設定 92
プログラムへのパスロック許可の設定 93

プログラム コンポーネントの管理 94

プログラム用のエキスパート ルールの作成 96
プログラム用のエキスパート ルールの作成 96
エキスパート ルールの共有 97

第 6 章　パイウェアおよびウイルス保護 99

スパイウェアおよびウイルス保護 100
ウイルスおよびスパイウェア保護の有効化 100
スキャンのスケジューリング 101
ウイルスおよびスパイウェア保護のアップデート 102

ウイルス保護オプションのカスタマイズ 104
スキャン ターゲットの指定 104
アクセス スキャン 106
メール スキャン 106
自動ウイルス処理の有効化 107
ウイルス検出方法の指定 107

スパイウェア保護オプションのカスタマイズ 108
自動スパイウェア処理の有効化 108
スパイウェア検出方法の指定 108
スキャンからのスパイウェアの除外 109
スパイウェア攻撃の防止 109

ウイルス スキャンの実行 110
ウイルススキャン結果の理解 111
ウイルス ファイルの手動処理 112
アーカイブ内のファイルの修復 112
Zone Labs での確認用のウイルスおよびスパイウェアの送信 113
記録されたウイルス イベントの表示 113

スパイウェア スキャンの実行 115
スパイウェア スキャン結果の理解 116
スパイウェア スキャン結果中のエラー 118
隔離内の項目の表示 118
記録されたスパイウェア イベントの表示 119

ウイルスおよびスパイウェア保護の状況の表示 121

ウイルス保護のモニタリング 122
モニタリング可能なソフトウェア 122
ZoneAlarm、ZoneAlarm Pro、および ZoneAlarm Wireless でのモニタリング 123
ZoneAlarm Anti-virus および ZoneAlarm Security Suite でのモニタリング 123
アンチウイルス モニタリングの有効化と無効化 124
［アンチウイルス モニタリング］パネルでの状況メッセージの表示 124
アンチウイルス モニタリング警告 125

第 7 章　メール保護 127

メール保護の概念 128
インバウンド MailSafe 保護 128
アウトバウンド MailSafe 保護 129
インバウンド MailSafe 保護の有効化 129
アウトバウンド MailSafe 保護の有効化 129

インバウンド MailSafe 保護のカスタマイズ 130
添付ファイル一覧の表示 130
添付ファイルの種類の隔離設定の変更 130
添付ファイルの種類の追加と削除 131
隔離された添付ファイルの表示 131

アウトバウンド MailSafe 保護のカスタマイズ 133
プログラム別のアウトバウンド MailSafe 保護の有効化 133

アウトバウンド MailSafe 保護オプションの設定 134

迷惑メールのフィルタリング 135
特定の送信者からのメールの許可またはブロック 135
特定の会社からのメールの許可またはブロック 136
許可リストへの連絡先の追加 136
受信トレイのスキャン 136
配布リストからのメールの許可 137
迷惑メールの報告 137
詐欺メールの報告 138
迷惑メール メッセージ オプションの指定 139
不明な送信者からのチャレンジ メール 140
外部へのメール サーバの指定 142
迷惑メール フィルタ設定のカスタマイズ 143
間違って迷惑メールと識別されたメールのリストア 144
迷惑メール フィルタ レポートの表示 145

メールのアンチウイルス保護 146
メール スキャンの有効化 146
感染したメールの処理方法 147

第 8 章 プライバシー保護 149

プライバシー保護の概念 150

全般的プライバシー オプションの設定 151
プライバシー保護レベルの設定 151
ブラウザ以外のプログラムへのプライバシー保護の適用 152

プライバシー アドバイザの使用 153

特定の Web サイトのプライバシー オプションの設定 154
プライバシー サイト一覧の表示 154
プライバシー サイト一覧へのサイトの追加 155
サイト一覧のサイトの編集 156

Cookie コントロールのカスタマイズ 157
セッション Cookie のブロック 157
永続 Cookie のブロック 157
サードパーティ Cookie のブロック 158
Cookie の有効期限の設定 158

広告ブロックのカスタマイズ 160
ブロックする広告の指定 160
広告のボイド コントロール オプションの設定 160

モバイル コード コントロールのカスタマイズ 162
ブロックするモバイル コードの種類の指定 162

キャッシュ クリーナの概念 164
キャッシュ クリーナの使用 164
ハード ドライブの削除オプションのカスタマイズ 165
ブラウザの削除オプションのカスタマイズ 165

第 9 章 警告とログ 169

警告とログの概念 170
Zone Labs セキュリティ ソフトウェアの警告について 170

イベントのログ 176

基本的な警告およびログ オプションの設定 177
警告イベント レベルの設定 177
イベントおよびプログラムのログ オプションの設定 177

特定の警告の表示または非表示 178
ファイアウォール警告の表示または非表示 178
システム トレイ警告の有効化 178

イベントおよびプログラムのログ オプションの設定 179
ログ形式の設定 179
イベントのログのカスタマイズ 179
プログラムのログのカスタマイズ 180
ログ エントリの表示 180
テキスト ログの表示 182
ログ エントリのアーカイブ 184

SmartDefense Advisor およびハッカー ID の使用 186

第 10 章 データの保護 187

ID ロック機能の概念 188
個人情報はどのように保護されるか 188
ID ロック保護レベルの設定 189
ID ロック ステータスのモニタリング 190

myVAULT について 191
myVAULT へのデータの追加 191
myVAULT コンテンツの編集と削除 193

トラスト サイト リストの使用 194
トラスト サイト リストの表示 194
トラスト サイト リストへの追加 195
信頼するサイトの編集と削除 196

第 11 章 ペアレント コントロール 197

ペアレント コントロールの概念 198

ペアレント コントロールとスマート フィルタリングの有効化 199
ペアレント コントロールの有効化と無効化 199
スマート フィルタリングの有効化と無効化 199
タイムアウト オプションの設定 200

ブロックするコンテンツ カテゴリの選択 201

第 12 章 インスタント メッセージングのセキュリティ 207

IM セキュリティの概要 208
アクセス 208
迷惑メールの防止 209
機能コントロール 209
外部からの保護 210
インスタント メッセージング トラフィックの暗号化 212

IM セキュリティ オプションの設定 215
保護レベルの設定 215
IM セキュリティ保護のステータスの表示 215
保護設定のカスタマイズ 216
詳細な IM セキュリティ オプションの設定 216
ログに記録された IM セキュリティ イベントの表示 218

付録 A 警告のリファレンス 221

情報警告 222
ファイアウォール警告 / 保護 222
MailSafe 警告 223
ブロックされたプログラム警告 224
インターネット ロック警告 225
リモート警告 226

プログラム警告 228
新しいプログラム警告 228
繰り返されたプログラム警告 229
変更されたプログラム警告 229
プログラム コンポーネント警告 230
サーバ プログラム警告 232
アドバンス プログラム警告 234
自動 VPN 設定警告 235
手動操作の要求警告 236

OSFirewall 警告 237
疑わしい動作の警告 237
危険な動作の警告 237
悪意のある動作の警告 238

ID ロック警告 239

新しいネットワーク警告 240

インスタント メッセージ警告 242

付録 B キーボードのショートカット 245

ナビゲーション ショートカット 246

グローバル機能ショートカット 247

ダイアログ ボックスのコマンド 249

ボタンのショートカット 250

付録 C トラブルシューティング 253

VPN 254
VPN 通信のための Zone Labs セキュリティ ソフトウェアの設定 254
VPN の自動設定およびエキスパート ルール 254
VPN の自動検出の遅延 255

ネットワーキング 256
ローカル ネットワークでのコンピュータの認識 256
ローカル ネットワークでのファイルおよびプリンタの共有 257

起動に時間がかかる場合の対処 257

インターネット接続 258
インストール後インターネットに接続できない 258
ISP ハートビート メッセージの許可 259
ICS クライアントを介した接続 260
プロキシ サーバを介した接続 260
プログラム アドバイス サーバに接続できない 260

IM セキュリティ 261
IM プログラムがステータスに表示されない 261

アンチウイルス 262
アンチウイルス機能のインストールに関する問題 262
アンチウイルス モニタリング警告 262
アンチウイルス製品同士の競合の解決 263
メール スキャンまたは IM セキュリティが使用できない 263

サードパーティのソフトウェア 264
アンチウイルス 264
ブラウザ 265
チャット プログラムおよびインスタント メッセージング プログラム 266
メール プログラム 266
インターネット留守番電話プログラム 267
ファイル共有プログラム 267
FTP プログラム 267
ゲーム 268
リモート コントロール プログラム 269
VNC プログラム 270
ストリーミング メディア プログラム 270
Voice over IP プログラム 271
Web 会議プログラム 271

付録 D プログラム動作 273

疑わしい動作 274

危険な動作 275

用語集 279

索引 1

表

表 2-3: システム トレイ アイコン 15

表 2-4: アップデート メッセージ 17

表 3-1: サポートされている VPN プロトコル 37

表 3-2: 必要な VPN 関連ネットワーク リソース 39

表 4-1: 通信ソースの一覧のフィールド 52

表 4-2: ファイアウォール イベント ログのフィールド 55

表 4-3: 外部からまたは外部への通信の種類に対するデフォルトのアクセス許可 56

表 5-1: プログラムのイベント ログ フィールド 81

表 5-2: OSFirewall イベント ログのフィールド 82

表 5-4: プログラム一覧の記号 88

表 6-3: スキャン ターゲットを示すアイコン 105

表 6-5: ウイルス イベント ログのフィールド 114

表 6-7: スパイウェア イベント ログのフィールド 120

表 9-7: ログ ビューアのフィールド 181

表 11-1: ペアレント コントロールのカテゴリ 201

表 A-1: IM 警告メッセージ 242

表 B-1: ナビゲーション ショートカット 246

表 B-2: グローバル ショートカット 247

表 B-3: ダイアログ ボックスのショートカット 249

表 B-4: ボタンをアクティブにするキー入力 250

表 C-1: VPN に関する問題のトラブルシューティング 254

表 C-2: ネットワークに関する問題のトラブルシューティング 256

表 C-3: インターネット接続に関するトラブルシューティング 258

表 C-4: IM セキュリティの問題に関するトラブルシューティング 261

表 C-5: Zone Labs アンチウイルスの問題に関するトラブルシューティング 262

表 D-1: 疑わしい動作のガイド 274

表 D-2: 危険な動作のガイド 275

図

図 2-1: Zone Labs セキュリティ ソフトウェアのコントロール センタ . . 12

図 2-2: Zone Labs セキュリティ ソフトウェアのダッシュボード 13

図 4-4: エキスパート ファイアウォール ルールのランク順 60

図 4-5: エキスパート ルールの一覧 70

図 5-3: プログラム一覧 86

図 5-5: コンポーネント一覧 94

図 6-1: アンチウイルスとアンチスパイウェアのステータス 102

図 6-2: [スキャン ターゲット] ダイアログ ボックス 104

図 6-4: [ウイルス スキャン結果] ダイアログ 111

図 6-6: [スパイウェア スキャン結果] ダイアログ 116

図 6-8: ZoneAlarm の [アンチウイルス モニタリング] パネルの [状況] エリア124

図 7-1: 添付ファイル一覧 130

図 7-2: [迷惑メール フィルタ] ツール バー 135

図 7-3: [チャレンジ] オプション タブ 141

図 7-4: 感染レポートの例 147

図 8-1: プライバシー アドバイザ 153

図 8-2: プライバシー サイト一覧 155

図 9-1: ファイアウォール警告 171

図 9-2: 新しいプログラム警告 172

図 9-3: 新しいネットワーク警告 173

図 9-4: ID ロック警告 174

図 9-5: 疑わしい動作の警告 175

図 9-6: 危険な動作の警告 176

図 10-1: myVAULT コンテンツの伝送 189

図 10-2: myVAULT コンテンツの受信 189

図 10-3: ID ロック ステータス エリア 190

図 10-4: トラスト サイト リスト 194

図 12-1: ブロックされた音声伝送の送信 210

図 12-2: 外部からの音声伝送のブロック 210

図 12-3: 実行可能 URL を接続に送信 211

図 12-4: 有害な可能性のあるリンクが削除されました 211

図 12-5: 暗号化された会話の例 213

図 12-6: 非暗号化された会話の例 213

はじめに

■ xiv ページの「バージョン情報 Zone Labs セキュリティ ソフトウェア」

■ xv ページの「リリース 6.0 の新機能」

■ xvi ページの「このガイドについて」

ZLD 1-0422-0650-2006-06-02

バージョン情報 Zone Labs セキュリティ ソフトウェア

Zone Labs セキュリティ ソフトウェアは、多数の機能と利点を提供するセキュリティ製品です。このリリースは、次のバージョンの Zone Labs セキュリティ ソフトウェアをサポートしています。

- ZoneAlarm

  ファイアウォール保護と制限付きのメール保護を提供します。

- ZoneAlarm Anti-virus

  無料の ZoneAlarm とウイルス保護で使用できる機能と同じ機能が含まれています。

- ZoneAlarm Wireless Security

  ワイヤレス ネットワークのサポートを含み、ファイアウォール保護と制限付きのメール保護を提供します。

- ZoneAlarm Pro

  エキスパート ファイアウォール保護、外部からと外部へのメール保護、プライバシー コントロール、スパイウェア保護、およびエキスパート ファイアウォール ルールが含まれています。

- ZoneAlarm Security Suite

  ZoneAlarm Pro で利用可能な機能に加え、IM セキュリティ、ペアレント コントロール、スパイウェアおよびウイルス保護、迷惑メール フィルタリングを含み、モバイル ラップトップ ユーザとワイヤレス ホーム ネットワークの保護を提供します。

リリース 6.0 の新機能

Zone Labs セキュリティ ソフトウェアのリリース 6.0 は、次の新機能を提供しています。

- スパイウェア保護－スパイウェアがコンピュータに被害を及ぼす前に予防、検出、削除を行います。自動処理オプションとアンチスパイウェア アドバイザにより、スパイウェアを容易に処理できます。100 ページの「スパイウェアおよびウイルス保護」を参照してください。
- OSFirewall(TM) 保護－プログラムのインストールやシステム レジストリの変更といった疑わしいプログラムの行為の有無についてオペレーティング システムを監視し、プログラムが悪意のあるプログラムによってハイジャックされるのを防ぎます。ブラウザ設定をハッカーによる変更から保護します。
- 拡張された SmartDefense Advisor －危険な行為または破壊行為を試行するプログラムを自動的に無効にする自動抹消制御が含みます。
- SmartDefense(TM) 即応ネットワーク－ Zone Labs のエキスパートで編成される専門チームは新しい脅威を常に監視し、ユーザの保護を最適化するようにセキュリティを自動調整します。署名データベースを最新のスパイウェアの発生に関する情報に基づいて自動的に更新します。新しいウイルス署名およびスパイウェア署名を自動的かつ定期的に配布します。
- Wi － fi ネットワーク サポート－新しいワイヤレス ネットワークを自動検出し､ネットワーク検出ダイアログに Service Set Identifier (SSID) を表示します。保護されていないワイヤレス ネットワークを特定し、適切なセキュリティを自動設定してコンピュータを保護します。
- 新しいフラッシュ チュートリアル－音声やアニメーションと共に Zone Labs セキュリティ ソフトウェア を紹介します。

このガイドについて

このガイドは、ZoneAlarm、ZoneAlarm Anti－virus、ZoneAlarm Pro、ZoneAlarm Wireless Security、および ZoneAlarm Security Suite のユーザー向けです。このガイドではこれらの製品の総称として、Zone Labs セキュリティ ソフトウェアを使用します。特定の製品を示す必要がある場合は、その製品名を使用します。

規則

このガイドでは、下記の表記およびグラフィックス規則が使用されています。

規則	説明
太字	パネル、タブ、フィールド、ボタン、メニュー オプションなどのユーザ インターフェイス エレメントの表記に使われています。
斜体	ファイル名およびパスの表記に使われています。
|	手順の説明において、選択対象のパネルとタブを区切るために使われています。 例：**[概要]**|**[状況]** を選択し、**[追加]** をクリックします。
	ヒント アイコン。タスクまたは手順を実行するための代替方法を提示します。
	ノート アイコン。関連情報、補足情報、重要情報などを強調します。
	注意アイコン。データやプログラムを破損する可能性のある操作やプロセスを示します。

Zone Labs ユーザ フォーラム

Zone Labs セキュリティ ソフトウェアのユーザ同士で交流できます。質問の投稿や回答の受信、他のユーザとの Zone Labs セキュリティ ソフトウェアの利用情報の交換などが可能になります。次の Web ページからアクセスします。

http://www.zonelabs.com/store/content/support/userForum/userForum_agreement.jsp

第 1 章

インストールとセットアップ

1

この章では、Zone Labs セキュリティ ソフトウェアのシステム要件、および、インストール、アップグレード、設定、アンインストールの手順について説明します。

トピック：

■ 2 ページの「システム要件とサポートされるソフトウェア」

■ 4 ページの「Zone Labs セキュリティ ソフトウェアのインストール」

■ 6 ページの「旧バージョンからのアップグレード」

■ 7 ページの「基本オプションの選択」

■ 9 ページの「Zone Labs セキュリティ ソフトウェアのアンインストール」

システム要件とサポートされるソフトウェア

このセクションでは、Zone Labs セキュリティ ソフトウェア を動作させるのに必要とされるハードウェアとソフトウェアについて説明します。

Zone Labs セキュリティ ソフトウェアに最適な解像度は、1024 x 768 以上です。800 x 600 以下の解像度では、一部のソフトウェア画面が正しく表示されないことがあります。

Zone Labs セキュリティ ソフトウェア をインストールするコンピュータに必要なシステム：

- 次のいずれかのオペレーティング システムと最小メモリが必要です。
  - Microsoft(R) Windows(R) XP、Home または Professional Edition と、128 MB のメモリ
  - Microsoft Windows 2000 Professional と、64MB のメモリ
- 50MB 以上のハードディスク空き容量
- Pentium(R) III 450Mhz 以上

メール保護がサポートしているプロトコル

- HTTP（Outlook または Outlook Express に連動する迷惑メール フィルタリング）
- IMAP4（受信のみ）－ウイルスの電子メール スキャンでは、IMAP4 をサポートしていません。
- POP3（受信のみ）
- SMTP（送信のみ）

サポートされているブラウザ ソフトウェア

- Internet Explorer 5.5、6.0 SP1、6.0 SP2
- Netscape Navigator 7.2、8.0 Beta
- FireFox 1.00 および最新版（1.02）
- Mozilla 1.4 以上
- MSN Explorer 6.0 および最新版（7.02）
- AOL 9.0

- サポートされている IM クライアント
- MSN 6.2.0205
- Windows メッセンジャ 4.7.3001
- Yahoo! IM6.0.0.1922
- Yahoo! Japan IM*6.0.0.1703

サポートされている IM クライアント

- MSN 6.2.0205
- Windows メッセンジャ 4.7.3001
- Yahoo! IM 6.0.0.1922
- Yahoo! Japan IM 6.0.0.1703

Japan Yahoo IM は、日本以外の Yahoo の ID をサポートしません。また、Japan IM は *YPagerJ.exe* という異なるプロセスを使用します。

- AOL インスタント メッセンジャ 5.9.3702
- ICQ Pro 2003b (build 3916)
- ICQ Lite 5.03 (build 2315)
- Trillian (/MSN/YIM/AIM/ICQ) 0.74i
- Trillian Pro (/MSN/YIM/AIM/ICQ) 3.1
- GAIM (/MSN/YIM/AIM/ICQ) 1.2.1
- Miranda (MSN/YIM/ICQ) 0.3.3.1

Zone Labs セキュリティ ソフトウェアのインストール

Zone Labs セキュリティ ソフトウェアのインストールおよび設定では、ソフトウェア ファイルをインストールし、設定ウィザードの実行によって基本的な保護のオプションを設定し、チュートリアルを表示します。

以前のバージョンの Zone Labs セキュリティ ソフトウェア がインストールされている場合は、インストール中にセキュリティ警告が表示されることがあります。この警告を閉じてインストールを進めるには、[OK] をクリックします。

ZoneAlarm のインストール

インストール プロセスを開始する前に、Zone Labs Web サイトから ZoneAlarm をダウンロードし、インストール ファイルを保存したコンピュータ上の場所を参照します。

1. ダウンロードしたインストール ファイルをダブルクリックします。

   インストール プログラムが起動します。

2. インストール ファイルの場所を指定するか、または［**次へ**］をクリックして続行します。

   デフォルトの場所は、*C:¥Program Files¥Zone Labs¥ZoneAlarm* です。

3. 氏名、会社名（オプション）、メール アドレスを入力し、［**次へ**］をクリックします。

4. 使用許諾契約書を読み、同意したら、［**インストール**］をクリックします。

   インストール プログラムが起動します。

5. ［**終了**］をクリックしてインストール プログラムを終了します。

6. ［**はい**］をクリックし、ZoneAlarm を起動します。

   ライセンス ウィザードが表示されます。

7. ZoneAlarm Pro の試用、または無料の ZoneAlarm を選択し、［次へ］をクリックします。

ZoneAlarm をインストールする際に、15 日間無料試用できる ZoneAlarm Pro の試用バージョンをインストールするオプションを選択できます。試用期間中は、ZoneAlarm Pro が提供する高度なセキュリティ保護機能を使用することができます。試用期間が終わったら、ZoneAlarm Pro を購入するとこ

れらの高度な機能を継続して使用できます、または ZoneAlarm に戻すことができます。ZoneAlarm Pro の試用期間が終わった後で ZoneAlarm に戻した場合、ZoneAlarm Pro で作成したカスタム設定はすべて破棄されます。

Zone Labs セキュリティ ソフトウェアのインストール

インストール操作を開始する前に、Zone Labs セキュリティ ソフトウェアの CD を CD-ROM ドライブに挿入します。Zone Labs の Web サイトからソフトウェアをダウンロードした場合は、インストール ファイルの保管場所を参照します。

Zone Labs セキュリティ ソフトウェアのインストール方法：

1. インストール ファイルをダブルクリックします。

   インストール プログラムが起動します。

2. インストール ファイルの場所を指定するか、または［**次へ**］をクリックして続行します。

   デフォルトの場所は、*C:¥Program Files¥Zone Labs¥ZoneAlarm* です。

3. 氏名、会社名（オプション）、メール アドレスを入力し、［**次へ**］をクリックします。

4. 使用許諾契約書を読み、同意したら、［**インストール**］をクリックします。

5. ［**終了**］をクリックしてインストール プログラムを終了します。

   旧バージョンからアップグレードする場合は、インストール処理を完了するために、コンピュータを再起動するようメッセージが表示されることがあります。

6. [OK] をクリックしてコンピュータを再起動するか、［**キャンセル**］をクリックします。

［キャンセル］をクリックした場合は、後でコンピュータを再起動して、インストール処理を完了してください。

旧バージョンからのアップグレード

Zone Labs セキュリティ ソフトウェア は、バージョン間で簡単にアップグレードできるようにデザインされています。通常、バージョン 6.0 にアップグレードする際に、既存のバージョンをアンインストールする必要はありません。ただし、Integrity クライアント（企業のみ）に限り、どのバージョンを使用している場合でも、アップグレードする前にアンインストールが必要になります。

アップグレードと Windows XP SP2 ファイアウォール

Windows XP SP2 の稼動中に、バージョン 6.0 にアップグレードする場合、アップグレード後に、Windows XP SP2 のインターネット接続ファイアウォールを手動で再度有効にしなければならないことがあります。Windows XP のインターネット接続ファイアウォールを有効にする方法については、Windows XP のヘルプ システムで、***ファイアウォール***を検索してください。

アップグレードおよび IMsecure myVault 設定

IMsecure または IMsecure Pro のスタンドアロン バージョンの稼動中に ZoneAlarm Security Suite にアップグレードする場合、セキュリティ上の理由から、アップグレード プログラムは米国社会保障番号、クレジット カード番号、およびアクセス PIN 番号を転送しないように設計されています。

アップグレードおよび MailFrontier 設定

MailFrontier のスタンドアロン バージョンの稼動中に ZoneAlarm Security Suite にアップグレードする場合、アップグレード処理によりアドレス帳は転送されますが、その他の MailFrontier 設定は失われることがあります。

旧バージョンからアップグレードするには、次のようにします。

1. インストール ファイルをダブルクリックします。

   インストール プログラムが起動します。

2. アップグレード オプションを選択し、[**次へ**] をクリックして、インストールを続けます。

アップグレード	このオプションを選択すると、既存のセキュリティ設定が維持され、新バージョンに適用されます。アップグレードで提供される新機能には、デフォルト設定が適用されます。
クリーン インストール	このオプションを選択すると、既存のセキュリティ設定は破棄され、デフォルトの設定が適用されます。

基本オプションの選択

インストールの完了後、設定ウィザードが表示されます。設定ウィザードはインストールの後にのみ表示されるもので、Zone Labs セキュリティ ソフトウェアの基本オプションの設定に役立ちます。設定ウィザードを使用すると、プライバシー保護、新しいネットワーク検出動作の設定、警告の設定の指定、アンチウイルス保護の有効化、およびプログラム許可の設定を行うことができます。

プログラムのアクセス許可の設定

Zone Labs セキュリティ ソフトウェア では、次のソフトウェア カテゴリに属する最も一般的なプログラムの多くを設定できます。

- インスタント メッセージング プログラム
- Web ブラウザ
- Microsoft Office
- 電子メール
- アンチウイルス
- Microsoft Windows プロセス
- 文書ユーティリティ
- Zone Labs ソフトウェア アプリケーション

プログラムに対する許可の割り当てについての詳細は、85 ページの「特定プログラムの許可の設定」を参照してください。

DefenseNet コミュニティへの参加

Zone Labs セキュリティ ソフトウェア ユーザは、DefenseNet コミュニティ保護ネットワークに参加し、Zone Labs に匿名の設定データを分析用として定期的に送信することで、Zone Labs のセキュリティ製品の今後の開発に協力することになります。DefenseNet に参加することにより、ユーザが最も頻繁に使用する機能やサービスに焦点を当てることに役立ち、より高度なセキュリティを提供する新しい機能を開発できるようになります。

ZoneAlarm または ZoneAlarm Anti-virus ユーザから設定データを収集することはありません。

［全般］|［設定］ タブで［Zone Labs のサーバに接続する前に警告する］設定を選択した場合でも、ZoneLabs に設定データを送信する前に警告は表示されません。

収集されたデータは完全に匿名が守られ、ZoneLabs の内部でのみ使用されます。外部と共有されることはありません。何百万人もの Zone Labs セキュリティ ソフトウェア ユーザのうち、情報の収集に協力しているユーザの割合は少数です。データ転送の頻度は、お使いのコンピュータの構成によって異なります。ほとんどのユーザの場合、データは 1 日に 1 回送信されます。

Zone Labs に設定データを送信するには、設定ウィザードで **[はい、自動的にかつ匿名で設定を共有します]** を選択してください。

後で匿名データの送信を停止する場合は、[Zone Labs への問い合わせ] エリアで [概要] | [設定] を選択し、[はい、設定を匿名で共有します] チェックボックスをオフにします。

Zone Labs セキュリティ ソフトウェアのアンインストール

Zone Labs セキュリティ ソフトウェア をアンインストールする場合は、Windows の［アプリケーションの追加と削除］ユーティリティではなく、インストールに含まれているアンインストール プログラムを実行します。これにより、Zone Labs セキュリティ ソフトウェアの全コンポーネントがコンピュータから削除されます。

Zone Labs セキュリティ ソフトウェア をアンインストールする際には、管理者権限を持つユーザとしてログインする必要があります。

アップグレードの際に、既存のバージョンをアンインストールする必要はありません。詳細については、4 ページの「Zone Labs セキュリティ ソフトウェアのインストール」を参照してください。

Zone Labs セキュリティ ソフトウェア をアンインストールするには、次のようにします。

1. ［スタート］|［プログラム］を選択します。
2. ［Zone Labs］|［アンインストール］を選択します。

   アンインストール プログラムが起動します。

第 2 章

Zone Labs セキュリティ ソフトウェアの基本

2

この章では、Zone Labs セキュリティ ソフトウェアの主要ツールと概念について説明します。

トピック：

■ 12 ページの「Zone Labs セキュリティ ソフトウェアコントロール センタの概要」

■ 18 ページの「ゾーンの概念」

■ 20 ページの「警告への対応」

■ 22 ページの「製品設定の指定」

■ 28 ページの「ライセンス、登録、およびサポート」

Zone Labs セキュリティ ソフトウェアコントロール センタの概要

Zone Labs セキュリティ ソフトウェア コントロール センタを使用すると、コンピュータを安全に保つためのセキュリティ機能に 1 箇所でアクセスできます。Zone Labs セキュリティ ソフトウェアの主な機能は、コントロール センタの左側のメニューに用意されています。

コントロール センタの使用法

機能を切り替えるには、まずメニューから目的の機能を選択し、次に表示するタブを選択します。

図 2-1: Zone Labs セキュリティ ソフトウェアのコントロール センタ

メニュー バー
メニュー バーから、使用可能なパネルにアクセスできます。各パネルのツールは、複数のタブで構成されています。

タブ セレクタ
タブ セレクタをクリックして、表示したいタブを前面に表示します。

[概要] パネルを除き、コントロール センタの各パネルには、[メイン] タブとその他 1 ～ 2 個のタブが含まれています。[メイン] タブには、そのパネルのグローバル コントロールが表示されます。

テキストの表示／非表示
このリンクをクリックし、選択したタブの説明テキストを表示または非表示にすることができます。このテキストは、タブおよびそのコントロールに関する簡潔な説明です。

[ヘルプ] ボタン
パネルの各コントロールのヘルプが必要な場合は、右上にある [ヘルプ] リンクをクリックします。Zone Labs セキュリティ ソフトウェアのオンライン ヘルプ システムから、該当するタブのヘルプ トピックを表示できます。

ダッシュボードの使用
ダッシュボードを使用すると、基本的なセキュリティ インジケータおよび機能にアクセスすることができます。ダッシュボードは、各パネルの上部に表示されます。

図 2-2: Zone Labs セキュリティ ソフトウェアのダッシュボード

外部から／外部への通信インジケータ
通信インジケータは、そのコンピュータでの通信の送受信を示します。送信の場合は赤色、受信の場合は緑色で表示されます。このインジケータは、違法な通信やセキュリティ問題が発生していることを意味するものではありません。

アプリケーションの中には、バックグラウンドでネットワークのリソースにアクセスするものもあります。そのため、意識的にインターネットにアクセスしていない場合でも、ネットワーク通信が表示される場合があります。

［停止］ボタン
［停止］ボタンをクリックすると、インターネット アクセスなどのネットワーク アクティビティすべてが即座にブロックされます。ダッシュボードの［停止］ボタンをクリックすると、コンピュータ上のインターネット通信の送受信すべてが直ちに停止されます。そのため、［停止］ボタンはコンピュータが攻撃されていると思われる場合にのみクリックするようにします。いったん［停止］ボタンをクリックすると、Zone Labs セキュリティ ソフトウェアは、アクセスを必要とする正当なプログラムの他、*DHCP（動的ホスト構成プロトコル）*メッセージや、インターネット接続の維持に使用される ISP の *ハートビート メッセージ* もブロックする可能性があります。アクセスを再開するには、もう一度［**停止**］ボタンをクリックします。

インターネット ロック
インターネット ロックは、*パスロック*許可を与えられたプログラムによって開始された通信を除き、すべての通信を停止します。［インターネット ロック］をクリックすると、DHCP メッセージや、インターネット接続の維持に使用される ISP ハートビートが即座にブロックされます。その結果、インターネット接続が切断されることもあります。アクセスを再開するには、［**インターネット ロック**］ボタンを再びクリックします。

システム トレイ アイコンを右クリックし、ショートカット メニューの［すべてのインターネット接続の停止］または［インターネット ロックの開始］を選択することによっても、［停止］ボタンと［インターネット ロック］を有効にできます。

ネットワーク インジケータ
ネットワーク インジケータは、トラスト ゾーンまたはインターネット ゾーンのいずれかで有線またはワイヤレスのネットワークを使用している場合に表示されます。

ネットワークのシンボルをクリックすると、ネットワークの設定を保存する［ゾーン］タブを直接表示できます。

［アクティブなプログラム］エリア
［アクティブなプログラム］エリアには、現在のセッションでインターネットにアクセスした、実行中のプログラムのアイコンが表示されます。ここに表示されているプログラムの詳細を表示するには、マウス ポインタでアイコンをポイントします。

プログラムがデータを送受信している間、アイコンが点滅します。

アイコンの下に手のイメージが表示されている場合は、プログラムがサーバとして動作していて、接続要求を待ち受けていることを示します。

［システム］エリア
ここには 2 つのメッセージが表示されます。

- システムはアクティブです

  Zone Labs セキュリティ ソフトウェアが正常に機能していることを示します。

■ エラー： 再起動してください

基礎的なセキュリティ プロセスが実行されていないため、ご使用のコンピュータが Zone Labs セキュリティ ソフトウェアによって保護されていないことを示します。Zone Labs セキュリティ ソフトウェアをリセットするためにコンピュータを再起動してください。

システム トレイ アイコン

システム トレイに表示されるアイコンを利用すると、数回クリックするだけで簡単にセキュリティ状態やインターネット接続を監視したり、セキュリティ設定にアクセスしたりできます。

アイコン	説明
	Zone Labs セキュリティ ソフトウェア がインストールされていて、実行中です。
	ご使用のコンピュータは、ネットワーク通信を送信中（赤色）または受信中（緑色）です。これらの色は、セキュリティ上の問題やネットワーク通信の危険性を意味するものではありません。
	Zone Labs セキュリティ ソフトウェアは通信をブロックしましたが、ユーザの設定によりフルサイズの警告は表示されません。
	（黄色のロック）インターネット ロック機能が適用されています。
	（赤いロック）［停止］ボタンが適用されています。多数の警告が表示されることがあります。

表 2-3: システム トレイ アイコン

ショートカットメニュー

システム トレイ アイコンを右クリックするとショートカット メニューを使用できます。

インターネット ロックの開始

このメニュー オプションはインターネット ロックを開始し、システム トレイに黄色のロック アイコンが表示されます。プログラムによって開始され、パスロック許可を持たない、すべてのインターネット通信はブロックされます。ダッシュボード上の［インターネット ロック］をクリックした場合と同じ機能を提供します。

すべてのインターネット通信の停止

このメニュー オプションは停止処理を開始し、システム トレイに赤のロック アイコンが表示されます。すべてのインターネット通信はブロックされます。ダッシュボード上の［停止］ボタンをクリックした場合と同じ機能を提供します。

バージョン情報

インストールした Zone Labs セキュリティソフトウェアのバージョン情報とドライバおよびエンジンの情報が表示されます。ソフトウェアで問題が

発生する場合は、この情報をクリップボードにコピーし、電子メールに貼り付けた後でサポートに送信できます。

コントロール センタのリストア
Zone Labs セキュリティソフトウェア コントロール センタをフル サイズにリストアします。このメニュー オプションのラベルはインストールした Zone Labs セキュリティソフトウェアのバージョンを反映します（たとえば、Zone Labs Anti-virus または ZoneAlarm Security Suite など）。

シャットダウン
Zone Labs セキュリティソフトウェア のアプリケーションを終了する。このメニュー オプションのラベルはインストールした Zone Labs セキュリティソフトウェアのバージョンを反映します（たとえば、Zone Labs Anti-virus または ZoneAlarm Security Suite など）。

［状況］タブの使用

［状況］タブの［保護］エリアは、セキュリティ設定が有効に設定されているかどうかを示し、セキュリティ アクティビティの要約を表示します。［状況］タブを使用して以下の操作を行うことができます。

- コンピュータの安全性を簡単に確認
- Zone Labs セキュリティ ソフトウェアの動作状況の要約を確認
- Zone Labs セキュリティ ソフトウェアのバージョンが最新かどうかを確認
- 製品チュートリアルにアクセス

ここに表示される警告数をリセットするには、パネルの下部で**［デフォルトに戻す］**をクリックします。

ブロックした侵入
Zone Labs セキュリティ ソフトウェアのファイアウォールおよび MailSafe 機能が保護を実行した回数と、*ポート*の数を示します。

外部からの保護
ファイアウォールが有効になっているかどうかを知らせ、前回のリセット以降に発生したファイアウォール警告、MailSafe 警告、およびインターネットロック警告の数を示します。警告が表示された場合、警告の下線付きテキストをクリックすると、その設定を変更できるパネルが表示されます。

外部への保護
プログラム コントロールが安全に設定されているかどうかを知らせ、前回のリセット以降に発生したプログラム警告の数を示します。プログラム コントロールが無効になっていると、Zone Labs セキュリティ ソフトウェアが警告を表示します。

アンチウイルス製品のモニタリング
コンピュータがウイルスに対して保護されているかどうかを示し、これまで処理されたウイルスの数を表示します。アンチウイルス保護のステータ

スは、ZoneAlarm Anti-virus と ZoneAlarm Security Suite をご使用の場合のみ表示されます。ZoneAlarm または ZoneAlarm Pro をご使用の場合は、代わりにアンチウイルス モニタリングのステータスが表示されます。

［メールの保護］エリア
MailSafe が有効になっているかどうかを知らせ、前回のリセット以降に隔離された添付ファイルの数を示します。警告が表示された場合、警告の下線付きテキストをクリックすると、その設定を変更できるパネルが表示されます。

アンチウイルス／アンチスパイウェア
ウイルスおよびスパイウェア保護が有効かどうかを示し、これまで処理されたウイルスとスパイの数を表示します。

IM セキュリティ保護
インスタント メッセージング保護が有効かどうかを示し、これまで処理されたメッセージの数を表示します。

アップデートとチュートリアル情報
Zone Labs セキュリティ ソフトウェアの購入時に、1 年間有効な自動アップデート サービスが提供されます

アップデート ボックスで、お使いのバージョンが Zone Labs セキュリティ ソフトウェアの最新版かどうかを確認し、アップデートの提供時にはアップデート版に簡単にアクセスできます。

メッセージ	意味
アップデートの確認。	このリンクをクリックし、Zone Labs セキュリティソフトウェアの重要なアップデートがダウンロード用に提供されているかどうかを確認できます。
アップデートが利用可能です。	自動アップデート サービスは、Zone Labs セキュリティ ソフトウェアのアップデートが提供されていることを示しています。リンクをクリックし、Zone Labs Web サイトからアップデートをダウンロードします。
ファイアウォールは最新版です。	お使いの Zone Labs セキュリティ ソフトウェアは最新版です。
アップデート サービスの有効期間が終了しました。クリックして更新してください。	自動アップデート サービスの有効期間が終了しました。サービスを更新するには、Zone Labs Web サイトへのリンクをクリックします。

表 2-4: アップデート メッセージ

Zone Labs セキュリティ ソフトウェア 基本動作を学習するには、**［チュートリアル］**をクリックします。

ゾーンの概念

Zone Labs セキュリティ ソフトウェアは、ゾーンと呼ばれる仮想コンテナを使って、インターネット上の善、悪、未知の通信相手の動向を記録し、お使いのコンピュータに接続するコンピュータとネットワークを分類します。

*インターネット ゾーン*は、「未知」の通信相手を意味します。他のゾーンに指定されない限り、世界中のコンピュータやネットワークがこのゾーンに属します。

*トラスト ゾーン*は、「善」の通信相手を意味します。このゾーンには、ローカル ネットワーク上または家庭用ネットワーク上のマシンなど、信頼でき、リソースの共有対象となるコンピュータやネットワークが属します。

ブロック ゾーン は、「悪」の通信相手を意味します。信頼できないコンピュータやネットワークはこのゾーンに属します。

他のコンピュータからお使いのコンピュータへの通信が要求されると、対応を決定するにあたり、Zone Labs セキュリティ ソフトウェアはそのゾーンを確認します。

コンピュータ、ネットワーク、プログラムをトラスト ゾーンに追加する方法については、52 ページの「通信ソースの管理」を参照してください。

ファイアウォール セキュリティを管理するゾーン

Zone Labs セキュリティ ソフトウェアは、セキュリティ レベルにより、各ゾーンからの通信を許可すべきか、ブロックすべきかを判断します。[ファイアウォール] パネルの [メイン] タブを使って、セキュリティ レベルの表示と変更を行います。

「高」セキュリティ設定

「高」セキュリティでは、コンピュータは*ステルス モード*になり、ハッカーから認識されなくなります。インターネット ゾーンのデフォルト設定は「高」セキュリティです。

「高」セキュリティでは、ファイルやプリンタの共有は無効になりますが、外部への DNS、外部への DHCP、およびブロードキャスト / マルチキャストは許可されるので、インターネットを使用することは可能です。アクセス許可やサーバ許可を与えられたプログラムが使用する場合を除き、コンピュータ上のすべてのポートが閉じられます。

「中」セキュリティ設定

〝中〟セキュリティでは、コンピュータは*コンポーネントの学習モード*になります。このモードでは、Zone Labs セキュリティ ソフトウェアは、多数の警告を表示してユーザの作業を中断することなしに、頻繁に使用される各

コンポーネントの MD5 署名をすばやく学習します。トラスト ゾーンのデフォルト設定は「中」セキュリティです。

「中」セキュリティでは、ファイルとプリンタの共有が有効になり、すべてのポートおよびプロトコルが許可されます。(「中」セキュリティがインターネット ゾーンに適用される場合、外部からの NetBIOS 通信はブロックされます。これにより、Windows ネットワーキング サービスに対する攻撃から、コンピュータが保護されます。)「中」セキュリティでは、ステルス モードは適用されません。

Zone Labs セキュリティ ソフトウェアのインストール後、普通に使用し始めてから数日間は、″中″ 設定を使用することをお勧めします。インターネットを数日間使用すると、Zone Labs セキュリティ ソフトウェアはインターネット アクセス プログラムが使用するコンポーネントの大半の署名を認識できるようになり、プログラム認証レベルを ″高″ に変更するように勧めるメッセージを表示します。

ブロック ゾーンではいかなる通信の送受信も許可されないため、セキュリティ レベルを設定する必要はありません。

上級レベルのユーザは、特定のポートをブロックまたは許可することで、各ゾーンの「高」および「中」セキュリティをカスタマイズできます。詳細については、56 ページの「ポートのブロックおよびブロック解除」を参照してください。

プログラム コントロールを提供するゾーン

プログラムが *アクセス許可* あるいは *サーバ許可* を要求しているということは、そのプログラムが特定のゾーン内のコンピュータまたはネットワークとの通信を試みているということです。各プログラムに対して、次の許可を与えたり拒否したりできます。

- トラスト ゾーンへのアクセス許可
- インターネット ゾーンへのアクセス許可
- トラスト ゾーンへのサーバ許可
- インターネット ゾーンへのサーバ許可

トラスト ゾーンへのアクセス許可またはサーバ許可を与えると、そのプログラムは、トラスト ゾーンに追加されているコンピュータやネットワークとのみ通信できるようになります。これは安全性の高い方法です。プログラムが改変された場合や、不注意で許可を与えてしまった場合でも、限られた数のネットワークやコンピュータとしか通信できません。

インターネット ゾーンへのアクセス許可またはサーバ許可を与えると、そのプログラムはあらゆるコンピュータやネットワークと通信できるようになります。

上級レベルのユーザは、特定のプログラムが使用できるポートとプロトコル、アクセス可能なホスト、およびその他の詳細を指定できます。詳細については、96 ページの「プログラム用のエキスパート ルールの作成」を参照してください。

警告への対応

Zone Labs セキュリティ ソフトウェアを始めて起動すると、多くの警告が表示されることがありますが、しかし、心配は無用です。これらの警告は、ハッカーの攻撃に対するものではありません。Zone Labs セキュリティ ソフトウェアがプログラムとネットワーク設定を確認し、ユーザのニーズに合わせてセキュリティを設定する機会を提供するために、これらの警告は表示されます。

警告への対応方法は、表示される警告の種類によって異なります。特定の警告に対応する方法については、221 ページから始まる付録 A「警告のリファレンス」を参照してください。

新しいプログラム警告

初期に表示される警告のほとんどが、新しいプログラム警告です。これらの警告は、コンピュータ上のプログラムがインターネットまたはローカル ネットワークに対するアクセス許可やサーバ許可を要求したときに表示されます。新しいプログラム警告を使って、プログラムが必要とするブラウザやメールなどへのアクセス許可を与えることができます。

［選択した結果を保存する］というチェックボックスをオンにすると、信頼できるプログラムに永久的な許可を与えることができます。

正常に機能するためにサーバ許可を必要とするプログラムやプロセスの数は多くありません。ただし、なかには正当な機能を実行するために Microsoft Windows によって使用されるプロセスもあります。警告に表示される可能性がある一般的なプログラムまたはプロセスは、次のとおりです。

- lsass.exe
- spoolsv.exe
- svchost.exe
- services.exe

■ winlogon.exe

サーバ許可を要求しているプログラムまたはプロセスを識別できない場合は、Microsoft Support Web サイト（http://support.microsoft.com/）で、プロセスに関する情報を検索して、その内容と用途を調べてください。上にリストしたプロセスを含む多くの正当な Windows プロセスは、ワームおよびウイルスを偽装するためにハッカーによって使用されたり、またはトロイの木馬にシステムへのバックドア アクセスを提供したりする可能性があることに注意してください。警告が表示されたときに（ファイルの参照、ネットワークへのログオン、またはファイルのダウンロードなどの）機能を実行していなかった場合は、サーバ許可を拒否することが最も安全な方法です。いつでも、[プログラム一覧] から特定のプログラムおよびサービスに許可を割り当てることができます。この一覧を開くには、**[プログラム コントロール]**|**[プログラム]** タブを選択します。

新しいプログラム警告と対応方法の詳細については、228 ページの「新しいプログラム警告」を参照してください。

新しいネットワークおよび VPN 警告

当初に表示される警告には、新しいネットワーク警告や VPN 設定警告があります。Zone Labs セキュリティ ソフトウェアがネットワークの接続または VPN 接続を検出した場合に、これら警告が表示されます。これらの警告により、ネットワーク上で安全に作業ができるよう、トラスト ゾーン、ポート / プロトコルの許可、プログラム許可を適切に設定できます。これら警告と対応方法の詳細については、221 ページから始まる付録 A「警告のリファレンス」を参照してください。

製品設定の指定

［設定］タブを使って次のことを行います： Zone Labs セキュリティ ソフトウェアのパスワードの設定と変更、ログインまたはログアウトの設定、アップデートの管理、Zone Labs セキュリティ ソフトウェアのコントロール センタの表示用全般オプションの設定、Zone Labs に連絡する際のプライバシー設定の指定。

アップデート オプションの設定

Zone Labs セキュリティ ソフトウェアの購入時に、1 年間の無料アップデート サービスが提供されます。アップデートは、手動で確認することもできますし、Zone Labs セキュリティ ソフトウェアにより自動的に確認することもできます。

アップデートの確認を設定するには、次のようにします。

1. **［概要］|［設定］**を選択します。
2. ［アップデートの確認］エリアで、アップデートのオプションを指定します。

自動	アップデートが提供されていると、Zone Labs セキュリティ ソフトウェアが自動的に通知します。
手動	［状況］タブでアップデートを確認します。アップデートの確認をすぐに開始するには、［アップデートの確認］をクリックします。

パスワードの設定

パスワードを設定することで、自分以外のユーザが Zone Labs セキュリティ ソフトウェアをシャットダウンしたりアンインストールしたり、セキュリティ設定を変更しようとするのを防ぐことができます。パスワードを設定しても、ご使用のコンピュータから他のユーザがインターネットにアクセスすることを防ぐことはできません。

ZoneAlarm では、パスワードの作成機能は使用できません。

管理者がインストール パスワードを使用して Zone Labs セキュリティ ソフトウェアをインストールした場合、その管理者はすべての機能にアクセスすることができます。

初めてパスワードを設定する際には、コンピュータを離れる前に必ずログアウトするようにしてください。ログアウトしないと、他のユーザが設定を変更することができます。

Zone Labs セキュリティ ソフトウェアのパスワードを設定または変更するには：

1. **［概要］|［設定］**を選択します。
2. **［パスワードの設定］**をクリックします。

3. 表示されるフィールドに、パスワードを入力し、確認のためもう一度入力します。
4. ［他のユーザがパスワードなしにプログラムを使用することを許可する（プログラム許可が「ブロック」に設定されていない場合のみ）］を ëlëš して、明示的にはブロックしていないプログラムは、パスワードを持っていないユーザでも使用できるように許可することができます。
5. ［OK］をクリックします。

有効なパスワードの文字数は 6 ～ 31 文字で、A ～ Z、a ～ z、0 ～ 9 の英数字、および !、@、#、$、%、^、&、* の記号を使用することができます。

パスワードの設定後に、設定の変更、TrueVector セキュリティ エンジンの終了、Zone Labs セキュリティ ソフトウェアのアンインストールを行う場合は、ログインする必要があります。

セキュリティ設定のバックアップとリストア

既存のセキュリティ設定を XML ファイルにバックアップして、後で必要に応じてリストアすることができます。

バックアップとリストアの機能は、異なるコンピュータ間で設定を共有したり、セキュリティ ポリシーを配布したりするために使用すべきではありません。このような用途で使用すると、それぞれのコンピュータ、アプリケーション、Windows プロセスには差異があるため、極めて多数の警告が表示されることがあります。

バックアップおよびリストアの設定機能は、ZoneAlarm Pro および ZoneAlarm Security Suite でのみ使用できます。

セキュリティ設定をバックアップするには、次のようにします。

1. **［概要］**|**［設定］**を選択します。
2. ［バックアップとリストア セキュリティ設定］エリアで、**［バックアップ］**をクリックします。
3. ファイル名を入力するか、または既存のファイルを選択して上書きします。
4. **［保存］**をクリックします。

セキュリティ設定をバックアップまたはリストアするには、次のようにします。

1. **［概要］**|**［設定］**を選択します。

2. ［バックアップとリストア セキュリティ設定］エリアで、**［リストア］**をクリックします。
3. 使用する設定を含んでいる XML ファイルを選択します。
4. **［開く］**をクリックします。

全般的な製品設定の指定

デフォルトでは、コンピュータを起動すると、Zone Labs セキュリティ ソフトウェアが自動的に開始します。これらのオプションを変更するには、［全般］エリアの設定を使用します。

全般的な表示設定を指定するには、次のようにします。

1. **［概要］**|**［設定］**を選択します。
2. ［全般］エリアで、設定を指定します。.

Zone Labs セキュリティ ソフトウェアをスタートアップ時に起動する	コンピュータを起動すると、Zone Labs セキュリティ ソフトウェアが自動的に開始します。
Zone Labs セキュリティ ソフトウェア クライアントを保護する	トロイの木馬による Zone Labs セキュリティ ソフトウェアへのキーボードとマウスのリクエストを阻止します。 注意：最大のセキュリティを維持するためには、リモート アクセス プログラムを使用する際にキーボードとマウスの操作に**問題が生じる場合に限って**この機能を無効にしてください。

3. ［全般］エリアで、**［オプション］**をクリックします。

［オプション］ダイアログ ボックスが表示されます。

4. ［表示設定］エリアで、表示設定を選択します。

最後に表示したタブを記憶	コントロール センタを前回終了した際に表示されていた Zone Labs セキュリティ ソフトウェアのタブを開きます。
スキンの色	コントロールセンタにおける配色のデフォルトを変更できるよう許可します。ZoneAlarm では、追加色を選択することはできません。

5. ［プロキシ設定］エリアでは、必要があることが確かな場合にのみ、プロキシ サーバ情報の IP アドレスを入力します。

Zone Labs セキュリティ ソフトウェア は、Internet Explorer で指定される設定など、ほとんどのプロキシ設定を自動的に検出するため、ここで情報を入力する必要はありません。プロキシ情報を入力する必要があるのは、スクリプトによるプロキシのように一般的でないプロキシ設定を行っている場合や、アンチウイルスのアップデートやインスタント メッセージングなど、一部の製品機能が動作していない場合に限られます。

連絡設定の指定

連絡設定により、Zone Labs セキュリティ ソフトウェアが Zone Labs と通信する際のユーザのプライバシーが保護されます（たとえば、アップデートの自動確認など）。

連絡設定を指定するには、次のようにします。

1. **［概要］|［設定］**を選択します。
2. ［Zone Labs への問い合わせ］エリアで、設定を指定します。

ZoneLabs のサーバに接続する前に警告する	Zone Labs に問い合わせて、登録情報の配信、製品アップデートの取得、警告の調査などをおこなったり DNS にアクセスして IP アドレスを調べる前に、警告を表示します。 **注意**：特定の状況では、接続が行われる前に通知されないことがあります。この状況には、DefeneseNet データを Zone Labs に送信する場合、プログラムのアドバイスを入手するために Zone Labs に接続する場合、アンチウイルスのアップデートが実行される場合、またはアンチウイルス ステータスをモニタリングしている場合などがあります。以下の［設定を匿名で共有］設定は、DefenseNet 転送をオフにします。その他のすべての設定は、それぞれのパネルの［メイン］タブから無効にできます。
必要に応じて IP アドレスを隠す	Zone Labs, LLC. に接続する際にコンピュータが識別されることを防止します。
必要に応じてローカル IP アドレスの最後の桁を隠す	Zone Labs, LLC. に接続する際に、IP アドレスの末尾の部分が省略されます（例、123.456.789.XXX）。
セキュリティ設定を Zone Labs と匿名で共有します	定期的に匿名の設定データを Zone Labs に送信します。詳細については、7 ページの「DefenseNet コミュニティへの参加」を参照してください。 注意：ZoneAlarm または ZoneAlarm Anti-virus ユーザから設定データを収集することはありません。

製品表示とプロキシ サーバのオプションの設定

［オプション］ダイアログ ボックスを使用して、表示設定のオプションおよびプロキシ サーバの情報を指定することができます。

製品表示とプロキシのオプションを指定するには、次のようにします。

1. **［概要］**|**［設定］**を選択します。
2. **［全般］**エリアで、**［オプション］**をクリックします。

   ［オプション］ダイアログ ボックスが表示されます。
3. ［表示］設定エリアで、設定を指定します。

パネル内で最後に表示したタブを記憶する	コントロール センタを開くと、Zone Labs セキュリティ ソフトウェアでは前回終了した際に表示されていたパネルとタブが表示されます。
スキンの色	コントロールセンタにおける配色のデフォルトを変更できるよう許可します。ZoneAlarm では、追加色を選択することはできません。

4. 必要に応じて、プロキシ サーバの情報を入力します。

Zone Labs のセキュリティ ソフトウェアは、ほとんどのプロキシ設定を自動的に検出するため、Internet Explorer などで設定されている場合などでは、ここで情報を入力する必要がありません。プロキシ情報を入力する必要があるのは、スクリプトによるプロキシのように一般的でないプロキシ設定を行っている場合や、アンチウイルスのアップデートなど一部の製品機能が動作しない場合に限られます。

オンライン詐称保護プロファイルの作成

eBay ユーザの場合は、オンライン認証情報を Zone Labs セキュリティ ソフトウェア に保存することで、オンライン詐称から保護することができます。Zone Labs セキュリティ ソフトウェア は、必ず認可された eBay の送信先にのみ送信が行われるようにすることで、プロファイルを保護します。

ZoneAlarm および ZoneAlarm Anti-virus でオンライン保護プロファイルを作成するには、次のようにします。

1. **［概要］**|**［設定］**を選択します。
2. ［eBay 保護プロファイル］エリアで、**［パスワード］**をクリックします。

   ［Alliance Partner パスワード］ダイアログが表示されます。
3. ［Alliance Partner］ドロップダウン リストから、［eBay］を選択します。
4. ［パスワード］フィールドおよび［パスワードの確認入力］フィールドに eBay パスワードを入力し、**［OK］**をクリックします。

eBay パスワードを ZoneAlarm Pro または ZoneAlarm Security Suite に入力する：

1. **[ID ロック]**｜**[myVAULT]** を選択し、次に **[追加]** をクリックします。

   [myVAULT に情報を追加] ダイアログが表示されます。

2. 項目の説明を入力し、次に [カテゴリ] ドロップダウン リストから **[eBay パスワード]** を選択します。

3. [パスワード] フィールドおよび [パスワードの確認入力] フィールドに eBay パスワードを入力し、**[OK]** をクリックします。

   データを入力した箇所にはアスタリスクが表示され、暗号化された eBay パスワードが VAULT に保存されます。元の情報は、コンピュータ上には保存されません。

4. Web またはメールを使用する際に情報を保護するかどうかを指定します。

5. **[OK]** をクリックし、変更を保存します。

   Zone Labs セキュリティ ソフトウェア が、どのようにパスワードなどの個人データを安全に保護するかについての詳細は、187 ページから始まる第 10 章「データの保護」を参照してください。

ライセンス、登録、およびサポート

Zone Labs セキュリティ ソフトウェアのサポートを利用し、アップデートを入手するには、有効なライセンスが必要です。

製品ライセンスのアップデート

評価版またはベータ版のライセンス キーを使用している場合や、評価版またはベータ版が期限切れになりそうな場合、Zone Labs から製品版のライセンスを購入することができます。

ライセンスを購入するには、次のようにします。

1. **[概要]**|**[製品情報]** を選択します。
2. [ライセンス情報] エリアで、**[購入する !]** をクリックします。

   Zone Labs Web サイトが表示され、製品版を購入できます。

ライセンス キーを変更するには、次のようにします。

1. **[概要]**|**[製品情報]** を選択します。
2. [ライセンス情報] エリアで、**[キーの変更]** をクリックします。

   [ライセンス情報] ダイアログが表示されます。
3. 表示される入力欄に、ライセンス キーを入力または貼り付けます。
4. **[適用]** をクリックし、[OK] をクリックします。

Zone Labs セキュリティ ソフトウェアの登録

Zone Labs セキュリティ ソフトウェア を登録すると、Zone Labs からセキュリティ ニュースを受け取ることができます。

Zone Labs セキュリティ ソフトウェアを登録するには：

1. **[概要]**|**[製品情報]** を選択します。
2. [登録] 部分で **[登録の変更]** をクリックします。

   [登録情報] ダイアログが表示されます。
3. 各フィールドに氏名、会社名、メール アドレスを入力します。

ここで入力するメール アドレスを使ってアウトバウンド MailSafe 保護が設定されます。正しいメール アドレスを入力するよう注意してください。詳細については、134 ページの「アウトバウンド MailSafe 保護オプションの設定」を参照してください。

4. 製品ニュースとアップデートの受信を希望する場合は、**[重要なアップデートやニュースを通知する]** チェックボックスをチェックします。

5. [OK] をクリックします。

登録情報を変更するには：

[概要]|[製品情報] を選択し、次に [登録の変更] をクリックします。

テクニカル サポートへのアクセス

テクニカル サービスの利用資格があるユーザは、Zone Labs セキュリティ ソフトウェア から直接 FAQ と既知の問題などのサポート リソースにアクセスできます。

サポート リソースにアクセスするには、次のようにします。

1. **[概要]|[製品情報]** を選択します。
2. [サポートとアップデート情報] エリアで、**[ここをクリック]** のリンクをクリックします。

   ZoneAlarm Pro の Web サイトが表示されます。
3. **[サービスお問い合わせ]** のリンクをクリックし、サポートが必要な製品を選択します。

第 3 章

Zone Labs セキュリティ ソフトウェア を使ったネットワーキング

3

家庭用ネットワーク、企業内ローカル エリア ネットワーク (LAN)、仮想プライベート ネットワーク (VPN) またはワイヤレス ネットワークにコンピュータが接続されている場合、高度なセキュリティを維持しながら、スムーズなネットワーク通信を実現することが望まれます。ネットワーク設定ウィザード、自動 VPN 設定、およびその他の Zone Labs セキュリティ ソフトウェア 機能を活用すれば、ネットワーク環境をすばやく設定することができます。

トピック：

- 32 ページの「新しいネットワーク接続の設定」
- 35 ページの「ネットワーク サービスとの統合」
- 37 ページの「VPN 接続の設定」

新しいネットワーク接続の設定

ご使用のコンピュータをネットワークに接続する場合、そのネットワークをトラスト ゾーンまたはインターネットゾーンのどちらに加えるかを判断する必要があります。

ネットワークをトラスト ゾーンに追加すると、ファイル、プリンタ、その他のリソースをネットワーク上のコンピュータと共有することができます。家庭用 ネットワークや企業内 LAN などの既知の信頼できるネットワークと既知の保護されているワイヤレス ネットワークはトラスト ゾーンに追加します。

ネットワークをインターネット ゾーンに追加すると、そのネットワーク上の他のコンピュータとリソースの共有はできませんが、リソース共有に伴うセキュリティ上のリスクからユーザのコンピュータを保護します。未知のネットワークとほとんどのワイヤレス ネットワーク（セキュリティ保護されたワイヤレス ネットワークであっても）はインターネット ゾーンに追加します。

ネットワーク設定ウィザードでは、検出された LAN ネットワークがパブリックかプライベートか判断されるため、それを参考にしてネットワークの追加先のゾーンを決定することができます。ワイヤレス ネットワーク設定ウィザードでは、検出されたワイヤレス ネットワークが保護されているか保護されていないかが判断されるため、それを参考にしてネットワークの追加先のゾーンを決定することができます。

- ワイヤレス ネットワーク設定ウィザードの無効化

ネットワーク設定ウィザードの使用

お使いのコンピュータが新しいネットワークに接続すると、Zone Labs セキュリティ ソフトウェア は、ネットワーク設定ウィザードを開き、検出されたネットワークの IP アドレスを表示します。

ネットワークの IP アドレスを基に、*プライベート ネットワーク*か、*パブリック ネットワーク*かが判別されます。

通常、プライベート ネットワークは家庭または企業内のローカルエリア ネットワーク（LAN）を意味します。デフォルトでは、プライベート ネットワークは*トラスト ゾーン*に追加されます。

パブリック ネットワークは通常、ISP などと関連した比較的大きなネットワークを意味します。デフォルトでは、パブリック ネットワークは*インターネット ゾーン*に追加されます。

ネットワーク設定ウィザードでネットワーク接続を設定するには、次のようにします。

1. ネットワークを追加するゾーンを選択し、[**次へ**] をクリックします。

2. ネットワークに名前を付けます。ここで入力する名前は、[ファイアウォール] パネルの [ゾーン] タブに表示されます。

ネットワーク設定ウィザードを使用しない場合は、ウィザード画面の [キャンセル] をクリックします。新しいネットワーク警告が表示されます。検出されたネットワークは、プライベート ネットワークであっても、インターネット ゾーンに追加されます。新しいネットワーク警告の使用に関する詳細は、240 ページの「新しいネットワーク警告」を参照してください。

ネットワーク設定ウィザードの無効化

デフォルトでは、ネットワーク設定ウィザードが有効に設定されています。新しいネットワーク警告を使ってネットワークの設定を行う場合は、ネットワーク設定ウィザードを無効にすることができます。

ネットワーク設定ウィザードを無効にするには、次のようにします。

- ウィザードのスクリーン 4 で、[新しいネットワークが検知された際にこのウィザードを表示しない] チェックボックスをオンにし、[終了] をクリックします。

ワイヤレス ネットワーク設定ウィザードの使用

お使いのコンピュータが新しいワイヤレス ネットワークに接続すると、Zone Labs セキュリティ ソフトウェア は、ワイヤレス ネットワーク設定ウィザードを開き、検出されたネットワークの IP アドレスを表示します。

ワイヤレス アクセス ポイントの WEP (Wireless Encryption Protocol) 設定は、*保護されている*ワイヤレス ネットワークか、*保護されていない*ワイヤレス ネットワークか判別するために使用されます。

保護されているワイヤレス ネットワークは WEP が有効です。WEP は初期防壁を提供しますが、ハッカーは容易に侵入が可能です。ネットワークを真に保護するためには、ワイヤレス アクセス ポイントに制限されたアクセス リストや SSID (Service Set Identifier) ブロードキャストの無効化など、他の機能を実装する必要があります。ワイヤレス ネットワークの配置は、高いレベルのセキュリティを備えていることがわかっており、*トラスト ゾーン*でリソースや印刷の共有を行う必要がある場合にのみ行います。

セキュリティ保護されていないワイヤレス ネットワークは完全に保護されず、誰でもアクセスできる状態の場合があります。デフォルトでは、保護されていないネットワークは*インターネット ゾーン*に追加されます。

ワイヤレス接続を設定するには、次のようにします。

1. ネットワークを追加するゾーンを選択し、[**次へ**] をクリックします。

2. ネットワークに名前を付けます。

設定ウィザードで入力する名前は、[ファイアウォール] パネルの [ゾーン] タブに表示されます。

ネットワーク設定ウィザードを使用しない場合は、ウィザード画面の [キャンセル] をクリックします。新しいネットワーク警告が表示されます。検出されたネットワークは、保護されているワイヤレス ネットワークであっても、インターネット ゾーンに追加されます。新しいネットワーク警告の使用に関する詳細は、240 ページの「新しいネットワーク警告」を参照してください。

ワイヤレス ネットワーク設定ウィザードの無効化

デフォルトでは、ネットワーク設定ウィザードが有効に設定されています。新しいネットワーク警告を使ってネットワークの設定を行う場合は、ネットワーク設定ウィザードを無効にすることができます。

ワイヤレス ネットワーク設定ウィザードを無効にするには、次のようにします。

ウィザードのスクリーン 4 で、[新しいネットワークが検知された際にこのウィザードを表示しない] チェックボックスをオンにし、[終了] をクリックします。

ネットワーク サービスとの統合

家庭用ネットワークまたはビジネス ネットワーク上で作業している場合は、ファイル、ネットワーク プリンタ、およびその他のリソースをネットワーク上の他のユーザと共有し、また、ネットワークのメール サーバを介してメールの送受信を行うことができます。ここでは安全にリソースを共有する方法を説明します。

ファイルおよびプリンタの共有の有効化

ネットワーク上の他のコンピュータとの間でプリンタやファイルを共有する場合は、リソース共有の対象となるコンピュータへのアクセスを許可するように Zone Labs セキュリティ ソフトウェア を設定する必要があります。

Zone Labs セキュリティ ソフトウェア でファイルとプリンタの共有を許可するには、次のようにします。

1. ネットワークのサブネット（または小規模なネットワーク環境では共有している各コンピュータの IP アドレス）をトラスト ゾーンに追加します。

   53 ページの「トラスト ゾーンへの追加」を参照してください。

2. トラスト ゾーンのセキュリティ レベルを［中］に設定します。これにより、信頼するコンピュータが共有ファイルにアクセスできるようになります。

   45 ページの「ゾーンのセキュリティ レベルの設定」を参照してください。

3. インターネット ゾーンのセキュリティ レベルを［高］に設定します。これにより、信頼できないマシンからご使用のコンピュータが認識されなくなります。

   45 ページの「ゾーンのセキュリティ レベルの設定」を参照してください。

ネットワーク メール サーバへの接続

メール クライアントにインターネット アクセス許可を与えると、Zone Labs セキュリティ ソフトウェア は、自動的に POP3 および IMAP4 プロトコルを使用したインターネット ベースのメール サーバと共に動作するように設定されます。

Microsoft Exchange など一部のメール サーバには、コラボレーションおよび同期機能が備わっているため、適切に動作させるためにはそのサーバを信頼しなければならないことがあります。

コラボレーションおよび同期機能を備えたメール サーバ用に Zone Labs セキュリティ ソフトウェア を設定するには、次のようにします。

1. メール サーバのネットワーク サブネットまたは IP アドレスをトラスト ゾーンに追加します。
2. トラスト ゾーンのセキュリティ レベルを［中］に設定します。これにより、メール サーバのコラボレーション機能が動作するようになります。
3. インターネット ゾーンのセキュリティ レベルを［高］に設定します。これにより、信頼できないマシンからご使用のコンピュータが認識されなくなります。

インターネット接続共有（ICS）の有効化

Windows のインターネット接続共有（ICS）オプションやサードパーティの接続共有プログラムを使用している場合、ゲートウェイ マシンのみに Zone Labs セキュリティ ソフトウェア をインストールすることで、接続を共有するすべてのコンピュータを外部からの脅威から守ることができます。ただし、外部への保護を有効にしたり、クライアント マシン上で警告を表示するには、クライアント マシン上にも Zone Labs セキュリティ ソフトウェア がインストールされていなければなりません。

Zone Labs セキュリティ ソフトウェア を設定する前に、ICS ソフトウェアを使用してゲートウェイとクライアントの関係を設定してください。Microsoft のインターネット接続共有（ICS）ではなく、ルータなどのハードウェアを使用してインターネット接続を共有する場合は、ローカル サブネットがトラスト ゾーンに含まれていることを確認してください。

VPN 接続の設定

Zone Labs セキュリティ ソフトウェア には多くの VPN クライアント ソフトウェアとの互換性があり、特定の VPN クライアントについては自動的に接続を設定できます。

サポートされている VPN プロトコル

Zone Labs セキュリティ ソフトウェア は、下記の表に記載されている VPN プロトコルを監視します。

ネットワーク プロトコル	説明とコメント
AH	Authentication Header Protocol（認証ヘッダ プロトコル）
ESP	Encapsulating Security Payload protocol（暗号ペイロード プロトコル）
GRE	Generic Routing Encapsulation protocol（ルーティングのカプセル化プロトコル）
IKE	Internet Key Exchange protocol（インターネット鍵交換プロトコル）
IPSec	IP Security protocol（IP セキュリティ プロトコル）
L2TP	Layer 2 Tunneling protocol（Layer 2 トンネリング プロトコル）L2TP は、PPTP の安全性の高いバリエーションです。
LDAP	Lightweight Directory Access protocol（簡易ディレクトリ アクセス プロトコル）
PPTP	Point-to-Point Tunneling protocol（ポイント ツー ポイント トンネリング プロトコル）
SKIP	Simple Key Management for Internet Protocol（簡易インターネット鍵管理プロトコル）

表 3-1: サポートされている VPN プロトコル

VPN 接続の自動設定

VPN 通信が検出されると、自動 VPN 設定警告が表示されます。検出された VPN アクティビティの種類によって、また、Zone Labs セキュリティ ソフトウェア が VPN 接続を自動設定できたかどうかによって、3 種類の自動 VPN 設定警告のうちいずれかが表示されます。

自動 VPN 設定警告の詳細と対処方法については、235 ページの「自動 VPN 設定警告」を参照してください。

たとえば、VPN ゲートウェイのループバック アダプタまたは IP アドレスが、ブロックした IP 範囲またはサブネットに含まれる場合は、手動操作が

必要になることがあります。詳細については、38 ページの「VPN 接続の手動設定」を参照してください。

VPN 通信をブロックするエキスパート ファイアウォール ルールを作成した場合は、VPN 通信を許可するようにエキスパート ルールを変更する必要があります。62 ページの「エキスパート ファイアウォール ルールの作成」を参照してください。

VPN 接続の手動設定

VPN 接続を自動的に設定できない場合は、Zone Labs セキュリティ ソフトウェア が手動操作の要求警告を表示し、接続の設定に必要とされる手動操作について通知します。

手動設定の手順については、下記のセクションを参照してください。

- VPN ゲートウェイとその他のリソースのトラスト ゾーンへの追加
- ブロックされた IP 範囲またはサブネットからの VPN ゲートウェイの削除
- VPN プロトコルの許可
- VNP ソフトウェアのアクセス許可

PPTP 通信をブロックするエキスパート ファイアウォール ルールを作成していて、ご使用の VPN ソフトウェアが PPTP を使用する場合は、エキスパート ルールを変更する必要があります。62 ページの「エキスパート ファイアウォール ルールの作成」を参照してください。

VPN ゲートウェイとその他のリソースのトラスト ゾーンへの追加

VPN の正常な動作を可能にするため、VPN ゲートウェイに加えて、その他の VPN 関連リソースもトラスト ゾーンへ追加しなければならないことがあります。

必要なリソース	その他のリソース
下記のリソースはすべての VPN クライアント コンピュータに必要とされるため、トラスト ゾーンに含める必要があります。	下記のリソースは、VPN 設定により、必要な場合と不要な場合があります。
VPN コンセントレータ	DNS サーバ
VPN クライアントに接続されるリモート ホスト コンピュータ（企業ネットワークのサブネット定義に含まれていない場合）	ローカル ホスト コンピュータの NIC loopback アドレス（Windows のバージョンによります）。127.0.0.1 のローカル ホスト ループバック アドレスを指定している場合は、プロキシ ソフトウェアをローカル ホストで実行しないようにしてください。
VPN クライアント コンピュータがアクセスする企業ワイド エリア ネットワーク (WAN) のサブネット	インターネット ゲートウェイ
VPN コンピュータがアクセスする企業 LAN	ローカル サブネット
	セキュリティ サーバ（RADIUS、ACE、または TACACS サーバなど）

表 3-2: 必要な VPN 関連ネットワーク リソース

コンピュータのトラスト ゾーンにリソースを追加する方法については、53 ページの「トラスト ゾーンへの追加」を参照してください。

ブロックされた IP 範囲またはサブネットからの VPN ゲートウェイの削除

VPN ゲートウェイがブロックした IP 範囲またはサブネットに一致する場合は、ブロックを手動で解除する必要があります。

IP 範囲またはサブネットのブロックを解除するには、次のようにします。

1. **［ファイアウォール］|［ゾーン］を選択します。**
2. ［ゾーン］カラムで、ブロックされた IP 範囲またはサブネットを選択します。
3. ショートカット メニューから **［トラスト］**を選択し、**［適用］**をクリックします。

VPN プロトコルの許可

ご使用の VPN ソフトウェアについて Zone Labs セキュリティ ソフトウェア 上で正しく設定するため、全般的なセキュリティ設定で VPN プロトコルを許可するように変更する必要があります。

VPN プロトコルを許可するには、次のようにします。

1. **［ファイアウォール］**|**［メイン］** を選択し、**［詳細設定］** をクリックします。
2. ［全般設定］エリアで **［VPN プロトコルを許可］チェックボックスをオンにします。**
3. **［OK］** をクリックします。

VPN プログラムが GRE、ESP および AH 以外のプロトコルを使用する場合も、［一般的でないプロトコルを〝高〟セキュリティの場合に許可する］を選択します。

VNP ソフトウェアのアクセス許可

コンピュータ上の VPN クライアントおよび VPN に関連するプログラムにアクセス許可を与えます。

VPN プログラムに許可を与えるには、次のようにします。

1. **［プログラム コントロール］**|**［プログラム］** を選択します。
2. ［プログラム］カラムで、VPN プログラムを選択します。
3. ［アクセス］カラムで［トラスト］の下をクリックし、ショートカット メニューから **［許可］** を選択します。

目的の VPN プログラムが一覧に表示されない場合は、［追加］をクリックして一覧に追加します。

VPN に関連するプログラムにアクセス許可を与えるには、次のようにします。

1. **［プログラム コントロール］**|**［コンポーネント］** を選択します。
2. ［コンポーネント］カラムで、アクセス許可を与える VPN コンポーネントを選択します。

3. ［アクセス］カラムで、ショートカット メニューから［**許可**］を選択します。

VPN の接続に問題がある場合は、253 ページから始まる付録 C「トラブルシューティング」で VPN のトラブルシューティングのヒントを参照してください。

第 4 章

ファイアウォール保護

4

ファイアウォール保護は、インターネット上の脅威に対応するための主要な保護機能です。Zone Labs セキュリティ ソフトウェアのデフォルトのゾーンとセキュリティ レベルをそのまま適用するのみでも、ほとんどの脅威からコンピュータを守ることができます。上級レベルのユーザは、カスタム ポート許可とエキスパート ルールを使って、発信元、送信先、ポート、プロトコル、およびその他の要素を基に、通信について詳細に設定できます。

トピック：

- 44 ページの「ファイアウォール保護の概念」
- 45 ページの「セキュリティ レベルの選択」
- 47 ページの「アドバンス セキュリティ オプションの設定」
- 52 ページの「通信ソースの管理」
- 56 ページの「ポートのブロックおよびブロック解除」
- 59 ページの「エキスパート ファイアウォール ルールの概念」

ファイアウォール保護の概念

建造物においては、ファイアウォール（防火壁）とは火災が広がるのを防ぐための壁のことです。コンピュータでも、同じような概念が使われています。インターネット上には、ハッカーの攻撃、ウイルス、ワームなど、「火災」に匹敵するさまざまな脅威があります。ファイアウォールとは、コンピュータをこのような攻撃から防ぐためのシステムです。

Zone Labs セキュリティ ソフトウェアのファイアウォールは、コンピュータへの「ドア」、すなわちインターネット通信が着信および発信するポートを保護します。Zone Labs セキュリティ ソフトウェア は、コンピュータに到達したすべてのネットワーク通信を検査し、次のことを確認します。

- その通信がどのゾーンから発信され、どのポートに着信するのか？
- そのゾーンのルールで、そのポートを介した通信が許可されているか？
- その通信はグローバル ルールに違反していないか？
- その通信はコンピュータ上のプログラム（プログラム コントロール設定）によって認可されているか？

上記の質問に対する答えを基準に、通信を許可するか、ブロックするかが決定されます。

セキュリティ レベルの選択

デフォルトのファイアウォールの*セキュリティ レベル*（インターネット ゾーンは「高」、トラスト ゾーンは 「中」）では、*ポート スキャン*などのハッカー活動からご使用のコンピュータを保護しながら、ローカル ネットワーク上の信頼できるコンピュータとの間でプリンタ、ファイル、その他のリソースを共有することができます。ほとんどの場合、これらのデフォルト設定を変更する必要はありません。Zone Labs セキュリティ ソフトウェアのインストールと同時にコンピュータが保護されます。

ゾーンのセキュリティ レベルの設定

セキュリティ レベルを使用すると、ファイアウォールの設定を簡単に行うことができます。事前に設定されたセキュリティ レベル（高、中、低）をそれぞれのゾーンに適用したり、各レベルのポートおよびプロトコルの制限をカスタマイズしたりすることもできます。56 ページの「ポートのブロックおよびブロック解除」を参照してください。

ゾーンのセキュリティ レベルを設定するには、次のようにします。

1. **[ファイアウォール]**|**[メイン]** を選択します。
2. ［インターネット ゾーン セキュリティ］エリアで、スライダをクリックして希望の設定になるようにドラッグします。

高	コンピュータはステルス モードになり、他のコンピュータから認識されなくなります。 Windows *パケット* サービスへのアクセスと、ファイルおよびプリンタの共有へのアクセスがブロックされます。 ポートの使用をプログラムに許可しない限り、ポートはブロックされます。
中	ご使用のコンピュータは他のコンピュータから認識されます。 Windows サービスへのアクセスと、ファイルおよびプリンタの共有へのアクセスが許可されます。 プログラム許可は引き続き施行されます。
低	ご使用のコンピュータは他のコンピュータから認識されます。 Windows サービスへのアクセスと、ファイルおよびプリンタの共有へのアクセスが許可されます。 プログラム許可は引き続き施行されます。

3. ［トラスト ゾーン セキュリティ］エリアで、スライダをクリックして希望の設定になるようにドラッグします。

高	コンピュータはステルス モードになり、他のコンピュータから認識されなくなります。 Windows (NetBIOS) サービスへのアクセスと、ファイルおよびプリンタの共有へのアクセスがブロックされます。 ポートの使用をプログラムに許可しない限り、ポートはブロックされます。
中	ご使用のコンピュータは他のコンピュータから認識されます。 Windows サービスへのアクセスと、ファイルおよびプリンタの共有へのアクセスが許可されます。 プログラム許可は引き続き施行されます。
低	ご使用のコンピュータは他のコンピュータから認識されます。 Windows サービスへのアクセスと、ファイルおよびプリンタの共有へのアクセスが許可されます。 プログラム許可は引き続き施行されます。

アドバンス セキュリティ オプションの設定

アドバンス セキュリティ オプションにより、ゲートウェイ施行やインターネット接続共有（ICS）などの特殊な状況を対象にファイアウォールを設定できます。

ゲートウェイ セキュリティ オプションの設定

社内の*ゲートウェイ*を介してインターネットに接続する際に、社員に Zone Labs セキュリティ ソフトウェアの使用を義務付ける企業もあります。**[セキュリティ施行のためゲートウェイを自動的にチェック]** というオプションがオンになっている場合、Zone Labs セキュリティ ソフトウェア を必要とするゲートウェイを介したアクセスが適切に許可されるよう、Zone Labs セキュリティ ソフトウェア は互換性のあるゲートウェイを調べ、それがインストールされているかどうかを確認します。

ゲートウェイを通して接続していない場合でも、このオプションを選択したままにすることができます。インターネット機能に影響はありません。

ICS（インターネット接続共有）オプションの設定

*ICS（インターネット接続共有）*を使用している場合、このコントロールを使用して ICS ゲートウェイおよびクライアントを認識するように Zone Labs セキュリティ ソフトウェア を設定します。

インターネット接続共有の設定を指定するには、次のようにします。

1. **[ファイアウォール]**|**[メイン]** を選択します。
2. **[詳細設定]** をクリックします。
3. ［インターネット接続共有（ICS)］で、セキュリティ設定を指定します。

このコンピュータは ICS/NAT を使用していない	インターネット接続共有は無効になります。
このコンピュータは Zone Labs セキュリティ ソフトウェア を実行している ICS/NAT ゲートウェイのクライアント	Zone Labs セキュリティ ソフトウェア は、ICS ゲートウェイの IP アドレスを自動的に検出し、［ゲートウェイ アドレス］フィールドに表示します。［ゲートウェイ アドレス］フィールドに IP アドレスを手動で入力することもできます。 ［ゲートウェイからの警告をこのコンピュータに転送する］をオンにすると、ゲートウェイで発生した警告がクライアントコンピュータ上でログに記録され、表示されます。

このコンピュータは ICS/NAT ゲートウェイ	Zone Labs セキュリティ ソフトウェア は、ICS ゲートウェイの IP アドレスを自動的に検出し、[ローカル アドレス] フィールドに表示します。[ゲートウェイ アドレス] フィールドに IP アドレスを手動で入力することもできます。 [クライアントに転送された警告は表示しない] **を選択すると、ゲートウェイからクライアントに転送された警告がゲートウェイでは表示されなくなります。**

4. **[OK]** をクリックします。

全般的セキュリティ オプションの設定

全般的なセキュリティ設定により、特定のプロトコルやパケット タイプなどの通信形式（サーバ通信など）に関連するグローバル ルールをトラスト ゾーンおよびインターネット ゾーンの両方に適用できます。

全般的なセキュリティ設定を変更するには、次のようにします。

1. **[ファイアウォール]**|**[メイン]** を選択します。
2. **[詳細設定]** をクリックします。
3. [全般] エリアで、セキュリティ設定を指定します。

全フラグメント パケットをブロック	すべての不完全な（フラグメント）IP データ パケットをブロック。ハッカーは、パケット ヘッダを読み取るネットワーク デバイスを回避もしくは妨害する目的で、フラグメント化したパケットを作成することがあります。 注意：このオプションを選択した場合、Zone Labs セキュリティ ソフトウェア は、警告を表示したりログ エントリを作成したりせずに、すべてのフラグメント パケットを自動的にブロックします。オンライン接続でどのようにフラグメント パケットが処理されるかを理解していない限り、このオプションを選択しないでください。
トラスト サーバをブロックする	コンピュータ上のすべてのプログラムについて、トラスト ゾーンに対してサーバとして動作することを拒否します。この設定は、[プログラム] パネルで指定した許可より優先されます。
インターネット サーバをブロック	コンピュータ上のすべてのプログラムについて、インターネット ゾーンに対してサーバ動作することを拒否します。この設定は、[プログラム] パネルで指定した許可より優先されます。

ARP 保護を有効	ターゲット コンピュータのアドレスに対するブロードキャスト リクエストを除く、外部からのすべての ARP（アドレス解決プロトコル）リクエストをブロックします。外部への ARP リクエストに応答するものを除き、外部からの ARP 応答もすべてブロックします。
VPN プロトコルの許可	「高」セキュリティが適用されている場合でも、VPN プロトコル（ESP、AH、GRE、SKIP）の使用を許可します。このオプションを無効にすると、これらのプロトコルは、「中」セキュリティでのみ許可されます。
一般的でないプロトコルを高セキュリティの場合に許可	「高」セキュリティで、ESP、AH、GRE、SKIP 以外のプロトコルの使用を許可します。
ホスト ファイルのロック	コンピュータのホスト ファイルが、スパイウェアまたはトロイの木馬によってハッカーに改変されることを防ぎます。一部の正当なプログラムはその動作のためにホスト ファイルを変更する必要があるため、このオプションはデフォルトでオフになっています。
Windows のファイアウォールを無効にする	Windows のファイアウォールを検出して、無効にします。このオプションは、Windows XP Service Pack 2 をご使用の場合にのみ表示されます。
IP over 1394 トラフィックのフィルタリング	FireWire トラフィックをフィルタリングします。

4. **[OK]** をクリックします。

ネットワーク セキュリティ オプションの設定

自動ネットワーク検出機能を利用すると、ファイルおよびプリンタの共有などの従来のローカル ネットワーク アクティビティを中断せずに、トラスト ゾーンを簡単に設定することができます。Zone Labs セキュリティ ソフトウェアは、物理的に接続しているネットワークだけを検出します。ルーテッド ネットワークまたは仮想ネットワークの接続は検出されません。

Zone Labs セキュリティ ソフトウェアの設定により、警告を表示せずに検出したネットワークすべてをトラスト ゾーンに追加することも、また、新たに検出したネットワークを追加するかどうかをそのつど尋ねる警告を表示させることもできます。

ネットワークの設定を指定するには、次のようにします。

1. **[ファイアウォール]**|**[メイン]** を選択します。
2. **[詳細設定]** をクリックします。
3. ［ネットワーク設定］エリアで、セキュリティ設定を指定します。

新しく検出したネットワークをトラスト ゾーンに含める	新しいネットワークを自動的にトラスト ゾーンに追加します。この設定は最低限のセキュリティを提供します。

新しく検出したネットワークをトラスト ゾーンに含めない	新しいネットワークをトラスト ゾーンに追加せずに、インターネット ゾーンに追加します。この設定は最大のセキュリティを提供します。
新しく検出したネットワークを含めるゾーンを問い合わせる	Zone Labs セキュリティ ソフトウェア が新しいネットワーク警告またはネットワーク設定ウィザードを表示します。これらを利用して、ゾーンを指定することができます。
新しく検出した保護されていないワイヤレス ネットワーク (WEP または WPA) をインターネット ゾーンに自動的に含める	保護されていないワイヤレス ネットワークをインターネット ゾーンに自動的に追加するので、他者がネットワークにアクセスし、許可を得ずにユーザのデータにアクセスすることを防ぎます。

4. **[OK]** をクリックします。

ネットワークの詳細については、31 ページから始まる第 3 章「Zone Labs セキュリティ ソフトウェア を使ったネットワーキング」を参照してください。

ワイヤレス ネットワーク セキュリティ オプションの設定

自動ワイヤレス ネットワーク検出は、インターネット ゾーンを設定して、新しいワイヤレス ネットワークが検出されるたびに、干渉されることなく、コンピュータのセキュリティ保護を維持するに便利です。Zone Labs セキュリティ ソフトウェア は、コンピュータが接続しているワイヤレス ネットワークのみを検出します。(実際に接続していないネットワークが使用可能なネットワークとして［マイ ネットワーク］に表示されることがありますが、新規ワイヤレス ネットワーク設定ウィザードは、そのネットワークへの接続を確立したときにのみ表示されます)

Zone Labs セキュリティ ソフトウェア がインターネット ゾーンで検出されたあらゆるワイヤレス ネットワークを自動的に含めるようにすることができます。

ネットワークの設定を指定するには、次のようにします。

1. **［ファイアウォール］**|**［メイン］** を選択します。
2. **［詳細設定］** をクリックします。
3. ［ワイヤレス ネットワーク設定］エリアで、セキュリティ設定を選択します。

新しく検出した保護されていないワイヤレス ネットワーク (WEP または WPA) を自動的にインターネット ゾーンに含める	Zone Labs セキュリティ ソフトウェア は検出された新しいワイヤレス ネットワークをインターネット ゾーンに追加します。

4. **[OK]** をクリックします。

ネットワークの詳細については、31 ページから始まる第 3 章「Zone Labs セキュリティ ソフトウェア を使ったネットワーキング」を参照してください。

通信ソースの管理

［ゾーン］タブには、［トラスト ゾーン］または［ブロック ゾーン］に追加された通信ソース（コンピュータ、ネットワーク、またはサイト）が表示されます。また、このタブには Zone Labs セキュリティ ソフトウェアが検出したネットワークもすべて含まれます。ネットワークに接続していない PC を単独で使用している場合は、通信ソースの一覧には、インターネット ゾーンに含まれる ISP（インターネット サービス プロバイダ）のネットワークだけが表示されます。

通信ソースの一覧の表示

通信ソースの一覧には、通信ソースとその所属するゾーンが表示されます。カラム ヘッダをクリックすると、そのフィールドを基準にして一覧をソートすることができます。ヘッダ名の隣の矢印（^）は、ソートの順序を示しています。同じヘッダを再度クリックすると、ソートの順序が逆になります。

フィールド	説明
名前	このコンピュータ、サイト、またはネットワークに割り当てた名前
IP アドレス / サイト	通信ソースの IP アドレスまたはホスト名
項目の種類	通信ソースの種類：ネットワーク、ホスト、IP、サイト、サブネットのいずれか
ゾーン	通信ソースが割り当てられているゾーン：インターネット ゾーン、トラスト ゾーン、ブロック ゾーンのいずれか

表 4-1: 通信ソースの一覧のフィールド

通信ソースの変更

通信ソースの一覧では、通信ソースを別のゾーンに移動したり、通信ソースの追加、編集、削除を行うことができます。

通信ソースのゾーンを変更するには、次のようにします。

1. **［ファイアウォール］**|**［ゾーン］**を選択します。
2. 通信ソースを選択し、**［ゾーン］**カラム内をクリックします。
3. ショートカット メニューからゾーンを選択し、**［適用］**をクリックします。

通信ソースを追加、削除、または編集するには、次のようにします。

1. **［ファイアウォール］**|**［ゾーン］**を選択します。
2. ［名前］カラムで通信ソースをクリックし、**［追加］**、**［編集］**、**［削除］**のいずれかをクリックします。

3. **[適用]** をクリックします。

トラスト ゾーンへの追加

トラスト ゾーンには、リソース共有の対象となる信頼できるコンピュータが含まれます。たとえば、3 台の家庭用 PC が Ethernet ネットワークでリンクしている場合、個々のコンピュータまたはネットワーク アダプタ サブネット全体をトラスト ゾーンに含めることができます。トラスト ゾーンのデフォルトである「中」セキュリティでは、ファイルやプリンタなどのリソースをホーム ネットワーク上で安全に共有することができます。そして、「高」セキュリティ設定となっているインターネット ゾーンの範囲にハッカーをとどめることができます。

単一の IP アドレスを追加するには、次のようにします。

1. **[ファイアウォール]**|**[ゾーン]** を選択します。
2. **[追加]** をクリックし、ショートカット メニューから **[IP アドレス]** を選択します。

   [IP アドレスの追加] ダイアログが表示されます。
3. [ゾーン] ドロップダウン リストから **[トラスト]** を選択します。
4. 表示されるボックスに IP アドレスとその説明を入力し、**[OK]** をクリックします。

IP アドレスの範囲を追加するには、次のようにします。

1. **[ファイアウォール]**|**[ゾーン]** を選択します。
2. **[追加]** をクリックし、ショートカット メニューから **[IP アドレス]** を選択します。

   [IP 範囲の追加] ダイアログが表示されます。
3. [ゾーン] ドロップダウン リストから **[トラスト]** を選択します。
4. 最初のフィールドに範囲の始めとなる IP アドレスを入力し、次のフィールドに範囲の終わりとなる IP アドレスを入力します。
5. 表示されるフィールドに説明を入力し、**[OK]** をクリックします。

サブネットを追加するには、次のようにします。

1. **[ファイアウォール]**|**[ゾーン]** を選択します。
2. **[追加]** をクリックし、ショートカット メニューから **[サブネット]** を選択します。

   [サブネットの追加] ダイアログが表示されます。
3. [ゾーン] ドロップダウン リストから **[トラスト]** を選択します。

4. 最初のフィールドに IP アドレスを入力し、次のフィールドにサブネット マスクを入力します。
5. 表示されるフィールドに説明を入力し、**[OK]** をクリックします。

トラスト ゾーンにホストまたはサイトを追加するには、次のようにします。
1. **[ファイアウォール]**|**[ゾーン]** を選択します。
2. **[追加]** をクリックし、**[ホスト / サイト]** を選択します。

   [ホスト / サイトの追加] ダイアログが表示されます。
3. [ゾーン] ドロップダウン リストから **[トラスト]** を選択します。
4. **[ホスト名]** フィールドに正式なホスト名（完全修飾ホスト名）を入力します。
5. ホスト / サイトの説明を入力し、**[OK]** をクリックします。

ネットワークをトラスト ゾーンに追加するには、次のようにします。
1. **[ファイアウォール]**|**[ゾーン]** を選択します。
2. [ゾーン] カラムでネットワークを含む行をクリックし、ショートカット メニューから **[トラスト]** を選択します。
3. **[適用]** をクリックします。

Zone Labs セキュリティ ソフトウェア は、自動的に新しいネットワーク接続を検出し、これらを適切なゾーンに追加する手助けをします。詳細については、31 ページから始まる第 3 章「Zone Labs セキュリティ ソフトウェア を使ったネットワーキング」を参照してください。

ブロック ゾーンへの追加

ブロック ゾーンへの追加は、トラスト ゾーンへの追加に関する説明に従って行いますが、ステップ 2 のドロップダウン リストで **[ブロック]** を選択します。

ログに記録されたファイアウォール イベントの表示

デフォルトでは、すべてのファイアウォール イベントがログ ビューアに記録されます。

ログに記録されたファイアウォール イベントを表示するには、次のようにします。
1. **[警告とログ]**|**[ログ ビューア]** を選択します。

2. ［警告の種類］ドロップ ダウン リストから**［ファイアウォール］**を選択します。

表 5-2 に、ファイアウォール イベントで表示されるログ ビューアのフィールドの例を示します。

フィールド	情報
レベル	各警告は、レベルが「高」または「中」です。高レベルの警告は、ハッカーの活動が原因となっている可能性があります。中レベルの警告は、不要な、しかし害のないネットワーク通信が原因となっている可能性があります。
日付 / 時間	警告が発生した日時。
種類	警告の種類： ファイアウォール、プログラム、ID ロック、ロック有効。
プロトコル	警告の原因となった通信で使用された通信プロトコル。
プログラム	データを送信または受信しようとしたプログラムの名前。（プログラム警告および ID ロック警告でのみ使用されます）
発信元 IP アドレス	Zone Labs セキュリティ ソフトウェア がブロックした通信の送信元であるコンピュータの IP アドレス。
送信先 IP アドレス	ブロックされた通信の送信先のコンピュータのアドレス。
方向	ブロックされた通信の方向。「外部から」は、ご使用のコンピュータに対して送信された通信を示します。「外部へ」は、ご使用のコンピュータから発信した通信を示します。
対応	Zone Labs セキュリティ ソフトウェア で通信が処理された方法。
回数	種類、発信元、送信先、およびプロトコルがすべて同じ警告が単一セッション中に発生した回数。
発信元 DNS アドレス	警告の原因となった通信の送信元のドメイン名。
送信先 DNS アドレス	警告の原因となった通信で意図されていた送信先のドメイン名。

表 4-2: ファイアウォール イベント ログのフィールド

ポートのブロックおよびブロック解除

Zone Labs セキュリティ ソフトウェアのデフォルトのセキュリティ レベルにより、許可およびブロックされるポートとプロトコルが決定されます。上級レベルのユーザは、ポート許可を変更し、カスタム ポートを追加して、セキュリティ レベルの定義を変更することができます。

デフォルトのポート許可設定

高セキュリティのデフォルト設定では、アクセス許可またはサーバ許可が与えられたプログラムによって使用されていないポートを介した、外部からおよび外部への通信はすべてブロックされます。ただし、以下の場合は例外となります。

- DHCP ブロードキャスト / マルチキャスト
- 外部への DHCP（ポート 67）ー Windows 9x システムの場合
- 外部への DNS（ポート 53）ー コンピュータが ICS ゲートウェイとして設定されている場合

通信の種類	セキュリティ レベル		
	高	中	低
外部への DNS	ブロック	該当なし	許可
外部への DHCP	ブロック	該当なし	許可
ブロードキャスト / マルチキャスト	許可	許可	許可
ICMP			
外部から（ping エコー）	ブロック	許可	許可
外部から（その他）	ブロック	許可	許可
外部へ（ping エコー）	ブロック	許可	許可
外部へ（その他）	ブロック	許可	許可
IGMP			
外部から	ブロック	許可	許可
外部へ	ブロック	許可	許可
NetBIOS			
外部から	該当なし	ブロック	許可
外部へ	該当なし	許可	許可
UDP（許可されたプログラムによって使用されていないポート）			

表 4-3: 外部からまたは外部への通信の種類に対するデフォルトのアクセス許可

通信の種類	セキュリティ レベル		
	高	中	低
外部から	ブロック	許可	許可
外部へ	ブロック	許可	許可
TCP（許可されたプログラムによって使用されていないポート）			
外部から	ブロック	許可	許可
外部へ	ブロック	許可	許可

表 4-3: 外部からまたは外部への通信の種類に対するデフォルトのアクセス許可

ポートのアクセス許可を変更するには、次のようにします。

1. **[ファイアウォール]**|**[メイン]** を選択します。
2. ［インターネット ゾーン セキュリティ］または［トラスト ゾーン セキュリティ］で、**[カスタム]** をクリックします。

   ［カスタム ファイアウォール設定］ダイアログが表示されます。
3. 「高」および「中」のセキュリティ設定にスクロールします。
4. 特定のポートかプロトコルをブロックまたは許可するには、その隣のチェックボックスをクリックします。

高セキュリティ設定の一覧で通信の種類を選択すると、その種類の通信が「高」セキュリティにおいてご使用のコンピュータに送信されることを許可することになります。そのため、「高」セキュリティ レベルの保護が緩和されますので注意してください。逆に、中セキュリティ設定の一覧で通信の種類を選択すると、その種類の通信を「中」セキュリティにおいてブロックすることになります。そのため、「中」セキュリティ レベルの保護が強化されます。

5. **[適用]** をクリックし、**[OK]** をクリックします。

カスタム ポートの追加

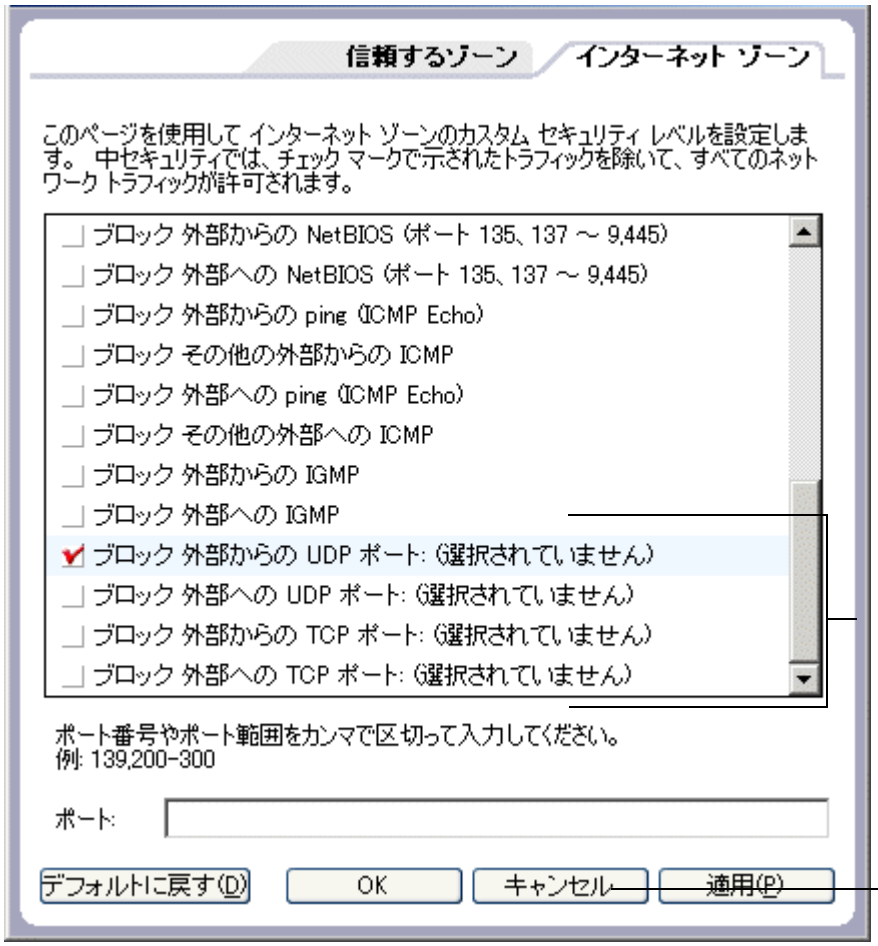
個々のポート番号またはポート範囲を指定することで、「高」セキュリティで通信を許可するポートを追加、または、「中」セキュリティでブロックするポートを追加することができます。

追加ポートを指定するには、次のようにします。

1. **[ファイアウォール]**|**[メイン]** を選択します。

2. ［トラスト ゾーン］または［インターネット ゾーン］で、**［カスタム］**をクリックします。

［カスタム ファイアウォール設定］ダイアログが表示されます。



3. ポートを追加するセキュリティ レベル（［高］または［中］）にスクロールします。

4. ポートの種類として外部からの UDP、外部への UDP、外部からの TCP、外部への TCP のいずれかを選択します。

5. 許可またはブロックするポートまたはポート範囲を、［ポート］フィールドにカンマで区切って入力します。例： 139, 200-300

6. **［適用］**をクリックしてから、**[OK]** をクリックします。

エキスパート ファイアウォール ルールの概念

エキスパート ファイアウォール ルールは、ファイアウォール セキュリティとネットワーク プロトコルに精通したユーザ向けのものです。

エキスパート ルールは、他のルールに取って替わるものではありません。複数階層で構成されたセキュリティ アプローチの一環として、他のファイアウォール ルールを補完するものです。

エキスパート ルールは次の 4 つの属性を使って、パケットをフィルタリングします。

- 発信元 / 送信先の IP アドレス
- 発信元 / 送信先のポート番号
- ネットワーク プロトコル / メッセージの種類
- 日時

発信元と送信先のアドレスは、IP ネットワーク アドレス、IP アドレス範囲、サブネットの記述、ゲートウェイ アドレス、ドメイン名など、さまざまな形式で指定できます。

発信元と送信先のポートは、UDP や TCP/IP などのポートを使用するネットワーク プロトコルの場合にのみ使用されます。たとえば、ICMP および IGMP メッセージでは、ポート情報は使用されません。

ネットワーク プロトコルは一般的な IP または VPN プロトコルの一覧から選択するか、IP プロトコル番号で指定することができます。ICMP の場合、メッセージの種類も指定できます。

日時の範囲をルールに適用して、曜日と時間を基準にアクセスを制限できます。

エキスパート ファイアウォール ルールの施行方法

エキスパート ルールが、ゾーン ルール、プログラム許可、およびその他のエキスパート ルールとどのように連携して施行されるかを理解することが重要です。

エキスパート ルールとゾーン ルール

エキスパート ファイアウォール ルールは、ゾーン ファイアウォール ルールに優先して施行されます。つまり、パケットがエキスパート ルールに一致する場合はそのルールが施行され、Zone Labs セキュリティ ソフトウェア はゾーン ルールの評価をスキップします。

例：トラスト ゾーンのセキュリティ レベルが「中」に設定されていると仮定します。この設定では、外部への NetBIOS 通信は許可されます。しかし

同時に、午後 5 時から午前 7 時の間の NetBIOS 通信をすべてブロックするエキスパート ルールも作成したとします。その場合、トラスト ゾーンの設定に関係なく、この時間帯は外部への NetBIOS 通信はすべてブロックされます。

エキスパート ファイアウォール ルールとプログラム許可

エキスパート ルールとゾーン ルールは共にプログラム許可と並行して適用されます。つまり、プログラム許可かゾーン ルール / エキスパート ファイアウォール ルールのいずれかで特定の通信をブロックするように設定されている場合、その通信はブロックされます。したがって、ファイアウォール ルールを使って、プログラム許可よりもルールを優先させたり、プログラム許可を再定義することができます。

エキスパート ファイアウォール ルールで許可されている場合、ブロックゾーンからのパケットはブロックされないことに注意してください。

エキスパート ファイアウォール ルールの適用ランク

ファイアウォール規則の領域内では、規則の評価順が要因となります。Zone Labs セキュリティ ソフトウェア は、エキスパート ファイアウォール ルールを最初に確認します。一致するルールが検出されて施行されると、その通信にはブロックまたは許可されたことを示すマークが付けられ、Zone Labs セキュリティ ソフトウェア はゾーン ルールの評価をスキップします。一致するエキスパート ファイアウォール ルールが見つからない場合は、Zone Labs セキュリティ ソフトウェア はゾーン ルールを確認し、通信をブロックすべきかどうかを判断します。

エキスパート ファイアウォール ルールの適用ランクも重要となります。各ルールには固有のランク番号が設定されていて、ルールはそのランク順に評価されます。最初に一致するルールだけが実行されます。次の 2 つのルールを例として説明します。

			名前	発信元	送信先	プロトコル	時間	コメント
1	✓		FTP Allow	マイ コンピュータ	信頼するゾーン	すべて	すべて	
2	✗		FTP Block	マイ コンピュータ	信頼するゾーン	すべて	すべて	

図 4-4: エキスパート ファイアウォール ルールのランク順

ルール 1 は、トラスト ゾーン内の FTP クライアントが、ポート 21 で FTP サーバに接続することを許可しています。ルール 2 は、ゾーンに関係なく、ポート 21 でのすべての FTP クライアントの接続をブロックしています。これら 2 つのルールから、トラスト ゾーン内のクライアントがクライアント コンピュータ上の FTP サーバを使用することは許可されますが、その他の FTP アクセスはすべてブロックされます。

これらルールの順序が逆になると、ルール 2 が先に一致するため、FTP アクセスはすべてブロックされます。ルール 1 はまったく実行されないため、トラスト ゾーン内の FTP クライアントはブロックされたままになります。

エキスパート ファイアウォール ルールの作成

エキスパート ファイアウォール ルールを作成する際には、ルールの適用対象となるネットワーク通信の発信元や送信先を指定し、トラッキング オプションを設定して、ルールのアクション（ルールの条件に一致する通信をブロックするか許可するか）を指定します。新しいルールを初めから作成することも、既存のルールをコピーしてプロパティを変更することもできます。

新しいエキスパート ファイアウォール ルールを作成するには、次のようにします。

1. **[ファイアウォール]**|**[エキスパート]** を選択し、**[追加]** をクリックします。

   [ルールの追加] ダイアログが表示されます。

2. [全般] で、ルールの設定を指定します。

ランク	ルールが適用される順序です。ランクが 1 のルールが最初に施行されます。
名前	そのルールに付ける、分かりやすい名前を入力します。
状態	ルールの有効または無効を指定します。
アクション	このルールに一致する通信のブロックまたは許可を指定します。
トラック	エキスパート ルールの施行時に、ログを作成するか、警告を生成してログを作成するか、何もしないかを指定します。
コメント	エキスパート ルールに関するメモを入力するオプションのフィールドです。

3. [発信元] エリアで一覧から場所を選択、または **[変更]** をクリックし、ショートカット メニューから **[場所の追加]** を選択します。ルールに追加する発信元の数に制限はありません。

マイ コンピュータ	ご使用のコンピュータから発信される通信にエキスパート ルールを適用します。
トラスト ゾーン	トラスト ゾーン内の発信元からのネットワーク通信にエキスパート ルールを適用します。
インターネット ゾーン	インターネット ゾーン内の発信元からのネットワーク通信にエキスパート ルールを適用します。
すべて	すべての発信元からのネットワーク通信にエキスパート ルールを適用します。
ホスト / サイト	指定のドメイン名からのネットワーク通信にエキスパート ルールを適用します。
IP アドレス	指定の IP アドレスからのネットワーク通信にエキスパート ルールを適用します。

IP 範囲	指定の IP アドレス範囲内のコンピュータからのネットワーク通信にエキスパート ルールを適用します。
サブネット	指定のサブネット内のコンピュータからのネットワーク通信にエキスパート ルールを適用します。
ゲートウェイ	指定のゲートウェイ上のコンピュータからのネットワーク通信にエキスパート ルールを適用します。
新規グループ	エキスパート ルールで使用する場所グループを新たに作成する場合は、このオプションを選択してから、**[追加]** をクリックします。
既存グループ	エキスパート ルールで使用する既存の場所グループを選択する場合は、このオプションを選択してから、**[OK]** をクリックします。

4. ［送信先］で一覧から場所を選択するか、**[変更]** をクリックして、ショートカット メニューから **[場所の追加]** を選択します。

   使用可能な場所の種類は、発信元、送信先のどちらも同じです。

5. ［プロトコル］エリアで一覧からプロトコルを選択、または **[変更]** をクリックし、**[プロトコルの追加]** を選択します。

プロトコルの追加	ルールにプロトコルを追加するには、このオプションを選択します。次のいずれかを指定します。TCP、UDP、TCP + UDP、ICMP、IGMP、カスタム
新規グループ	エキスパート ルールで使用するプロトコル グループを新たに作成する場合は、このオプションを選択してから、**[追加]** をクリックします。
既存グループ	エキスパート ルールで使用する既存のプロトコル グループを選択する場合は、このオプションを選択してから、**[OK]** をクリックします。

6. ［時間］エリアで一覧から時間を選択、または **[変更]** をクリックし、**[時間の追加]** を選択します。

日時の範囲	ルールに日時の範囲を追加するには、このオプションを選択します。説明、時間の範囲、および曜日を指定します。時間の範囲は 24 時間制で指定します。
新規グループ	エキスパート ルールで使用する曜日 / 時間グループを新たに作成する場合は、このオプションを選択してから、**[追加]** をクリックします。
既存グループ	エキスパート ルールで使用する既存の曜日 / 時間グループを選択する場合は、このオプションを選択してから、**[OK]** をクリックします。

7. **[OK]** をクリックします。

既存のルールから新しいルールを作成するには、次のようにします。

1. **[ファイアウォール]**|**[エキスパート]** を選択します。

2. コピーするエキスパート ファイアウォール ルールを選択し **Ctrl+C** を押す、またはそのルールを右クリックして **[コピー]** を選択します。
3. **Ctrl+V** を押す、または右クリックして **[貼り付け]** を選択し、コピーしたルールを貼り付けます。

一覧で選択されているルールがあれば、その前の位置に挿入されます。一覧でルールが選択されていなければ、ルール一覧の一番上の位置に貼り付けられます。

コピーされたルール名には「1」が付加されます。ルールの貼り付けが 2 度目の場合は、「2」が付加されます。

4. **[適用]** をクリックし、変更を保存します。
5. 新しいルールを右クリックし **[編集]** を選び、必要に応じてルールのプロパティを変更します。

グループの作成

グループを使用することで、エキスパート ファイアウォール ルールで使用する場所、プロトコル、曜日 / 時間の管理を単純化できます。

場所グループの作成

場所グループを使って、非連続的な IP アドレスと IP 範囲、異なる種類の場所（サブネットとホストなど）を管理しやすいセットとしてまとめることができます。この場所のセットは、エキスパート ファイアウォール ルールに簡単に追加できます。

場所グループを作成するには、次のようにします。

1. **[ファイアウォール]**|**[エキスパート]** を選択し、**[グループ]** をクリックします。

   [グループ マネージャ] ダイアログが表示されます。

2. **[場所]** タブを選択し **[追加]** をクリックします。

   [場所グループの追加] ダイアログが表示されます。

3. 場所グループの名前と説明を入力し、**[追加]** をクリックして、メニューから場所の種類を選択します。

ホスト / サイト	ホスト / サイトの場所についての説明とホスト名を入力し、**[OK]** をクリックします。ホスト名には、「http://」は含めません。サイトの IP アドレスをプレビューするには、**[検索]** をクリックします。
IP アドレス	IP アドレスの場所についての説明と IP アドレスを入力し、**[OK]** をクリックします。
IP 範囲	IP 範囲の場所についての説明、および範囲の始めと終わりの IP アドレスを入力し、**[OK]** をクリックします。
サブネット	サブネットの場所についての説明、IP アドレス、およびサブネットマスクを入力し、**[OK]** をクリックします。
ゲートウェイ	ゲートウェイの場所の IP アドレスと MAC アドレス、説明を入力し、**[OK]** をクリックします。

4. **[OK]** をクリックし [グループ マネージャ] ダイアログ ボックスを閉じます。

グループの作成後は、グループ名を変更することはできません。たとえば、「Home」という名前の場所グループを作成した後で、そのグループ名を「Work」に変更する場合は、「Home」という名前のグループを削除し、「Work」という名前を使ってグループを新たに作成する必要があります。

プロトコル グループの作成

TCP/UDP ポート、プロトコル、プロトコル固有のメッセージ タイプ（ICMP メッセージ タイプなど）をセットとして組み合わせてプロトコル グループを作成すると、エキスパート ルールに簡単に追加できるようになります。たとえば、メール通信に関するルールの管理を単純化するために、POP3 と IMAP4 プロトコルを含むグループを作成することができます。

プロトコル グループを作成するには、次のようにします。

1. **[ファイアウォール]**|**[エキスパート]** を選択し、**[グループ]** をクリックします。

   [グループ マネージャ] ダイアログが表示されます。

2. **[プロトコル]** タブを選択し、**[追加]** をクリックします。

   [プロトコル グループの追加] ダイアログが表示されます。

3. プロトコル グループの名前と説明を入力し、**[追加]** をクリックします。

   [プロトコルの追加] ダイアログが表示されます。

4. [プロトコル] ドロップダウン リストからプロトコルの種類を選択します。

   ■TCP

   ■UDP

   ■TCP + UDP

   ■ICMP

   ■IGMP

   ■ カスタム

5. ステップ 4 で TCP、UDP または TCP/UDP を選択した場合は、送信先、発信元、ポート番号を指定します。

名前	ポート番号
FTP	21
Telnet	23
POP3	110
NNTP	119
NetBIOS 名	137
NetBIOS データグラム	138
NetBIOS セッション	139
IMAP4	143

HTTPS	443
RTSP	554
Windows メディア	1755
AOL	5190
Real Networks	7070
その他	ポート番号を指定
FTP データ	20
TFTP	69
HTTP	80
DHCP	67
DHCP クライアント	68
SMTP	25
DNS	53

6. ステップ 4 で ICMP を選択した場合は、説明、メッセージ名、タイプ番号を指定します。

メッセージ名	タイプ番号
ソース クエンチ	4
リダイレクト	5
Alt	6
エコー要求	8
ルータ広告	9
ルータ勧誘	10
超過時間	11
パラメータ問題	12
タイムスタンプ	13
タイムスタンプ応答	14
情報要求	15
情報応答	16
アドレス マスク要求	17
アドレス マスク応答	18
トレースルート	30
その他	タイプ番号を指定

7. ステップ 4 で IGMP を選択した場合は、説明、メッセージ名、タイプ番号を指定します。

メンバーシップ クエリ	17
メンバーシップ レポート（バージョン 1）	18
Cisco Trace	21
メンバーシップ レポート（バージョン 2）	22
グループから除外（バージョン 2）	23
マルチキャスト トレースルート応答	30
マルチキャスト トレースルート	31
メンバーシップ レポート（バージョン 3）	34
その他	タイプ番号を指定

8. ステップ 4 でカスタムを選択した場合は、説明、プロトコルの種類、プロトコル番号を指定します。

RDP	27
GRE	47
ESP	50
AH	51
SKIP	57
その他	プロトコル番号を指定

9. **[OK]** をクリックし、[プロトコルの追加] ダイアログを閉じます。

曜日 / 時間グループの作成

指定した時間帯にコンピュータ上のネットワーク通信を許可またはブロックするために、曜日 / 時間グループを作成してエキスパート ルールに追加することができます。たとえば、営業時間帯にポップアップ広告サーバからの通信をブロックするには、月曜から金曜の午前 9 時から午後 5 時まで特定のドメインからの HTTP 通信をブロックするグループを作成します。

曜日 / 時間グループを作成するには、次のようにします。

1. **[ファイアウォール]**|**[エキスパート]** を選択し、**[グループ]** をクリックします。

   [グループ マネージャ] ダイアログが表示されます。

2. **[時間]** タブを選択し、**[追加]** をクリックします。

   [時間グループの追加] ダイアログが表示されます。

3. 時間グループの名前と説明を入力し、**[追加]** をクリックします。

   [時間の追加] ダイアログが表示されます。

4. 時間の説明を入力し、時間と曜日の範囲を選択します。

5. **[OK]** をクリックし、もう一度 **[OK]** をクリックして、[グループ マネージャ] を閉じます。

エキスパート ファイアウォール ルールの管理

［ファイアウォール］パネルの［エキスパート］タブを使って、既存のエキスパート ルールの状況の表示、ルールの有効化または無効化、ルールの編集または削除、新規ルールの追加、ルールの順序変更、およびグループの作成を行うことができます。

エキスパート ルールの一覧の表示

［エキスパート ルール］タブには、すべてのエキスパート ファイアウォール ルールの一覧が表示されます。ルールは適用の優先順位（ランク）を基にリストされています。右側の矢印ボタンを使って、選択したルールを一覧内で上下に移動し、その適用順序を変更できます。

また、ルールを別の位置にドラッグ アンド ドロップすることで、ルールのランク順を変更することもできます。

たとえば、ルール 2 を一覧の先頭の位置にドラッグ アンド ドロップすると、そのルールのランクは 1 に変更されます。

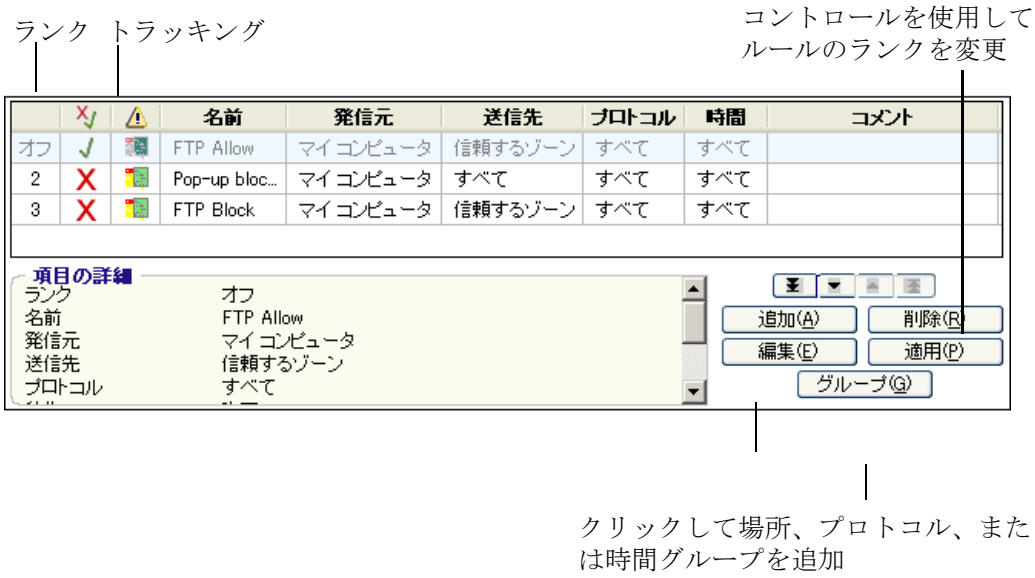


図 4-5: エキスパート ルールの一覧

ランク
ルールを適用する優先順位。ルールはランク 1 から順番に評価され、最初に一致するルールが施行されます。無効化されたルールでは、ランク番号のかわりに「オフ」が表示されますが、一覧中のランク順はそのままになります。

操作
赤色の X は、このルールがネットワーク通信をブロックすることを示します。緑色の ✓ は、このルールがネットワーク通信を許可することを示します。

トラック
何も表示されていない場合は、ルールの適用時に通知が行われません。ログ（ ）は、ルールの適用時にログ エントリが作成されることを示します。警告とログ（ ）は、エキスパート ルールの適用時に警告が表示され、ログ エントリが作成されることを示します。

名前
ルールを説明する名前。

発信元
ルールの発信元アドレスとポート。

送信先
ルールの送信先アドレスとポート。

プロトコル
ルールが適用されるネットワーク プロトコル。

時間
ルールが有効な時間帯。

ルールの編集とランク変更

［エキスパート ルール］一覧で、ルールを選択して適切なランクにドラッグすることで、既存のエキスパート ルールの編集または順序の並べ替えができます。エキスパート ルールをプログラム ルールにコピーした場合は、エキスパート ルールを変更しても、プログラム ルールは自動的には変更されません。詳細については、96 ページの「プログラム用のエキスパート ルールの作成」を参照してください。

ルールを編集するには、次のようにします。

1. **［ファイアウォール］**|**［エキスパート］** を選択します。
2. 編集するルールを選択し、**［編集］** をクリックします。

   ［ルールの編集］ダイアログが表示されます。
3. 必要に応じてルールの属性を変更し、**[OK]** をクリックします。

ルールのランクを変更するには、次のようにします。

1. **[ファイアウォール]**|**[エキスパート]** を選択します。
2. 移動するルールを右クリックし、**[ルールの移動]** をクリックします。

先頭へ移動	選択したルールをルール一覧の先頭に移動します。
最後尾へ移動	選択したルールをルール一覧の最後尾に移動します。
上へ移動	選択したルールをルール一覧の 1 つ上の行に移動します。
下へ移動	選択したルールをルール一覧の 1 つ下の行に移動します。

第 5 章

プログラム コントロール

5

プログラム コントロールは、信頼できるプログラムのみがインターネットにアクセスしたり、コンピュータ上で一定のアクションを実行したりできるように管理することで、ユーザを保護します。プログラム許可は手動で割り当てることもできますが、プログラム アドバイスが使用可能なときに Zone Labs セキュリティ ソフトウェアを使用して許可を割り当てることもできます。上級レベルのユーザは、プログラムごとに使用を許可するポートを設定できます。

ZoneAlarm Security Suite Triple Defense Firewall という追加の保護が含まれています。Triple Defense Firewall は信頼できるプログラムについても、潜在的に危険な動作を禁止します。

トピック：

- 74 ページの「プログラム コントロールの概念」
- 77 ページの「全般的プログラム コントロール オプションの設定」
- 83 ページの「アドバンス プログラム設定の指定」
- 85 ページの「特定プログラムの許可の設定」
- 94 ページの「プログラム コンポーネントの管理」
- 96 ページの「プログラム用のエキスパート ルールの作成」

プログラム コントロールの概念

インターネット上で行うすべての作業 － Web ページの閲覧から MP3 ファイルのダウンロードまで － は、コンピュータの特定のプログラム により管理されます。

ハッカーはこのことを利用して、「悪意のあるプログラム」、すなわち有害なソフトウェアをユーザのコンピュータに送り込みます。悪意のあるプログラムは無害なメール添付ファイルや正当なプログラムのアップデートを装うことがあります。そして、悪意のあるプログラムはコンピュータ上で信頼できるプログラムをハイジャックし、正当であるとみせかけて危険な行為を実行することがあります。

Zone Labs セキュリティ ソフトウェアはプログラムに対して信頼性のレベルを示し、実行を許可するアクションを指定するポリシーを割り当てることにより、ハッカーや悪意のある攻撃からコンピュータを保護します。

ZoneAlarm Security Suite ユーザには OSFirewall 保護という追加機能が提供されています。この機能はプログラムがコンピュータのレジストリ設定の変更など、疑わしいアクションまたは潜在的に危険なアクションを実行しようとするところを検出します。

自動によるプログラム許可の設定

SmartDefense Advisor とプログラム コントロールを両方とも適切に設定することで、無害なプログラムにアクセスを許可し、悪意のあるプログラムのアクセスを拒否することができるようになります。プログラム コントロールと SmartDefense Advisor のデフォルト設定に基づいて、デフォルトではプログラム コントロールは「中」に、SmartDefense Advisor は「自動」に設定されています。これらのデフォルト設定では、Zone Labs セキュリティ ソフトウェア は自動的にプログラムに許可を割り当てます。プログラム コントロールおよび SmartDefense Advisor のカスタマイズについての詳細は、77 ページの「全般的プログラム コントロール オプションの設定」を参照してください。

プログラムが最初にアクセスを要求すると、次のいずれかの処理が行われます。

- アクセスを許可 － プログラムが安全であることがわかっており、プログラムが正しく動作するために必要な許可を問い合わせている場合、アクセスは許可されます。これは、プログラム コントロールが「中」に設定されており、SmartDefense Advisor が「自動」に設定されている場合に発生します。
- アクセスを拒否 － プログラムが有害なプログラムであることがわかっているか、または問い合わせている許可をプログラムが必要としない場合、アクセスは拒否されます。これは、プログラム コントロールが「中」に設定されており、SmartDefense Advisor が「自動」に設定されている場合に発生します。

■ 新しいプログラムの警告が表示される ― プログラムのアクセスを許可するか、または拒否するかを決定する必要がある場合は、プログラム警告が表示されます。プログラム警告では、どのように応答するかを決定するために役立つアドバイスが提供されます。

一部のケースでは、SmartDefense Advisor に特定のプログラムの情報がなく、自動的に許可を割り当てることができない場合があります。このような場合は、プログラム警告が表示されます。警告の［詳細情報］をクリックすると、どのように応答するかの参考になるプログラムの詳細が表示されます。詳細については、228 ページの「プログラム警告」を参照してください。

安全なプログラム

Zone Labs セキュリティ ソフトウェア は、既知の安全なプログラムのデータベースを使用してプログラムを検証し、正しく動作するために必要な許可をプログラムに自動的に割り当てます。設定ウィザードでデフォルトのプログラム設定を受け入れた場合、Zone Labs セキュリティ ソフトウェアには、次の全般的なカテゴリに含まれる最も一般的なプログラムが自動的に設定されます。

■ ブラウザ（Internet Explorer、Netscape など）

■ 電子メール アプリケーション（Microsoft Outlook、Eudora など）

■ インスタント メッセンジャ（AOL、Yahoo! など）

■ アンチウイルス（Symantec、Zone Labs など）

■ 文書ユーティリティ（WinZip(R) および Adobe(R) Acrobat(R) など）

■ Zone Labs ソフトウェア アプリケーション

安全とみなされるプログラムもハッカーによって、安全でないアクションを実行するために用いられることがあります。ZoneAlarm Security Suite で利用可能な OSFirewall 保護は、疑わしい、または危険なプログラム動作を検出すると警告を表示します。これらの警告の詳細については、228 ページから始まる付録 A「プログラム警告」を参照してください。

手動によるプログラム許可の設定

独自にプログラムに許可を割り当てる場合や、Zone Labs セキュリティ ソフトウェア によって自動的に許可を割り当てることができない場合は、プログラム警告を使用して手動で許可を設定するか、［プログラム］パネルの［プログラム］タブで特定のプログラムに許可を設定することができます。

プログラム警告

プログラムが初めてアクセスを要求すると、そのプログラムにアクセス許可を与えるかどうかを確認する新しいプログラム警告が表示されます。コ

ンピュータ上のポートで待ち受けているプログラムが検出されると、サーバ プログラム警告が表示されます。

疑わしい動作の警告および危険な動作の警告は、コンピュータ上の信頼できるプログラムが疑わしい、または危険であるとみなされるアクションを実行しようとしていることを通知します。疑わしい、または危険であるとみなされるアクションの一覧については、273 ページの「プログラム動作」を参照してください。

同一のプログラムに多数の警告を表示しないようにするには、**[選択した結果を保存する]** チェックボックスを選択してから、**[許可]** または **[拒否]** をクリックします。そうすることで、Zone Labs セキュリティ ソフトウェア は警告を表示することなく、バックグラウンドでプログラムをブロックまたは許可します。同じプログラムが再びアクセスを要求する場合は、以前アクセス許可を要求したプログラムに許可を与えるか（または拒否するか）どうかを確認する、繰り返されたプログラム警告が表示されます。

トロイの木馬などの悪意のあるプログラムは、破壊工作をするためにサーバ権限を必要とする場合が多いため、サーバ許可を与える際には、信頼ができ、正常に動作するためにサーバ許可が必要な既知のプログラムにのみ許可を与えるように特に注意してください。チャット プログラム、メール クライアント、およびインターネット キャッチホン プログラムなど、いくつかの一般的なプログラムは、正常に動作するためにサーバ許可を必要とする場合があります。確実に信頼できて、しかも正常に動作するために許可を必要とするプログラムに対してのみ、サーバ許可を与えてください。

インターネット ゾーンでは、できる限りサーバ許可を与えないようにします。接続を受け入れる必要のあるマシンが少数の場合は、トラスト ゾーンにそれらのマシンを追加し、トラスト ゾーンでのサーバ許可のみをプログラムに与えます。

プログラム警告の詳細については、228 ページの「プログラム警告」を参照してください。

また、警告を表示しないで Zone Labs セキュリティ ソフトウェア が自動的に新しいプログラムを許可または拒否するように指定することもできます。たとえば、必要なプログラムすべてにアクセス許可をすでに与えている場合は、新たに許可を要求するプログラムがあったときに、アクセスをすべて自動的に拒否するように設定できます。詳細については、83 ページの「新しいプログラムのアクセス許可の設定」を参照してください。

プログラム一覧

プログラム一覧では、個々の必要に基づいて特定のプログラムの許可を設定したりカスタマイズしたりすることができます。プログラム一覧の使用方法と許可のカスタマイズの詳細については、85 ページの「プログラム一覧の使用」を参照してください。

全般的プログラム コントロール オプションの設定

Zone Labs セキュリティ ソフトウェアの起動中は、許可がない限り、コンピュータ上のプログラムがインターネットまたはローカル ネットワークへアクセスしたり、サーバとして動作することはありません。

プログラム コントロール レベルの設定

プログラム コントロール レベルにより、Zone Labs セキュリティ ソフトウェアの初回使用時のプログラム警告の表示数を調整できます。

Zone Labs, LLC. では、通常使用する場合の最初の数日間は、「中」に設定することをお勧めします。この*コンポーネントの学習モード*を使用すると、Zone Labs セキュリティ ソフトウェアは、多数の警告によりユーザの作業を中断することなしに、頻繁に使用される各コンポーネントの MD5 署名をすばやく学習します。Zone Labs セキュリティ ソフトウェア が起動した状態でインターネット アクセス プログラム（ブラウザ、メール、チャット プログラムなど）をそれぞれ少なくとも一回使用するまでは、この設定を使用してください。インターネット アクセスを必要とする各プログラムを使用したら、プログラム コントロールの設定を 「高」に変更します。

グローバルなプログラム コントロール レベルを設定するには、次のようにします。

1. **［プログラム コントロール］|［メイン］**を選択します。
2. ［プログラム コントロール］エリアで、スライダをクリックして希望の設定になるようにドラッグします。

高	アドバンス プログラムおよびコンポーネント コントロールが有効になります。この設定では、多数の警告が表示されることがあります。 ◆ プログラムおよびコンポーネントが認証されます。 ◆ プログラム許可が施行されます。 ◆ プログラムは疑わしく危険な行為を監視されます。

中	これは、デフォルトの設定です。 ◆ アドバンス プログラム コントロールは無効になります。 ◆ コンポーネントの学習モードはアクティブになります。 ◆ プログラムが認証され、コンポーネントが学習されます。 ◆ プログラム許可が施行されます。 ◆ プログラムは危険な行為を監視されます。 注意：インターネット アクセスを必要とする各プログラムを使用後、［プログラム コントロール］の設定を「高」に変更します。
低	◆ アドバンス プログラム コントロールは無効になります。 ◆ プログラムとコンポーネントの学習モードはアクティブになります。 ◆ プログラム警告は表示されません。
オフ	プログラム コントロールは無効になります。 ◆ プログラムおよびコンポーネントは認証も学習もされません。 ◆ プログラム許可は施行されません。 ◆ すべてのプログラムにアクセス/サーバ権限が与えられます。 ◆ すべてのプログラムは疑わしく危険な行為を実行できます。 ◆ プログラム警告は表示されません。

カスタム プログラム コントロール オプションを設定するには：

1. ［**プログラム コントロール**］|［**メイン**］を選択します。
2. ［プログラムのコントロール］エリアで、［**カスタム**］をクリックします。

   ［カスタム プログラム コントロール設定］ダイアログが表示されます。
3. 適用する設定を指定します。

アドバンス プログラム コントロールを有効にする	委任されたプログラムが、外部への保護を回避するために信頼できるプログラムを利用することを防ぎます。
アプリケーション対話コントロールを有効にする	あるプロセスが別のプロセスを使用しようとしたり、プログラムが別のプログラムを起動しようとすると警告します。
コンポーネント コントロールを有効にする	未承認の動作についてプログラムのコンポーネントのモニタリングを有効化します。

4. ［OK］をクリックします。

SmartDefense Advisor のレベルの設定

アクセスが必要なプログラムを使用するたびに、SmartDefense Advisor はそのプログラムのポリシーを判別するために Zone Labs サーバに問い合わせを行います。SmartDefense Advisor が自動的にプログラムに許可を設定するように指定するか、またはプログラム アクセスを手動で設定することができます。デフォルトでは、SmartDefense Advisor のレベルは「自動」に設定されます。

SmartDefense Advisor のレベルを設定するには

1. **[プログラム コントロール]**|**[メイン]** を選択します。
2. [SmartDefense Advisor] エリアで、設定を指定します。

自動	自動モードでは、SmartDefense Advisor はサーバから返された推奨を自動的に実装します。SmartDefense Advisor を「自動」に設定するには、プログラム コントロールを「中」または「高」に設定しておく必要があります。
手動	手動モードでは、プログラムがアクセスを要求するたびにプログラム警告が表示され、独自に許可を設定することができます。
オフ	SmartDefense Advisor は、プログラム アドバイスを取得するためにサーバに接続することはありません。

プログラムについてのアドバイスがないか、または SmartDefense Advisor が「オフ」に設定されている場合は、プログラム許可を手動で設定できます。85 ページの「特定プログラムの許可の設定」を参照してください。

自動ロックの有効化

自動インターネット ロックは、インターネットに接続したままネットワークやインターネット リソースを長時間使用しない場合にコンピュータを守ります。

ロックが有効になっていると、パスロック 許可が与えられたプログラムによって開始された通信のみが許可されます。DHCP メッセージや、インターネット接続を維持するために使われる ISP ハートビートも含め、ご使用のコンピュータ上の通信はすべて停止されます。その結果、インターネット接続が切断されることもあります。

インターネット ロックは次のように設定できます。

- スクリーン セーバーの起動時にロックする、または
- ネットワークが使用されない状態で指定した時間（分）が経過するとロックする。

自動ロックを適用または解除するには、次のようにします。

1. **[プログラム コントロール]**|**[メイン]** を選択します。
2. [自動ロック] エリアで、**[オン]** または **[オフ]** を選択します。

自動ロックのオプションを設定するには、次のようにします。

1. ［**プログラム コントロール**］|［**メイン**］を選択します。
2. ［自動ロック］エリアで、［**カスタム**］をクリックします。

   ［カスタム ロック設定］ダイアログが表示されます。
3. 使用するロック モードを指定します。

n 分間以上使用しなかったらロックする	一定の分数の経過後に自動ロックを適用します。1 ～ 999 の範囲の値を指定します。
スクリーン セーバーの起動時にロックする	スクリーン セーバーの起動時に自動ロックを適用します。

ログに記録されたプログラム イベントの表示

デフォルトでは、すべてのプログラム イベントがログ ビューアに記録されます。

プログラム イベントのログを表示するには、次のようにします。

1. ［**警告とログ**］|［**ログ ビューア**］を選択します。
2. ［警告タイプ］ドロップ ダウン リストから［**プログラム**］を選択します。

表 5－1 は、プログラム イベントで使用可能なログ ビューアのフィールドの説明です。

フィールド	説明
レベル	セキュリティ オプションの**保護レベル**に基づいたイベントのレベル。
日付 / 時間	イベントが発生した日付と時間。
種類	発生したプログラム警告のタイプ。このカラムに表示される可能性がある値： ・プログラム アクセス ・繰り返されたプログラム ・新しいプログラム
プログラム	アクセスを要求しているプログラム（アプリケーション ファイルとして表示される）。プログラム名が不明な場合は、［項目の詳細］ウィンドウの［説明］フィールドを参照します。
発信元 IP アドレス	要求を送信しているコンピュータの IP アドレス。発信元の IP アドレスを判別できない場合、このフィールドは空白のままになります。
送信先 IP アドレス	要求を受信しているコンピュータの IP アドレス。送信先の IP アドレスを判別できない場合、このフィールドは空白のままになります。
方向	イベントを発生させているのが外部からの要求であるか、外部への要求であるか、または使用しているコンピュータの内部トラフィック（データ）の結果として発生した要求であるかを特定します。
対応	要求を許可するか、ブロックするかを指定します。アクションの後に / が続きます。
回数	この行動が実行された回数。
発信元 DNS アドレス	要求を送信しているコンピュータのドメイン名サーバ。
送信先 DNS アドレス	要求を受信しているコンピュータのドメイン名サーバ。

表 5-1: プログラムのイベント ログ フィールド

記録された OSFirewall イベントの表示

デフォルトでは、すべての OSFirewall イベントがログ ビューアに記録されます。

プログラム イベントのログを表示するには、次のようにします。

1. ［**警告とログ**］|［**ログ ビューア**］を選択します。
2. ［警告の種類］ドロップダウン リストから［OSFirewall］を選択します。

表 5 － 2 は、OSFirewall イベントで使用可能なログ ビューアのフィールドの説明です。

フィールド	説明
レベル	セキュリティ オプションの**保護レベル**に基づいたイベントのレベル。
日付 / 時間	イベントが発生した日付と時間。
種類	発生した OSFirewall 警告のタイプ。このカラムに表示される可能性がある値： ・プロセス ・メッセージ ・モジュール ・レジストリ ・ファイル ・実行 ・ドライバ ・物理メモリ
サブタイプ	要求されたタイプのアクセスを開始した特定のイベント。たとえば、OpenThread はプロセスというサブタイプです。
データ	変更されようとしていたファイルへのパス。
プログラム	動作を実行したプログラムへのパスを表示します。
対応	要求を許可するか、ブロックするかを指定します。アクションの後に /manual または /auto が続き、アクションがユーザによって実行されたのか、SmartDefense Advisor によって実行されたのかが示されます。
回数	この行動が実行された回数。

表 5-2: OSFirewall イベント ログのフィールド

アドバンス プログラム設定の指定

デフォルトでは、Zone Labs セキュリティ ソフトウェア は、インターネット ゾーンとトラスト ゾーンへの接続試行およびサーバ アクセス試行をブロックするか、許可するかを常にユーザに確認します。さらに、TrueVector サービスの実行中に Zone Labs セキュリティ ソフトウェアが起動していない場合には、デフォルトでプログラム アクセスは拒否されます。

グローバルなプログラム プロパティの設定

インターネット ゾーンまたはトラスト ゾーンのプログラムがアクセスを要求するたびに、アクセスを常に許可する、拒否する、その都度問い合わせするかどうかをユーザに確認する、のいずれかに指定して、プログラム コントロールをカスタマイズできます。

グローバルなプログラム プロパティを設定するには、次のようにします。

1. ［**プログラム コントロール**］|［**メイン**］を選択します。
2. ［**詳細設定**］をクリックして［**警告と機能**］タブを選択します。
3. グローバルなプログラム オプションを指定します。

インターネット アクセスが拒否された場合に警告を表示する	Zone Labs セキュリティ ソフトウェア がプログラムへのアクセスを拒否すると、ブロックされたプログラム警告を表示します。警告を表示しないでアクセスを拒否するには、このオプションをオフにします。
アクセス許可が「問い合わせ」に設定されていて TrueVector サービスが実行中の場合、Zone Labs セキュリティ ソフトウェア が実行中でなくてもアクセスを拒否する	トロイの木馬などの独立したプロセスが、TrueVector サービスを停止させずに Zone Labs セキュリティ ソフトウェア ユーザ インターフェイスをシャットダウンすることがあります。 この設定は、そのような事態が生じた場合にアプリケーションがハングするのを防ぎます。
プログラムの一時的なインターネット アクセス許可にパスワードを要求する	アクセス許可を与える場合にパスワードの入力を要求します。プログラム警告で［はい］を選択するには、ユーザがログインしている必要があります。 パスワードなしでのアクセスを許可する場合は、このオプションをオフにします。

4. ［OK］をクリックします。

新しいプログラムのアクセス許可の設定

コンピュータ上のプログラムが初めてインターネットまたはローカル ネットワーク リソースにアクセスする際に、Zone Labs セキュリティ ソフトウェア は、新しいプログラム警告を表示します。プログラムが初めてサーバとして動作しようとした際には、サーバ プログラム警告を表示します。

また、これらのデフォルト動作の代わりに、警告を表示せずに新しいプログラムを自動的に許可またはブロックするように Zone Labs セキュリティ ソフトウェアを設定することもできます。たとえば、必要なプログラムすべてにアクセス許可をすでに与えている場合は、新たに許可を要求するプログラムに対しては、アクセスをすべて自動的に拒否するように設定できます。

新しいプログラムへの接続動作の許可を設定するには、次のようにします。

1. **［プログラム コントロール］**|**［メイン］**を選択します。
2. **［詳細設定］**をクリックします。
3. ［接続動作］エリアで、各ゾーンの設定を指定します。

常にアクセスを許可する	指定ゾーンへのすべての新しいプログラムのアクセスを許可します。
常にアクセスを拒否する	指定ゾーンへのプログラムのアクセスを拒否します。
常に許可を問い合わせる	指定ゾーンへのプログラムのアクセス許可を問い合わせる警告を表示します。

各プログラムの設定は、［プログラム］タブで行なうことができます。このパネルの設定は、［プログラム］タブに表示されていないプログラムにのみ適用されます。

新しいプログラムのサーバ動作の許可を設定するには、次のようにします。

1. **［プログラム コントロール］**|**［メイン］**を選択します。
2. **［詳細設定］**をクリックします。

［サーバ動作］エリアで、各ゾーンの設定を指定します。

常に接続を許可する	すべてのプログラムがサーバとして動作することを許可します。
常に接続を拒否する	すべてのプログラムがサーバとして動作することを拒否します。
常に許可を問い合わせる	プログラムのサーバ動作の許可を問い合わせる警告を表示します。

特定プログラムの許可の設定

プログラム コントロール レベルを**「高」**、**「中」**、**「低」**に設定することで、プログラムとそのコンポーネントがインターネットへアクセスする前やサーバとして動作する前に許可を問い合わせるかどうかをグローバルに指定できます。場合によっては、特定のプログラムについて、グローバルな設定と異なる設定をする必要が生じることもあります。たとえば、特定のプログラムへのアクセスを許可する一方で、その他のすべてのプログラムのセキュリティは「高」設定を維持する場合など、そのプログラムのみを対象に［**許可**］を設定することができます。

プログラムの許可を手動で設定すると、そのプログラムに対する許可は、後で SmartDefense Advisor を「自動」に設定した場合でも変更されません。自動プログラム アドバイスを活用するには、プログラム一覧からプログラムを削除し、次に SmartDefense Advisor を「自動」に設定します。

プログラム一覧の使用

プログラム一覧には、コンピュータ上でインターネットまたはローカル ネットワークへのアクセスを試みたプログラムの概要が表示されます。各プログラムについて、プログラム一覧には、現在の状態、信頼性、および実行を許可している機能に関する詳細情報が表示されます。プログラム一覧は、アルファベット順に表示されます。カラム ヘッダをクリックすることで、特定のカラムを基準に一覧内のプログラムをソートすることができます。コンピュータを使用すると、Zone Labs セキュリティ ソフトウェアはネットワーク アクセスを要求する各プログラムを検出し、そのプログラムを一覧に追加します。プログラム一覧にアクセスするには、**［プログラム コントロール］**|**［プログラム］**を選択します。

一覧中のプログラム名を選択すると、一覧の下の黄色の［項目の詳細］エリアにプログラム情報が表示されます。このエリアには、完全な名前、プログラムの OSFirewall ポリシー、およびポリシーの最終更新日など、プログラムに関する詳細が表示されます。

[SmartDefense Advisor] カラムと［トラスト レベル］カラムはコンピュータの OSFirewall 保護を示し、プログラムが TCP/IP パラメータの変更、ドライバのロードまたはインストール、ブラウザのデフォルト設定の

変更といったオペレーティング システム レベルのアクションを実行できるかどうかを指定します。

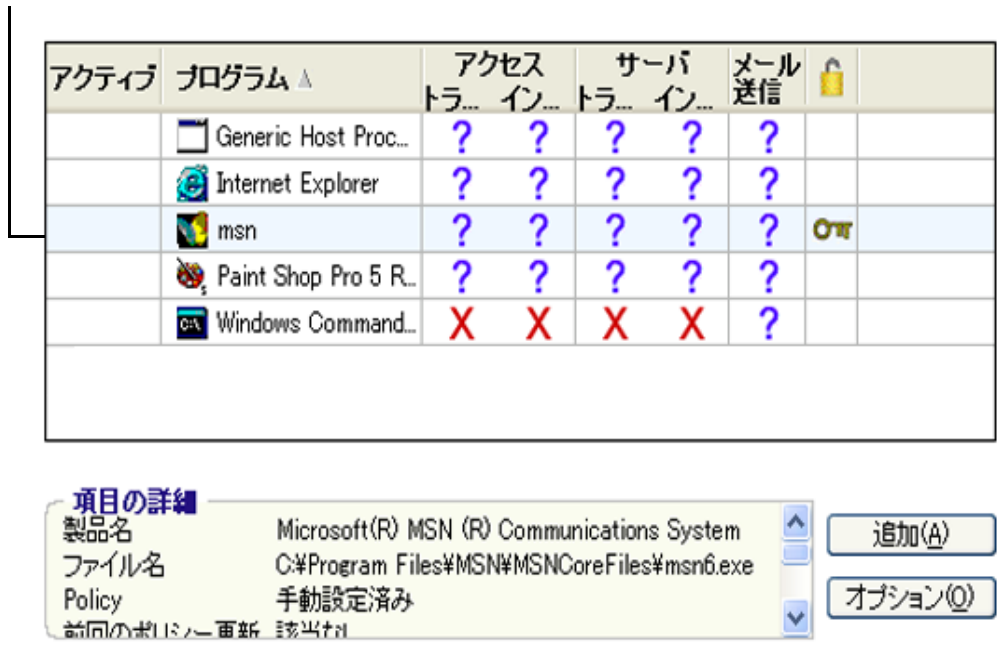


図 5-3: プログラム一覧

アクティブ
プログラムの現在のステータスを示します。緑色の円はプログラムが現在実行中であることを示します。

プログラム
プログラムの名前。

SmartDefense Advisor
[自動] はプログラム ポリシーが Zone Labs セキュリティ エキスパートによって判別されたことを意味します。[カスタム] はポリシーがユーザにより手動で判別されたことを意味します。プログラムの許可のいずれかに変更を行うと (たとえば、プログラムの列のいずれかのカラムで値を変更する)、そのプログラムの [SmartDefense Advisor] に [カスタム] と表示されます。[システム] のマークが付いたプログラムのポリシーも Zone Labs によって自動的に判別されます。これらのプログラムは [自動] ではなく [システム] のマークが付き、コンピュータのオペレーティングシステムによって使用されることが示されます。

システム プログラムのポリシーを手動で変更すると、コンピュータの通常の機能に影響する可能性があります。

トラスト レベル

[トラスト レベル] はプログラムが実行を許可されているアクションを判別します。トラスト レベルには、[スーパー]、[トラスト]、[制限]、[問い合わせ]、[抹消] の 5 つがあります。プログラムのトラスト レベル指定はポリシーによって判別されます。Zone Labs セキュリティ ソフトウェアは既知のプログラムにポリシーを自動的に割り当てます。SmartDefense Advisor セキュリティ チームはプログラムの動作と信頼性に変更がないか常に監視し、プログラム許可を適切に更新します。今日、[トラスト レベル] が [スーパー] になっているプログラムでも、セキュリティ エキスパートによってプログラムがコンピュータにリスクを負わせる可能性があると判断された場合、明日になって [トラスト レベル] が [制限] になることが考えられます。ただし、プログラムのポリシー設定が [自動] から [カスタム] に変更されると、[トラスト レベル] の変更の有無は監視されなくなります。このため、プログラムのデフォルトの

OSFirewall 設定を維持することを推奨します。この一覧で使われる記号の説明は、下記の表を参照してください。

アクセス
［アクセス］カラムは、インターネットまたはネットワークのトラストゾーンから情報を取得するためのプログラムの権限を指します。

サーバ
インターネットまたはネットワークからのアクセスをプログラムが受動的に待ち受けることを許可します。一部のプログラムではサーバ権限が必要です。

メール送信
プログラムが電子メールを送受信することを許可します。

この一覧で使われる記号の説明は、下記の表を参照してください。

記号	意味
	プログラムにはアクセス / サーバ権限が許可されています。
	［アクセス］カラムまたは［サーバ］カラムにこの記号が表示される場合、プログラムがアクセス権やサーバ権を要求すると、Zone Labs セキュリティ ソフトウェアはプログラム警告を表示します。 ［トラスト レベル］カラムにこの記号が表示される場合、プログラムが疑わしい、または危険であるとみなされるアクションを実行すると、Zone Labs セキュリティ ソフトウェア は疑わしい動作の警告または危険な動作の警告を表示します。
	プログラムにはアクセス / サーバ権限が拒否されています。
	プログラムは現在アクティブです。
	スーパー アクセス。プログラムは許可を求めずに、疑わしく危険なアクションを実行できます。警告は何も表示されません。
	トラスト アクセス。プログラムは許可を求めずに疑わしいアクションを実行できますが、危険なアクションを実行するには許可が必要です。
	制限アクセス。プログラムはトラストレベルのアクションを実行できますが、疑わしいアクションまたは危険なアクションは実行できません。
	アクセスなし。アクセスなし（抹消）記号が付いているプログラムは実行できません。

表 5-4: プログラム一覧の記号

疑わしい、または危険であるとみなされるプログラム アクションの詳細については、273 ページから始まる付録 D「プログラム動作」を参照してください。

プログラム一覧へのプログラムの追加

プログラム一覧に表示されないプログラムのアクセス許可またはサーバ許可を指定するには、一覧にプログラムを追加してから、適切な許可を与えます。

プログラムをプログラム一覧に追加するには、次のようにします。

1. **［プログラム コントロール］**|**［プログラム］**を選択し、**［追加］**をクリックします。

   ［プログラムの追加］ダイアログが表示されます。

2. 追加するプログラムを選択し、**［開く］**をクリックします。

   プログラムの実行可能ファイルを選択する必要があります（たとえば、program.exe）。

プログラム一覧のプログラムを編集するには、次のようにします。

1. **［プログラム コントロール］**|**［プログラム］**を選択します。
2. ［プログラム］カラムのプログラムを右クリックし、使用可能なオプションから 1 つ選択します。

頻繁に変更	このオプションが選択されている場合、Zone Labs セキュリティ ソフトウェア はファイルのパス情報だけを使用してプログラムの認証を行います。MD5 署名は、チェックされません。 注意：これは、低セキュリティ設定です。
オプション	［プログラム オプション］ダイアログ ボックスが表示され、プログラムのセキュリティ オプションをカスタマイズして、エキスパート ルールを作成することができます。
プロパティ	プログラムに対するオペレーティング システムのプロパティ ダイアログ ボックスを表示します。
削除	一覧からプログラムを削除します。

プログラムのインターネット アクセスの許可

多くの頻繁に使用されるプログラムでは、安全なインターネット アクセスが自動的に設定されます。プログラムが手動または自動のどちらで設定されたかを調べるには、プログラム一覧でそのプログラムを選択し、［項目の詳細］エリアの［ポリシー］フィールドを参照します。

プログラムのインターネット アクセスを許可するには、次のようにします。

1. **［プログラム コントロール］**|**［プログラム］**を選択します。

2. ［プログラム］カラムで、アクセスを与えるプログラムをクリックし、ショートカット メニューから［**許可**］を選択します。

警告に対応することでプログラムに許可を与える方法については、228 ページの「新しいプログラム警告」を参照してください。

ビルトイン ルールによって、各プログラムに一貫性のあるセキュリティ ポリシーを設定できます。インターネット ゾーンにアクセスできるプログラムは、トラスト ゾーンにもアクセスできます。また、あるゾーンでサーバ許可を付与されているプログラムには、そのゾーンへのアクセス許可も付与されています。たとえば、トラスト ゾーン / サーバで［許可］を選択するとプログラムのほかの許可も自動的に［許可］となります。

プログラムのサーバ動作の許可

トロイの木馬などの悪意のあるソフトウェアは、破壊工作をするためにサーバ権限を必要とする場合があるため、プログラムにサーバ許可を与える際には、十分な注意を払うようにします。サーバ動作の許可は、信頼ができ、正常に動作するためにサーバ許可を必要とする既知のプログラムのみに与えます。

プログラムにサーバ動作の許可を与えるには、次のようにします。

1. ［**プログラム コントロール**］|［**プログラム**］を選択します。
2. ［プログラム］カラムで、サーバ アクセスを与えるプログラムをクリックし、ショートカット メニューから［**許可**］を選択します。

プログラムへのメール送信許可の付与

メール プログラムにメール送信許可を与えると、メール プログラムによるメール メッセージの送信が可能になり、メールに関する脅威について保護が有効になります。メールの保護に関する詳細については、127 ページから始まる第 7 章「メール保護」を参照してください。

プログラムにメール送信許可を与えるには、次のようにします。

1. ［**プログラム コントロール**］|［**プログラム**］を選択します。
2. 一覧からプログラムを選択し、［メール送信］カラム内をクリックします。
3. ショートカット メニューから［**許可**］を選択します。

プログラム名を右クリックし、［**オプション**］を選択して、［プログラム オプション］ダイアログにアクセスすることもできます。

特定プログラムの許可の設定

プログラム コントロール レベルを設定すると、プログラムをどのように認証するか、アウトバウンド MailSafe 保護を使用するか、プライバシー基準に従わせるか、といったことがグローバルに決定されます。こうした設定について、プログラム一覧からプログラムごとに変更できます。

アドバンス プログラム コントロール オプションの設定

アドバンス プログラム コントロールは、未知のプログラムが信頼できるプログラムを利用してインターネットにアクセスすることや、ハッカーが Windows の CreateProcess 関数および OpenProcess 関数を使用してコンピュータを操作することを防ぐことにより、セキュリティを強化します。

プログラムについて、アドバンス プログラム コントロールを有効にするには、次のようにします。

1. **[プログラム コントロール]**|**[プログラム]** を選択します。
2. [プログラム] カラムで、プログラムを選択して **[オプション]** をクリックします。

   [プログラム オプション] ダイアログが表示されます。
3. **[セキュリティ]** タブを選択してから、アドバンス プログラム コントロール オプションを選択します。

このプログラムは、他のプログラムを使用してインターネットにアクセスする可能性があります	選択されたプログラムが他のプログラムを使用してインターネットにアクセスすることを許可します。
アプリケーション対話の許可	選択されたプログラムがコンピュータ上の OpenProcess 関数および CreateProcess 関数を使用することを許可します。

4. **[OK]** をクリックします。

プログラムのアウトバウンド メール保護の無効化

デフォルトでは、アウトバウンド メール保護はすべてのプログラムについて有効になっています。しかし、すべてのプログラムにメール送信の機能が備わっているわけではないため、保護する必要のないプログラムについて、アウトバウンド メール保護を無効にすることができます。

プログラムについて、アウトバウンド メール保護を無効にするには、次のようにします。

1. **[プログラム コントロール]**|**[プログラム]** を選択します。

2. 一覧からプログラムを選択し、[**オプション**] をクリックします。

   [プログラム オプション] ダイアログが表示されます。

3. [**セキュリティ**] タブを選択します。

4. [**このプログラムのアウトバウンド メール保護を有効にする**] チェックボックスをオフにします。

5. [**適用**] をクリックして変更を保存してから、[OK] をクリックします。

アウトバウンド メール保護に関する詳細については、129 ページの「アウトバウンド MailSafe 保護」を参照してください。

プログラムのフィルタ オプションの設定

ペアレント コントロール機能とプライバシー機能がグローバルに有効になっていても、フィルタ オプションも有効でなければ、ワープロなどの個々のプログラムは制限されたコンテンツにアクセス可能です。たとえば、ペアレント コントロールがブラウザから「http://www.playboy.com」へのアクセスをブロックしても、Microsoft Word のペアレント コントロールが有効でなければ、Word 文書内の URL をクリックすることでサイトにアクセス可能な場合があります。

プログラムのフィルタ オプションを有効にするには、次のようにします。

1. [**プログラム コントロール**]|[**プログラム**] を選択します。

2. 一覧からプログラムを選択し、[**オプション**] をクリックします。

   [プログラム オプション] ダイアログが表示されます。

3. [**セキュリティ**] タブを選択します。

4. [フィルタ オプション] で、必要な保護の横のチェックボックスをオンにし、[OK] をクリックします。

プライバシー保護の詳細については、149 ページから始まる第 8 章「プライバシー保護」を参照してください。ペアレント コントロールの詳細については、197 ページから始まる第 11 章「ペアレント コントロール」を参照してください。

認証オプションの設定

プログラムがフルパス名で認証されるか、コンポーネントで認証されるかを指定できます。デフォルトでは、すべてのプログラムがそのコンポーネントによって認証されています。

認証方法を指定するには、次のようにします。

1. [**プログラム コントロール**]|[**プログラム**] を選択します。

2. 一覧からプログラムを選択し、[**オプション**] をクリックします。

   [プログラム オプション] ダイアログが表示されます。

3. [**セキュリティ**] タブを選択します。

4. [認証] で、必要なオプションの横のチェックボックスをオンにし、[OK] をクリックします。

プログラムへのパスロック許可の設定

インターネット ロックが適用されている場合でも、パスロック許可が与えられているプログラムはインターネットへのアクセスを維持することができます。プログラムにパスロック許可を与える際に、そのプログラムが機能の実行に他のプログラム（たとえば、services.exe）を使用する場合は、使用される他のプログラムにもパスロック許可を与える必要があります。

パスロック許可を付与する、または無効にするには、次のようにします。

1. [**プログラム コントロール**]|[**プログラム**] を選択します。

2. 一覧からプログラムを選択し、[**オプション**] をクリックします。

3. [**パスロックを有効にする**] チェックボックスをオンにします。

4. [**適用**] をクリックし、[OK] をクリックします。

プログラム コンポーネントの管理

コンピュータ上のプログラムごとに、Zone Labs セキュリティ ソフトウェアがベースとなる実行可能ファイルのみを認証するか、またはそのファイルによってロードされる他の実行可能ファイルやコンポーネントをも認証するかを指定できます。さらに、個別のプログラム コンポーネントに対し、アクセスを許可または拒否できます。

コンポーネント一覧には、インターネットまたはローカル ネットワークへのアクセスを試みた許可済みプログラムのプログラム コンポーネントのリストが表示されます。[アクセス] カラムは、コンポーネントに常にアクセス許可が与えられるか、またはコンポーネントがアクセスを要求した場合に Zone Labs セキュリティ ソフトウェア が警告を表示すべきかを示します。

コンポーネント一覧は、アルファベット順に表示されます。コンポーネントのカラム ヘッダをクリックすることで、特定のカラムを基準に一覧内のコンポーネントをソートすることができます。Zone Labs セキュリティ ソフトウェア は、コンピュータの使用時にプログラムによって使用されるコンポーネントを検出し、コンポーネント一覧に追加します。

コンポーネント一覧にアクセスするには、次のようにします。

- [**プログラム コントロール**] | [**コンポーネント**] を選択します。

コンポーネント	説明	ア
actxprxy.dll	ActiveX Interface Marshaling Library	
advapi32.dll	Advanced Windows 32 Base API	
apphelp.dll	Application Compatibility Client Library	
atl.dll	ATL Module for Windows XP (Unicode)	
authz.dll	Authorization Framework	
browselc.dll	Shell Browser UI Library	
browseui.dll	Shell Browser UI Library	
clbcatq.dll	COM Services	
comctl32.dll	User Experience Controls Library	
comctl32.dll	Common Controls Library	
comdlg32.dll	Common Dialogs DLL	
comres.dll	COM Services	
credui.dll	Credential Manager User Interface	
crypt32.dll	Crypto API32	
cryptui.dll	Microsoft Trust UI Provider	

項目の詳細

図 5-5: コンポーネント一覧

プログラム コンポーネントにアクセス許可を与えるには、次のようにします。

1. ［**プログラム コントロール**］|［**コンポーネント**］を選択します。
2. 一覧からコンポーネントを選択し、［アクセス］カラム内をクリックします。
3. ショートカット メニューから［**許可**］を選択します。

プログラム用のエキスパート ルールの作成

デフォルトでは、アクセス許可またはサーバ許可を与えられたプログラムは、すべてのポートやプロトコルを使用でき、IP アドレスやホストへのアクセスも制限されません。それとは逆に、プログラムをブロックすると、これらアクセス権限は一切与えられません。特定のプログラム用のエキスパート ルールを作成すると、ポート、プロトコル、発信元アドレス、送信先アドレス、およびアクティビティを許可または拒否する日時範囲を指定して、プログラムのハイジャックに対する保護を強化することができます。また、特定の種類の通信にトラッキング オプションを適用し、許可されたプログラム通信が発生した際に警告の表示や、ログ エントリの生成をしたり、ルールを有効または無効にしたり、ランク付けした複数のルールをプログラムに適用したりすることができます。

4.0 以前のバージョンの Zone Labs セキュリティ ソフトウェア で作成したプログラム用のポート ルールは、自動的にエキスパート ルールに変換され、[プログラム オプション] ダイアログの [エキスパート] タブに表示されます。[エキスパート] タブにアクセスするには、[プログラム コントロール]|[プログラム] を選択し、[オプション] をクリックします。

プログラム用のエキスパート ルールの作成

プログラム用のエキスパート ルールは、ランク順に適用されます。したがって、プログラム用のエキスパート ルールを作成するときは、「すべてをブロック」ルールを最後に作成するようにしてください。

プログラム用のエキスパート ルールを作成するためのヒントについては、Zone Labs ユーザ フォーラム (http://www.zonelabs.com/forum) で、「プログラム規則」を検索して参照してください。

プログラム用のエキスパート ルールを作成するには、次のようにします。

1. **[プログラム コントロール]|[プログラム]** を選択し、**[オプション]** をクリックします。
2. **[エキスパート ルール]** を選択して、**[追加]** をクリックします。

   [ルールの追加] ダイアログが表示されます。

3. エキスパート プログラム ルールを作成します。

［ルールの追加］ダイアログのフィールドとオプションは、エキスパート ファイアウォール ルールの作成時に表示されるものと同じです。ただし、プログラム用のエキスパート ルールには、IGMP とカスタム プロトコルは適用できません。62 ページの「エキスパート ファイアウォール ルールの作成」を参照してください。

4. [OK] をクリックします。

エキスパート ルールの共有

エキスパート ファイアウォール ルール（[ファイアウォール] パネルの [エキスパート] タブで作成 ）を、単独のプログラムに直接適用することはできません。ルールが有効な場合は、グローバルに適用されます。同様に、特定のプログラム用に作成したエキスパート ルールは、他のプログラムに直接適用することはできません。

ただし、既存のエキスパート ルールのコピーを作成して、任意のプログラムに適用することができます。コピーに加えた変更は、オリジナルのルールには反映されないことに留意してください。

既存のエキスパート ファイアウォール ルールを個々のプログラムに適用するには、次のようにします。

1. **[ファイアウォール]**|**[エキスパート]** を選択します。
2. 適用するルールを選択して、CTRL+C を押します。
3. **[プログラム コントロール]**|**[プログラム]** を選択します。
4. ［プログラム ］カラムで、エキスパート ルールを適用するプログラムを選択して、**[オプション]** をクリックします。
5. ［エキスパート ルール ］を選択して CTRL+V を押します。

   エキスパート ルールがプログラムに適用されます。
6. **[適用]** をクリックし、[OK] をクリックします。

エキスパート ルールを無効にするには、次のようにします。

1. **[プログラム コントロール]**|**[プログラム]** を選択します。
2. エキスパート プログラム ルールを無効にするプログラムを選択し、右クリックして、ショートカット メニューから **[無効]** を選択します。

   このルールがグレイ表示されます。
3. **[適用]** をクリックし、[OK] をクリックします。

第 6 章

スパイウェアおよびウイルス保護

6

統合されたアンチウイルスおよびアンチスパイウェア機能は単一の強力な操作でコンピュータをウイルスやスパイウェアから保護します。複数のスキャン オプションはウイルスおよびスパイウェアを自動検出し、コンピュータに危害を加える前に無害にします。

Spyware Community Watch は 3000 万人を超える Zone Labs ユーザから集められた最新のスパイウェア事例に関する情報を利用して、署名データベースを更新します。

アンチウイルス機能は、ZoneAlarm Anti-virus と ZoneAlarm Security Suite でのみ利用できます。

アンチスパイウェア機能は、ZoneAlarm Pro、および ZoneAlarm Security Suite でのみ利用できます。

トピック：

- 100 ページの「スパイウェアおよびウイルス保護」
- 104 ページの「ウイルス保護オプションのカスタマイズ」
- 108 ページの「スパイウェア保護オプションのカスタマイズ」
- 110 ページの「ウイルス スキャンの実行」
- 115 ページの「スパイウェア スキャンの実行」
- 121 ページの「ウイルスおよびスパイウェア保護の状況の表示」
- 122 ページの「ウイルス保護のモニタリング」

スパイウェアおよびウイルス保護

アンチスパイウェア機能はコンピュータ上のスパイウェア コンポーネントを検出し、自動的に削除するか、隔離してリスクの評価後に手動で削除できるようにします。

アンチウイルス機能は、ファイルをスキャンして、既知のウイルスのデータベースや、ウイルスの活動を反映する傾向のある一連の特徴と照合することにより、既知および未知のウイルスがコンピュータに影響を及ぼさないようにします。ファイルのスキャンは、ファイルを開く時や閉じる時、実行する時に実行できます。また、コンピュータ全体のスキャンの一部として実行することもできます。ウイルスが検出されると、Zone Labs セキュリティ ソフトウェア は、ウイルスに感染したファイルを修復するか、そのファイルへのアクセスを禁止することによって、それらのファイルによる被害を防ぎます。

ウイルスおよびスパイウェア保護の有効化

ZoneAlarm Security Suite をご使用で、インストール後に設定ウィザードで Viand Virus 保護機能を有効にしなかった場合は、手動で有効にすることができます。

Zone Labs ウイルス保護機能と、他のウイルス保護ソフトウェアとの間には互換性はありません。ウイルス保護機能を有効にする前に、お使いのコンピュータから、他のアンチウイルス ソフトウェア（機能の一部としてウイルス保護が組み込まれている製品も含みます）をアンインストールする必要があります。一部のアンチウイルス アプリケーションについては、Zone Labs セキュリティ ソフトウェア で自動的にアンインストールできます。自動的にアンインストールできないプログラムをご使用の場合は、Windows のコントロール パネルにある［プログラムの追加と削除］を使用してアンインストールできます。

ウイルスおよびスパイウェア保護を有効にするには、次のようにします。

1. ［**アンチウイルス / アンチスパイウェア**］|［**メイン**］を選択します。
2. ［**アンチウイルス**］エリアで、［**オン**］を選択します。
3. ［**アンチスパイウェア**］エリアで、［**オン**］を選択します。

スキャンのスケジューリング

コンピュータ上でのウイルスおよびスパイウェアのスキャンの実行は、データの完全性とコンピュータ環境を保護するためにユーザが実行できる作業のなかで最も重要なものです。スキャンは一定の間隔で実行すると最も効果的であることから、通常、自動的に実行するタスクとしてスケジュールしておくことをお勧めします。スケジュールしたスキャンの実行時刻にコンピュータの電源が入っていなかった場合は、コンピュータが次に起動してから 15 分後にスキャンが実行されます。

スキャンをスケジュールするには、次のようにします。

1. **［アンチウイルス / アンチスパイウェア］**|**［メイン］** を選択します。
2. ［アンチウイルス］エリアで、**［詳細オプション］** をクリックします。

   ［詳細オプション］ダイアログが表示されます。
3. ［詳細設定］で、**［スキャン スケジュール］** を選択します。
4. **［ウイルスのスキャン］** チェックボックスをオンにし、スキャンの日時を指定します。
5. スキャン頻度を指定します。

   デフォルトでは、ウイルス スキャンは週に一度実行されます。
6. **［スパイウェアのスキャン］** チェックボックスをオンにし、スキャンの日時を指定します。
7. スキャン頻度を指定します。

   デフォルトでは、スパイウェア スキャンは週に一度実行されます。
8. **［OK］** をクリックします。

ウイルスおよびスパイウェア保護のアップデート

あらゆるウイルスまたはスパイウェア アプリケーションは定義ファイルという固有の識別情報を含みます。これらの定義ファイルはコンピュータ上のウイルスとスパイウェアを特定するために使用されるマップです。新しいウイルスまたはスパイウェア アプリケーションが発見されると、Zone Labs セキュリティ ソフトウェア はこうした新しい脅威を検出するのに必要な定義でデータベースを更新します。したがって、ウイルス定義ファイルのデータベースが古くなると、コンピュータはウイルスおよびスパイウェアに対して脆弱になります。[**アンチウイルス / アンチスパイウェア**] パネルの [メイン] タブにある [**詳細**] エリアに定義ファイルのステータスが表示されます。

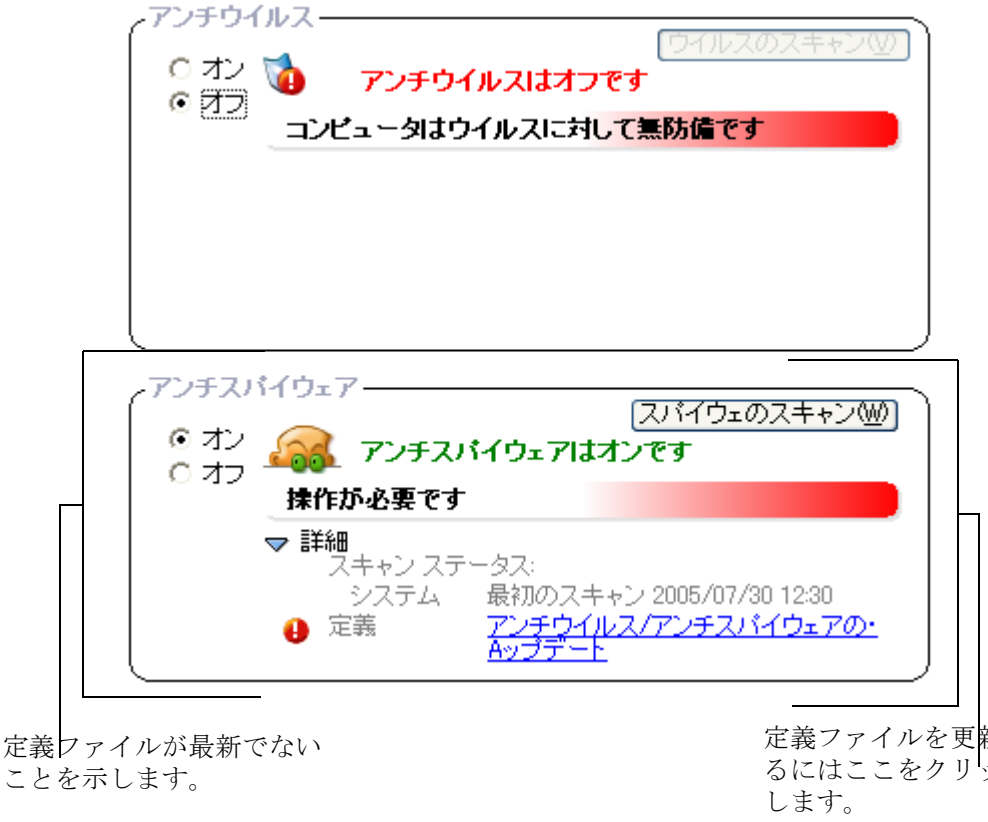


図 6-1: アンチウイルスとアンチスパイウェアのステータス

自動アップデート機能を有効にすることで、常に最新の定義ファイルが利用可能になった時点で受け取ることができます。

自動アップデートを有効にするには、次のようにします。

1. [**アンチウイルス / アンチスパイウェア**] | [**メイン**] を選択します。

2. ［アンチウイルス］エリアで、**［詳細オプション］**をクリックします。

   ［詳細オプション］ダイアログが表示されます。

3. **［アップデート］**を選択して、**［自動アンチウイルス アップデートを有効にする］**チェックボックスをオンにします。

4. **［自動アンチスパイウェア アップデートを有効にする］**チェックボックスをオンにします。

5. **[OK]** をクリックします。

ウイルス保護オプションのカスタマイズ

実行するスキャンの種類を選択するのに加えて、ウイルス検出に使用される方法の指定や処理方法の設定が可能です。

Zone Labs セキュリティ ソフトウェア は、システムスキャン、アクセス中スキャン、およびメール スキャンという複数の種類のウイルス スキャンを提供して、お使いのコンピュータとデータを保護します。

スキャン ターゲットの指定

システム スキャンの実行時にスキャンされるドライブ、フォルダ、およびファイルを指定できます。項目の横のチェックボックスを選択することにより、スキャンから除外したり、スキャンに含めたりすることができます。デフォルトでは、Zone Labs セキュリティ ソフトウェアはローカル ハードディスクのみをスキャンします。

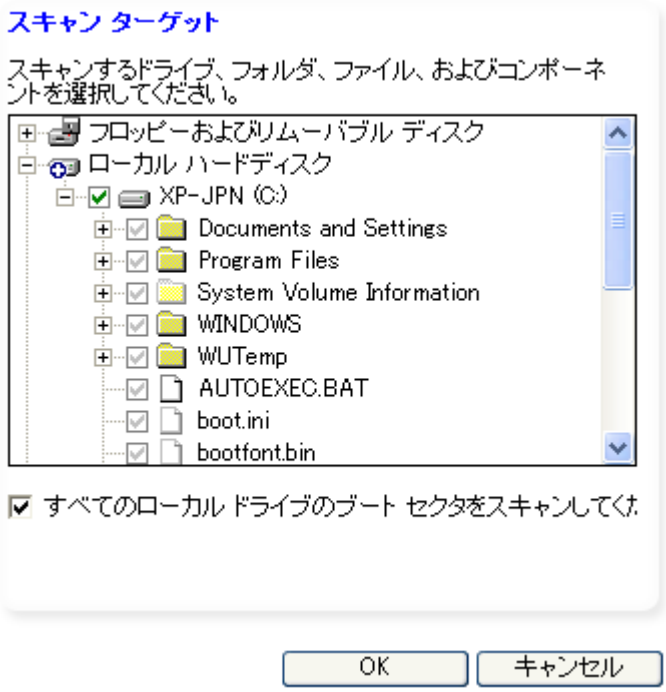


図 6-2: ［スキャン ターゲット］ダイアログ ボックス

表 6-2 では、［スキャン ターゲット］ダイアログ ボックスに表示される

アイコンを説明しています。

アイコン	説明
	選択されたディスクとすべてのサブフォルダおよびファイルはスキャンに含まれます。
	選択されたディスクとすべてのサブフォルダおよびファイルはスキャンから除外されます。
	選択されたディスクはスキャンに含まれますが、1 つ以上のサブフォルダまたはファイルはスキャンから除外されます。
	選択されたディスクはスキャンから除外されますが、1 つ以上のサブフォルダまたはファイルはスキャンに含まれます。
	選択されたフォルダはスキャンに含まれます。グレーのチェック マークは、これより上位にあるディスクまたはフォルダのスキャンが有効になっているので、このフォルダまたはファイルのスキャンが有効であることを示します。
	選択されたフォルダはスキャンから除外されます。グレーの「x」チェック マークは、これより上位にあるディスクまたはフォルダのスキャンが無効になっているので、このフォルダまたはファイルのスキャンが無効であることを示します。

表 6-3: スキャン ターゲットを示すアイコン

スキャン ターゲットを指定するには、次のようにします。

1. **[アンチウイルス / アンチスパイウェア]**|**[メイン]** を選択します。
2. **[詳細オプション] をクリックします。**

   [詳細オプション] ダイアログが表示されます。
3. [ウイルス管理] で、**[スキャン ターゲット]** を選択します。
4. スキャンするドライブ、フォルダ、およびファイルを選択してください。
5. **[すべてのローカル ドライブのブート セクタをスキャンする]** チェックボックスをオンまたはオフにして、**[OK]** をクリックします。

アクセス スキャン

アクセス スキャンは、お使いのコンピュータ上に潜んでいるウイルスを検出して処理することにより、ウイルスからコンピュータを守ります。アクセス スキャンは、デフォルトで有効になっています。アクセス スキャンは、最もアクティブな形のウイルス保護です。ファイルを開いたり、実行したり、閉じる際に、ウイルスがないかどうかスキャンします。これにより、ウイルスを即時に検出して対応することができます。

アクセス スキャンを有効にするには、次のようにします。

1. **［アンチウイルス / アンチスパイウェア］**|**［メイン］** を選択します。
2. **［保護］** エリアで、**［詳細オプション］** を選択します。

   ［高度なアンチウイルス設定］ダイアログが表示されます。
3. ［詳細設定］で、**［アクセス スキャン］** を選択します。
4. **［アクセス スキャンを有効にする］** チェックボックスをオンにして、**[OK]** をクリックします。

メール スキャン

メール スキャンは、MailSafe が提供する保護の上に構築され、メールの本文と添付ファイルに含まれているウイルスをスキャンして、それらが破壊活動を行えないように削除します。MailSafe ではファイル拡張子をベースにして、有害な可能性のある添付ファイルがないかどうかスキャンしますが、メール スキャン機能は、添付ファイルを既知ウイルスの署名ファイルと比較して、有害なファイルがないかどうかスキャンします。ウイルスに感染した添付ファイルが検出されると、その添付ファイルはメールから削除され、代わりに、削除されたファイルについての詳細が記載されたテキスト ファイルのログが添付されます。メール スキャンの実行についての詳細は、146 ページの「メールのアンチウイルス保護」を参照してください。メール スキャンは、デフォルトで有効になっています。

メール スキャンを有効または無効にするには、次のようにします。

1. **［アンチウイルス / アンチスパイウェア］**|**［メイン］** を選択し、**［詳細オプション］** をクリックします。

   ［詳細オプション］ダイアログが表示されます。
2. ［ウイルス管理］で、**［メール スキャン］** を選択します。
3. **［メール スキャンを有効にする］** チェックボックスをオンまたはオフにして、**[OK]** をクリックします。

自動ウイルス処理の有効化

ウイルスの感染が検出されると、[スキャン] ダイアログに [隔離]、[修復]、または [削除] という利用可能な処理オプションが表示されます。デフォルトでは、Zone Labs セキュリティ ソフトウェアは、ウイルスに感染したファイルの処理を自動的に試みます。ファイルが修復できない場合には、ユーザが適切な対応を取れるよう、[スキャン] ダイアログに情報が表示されます。

自動ウイルス処理を有効にするには、次のようにします。

1. **[アンチウイルス / アンチスパイウェア]**|**[メイン]** を選択し、**[詳細オプション]** をクリックします。
2. [ウイルス管理] で、**[自動処理]** を選択します。
3. 必要な処理オプションを選択します。

	警告する - 自動的に処理しない
	修復を試みて、修復が失敗した場合は警告する
	修復を試みて、修復が失敗した場合は隔離する（推奨）

4. [OK] をクリックします。

ウイルス検出方法の指定

ファイルをスキャンし、ウイルスを検出するために、発見的分析とバイトレベル スキャンという 2 つの方法があります。発見的分析では、ウイルスの持つ特徴的な動作に基づいてファイルをスキャンし、感染を検出します。発見的分析は、デフォルトで有効になっています。バイトレベル フィルタでは、ファイルを 1 バイト単位でスキャンして、ウイルスを検出します。バイトレベル スキャンの実行には長時間を要するため、この方法の使用は、大きなウイルス攻撃を受けた後で感染ファイルが残っていないことを確認する場合のみとすることをお勧めします。

発見的スキャンの有効化または無効化はメール添付ファイルのスキャンには影響を与えません。添付ファイルはこの方法でスキャンされます。バイト レベル スキャンはアクセス スキャンおよびメール スキャンをサポートしません。

検出方法を指定するには、次のようにします。

1. **[アンチウイルス / アンチスパイウェア]**|**[メイン]** を選択し、**[詳細オプション]** をクリックします。

   [詳細オプション] ダイアログが表示されます。
2. **[ウイルス管理]** で、**[検出]** を選択します。
3. 使用する検出方法を選択し、[OK] をクリックします。

スパイウェア保護オプションのカスタマイズ

実行するスキャンの種類を選択するのに加えて、スパイウェア検出に使用される方法の指定や処理方法の設定が可能です。

Zone Labs セキュリティ ソフトウェア は、システムスキャン、アクセス中スキャン、およびメール スキャンという複数の種類のウイルス スキャンを提供して、お使いのコンピュータとデータを保護します。

自動スパイウェア処理の有効化

スパイウェアが検出されると、[スキャン] ダイアログに [隔離]、または [削除] という利用可能な処理オプションが表示されます。[スキャン] ダイアログには、ユーザが適切なアクションをとれるように推奨するスパイウェア処理方法が表示されます。

自動ウイルス処理を有効にするには、次のようにします。

1. **[アンチウイルス / アンチスパイウェア]**|**[メイン]** を選択し、**[詳細オプション]** をクリックします。
2. [スパイウェア管理] で、**[自動処理]** を選択します。
3. **[自動スパイウェア処理を有効にする]** チェックボックスをオンにして、**[OK]** をクリックします。

スパイウェア検出方法の指定

アクティブなスパイウェアの有無についてコンピュータのレジストリを検索するデフォルトの検出に加えて、潜伏しているスパイウェアと見つけにくいスパイウェアを検出するための方法があります。

スパイウェア検出方法を指定するには、次のようにします。

1. **[アンチウイルス / アンチスパイウェア]**|**[メイン]** を選択し、**[詳細オプション]** をクリックします。
2. [スパイウェア管理] で、**[検出]** を選択します。
3. **[スパイ Cookie のスキャン]** チェックボックスをオンにします。
4. [最大強度検出] で、必要なオプションを選択します。

インテリジェント クイック スキャン	このオプションはデフォルトで選択されます。
全システム スキャン	ローカル ファイル システムをスキャンします。このオプションはスキャンのパフォーマンスを低下させます。このオプションはコンピュータに検出されていないスパイウェアが存在することを疑っている場合にのみ選択します。

詳細検査スキャン	コンピュータ上のデータを 1 バイトずつスキャンします。このオプションはスキャンのパフォーマンスを低下させます。このオプションはコンピュータに検出されていないスパイウェアが存在することを疑っている場合にのみ選択します。

5. [OK] をクリックします。

スキャンからのスパイウェアの除外

一部のスパイウェアはコンピュータに危害を加えたり、データをハッカーに対して脆弱にしたりする可能性がありますが、多くの良性のアプリケーションがスキャン時にスパイウェアとして検出されます。こうしたアプリケーション（音声認識ソフトウェアなど）を使用している場合は、例外リストに追加することにより、スパイウェア スキャンから除外できます。項目を右クリックし、メニューから［常に無視］を選択して、スパイウェアを例外リストに追加できます。

スパイウェアが例外リストに含まれると、スパイウェア スキャン中に検出されません。スパイウェアが誤って例外リストに追加された場合は、手動で削除できます。

スパイウェアを例外リストから削除するには、次のようにします。

1. **［アンチウイルス / アンチスパイウェア］|［メイン］** を選択し、**［詳細オプション］** をクリックします。
2. ［スパイウェア管理］で、**［例外］** を選択します。
3. ［スパイウェア処理の例外］エリアで、削除するスパイウェア アプリケーションを選択し、**［リストから削除する］** をクリックします。
4. [OK] をクリックします。

スパイウェア攻撃の防止

スパイウェアはコンピュータに侵入するために、正当なプログラムを装い、ユーザを騙してファイルのアクセスや機能の実行に関する許可を得ることがよくあります。オペレーティング システムの更新を警告するポップアップが表示内容のとおり無害であることをどうやって確認すればよいでしょうか。Zone Labs セキュリティ ソフトウェア はスパイウェアが自分自身をコンピュータ上にインストールするのを防ぐ特殊なコントロールを提供します。プログラム一覧上の［SmartDefense Advisor］カラムと［トラストレベル］カラムはプログラムが特定の機能を実行する権限を識別します。これらのコントロールとスパイウェアからの保護のしくみについては、85 ページの「プログラム一覧の使用」を参照してください。

ウイルス スキャンの実行

コンピュータ上でウイルス スキャンを開始するにはいくつかの方法があります。

- **[アンチウイルス/アンチスパイウェア]** パネルの［メイン］タブにある［アンチウイルス］エリアの **［ウイルスのスキャン］** をクリックできます。
- コンピュータ上のファイルを選択して右クリックし、**[Zone Labs Anti-virus によるスキャン]** を選択できます。
- システム スキャンを 1 回のみ、あるいは一定の間隔で実行するようスケジュールできます。
- ファイルを開くことができます（アクセス スキャンが有効な場合）。

最大 5 つのスキャンを同時に実行できます。スキャンは、最初に開始したものから順に実行されます。システム スキャンでは、お使いのコンピュータ上のすべてのコンテンツを一度にスキャンすることができ、さらに高いレベルの保護を提供します。システム スキャンでは、コンピュータのハード ディスク上に潜んでいるウイルスを検出します。システム スキャンを定期的に実行することで、アンチウイルス署名ファイルを確実に最新の状態に保つことができます。

システム全体を厳密にスキャンすることから、完了までには多少時間がかかります。このため、システム全体のスキャンの実行中には、ご使用のシステムのパフォーマンスが低下する可能性があります。コンピュータの使用率が最も低い時間帯にシステム スキャンを実行するようスケジュールすることで、作業フローに対する影響を回避することができます。

スキャンの実行中に［スキャン］ダイアログで［一時停止］をクリックすると、現在のスキャンが停止し、アクセス スキャンが無効になります。［一時停止］を再度クリックすると、スキャンが再開し、アクセス スキャンが有効になります。

ウイルススキャン結果の理解

スキャンを開始する方法に関係なく、スキャンの結果は［スキャン結果］ダイアログ ボックス（図 6-4 参照）で表示されます。

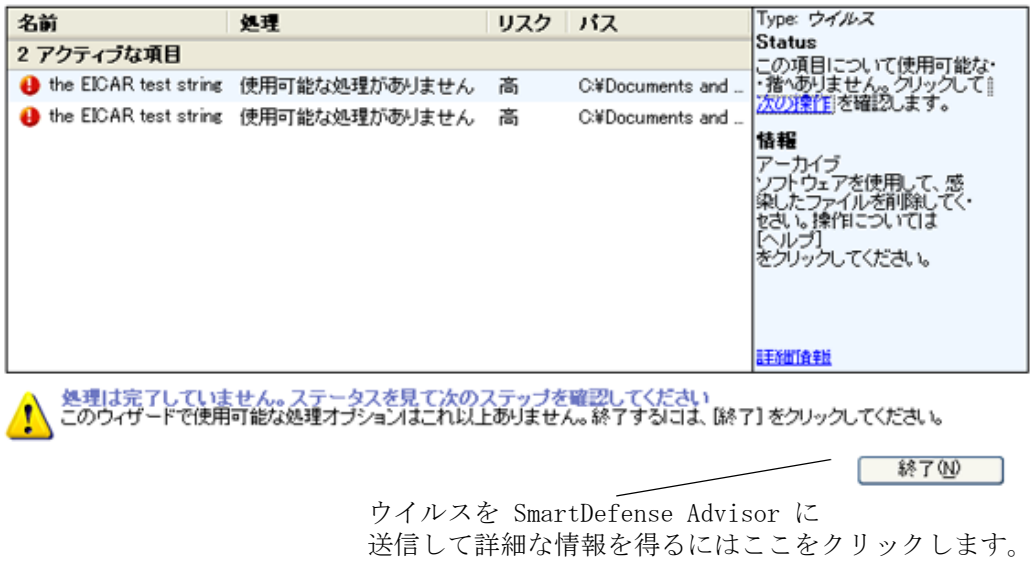


図 6-4:［ウイルス スキャン結果］ダイアログ

［スキャンの詳細］ダイアログの［アクティブな項目］エリアに、スキャン中に発見され、自動的に処理できなかった感染が一覧表示されます。［処理］カラムの推奨処理を受け入れるには、**［適用］**をクリックします。［自動処理］の下に表示される項目は既に処理済みなので、さらにアクションを取る必要はありません。

名前
感染の原因となったウイルスの名前。

処理
感染に適用される処理を指定します。可能な値は［隔離］または［削除］です。

セキュリティ リスク
感染のリスク レベルを示します。すべてのウイルスは「高」リスクとみなされます。

パス

感染の原因となったウイルスの場所。

種類
検出されたスパイウェアのカテゴリ。このフィールドの可能な値にはキーロギング ソフトウェアや トラッキング Cookie があります。

ステータス
ファイルが修復されたか、削除されたか、あるいは感染した状態のままであるかを示します。Zone Labs セキュリティ ソフトウェア が項目を処理できなかった場合、ここに［**次の操作**］リンクが表示されることがあります。このリンクに従うと、詳細な情報と指示が得られます。

情報
感染に関する詳細情報を提供します。ウイルスまたはスパイウェアに関する情報を得るには、［**詳細情報**］リンクをクリックします。

ウイルス ファイルの手動処理

自動処理を有効にしていない場合や、ファイルを自動的に修復できなかった場合には、［スキャンの詳細］ダイアログから手動でファイルを処理することができます。

ファイルを手動で処理するには、次のようにします。

1. ［スキャン結果］ダイアログで、処理する項目を選択します。
2. ［処理］カラムで、必要な処理オプションを選択します。

修復	選択したファイルの修復を試みます。
削除	選択したファイルを削除します。
隔離	感染したファイルに .z16 という拡張子を追加して無害にします。ファイルは隔離されます。

3. ファイルの処理が終わったら、［**閉じる**］をクリックします。

アーカイブ内のファイルの修復

感染したファイルがアーカイブ ファイル（.zip ファイルなど）に含まれている場合、Zone Labs セキュリティ ソフトウェア は、そのままの状態ではファイルの修復、削除、隔離などの処理を行うことはできません。

アーカイブ内のファイルを修復するには、次のようにします。

1. ［**アンチウイルス / アンチスパイウェア**］|［**メイン**］を選択し、［**詳細オプション**］をクリックします。
2. ［**アクセス スキャン**］を選択し、［**アクセス スキャンを有効にする**］チェックボックスをオンにします。
3. ［**適用**］をクリックし、［**OK**］をクリックします。

4. ［スキャン結果］ダイアログに表示されたファイルを、WinZip などのアーカイブ ユーティリティで開きます。

   アクセス スキャンにより、ファイルが感染していないかどうかスキャンされます。［スキャン結果］ダイアログに、スキャンの結果が表示されます。この方法でもファイルが修復できない場合は、112 ページの「ウイルス ファイルの手動処理」を参照してください。

Zone Labs での確認用のウイルスおよびスパイウェアの送信

不正を疑われるプログラムを Zone Labs, LLC. に報告および送信することは、インターネット ユーザのセキュリティと保護の向上に役立ちます。Zone Labs セキュリティ チームは受信したすべての情報を監視し、新しいファイルがあるかどうかを確認します。Zone Labs セキュリティ チームは提出された情報に対して適宜対応し、ユーザに連絡して送信されたファイルの詳細を確認することがあります。

毎日多くの不正プログラムが発覚するため、ユーザが送信するすべてのファイルに応答できません。ただし、ユーザの支援には感謝し、インターネットのセキュリティ保護にご協力いただいていることに御礼申し上げます。ご質問やご意見がある場合は、security@zonelabs.com までご連絡ください。

Zone Labs で確認するために不正プログラムを送信するには、次のようにします。

1. 不正プログラムをパスワード保護された .zip アーカイブ内に格納し、パスワードを *infected* に設定します。

   パスワード保護されたアーカイブを作成する際のヘルプが必要な場合は WinZip のヘルプを参照してください。

2. .zip ファイルを malware@zonelabs.com に送信します。

   このメール アドレスは Zone Labs セキュリティ チームに不正プログラムを送信する場合にのみ使用します。

不正プログラム ファイルの送信は、安全に実行できないと思われたり、システムへの感染や損害のリスクが高まる可能性があったりする場合は行わないでください。悪意の可能性があるため、疑わしい不正プログラム ファイルを他者にメール送信しないでください。

記録されたウイルス イベントの表示

デフォルトでは、すべてのウイルス イベントがログ ビューアに記録されます。

ウイルス イベントのログを表示するには、次のようにします。

1. **［警告とログ］|［ログ ビューア］**を選択します。

2. ［警告の種類］ドロップ ダウン リストから［**ウイルス**］を選択します。

表 6-3 は、ウイルス イベントで使用可能なログ ビューアのフィールドの説明です。

フィールド	情報
日付	感染した日付。
種類	発生したイベントの種類。このフィールドに表示される可能性がある値： ・アップデート ・スキャン ・処理 ・電子メール
ウイルス名	ウイルスの共通名。たとえば、*iloveyou.exe* など。
ファイル名	感染したファイルの名前、スキャンされたファイルの名前、アップデートまたはエンジンの名前とバージョン番号。
対応	Zone Labs セキュリティ ソフトウェア で通信が処理された方法。表示される可能性がある値は次のとおりです。 ・更新済み、更新取消、更新失敗 ・スキャン済み、スキャン取消、スキャン失敗 ・ファイル修復済み、ファイル修復失敗 ・隔離済み、隔離失敗 ・駆除済み、駆除失敗 ・リストア済み、リストア失敗 ・名前変更済み、名前変更失敗
アクタ	アクションが手動であるか自動であるか。
電子メール	ウイルスが電子メール中に検出された場合、感染メッセージの送信者の電子メール アドレス。

表 6-5: ウイルス イベント ログのフィールド

スパイウェア スキャンの実行

コンピュータ上でスパイウェア スキャンを開始するにはいくつかの方法があります。

- **[アンチウイルス/アンチスパイウェア]** パネルの［メイン］タブにある［**アンチスパイウェア**］エリアの［**スパイウェアのスキャン**］をクリックできます。
- コンピュータ上のファイルを選択して右クリックし、**[Zone Labs Anti-virus によるスキャン]** を選択できます。
- システム スキャンを 1 回のみ、あるいは一定の間隔で実行するようスケジュールできます。

■ ファイルを開くことができます（アクセス スキャンが有効な場合）。

最大 5 つのスキャンを同時に実行できます。スキャンは、最初に開始したものから順に実行されます。システム スキャンでは、お使いのコンピュータ上のすべてのコンテンツを一度にスキャンすることができ、さらに高いレベルの保護を提供します。システム スキャンでは、コンピュータのハード ディスク上に潜んでいるウイルスを検出します。システム スキャンを定期的に実行することで、アンチウイルス署名ファイルを確実に最新の状態に保つことができます。

システム全体を厳密にスキャンすることから、完了までには多少時間がかかります。このため、システム全体のスキャンの実行中には、ご使用のシステムのパフォーマンスが低下する可能性があります。コンピュータの使用率が最も低い時間帯にシステム スキャンを実行するようスケジュールすることで、作業フローに対する影響を回避することができます。

スパイウェア スキャン結果の理解

図 6-4 に示すように、スパイウェア スキャンの結果は、[スキャン結果] ダイアログ ボックスに表示されます。

図 6-6: [スパイウェア スキャン結果] ダイアログ

[スキャンの詳細] ダイアログの [アクティブな項目] エリアに、スキャ

ン中に発見され、自動的に処理できなかった感染が一覧表示されます。[処理] カラムの推奨処理を受け入れるには、**[適用]** をクリックします。[自動処理] の下に表示される項目は既に処理済みなので、さらにアクションを取る必要はありません。

名前
スパイウェアの名前。

処理
感染に適用される処理を指定します。可能な値は [隔離] または [削除] です。

セキュリティ リスク
感染のリスク レベルを示します。このカラムに表示される可能性がある値：

- 低－アドウェアまたはその他の良性ではあるが迷惑なソフトウェア。
- 中－潜在的なプライバシーの侵害。

■ 高ーセキュリティの脅威をもたらします。

パス

感染の原因となったウイルスまたはスパイウェアの場所。

種類
検出されたスパイウェアのカテゴリ。このフィールドの可能な値にはキーロギング ソフトウェアや トラッキング Cookie があります。

ステータス
ファイルが修復されたか、削除されたか、あるいは感染した状態のままであるかを示します。Zone Labs セキュリティ ソフトウェア が項目を処理できなかった場合、ここに［**次の操作**］リンクが表示されることがあります。このリンクに従うと、詳細な情報と指示が得られます。

情報
感染に関する詳細情報を提供します。ウイルスまたはスパイウェアに関する情報を得るには、［**詳細情報**］リンクをクリックします。

スパイウェア スキャン結果中のエラー

スパイウェアの結果に［エラー］、［使用可能な処理がありません］、［処理失敗］が含まれる場合、コンピュータまたは他のファイルの整合性に対するリスクを負うことなく、スパイウェアを自動削除する方法がまだ存在しないことを意味します。これは珍しいことではありません。なぜなら、スパイウェアの作成者は強引な手法を用いて、スパイウェアが引き起こす損害とは無関係にコンピュータ上に留めておくことが多いからです。

ほとんどの場合、手動の処理が利用できます。処理を特定するには、Google や Yahoo などの検索エンジンでスパイウェアの名前と「削除」という語を組み合わせて入力し、削除方法を確認します。また、弊社は常にこうしたスパイウェアを調査し、安全な削除方法を開発しています。したがって、後日処理を提供できる場合があります。

隔離内の項目の表示

ウイルスまたはスパイウェア スキャン中に検出された項目は自動的に処理または削除できないことがあります。通常、こうした項目は隔離され、無害になりますが保存されます。後日、ウイルスおよびスパイウェア署名ファイルを更新後に処理できることがあります。

隔離されたウイルスを表示するには、次のようにします。

1. ［**アンチウイルス / アンチスパイウェア**］を選択します。
2. ［**隔離**］タブを選択します。

3. ［隔離された表示］ドロップダウン リストから、［ウイルス］を選択します。

隔離中のウイルス表示には次のカラムの情報が含まれます。

感染
感染の原因となったウイルスの名前。

隔離日数
ウイルスが隔離中の日数。

パス
コンピュータ上のウイルスの場所。

隔離されたスパイウェアを表示するには、次のようにします。
1. ［アンチウイルス / アンチスパイウェア］を選択します。
2. ［隔離］タブを選択します。
3. ［隔離された表示］ドロップダウン リストから、［スパイウェア］を選択します。

隔離中のスパイウェア表示には次のカラムの情報が含まれます。

種類
感染の原因となったウイルスの名前。

名前
検出されたスパイウェアの名前。

リスク
感染のリスク レベル。スパイウェアがアドウェアのように良性であるか、キーロギング ソフトウェアのように深刻な脅威であるかを示します。

隔離日数
スパイウェアが隔離中の日数。

記録されたスパイウェア イベントの表示

デフォルトでは、すべてのスパイウェア イベントがログ ビューアに記録されます。

ログに記録されたスパイウェア イベントを表示するには、次のようにします。
1. ［警告とログ］|［ログ ビューア］を選択します。

2. ［警告の種類］ドロップ ダウン リストから［**スパイウェア**］を選択します。

表 6-3 に、スパイウェア イベントで表示されるログ ビューアのフィールドの例を示します。

フィールド	情報
日付	感染した日付。
種類	検出されたスパイウェアの種類。このフィールドに表示される可能性がある値： ・アドウェア ・ブラウザ ヘルパ オブジェクト ・ダイヤラ ・キーロガー ・スクリーンロガー ・トロイの木馬 ・ワーム ・スパイ Cookie
スパイウェア名	スパイウェアの共通名。たとえば、*NavExcel* など
ファイル名	スパイウェア ファイルの名前。たとえば、*gmt.exe* など。
操作	Zone Labs セキュリティ ソフトウェア でスパイウェアが処理された方法。
アクタ	アクションがユーザで処理されたか（手動）、Zone Labs セキュリティ ソフトウェアで処理されたか（自動）。

表 6-7: スパイウェア イベント ログのフィールド

ウイルスおよびスパイウェア保護の状況の表示

ウイルスおよびスパイウェア保護の状況は、2 箇所で確認できます。1 つは［**概要**］|［**状況**］ページで、もう 1 つは［**アンチウイルス / アンチスパイウェア**］|［**メイン**］タブです。

［アンチウイルス / アンチスパイウェア］パネルの［メイン］タブに、ウイルスおよびスパイウェア保護の状況が表示されます。このエリアで次の処理を行うことができます。

- ウイルスおよびスパイウェア保護が有効であることの確認。
- 最後のスキャン日時。
- 定義ファイルの更新。
- スキャンの開始。
- 最新のスキャン結果の表示。
- 詳細設定のアクセス。

［概要］パネルに表示される状況についての詳細は、16 ページから始まる第 2 章「［状況］タブの使用」を参照してください。以下のセクションでは、［アンチウイルス / アンチスパイウェア］パネルの［メイン］タブに表示される状況について説明します。

ウイルス保護のモニタリング

アンチウイルス ソフトウェア製品をインストールすることは、お使いのコンピュータをウイルスから守るうえで重要なポイントの 1 つです。ただし、新たに作成されたウイルスに対してコンピュータを確実に保護するためには、アンチウイルス ソフトウェアをインストールした後も、常に最新の状態に保つ必要があります。

どのアンチウイルス ソフトウェア製品を使用しているかに関わらず、次のいずれかの状態に当てはまる場合は、お使いのコンピュータがウイルスの攻撃を受ける危険性があります。

- お使いのアンチウイルス ソフトウェアの試用期間、または有効期限が切れている。
- ウイルス署名ファイルが最新ではない。

ZoneAlarm、ZoneAlarm Anti-virus、ZoneAlarm Pro、および ZoneAlarm Security Suite では、アンチウイルス モニタリング機能を備えています。

アンチウイルス モニタリングは、コンピュータにインストールされているアンチウイルス ソフトウェアをチェックして、アンチウイルス ソフトウェアが最新状態ではない場合や停止されている場合にユーザに通知する、二次的な防御システムです。この二次的な警告システムは、アンチウイルス ソフトウェアに組み込まれている警告やアップデート システムのバックアップとして動作します。対応していないアンチウイルス製品もありますので、あらかじめご了承ください。

ほとんどのアンチウイルス製品は自動アップデート機能を備えており、ウイルス定義ファイルが古くなると警告が表示されます。

モニタリング可能なソフトウェア

現在、アンチウイルス モニタリングは普及している次のメーカーのアンチウイルス ソフトウェアを検出します。

- Symantec
- McAfee
- Computer Associates

■ Trend Micro

アンチウイルス モニタリングでは現在、これら以外のアンチウイルス製品は認識されません。ただし、その場合でも ZoneAlarm 製品の動作には影響はありません。お使いのコンピュータのセキュリティは最大限に保護されます。Zone Labs セキュリティ ソフトウェア では今後、認識できるアンチウイルス製品をさらに追加する予定です。お使いのアンチウイルス製品が現在サポートされていない場合には、アンチウイルス モニタリング機能をオフにします。アンチウイルス モニタリングはアンチウイルス製品をモニタリングするのみの機能です。ファイアウォールに対する影響や、セキュリティに対する直接の影響はないため、心配する必要はありません。

ZoneAlarm、ZoneAlarm Pro、および ZoneAlarm Wireless でのモニタリング

これらの製品では、[アンチウイルス モニタリング] パネルが表示されます。このパネルから、お使いのアンチウイルス製品の状況を確認できます。また、モニタリングのオン / オフを切り替えることができるほか、モニタリング警告のオン / オフのみを切り替えることもできます。

モニタリングおよびモニタリング警告をオフにするには、次のようにします。

1. **[アンチウイルス モニタリング]**|**[メイン]** を選択します。
2. **[モニタリング]** エリアで、**[オフ]** を選択します。
3. **[アンチウイルス セキュリティの問題を通知]** チェックボックスをオフにします。

ZoneAlarm Anti-virus および ZoneAlarm Security Suite でのモニタリング

これらの製品には Zone Labs Anti-virus が含まれているため、[アンチウイルス モニタリング] パネルはありません。代わりに、モニタリング警告が表示されます。Zone Labs Anti-virus がオフになっている場合は、アンチウイルス モニタリング機能が有効になります。モニタリングは、モニタリング警告からオフにできるほか、[詳細オプション] ダイアログからもオフにすることができます。

モニタリングをオフにするには、次のようにします。

1. **[警告とログ]** を選択し、**[詳細設定]** をクリックします。
2. **[警告イベント]** タブを選択します。
3. 次のチェックボックスをオフにします。

	アンチウイルス保護が検出されません
	アンチウイルス モニタリング イベント

4. **[OK]** をクリックします。

アンチウイルス モニタリングの有効化と無効化

Zone Labs Anti-virus をインストールしておらず、他のアンチウイルス ソフトウェア製品を使用している場合は、アンチウイルス モニタリングがデフォルトで有効になります。さらに、モニタリング警告を有効にして、システムの保護上の問題が検出された場合に警告を表示させることもできます。

アンチウイルス モニタリングを有効または無効にするには、次のようにします。

1. **［アンチウイルス モニタリング］**|**［メイン］**を選択します。
2. ［アンチウイルス モニタリング］エリアで**［オン］**を選択します。

［アンチウイルス モニタリング］パネルでの状況メッセージの表示

［アンチウイルス モニタリング］パネルの［状況］エリアには、アンチウイルス モニタリングの状況のほか、インストールされているアンチウイルス製品の現在の状況が表示されます。

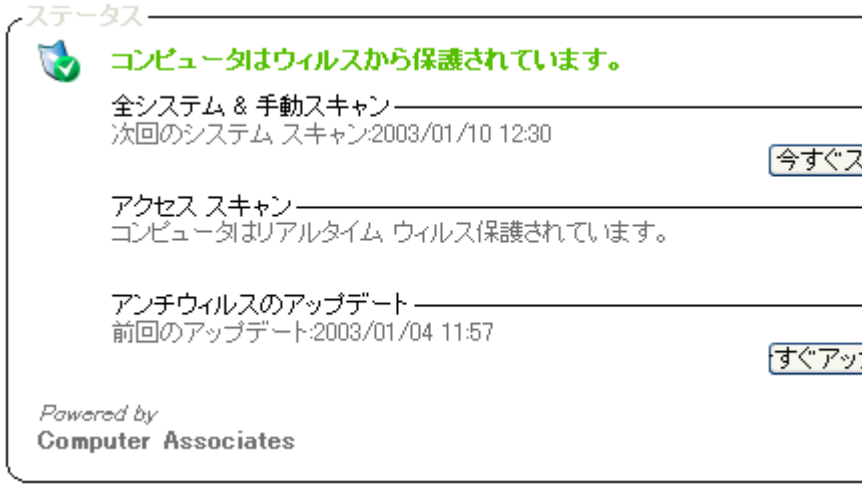


図 6-8: ZoneAlarm の［アンチウイルス モニタリング］パネルの［状況］エリア

アンチウイルス製品のモニタリング
Zone Labs セキュリティ ソフトウェアでは、主要なアンチウイルス ソフトウェア製品のほとんどを検出することができます。このエリアにあるドロップダウン リストには、検出されたアンチウイルス ソフトウェア製品が表示されます。

保護
アンチウイルス製品が有効でシステムが保護されているかどうかを表示します。

アンチウイルス アップデート
アンチウイルス製品が最新の状態であるかどうか、または、有効期限が切れていないかどうかが表示されます。

Zone Labs Anti-virus を試用する場合は、[状況] エリアの [試用 ...] ボタンをクリックします。

アンチウイルス モニタリング警告

お使いのアンチウイルス ソフトウェアのベンダが最新のウイルス定義ファイルを提供していない場合や、アンチウイルス製品の通知機能が無効になっている場合、あるいは、本製品で検出されないアンチウイルス製品 (122 ページの「モニタリング可能なソフトウェア」を参照) を実行している場合、アンチウイルス モニタリングは二次的な保護機能としてユーザに警告を表示します。

システム保護上の問題が見つかった場合は、モニタリング警告が表示されます。お使いのアンチウイルス製品の警告が先に表示されるよう、この警告はやや遅れて表示されます。警告では、お使いのアンチウイルス製品でセキュリティを確保するための情報と手順が表示されます。

Windows 98 が稼動していると、アンチウイルス メール スキャン機能は MailSafe の名前を、そのコンピュータの電子メール プログラムの名前ではなく、*isafe.exe* に変更します。

第 7 章

メール保護

7

ワーム、ウイルスなどは、メールを介してコンピュータからコンピュータへと感染します。MailSafe はメールで広がるこれらの脅威からユーザのコンピュータを保護するとともに、アドレス帳に記載されている友人、同僚などのコンピュータへの感染も阻止します。

トピック：

- 128 ページの「メール保護の概念」
- 129 ページの「インバウンド MailSafe 保護の有効化」
- 129 ページの「アウトバウンド MailSafe 保護の有効化」
- 130 ページの「インバウンド MailSafe 保護のカスタマイズ」
- 133 ページの「アウトバウンド MailSafe 保護のカスタマイズ」
- 135 ページの「迷惑メールのフィルタリング」
- 146 ページの「メールのアンチウイルス保護」

メール保護の概念

メールにファイルを添付することで、情報交換を便利に行うことができます。一方で、添付ファイルはウイルス、ワーム、トロイの木馬プログラム、その他の破壊工作ソフトを広める簡単な方法でもあります。

インバウンドおよびアウトバウンド MailSafe 機能は、ご使用のコンピュータにこうしたプログラムが感染しないよう、疑わしい添付ファイルを隔離し、ワームが大量のメールで自動的に送信されるのを阻止します。

インバウンド MailSafe 保護

危険性のある添付ファイルはファイル名の拡張子によって識別できます。拡張子とは、ファイル名の「ドット」より後にある文字の部分です。ファイルの種類が拡張子によって識別されるので、対応するプログラムやシステム コンポーネントによってそのファイルを開くことができます。

例：

- .exe（実行可能ファイル）
- .js（JavaScript ファイル）
- .bat（バッチ処理ファイル）

受信トレイで添付ファイル付きのメールを受信すると、MailSafe は添付ファイルのファイル名拡張子を確認し、添付ファイル一覧の拡張子と比較します。添付ファイルの種類が一覧に含まれていて、その種類の添付ファイルを隔離するように設定されている場合は、Zone Labs セキュリティ ソフトウェア がそのファイル名拡張子を「.zl*」(* は数字または文字）に変更します。

ファイルの拡張子を変更することで、その添付ファイルは自動的に実行されずに、隔離されます。その添付ファイルを含むメールを開くと、Zone Labs セキュリティ ソフトウェア が MailSafe 警告を表示して、添付ファイルが隔離されていることを通知します。その添付ファイルを開こうとすると、危険性を知らせる警告が表示されます。添付ファイルが安全であることが確認されている場合は、そのファイルを開くことができます。

ファイル名拡張子によるメッセージの確認に加えて、Zone Labs セキュリティ ソフトウェア では受信した添付ファイルをスキャンして、ウイルスが潜んでいないかどうかをチェックします。ウイルスが検出されると、破壊活動を行えないように、メッセージから削除されます。アンチウイルス保護とメール メッセージに関する詳細については、106 ページの「メール スキャン」を参照してください。

インバウンド MailSafe 保護は、POP3 または IMAP プロトコルを使用するメール アプリケーションで動作します。

インバウンド MailSafe 保護はローカル アクセス専用です。POP3 クライアントをリモート アクセス用に設定した場合は、インバウンド MailSafe 保護が使用できない場合もあります。

アウトバウンド MailSafe 保護

アウトバウンド MailSafe 保護により、メール プログラムが一定数を超えたメッセージの送信や一定数を超えた受信者への同一メールの送信を試みた場合に警告が表示されます。これにより、ユーザの知らないうちにコンピュータが悪用され、ウイルスなどに感染した添付ファイルが勝手に他の人へ送信される事態を防止できます。さらに、アウトバウンド MailSafe 保護は、メール送信を試みているプログラムにメッセージ送信許可が与えられているかどうかを確認します。

アウトバウンド MailSafe 保護は、SMTP を使用するすべてのメール アプリケーションで動作します。

アウトバウンド MailSafe 保護機能は、ZoneAlarm with Anti-virus、ZoneAlarm Pro、および ZoneAlarm Security Suite でのみ利用できます。

インバウンド MailSafe 保護の有効化

インバウンド MailSafe 保護は、デフォルトで有効に設定されています。インバウンド MailSafe が有効にされている場合、[添付ファイル] タブに一覧表示される添付ファイルの種類が隔離されます。

インバウンド MailSafe を有効または無効にするには、次のようにします。

1. **[メール保護]**|**[メイン]** を選択します。
2. **[オン]** または **[オフ]** を選択します。

オン	MailSafe は [添付ファイル] タブで指定されている種類の添付ファイルを隔離します。
オフ	MailSafe はすべての種類の添付ファイルを許可します。

アウトバウンド MailSafe 保護の有効化

セキュリティを維持するため、アウトバウンド メール保護はデフォルトで有効に設定されています。アウトバウンドのメール保護が有効にされている場合、メール送信権限を持つプログラムすべてに対してアウトバウンド MailSafe 設定が適用されます。

アウトバウンド メール保護を有効または無効にするには、次のようにします。

1. **[メール保護]**|**[メイン]** を選択します。
2. [アウトバウンド メール保護] エリアで、**[オン]** または **[オフ]** を選択します。

インバウンド MailSafe 保護のカスタマイズ

インバウンド MailSafe 保護でサポートされる添付ファイルの種類は、すべて隔離されるようにデフォルトで設定されています。添付ファイルの種類の設定を［許可］に変更するか、または新しい添付ファイルの種類を追加して、インバウンド MailSafe 保護をカスタマイズすることができます。

ZoneAlarm では、インバウンド MailSafe 保護の設定をカスタマイズすることはできません。

添付ファイル一覧の表示

添付ファイルの種類は、アルファベット順に表示されます。カラム ヘッダをクリックし、一覧をソートすることができます。ヘッダ名の隣の矢印（^）は、ソートの順序を示しています。同じヘッダを再度クリックすると、ソートの順序が逆になります。

添付ファイル一覧にアクセスするには、次のようにします。

［メール保護］|［添付ファイル］を選択します。

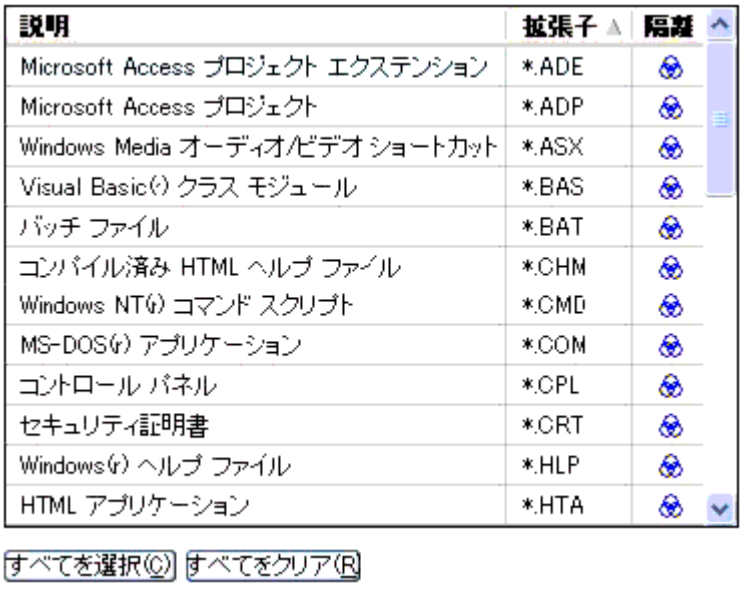


図 7-1: 添付ファイル一覧

添付ファイルの種類の隔離設定の変更

Zone Labs セキュリティ ソフトウェア では、ワームなどの有害なコードの感染源となる可能性のある、45 種類以上の添付ファイル形式が事前に定義

されています。デフォルトで、Zone Labs セキュリティ ソフトウェア はその全種類の添付ファイルを隔離します。これらの添付ファイルの種類は、添付ファイル一覧に表示されます。

特定の添付ファイルの種類について隔離設定を変更するには、次のようにします。
1. ［メール保護］|［添付ファイル］を選択します。
2. ［隔離］カラムで、拡張子の種類をクリックします。
3. ［隔離］または［許可］を選択して、［適用］をクリックします。

添付ファイルの種類の追加と削除

添付ファイル一覧に表示されない添付ファイルの種類を隔離する場合は、添付ファイルの種類をいくつでも一覧に追加することができます。

ユーザの保護のため、Zone Labs セキュリティ ソフトウェア ではデフォルトの添付ファイルの種類を削除することはできません。ただし、ユーザが追加した添付ファイルの種類は自由に削除できます。

添付ファイルの種類を一覧に追加するには、次のようにします。
1. ［メール保護］|［添付ファイル］を選択します。
2. ［追加］をクリックします。
3. 説明とファイル名の拡張子（ドットを含めても含めなくてもよい）を入力し、[OK] をクリックします。
4. ［適用］をクリックし、変更を保存します。

添付ファイルの種類を一覧から削除するには、次のようにします。
1. ［メール保護］|［添付ファイル］を選択します。
2. ［拡張子］カラムで、添付ファイルの種類を右クリックします。
3. ［削除］を選択します。

隔離された添付ファイルの表示

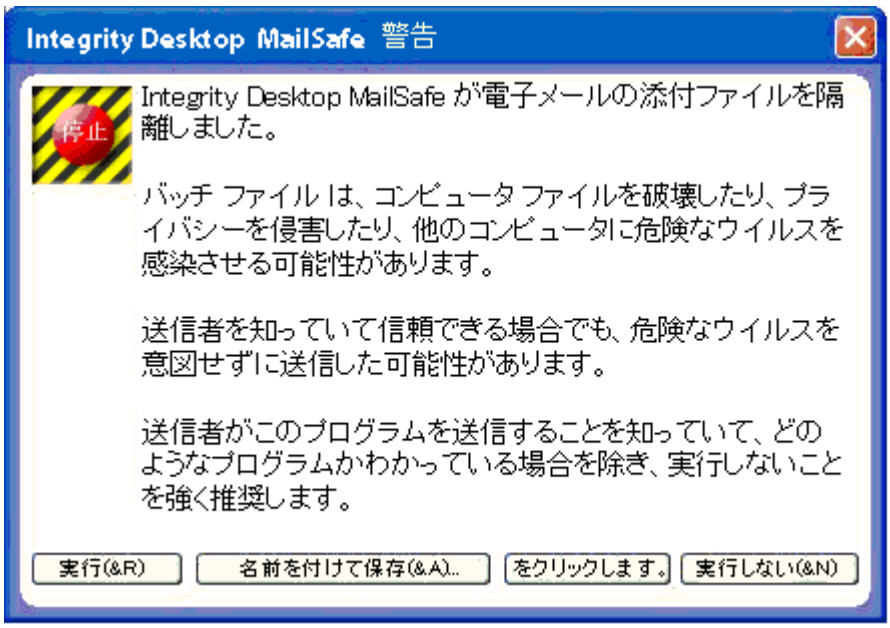
添付ファイル自体のコードを表示する場合は、メモ帳で添付ファイルを開くことができます。

最高のセキュリティを得るため、送信者が信頼できる相手であり、かつ、その送信者が意図的にメッセージを送ったこと、およびその添付ファイルの安全性が確認されている場合以外は、Zone Labs セキュリティ ソフトウェア が隔離した添付ファイルは開かないでください。

隔離された添付ファイルを開くには、次のようにします。
1. Windows エクスプローラで、目的のファイルを見つけます。
2. 添付ファイルをダブルクリックして表示します。

3. 隔離された添付ファイルを開こうとすると、Zone Labs セキュリティ ソフトウェア がその表示に伴う危険性についてユーザに警告します。

.



4. ［メモ帳で調査］をクリックします。

アウトバウンド MailSafe 保護のカスタマイズ

デフォルトでは、メール アプリケーションが 2 秒以内に 5 通を超えるメッセージの送信を試みた場合、あるいは、同一メッセージの受信者が 50 名を超えている場合に、アウトバウンド MailSafe 保護警告が表示されます。この設定をカスタマイズして、許容する秒間隔、メッセージ数、受信者数を増やしたり、ご使用のコンピュータから送信できるメール アドレスを指定したりできます。

プログラム別のアウトバウンド MailSafe 保護の有効化

アウトバウンド MailSafe 保護がオンに設定されていると、メール送信の許可が与えられた全プログラムに対して保護が適用されます。

この設定をカスタマイズして、特定のプログラムに対してアウトバウンド MailSafe 保護を有効または無効にすることができます。

特定のプログラムに対する許可の設定の詳細については、85 ページの「特定プログラムの許可の設定」を参照してください。

プログラムに対してアウトバウンド MailSafe 保護を有効または無効にするには、次のようにします。

1. **[プログラム コントロール]**|**[プログラム]** を選択します。
2. ［プログラム］カラムで、プログラム名を右クリックして **[オプション]** を選択します。
3. **[セキュリティ]** タブを選択します。
4. ［アウトバウンド メール保護］エリアで、**[このプログラムのアウトバウンド メール保護を有効にする]** チェックボックスをオンにします。

   アウトバウンド MailSafe 保護を無効にするには、このチェックボックスをオフにします。
5. **[OK]** をクリックします。

アウトバウンド MailSafe 保護オプションの設定

デフォルトでは、コンピュータが 2 秒以内に 5 通を超えるメッセージの送信を試みた場合、あるいは、同一メッセージの受信者が 50 名を超えている場合に、アウトバウンド MailSafe 保護が適用されます。

正当なメール メッセージでも上記の条件に該当する場合もあるため、個々のニーズに対応できるようにアウトバウンド MailSafe 保護設定をカスタマイズできます。

アウトバウンド MailSafe 保護設定をカスタマイズするには、次のようにします。

1. **［メールの保護］**|**［メイン］** を選択して、**［詳細設定］** をクリックします。

   ［高度な電子メール保護］ダイアログが表示されます。

2. **［アウトバウンド メール保護の警告を表示するとき］** エリアで、設定を選択します。

一度に多くのメールが送信される場合	指定された時間間隔内に所定の数を超えるメールの送信が試行された場合に、アウトバウンド MailSafe 保護警告が表示されます。
同一メッセージに多くの受信者がいる場合	指定された数を超える受信者に対して同一メールの送信が試行された場合に、アウトバウンド MailSafe 保護警告が表示されます。
送信者のアドレスが一覧にない場合	一覧に表示されていない送信元アドレス（［差出人］フィールドのアドレス）を使ってメールの送信が試行された場合に、アウトバウンド MailSafe 保護警告が表示されます。Zone Labs セキュリティ ソフトウェア が外部へのメールをすべてブロックしないように、ご使用の有効なメール アドレスが必ずこの一覧に含まれていることを確認してください。

3. **［OK］** をクリックします。

迷惑メールのフィルタリング

迷惑メール フィルタは ZoneAlarm Security Suite で使用できます。

迷惑メール フィルタを使用して、不要な迷惑メール（一般に *スパム* と呼ばれる）のために受信トレイが乱雑になるのを防ぎます。迷惑メール フィルタは Microsoft Outlook と Outlook Express をサポートします（この文書では両者とも単に「Outlook」と呼びます）。

インストール中に、Zone Labs セキュリティ ソフトウェア は Outlook 電子メール プログラムのツール バーに［迷惑メール フィルタ］ツール バーを追加します。

図 7-2:［迷惑メール フィルタ］ツール バー

Zone Labs セキュリティ ソフトウェア をインストールし、Outlook ツール バーに迷惑フィルタ ツール バーが表示されない場合、Outlook ツール バーを右クリックし、[ZoneAlarmOutlookAddin] を選択します。

迷惑メール フィルタは Outlook フォルダ リストにも［ZoneAlarm チャレンジ済みメール］、［ZoneAlarm 迷惑メール］、［ZoneAlarm 詐欺メール］という 3 つの特別なフォルダを追加します。Zone Labs security software が電子メール メッセージを迷惑、詐欺、チャレンジ済みと判断すると、メッセージをこれらのフォルダのいずれかに格納します。Outlook を使用して Hotmail にアクセスする場合、Hotmail の機能の代わりに迷惑メール フィルタのスパム ブロック機能と特別なフォルダを使用する必要があります。

特定の送信者からのメールの許可またはブロック

新しい人にメールを送信するたびに、迷惑メール フィルタは［許可］リストに、［宛先］フィールドのアドレスを自動的に追加します。これらのアドレスから送信されたメッセージは受信トレイに格納されます。

［ブロック］リストに含まれる送信者からメールを受信した場合、迷惑メール フィルタは *[ZoneAlarm 迷惑メール]* という Outlook フォルダにメッセージを自動的に移動します。

Outlook 受信トレイに不要な電子メールが届いた場合は、そのメッセージの送信者を［ブロックされている人］リストに簡単に追加できます。

電子メール アドレスを［許可］または［ブロック］リストに追加するには、次のようにします。

1. Outlook または Outlook Express 電子メール プログラムで、電子メールを送信します。
2. ［迷惑メール フィルタ］ツール バーで、**[ZoneAlarm オプション]** をクリックし、**［送信者を許可］**または **［送信者をブロック］**を選択します。

特定の会社からのメールの許可またはブロック

迷惑メール フィルタを使用して、特定の会社またはネットワーク ドメインから発信されたすべてのメール アドレスを［許可される会社］リストまたは［ブロックされる会社］リストに追加できます。

会社を［許可］または［ブロック］リストに追加するには、次のようにします。

1. Outlook または Outlook Express 電子メール プログラムで、電子メールを送信します。
2. ［迷惑メール フィルタ］ツール バーで、**[ZoneAlarm オプション]** をクリックし、**［送信者の会社を許可］**または **［送信者の会社をブロック］**を選択します。

   迷惑メール フィルタは送信者のアドレスのドメイン部分（たとえば、*example.com* など）を許可またはブロックされるアドレスのリストに追加します。

許可リストへの連絡先の追加

電子メール プログラム中のデフォルトの連絡先フォルダをスキャンして、電子メールの受信を希望する送信者のリストに連絡先を追加できます。

許可リストに連絡先を追加するには、次のようにします。

1. Outlook または Outlook Express 電子メール プログラムを開きます。
2. ［迷惑メール フィルタ］ツール バーで、**[ZoneAlarm オプション]** をクリックし、**［許可リストに格納］**を選択します。

受信トレイのスキャン

受信トレイの内容をスキャンして、詐欺メールおよびスパムの有無を確認できます。

受信トレイをスキャンするには、次のようにします。

1. Outlook または Outlook Express 電子メール プログラムを開きます。
2. スキャンする受信トレイを選択します。

3. ［迷惑メール フィルタ］ツール バーで、**[ZoneAlarm オプション]** をクリックし、**［受信トレイのスキャン］** を選択します。

受信トレイのオプションを使用して、Outlook Express で作成される IMAP、POP3、Hotmail アカウント、および Outlook で作成される POP3 アカウントをスキャンすることができます。ただし、Outlook で作成される IMAP アカウントはスキャンできません。

配布リストからのメールの許可

配布リストに含まれる複数のアドレスに対してメールの送受信を行う場合、リスト名が［リスト］タブに追加されていなければ、迷惑メール フィルタはそのリスト名をブロックすることがあります。

メール リストからのメールを許可するには、次のようにします。

1. Outlook または Outlook Express 電子メール プログラムを起動します。
2. ［迷惑メール フィルタ］ツール バーで、**[ZoneAlarm オプション]|[設定の指定]|[リスト] をクリックします。**
3. **［追加］** をクリックします。
4. テキスト入力エリアに配布リストのメール アドレスを入力し、**[OK]** をクリックします。

   迷惑メール フィルタは配布リストのメール アドレスを許可されたアドレスの一覧に追加します。
5. **［閉じる］** をクリックすると、変更が保存され、［リスト］タブが閉じます。

迷惑メールの報告

迷惑メール フィルタを使用して、迷惑メールのインスタンスを Zone Labs 協調フィルタ データベースに提供できます。

迷惑メール フィルタは、ユーザの許可がないかぎり、コンピュータ上のどの種類の電子メールも送信しません。迷惑メールを協調フィルタ データベースに提供する場合、実際のメールまたはデジタル処理された（「ハッシュ」ということがあります）電子メールの概要を選択して送信できます。後者の場合、メッセージからすべてのコンテンツ、ヘッダ、および個人識別情報が削除されます。メッセージ全体を送信するとコンテンツの完全な

分析が可能になります。デジタル処理されたメッセージの概要を送信するとプライバシーが完全に守られます。

MailFrontier は信頼できる Zone Labs パートナーで、Zone Labs 協調フィルタ データベースを管理します。MailFrontier のプライバシー ポリシーについて、http://www.mailfrontier.com/privacy.html で完全な文章を確認できます。

迷惑メールを報告するには、次のようにします。

1. Outlook または Outlook Express 電子メール プログラムで、電子メールを送信します。
2. ［迷惑メール フィルタ］ツール バーで次の操作を行います。
   - 迷惑メールそのものを送信するには、**[ZoneAlarm オプション]** をクリックし、**［迷惑メールの報告］** を選択します。
   - デジタル処理された迷惑メールの概要を送信するには、**［迷惑］** をクリックします。
3. **［メールの提供］** ダイアログ ボックスで、**[OK]** をクリックします。

   迷惑メール フィルタは迷惑メールを協調フィルタ データベースに報告し、メッセージを **[ZoneAlarm 迷惑メール]** という特別な Outlook フォルダに移動します。

誤って迷惑と判別された電子メールを復元するには、[ZoneAlarm 迷惑メール] フォルダで電子メールを選択し、［迷惑ではない］をクリックします。電子メールは Outlook 受信トレイに復元されます。

詐欺メールの報告

迷惑メール フィルタを使用して、詐欺メール（*フィッシング* と呼ばれることがあります）のインスタンスを Zone Labs に提供できます。

迷惑メール フィルタは、ユーザの許可がないかぎり、コンピュータ上のどの種類の電子メールも送信しません。詐欺メールを報告する場合、迷惑メール フィルタは完全な元のメッセージを Zone Labs に転送します。

Zone Labs は、詐欺メッセージの発信者を調査し、告訴するために必要な場合を除き、詐欺メールに含まれるユーザのメール アドレス、名前、その他の個人情報を外部に開示することは一切ありません。

Zone Labs は、電子メール詐欺として、報告されたメッセージの選択部分を管轄の政府および法執行機関に転送します。これらの機関は法に基づいて、メッセージに含まれる情報の機密を保護する必要があります。Zone Labs は

脅威を受けた個人または組織に対して、警告に必要な情報のみを転送することにより、別々に通知します。

詐欺メールを報告するには、次のようにします。

1. Outlook または Outlook Express 電子メール プログラムで、電子メールを送信します。
2. [迷惑メール フィルタ] ツール バーで、**[ZoneAlarm オプション]** をクリックし、**[詐欺メールの報告]** を選択します。
3. **[メールの提供]** ダイアログ ボックスで、**[OK]** をクリックします。

   迷惑メール フィルタは詐欺メールを Zone Labs に報告し、メッセージを *[ZoneAlarm 詐欺メール]* という特別な Outlook フォルダに移動します。Outlook を使用して Hotmail にアクセスする場合、Hotmail の機能の代わりに迷惑メール フィルタのスパム ブロック機能と特別なフォルダを使用する必要があります。

MailFrontier は信頼できる Zone Labs パートナーで、Zone Labs のために詐欺メールの処理を管理します。MailFrontier のプライバシー ポリシーについて、http://www.mailfrontier.com/privacy.html で完全な文章を確認できます。

迷惑メール メッセージ オプションの指定

迷惑メール フィルタは *協調フィルタ*、*メッセージ フィルタ*、および *外国語フィルタ* という 3 つのメッセージ フィルタリング テクニックを使用します。フィルタ設定は不明な送信者から受信したメッセージの処理方法を特定します。

協調フィルタ

協調フィルタリングでは、自分と自分以外の Zone Labs セキュリティ ソフトウェア ユーザから報告された迷惑メールから抽出した情報を使って、不

明なユーザから受信した新しいメッセージが スパム かどうかが判断されます。

メッセージ フィルタ
メッセージ フィルタは発見的ルールを使って、さまざまな種類の迷惑メールに共通した特徴について、メールを分析します。

外国語フィルタ
外国語フィルタは、ヨーロッパ言語以外の言語を含むメールをブロックします。(迷惑メール フィルタはフランス語、ドイツ語、スペイン語といった一般的なヨーロッパ言語の電子メールを自動的に管理します)

メッセージ フィルタリング オプションをカスタマイズするには、次のようにします。

1. Outlook または Outlook Express 電子メール プログラムを起動します。
2. [迷惑メール フィルタ] ツール バーで、**[ZoneAlarm オプション]**|**[設定の指定]**|**[メッセージ]** をクリックします。

協調フィルタ	このエリアでスライダを移動し、他の Zone Labs セキュリティ ソフトウェア ユーザによって報告された迷惑メールの特性に対する反応を調整します。
メッセージ フィルタ	スライダを移動して、一般的な迷惑メールへの反応を調整します。特定のカテゴリの迷惑メールに対する反応を調整することもできます。
言語フィルタ	このエリアで [設定] をクリックし、ブロックする言語を選択します。

3. **[閉じる]** をクリックします。

不明な送信者からのチャレンジ メール

迷惑メール フィルタを使用して、不明な送信者からのメールにチャレンジ メールで応答できます。迷惑メールは有効な返信アドレスを含むことがほとんどないため、チャレンジに応答がないことで電子メールがおそらく迷惑であることを確認できます。

チャレンジ メールによって、受信者はメッセージ中のボタンをクリックし、その人がメッセージの所有者であることを確認すよう指示されます。ボタンをクリックすると、迷惑メール フィルタは **[ZoneAlarm チャレンジ**

済みメール メール］という特別な Outlook フォルダにある電子メールを Outlook 受信トレイに移動します。

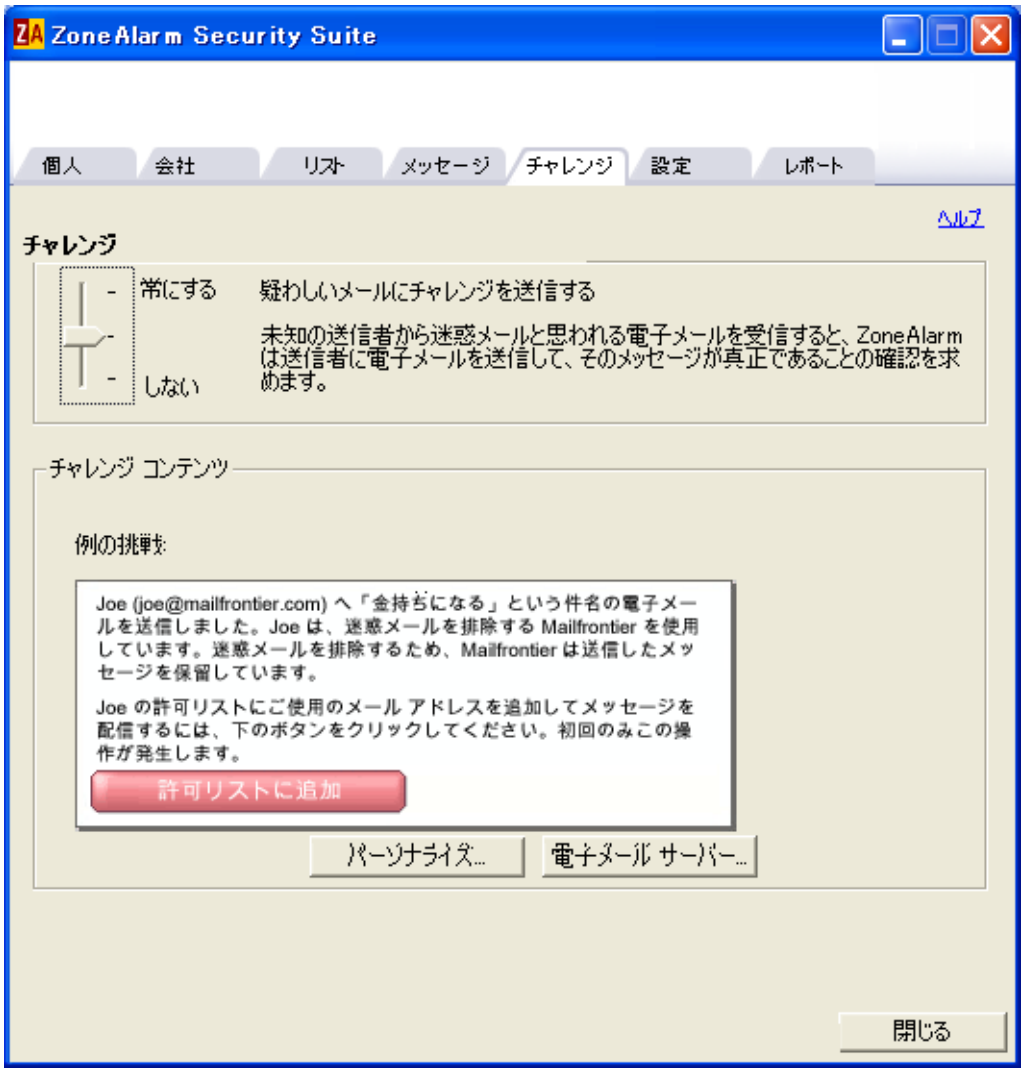


図 7-3:［チャレンジ］オプション タブ

不明な送信者からのメッセージについて、常にチャレンジ メールを送信するか、受信メッセージが迷惑メールと思われる場合にのみチャレンジを送信するか、チャレンジを送信しないかを選択できます。さらに、ユーザに送信されるチャレンジ メールをカスタマイズできます。

チャレンジ メールを有効にするには、次のようにします。

1. Outlook または Outlook Express 電子メール プログラムを起動します。
2. ［迷惑メール フィルタ］ツール バーで、**[ZoneAlarm オプション]**|**[設定の指定]**|**[チャレンジ]** をクリックします。

3. ［チャレンジ］エリアで、スライダを使用し、チャレンジを送信するタイミングを選択します。

高	Zone Labs security software はユーザにとっての妥当性（許可リストに含まれている）または MailFrontier にとっての妥当性（既知の適切な送信者）が判別されていない場合、受信したすべての電子メールをチャレンジします。 受信されてすぐに迷惑と分類可能なすべての電子メール メッセージは後で削除するために ZoneAlarm メール フォルダに直接送られ、チャレンジは発行されません。
低	Zone Labs security software は不明なメールをチャレンジします。 Zone Labs security software はスパムか良性かを明確に判断できない電子メールのみをチャレンジします。これは通常、受信メールのわずかなパーセンテージを占めます。
オフ	チャレンジ メールは送信されません。 Zone Labs security software はチャレンジ メールを送信しません。スライダを上に移動すると、メール チャレンジがオンになり、スパム コンピュータによって送信される迷惑メールが排除されます。

4. 個人メッセージを標準のチャレンジ メールに追加するには、[パーソナライズ］をクリックし、名前と個人メッセージを入力して、[OK] をクリックします。

5. ［閉じる］をクリックします。

迷惑メール フィルタはメッセージを [ZoneAlarm チャレンジ済みメール］フォルダに移動します。

チャレンジ メッセージの応答を待つ一方で、迷惑メール フィルタはユーザの電子メール アドレスを格納します。チャレンジの処理が完了するとすぐに、迷惑メール フィルタはアドレスを破棄します。チャレンジ メールの送信に問題がある場合は、142 ページの「外部へのメール サーバの指定」を参照してください。

外部へのメール サーバの指定

チャレンジ メールを送信するために、迷惑 メール フィルタは電子メールを送信可能でなければなりません。ほとんどの場合、迷惑メール フィルタは Outlook のデフォルトのアウトバウンド メール サーバを使用します。チャレンジ メールの送信で問題がある場合は、アウトバウンド メール サーバの名前を指定しなければならないことがあります。

アウトバウンド メール サーバの名前を指定するには、次のようにします。

1. Outlook または Outlook Express 電子メール プログラムを起動します。

2. ［迷惑メール フィルタ］ツール バーで、[ZoneAlarm オプション]|[設定の指定]|[チャレンジ］をクリックします。
3. ［チャレンジ コンテンツ］エリアで、[メール サーバ］をクリックします。
4. アウトバウンド メール サーバの名前を入力し、[OK] をクリックします。
5. ［閉じる］をクリックします。

迷惑メール フィルタ設定のカスタマイズ

デフォルトで、迷惑メール フィルタは、詐欺メールを手動で削除するまで、[ZoneAlarm 詐欺メール］フォルダに保持します。[ZoneAlarm 迷惑メール］フォルダおよび［ZoneAlarm チャレンジ済みメール］フォルダにおけるメールの保持期間を指定できるほか、偽者メールの報告を自動化したり、ワイヤレス デバイス転送を設定したりできます。

迷惑メールの保存期間を指定するには、次のようにします。

1. Outlook または Outlook Express 電子メール プログラムを起動します。
2. ［迷惑メール フィルタ］ツール バーで、[ZoneAlarm オプション]|[設定の指定]|[設定］をクリックします。
3. ［迷惑フォルダ設定］エリアで、[設定］をクリックします。
4. 疑わしい迷惑メールを［ZoneAlarm 迷惑メール］フォルダおよび［Zone Alarm チャレンジ済みメール］フォルダに保持する日数を入力します。

   迷惑メール フォルダは、指定された日数の間、検証されずにフォルダに存在したメールを Outlook の［削除済みアイテム］に移動します。
5. ［閉じる］をクリックします。

詐欺メールの自動報告を有効にするには、次のようにします。

1. Outlook または Outlook Express 電子メール プログラムを起動します。
2. ［迷惑メール フィルタ］ツール バーで、[ZoneAlarm オプション]|[設定の指定]|[設定］をクリックします。
3. ［詐欺メールの自動報告］エリアで、[自動報告を有効にする］を選択します。
4. ［閉じる］をクリックします。

ワイヤレス デバイスを設定するには、次のようにします。

1. Outlook または Outlook Express 電子メール プログラムを起動します。

2. ［迷惑メール フィルタ］ツール バーで、**[ZoneAlarm オプション]**|**[設定の指定]**|**[設定]** をクリックします。
3. **［ワイヤレス デバイス サポート］** エリアで、**［設定］** をクリックします。
4. **[Zone Alarm ワイヤレス サポート]** ダイアログ ボックスで、ワイヤレス デバイスのメール アドレスを入力します。

   メール ヘッダのみを転送したり、24 時間以内にワイヤレス デバイスに転送される検証メッセージの数を指定したりすることも可能です。
5. デフォルトでないメール サーバを指定する必要がある場合は、**［メール サーバ］** をクリックし、アウトバウンド メール サーバの名前を入力し、**[OK]** をクリックします。
6. **［閉じる］** をクリックすると、変更が保存され、［設定］タブが閉じます。

確認メッセージをカスタマイズするには、次のようにします。

1. Outlook または Outlook Express 電子メール プログラムを起動します。
2. ［迷惑メール フィルタ］ツール バーで、**[ZoneAlarm オプション]**|**[設定の指定]**|**[設定]** をクリックします。
3. **［表示設定］** エリアで、必要な設定を指定します。

迷惑メールの提供	迷惑メールを Zone Labs に送信する前に警告を表示します。
詐欺メールの提供	詐欺メールを Zone Labs に送信する前に警告を表示します。

4. **[OK]** をクリックします。

間違って迷惑メールと識別されたメールのリストア

迷惑メール フィルタは Outlook フォルダ リストに **[ZoneAlarm チャレンジ済みメール]**、**[ZoneAlarm 迷惑メール]**、**[ZoneAlarm 詐欺メール]** という 3 つの特別なフォルダを追加します。Zone Alarm が電子メール メッセージを迷惑、詐欺、チャレンジ済みと判断すると、メッセージをこれらの特別なフォルダのいずれかに格納します。

Outlook を使用して Hotmail にアクセスする場合、Hotmail の機能の代わりに迷惑メール フィルタのスパム ブロック機能と特別なフォルダを使用する必要があります。

迷惑メール フィルタが間違って特別なフォルダに格納したメールを Outlook 受信トレイに復元できます。

間違って迷惑メールと識別されたメールを復元するには、次のようにします。

1. Outlook or Outlook Express 電子メール プログラムの **[ZoneAlarm チャレンジ済みメール]**、**[Zone Alarm 迷惑メール]**、または **[Zone Alarm 詐欺メール]** フォルダで、メールを選択します。
2. **[迷惑メール フィルタ]** ツール バーで、**[迷惑ではない]** をクリックします。

   迷惑メール フィルタは選択されたメッセージを Outlook 受信トレイに復元します。

迷惑メール フィルタ レポートの表示

迷惑メール フィルタの [レポート] タブを使用して、メール処理活動の概要を表示します。

迷惑メール フィルタ レポートを表示するには、次のようにします。

1. Outlook または Outlook Express 電子メール プログラムを起動します。
2. **[迷惑メール フィルタ]** ツール バーで、**[ZoneAlarm オプション]**|**[設定の指定]**|**[レポート]** をクリックします。
3. 次の 4 つのレポート タイプのいずれかを選択します。

日別の迷惑メール	日別に受信された正当なメールと迷惑メールの総数。
理由	日別に迷惑メール フィルタが受信メールをブロックした理由。
日別の全体履歴迷惑メール	Zone Labs セキュリティ ソフトウェアのインストール以降、日別に受信された正当なメールと迷惑メールの総数。
全体理由	Zone Labs セキュリティ ソフトウェアのインストール以降、迷惑メール フィルタが受信メールをブロックした理由の総数。

4. **[閉じる]** をクリックして [レポート] タブを閉じます。

メールのアンチウイルス保護

ZoneAlarm Anti-virus と ZoneAlarm Security Suite では、受信メールに対する MailSafe による保護に加えて、受信メールのメッセージにウイルスが含まれていないかどうかをスキャンする保護機能も提供します。MailSafe とは異なり、メール スキャンでは、添付ファイル内のみでなくメール メッセージの本文に含まれているウイルスも検出することができます。

- メール スキャンの有効化
- 感染したメールの処理方法

メール スキャンの有効化

ZoneAlarm Anti-virus および ZoneAlarm Security Suite では、メールに対するアンチウイルス保護がデフォルトで有効になっています。

メール スキャンを有効または無効にするには、次のようにします。

1. **[アンチウイルス / アンチスパイウェア]**|**[メイン]** を選択します。
2. [保護] エリアで、**[詳細オプション]** を選択します。

   [詳細オプション] ダイアログが表示されます。
3. [ウイルス管理] で、**[メール スキャン]** を選択します。
4. **[メール スキャンを有効にする]** チェックボックスをオンまたはオフにして、**[OK]** をクリックします。

感染したメールの処理方法

Zone Labs セキュリティ ソフトウェア は、ウイルスに感染した添付ファイルを検出すると、感染したファイルを除去して、感染レポートをそのメールに添付します。感染レポートは、ウイルスに感染したファイルの名前などの、メールから除去された添付ファイルに関する情報が含まれたテキスト ファイルです。

図 7-4: 感染レポートの例

ウイルスに感染した添付ファイルが開かれないよう、ファイル拡張子は .z16 に変更されます。

Eudora をお使いの場合で、受信トレイに複数の感染レポートが含まれていると、感染レポート名の拡張子 .txt の前に数値が追加されます。

Windows 98 が稼動していると、メール スキャン機能は MailSafe の名前を、そのコンピュータの電子メール プログラムの名前ではなく、*isafe.exe* に変更します。

ウイルスからのコンピュータの保護に関する詳細については、99 ページから始まる第 6 章「スパイウェアおよびウイルス保護」を参照してください。

第 8 章

プライバシー保護

8

一昔前の Web ページには、無害なテキスト ベースのファイルしか含まれていませんでした。今日では、Web ページには、ユーザの個人情報を公開し、迷惑なポップアップを表示し、そして場合によってはコンピュータを破損してしまう、各種エレメントが含まれていることが少なくありません。さらに、Web の利用後もコンピュータ上に残されるファイルによって、コンピュータのパフォーマンスが低下することもあります。プライバシー保護を利用することで、Cookie、広告、およびダイナミック Web コンテンツの悪用を防ぎ、不要なインターネット ファイルを定期的にコンピュータから削除することができます。

ZoneAlarm Pro および ZoneAlarm Pro Security Suite では、プライバシー機能を使用できます。

トピック：

- 150 ページの「プライバシー保護の概念」
- 151 ページの「全般的プライバシー オプションの設定」
- 153 ページの「プライバシー アドバイザの使用」
- 154 ページの「特定の Web サイトのプライバシー オプションの設定」
- 157 ページの「Cookie コントロールのカスタマイズ」
- 160 ページの「広告ブロックのカスタマイズ」
- 162 ページの「モバイル コード コントロールのカスタマイズ」
- 164 ページの「キャッシュ クリーナの概念」

プライバシー保護の概念

プライバシー保護は、広告コンテンツの表示や、Web アクセス動向などのユーザに関するデータの収集のために一般的に使われている Web サイトのエレメントを管理する際に役立ちます。さらに、プライバシー設定により、特定の種類のダイナミック Web コンテンツやモバイル コードの悪用を防ぐことができます。

*Cookie コントロール*は、広告主がユーザのインターネット利用動向を密かに監視することを防止します。また、ご使用のコンピュータにハッカーが侵入した際に Cookie の情報が盗まれることもあるため、重要情報（パスワードなど）が Cookie に保管されないよう管理します。

*広告ブロック*は、迷惑な広告によりインターネット上の作業が中断されないようにします。Zone Labs セキュリティ ソフトウェアでは、すべての種類の広告（*バナー広告*、*アニメーション広告*など）をブロックすることも、指定した種類のみブロックすることもできます。

*モバイル コード コントロール*は、アクティブな Web ページ コンテンツ（Java アプレット、*ActiveX コントロール* コントロール、プラグインなど）を、ユーザのセキュリティの低下やコンピュータの破損を目的にして、ハッカーが悪用することを防止します。ただし、モバイル コードは正規の Web サイトでも多く使用されているため、モバイル コード コントロールを有効にすると、それらの Web サイトの機能に影響が生じる場合があります。

*キャッシュ クリーナ*は、Web サーフィンやコンピュータの使用中に蓄積される余分なファイルを削除し、コンピュータをすっきりとした状態に整理します。また、URL の履歴、ブラウザ キャッシュ、その他ユーザが指定するファイルも削除するため、プライバシーの維持にも役立ちます。

ZoneAlarm Pro および ZoneAlarm Security Suite では、プライバシー機能を使用できます。

全般的プライバシー オプションの設定

ブラウザのプライバシー保護を有効にするには、セットアップ時に指定する必要があります。セットアップ時にプライバシー保護を有効にしなかった場合は、手動で設定することもできます。

全般的なプライバシー オプションを含む一連のプライバシー機能は、ZoneAlarm Pro および ZoneAlarm Security Suite で提供されています。

プライバシー保護レベルの設定

プライバシー保護レベルを設定すると、Cookie、広告、モバイル コードの許可またはブロックを指定できます。

プライバシー レベルを設定するには、次のようにします。

1. **[プライバシー]**|**[メイン]** を選択します。
2. [Cookie コントロール] エリアで、スライダをクリックして希望の設定になるようにドラッグします。

高	セッション Cookie 以外のすべての Cookie をブロックします。この設定の場合、一部の Web サイトがロードできないことがあります。
中	永続 Cookie と サードパーティ Cookie による Web サイトのトラッキングをブロックします。個人的なサービス用の Cookie は許可されます。
オフ	すべての Cookie を許可します。

3. [広告ブロック] エリアで、スライダをクリックして希望の設定になるようにドラッグします。

高	すべての広告をブロックします。すべてのポップアップ / ポップアンダーおよび アニメーション広告 をブロックします。
中	すべてのポップアップ / ポップアンダーおよびアニメーション広告をブロックします。バナー広告は許可します。
オフ	すべての広告を許可します。

4. [モバイル コード コントロール] エリアで、**[オン]** または **[オフ]** を選択します。
5. **[OK]** をクリックします。

ブラウザ以外のプログラムへのプライバシー保護の適用

デフォルトでは、プライバシー保護は Internet Explorer などの標準のブラウザ プログラムのみに適用されます。また、コンピュータ上の他のプログラムにもプライバシー保護を適用することができます。

ブラウザ以外のプログラムにプライバシー保護を適用するには、次のようにします。

1. **[プログラム コントロール]**|**[プログラム]** を選択します。
2. ［プログラム ］カラムで、プログラム名をクリックし **[オプション]** を選択します。

   ［プログラム オプション ］ダイアログが表示されます。
3. **[セキュリティ]** タブを選択します。
4. ［フィルタ オプション ］エリアで、**[このプログラムのプライバシーを有効にする]** チェックボックスをオンにします。

プライバシー アドバイザの使用

プライバシー アドバイザは、Zone Labs セキュリティ ソフトウェアが Cookie やモバイル コードをブロックする際に表示される警告で、特定のページについてそれらのエレメントを許可することができます。

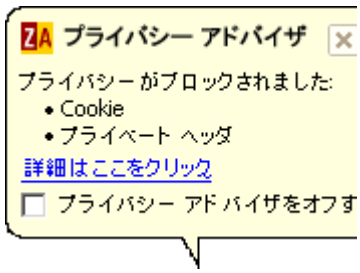


図 8-1: プライバシー アドバイザ

全般的なプライバシー アドバイザを含む一連のプライバシー機能は、ZoneAlarm Pro および ZoneAlarm Security Suite で提供されています。Web ページのエレメントがブロックされるたびにプライバシー アドバイザが表示されないようにするには、**[プライバシー アドバイザをオフする]** チェックボックスをオンにします。

サイト検証は、プライバシー アドバイザと同じ警告ウィンドウに表示されますが、これらの 2 つは個別に有効または無効に設定することができます。プライバシー アドバイザを無効にすると、サイト検証の警告は単体で表示されます。逆の場合も同様です。サイト検証の詳細については、28 ページの「ライセンス、登録、およびサポート」を参照してください。

プライバシー アドバイザを無効にするには、次のようにします。

1. **[プライバシー]**|**[メイン]** を選択します。
2. [Cookie コントロール] エリアで、**[カスタム]** をクリックします。

   [カスタム プライバシー設定] ダイアログ ボックスが表示されます。
3. [プライバシー アドバイザ] エリアで、**[プライバシー アドバイザを表示する]** チェックボックスをオフにします。
4. **[OK]** をクリックします。

プライバシー設定の詳細を表示したり、設定を変更するには、[詳細はここをクリック] と書かれたリンクをクリックします。Zone Labs セキュリティ ソフトウェア が [プライバシー] パネルを開きます。

特定の Web サイトのプライバシー オプションの設定

インターネットを利用する際にアクセスしたサイトがプライバシー サイト一覧に追加されます。この一覧を使ってサイトごとにカスタマイズされたプライバシー オプションを指定できます。また、サイトを一覧に追加して、プライバシー設定をカスタマイズすることもできます。ZoneAlarm Pro および ZoneAlarm Security Suite では、一連のプライバシー機能を使用できます。

プライバシー サイト一覧の表示

この一覧には、Zone Labs セキュリティ ソフトウェアの現在のセッション中にアクセスしたサイトと、過去に設定をカスタマイズしたサイトが表示されます。アクセスしたサイトの設定をカスタマイズしなかった場合、コンピュータのシャットダウン時または Zone Labs セキュリティ ソフトウェアの終了時に、そのサイトは一覧から削除されます。

サイト一覧にサブドメインが表示されていても、プライバシー保護はドメインレベルで適用されます。たとえば、news.google.com というサブドメインを手動で一覧に追加した場合、プライバシー保護は google.com のドメイン全体に適用されます。

プライバシー サイト一覧にアクセスするには、次のようにします。
［プライバシー］|［サイト一覧］**を選択します。**

図 8-2: プライバシー サイト一覧

［編集済み］カラムの鉛筆のアイコンは、そのサイトのプライバシー設定がカスタマイズされているため一覧に保持されることを示すものです。

サードパーティの広告ブロック ソフトウェアを Zone Labs セキュリティ ソフトウェア と同時に使用する場合、プライバシー サイト一覧に情報が正しく入力されないことがあります。

プライバシー サイト一覧へのサイトの追加

サイト一覧に表示されないサイトのプライバシー設定をカスタマイズするには、サイトを手動で追加してから、そのサイトのプライバシー オプションを編集します。

サイトをプライバシー サイト一覧に追加するには、次のようにします。

1. ［**プライバシー**］|［**サイト一覧**］を選択します。
2. ［**追加**］をクリックします。

［サイトの追加］ダイアログが表示されます。

3. [URL] フィールドに、追加するサイトの URL を入力し、[OK] をクリックします。

   URL は、www.yahoo.com などの完全修飾ホスト名にする必要があります。

ZoneAlarm Pro と AOL を使用していて、プライバシー プロテクションを有効にしている場合、AOL セッション中であればどのサイトにアクセスしても、プライバシー サイト一覧には ie3.proxy.aol.com というサイトが追加されます。たとえば、AOL セッション中に www.cnn.com というサイトにアクセスした場合、プライバシー サイト一覧には AOL のプロキシ サイトである ie3.proxy.aol.com のみが追加されます。ie3.proxy.aol.com サイトのプライバシー設定が、AOL 内でアクセスするサイトすべてに適用されます。サイト一覧に手動でサイトを追加する場合は、そのサイトのプライバシー設定は無視され、AOL プロキシ サイト ie3.proxy.aol.com のセキュリティ設定のみが有効となります。

サイト一覧のサイトの編集

サイト一覧に含まれているサイトのプライバシー オプションを編集して、Cookie コントロール、広告ブロック、およびモバイル コード コントロールの動作をカスタマイズできます。

1. **[プライバシー]**|**[サイト一覧]** を選択します。
2. [サイト] カラムで編集するサイトを選択し、**[オプション]** をクリックします。

   [サイト オプション] ダイアログが表示されます。

3. [Cookie]、[広告ブロック]、[モバイル コード] のいずれかのタブを選択します。

   カスタム オプション選択のヘルプは、157 ページの「Cookie コントロールのカスタマイズ」、160 ページの「広告ブロックのカスタマイズ」、および 162 ページの「モバイル コード コントロールのカスタマイズ」を参照してください。

4. オプションを指定して、[OK] をクリックします。

Cookie コントロールのカスタマイズ

インターネット Cookie を使用することで、E コマース サイト（Amazon など）ではアクセスと同時にユーザを識別して、訪問するページをカスタマイズできます。しかし、Cookie は、ユーザの Web 閲覧動向を記録し、その情報をマーケターや広告主に提供するために使用されることもあります。

デフォルトでは、Cookie コントロールは無効で、すべての種類の Cookie が許可されます。Cookie コントロールを「高」に設定することで、すべての Cookie を即座にブロックすることができます。この設定では、あらゆる種類の Cookie の悪用からコンピュータが完全に保護されますが、Cookie が提供する便利な機能も使えなくなります。

Cookie コントロールを「高」に設定することで、すべての Cookie を即座にブロックすることができます。この設定では、あらゆる種類の Cookie の悪用からコンピュータが完全に保護されますが、Cookie が提供する便利な機能も使えなくなります。

ブロックする Cookie の種類、および、許可する Cookie の有効期限を指定して、Cookie コントロールをカスタマイズできます。

Cookie コントロールを含む一連のプライバシー機能は、ZoneAlarm Pro および ZoneAlarm Security Suite で提供されています。

セッション Cookie のブロック

セッション Cookie は Web サイトの閲覧中にブラウザのメモリ キャッシュに保存され、ブラウザ ウィンドウを閉じると同時に消えます。セッション Cookie は、その有効時間が短いため、最も安全な *Cookie* と言えます。

セッション Cookie をブロックするには、次のようにします。

1. **[プライバシー]**|**[メイン]** を選択します。
2. [Cookie コントロール] エリアで、**[カスタム]** をクリックします。
3. [セッション Cookie] エリアで、**[セッション Cookie をブロックする]** チェックボックスをオンにします。
4. **[OK]** をクリックします。

永続 Cookie のブロック

永続 Cookie はアクセスした Web サイトによってユーザのハード ディスク上に保管され、次回その Web サイトにアクセスする際に読み込まれます。これは便利な機能ですが、同時に、個人情報、コンピュータ情報またはインターネット使用に関する情報がテキスト ファイルで保管されるため、危険性も増加します。

永続 Cookie をブロックするには、次のようにします。

1. **[プライバシー]**|**[メイン]** を選択します。

2. ［Cookie コントロール］エリアで、［**カスタム**］をクリックします。
3. ［永続 Cookie］エリアで［**永続 Cookie をブロックする**］チェックボックスをオンにします。
4. **[OK]** をクリックします。

サードパーティ Cookie のブロック

サードパーティ Cookie は永続 Cookie の 1 種で、アクセスする Web サイトではなく、広告主その他のサードパーティによってコンピュータ上に配置されます。この Cookie は、一般的にユーザのインターネット動向をサードパーティに報告するために使用されます。

サードパーティ Cookie をブロックするには、次のようにします。

1. ［**プライバシー**］|［**メイン**］を選択します。
2. ［Cookie コントロール］エリアで、［**カスタム**］をクリックします。
3. ［サードパーティ Cookie］エリアで、ブロックする Cookie の種類を指定します。

サードパーティ Cookie をブロックする	サードパーティの Web サイトからの Cookie をブロックします。
Web のバグを無効にする	ユーザがどの広告や Web ページを閲覧したかについて、広告主が知ることができないようにします。ブロックされた Web バグは、空白のボックスとして表示されます。
プライベート ヘッダ情報を削除する	ユーザの IP アドレス、ワークステーション名、ログイン名、およびその他の個人情報がサードパーティ ソースに転送されることを防止します。

Cookie の有効期限の設定

永続 Cookie を使用するサイトでは、永続 Cookie の有効期限を数日間、数ヶ月、または無期限に設定できます。Cookie が有効な間、その Cookie を作成したサイト（またはサードパーティ）は、Cookie を使用して情報を検出することができます。Cookie が無効になると、その Cookie にアクセスすることはできません。

永続 Cookie を許可する場合、有効期限を上書きし、無効になるまでの期間を指定することができます。

Cookie の有効期限日を設定するには、次のようにします。

1. ［**プライバシー**］|［**メイン**］を選択します。
2. ［Cookie コントロール］エリアで、［**カスタム**］をクリックします。
3. ［Cookie の有効期限］エリアで、**[Cookie を期限切れにする]** チェックボックスをオンにします。

4. Cookie の有効期限日を指定します。

受信したらすぐに	永続 Cookie を受信したセッション中に限ってその Cookie が有効になるよう許可します。
受信してから n 日後	永続 Cookie が指定した日数の間有効になるよう許可します。1 から 999 の数値を選択することができます。デフォルトの設定は 1 です。

5. [適用] をクリックし、[OK] をクリックします。

広告ブロックのカスタマイズ

広告ブロックはデフォルトでは無効になっています。広告ブロックでは、すべての広告をブロックするようにも、特定のタイプの広告をブロックするようにもカスタマイズできます。さらに、Zone Labs セキュリティ ソフトウェア がブロックした広告の代わりに何を表示するかを指定できます。

広告ブロックを含む一連のプライバシー機能は、ZoneAlarm Pro および ZoneAlarm Security Suite で提供されています。

ブロックする広告の指定

プライバシー保護では、ブロックまたは許可する広告の種類を指定できます。

ブロックする広告を指定するには、次のようにします。

1. **[プライバシー]**|**[メイン]** を選択します。
2. [広告ブロック] エリアで、**[カスタム]** をクリックします。

   [カスタム プライバシー設定] ダイアログが表示されます。
3. [ブロックする広告] エリアで、ブロックする広告の種類を選択します。

バナー / スカイスクレイパー広告	水平または垂直バナー形式の広告をブロックします。
ポップアップ / ポップアンダー広告	表示中のウィンドウの前面または背面に新しいブラウザ ウィンドウとして表示される広告をブロックします。
アニメーション広告	動く画像を含む広告をブロックします。

4. **[OK]** をクリックします。

広告のボイド コントロール オプションの設定

Zone Labs セキュリティ ソフトウェアがバナー、スカイスクレイパー、またはアニメーション広告をブロックすると、その広告が表示されるはずだった画面上の場所は、「ボイド」すなわち空白になります。広告のボイドコントロールを使用すると、そのスペースに何を表示するかを指定できます。

ブロックされた広告に代わる表示内容を指定するには、次のようにします。

1. **[プライバシー]**|**[メイン]** を選択します。
2. [広告ブロック] エリアで、**[カスタム]** をクリックします。

   [カスタム プライバシー設定] ダイアログが表示されます。

3. ［広告のボイド コントロール］エリアで、ブロックされた広告のコントロール方法を指定します。

空白	広告の表示場所であることを示さずに広告をブロックします。
「[AD]」というテキストが表示されたボックス	「[AD]」というテキストを含むウィンドウを表示します。これは、デフォルトの設定です。
マウスでポイントすると広告を表示するボックス	広告を含んだウィンドウを表示します。マウスを使用してウィンドウをアクティブにしたときのみ、広告が表示されます。

4. [OK] をクリックします。

モバイル コード コントロールのカスタマイズ

モバイル コードは Web ページ上のアクティブまたは実行可能なコンテンツです。アクティブなコンテンツの例としては、*Java アプレット*、*ActiveX コントロール*、および *JavaScript* などがあり、これらを使用するとよりインタラクティブでダイナミックな Web ページを作成できます。

その一方、悪意のあるモバイル コードにより、ファイルのコピーやハードディスクの削除、パスワードの盗取、またはサーバに対する命令などが行われることがあります。モバイル コード コントロールは、ユーザのセキュリティの低下やコンピュータの破損を目的にした、ハッカーによるアクティブ コンテンツの悪用を防止します。

モバイル コード コントロールは、デフォルトではオフに設定されています。オンに設定すると、JavaScript 以外のモバイル コードがすべてブロックされます。モバイル コード コントロールがオンの場合でも、モバイル コード コントロールの設定をカスタマイズして、ブロックするモバイル コードの種類を指定することができます。

モバイル コードを含む一連のプライバシー機能は、ZoneAlarm Pro および ZoneAlarm Security Suite で提供されています。

ブロックするモバイル コードの種類の指定

ブロックまたは許可するアクティブ コンテンツの種類を指定して、モバイル コード コントロールをカスタマイズできます。

モバイル コード コントロールをカスタマイズするには、次のようにします。

1. **［プライバシー］**|**［メイン］** を選択します。
2. ［モバイル コード コントロール］エリアで、**［カスタム］** をクリックします。

   ［カスタム プライバシー設定］ダイアログが表示されます。
3. ［モバイル コード コントロール］エリアで、ブロックするモバイル コードの種類を指定します。

JavaScript をブロックする	JavaScript コンテンツをブロックします。［戻る］および［履歴］のリンク、ロールオーバ イメージ、ブラウザ ウィンドウの開閉など、一般的な用途に必要とされるコンテンツもブロックされます。
スクリプトをブロックする (vbscript など)	自動的に実行されるスクリプトをブロックします。バナー、ポップアップ広告、ダイナミック メニューの表示に必要とされるスクリプトもブロックされます。

埋め込みオブジェクトをブロックする（java、ActiveX など）	サウンド ファイルや画像ファイルなど、Web ページに埋め込まれているオブジェクトをブロックします。
MIME オブジェクトをブロックする	MIME オブジェクトのブロックは、オブジェクトがアプリケーションであることを示す MIME タイプのオブジェクトをブロックします。 注意：このオプションは、許可する必要のあるファイルのダウンロードを含め、ブラウザを通じて送信された正当な実行可能ファイルもブロックします。このような場合、ブラウザには「このオブジェクトはブロックされました」というエラーが表示されます。ユーザが意識的に開始したダウンロードについては、MIME のブロック機能を無効にしても安全です。

キャッシュ クリーナの概念

ファイルや Web ページの表示、またはオンライン フォームの記入を行うたびに、表示される Web ページのコピーがブラウザのキャッシュに保管され、各ページがよりすばやくロードされるようになります。コンピュータを共有している場合は、他のユーザもこれらのファイルを表示することができます。

同様に、コンピュータ上でファイルの表示や削除、検索を行うと、電子的な痕跡が残り、後でこれらの操作を簡単に確認することができます。これらは便利な機能ではありますが、時間が経過すると不要なファイルがたまり、コンピュータのパフォーマンスと処理効率に支障をきたすことがあります。また、コンピュータを共有している場合は、アクセスした Web サイトを他のユーザに知られてしまう可能性があります。

Zone Labs セキュリティ ソフトウェアのキャッシュ クリーナを使ってこうした不要なファイルを定期的に削除することでディスク スペースを開放し、プライバシーを保護することができます。

キャッシュ クリーナを含む一連のプライバシー機能は、ZoneAlarm Pro および ZoneAlarm Security Suite で提供されています。

キャッシュ クリーナの使用

キャッシュ クリーナは必要に応じていつでも手動で実行できます。定期的にキャッシュのクリーニングを行うために、一定の間隔でキャッシュ クリーナを自動実行するように設定することもできます。自動実行の頻度は毎日から 99 日ごとまで設定できます。自動実行のデフォルトは 14 日ごとに設定されています。

キャッシュ クリーナを手動で実行するには、次のようにします。

1. **［プライバシー］**|**［キャッシュ クリーナ］**を選択します。
2. **［削除］**をクリックします。

   確認のメッセージが表示されます。
3. **[OK]** をクリックします。

   キャッシュ クリーナの実行中は進行状況を示すメータが表示されます。

キャッシュ クリーナの自動実行を設定するには、次のようにします。

1. **［プライバシー］**|**［キャッシュ クリーナ］**を選択します。
2. **［設定した周期でキャッシュを自動的に削除する］**チェックボックスをオンにします。

3. ［自動でキャッシュを削除］エリアで、1 ～ 99 までの間隔を指定します。

   チェックボックスの下に、キャッシュ クリーナの最終実行日と次回の実行予定日が表示されます。

ハード ドライブの削除オプションのカスタマイズ

デフォルトでは、キャッシュ クリーナはご使用のハード ドライブから次のファイルを削除します。

- ごみ箱の中身
- 一時ファイル ディレクトリの中身
- Windows ScanDisk ファイル断片

ファイルの履歴、検索の履歴、Windows Media Player の履歴など、削除の対象とするエリアを追加して、この設定をカスタマイズできます。

ハード ドライブの削除オプションをカスタマイズするには、次のようにします。

1. ［**プライバシー**］|［**キャッシュ クリーナ**］を選択し、［**カスタム**］をクリックします。
2. ［**ハード ドライブ**］を選択して、削除オプションを指定します。

最近使ったファイルの履歴	［スタート］|［最近使ったファイル］に表示されるファイルの一覧を削除します。この設定は、現在ログオンしているユーザの最近使ったファイルの履歴のみに適用されます。
ごみ箱	Windows のごみ箱の中身を削除します。デフォルトで選択されています。
一時ファイル ディレクトリ	Windows の一時ファイル ディレクトリ内を削除します。デフォルトで選択されています。
Windows 検索の履歴	Windows 検索の一覧内の項目を削除します。
Windows Scandisk ファイル断片	Windows の ScanDisk プログラムによって回復された紛失データや破損データの断片を削除します。デフォルトで選択されています。
Windows Media Player の履歴	Windows Media Player で最近再生されたメディア クリップの一覧を削除します。
ファイル名を指定して実行の履歴	［スタート］|［ファイル名を指定して実行］の［名前］ドロップダウン リストに表示される一覧を削除します。

3. ［**適用**］をクリックし、[OK] をクリックします。

ブラウザの削除オプションのカスタマイズ

Internet Explorer または Netscape のいずれかをご使用の場合は、Web の閲覧中にコンピュータに保管される Cookie ファイルを削除するように

キャッシュ クリーナを設定することができます。キャッシュ クリーナは、個々の Cookie ファイルそのものではなく、Cookie の発信元を基準に、削除する Cookie を識別します。削除する Cookie の発信元を指定すると、キャッシュ クリーナがその発信元の Cookie をすべて削除します。コンピュータ上の特定の Cookie を削除したくない場合は、それらの Cookie を保持するようにキャッシュ クリーナを設定できます。

IE/MSN の削除オプションをカスタマイズするには、次のようにします。

1. **[プライバシー]**|**[キャッシュ クリーナ]** を選択し、**[カスタム]** をクリックします。
2. **[IE/MSN]** タブを選択します。
3. Internet Explorer/MSN の削除オプション部分で、削除の対象を指定します。

キャッシュを削除する	Internet Explorer ブラウザのキャッシュを削除します。デフォルトで選択されています。
URL の履歴を削除する	[アドレス] フィールドの URL の一覧を削除します。デフォルトで選択されています。
オートコンプリート フォームを削除する	パスワードなど、過去に Web フォームに記入した情報を削除します。 **注意**： パスワードを削除したくない場合は、[オートコンプリート フォームを削除する] チェックボックスをオフにします。
オートコンプリート パスワードの削除	[パスワードを保存する] を選択して、以前に保存したパスワードを削除します。
ロックした Index.dat ファイルを削除する	現在コンピュータで使用中の *index.dat* ファイルを削除します。デフォルトで選択されています。
入力した URL の履歴を削除する	[アドレス] フィールドに手動で入力した URL を削除します。デフォルトで選択されています。

4. Cookie を削除するには、**[IE/MSN の Cookie を削除する]** チェックボックスをオンにしてから、**[選択]** をクリックします。

   [削除しない IE/MSN の Cookie を選択する] ダイアログが表示されます。左の一覧には、現在ブラウザによって Cookie が保管されているサイトが表示されます。右の一覧には、削除しないように指定した Cookie の発信元であるサイトが表示されます。

5. Cookie の発信元を保持するには、Cookie の発信元を選択して、**[残す]** をクリックします。
6. 残りの Cookie を削除するには、**[削除]** をクリックしてから、**[OK]** をクリックします。

Netscape の削除オプションをカスタマイズするには、次のようにします。

1. ［**プライバシー**］|［**キャッシュ クリーナ**］を選択し、［**カスタム**］をクリックします。
2. ［Netscape］タブを選択します。
3. Netscape の削除オプションのエリアで、削除の対象を指定します。

キャッシュを削除する	Netscape ブラウザのキャッシュを削除します。デフォルトで選択されています。
URL の履歴を削除する	［場所］フィールドの URL の一覧を削除します。デフォルトで選択されています。
メール用ごみ箱内を削除する	Netscape のメール用ごみ箱フォルダ内を削除します。
フォーム データを削除する	過去に Web フォームに記入した情報を削除します。

4. Cookie を削除するには、［Netscape の Cookie の削除］チェックボックスをオンにします。

   ［削除しないネットスケープ Cookie を選択する］ダイアログが表示されます。左の一覧には、現在ブラウザによって Cookie が保管されているサイトが表示されます。右の一覧には、削除しないように指定した Cookie の発信元であるサイトが表示されます。

5. Cookie の発信元を保持するには、Cookie の発信元を選択して、［**残す**］をクリックします。
6. 残りの Cookie を削除するには、［**削除**］をクリックしてから、［OK］をクリックします。

第 9 章

警告とログ

9

Zone Labs セキュリティ ソフトウェア は、コンピュータ上で発生していることをすべて把握したい場合から、コンピュータが安全であることが確認できればよい場合まで、ユーザのニーズに合わせて調整することができます。Zone Labs セキュリティ ソフトウェアの保護機能が動作するたびにユーザに警告を通知することもできますし、ハッカーによる活動と思われる場合のみに警告を表示することもできます。また、ログに記録する対象として、すべての警告、高レベルの警告のみ、または特定の種類の通信によって発生した警告のみを選択することができます。

トピック：

- 170 ページの「警告とログの概念」
- 177 ページの「基本的な警告およびログ オプションの設定」
- 178 ページの「特定の警告の表示または非表示」
- 179 ページの「イベントおよびプログラムのログ オプションの設定」
- 186 ページの「SmartDefense Advisor およびハッカー ID の使用」

警告とログの概念

Zone Labs セキュリティ ソフトウェアの警告とログ機能は、コンピュータでのユーザの作業を大幅に妨げることなくコンピュータ上でのイベントを知らせるとともに、過去の警告の調査を可能にします。エキスパート ルール オプションでは、ブロックされた通信のみでなく、許可された通信のトラッキングも可能になるため、上級ユーザが各環境に合わせてセキュリティ ルールをカスタマイズする際には最大限の情報を利用できます。

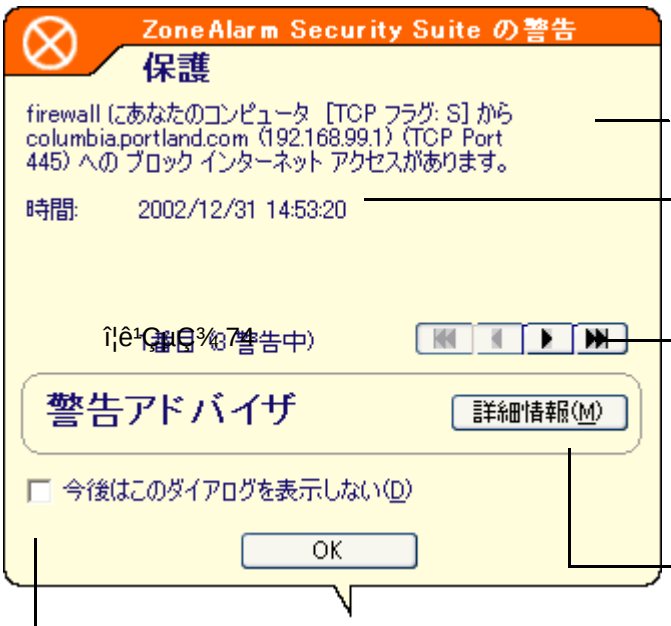
Zone Labs セキュリティ ソフトウェアの警告について

Zone Labs セキュリティ ソフトウェアの警告は、情報警告、プログラム警告、ネットワーク警告の 3 つの基本的なカテゴリに分類されます。ご使用の Zone Labs セキュリティ ソフトウェアに基づいて表示される可能性がある追加警告には、ID ロック警告および OSFirewall 警告が含まれます。

表示される警告の種類と対処法については、221 ページから始まる付録 A「警告のリファレンス」を参照してください。

情報警告

情報警告は、Zone Labs セキュリティ ソフトウェア がセキュリティ設定に合致しない接続をブロックしたことを通知するものです。最も一般的な情報警告は、ファイアウォール警告です。



ブロックされたパケットを送信したコンピュータの IP アドレス、使用されたプロトコル、そのパケットの送信先のポート。

警告が発生した日時。

警告ボックスが開いてから発生した警告の数。警告を表示するには、矢印ボタンを使用する。

警告データを SmartDefense Advisor に送信するには［詳細情報］をクリックする。

このダイアログ ボックスを今後表示しないようにするには、[OK] をクリックする前にこのチェックボックスをオンにする。

図 9-1: ファイアウォール警告

情報警告については、ユーザによる対応は必要ありません。警告ポップアップの下部にある **[OK]** ボタンをクリックすると、警告が閉じます。この操作は、お使いのコンピュータに対する通信を許可するものではありません。

プログラム警告

プログラム警告では、プログラムに対して、インターネットまたはローカル ネットワークへのアクセスを許可するか、またはサーバとして動作することを許可するかをユーザに問い合わせるメッセージが表示されます。プログラム警告では、応答として［許可］または［拒否］を選択する必要が

あります。プログラム警告のなかで最も頻繁に表示されるものは、新しいプログラム警告および繰り返されたプログラム警告です。

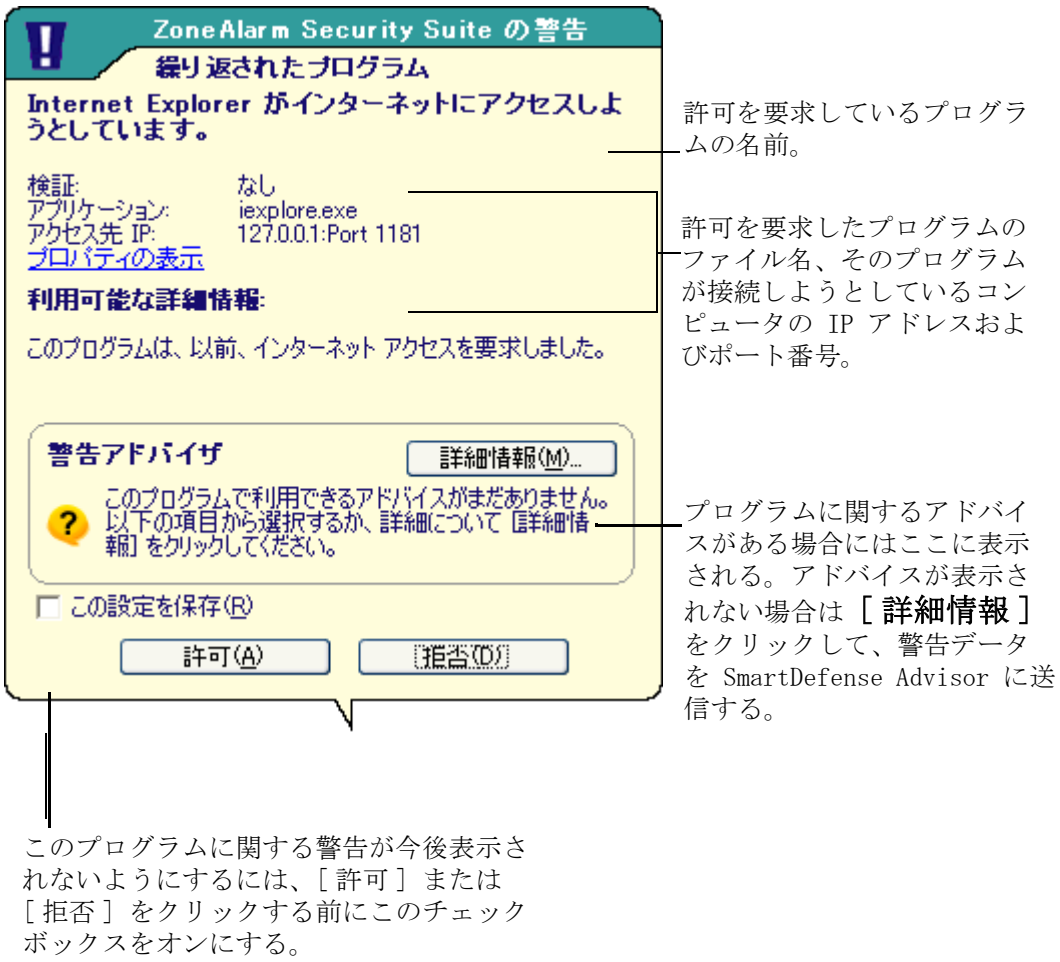
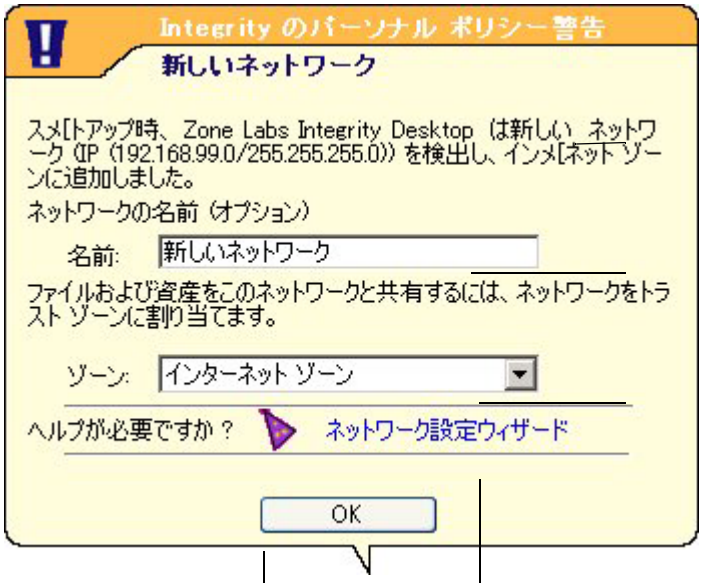


図 9-2: 新しいプログラム警告

［許可］ボタンをクリックすると、プログラムに許可を与えます。［拒否］ボタンをクリックすると、プログラムに許可を与えません。

新しいネットワーク警告

新しいネットワーク警告は、家庭内のワイヤレス ネットワーク、企業内 LAN、または ISP のネットワークのいずれのネットワークに接続する場合でも表示されます。



ネットワークの種類（ワイヤレスまたはその他）、IP アドレス、および検出されたネットワークのサブネット マス

ここにネットワークの名前を入力する。この名前は、後でネットワークを識別できるように、[ゾーン] タブに表示

新しいネットワークを配置するゾーンを選択する。ISP ではなく、家庭内または企業内 LAN であることがわかっている場合にのみ、トラスト ゾーンにネットワークを配置する。

[OK] をクリックして選択したゾーンにネットワークを配置し、警告ボックスを閉じる。

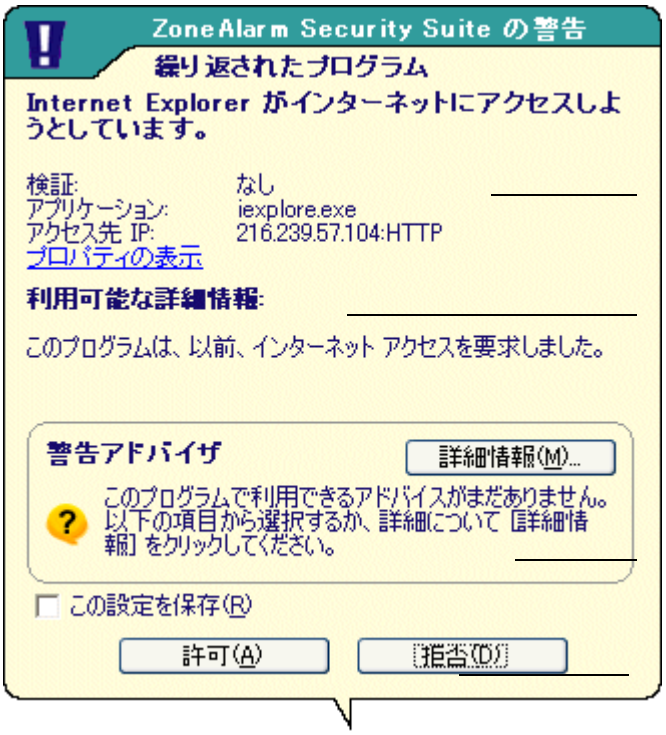
ネットワークの設定の詳細なヘルプについては、ネットワーク設定ウィザードにアクセスしてください。

図 9-3: 新しいネットワーク警告

ID ロック警告

ZoneAlarm Pro および ZoneAlarm Security Suite では、ID ロック機能を有効している場合、myVAULT に保存されている個人情報がトラスト サイト

リストに登録されていない宛先へ送信されようとすると ID ロック警告が表示されます。



送信される情報についての説明。

ここには、情報を送信しようとしているアプリケーションと、送信先のコンピュータの IP アドレスが表示される。

警告データを SmartDefense Advisor に送信するには **[詳細情報]** をクリックする。

この送信先をトラスト サイト リストに追加するには、このチェックボックスをオンにする。

図 9-4: ID ロック警告

[はい] ボタンをクリックすると、要求元 IP アドレスへの情報の送信を許可します。今後この送信先への myVAULT データの送信時に警告が表示されないようにするには、**[記憶しますか…]** チェックボックスをオンにして、この送信先をトラスト サイト リストに追加します。

OSFirewall 警告

表示される OSFirewall 警告には、「疑わしい」と「悪意がある」という 2 つの種類があります。これらの OSFirewall 警告はいずれも、ZoneAlarm

Security Suite がコンピュータ上のプログラムによるデータやコンピュータに有害な可能性のあるアクションの実行を検出したことを通知します。

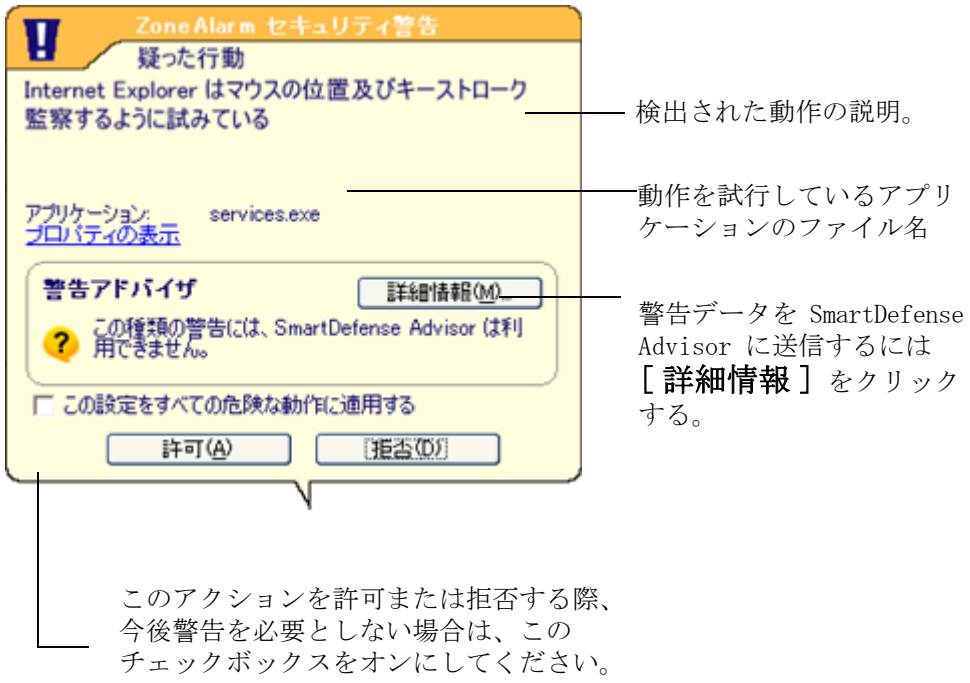


図 9-5: 疑わしい動作の警告

疑わしい動作の警告は、プログラムのデフォルトの動作に変更を加える可能性のあるアクションを通知します。たとえば、プログラムがご使用のブラウザのホームページを修正しようとすると、疑わしい動作の警告が通知されます。これに対し、危険な動作の警告は、プログラムやオペレーティ

ング システムの基本的な機能を停止する可能性があったり、アクティビティを監視しようとするスパイウェアになりうるアクションを通知します。

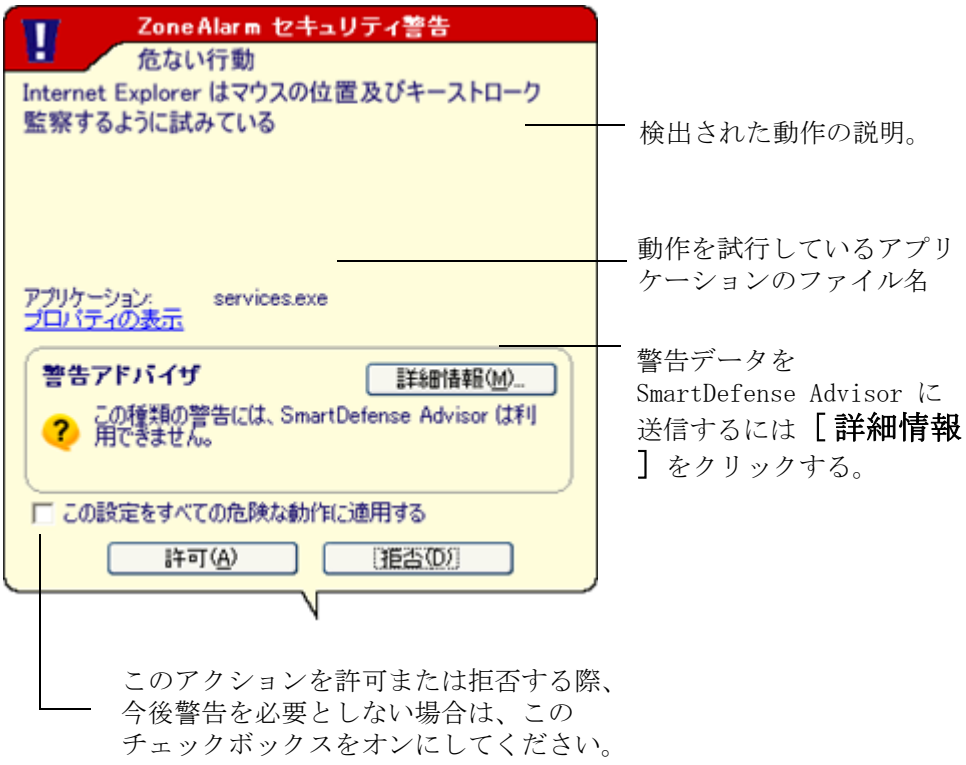


図 9-6: 危険な動作の警告

OSFirewall 警告および検出された動作の種類については、273 ページから始まる付録 D「プログラム動作」を参照してください。

イベントのログ

デフォルトでは、Zone Labs セキュリティ ソフトウェア は、警告が表示されるかどうかに関わらず、通信がブロックされるたびにログ エントリを作成します。ログ エントリには、発信元、送信先、ポート、プロトコル、およびその他の詳細が記録されます。これらの情報は ZALOG.txt という名前のテキスト ファイルに記録され、Internet Logs フォルダに保管されます。ログ ファイルは、サイズが大きくなりすぎないように、60 日ごとに日付を記したファイルにアーカイブされます。

ファイアウォール警告のみを対象にログ エントリを作成する場合、または、特定の種類のプログラム警告についてログ エントリを抑制する場合など、特定のイベント カテゴリがログされないように指定することもできます。また、トラッキング機能を有効にしたエキスパート ルールを作成して、許可を与えた特定の通信タイプをログするように Zone Labs セキュリティ ソフトウェア を設定することもできます。

基本的な警告およびログ オプションの設定

基本的な警告とログ オプションでは、Zone Labs セキュリティ ソフトウェア が警告を表示するイベントの種類とログ エントリを作成するイベントの種類を指定することができます。

警告イベント レベルの設定

[警告とログ]の［メイン］タブにある［警告イベントの表示］コントロールにより、警告の表示をレベル別に設定できます。プログラム警告と ID ロック警告は、許可を与えるかどうかをユーザが選ぶ必要があるため、常に表示されます。

警告イベント レベルを設定するには、次のようにします。

1. **［警告とログ］|［メイン］**を選択します。
2. ［警告イベントの表示］で、適切な設定を選択します。

高	「中」および「高」両方のレベルのすべてのセキュリティ イベントについて警告を表示します。
中	ハッカーによる活動の結果である可能性が高い、高レベルの警告のみを表示します。
オフ	プログラム警告および ID ロック警告のみを表示します。情報警告は表示されません。

イベントおよびプログラムのログ オプションの設定

［イベントのログ］エリアと［プログラムのログ］エリアで、ログの対象とする情報警告とプログラム警告の種類を選択します。

イベント ログとプログラム ログを有効または無効にするには、次のようにします。

1. **［警告とログ］|［メイン］**を選択します。
2. ［イベントのログ］エリアで、適切な設定を選択します。

オン	すべてのイベントについてログ エントリを作成します。
オフ	イベントについてログを作成しません。

3. ［プログラムのログ］で、ログのレベルを指定します。

高	すべてのプログラム警告についてログ エントリを作成します。
中	高レベルのプログラム警告についてのみログ エントリを作成します。
オフ	プログラム イベントについてログを作成しません。

特定の警告の表示または非表示

表示設定を指定して、すべてのセキュリティおよびプログラム イベントについて警告を表示することも、ハッカーの活動が原因と思われるイベントのみに警告を表示することもできます。

ファイアウォール警告の表示または非表示

[警告イベント] タブでは、ファイアウォールおよびプログラム警告が表示されてブロックされた通信の種類を指定することにより、警告表示についてより詳細に設定できます。

ファイアウォールまたはプログラム警告を表示 / 非表示にするには、次のようにします。

1. **[警告とログ]**|**[メイン]** を選択し、**[詳細設定]** をクリックします。

   [警告とログ設定] ダイアログが表示されます。

2. [警告イベント] タブを選択します。

3. [警告] カラムでは、Zone Labs セキュリティ ソフトウェア で警告を表示するブロックされた通信の種類を選択します。

4. **[適用]** をクリックし、変更を保存します。

システム トレイ警告の有効化

一部またはすべての情報警告を非表示にした場合でも、Zone Labs セキュリティ ソフトウェア が小さな警告アイコン  をシステム トレイに表示して警告の存在を知らせるようにできます。

システム トレイ警告を有効にするには、次のようにします。

1. **[警告とログ]**|**[メイン]** を選択します。

2. **[詳細設定]** をクリックして、**[システム トレイ警告]** タブをクリックします。

3. **[システム トレイ アイコン警告を有効にする]** チェックボックスをオンにします。

イベントおよびプログラムのログ オプションの設定

各種警告のログを有効または無効にすることで、Zone Labs セキュリティ ソフトウェア がセキュリティ イベントおよびプログラム イベントを記録するかどうかを指定できます。

ログ形式の設定

次のコントロールを使用して、テキスト形式のログ ファイルのフィールド区切りを指定します。

ログ エントリ形式を設定するには、次のようにします。

1. **［警告とログ］**を選択し、**［詳細設定］**をクリックします。

   ［警告とログの詳細設定］ダイアログ ボックスが表示されます。

2. **［ログ コントロール］**タブを選択します。

3. ［ログ ファイルの形式］エリアで、ログに使用する形式を選択します。

タブ	タブ文字でフィールドを区切る場合は、［タブ］を選択します。
コンマ	コンマでフィールドを区切る場合は、［コンマ］を選択します。
セミコロン	セミコロンでログ フィールドを区切る場合は、［セミコロン］を選択します。

イベントのログのカスタマイズ

デフォルトでは、Zone Labs セキュリティ ソフトウェア は高レベルのファイアウォール イベントが発生した場合にログ エントリを作成します。MailSafe での添付ファイルの隔離、非 IP パケットのブロック、ロック違反など、特定のセキュリティ イベントに関するログ エントリの作成を抑制または許可することで、ファイアウォール警告のログ機能をカスタマイズできます。

イベントの種類に基づいてログ エントリを作成または抑制するには、次のようにします。

1. **［警告とログ］**|**［メイン］**を選択します。

2. **［詳細設定］**をクリックします。

   ［警告とログの詳細設定］ダイアログ ボックスが表示されます。

3. **［警告イベント］**を選択します。

4. ［ログ］カラムで、Zone Labs セキュリティ ソフトウェア がログ エントリを作成するイベントの種類を選択します。

5. **［適用］**をクリックし、変更を保存します。

6. [OK] をクリックして［警告とログ設定］ダイアログを閉じます。

プログラムのログのカスタマイズ

デフォルトでは、Zone Labs セキュリティ ソフトウェア は、発生したすべてのプログラム警告についてログ エントリを作成します。新しいプログラム警告、繰り返されたプログラム警告、サーバ プログラム警告など、特定の種類のプログラム警告に関するログ エントリを抑制することで、プログラム警告のログをカスタマイズできます。

イベントの種類に基づいてログ エントリを作成または抑制するには、次のようにします。

1. **［警告とログ］**|**［メイン］** を選択します。
2. ［プログラムのログ］エリアで、**［カスタム］** をクリックします。
3. ［プログラムのログ］カラムで、Zone Labs セキュリティ ソフトウェア がログ エントリを作成するイベントの種類を選択します。
4. **［適用］** をクリックし、変更を保存します。
5. [OK] をクリックして［警告とログ設定］ダイアログを閉じます。

ログ エントリの表示

ログ エントリは、テキスト エディタを使ってテキスト ファイルとして表示、またはログ ビューアで表示することができます。各ログの形式は多少異なっていますが、ログに含まれる一般的な情報は同じです。

［ログ ビューア］の現在のログを表示するには：

1. **［警告とログ］**|**［ログ ビューア］** を選択します。
2. 警告の一覧で表示する警告数（1 ～ 999）を選択します。

   カラム ヘッダをクリックすると、そのフィールドを基準にして一覧をソートすることができます。ヘッダ名の隣の矢印（^）は、ソートの順序を示しています。同じヘッダを再度クリックすると、ソートの順序が逆になります。

3. 表示する警告の種類を、次から選択します。

アンチウイルス	日付 / 時間、種類、ウイルス名、ファイル名、対応、モード、メール情報の各カラムが表示されます。
ファイアウォール	レベル、日付 / 時間、種類、プロトコル、プログラム、発信元 IP アドレス、送信先 IP アドレス、方向、対応、回数、発信元 DNS アドレス、送信先 DNS アドレスの各カラムが表示されます。
IM セキュリティ	日付 / 時間、種類、発信元、プログラム、ローカル ユーザ、リモート ユーザ、動作の各カラムが表示されます。
OSFirewall	レベル、日付 / 時間、種類、サブタイプ、データ、プログラム、方向、動作、回数の各カラムが表示されます。
プログラム	レベル、日付 / 時間、種類、プログラム、発信元 IP アドレス、送信先 IP アドレス、方向、対応、回数、発信元 DNS アドレス、送信先 DNS アドレスの各カラムが表示されます。
アンチスパイウェア	日付、種類、スパイウェア名、ファイル名、動作、アクタの各カラムが表示されます。

ログ ビューアには、Zone Labs セキュリティ ソフトウェアのログに記録されたセキュリティ イベントが表示されます。各種警告についてのログ ビューアのフィールドの詳細は、「ファイアウォール」、「プログラム コントロール」、「アンチウイルス」、および「IM セキュリティ」の各章を参照してください。

フィールド	情報
説明	イベントの説明。
方向	ブロックされた通信の方向。「外部から」は、ご使用のコンピュータに対して送信された通信を示します。「外部へ」は、ご使用のコンピュータから発信した通信を示します。
種類	警告の種類： ファイアウォール、プログラム、ID ロック、ロック有効。
発信元 DNS アドレス	警告の原因となった通信を送信したコンピュータのドメイン名。
発信元 IP アドレス	Zone Labs セキュリティ ソフトウェア がブロックした通信の送信元であるコンピュータの IP アドレス。

表 9-7: ログ ビューアのフィールド

フィールド	情報
レベル	各警告は、レベルが「高」または「中」です。高レベルの警告は、ハッカーの活動が原因となっている可能性があります。中レベルの警告は、不要な、しかし害のないネットワーク通信が原因となっている可能性があります。
プロトコル	警告の原因となった通信で使用された通信プロトコル。
対応	Zone Labs セキュリティ ソフトウェア で通信が処理された方法。
送信先 DNS アドレス	警告の原因となった通信で意図されていた送信先のドメイン名。
送信先 IP アドレス	ブロックされた通信の送信先のコンピュータのアドレス。
回数	種類、発信元、送信先、およびプロトコルがすべて同じ警告が単一セッション中に発生した回数。
日付 / 時間	警告が発生した日時。
プログラム	データを送信または受信しようとしたプログラムの名前。(プログラム警告および ID ロック警告でのみ使用されます)

表 9-7: ログ ビューアのフィールド

テキスト ログの表示

デフォルトでは、Zone Labs セキュリティ ソフトウェア により生成された警告は *ZAlog.txt* というファイルに保存されます。Windows95、Windows98 または Windows Me を使用している場合、このファイルは、(x):¥Windows¥Internet Logs フォルダに保存されます。WindowsNT または Windows2000 を使用している場合は、(x):¥Winnt¥Internet Logs フォルダに保存されます。

現在のログをテキスト ファイルとして表示するには、次のようにします。

1. **［警告とログ］**|**［メイン］**を選択します。
2. **［詳細設定］**をクリックします。

［警告とログの詳細設定］ダイアログ ボックスが表示されます。

3. ［ログ コントロール］タブを選択します。

［ログ ファイルの場所］エリアで、［**ログの表示**］をクリックします。

テキスト ログのフィールド

ログのエントリには、次の表に示すフィールドが組み合わせて使用されます。

フィールド	説明	例
種類	記録されたイベントの種類。	FWIN
日付	警告の日付（yyyy/mm/dd 形式）。	2001/12/31(2001 年 12 月 31 日)
時間	警告が発生したローカル時間。このフィールドは、ローカル時間とグリニッジ標準時（GMT）との時差も表示します。	17:48:00 -8:00GMT（午後 5:48、グリニッジ標準時よりも 8 時間進んでいます。グリニッジ標準時では、01:48 です。）
ウイルス名	イベントの原因となったウイルスの名前。このフィールドは、アンチウイルス イベントの場合にのみ表示されます。	iloveyou
ファイル名	イベントの原因となったファイルの名前。このフィールドは、アンチウイルス イベントの場合にのみ表示されます。	iloveyou.exe
操作	イベントが処理された方法。このフィールドの値は、発生したイベントの種類によって異なります。	アンチウイルス名前変更 IM Security: 暗号化 MailSafe: 隔離 ID ロック ：ブロック
カテゴリ	イベントで検出された情報の ID ロック カテゴリ。このフィールドは、ID ロック イベントの場合にのみ表示されます。	アクセス PIN
プログラム	ID ロック情報を含んだメールを送信または受信しようとしているプログラム。このフィールドは、ID ロック イベントの場合にのみ表示されます。	Outlook.exe

フィールド	説明	例
発信元	ブロックされたパケットを送信したコンピュータの IP アドレスと使用されたポート；またはアクセス許可を要求したコンピュータ上のプログラム。	192.168.1.1:7138 Outlook.exe
送信先	ブロックされたパケットの送信先のコンピュータの IP アドレスおよびポート。	192.168.1.101:0
トランスポート	使用されたプロトコル（パケット タイプ）。	UDP

ログ エントリのアーカイブ

ZAlog.txt の内容は、ZALog2004.06.04.txt（2004 年 6 月 4 日の場合）などの日付の付いたファイルに定期的にアーカイブされます。これにより、ZAlog.txt のサイズは大きくなり過ぎることはありません。

アーカイブされたログ ファイルを表示するには、Windows エクスプローラでログが保存されている場所を参照します。

アーカイブの頻度を設定するには、次のようにします。

1. ［**警告とログ**］|［**メイン**］を選択し、［**詳細設定**］をクリックします。
2. ［**ログ コントロール**］タブを選択します。
3. ［**ログ アーカイブの頻度**］チェックボックスをオンにします。

［ログ アーカイブの頻度］チェックボックスがオンになっていない場合でも、Zone Labsセキュリティ ソフトウェア は引き続きイベントを記録して［ログ ビューア］タブに表示します。ただし、ZAlog.txt ファイルにアーカイブはしません。

4. ［ログ アーカイブの頻度］エリアで、ログの頻度（1 ～ 60 日）を指定して、［**適用**］をクリックします。

アーカイブの場所の指定

ZAlog.txt ファイルおよびすべてのアーカイブされたログ ファイルは同じディレクトリに保存されます。

ログとアーカイブの場所を変更するには、次のようにします。

1. ［**警告とログ**］|［**メイン**］を選択します。
2. ［**詳細設定**］をクリックします。

   ［警告とログの詳細設定］ダイアログ ボックスが表示されます。
3. ［**ログ コントロール**］タブを選択します。

4. ［ログ アーカイブの場所］エリアで、**［参照］**をクリックします。
   ログとアーカイブ ファイルの場所を選択します。

SmartDefense Advisor およびハッカー ID の使用

Zone Labs の SmartDefense Advisor は、警告の原因を即座に分析することのできるサービスであり、対応処置を決定する際に役立ちます。プログラム警告への対処方法が用意されている場合、SmartDefense Advisor はその対処方法をアドバイスとして表示します。アドバイスが表示されない場合、警告の［**詳細情報**］をクリックすると、警告についての詳細情報を確認できます。SmartDefense Advisor は、警告に関する説明、およびセキュリティの確保に必要な対策についてのアドバイスなどを返信します。

警告の原因となる発信元の IP アドレスまたは送信先 IP アドレスの物理的な場所およびその他の情報を表示するには、［ハッカー ID］タブをクリックします。このタブには、送信された IP アドレスについての情報が表示されます。

eBay を頻繁に利用しており、eBay のパスワードをブロックしたことを示す ID ロック警告が表示された場合には、SmartDefense Advisor を使用して詐称レポートを eBay に送信できます。Zone Labs セキュリティ ソフトウェア による eBay ID の保護方法についての詳細は、26 ページの「オンライン詐称保護プロファイルの作成」を参照してください。

SmartDefense Advisor に警告を送信するには、次のようにします。

1. ［**警告とログ**］|［**ログ ビューア**］を選択します。
2. 送信する警告レコードを右クリックします。
3. ショートカット メニューから［**詳細情報**］を選択します。

ZoneAlarm Antivirus、ZoneAlarm Pro、または ZoneAlarm Security Suite を購入すると、1 年 あるいは 2 年のアップデート、サポート、サービス各種へのアクセスが提供されます。その期間の終了後、これらのサービスにアクセスするには年間保守契約が必要となります。Zone Labs は ZoneAlarm の機能およびサービス提供をいつでも停止する権利を有しています。

第 10 章

データの保護

10

代金の支払いや借金の申し込み、飛行便の予約など、これまで出向いて、または電話で行ってきた数多くのことが、インターネットのおかげでオンラインでできるようになりました。これにより、多数の歓迎すべき便宜のみでなく、いくつかの有り難くない危険も生じています。残念なことに、E コマースの増大の結果、個人情報の盗難事件も増加しています。

Zone Labs セキュリティ ソフトウェアの ID ロック機能は、個人情報をハッカーや盗難から保護します。

トピック：

- 188 ページの「ID ロック機能の概念」
- 191 ページの「myVAULT について」
- 194 ページの「トラスト サイト リストの使用」

ID ロック機能の概念

ユーザのコンピュータを使用して、ユーザまたは他人がクレジット カード番号、住所、米国の社会保障番号などの個人情報を電子メール メッセージや Web フォームに入力するたびに、その情報が盗まれる可能性が生じます。それを防ぐために、ID ロックは信頼できるサイトにのみ個人情報が送信されるようにします。

ID ロック機能は、myVAULT と呼ばれる安全なエリアを提供しており、ここに保護する個人情報を保存することができます。myVAULT のコンテンツは、無許可の場所への送信が阻止されます。これは、その個人情報を送信しようとしているのが、ユーザのコンピュータを使用するユーザ、他人、またはトロイの木馬かどうかにかかわらずすべて阻止されます。

ID ロック機能は、ZoneAlarm Pro および ZoneAlarm Security Suite で使用できます。

個人情報はどのように保護されるか

Zone Labs セキュリティ ソフトウェア は、電子メールでも Web 上でも、個人情報が許可なく送信されることを阻止します。

電子メール伝送

ユーザのコンピュータを使用するユーザまたは他人が、myVAULT のデータをメール メッセージで送信しようとすると、Zone Labs セキュリティ ソフトウェア はその情報の送信を許可するかどうかを問い合わせる警告を表示します。この送信先へのその情報の送信を常に許可、または常にブロックするには、[はい] または [いいえ] をクリックする前に、**[記憶しますか…]** チェックボックスをオンにし、この送信先をトラスト サイト リストに追加して、対応するアクセス許可が自動的に設定されるようにします。たとえば、[記憶しますか…] チェックボックスをオンにし、**[はい]** をクリックすると、その送信先はトラスト サイト リストに追加され、アクセス許可には **[許可]** が設定されます。逆に、**[いいえ]** をクリックすると、アクセス許可には **[ブロック]** が設定されます。

メール伝送の結果表示された ID ロック警告に応答する際に、[記憶する…] チェックボックスをオンにすると、そのメールの受信者ではなく、受信者のメール サーバのドメインがトラスト サイト リストに追加されます。たとえば、john@example.com 宛の myVAULT データの送信を許可し、それを記憶した場合、次に myVAULT データを送信する際には、example.com のメール サーバ上の任意の宛先への送信が許可され、警告は表示されません。

Web 伝送

myVAULT データを Web 上で送信するとき、Zone Labs セキュリティ ソフトウェア はトラスト サイト リスト内のドメインに対するアクセス許可に従って、その伝送を許可、またはブロックします。myVAULT コンテンツの

メール伝送の場合と同様に、特定の Web サイトに対する ID ロック警告への応答を記憶することを選択すると、その Web サイトは自動的にトラスト サイト リストに追加され、対応するアクセス許可が設定されます。

IM 伝送

myVAULT データをインスタント メッセージングの会話で送信する際、Zone Labs セキュリティ ソフトウェア はその情報が受信されることを阻止します。

図 10-1 に、myVAULT に保存されている情報が送信されるインスタント メッセージングの会話を示します。myVAULT に保存されている項目の説明（この例では、「My Visa Card」）が、角括弧で囲まれて表示されます。

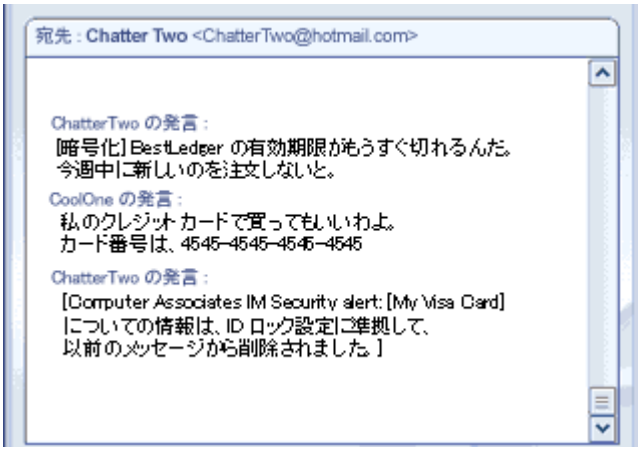


図 10-1： myVAULT コンテンツの伝送

図 10-2 に、送信された情報がどのように受信者に表示されるかを示します。保護される情報はアスタリスクに置き換えられるので、読み取れません。

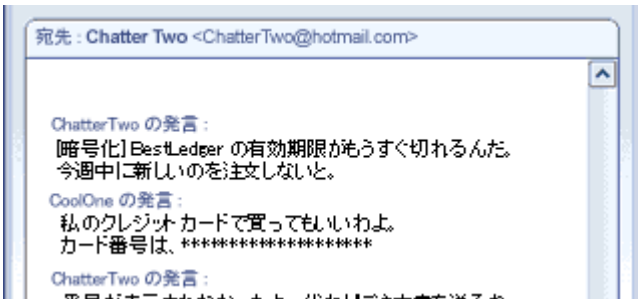


図 10-2： myVAULT コンテンツの受信

ID ロック保護レベルの設定

デフォルトでは、ID ロックは無効になっています。ID ロックを有効にすることで、myVAULT に入力したデータを保護することができます。

1. ［ID ロック］|［メイン］を選択します。
2. ［ID ロック］エリアで、適切な保護レベルを指定します。

高	myVAULT のコンテンツが無許可の場所に送信されるのを防ぎます。Zone Labs セキュリティ ソフトウェア は、データの伝送を警告を表示せずにブロックします。共有コンピュータを使用している場合は、セキュリティを最大にするために、この設定を推奨します。
中	ID 情報がトラスト サイト リストに登録されていない場所へ送信されそうになると警告します。これは、デフォルトの設定です。
オフ	ID 保護が無効です。myVAULT のコンテンツは、送信先がトラスト サイト リストに登録されているかどうかにかかわらず、どこにでも送信可能です。

ID ロック ステータスのモニタリング

Zone Labs セキュリティ ソフトウェアの［ステータス］エリアには、myVAULT に保存されている項目の数と、情報が保護された回数が表示されます。

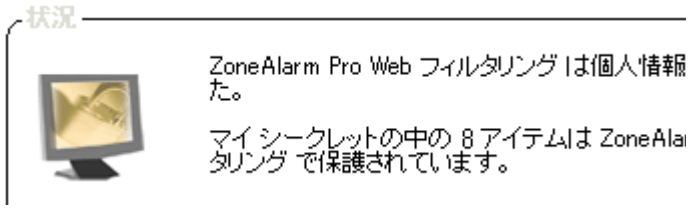


図 10-3: ID ロック ステータス エリア

myVAULT について

myVAULT 機能は、ハッカーおよび個人情報盗難から守る重要な個人データを入力するために、安全なエリアを提供します。Zone Labs セキュリティ ソフトウェア は、myVAULT に保存されているデータが送信されようとしていることを検出すると、その情報をブロックするか、許可するかを判断します。デフォルトでは Zone Labs セキュリティ ソフトウェア は、myVAULT データを入力時に暗号化し、データそのものではなく、そのデータのハッシュ値のみ保存します。データを暗号化すると、そのハッシュ値を使ってデータを読み出すことはできないので、情報は安全に保存されます。

myVAULT へのデータの追加

myVAULT にはどのような種類の情報でも保存できますが、クレジット カード番号や ID 情報など、安全に保存したい情報のみ保存しておくことをお勧めします。myVAULT に自分の住所から州（たとえば、カリフォルニア）などの情報のみ別にして保存すると、オンライン Web フォームに「カリフォルニア」と入力するたびに、Zone Labs セキュリティ ソフトウェア によってそのデータの伝送がブロックされます。

myVAULT にどのような情報を入力するべきかよくわからない場合には、事前に定義されているカテゴリを参考にしてください。カテゴリのリストにアクセスするには、**[ID ロック]**|**[myVAULT]** を選択し、次に **[追加]** をクリックします。

myVAULT に情報を追加するには、次のようにします。

1. **[ID ロック]**|**[myVAULT]** を選択します。
2. **[追加]** をクリックします。

   [myVAULT に情報を追加] ダイアログ ボックスが表示されます。

   Zone Labs セキュリティ ソフトウェア は最大限の保護を提供するため、デフォルトで myVAULT データを暗号化します。入力するデータを暗号化したくない場合には、**[非可逆性暗号化の使用 ...]** チェックボックスをオフにします。

3. 追加する項目の説明を入力します。

Zone Labs セキュリティ ソフトウェア は、この項目の説明を ID ロック警告に表示します。入力する説明は、追加する項目の値とは別にするように注意してください。保護する情報および説明に、そのデータの一部またはすべてが含まれている場合、複数の ID ロック警告が表示されることがあります。

4. ドロップダウン リストからカテゴリを選択します。

アクセス PIN	個人のアクセス コードなどの ID 番号です。最大の長さは 6 文字です。セキュリティを強化するため、アクセス PIN は常に暗号化されます。
アドレス	最大の長さは 30 文字です。
アメリカン・エキスプレス カード	Zone Labs セキュリティ ソフトウェア ではセキュリティを強化するため、アメリカン・エキスプレス カード番号の最後の 5 桁は記録されません。
銀行口座	最大の長さは 14 文字です。
クレジット カード	Zone Labs セキュリティ ソフトウェア ではセキュリティを強化するため、クレジット カード番号の最後の 4 桁は記録されません。
運転免許証	最大の長さは 15 文字です。
eBay パスワード	eBay Web サイトへのアクセスに使用するパスワードです。eBay パスワードは、eBay にしか送信できません。最大の長さは 20 文字です。
電子メール アドレス	最大の長さは 60 文字です。
国際租税 ID	最大の長さは 15 文字です。
母の旧姓	最大の長さは 30 文字です。
名前	最大の長さは 30 文字です。
パスポート番号	米国のパスポート番号などの国際 ID 番号です。最大の長さは 30 文字です。
パスワード	保護するパスワードを入力します。最大の長さは 20 文字です。
電話	括弧やダッシュなどの区切り文字は入力できません。最大の長さは 13 文字です。
米国社会保障番号	9 桁必要です。
その他	このフィールドを使用して、事前に設定されたカテゴリに該当しない項目や、対応するカテゴリの文字数制限を越える項目を入力します。最大の長さは 30 文字です。

5. 保護するデータを入力します。

デフォルトで、データの暗号化は、有効になっています。データを暗号化したくない場合は、[非可逆性暗号化の使用 ...] チェックボックスをオフにします。データの機密性を考慮して、PIN 番号、パスワード、米国社会保障番号の最後の 4 桁、およびクレジット カード番号の最後の 4 桁は、暗号化を選択したかどうかに関わらず、常にアスタリスクで表示されます。

デフォルトで表示される暗号化の確認を表示しないようにするには、[ID ロック]|[myVAULT] を選択し、[オプション] をクリックします。**[暗号化の確認の表示]** チェックボックスをオフにします。

データを入力した箇所にはアスタリスクが表示され、暗号化されたデータが myVAULT に保存されます。

6. Web、メール、およびインスタント メッセンジャ（ZoneAlarm Security Suite のみ）を使用する際に情報を保護するかどうかを指定します。
7. [OK] をクリックし、変更を保存します。

myVAULT コンテンツの編集と削除

[myVAULT] タブでは、暗号化の設定の変更、myVAULT コンテンツの削除、および暗号化されていないデータの編集を行うことができます。暗号化されたデータはアスタリスクで表示されるので、読み取れないため、編集できません。

myVAULT コンテンツを編集するには、次のようにします。

1. [ID ロック]|[myVAULT] を選択します。
2. 編集する項目を選択し、[**編集**] をクリックします。

   [myVAULT からの情報を編集] ダイアログが表示されます。
3. 必要に応じてデータを変更し、[OK] をクリックして変更を保存します。

myVAULT コンテンツを削除するには、次のようにします。

削除する項目を選択し、[削除] **をクリックします。**

myVAULT 内の最後の項目を削除すると、ID ロック保護レベルは、オフに設定されます。後で myVAULT に項目を追加すると、保護レベルはデフォルトの [中] に再設定されます。

トラスト サイト リストの使用

myVAULT 機能は、ハッカーや個人情報盗難により使用される可能性のある重要な個人データを入力するために、安全なエリアを提供します。Zone Labs セキュリティ ソフトウェア は、myVAULT に保存されているデータが送信されようとしていることを検出すると、その送信先が信頼できるかどうかを確認することにより、その情報をブロックするか、許可するかを判断します。

トラスト サイト リストには、2 種類のサイトが表示されます。Security Alliance サイトとカスタム サイトです。Security Alliance サイトは、認証によって Zone Labs, LLC. が詐欺ではないことを確認した Web サイトです。カスタム サイトは、ユーザがリストに追加するサイトです。

トラスト サイト リストの表示

個人情報を信頼して任せられるサイトをリストするのみでなく、既知のスパム サイトやチャット サイトなど、*信頼しない*ことを明示するリストにサイトを追加して、それらのサイトへの情報の送信を阻止することができます。

トラスト サイト リストでは、*平文*でパスワードを送信することを許可するサイトを指定することもできます。平文パスワードは暗号化されていないので、伝送中に傍受されると、他人に簡単に読み取られます。

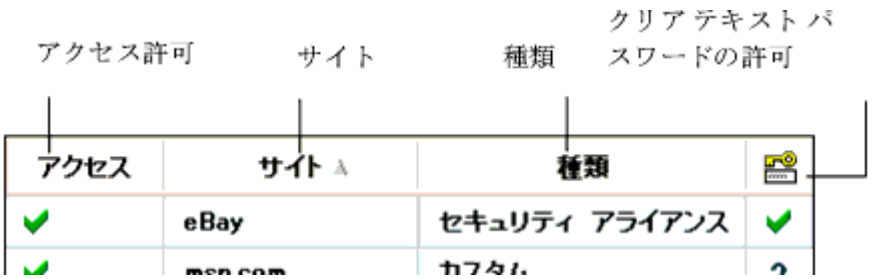


図 10-4: トラスト サイト リスト

アクセス許可

リストされている送信先に myVAULT コンテンツを送信することを、Zone Labs セキュリティ ソフトウェア が許可するか、ブロックするか、またはその前にユーザに警告するかを指定します。サイトに対するアクセス許可

を変更するには、サイトの隣の［アクセス］カラムをクリックし、**［許可］**、**［ブロック］**、または **［問い合わせ］** を選択します。

サイト
サイトのドメインを表示します。

種類
そのサイトが Security Alliance Partner かカスタム サイトかを示します。

平文パスワード
リストされている送信先にパスワードを平文で送信することを、Zone Labs セキュリティ ソフトウェアが許可するか、ブロックするか、またはその前にユーザに警告するかを示します。サイトに対するアクセス許可を変更するには、サイトの隣の［平文パスワード］カラムをクリックし、**［許可］**、**［ブロック］**、または **［問い合わせ］** を選択します。

サイト項目の詳細
サイト名と種類の他に、［項目の詳細］ボックスにサイトの IP アドレスと、そのサイトに最後にアクセスした日付と時間が表示されます。

トラスト サイト リストへの追加

トラスト サイト リストには、2 種類のサイトが表示されます。カスタム サイトと Security Alliance サイトです。カスタム サイトは、ユーザがリストに追加するサイトです。Security Alliance Partner サイトは、Zone Labs が正当なサイトであることを確認したサイトで、自動的に追加されます。

カスタム サイトはドメイン レベルで信頼されるので、ユーザは信頼するサブドメインをそれぞれ別個に追加する必要があります。たとえば、www.msn.com と shopping.msn.com は、別々に追加する必要があります。Security Alliance サイトは、すべてのサブドメインを明示的に信頼するので、信頼するサブドメインごとにエントリを作成する必要はありません。

サイトをトラスト サイト リストに追加するには、次のようにします。

1. **［ID ロック］**|**［信頼するサイト］** を選択し、**［追加］** をクリックします。

   ［信頼するサイトを追加］ダイアログが表示されます。

2. サイトの URL（http://www は省略）を入力し、**[OK]** をクリックします。

   [OK] をクリックすると、Zone Labs セキュリティ ソフトウェア がサイト アドレスを確認し、IP アドレスを記録します。この処理には数秒かかります。

3. 必要に応じて、サイトのアクセス許可を変更します。

   デフォルトでは、カスタム サイトのアクセス許可および平文パスワード許可は、[問い合わせ] に設定されます。

信頼するサイトの編集と削除

[信頼するサイト] タブでは、サイトに対するアクセス許可の変更、およびカスタム サイトの編集や削除を行うことができます。Security Alliance Partner サイトの許可を変更することはできますが、サイトのエントリの編集や削除を行うことはできません。

カスタム サイトを編集するには、次のようにします。

1. 編集するサイトをダブルクリックします。

   [信頼するサイトを編集] ダイアログが表示されます。

2. 必要に応じてサイトを編集してから、[OK] をクリックして変更を保存します。

カスタム サイトを削除するには、次のようにします。

- 削除するサイトを右クリックし、[削除] をクリックします。

第 11 章

ペアレント コントロール

11

ペアレント コントロールは、暴力、ポルノ、その他の望ましくないコンテンツを含む Web サイトから家族を保護します。ブロックする Web サイトのカテゴリを選択し、スマート フィルタリングを使用して、格付けされていないサイトの分類とフィルタリングを即座に行うことができます。

ペアレント コントロール機能は、ZoneAlarm Security Suite でのみ使用できます。

トピック：

■ 198 ページの「ペアレント コントロールの概念」

■ 199 ページの「ペアレント コントロールとスマート フィルタリングの有効化」

■ 201 ページの「ブロックするコンテンツ カテゴリの選択」

ペアレント コントロールの概念

ご使用のブラウザで Web サイトなどの Web ベースのコンテンツを指定すると、ZoneAlarm Security Suite が ***Blue Coat***(TM) ペアレント コントロール サーバに接続し、そのサイトまたはコンテンツがどのようにカテゴリ化されているかを確認します。ブラウザがアクセスを試みているサイトが、Blue Coat(TM) によってブロック対象のカテゴリに指定されていると、そのサイトへのアクセスは拒否されます。この処理には通常 1 秒もかかりません。ペアレント コントロール違反のページが表示され、ブロックされた理由が示されます。サイトのカテゴリ分類に同意しない場合は、サイトがブロックされると表示されるフィルタリング違反ページのリンクをクリックして、サイトの再評価をリクエストできます。

ペアレント コントロール機能は、ZoneAlarm Security Suite でのみ使用できます。

ペアレント コントロールとスマート フィルタリングの有効化

ペアレント コントロールを有効にすると、ヌード、ポルノ、違法薬品に関する情報、人種差別主義のテキストや画像、その他子供達に見せたくないコンテンツを含んでいると Blue Coat によって判断される Web サイトは直ちにブロックされます。スマート フィルタリングを有効にすると、新しいサイトとレーティングされていないサイトの分類とフィルタリングが即座に実行され、保護が強化されます。

子供達によるペアレント コントロール設定の変更を防止するには、Zone Labs セキュリティ ソフトウェアのパスワードを設定します。22 ページの「パスワードの設定」を参照してください。

ペアレント コントロール機能は、ZoneAlarm Security Suite でのみ使用できます。

ペアレント コントロールの有効化と無効化

ペアレント コントロールにより、カテゴリ一覧でブロックするように指定したサイトがブロックされます。ペアレント コントロールが無効の場合、カテゴリとスマート フィルタリングの設定は無視されます。

ペアレント コントロールを有効または無効にするには：

1. ［プログラム コントロール］|［メイン］を選択します。
2. ［ペアレント コントロール］部分で［オン］または［オフ］を選択します。

スマート フィルタリングの有効化と無効化

スマート フィルタリング（Dynamic Real-Time Rating）により、新しいサイトでも、カテゴリに分類されていないサイトでも、望ましくないサイトはすべてブロックできます。この機能が有効になっていて、お使いのコンピュータがカテゴリ化されていないコンテンツへのアクセスを試行すると、Blue Coat(TM) が即座にその Web サイトのコンテンツを分析し、該当するカテゴリに割り当てます。その後、ユーザのペアレント コントロール設定に応じて、そのサイトがブロックまたは許可されます。この処理には通常 2 秒から 4 秒ほどかかります。

スマート フィルタリングを有効または無効にするには：

1. ［プログラム コントロール］|［メイン］を選択します。
2. ［スマート フィルタリング］部分で［オン］または［オフ］を選択します。

   このオプションにアクセスするには、ペアレント コントロールを有効にする必要があります。

タイムアウト オプションの設定

タイムアウト オプションにより、Zone Labs セキュリティ ソフトウェアが Web サイトのレーティングを入手する際の試行時間と入手できない場合の処置を指定します。

タイムアウト オプションを設定するには：

1. ［ペアレント コントロール］の［メイン］を選択し、［詳細設定］をクリックします。

   ［ペアレント コントロール オプション］ダイアログが表示されます。

2. タイムアウトの設定を指定します。

ペアレント コントロール タイムアウト（秒）	スマート フィルタリングが無効の場合に、Zone Labs セキュリティ ソフトウェア がレーティングの入手を試行する秒数。
DRTR が有効な場合のタイムアウト（秒）	スマート フィルタリングが有効の場合に、Zone Labs セキュリティ ソフトウェア がレーティングの入手を試行する秒数。
評価が利用可能でない場合	Zone Labs セキュリティ ソフトウェア がレーティングの提供されていないサイトを許可するか、ブロックするかを指定します。

3. ［OK］をクリックします。

［評価が利用可能でない場合］ にサイトを許可するよう設定した場合、タイムアウト オプションの秒数を少なく指定すると、望ましくないサイトが許可される場合があります。タイムアウト オプションのデフォルト設定を維持するようお勧めします。

ブロックするコンテンツ カテゴリの選択

ペアレント コントロール機能は、ZoneAlarm Security Suite でのみ使用できます。

ペアレント コントロールは Web コンテンツをフィルタリングするために多数のカテゴリを提供します。表 11-1 に、各カテゴリの説明とデフォルト設定を示します。

カテゴリの設定を変更するには：

1. ［ペアレント コントロール］|［カテゴリ］を選択します。
2. ［ブロックするサイト カテゴリ］カラムで、該当するカテゴリの隣のチェックボックスをオンまたはオフにします。

   赤いチェックマークは、そのカテゴリに属するコンテンツがブロックされることを意味しています。チェックボックスに何も印が付いていない場合は、そのカテゴリに属するコンテンツが許可されることを意味しています。

すべてのサイト カテゴリをブロックする場合は、［すべてを選択］をクリックします。すべてのサイト カテゴリを許可する場合は、［すべてをクリア］をクリックします。デフォルトの設定に戻すには、［デフォルトに戻す］リンクをクリックします。

カテゴリ	定義	デフォルト設定
妊娠中絶	妊娠中絶に関する情報、賛否両論を含む意見を提供するサイト、中絶手術の処置方法の説明および中絶を受けるに当たっての支援または中絶を回避するための支援を提供するサイト、中絶が身体、精神、道徳、感情面でもたらす影響に関する情報を提供するサイト。	許可
成人：性的な服装 / 水着	下着、水着、その他性的な服装を身に付けたモデルの画像を提供するサイト。他に提供する製品のサブセクションとして下着を販売するサイトは含まれません。	許可
成人：ヌード	人間の体のヌードおよびセミヌードの写真または描画を含むサイト。これら画像は必ずしも性的な意図のものとは限らず、芸術的なヌードの絵画や写真を提供するサイトも含まれます。また、ヌードの写真を掲載するヌーディスト サイトやナチュラリスト サイトも含まれます。	ブロック
成人：ポルノ	性的または猥褻な意図の性的に露骨なデータを含むサイト。	ブロック

表 11-1: ペアレント コントロールのカテゴリ

カテゴリ	定義	デフォルト設定
成人：性教育	生殖、性的発育、性病、避妊、安全な性行為、性行動、性的指向についての情報を提供するサイト。性行為を改善するための提案やヒントを提供するサイトは含まれません。	許可
アルコール / タバコ	アルコール類 / タバコ製品の促進および販売を行うサイト、および製造方法を提供するサイト。また、アルコール / タバコ類の消費を賞賛、勧誘、奨励するサイトも含まれることがあります。	ブロック
チャット ルーム / インスタント メッセンジャ	チャットとインスタント メッセージ機能を提供するサイト。	許可
犯罪技術 / 違法技術 / 不正行為	サービスの盗難、法律の回避、詐欺、違法行為、窃盗技術、盗作などの違法行為を支持、あるいは、その実行にあたってのアドバイスを提供するサイト。犯罪、非倫理的行為、不正行為、訴訟の回避に関する手順説明を提供するサイト、またはそれらを促進するサイト。	ブロック
カルト / オカルト	3 つ以上の権威筋により「カルト」と特定されている有名で組織化された現代宗教グループ。方法、指示の手段、またはその他のリソースを促進または提供して、魔法、呪文、魔力、超自然的な存在を用いて現実の出来事に影響を及ぼすサイト。	許可
デート / 出会い	対人関係を促進するサイト。同性愛関連のサイトは含まれません。	許可
麻薬：違法薬品	麻薬、薬品、麻薬原料植物、化学物質ならびに関連用品の促進、提供、販売、供給、奨励、あるいはのそれらの違法使用、栽培、製造、配布を擁護するサイト。	ブロック
電子メール	Web ベースの電子メール サービスを提供するサイト。	許可
フリーウェア / ソフトウェアのダウンロード	無料のソフトウェアまたは製品を一般ダウンロードまたは試用目的で促進または提供するサイト。	許可
ギャンブル	ユーザがオンラインで賭けをしたり、賭博行為（宝くじも含む）に参加できるサイト。賭けに関する情報や援助、アドバイスを得ることのできるサイト。ギャンブル参加の手順、援助、トレーニングを入手できるサイト。ギャンブル関連製品やマシンを販売するサイトは含まれません。	ブロック
同性愛	同性愛者のライフスタイルに関する情報を提供するサイト、または同性愛者のニーズに対応するサイト。性的な意図を持ったサイトは含まれません。	許可

表 11-1: ペアレント コントロールのカテゴリ

カテゴリ	定義	デフォルト設定
グラマー / ライフスタイル	外見、容姿の面で魅力的な身体、美容、スタイルを向上するための方法に焦点をあてたサイトまたは関連情報やニュースを提供するサイト。	許可
政府：軍事	軍事機関の情報促進および提供を行うサイト。	許可
ハッキング / プロキシ回避システム	通信装置 / ソフトウェアの不正アクセスや不正利用に関する情報を提供するサイト、または、プロキシ サーバ機能の回避方法またはプロキシ サーバをバイパスして URL にアクセスする方法に関する情報を提供するサイト。	ブロック
ユーモア / ジョーク	コメディ、ジョークなどを主要題材とするサイト。成人向けのジョークを掲載するサイトは含まれません。	許可
インターネット オークション	個人間の品目の販売と購入をサポートするサイト。	許可
MP3/ ストリーミング	MP3、MPG、MOV などの音楽ファイルやメディア ファイルのユーザによるダウンロードをサポートまたは許可するサイト。ストリーミング メディア（ラジオ、映画、TV）を提供するサイトも含まれます。	許可
ニュース グループ	Usenet ニュース グループなどのサイトへのアクセスを提供するサイト。	許可
ニュースとメディア	毎日の出来事や最新ニュースに関する情報またはコメントを主に提供するサイト。主要なニュース サイト内の天気予報、論説、三面記事なども対象となります。	許可
オンライン ゲーム	ゲームのプレイまたはダウンロード、ビデオ ゲーム、コンピュータ ゲーム、電子ゲームに関する情報とサポート、ゲームのヒントとアドバイス、チート コードの入手方法、ゲーム雑誌、オンライン ゲームに関する情報とサポートを提供するサイト、ならびに、スイープステークや懸賞も含めオンライン ゲームをサポートまたは主催するサイト。	許可
Pay to Surf Sites	特定のリンクや場所をクリックすると、ユーザに報酬を支払うサイト。	ブロック
政治 / 活動家 / 擁護団体	特定の政党やグループが提供するサイト、またはそれらの情報を提供するサイト。公共政策、大衆の意見、社会慣行、経済活動、経済関係における変化や改革を促進する組織が提供するサイト、またはそれら組織をサポートするサイト。選挙戦や法律のために民間組織がスポンサーするサイトは含まれません。	許可

表 11-1: ペアレント コントロールのカテゴリ

カテゴリ	定義	デフォルト設定
宗教	仏教、バハーイ教、キリスト教、クリスチャン サイエンス、ヒンズー教、イスラム教、ユダヤ教、モルモン教、神道、シーク教、無神教、その他、伝統宗教または新興宗教、半宗教、ならびに、教会、ユダヤ教会、その他の崇拝場、魔術やウィッチクラフトなど「代替」宗教も含めるあらゆる信仰と宗教を促進し、関連情報を提供するサイト。	許可
検索エンジン / ポータルサイト	Web、インデックス、ディレクトリの検索をサポートするサイト。	許可
ショッピング	個人の欲求とニーズを満足させるための製品とサービスの入手手段を提供するサイト。主に業界向け、企業向けの製品とサービスは含まれません。	許可
スポーツ / 娯楽 / 趣味	観戦用のスポーツを促進し、関連する情報を提供するサイト。	許可
暴力 / 憎悪 / 人種差別	武器、爆破物、悪戯、その他の暴力を使って対人、対物の被害を生じるための方法を提唱または提供するサイト。人種、宗教、性別、国籍、民族的背景、その他非自発的な性質を根拠にした個人またはグループに対する敵愾心や攻撃心を擁護するサイト。これら性質を基に他人を侮辱し、これら性質を基に不平等を正当化するサイト。科学的方法またはその他一般的に認められている方法を使って、前述の攻撃心、敵愾心、誹毀を正当化することを表明するサイト。	ブロック
武器	銃、ナイフ、格闘技用の道具などの武器を販売、評価、説明するサイト、または、武器の使用、付属品、その他の改造品に関する情報を提供するサイト。	ブロック
Web 通信 / 掲示板	以下の媒体を使用する Web ベースの通信を許可または提供するサイト。メール（Web ベース）、チャット、インスタント メッセージ、掲示板、その他。	許可
Web ホスティング / パーソナル Web ページ	Web コミュニティまたはホスティング サービスの最上位ドメイン ページを提供する組織のサイト。Web チャット サービスをホストするサイト、オン IRC チャット ルーム、HTTP によるチャット サイト、IRC 専用のホーム ページ、およびフォーラムまたはディスカッション グループを提供するサイト。コンピュータ プログラミング技術（ハッキング）を用いて違法または未承認の行為を実践する手段を促進または提供するサイト。 また、GEO Cities などのあらゆる種類のコンテンツを含むサイト。	許可

表 11-1: ペアレント コントロールのカテゴリ

ZoneAlarm Security Suite を使用している場合、新しいカテゴリのブロックを選択する際には、新たにブロックされたサイトのページがブラウザ キャッシュに保管されていることがあるため、ブラウザ キャッシュのクリーニングを行ってそれらページを削除することをお勧めします。それらページをブロックしても、ブラウザ キャッシュに保管されたままになっていると、コンピュータを使用するユーザは誰でもそのコンテンツにアクセスできます。

第 12 章

インスタント メッセージングのセキュリティ

12

Zone Labs IM セキュリティは、インスタント メッセージングの脅威に対応するための主要な保護機能です。IM セキュリティのデフォルトのセキュリティ レベルは、ハッカーやスパムから直ちに保護し、インスタント メッセージング クライアントに送信される不適切な Web コンテンツを防止するためのコントロールを提供します。

IM セキュリティ機能は、ZoneAlarm Security Suite でのみ使用できます。

トピック：

- 208 ページの「IM セキュリティの概要」
- 215 ページの「IM セキュリティ オプションの設定」

IM セキュリティの概要

Zone Labs セキュリティ ソフトウェア は、MSN Messenger、Yahoo! メッセンジャ、AOL インスタント メッセンジャ、ICQ など、ほとんどの一般的なインスタント メッセージング サービスに対して包括的なインスタント メッセージング (IM) セキュリティを提供します。また IM セキュリティは、これらのサービス上で実行される Trillian などのサードパーティ製プログラムもサポートしています。IM セキュリティは、インスタント メッセージングの会話をプライベートに保ち、無防備な IM 接続を悪用する IM スパマー、個人情報盗難、ハッカー、略奪者などからコンピュータを保護します。

IM セキュリティは、次の機能を提供します。

- **アクセス コントロール** — コンピュータを使用してアクセス可能な IM サービスへのアクセスをコントロールします。
- **迷惑メール防止** — 連絡先リストにない相手から送信されたメッセージをブロックします。
- **機能コントロール** — コンピュータ上で許可される IM 機能を判別します。
- **外部からの脅威保護** — 無効なメッセージ、危険なスクリプト、実行可能 URL などをフィルタリングすることで、コンピュータを攻撃から保護します。
- **メッセージの暗号化** — IM トラフィックが阻止されたり他者によって読み取られたりすることを防止します。

上記で説明した保護機能は、1 対 1 の会話に対してのみ適用されます。Zone Labs セキュリティ ソフトウェア は、参加者が 2 人以上の会話は保護しません（たとえば、チャット ルームの会話など）。

アクセス

アクセス コントロールを使用すると、特定のインスタント メッセージング サービスのトラフィックを許可またはブロックできます。

特定のサービスの IM トラフィックをブロックまたは許可するには：

1. ［**セキュリティ**］|［**設定**］を選択します。
2. ［**アクセス**］カラムで、トラフィックをブロックまたは許可したいインスタント メッセージングの横をクリックします。
3. ［**許可**］または［**ブロック**］を選択します。

迷惑メールの防止

迷惑メールの防止は、コンタクト リストにない送信者による意図しない通信をフィルタによって除外します。デフォルトでは、IM セキュリティ レベルが「高」に設定されている場合のみ、迷惑メール防止が有効になっています。ただし、保護レベルに関係なく、特定のサービスに対して迷惑メール防止が有効になるように設定をカスタマイズできます。

Zone Labs セキュリティ ソフトウェア が外部からのメッセージをブロックしたときに確認メッセージは表示されませんが、ログを参照すると送信者の識別情報を判別できます。今後、その送信者からメッセージを受信したい場合は、インスタント メッセージング プログラムのコンタクト リストに送信者の ID を追加してください。ブロックされたメッセージは、[コンタクト リストにない人からのメッセージがブロックされました] というメッセージ付きでログ ビューアの [種類] カラムに表示されます。

特定のサービスについて迷惑メールの防止を有効または無効にするには：

1. **[セキュリティ]**|**[設定]** を選択します。
2. カスタマイズするインスタント メッセージ サービスを特定し、次に **[迷惑メールの防止]** カラムをクリックします。
3. [オン] または [オフ] を選択します。

機能コントロール

機能コントロール設定を使用すると、インスタント メッセージング セッション中に受信できるメディアの種類を制限できます。さまざまな形式で不適切なコンテンツを送信することができるため、Zone Labs セキュリティ ソフトウェア では、両親が児童を保護するために、オーディオ、ビデオ、

音声伝送など、特定の種類のメディアをインスタント メッセージング セッションでブロックすることができます。

メッセージがブロックされると、図 12-1 に示すように送信者に通知されます。

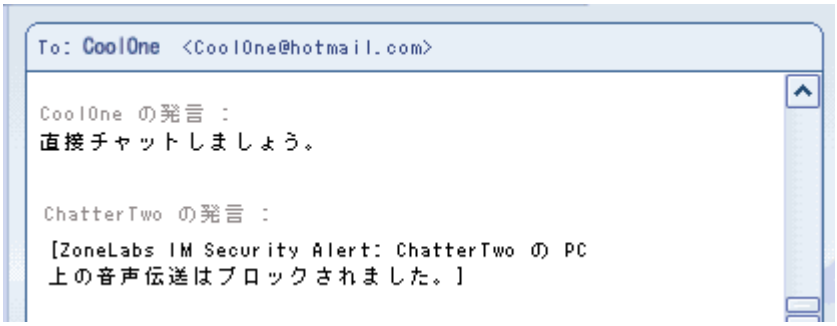


図 12-1: ブロックされた音声伝送の送信

受信者にも、図 12-2 に示すように通知されます。

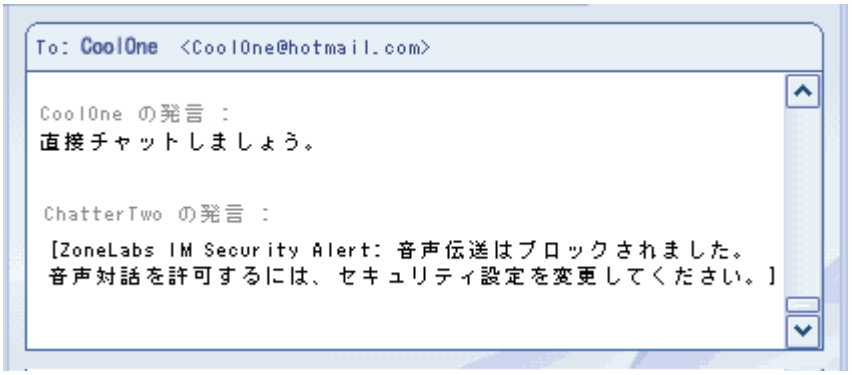


図 12-2: 外部からの音声伝送のブロック

機能コントロールをカスタマイズするには：

1. **[セキュリティ]**|**[設定]** を選択します。
2. カスタマイズするインスタント メッセージ サービスを特定し、次に **[機能コントロール]** カラムをクリックします。
3. **[オーディオ]**、**[ビデオ]**、または **[ファイル]** を選択し、次に **[許可]** または **[ブロック]** を選択します。

外部からの保護

外部からの保護設定を使用すると、どのインスタント メッセージング サービスで JavaScript などのアクティブ リンクや書式タグの送信を許可するかを指定できます。アクティブ リンクや書式タグには、メッセージ中のリ

ンクをクリックするとコンピュータを攻撃するようなウイルスを含めることができます。

インバウンド「タグ」の設定により、スクリプトなどの有害な可能性のあるコードを含む拡張書式を削除できます。また「タグ」設定では、太字、下線付き、イタリックなどの無害な書式も削除できます。

「アクティブ」設定では、クリックによってコードを実行したり、危険なファイルをコンピュータにダウンロードしたりするリンクをブロックできます。

アクティブ リンクを接続に送信すると、図 12-3 のように表示されます。

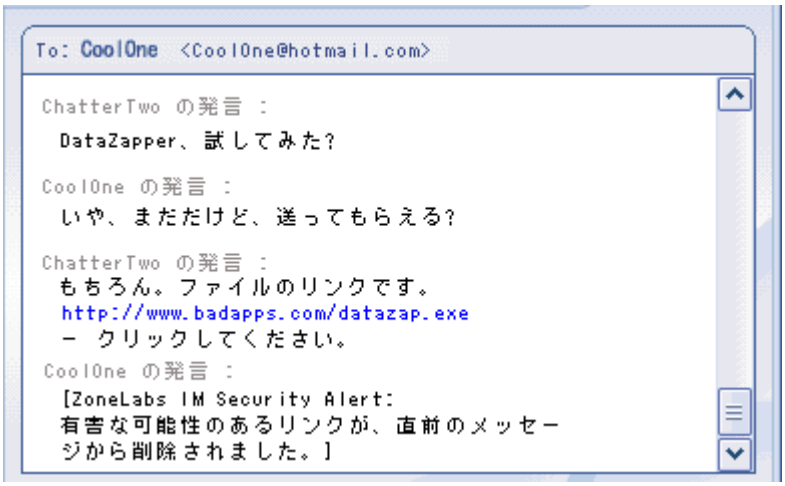


図 12-3: 実行可能 URL を接続に送信

アクティブ リンクがメッセージからフィルタリングされると、受信者には図 12-4 のような通知が表示されます。

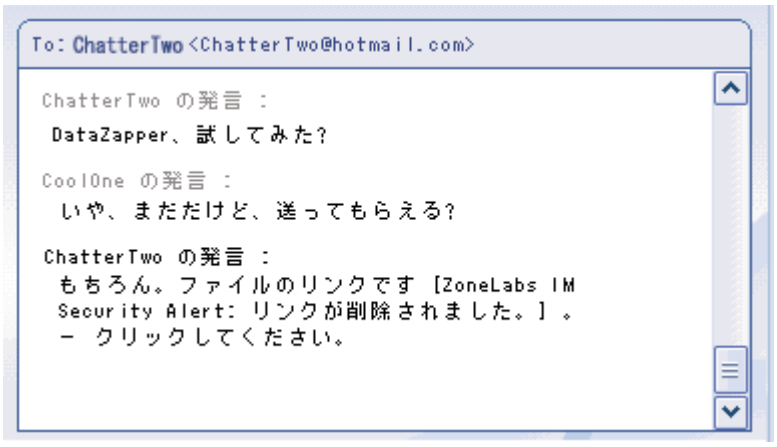


図 12-4: 有害な可能性のあるリンクが削除されました

外部からの保護設定をカスタマイズするには：

1. ［**セキュリティ**］|［**設定**］を選択します。
2. カスタマイズするインスタント メッセージ サービスを特定し、次に［**インバウンド**］カラムをクリックします。
3. ［タグ］または［アクティブ］の下をクリックし、次に［許可］または［ブロック］を選択します。

インスタント メッセージング トラフィックの暗号化

暗号化を使用することで、インスタント メッセージの会話を阻止されたり読み取られたりすることを防止できます。インスタント メッセージングの会話を暗号化するには、両方の参加者が ZoneAlarm Security Suite をインストールし、同一の IM サービスにアカウントを持っている必要があります。それぞれのコンピュータに ZoneAlarm Security Suite がインストールされていても、参加者が互いのコンタクト リストに登録されていない場合、会話は暗号化されません。

接続している IM サービスの暗号化を有効にした状態で他の ZoneAlarm Security Suite ユーザと会話を開始すると、接続しているインスタント メッセージング ID の後にかっこに囲まれた**暗号化**という言葉が表示されます。ZoneAlarm Security Suite を使用していない参加者や、暗号化を有効

にしていない参加者と会話を開始すると、接続しているインスタント メッセージング ID の後に**非暗号化**という言葉が表示されます。

図 12-5 は、暗号化された会話です。

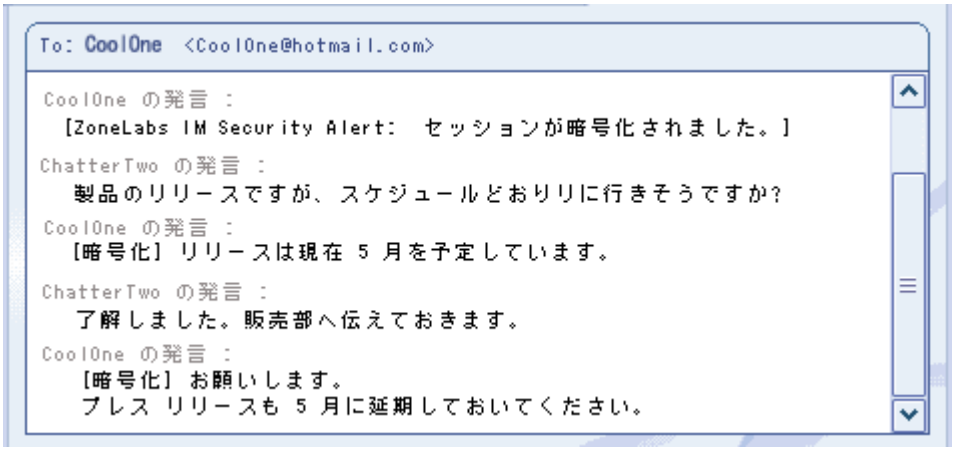


図 12-5: 暗号化された会話の例

上に示すのは会話の例ですが、こちらは非暗号化モードです。

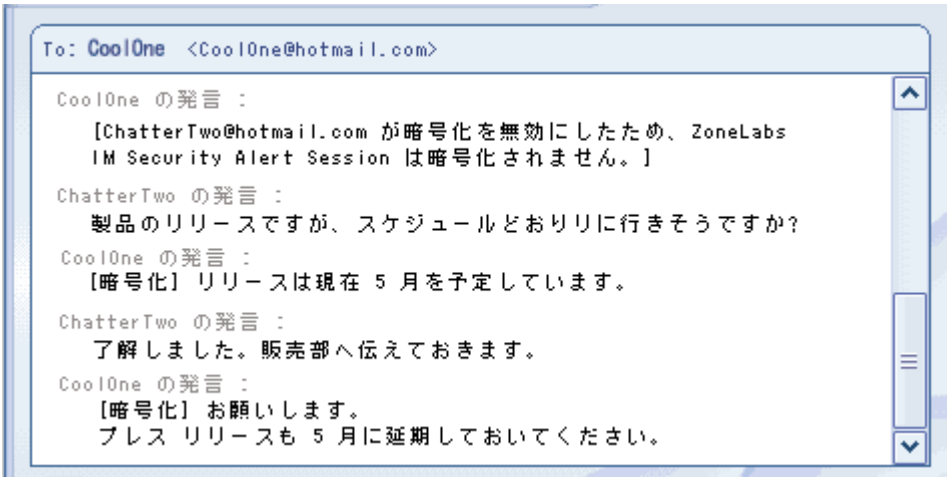


図 12-6: 非暗号化された会話の例

特定の IM サービスで暗号化を有効または無効にするには：

1. **［セキュリティ］**|**［設定］**を選択します。
2. ［暗号化］カラムで暗号化するトラフィックのサービスの横をクリックします。
3. **［許可］**または**［ブロック］**を選択します。

インスタント メッセージが暗号化される方法

ZoneAlarm Security Suite の暗号化サービスは、*OpenSSL* ライブラリに基づいています。安全なセッションでの各メッセージのテキストは、*3DES* の 168 ビット暗号によって暗号化されています。ZoneAlarm Security Suite は、最初のログイン時に各ユーザの IM アカウントに対して、自動で透過的に *自己署名証明書* を作成します。ZoneAlarm Security Suite をインストールした後で、2 人の ZoneAlarm Security Suite ユーザが初めて IM 会話を開始すると、ユーザ間で透過的に証明書が交換され、それぞれのコンピュータに保存されます。セッションの間に使用されるセッション キーは、片方の証明書の公開キーを使用して暗号化されます。

IM セキュリティ オプションの設定

Zone Labs セキュリティ ソフトウェア は、インスタント メッセージング ソフトウェアに制限を適用し、迷惑メールをフィルタによって除外し、インスタント メッセージのトラフィックを暗号化することによって、お使いのコンピュータを保護します。ID ロック機能と組み合わせることによって、Zone Labs セキュリティ ソフトウェア は、インスタント メッセージング セッション中に、許可なく個人データが送信されることを防止します。適切な保護のレベルを指定するには、あらかじめ定義されているオプションを使用するか、または手動で個々のセキュリティ設定をカスタマイズします。

- 保護レベルの設定
- IM セキュリティ保護のステータスの表示
- 保護設定のカスタマイズ
- 詳細な IM セキュリティ オプションの設定
- ログに記録された IM セキュリティ イベントの表示

保護レベルの設定

デフォルトの保護レベルである「中」は、インスタント メッセージング機能を許可するとともに、インスタント メッセージング通信の安全を保つため、セキュリティと使いやすさのバランスが取れています。

グローバルなプログラム コントロール レベルを設定するには：

1. **[IM セキュリティ]|[メイン]** を選択します。
2. **[保護レベル]** エリアで、スライダをクリックして希望の設定になるようにドラッグします。

高	インスタント メッセージング プログラムによるすべてのメディア ファイルの送信を禁止し、迷惑メッセージや実行可能 URL をフィルタで除外し、インスタント メッセージングのトラフィックを暗号化します。
「中」	これは、デフォルトの設定です。インスタント メッセージングのトラフィックを暗号化し、実行可能 URL をフィルタで除外します。
オフ	インスタント メッセージングの保護は無効です。

IM セキュリティ保護のステータスの表示

[メイン] タブでは、IM セキュリティ保護のステータスを表示できます。[保護ステータス] エリアには、インバウンド、迷惑メール防止、機能コン

トロール オプションなどのセキュリティ設定に違反したためにブロックされたメッセージの数の統計が表示されます。

プログラム履歴ログには、すべてのアクティブな IM プログラムが一覧表示され、プログラムが最後に使用された日付と時間が表示されます。

Zone Labs セキュリティ ソフトウェアを起動する前に IM プログラムを起動した場合、IM プログラムは履歴ログに表示されません。すべての IM プログラムのアクティビティを正確に反映するには、Zone Labs セキュリティ ソフトウェア を起動した後で IM プログラムを起動してください。

保護設定のカスタマイズ

保護レベルを「高」、「中」、または「オフ」に設定することで、ファイル、JavaScript、リンクなどをインスタント メッセージング プログラムがインスタント メッセージング クライアントに送信するかどうかをグローバルに指定できます。場合によっては、特定のサービスを対象として、これらグローバルな設定とは異なる設定を指定することが必要なこともあります。

保護設定をカスタマイズするには：

1. ［**IM セキュリティ**］|［**設定**］を選択します。
2. 変更するサービスを特定し、カスタマイズするコンテンツのカラムを右クリックします。

アクセス	「ブロック」に設定すると、選択されたサービスを使用しているプログラムからのインスタントメッセージング トラフィックは停止されます。
迷惑メール防止	「オン」に設定すると、コンタクト リストにない参加者から送信されたメッセージはブロックされます。
機能コントロール	「ブロック」に設定すると、音声伝送、ビデオ伝送、またはファイル伝送のブロックが許可されます。
インバウンド	外部からのメッセージに JavaScript や実行可能リンクなどの書式タグを含めることができるかどうかを指定します。
暗号化	インスタント メッセージングのトラフィックを暗号化するかどうかを指定します。

デフォルトの保護レベルである「中」に戻すには、［IM セキュリティ］|［メイン］を選択し、次に［デフォルトに戻す］をクリックします。

詳細な IM セキュリティ オプションの設定

デフォルトでは、IM 会話から有害なコンテンツがフィルタによって除外されると、Zone Labs セキュリティ ソフトウェア は警告を表示し、セッショ

ンが暗号化されているかどうかを通知します。[詳細] ダイアログを使用すると、これらおよびその他の設定を変更できます。

詳細な IM セキュリティ オプションを設定するには：

1. **[IM セキュリティ]|[設定]** を選択し、**[詳細]** をクリックします。
2. 設定を指定します。

Zone Labs の IM セキュリティで保護されていることを私の接続先に通知	Zone Labs セキュリティ ソフトウェアをインストールした後で、接続先と会話を開始すると、保護されていることが接続先に通知されます。 注意：この通知が行われるのは、インストール後の最初のセッションだけです。その後のセッションでは、接続先に通知は行われません。
各 IM セッションの暗号化状態を通知	Zone Labs セキュリティ ソフトウェアは、各 IM セッションの最初に、デフォルトの「暗号化」ラベルまたは「非暗号化」ラベルによるマークを付けます。
暗号化メッセージにラベルを付ける	**暗号化された**外部からのメッセージに、指定されたラベルを付けます。デフォルトのラベルは、「暗号化」です。
非暗号化メッセージにラベルを付ける	**非暗号化された**外部からのメッセージに、指定されたラベルを付けます。デフォルトのラベルは、「非暗号化」です。
危険なコンテンツをフィルタリングしたときに通知	Zone Labs セキュリティ ソフトウェアは、有害な可能性のあるコンテンツが IM 会話からフィルタによって除外されると、IM ウィンドウにメッセージを表示します。
IRC をブロック	コンピュータのセキュリティが低下するイベントが発生すると、この機能によって IRC チャネルとの接続を確立する試みがブロックされます。これにより、有害な接続の確立によるコンピュータの感染が防止されます。 IRC アプリケーションを使用する必要のある IRC ユーザは、このオプションを選択解除してください。
すべてのリンクをブロック	ワームを拡散するために使用される可能性のある URL をすべてフィルタで除外します。

3. **[OK]** をクリックし、変更を保存します。

ログに記録された IM セキュリティ イベントの表示

デフォルトでは、すべての IM セキュリティ イベントはログ ビューアに記録されます。Zone Labs セキュリティ ソフトウェア が迷惑メールをブロックした場合、通知は表示されませんが、ログ ビューアを使用すると、ブロックされたすべてのメッセージの詳細を表示することができます。

ログに記録された IM セキュリティ イベントを表示するには：

1. ［**警告とログ**］|［**ログ ビューア**］を選択します。
2. ［警告タイプ］ドロップ ダウン リストから［**IM セキュリティ**］を選択します。

表 12-6 は、IM セキュリティで使用可能なログ ビューアのフィールドの説明です。

フィールド	説明
レベル	セキュリティ オプションの**保護レベル**に基づいたイベントのレベル。
日付 / 時間	イベントが発生した日付と時間。
種類	イベントの簡単な説明。このフィールドには、違反が発生したセキュリティ設定によって（たとえば、迷惑メール防止、ID ロックなど）、次の説明が表示されます。 **・接続はブロックされました。** **・コンタクト リストにない人からのメッセージがブロックされました。** **・メディア伝送** **・有害な可能性のある内容が削除されました。** **・アクティブ コンテンツへのリンクが削除されました。** **・暗号化されたセッションが確立されました。** **・セッションは暗号化されません。** **・重要なデータが削除されました。**
サービス	イベントが発生したサービス。
プログラム	イベントが発生したときに接続されていたインスタント メッセージング プログラム（アプリケーション ファイルとして表示）。
ローカル ユーザ	メッセージを受信したインスタント メッセージング接続先のユーザ ID。
リモート ユーザ	イベントを発生させたインスタント メッセージング接続先のユーザ ID。

フィールド	説明
操作	取られたアクションの説明。このカラムの一般的な値は、暗号化、暗号化無効、ブロックされた音声 / ビデオ / ファイル、ブロックされたスクリプトです。

付録

警告のリファレンス

A

この章では、Zone Labs セキュリティ ソフトウェアの使用中に表示される各種警告の詳細について説明します。この章を参考に、警告の原因、意味、および対応方法を調べることができます。

トピック：

- 222 ページの「情報警告」
- 228 ページの「プログラム警告」
- 237 ページの「OSFirewall 警告」
- 239 ページの「ID ロック警告」
- 240 ページの「新しいネットワーク警告」
- 242 ページの「インスタント メッセージ警告」

情報警告

情報警告は、Zone Labs セキュリティ ソフトウェア がセキュリティ設定に合致しない接続をブロックしたことを通知するものです。ユーザはいかなる対応をもする必要ありません。

ファイアウォール警告 / 保護

ファイアウォール警告は、最も一般的な種類の情報警告です。ファイアウォール警告は、設定されたポート制限およびプロトコル制限、またはその他のファイアウォール規則に基づいて、Zone Labs セキュリティ ソフトウェアのファイアウォールが通信をブロックしたことを通知します。

警告が表示される原因

上部が赤色で表示されているファイアウォール警告は、高レベルの警告を意味します。高レベルの警告は多くの場合、ハッカーの活動が原因となっています。

上部がオレンジ色で表示されているファイアウォール警告は、中レベルの警告を意味します。中レベルの警告は、たとえば、ISP が *ping* を使用して接続状態を確認する場合などの、害のないネットワーク通信により表示される場合がほとんどです。しかし、ハッカーがコンピュータ上の保護されていないポートを見つけようとした場合にも表示されます。

対応方法

ホームまたはビジネス ネットワークを使用し、トラスト ゾーンのセキュリティが「高」に設定されている場合、NetBIOS ブロードキャストなどの標準 LAN 通信がファイアウォール警告の原因となる可能性があります。トラスト ゾーンのセキュリティを 「中」に下げます。

デフォルトでは、Zone Labs セキュリティ ソフトウェア は高レベルのファイアウォール警告のみを表示します。デフォルトを変更すると、中レベルの警告が多数表示されるようになります。警告表示の設定を「中」に設定します。

多数のファイアウォール警告が表示される場合、ホーム ネットワークまたはビジネス LAN で作業しているのであれば、通常のネットワーク通信がブロックされている可能性があります。この場合は、ネットワークをトラスト ゾーンに含めることで、警告が表示されなくなります。

警告の表示数を減らす方法

警告が繰り返される場合、信頼できる発信元が、お使いのコンピュータとの接続を繰り返し試みている可能性があります。ファイアウォール警告が頻繁に表示されるが攻撃されているとは思わない場合は、次の操作を行ないます：

- 警告を発生した発信元が信頼できるものかどうか確認します。

  繰り返し表示される警告を SmartDefense Advisor に送信して、警告の原因となっている発信元 IP アドレスを確定します。

警告の原因が信頼できる発信元である場合、トラスト ゾーンにその発信元を追加します。

- インターネット サービス プロバイダが「ハートビート」メッセージを送信してきているかを確認します。

  ISP ハートビートの管理について推奨される手順を行います。259 ページの「ISP ハートビート メッセージの許可」を参照してください。

MailSafe 警告

MailSafe 警告は、Zone Labs セキュリティ ソフトウェア が、外部からのメール メッセージに添付された危険性のあるファイルを隔離したことを通知するものです。[OK] をクリックすると、コンピュータへの受信を拒否します。

警告が表示される原因

MailSafe 警告は、インバウンドまたはアウトバウンド MailSafe 保護の設定に対する違反があった場合に表示されます。たとえば、メールに添付されたファイルの拡張子が隔離対象の拡張子の一覧（[メール保護] パネルの [添付ファイル] タブ）に含まれている場合、そのメールを開くとインバウンドの保護違反が発生します。その場合、警告なしで添付ファイルが開かれることを防ぐために Zone Labs セキュリティ ソフトウェア が拡張子を変更したことを知らせる警告が表示されます。たとえば、受信者数が多すぎるメールを送信する場合や、短時間であまりに多くのメールを送信する場合は、アウトバウンド MailSafe 保護設定に違反するため MailSafe 警告が表示されることがあります。

対応方法

MailSafe 警告への対処は、インバウンドまたはアウトバウンドのどちらの MailSafe 保護設定に違反しているかによって異なります。

インバウンド MailSafe 保護違反により警告が生成された場合は、次の操作を行います。

- 電子メール メッセージを注意深く確認します。信頼できる送信者からのメールですか？ハッカーは、知人からのメールに見せかけたメール メッセージを送信することがあるので気を付けてください。また、ワームを含むファイルを知人が間違って開いてしまった場合、その知人のメール プログラムからワームが自動的に送信されている可能性もあります。
- 添付ファイルを開く前に、電話またはメールで送信者に連絡して、メッセージが本人から送信されたものかどうかを確認してください。

- 添付ファイルが無害であることが確認できた場合にのみ、添付ファイルを開きます。隔離アイコン（標準ファイル アイコンに代わって表示されるアイコン）をクリックすると、添付ファイルが表示されます。

隔離された添付ファイルを表示する場合、Zone Labs セキュリティ ソフトウェア は添付ファイルが潜在的に危険であることを知らせる警告ダイアログボックスを表示します。

アウトバウンド MailSafe 保護違反により警告が生成された場合は、次の操作を行います。

- 警告を注意深く確認します。記載されているアクティビティは、最近自分で行った操作に該当しますか？このような操作を実際に行っていた場合は、各自のニーズに合わせてアウトバウンド MailSafe 設定を変更する必要があります。129 ページの「アウトバウンド MailSafe 保護」を参照してください。そうでない場合は、警告の原因はコンピュータ上のウイルスの可能性があります。この場合、外部へのメールを拒否し、アンチウイルス プログラムでコンピュータをスキャンしてください。
- ユーザのメール アドレスが、承認された送信者の一覧に記載されていることを確認します。**[送信者のアドレスが一覧にない場合]** オプションを選択していて、ユーザのメール アドレスが一覧に含まれていなかったり、スペルが間違っていたりする場合は、正しいメール アドレスを一覧に追加します。

警告の表示数を減らす方法

外部へのメール保護は、インターネット セキュリティ システムの重要な部分なので、有効にしておくことを推奨します。これらの誤ったメッセージが大量に表示される場合には、この機能の感度を調整、または機能をオフにすることもできます。129 ページの「アウトバウンド MailSafe 保護」を参照してください。

ブロックされたプログラム警告

ブロックされたプログラム警告は、インターネットまたはトラスト ゾーンのリソースに対するアプリケーションのアクセスが、Zone Labs セキュリティ ソフトウェア によって制限されたことを通知するものです。[OK] を

クリックすると、プログラムのアクセスを許可するのではなく、警告を見たことを確認します。

警告が表示される原因
ブロックされたプログラム警告は、アクセス許可を明示的に拒否したにもかかわらず、プログラムがインターネット ゾーンまたはトラスト ゾーンにアクセスしようとした場合に表示されます。

対応方法
ブロックされたプログラムをインターネット ゾーンまたはトラスト ゾーンにアクセスさせる必要がある場合は、[プログラム] タブを使用して、そのプログラムにアクセス許可を与えます。

警告の表示数を減らす方法
ブロックされたプログラム警告の表示をオフにするには、次のいずれかの操作を行います。

- ブロックされたプログラム警告が表示されたら [OK] をクリックする前に、[**今後はこのダイアログを表示しない**] を選択します。以後、ブロックされたプログラム警告がすべて非表示になります。これは、新しいプログラム警告、繰り返されたプログラム警告、およびサーバ プログラム警告には影響しません。
- [プログラム コントロール] パネルで **[詳細設定]** をクリックして [警告と機能] タブにアクセスし、[**インターネット アクセスが拒否された場合に警告を表示する**] チェックボックスをオフにします。

ブロックされたプログラム警告をオフにしても、セキュリティのレベルには影響しません。

インターネット ロック警告

インターネット ロック警告は、インターネット ロック（または [停止] ボタン）が有効であるために Zone Labs セキュリティ ソフトウェア が外部との通信をブロックしたことを通知するものです。[OK] をクリックする

ことは、ロックの解除を意味するのではなく、警告を確認したことを意味します。

インターネット ロックが自動的（または偶然）に有効になっていた場合は、今後警告が表示されないようにインターネット ロックを解除します。18 ページの「ゾーンの概念」を参照してください。

警告が表示される原因
これらの警告は、インターネット ロックが有効な場合にのみ表示されます。

対応方法
[OK] をクリックして警告ポップアップを閉じます。

インターネット ロックが自動的（または偶然）に有効になっていた場合は、今後警告が表示されないようにインターネット ロックを解除します。18 ページの「ゾーンの概念」を参照してください。

特定のプログラム（ブラウザなど）にインターネット ロックをバイパスする許可を与えると、ロックの高セキュリティを保ちつつ、基本的な機能を継続して使用することができます。93 ページの「プログラムへのパスロック許可の設定」**を参照してください。**

警告の表示数を減らす方法
インターネット ロック警告が頻繁に表示される場合は、一定時間コンピュータがアクティブでなかった場合にインターネット ロックが有効になるように、自動インターネット ロック機能が設定されている可能性があります。

警告の表示数を減らすには、次のいずれかの操作を行います。

- 自動インターネット ロックをオフにする。
- 自動インターネット ロックが有効になるために必要なコンピュータの非アクティブ時間の設定を長くする。詳細については、79 ページの「自動ロックの有効化」を参照してください。

リモート警告

リモート警告は、Zone Labs セキュリティ ソフトウェア が ICS ゲートウェイで通信をブロックした場合に ICS クライアント マシンに表示されます。ご使用のマシンが ICS ネットワークのクライアントでない場合、この警告が表示されることはありません。

警告が表示される原因
リモート警告は次の場合に表示されます。

- Zone Labsセキュリティ ソフトウェア が ICS ゲートウェイで起動した場合。「リモート ファイアウォールが開始しました。」というメッセージが表示されます。

- Zone Labsセキュリティ ソフトウェア が ICS ゲートウェイで終了した場合。「リモート ファイアウォールが停止しました。」というメッセージが表示されます。
- インターネット ロックが ICS ゲートウェイで有効になった場合。これにより、クライアント マシンでいくつかのタスクが実行できなくなることがあります。「リモート ファイアウォールはインターネット ロックを設定しました。」というメッセージが表示されます。
- インターネット ロックが ICS ゲートウェイで解除された場合。「リモート ファイアウォールはインターネット ロックを解除しました。」というメッセージが表示されます。

対応方法

[OK] をクリックして警告ボックスを閉じます。セキュリティを維持するために、特別な操作は必要ありません。

警告の表示数を減らす方法

ICS クライアント マシンでリモート警告を表示しない場合は、次の操作を行います。

1. ［ファイアウォール］|［メイン］を選択し、［詳細設定］をクリックします。
2. ［インターネット接続共有（ICS)］エリアで、［ゲートウェイからの警告をこのコンピュータに転送する］チェックボックスをオフにします。

プログラム警告

ほとんどの場合、プログラム警告はプログラムの使用中に表示されます。たとえば、Zone Labs セキュリティ ソフトウェア をインストールした直後に Microsoft Outlook を開いてメールを送信しようとすると、Outlook にインターネット アクセスを許可してもよいかを問い合わせるプログラム警告が表示されます。また、ご使用のコンピュータ上でトロイの木馬やワームが感染の拡散を試みている場合やコンピュータ上のプログラムがオペレーティング システムの変更を試みている場合にも、プログラム警告が表示されます。

新しいプログラム警告

新しいプログラム警告では、以前にインターネット ゾーンまたはトラスト ゾーンへのアクセスを要求したことのないプログラムに対してアクセス許可を設定できます。[許可] をクリックすると、プログラムのアクセスが許可されます。[拒否] をクリックすると、プログラムのアクセスが拒否されます。

警告が表示される原因

新しいプログラム警告は、ご使用のコンピュータ上のプログラムがインターネット ゾーンまたはトラスト ゾーンのコンピュータに接続しようとした場合に、そのプログラムにアクセスが許可されていないと表示されます。

Zone Labs セキュリティ ソフトウェアの使用を開始すると、通常、新しいプログラム警告が 1 回または複数回表示されます。

対応方法

次の点を確認してから、警告ポップアップで [許可] または [拒否] をクリックします。

- 今起動したプログラムやプロセスは、許可すべきものですか？そうである場合は、**[許可]** をクリックしてもおそらく問題はありません。それ以外の場合は、次の質問に進んでください。
- 警告ポップアップに示されているプログラム名は既知のものですか？その場合、そのプログラムは通常許可を必要とするものですか？そうである場合は、**[許可]** をクリックしてもおそらく問題はありません。そうでない場合やわからない場合には、次に進みます。
- 警告ボックスの **[詳細情報]** ボタンをクリックします。これにより、警告情報（たとえば、プログラム名やプログラムがアクセスしようとしているアドレスなど）を SmartDefense Advisor に送信します。警告アドバイザは、この警告とプログラムについての情報を記載した Web ページ

を表示します。SmartDefense Advisor の情報を参考に、アクセスを許可しても問題がないかどうかを判断します。

お使いのブラウザにインターネットへのアクセス許可が与えられていない場合、このヘルプ ファイルが表示されます。SmartDefense Advisor にアクセスするには、ブラウザにインターネットへのアクセス許可を与えてください。

- どうしても対応方法がわからない場合は、[**拒否**] をクリックすることを推奨します。後で [プログラム] タブを使って、いつでも許可を与えることができます。83 ページの「新しいプログラムのアクセス許可の設定」.

警告の表示数を減らす方法

Zone Labs セキュリティ ソフトウェア をインストールした直後に新しいプログラム警告が頻繁に表示されることがありますが、これは通常の動作です。それぞれの新しいプログラムに許可を与えていくと、警告の数は減ります。[繰り返されたプログラム] 警告の表示を避けるには、[許可] または [拒否] をクリックする前に [**選択した結果を保存する**] チェックボックスをオンにします。

繰り返されたプログラム警告

繰り返されたプログラム警告は、以前に許可を要求したコンピュータ上のプログラムが、再度インターネット ゾーンまたはトラスト ゾーンのコンピュータへの接続を開始しようとした際に表示されます。

警告が表示される原因

[**選択した結果を保存する**] をオンにしないで [許可] または [拒否] を選択した場合、そのプログラムが再度アクセス許可を要求すると、繰り返されたプログラム警告が表示されます。

対応方法

繰り返されたプログラム警告には、新しいプログラム警告と同様に対応します。228 ページの「新しいプログラム警告」を参照してください。

警告の表示数を減らす方法

繰り返されたプログラム警告が表示されないようにするには、新しいプログラム警告または繰り返されたプログラム警告で [許可] または [拒否] をクリックする前に [**選択した結果を保存する**] をオンにします。これにより、プログラムの許可が [プログラム] タブで [許可] または [ブロック] に設定されます。

変更されたプログラム警告

変更されたプログラム警告は、以前にアクセス許可またはサーバ許可を問い合わせたプログラムが何らかの形で変更されたことを警告します。[許可

］をクリックすると、変更されたプログラムのアクセスが許可されます。［拒否］をクリックすると、プログラムのアクセスが拒否されます。

警告が表示される原因
変更されたプログラム警告は、プログラムがインターネットに最後にアクセスした後で、そのプログラムを更新した場合に表示されます。ただし、何らかの方法でハッカーにプログラムを変更された場合に表示されることもあります。

プログラムによっては、最新アップデートを確認するために、定期的にインターネットにアクセスするように設定されている場合があります。プログラムに自動更新機能が備わっているかどうかを確認するには、各プログラムのマニュアルまたはベンダのサポート Web サイトを参照してください。

対応方法
次の点を参考にして、変更されたプログラム警告に対応してください。

- 最近、ユーザもしくはシステム管理者（ビジネス環境の場合）が許可を求めているプログラムを更新しましたか？
- そのプログラムは通常許可を必要とするものですか？

両方とも該当する場合、**［許可］**をクリックしてもおそらく問題はありません。

よくわからない場合は、［拒否］をクリックすることを推奨します。後で［プログラム］タブを使って、いつでも許可を与えることができます。85 ページの「特定プログラムの許可の設定」を参照してください。

警告の表示数を減らす方法
変更されたプログラム警告は、［許可］または［拒否］のいずれかを選択する必要があるため、常に表示されます。チェックサムが頻繁に変更されるプログラムを使用している場合は、Zone Labs セキュリティ ソフトウェア でプログラムのファイル名のみが確認されるように設定して、警告の表示数を減らすことができます。89 ページの「プログラム一覧へのプログラムの追加」

プログラム コンポーネント警告

プログラム コンポーネント警告を使用して、Zone Labs セキュリティ ソフトウェア でアクセスを承認されていないコンポーネントを使用するプログラムのインターネット接続を許可または拒否します。これにより、プログラム コントロールの制限を回避するために改変または偽造されたコンポー

ネントを使用しようとするハッカーからコンピュータを守るのに役立ちます。

[許可] をクリックすると、プログラムが新規のコンポーネントや変更されたコンポーネントを使用してインターネットへアクセスすることを許可します。[拒否] をクリックすると、プログラムがこれらのコンポーネントを使用してインターネットにアクセスすることを防ぎます。

警告が表示される原因

プログラム コンポーネント警告は、Zone Labs セキュリティ ソフトウェアでアクセスを承認されていないコンポーネント、またはいったんアクセスを承認された後に変更されたコンポーネントを使用するプログラムが、インターネットまたはローカル ネットワークにアクセスしようとした場合に表示されます。

Zone Labs セキュリティ ソフトウェア は、アクセスを許可する際に、プログラムが使用するコンポーネントに対して自動的にアクセスを承認します。これにより、ブラウザによってロードされる全コンポーネントについてコンポーネント警告が表示されるのを防ぎます。Zone Labs セキュリティ ソフトウェア によるプログラム コンポーネントを保護する方法の詳細については、94 ページの「プログラム コンポーネントの管理」を参照してください。

対応方法

プログラム コンポーネント警告に対する対処は、状況により異なります。次の質問について考慮してください。

- 次のいずれかが当てはまりますか？
  - Zone Labs セキュリティ ソフトウェア をインストールまたは再インストールした直後である。
  - コンポーネントをロードしているアプリケーションを最近更新したばかりである（アプリケーション名については、警告ポップアップの技術的情報を参照してください）。
  - コンポーネントをロード中のアプリケーションに自動更新機能が備わっている。
  - 知らない間に誰か（社内のシステム管理者など）がご使用のコンピュータのプログラムを更新した可能性がある。
- コンポーネントをロードしたアプリケーションを頻繁に使用していますか？

いずれの質問にも該当する場合、Zone Labs セキュリティ ソフトウェア は、ブラウザまたは他のプログラムが必要とする正当なコンポーネントを

検出した可能性があります。この場合は、[プログラム コンポーネント] 警告が表示されたら、[許可] をクリックしても問題ありません。

[許可] をクリックすると、プログラムが新規のコンポーネントや変更されたコンポーネントを使用してインターネットへアクセスすることを許可します。いずれにも当てはまらない場合や、何らかの理由でコンポーネントについて不安がある場合には、[拒否] をクリックしたほうが無難です。

[拒否] をクリックすると、プログラムがこれらのコンポーネントを使用してインターネットにアクセスすることを防ぎます。

適切な対処が不明の場合や、[拒否] を選択した場合は、コンポーネントについて調査し、その安全性を確認してください。

警告の表示数を減らす方法

Zone Labs セキュリティ ソフトウェア をインストールした後すぐにプログラム認証レベルを上げると、多くのコンポーネント警告が表示される可能性があります。認証を [高] に設定すると、Zone Labs セキュリティ ソフトウェア は、ブラウザや他のプログラムで通常使用される多数の DLL およびその他のコンポーネントに対して、アクセスを自動的に承認できなくなります。

警告の表示数を減少させるには、Zone Labs セキュリティ ソフトウェア をインストールした後、数日間は認証レベルを [中] に設定します。

Zone Labs セキュリティ ソフトウェア を数日以上使用すると、多くの場合プログラム警告が多数表示されることはなくなります。

サーバ プログラム警告

サーバ プログラム警告では、コンピュータ上のプログラムに対するサーバ許可を設定できます。

警告が表示される原因

サーバ プログラム警告は、コンピュータ上のプログラムがインターネット ゾーンまたはトラスト ゾーンについてサーバ許可を要求した場合に、そのプログラムにまだサーバ許可が与えられていないと表示されます。

コンピュータ上のプログラムでサーバ許可を必要とするものは限られています。サーバ許可を必要とする一般的なプログラムには次のようなものがあります。

- チャット
- インターネット キャッチホン
- 音楽ファイルの共有 (Napster など)

- ストリーミング メディア（RealPlayer など）
- Voice-over-Internet
- Web ミーティング

正常に動作するためにサーバ許可を必要とする上記の種類のプログラムを使用する場合は、プログラムの使用前に許可を与える必要があります。90 ページの「プログラムのサーバ動作の許可」を参照してください。

ブラウザにインターネットへのアクセス許可が与えられていない場合、オンライン ヘルプが表示されます。SmartDefense Advisor にアクセスするには、ブラウザにインターネットへのアクセス許可を与えてください。89 ページの「プログラムのインターネット アクセスの許可」を参照してください。

対応方法

サーバ プログラム警告に対応するには、以下を考慮してください。

- 今起動したプログラムやプロセスは、許可すべきものですか？そうである場合は、[許可] をクリックしてもおそらく問題はありません。それ以外の場合は、次の質問に進んでください。
- 警告ポップアップに記載されたプログラム名は既知のものですか？ その場合、そのプログラムは通常許可を必要とするものですか？そうである場合は、[許可] をクリックしてもおそらく問題はありません。
- 警告ボックスの **[詳細情報]** ボタンをクリックします。これにより、警告情報（たとえば、プログラム名やプログラムがアクセスしようとしているアドレスなど）を SmartDefense Advisor に送信します。警告アドバイザは、この警告とプログラムについての情報を記載した Web ページを表示します。SmartDefense Advisor の情報を参考に、アクセスを許可しても問題がないかどうかを判断します。詳細については、186 ページの「SmartDefense Advisor およびハッカー ID の使用」を参照してください。
- サーバ許可を求めているプログラムが正当なものであるかどうかの判断がつかない場合は、[拒否] を選択すると安全です。後で必要となった場合に、[プログラム] タブを使用してサーバ許可をプログラムに与えることができます。90 ページの「プログラムのサーバ動作の許可」を参照してください。

警告の表示数を減らす方法

正常に動作するためにはサーバ許可が必要な上記種類のプログラムを使用する場合は、それらのプログラムの使用を開始する前に Zone Labs セキュリティ ソフトウェアの [プログラム] タブを使用して許可を与えます。多数のサーバ プログラム警告が表示される場合は、追加の予防措置として、

アンチウイルス ツールまたはアンチスパイウェア ツールをダウンロードして実行することをお勧めします。

アドバンス プログラム警告

アドバンス プログラム警告は、他のプログラム警告（新しいプログラム警告、繰り返されたプログラム警告、および変更されたプログラム警告）と同様に、プログラムがネットワークへのアクセスを試みていることを通知するものです。

他のプログラム警告と異なるのは、そのプログラムが他のプログラムを使用してインターネットへアクセスしようとしているか、または他のプログラムの機能を操作しようとしている点です。

警告が表示される原因

アドバンス プログラム警告が表示されるのは次の 2 つの場合です。コンピュータ上のプログラムが、インターネット ゾーンまたはトラスト ゾーンのコンピュータとの接続を開始するために、他のプログラムに接続を指示した場合や、OpenProcess 関数を呼び出して他のプログラムのプロセスをハイジャックしようとした場合。

オペレーティング システム関連の正当なプログラムのなかには、他のプログラムへのアクセスを必要とするものもあります。たとえば、Windows タスク マネージャを使用して Internet Explorer をシャットダウンする場合、Windows タスク マネージャは Internet Explorer プログラムの OpenProcess 関数を呼び出す必要があります。

対応方法

アドバンス プログラム警告への対処方法は、警告の原因によって異なります。OpenProcess 関数が呼び出されたためにアドバンス プログラム警告が表示された場合は、この関数が正当なプログラムによって呼び出されたか、不正なプログラムによって呼び出されたかを判断する必要があります。警告に示されているプログラムがこの関数を実行しても問題がないかどうか確認してください。たとえば、Windows タスク マネージャを使ってプログラムを終了しようとしている際にアドバンス プログラム警告が表示された場合は、[**許可**] を選択してもおそらく問題はありません。同様に、他のプログラムを使ってインターネットにアクセスするプログラムが警告の原因となっている場合も、そのプログラムが定期的にアクセス許可を要求するプログラムであれば、[**許可**] を選択して問題はないと考えられます。警告の原因が不明な場合や、要求元であるプログラムの通常の動作が不明な場合は、[**拒否**] を選択するのが最も安全です。プログラムのアドバンス許可を拒否した後に、プログラムのファイル名をインターネットで検索します。悪質なプログラムの場合、コンピュータからの削除方法など、プログラムに関する情報がインターネットで検索できます。

警告の表示数を減らす方法

通常、多数のアドバンス プログラム警告が表示されることはありません。警告が繰り返し表示される場合、プログラム名をインターネットで調査し、

コンピュータからプログラムを削除するか、プログラムに適切なアクセス権を与えるかを検討してください。

自動 VPN 設定警告

自動 VPN 設定警告は、Zone Labs セキュリティ ソフトウェア が VPN アクティビティを検出すると表示されます。検出された VPN アクティビティの種類によって、また、Zone Labs セキュリティ ソフトウェア が VPN 接続を自動設定できたかどうかによって、3 種類の自動 VPN 設定警告のうちいずれかが表示されます。

警告が表示される原因

自動 VPN 設定警告は、許可するように設定されていない VPN アクティビティを Zone Labsセキュリティ ソフトウェア が検出すると表示されます。

対応方法

自動 VPN 設定警告への対処は、どの自動 VPN 設定警告が表示されているか、VPN ソフトウェアを起動しているか、および Zone Labs セキュリティ ソフトウェア で VPN 接続を許可するか、という条件によって異なります。

VPN 通信をブロックするエキスパート ファイアウォール ルールを作成した場合は、VPN 通信を許可するようにエキスパート ルールを変更する必要があります。62 ページの「エキスパート ファイアウォール ルールの作成」を参照してください。

- お使いのコンピュータ上で VPN ソフトウェアを起動していて、VPN 接続を設定する場合は、次のいずれかを選択します。

  [この VPN 接続をサポートするために Zone Labs セキュリティ ソフトウェアを設定する。]、または

  [VPN ソフトウェアを実行中で、これをサポートするために Zone Labs セキュリティ ソフトウェア を設定する。]

- VPN ソフトウェアを実行していて、Zone Labsセキュリティ ソフトウェアで接続を設定しない場合は、**[この VPN 接続をサポートするために Zone Labs セキュリティ ソフトウェア を設定しない。]** を選択します。

- VPN ソフトウェアを実行していない場合は、**[VPN ソフトウェアを実行していません。]** を選択します。

警告の表示数を減らす方法

VPN ソフトウェアを実行している場合に警告の表示数を減らすには、VPN ソフトウェアとその必要とするリソースを許可するよう、Zone Labs セキュリ

ティ ソフトウェア を正しく設定する必要があります。38 ページの「VPN 接続の手動設定」を参照してください。

手動操作の要求警告

手動操作の要求警告は、VPN 接続をサポートするように Zone Labs セキュリティ ソフトウェア を正しく設定するために、さらに操作が必要であることを通知するものです。

警告が表示される原因

手動操作の要求警告は、Zone Labs セキュリティ ソフトウェア が VPN 接続を自動設定できない場合、あるいは、自動設定を完了するためにさらに手動で設定を変更しなければならない場合に表示されます。

対応方法

手動操作の要求警告に対して、ユーザが何らかの対処をする必要はありません。VPN 接続を手動で設定するには、38 ページの「VPN 接続の手動設定」を参照し、手動設定の説明に従ってください。

警告の表示数を減らす方法

通常、手動操作の要求警告が頻繁に表示されることはありません。この警告が多く表示される場合は、VPN 接続をサポートするための手順を実行して Zone Labs セキュリティ ソフトウェア を適切に設定するか、または VPN ソフトウェアをコンピュータから削除してください。

OSFirewall 警告

OSFirewall 警告は、コンピュータ上のプログラムまたはプロセスがコンピュータの設定またはプログラムを変更しようとしている場合に表示される警告です。

応答が必要な OSFirewall 警告には、「疑わしい」、「危険」、および「悪意がある」という 3 つの種類があります。

OSFirewall 保護は、ZoneAlarm Pro および ZoneAlarm Security Suite で使用できます。

疑わしい動作の警告

疑わしい動作の警告は、コンピュータ上のプログラムが疑わしいとみなされる活動を試行していることを示します。[許可] をクリックすると、プログラムは活動を実行できます。[拒否] をクリックすると、プログラムは活動を実行できず、制限されたアクセスを与えられます。これは、その後の疑わしい動作と危険な動作のすべてが拒否されることを意味します。

警告が表示される原因

ハッカーは、信頼されているプログラムを用いて、ブラウザ設定のような他のプログラムを変更したり、コンピュータのオペレーティング システムを破壊したりすることがよくあります。

対応方法

[許可] または **[拒否]** をクリックします。アクションを許可するか拒否するかが不明な場合、警告ボックス内の **[詳細情報]** ボタンをクリックします。これにより、警告情報（たとえば、プログラム名やプログラムが実行しようとしている活動など）を SmartDefense Advisor に送信します。警告アドバイザは、この警告と動作についての情報を記載した Web ページを表示します。SmartDefense Advisor の情報を参考に、アクションを許可するか拒否するかを判断します。疑わしい動作の警告に関する原因の詳細については、274 ページの「疑わしい動作」を参照してください。

[許可] または [拒否] をクリックする前に **[この設定を保存]** チェックボックスをオンにすると、今後はプログラムまたはコンポーネントは任意の疑わしい機能を実行可能になり、警告は表示されなくなります。

危険な動作の警告

危険な動作の警告は、コンピュータ上のプログラムが危険とみなされる活動を試行していることを示します。[許可] をクリックすると、プログラムは活動を実行できます。[拒否] をクリックすると、プログラムは活動

を実行できず、制限されたアクセスを与えられます。これは、その後の疑わしい動作と危険な動作のすべてが拒否されることを意味します。

警告が表示される原因
これらの警告は、コンピュータ上のプログラムまたはコンポーネントがコンピュータ上のプロセスまたはプログラムをハイジャックしようとしたり、コンピュータまたはプログラムのデフォルト設定を変更しようとしたりするところを検出された場合に発生します。

対応方法
危険な動作の警告が表示される原因となるアクションの性質を考慮すると、警告ポップアップで［拒否］をクリックするのが最も安全です。不明な場合は、警告ボックスの［**詳細情報**］ボタンをクリックします。これにより、警告情報（たとえば、プログラム名やプログラムが実行しようとしている活動など）を SmartDefense Advisor に送信します。警告アドバイザは、この警告と動作についての情報を記載した Web ページを表示します。SmartDefense Advisor の情報を参考に、アクションを許可するか拒否するかを判断します。危険な動作の警告に関する原因の詳細については、275 ページの「危険な動作」を参照してください。

［許可］または［拒否］をクリックする前に［**この設定を保存**］チェックボックスをオンにすると、今後はプログラムまたはコンポーネントは任意の危険な機能を実行可能になり、警告は表示されなくなります。

悪意のある動作の警告

悪意のある動作の警告は、悪意のあるプログラムがコンピュータ上で実行を試みていることを示します。Zone Labs セキュリティ エキスパートによって指定されるプログラムはワーム、ウイルス、トロイの木馬、その他の破壊工作プログラムとして知られています。

警告が表示される原因
この警告はコンピュータ上のプログラムが抹消（シャットダウン）されることを通知するために表示されます。

対応方法
悪意のある警告に対して、ユーザは対応する必要はありません。発生しているアクションのみが通知されます。信頼できるプログラムが誤って抹消された場合、プログラム リストからプログラムを有効化できます。

ID ロック警告

ID ロック警告は、myVAULT に保存された情報が、トラスト サイト リストに含まれていない送信先に送信されようとしていることを通知するものです。

警告が表示される原因

ID ロック警告は、myVAULT に保存された情報が Web ページまたはメールに入力された場合、あるいは、パスワードがユーザの承認なしに平文（暗号化されていない）形式で送信されようとしている場合に表示されます。

対応方法

情報を要求しているサイトが、信頼できるサイトであるかどうかを判断する必要があります。送信する情報の機密性、要求の正当性、およびそのサイトの信頼性に基づいて、情報の送信を許可するか拒否するかを判断してください。信頼できるベンダでオンライン ショッピングをしている時にこの警告が表示された場合は、情報の送信を許可しても問題ありません。そうしたケース以外でこの警告が表示された場合は、情報の送信をブロックするほうが安全です。

また、一部のサイトでは、パスワードを平文形式で送信します。あるサイトに対して、平文でのパスワード送信をブロックしたことがある場合、そのサイトにアクセスしてパスワードを入力すると、ID ロック警告が表示されます。

警告の表示数を減らす方法

トラスト サイト リストに登録されていないサイトに対して myVAULT のコンテンツを頻繁に送信する場合や、平文パスワードを使用するサイトに対して平文でのパスワード送信をブロックした場合には、ID ロック警告が頻繁に表示されます。個人情報を送信する機会の多いサイトをトラスト サイト リストに追加したり、平文パスワードを使用するサイトに対して平文でのパスワード送信を許可することによって、ID ロック警告の表示を最小限に抑えることができます。

新しいネットワーク警告

新しいネットワーク警告は、Zone Labs セキュリティ ソフトウェア が以前に接続したことのないネットワークに対する接続を検出した際に表示されます。警告ポップアップを使用して、そのネットワークでのファイルとプリンタの共有を許可することができます。新しいネットワーク警告は、家庭内のワイヤレス ネットワーク、企業内 LAN、または ISP のネットワークなど、いずれのネットワークに接続する場合でも表示されます。

Zone Labs セキュリティ ソフトウェア を初めて使用する際には、ほとんどの場合、新しいネットワーク警告が表示されます。心配は不要です。この警告は、Zone Labs セキュリティ ソフトウェアの設定に役立つようデザインされた便利なツールです。

警告が表示される原因

新しいネットワーク警告は、家庭内のワイヤレス ネットワーク、企業内 LAN、または ISP のネットワークなど、いずれのネットワークに接続する場合でも表示されます。

対応方法

新しいネットワーク警告についての対処方法は、ご使用のネットワークの状況により異なります。

ホーム ネットワークまたはビジネス ローカル ネットワークに接続していて、ネットワーク上の他のコンピュータとリソースを共有したい場合は、ネットワークをトラスト ゾーンに追加します。

新しいネットワークをトラスト ゾーンに追加するには、次のようにします。

1. 新しいネットワーク警告のポップアップで、[名前] ボックスにネットワーク名を入力します (たとえば、「Home NW」)。
2. [ゾーン] ドロップ ダウン リストから **[トラスト ゾーン]** を選択します。
3. [OK] をクリックします。

Zone Labs セキュリティ ソフトウェアが検出したネットワークが不明な場合は、警告ボックスに表示されている IP アドレスを書き写しておきます。その上で、ホーム ネットワークのマニュアルを参照するか、システム管理者または ISP に問い合わせてネットワークを確認します。

Zone Labs セキュリティ ソフトウェア がワイヤレス ネットワークを検出した場合は、注意が必要です。ワイヤレス ネットワーク アダプタが、ご使用のネットワーク以外のネットワークを検出する可能性があります。トラスト ゾーンに追加する前に、新しいネットワーク警告に表示されている IP アドレスが正しいことを確認してください。

標準モデムおよびダイヤルアップ接続、デジタル加入者線（DSL）、またはケーブル モデムを使用してインターネットに接続する場合は、新しい警告ポップアップで［OK］をクリックします。

［キャンセル］をクリックすると、Zone Labs セキュリティ ソフトウェア はインターネット接続をブロックします。トラスト ゾーンには ISP のネットワークを追加しないでください。

警告の表示数を減らす方法

新しいネットワーク警告が頻繁に表示されるのは異常です。

インスタント メッセージ警告

このセクションでは、Zone Labs セキュリティ ソフトウェア で保護されたインスタント メッセージ セッション中に表示されることのある、さまざまな警告メッセージについて説明します。

次の表は、Zone Labs セキュリティ ソフトウェアの使用時に表示されることがある警告メッセージの一覧です。表の説明で警告が表示された原因を確認し、対応が必要かどうかを判断してください。すべての警告メッセージは、インスタント メッセージング ウィンドウで、角括弧 [ ] 内に表示されます。

警告テキスト	説明
[コンタクトの IM ID] が暗号化を無効にしたため、セッションは暗号化されません。	この警告は、ユーザが暗号化を有効にしている場合に、コンタクト側で暗号化が無効に設定されていると表示されます。
[コンタクトの IM ID] が ZoneAlarm Security Suite によって保護されていないため、セッションは暗号化されません。	この警告は、ZoneAlarm Security Suite を使用していないコンタクトと対話している場合に、インスタント メッセージング ウィンドウに表示されます。
[説明] についての情報は、ID ロック設定に準拠して、以前のメッセージから削除されました。	この警告は、myVAULT に保存されている情報を送信しようとした場合に表示されます。myVAULT 内にある項目の説明は、角括弧 [ ] で囲まれて表示されます。
リンクが削除されました。	この警告は、削除されたリンクの代わりに、メッセージ受信者のウィンドウに表示されます。
セッションは暗号化されました。	この警告は、暗号化されたインスタント メッセージング対話の開始時に表示されます。
有害な可能性のある内容がこのメッセージから削除されました。	この警告は、フィルタリングされたメッセージに追加されます。
[コンタクトの IM ID] のコンタクト リストに登録されていないため、メッセージはブロックされました。	この警告は、迷惑メール防止を有効にしている受信者のコンタクト リストに自分が載っていない場合に、メッセージを送信しようとすると表示されます。
[コンタクトの IM ID] の PC 上のファイルの転送はブロックされました。	この警告は、ファイルをコンタクトに送信しようとした場合に、コンタクト側の ZoneAlarm Security Suite でファイル転送がブロックされると表示されます。
[コンタクトの IM ID] の PC でビデオ伝送がブロックされました。	この警告は、ビデオをコンタクトに送信しようとした場合に、コンタクト側でビデオ伝送がブロックされると表示されます。

表 A-1: IM 警告メッセージ

警告テキスト	説明
有害な可能性のある書式またはスクリプトが、直前のメッセージから削除されました。	この警告は、コンタクト側でタグについて［外部からの保護］オプションが［ブロック］に設定されている場合に、書式またはスクリプトを含むメッセージをコンタクトに送信しようとすると表示されます。
有害な可能性のあるリンクが、直前のメッセージから削除されました。	この警告は、コンタクト側でアクティブについての［外部からの保護］オプションが［ブロック］に設定されている場合に、実行可能リンクを含むメッセージをコンタクトに送信しようとすると表示されます。

表 A-1: IM 警告メッセージ

付録 B
キーボードのショートカット

キーボードのショートカットを使って Zone Labs セキュリティ ソフトウェアの多くの機能にアクセスできます。

- 246 ページの「ナビゲーション ショートカット」
- 247 ページの「グローバル機能ショートカット」
- 249 ページの「ダイアログ ボックスのコマンド」
- 250 ページの「ボタンのショートカット」

ナビゲーション ショートカット

これらのキー入力を使用して、Zone Labs セキュリティ ソフトウェアのパネル、タブ、ダイアログ内を移動します。F6 を使用すると、目的の項目まで移動することができます。その後、上下左右の矢印を使用し、そのグループ内の選択項目まで移動します。

例：

［ファイアウォール］パネルの［ゾーン］タブへ移動するには、次のようにします。

1. 左のメニュー バーが選択されるまで **F6** を押します。
2. ［ファイアウォール］パネルが選択されるまで、**下矢印**を押します。
3. タブが選択されるまで **F6** を押します。
4. **上**、**下**、**左**、**右**の矢印を使用して、［ゾーン］タブを選択します。

キー入力	機能
F1	表示されているパネルのオンライン ヘルプを表示します。
F6	次の順にインターフェイス エリアを移動します。パネル選択、タブ選択、パネル エリア、［停止］/［ロック］コントロール。
TAB	F6 と同じ順にインターフェイス エリアを移動します。パネル範囲がアクティブなときに［Tab］を押すと、パネル内のコントロール部分を移動します。
上下矢印	コントロール部分で個々のコントロールを移動します。
左右矢印	コントロール部分で個々のコントロールを移動します。一覧表示では、水平方向にスクロールします。
ALT + スペース バー	Windows のコントロール メニュー（最大化、最小化、閉じる）を表示します。

表 B-1: ナビゲーション ショートカット

グローバル機能ショートカット

次のキー入力を使用して、インターフェイス内のさまざまな場所から機能をアクティブにすることができます。キー入力の中には、パネルによって別の機能を割り当てられたものもあります。これらのキー入力は、後述の［ボタンのショートカット］にリストされています。

キー入力	機能
CTRL + S	［停止］ボタン（緊急ロック）を有効および無効にします。
CTRL + L	インターネット ロックを有効および無効にします。
ALT + T	説明テキストを非表示および表示します。
ALT + D	デフォルト設定に戻します。
ALT + C	利用可能な場合、カスタム ダイアログ ボックスを開きます。
ALT + U	2 つの［カスタム］ボタンが表示されている場合は（たとえば、［プログラム コントロール］パネルの［メイン］タブ）、2 番目の［カスタム］ダイアログ ボックスを開きます。
ALT + A	利用可能な場合、詳細ダイアログ ボックスを表示します。
ALT + 下矢印	アクティブなドロップダウン リスト ボックスを表示します。利用可能な場合、一覧表示で左クリックのショートカット メニューを表示します。
SHIFT + F10	利用可能な場合、一覧表示で右クリックのショートカットを表示します。
ESC	［キャンセル］ボタンのクリックに相当します。
ENTER	アクティブなボタンのクリックに相当します。

表 B-2: グローバル ショートカット

キー入力	機能
ALT + P	[適用] ボタンのクリックに相当します。
削除	一覧表示から選択した項目を削除します。
ALT + F4	Zone Labs セキュリティ ソフトウェア をシャットダウンします。
ALT + K	ダッシュボード以外を非表示にします。
ALT + A	利用可能な場合、[追加] ボタンのクリックに相当します。
ALT + R	[削除] ボタンのクリックに相当します。
ALT + E	[編集] ボタンのクリックに相当します。
ALT + M	[詳細情報] ボタンが利用可能な場合、[詳細情報] ボタンのクリックに相当します。

表 B-2: グローバル ショートカット

ダイアログ ボックスのコマンド

ダイアログ ボックスが開いている時に、次のキー入力を使用できます。

キー入力	機能
タブ	ダイアログ ボックス内の次のコントロールをアクティブにします。
SHIFT + TAB	ダイアログ ボックス内の前のコントロールをアクティブにします。
CTRL + TAB	複数のタブを持つダイアログ ボックスで、次のタブを表示します。
CTRL + SHIFT + TAB	複数のタブを持つダイアログ ボックスで、前のタブを表示します。
ALT + 下矢印	アクティブなドロップダウン リスト ボックスを表示します。
スペース バー	アクティブなボタンをクリックします。アクティブなチェックボックスをオン / オフにします。
ENTER	アクティブなボタンのクリックに相当します。
ESC	[キャンセル] ボタンのクリックに相当します。

表 B-3: ダイアログ ボックスのショートカット

ボタンのショートカット

次のキー入力を使用して、アクティブなウィンドウ内のボタンをクリックします。

パネル	タブ	キー入力	相当するボタン
概要	[状況] タブ	Alt + R	チュートリアル
概要	[状況] タブ	Alt + M	Zone Labs の最新情報
概要	製品情報	Alt + I	ライセンスの変更
概要	製品情報	Alt + B	購入する
概要	製品情報	Alt + N	更新
概要	製品情報	Alt + R	登録の変更
概要	設定	Alt + P	パスワードの設定
概要	設定	Alt + B	バックアップ
概要	設定	Alt + R	復元
概要	設定	Alt + O	ログイン / ログアウト
概要	設定	Alt + U	アップデートの確認
ファイアウォール	メイン	Alt + C	インターネット ゾーンのカスタム
ファイアウォール	メイン	Alt + U	トラスト ゾーンのカスタム
ファイアウォール	メイン	Alt + A	詳細
ファイアウォール	ゾーン	Alt + A	追加
ファイアウォール	ゾーン	Alt + R	削除
ファイアウォール	ゾーン	Alt + E	編集
ファイアウォール	ゾーン	Alt + P	適用
ファイアウォール	エキスパート	Alt + A	追加
ファイアウォール	エキスパート	Alt + R	削除
ファイアウォール	エキスパート	Alt + E	編集
ファイアウォール	エキスパート	Alt + P	適用
ファイアウォール	エキスパート	Alt + G	グループ
プログラム コントロール	メイン	Alt + C	プログラム コントロールのカスタム
プログラム コントロール	メイン	Alt + U	自動ロックのカスタム
プログラム コントロール	メイン	Alt + A	詳細

表 B-4: ボタンをアクティブにするキー入力

パネル	タブ	キー入力	相当するボタン
プログラム コントロール	プログラム	Alt + A	追加
プログラム コントロール	プログラム	Alt + O	オプション
プログラム コントロール	コンポーネント	Alt + M	詳細情報
アンチウイルス / アンチスパイウェア	メイン	Alt + S	ウイルス / スパイウェアのスキャン
アンチウイルス / アンチスパイウェア	メイン	Alt + U	今すぐアップデート
アンチウイルス / アンチスパイウェア	メイン	Alt + A	詳細オプション
アンチウイルス / アンチスパイウェア	メイン	Alt + V	ウイルスのスキャン
アンチウイルス / アンチスパイウェア	メイン	Alt + W	スパイウェアのスキャン
アンチウイルス / アンチスパイウェア	隔離	Alt + D	削除
アンチウイルス / アンチスパイウェア	隔離	Alt + E	復元
アンチウイルス / アンチスパイウェア	隔離	Alt + M	詳細情報
メール保護	メイン	Alt + A	詳細
メール保護	添付ファイル	Alt + C	すべてを選択
メール保護	添付ファイル	Alt + R	すべてをクリア
メール保護	添付ファイル	Alt + A	追加
メール保護	添付ファイル	Alt + P	適用
プライバシー	メイン	Alt + C	Cookie コントロールのカスタム
プライバシー	メイン	Alt + U	広告ブロックのカスタム
プライバシー	メイン	Alt + S	モバイル コード コントロールのカスタム
プライバシー	サイト一覧	Alt + A	追加
プライバシー	サイト一覧	Alt + O	オプション
プライバシー	キャッシュ クリーナ	Alt + N	削除
プライバシー	キャッシュ クリーナ	Alt + U	カスタム

表 B-4: ボタンをアクティブにするキー入力

パネル	タブ	キー入力	相当するボタン
プライバシー	ハード ドライブ IE/MSN Netscape	Alt + D	デフォルトに戻す
プライバシー	ハード ドライブ IE/MSN Netscape	Alt + P	適用
プライバシー	IE/MSN Netscape	Alt + S	選択
ID ロック	myVAULT	Alt + A	追加
ID ロック	myVAULT	Alt + O	オプション
ID ロック	myVAULT	Alt + N	暗号化
ID ロック	myVAULT	Alt + E	編集
ID ロック	myVAULT	Alt + R	削除
ID ロック	信頼するサイト	Alt + A	追加
ID ロック	信頼するサイト	Alt + R	削除
ペアレント コントロール	メイン	Alt + A	詳細
ペアレント コントロール	カテゴリ	Alt + C	すべてを選択
ペアレント コントロール	カテゴリ	Alt + R	すべてをクリア
警告とログ	メイン	Alt + D	デフォルトに戻す
警告とログ	メイン	Alt + C	カスタム
警告とログ	メイン	Alt + A	詳細
警告とログ	ログ ビューア	Alt + M	詳細情報
警告とログ	ログ ビューア	Alt + D	一覧をクリア
警告とログ	ログ ビューア	Alt + A	ゾーンに追加
警告とログ	ログ コントロール	Alt + B	参照
警告とログ	ログ コントロール	Alt + E	ログの削除

表 B-4: ボタンをアクティブにするキー入力

付録 C
トラブルシューティング

この章では、Zone Labs セキュリティ ソフトウェアの使用時に発生する問題のトラブルシューティングとなるガイダンスを提供します。

トピック：

- 254 ページの「VPN」
- 256 ページの「ネットワーキング」
- 258 ページの「インターネット接続」
- 261 ページの「IM セキュリティ」
- 262 ページの「アンチウイルス」
- 264 ページの「サードパーティのソフトウェア」

VPN

Zone Labs セキュリティ ソフトウェア と VPN ソフトウェアの併用に問題がある場合は、次の表のトラブルシューティングのヒントを参照してください。

該当する状況	参照先
仮想プライベート ネットワーク (VPN) に接続できない	254 ページの「VPN 通信のための Zone Labs セキュリティ ソフトウェアの設定」
エキスパート ファイアウォール ルールを作成した	254 ページの「VPN の自動設定およびエキスパート ルール」
サポートされている VPN クライアントを使用しているが、初回接続時に Zone Labs セキュリティ ソフトウェア によって自動検出されない	255 ページの「VPN の自動検出の遅延」

表 C-1: VPN に関する問題のトラブルシューティング

VPN 通信のための Zone Labs セキュリティ ソフトウェアの設定

VPN に接続できない場合は、VPN からの通信を許可するように Zone Labs セキュリティ ソフトウェア を設定する必要がある可能性があります。

Zone Labs セキュリティ ソフトウェア で VPN 通信を許可するには、次のようにします。

1. VPN に関連するネットワーク リソースをトラスト ゾーンへ追加します。

   53 ページの「トラスト ゾーンへの追加」を参照してください。

2. コンピュータ上の VPN クライアントおよび VPN に関連するプログラムにアクセス許可を与えます。

   85 ページの「特定プログラムの許可の設定」を参照してください。

3. VPN プロトコルを許可します。

   39 ページの「VPN ゲートウェイとその他のリソースのトラスト ゾーンへの追加」を参照してください。

VPN の自動設定およびエキスパート ルール

VPN プロトコルをブロックするエキスパート ファイアウォール ルールを作成した場合は、接続を開始しても Zone Labs セキュリティ ソフトウェア は VPN を自動検出しません。VPN 接続の設定にあたっては、VPN クライアントと VPN に関連するコンポーネントがトラスト ゾーンに含まれていて、

それらにインターネットへのアクセス許可が与えられていることを確認する必要があります。37 ページの「VPN 接続の設定」を参照してください。

VPN の自動検出の遅延

Zone Labs セキュリティ ソフトウェア は定期的にコンピュータのポーリングを行い、サポートされている VPN プロトコルが使用されているかどうかを確認します。サポートされている VPN プロトコルを検出すると、Zone Labs セキュリティ ソフトウェア は接続の自動設定を行うようにユーザにメッセージを表示します。VPN クライアントをインストールしたばかりの状態で接続を試みる場合、Zone Labs セキュリティ ソフトウェア で VPN 設定が検出されないことがあります。Zone Labs セキュリティ ソフトウェア を使って接続を自動設定する場合は、10 分ほど時間をおいてから再度接続を試みてください。すぐに接続したい場合は、手動で接続を設定できます。37 ページの「VPN 接続の設定」を参照してください。

ネットワーキング

ネットワークへの接続またはネットワーキング サービスの使用に問題がある場合は、次の表のトラブルシューティングのヒントを参照してください。

該当する状況	参照先
[マイ ネットワーク] に他のコンピュータが表示されない、または他のコンピュータで自分のコンピュータが表示されない	256 ページの「ローカル ネットワークでのコンピュータの認識」
家庭内ネットワークまたはローカル ネットワーク上で、ファイルまたはプリンタを共有できない	257 ページの「ローカル ネットワークでのファイルおよびプリンタの共有」
コンピュータがローカル エリア ネットワーク (LAN) 内にあり、Zone Labs セキュリティ ソフトウェア がインストールされていると、起動に時間がかかる	257 ページの「起動に時間がかかる場合の対処」

表 C-2: ネットワークに関する問題のトラブルシューティング

ローカル ネットワークでのコンピュータの認識

ローカル ネットワーク上の他のコンピュータを認識できない場合や、他のコンピュータがお使いのコンピュータを認識できない場合は、Zone Labs セキュリティ ソフトウェア が Windows ネットワークの認識に必要な NetBIOS 通信をブロックしている可能性があります。

ローカル ネットワークでコンピュータを認識させるには、次のようにします。

1. ネットワークのサブネット (または小規模なネットワーク環境では共有している各コンピュータの IP アドレス) をトラスト ゾーンに追加します。53 ページの「トラスト ゾーンへの追加」を参照してください。
2. トラスト ゾーンのセキュリティ レベルの設定を [中] にし、インターネット ゾーンのセキュリティ レベルを [高] にします。これにより、信頼できるコンピュータによる共有ファイルへのアクセスは可能になりますが、他のマシンからのアクセスはブロックされます。47 ページの「アドバンス セキュリティ オプションの設定」を参照してください。

Zone Labs セキュリティ ソフトウェア はネットワークを自動的に検出し、新しいネットワーク警告を表示します。警告を使用して、ネットワーク サブネットをトラスト ゾーンに追加することができます。詳細については、240 ページの「新しいネットワーク警告」を参照してください。

ローカル ネットワークでのファイルおよびプリンタの共有

Zone Labs セキュリティ ソフトウェア を使用して、すばやくかつ簡単にコンピュータを共有することができます。ネットワーク上の信頼できるマシンに対しては共有リソースへのアクセスを許可し、システムを破壊しようとするインターネットの侵入者に対しては共有リソースへのアクセスを許可しないように設定できます。

Zone Labs セキュリティ ソフトウェア でリソースの安全な共有を設定するには、次のようにします。

1. ネットワークのサブネット（または小規模なネットワーク環境では共有している各コンピュータの IP アドレス）をトラスト ゾーンに追加します。53 ページの「トラスト ゾーンへの追加」を参照してください。
2. トラスト ゾーンのセキュリティ レベルを［中］に設定します。これにより、信頼するコンピュータが共有ファイルにアクセスできるようになります。45 ページの「セキュリティ レベルの選択」を参照してください。
3. インターネット ゾーンのセキュリティ レベルを［高］に設定します。これにより、信頼していないコンピュータからはご使用のコンピュータが認識されなくなります。45 ページの「ゾーンのセキュリティ レベルの設定」を参照してください。

起動に時間がかかる場合の対処

Zone Labs セキュリティ ソフトウェア がシステム起動時にロードされるように設定してある場合、ローカル エリア ネットワークに接続しているコンピュータの起動プロセスが完了するまでに数分を要することがあります。

ほとんどの場合この問題は、コンピュータがスタートアップ プロセスおよびログイン プロセスを完了するにあたってネットワークのドメイン コントローラへのアクセスを必要としているにもかかわらず、コントローラがトラスト ゾーンに含まれていないために Zone Labs セキュリティ ソフトウェア がアクセスをブロックしていることが原因になっています。

この問題を解決するには、ネットワークのドメイン コントローラのホスト名または IP アドレスをトラスト ゾーンに含めます。

インターネット接続

インターネットへの接続に問題がある場合は、次の表のトラブルシューティングのヒントを参照してください。

該当する状況	参照先
インターネットに接続できない	258 ページの「インストール後インターネットに接続できない」
インターネットに接続はできるが、短時間で切断されてしまう	259 ページの「ISP ハートビート メッセージの許可」
インターネット接続共有（ICS）クライアントのコンピュータを使っていて､インターネットに接続できない	260 ページの「ICS クライアントを介した接続」
インターネットの接続にプロキシ サーバを使用していて、インターネットに接続できない	260 ページの「プロキシ サーバを介した接続」
プログラム警告に「自動プログラム サーバに接続できませんでした。」というメッセージが表示される	260 ページの「プログラム アドバイス サーバに接続できない」

表 C-3: インターネット接続に関するトラブルシューティング

インストール後インターネットに接続できない

Zone Labs セキュリティ ソフトウェア をインストールした後でインターネットに接続できない場合は、Zone Labs セキュリティ ソフトウェア が問題の原因となっているかどうかをまず判別する必要があります。下記の手順を実行できない場合（**[Zone Labs セキュリティ ソフトウェア をスタートアップ時に起動する]** チェックボックスをオフにできない場合など）は、Zone Labs のテクニカル サポートまたは販売代理店にご連絡ください。

Zone Labs セキュリティ ソフトウェア が接続の問題の原因かどうかを判別するには、次のようにします。

1. **[概要]**|**[設定]** を選択します。
2. [全般] エリアで、**[Zone Labs セキュリティ ソフトウェア をスタートアップ時に起動する]** のチェックボックスをオフにします。

   Zone Labs TrueVector サービス警告ダイアログ ボックス表示されます。
3. **[許可]** をクリックします。
4. コンピュータを再起動し、インターネットへの接続を再度試行します。

接続できる場合：	Zone Labs セキュリティ ソフトウェアの設定が、接続に関する問題の原因である可能性があります。ブラウザにアクセス許可が与えられていることを確認してください。

接続できない場合：	Zone Labs セキュリティ ソフトウェアの設定は、接続に関する問題の原因ではありません。

ISP ハートビート メッセージの許可

インターネット サービス プロバイダ（ISP）は、接続中のダイヤルアップ カスタマに定期的に ハートビート メッセージ を送信し、カスタマの存在を確認します。カスタマの存在が確認できない場合、ISP はそのカスタマが使用している IP アドレスを他のカスタマに提供するために、接続を切断することがあります。

Zone Labs セキュリティ ソフトウェア はデフォルトでは、ハートビート メッセージで一般的に使用されるプロトコルをブロックします。そのため、インターネットとの接続が切断される可能性があります。これを防止するには、そのメッセージ発信元のサーバを識別してトラスト ゾーンに追加、または ping メッセージを許可するようにインターネット ゾーンを設定する必要があります。

ハートビート メッセージの送信元の識別

この方法では、ISP が接続状況を確認するために NetBIOS または *ICMP（インターネット制御メッセージ プロトコル）*のいずれを使用している場合でも対応でき、しかもインターネット ゾーンのセキュリティを「高」に維持したままで行えるため、この方法の使用を推奨します。

ISP が接続状況を確認するために使用しているサーバを識別するには、次のようにします。

1. ISP 側によりインターネットから切断された際に、**[警告とログ]** の **[ログ ビューア]** を選択します。
2. 警告の一覧で、切断時に生成された警告を特定します。
3. [項目の詳細] エリアで、検出された発信元の DNS アドレスを確認します。

   この方法でサーバを識別できない場合は、ISP に問い合わせて、アクセス許可を設定する必要のあるサーバを確認します。
4. サーバの確認後、サーバをトラスト ゾーンに追加します。

53 ページの「トラスト ゾーンへの追加」を参照してください。

Zone Labs セキュリティ ソフトウェア での ping メッセージ許可の設定

ISP が接続状況の確認に ICMP エコー（または ping）メッセージを使用している場合は、Zone Labs セキュリティ ソフトウェア がインターネット ゾーンからの ping メッセージを許可するように設定します。

Zone Labs セキュリティ ソフトウェア で ping メッセージ許可を設定するには、次のようにします。

1. **[ファイアウォール]**|**[メイン]** を選択します。
2. **[インターネット ゾーン]** エリアで **[カスタム]** をクリックします。

3. ［許可： 外部からの Ping (ICMP エコー)］チェックボックスをオンにします。
4. [OK] をクリックします。
5. インターネット ゾーンのセキュリティ レベルを［中］に設定します。

45 ページの「セキュリティ レベルの選択」を参照してください。

ICS クライアントを介した接続

Windows のインターネット接続共有（ICS）オプションやサードパーティの接続共有プログラムを使用していて、インターネットに接続できない場合は、クライアントとゲートウェイのマシンについて Zone Labs セキュリティ ソフトウェア が正しく設定されていることを確認してください。36 ページの「インターネット接続共有（ICS）の有効化」を参照してください。

PC ではなく、サーバやルータのようなハードウェアを使用している場合は、Zone Labs セキュリティ ソフトウェア でインターネット接続共有の設定をしないようにします。

プロキシ サーバを介した接続

プロキシ サーバを介してインターネットに接続していて、インターネットに接続できない場合は、プロキシ サーバの IP アドレスがトラスト ゾーンに含まれていることを確認します。53 ページの「トラスト ゾーンへの追加」を参照してください。

プログラム アドバイス サーバに接続できない

「自動プログラム サーバに接続できませんでした。」というメッセージのプログラム警告が［SmartDefense Advisor］エリアに表示された場合は、インターネット接続が正常に機能していることを確認してください。

- お使いのコンピュータがネットワークまたはモデムに正しく接続されていることを確認します。
- ケーブル モデムまたは DSL を使用してインターネットに接続している場合、その接続サービスが一時的に中断している可能性があります。
- 活動中の設定がある場合には、通常、後で再試行すると問題が解消されます。
- お使いのブラウザを起動します。インターネット上のいかなるサイトにも接続できない場合は、Zone Labs セキュリティ ソフトウェアがインターネット アクセスをブロックするよう設定されている可能性があります。ブラウザに適切なアクセス許可を設定することで、問題が解決されます。

上記のケースのいずれにも該当しない場合は、サーバが一時的に利用できない状態となっている可能性があります。

IM セキュリティ

IM セキュリティ機能の使用に問題がある場合は、次の表のトラブルシューティングのヒントを参照してください。

該当する状況	参照先
アクティブな IM プログラムが［保護ステータス］テーブルに表示されない	261 ページの「IM プログラムがステータスに表示されない」

表 C-4: IM セキュリティの問題に関するトラブルシューティング

IM プログラムがステータスに表示されない

実行中のインスタント メッセージング プログラムが［IM セキュリティ］パネルの［保護ステータス］テーブルに表示されない場合は、インスタント メッセージング プログラムを一度終了してから再起動してください。

この問題は、インスタント メッセージング プログラムと Zone Labs セキュリティ ソフトウェアの双方がスタートアップ時に起動するよう設定されている場合に発生することがあります。今後この問題が発生しないようにするには、お使いのインスタント メッセージング プログラムを手動で起動できるように設定を変更します。

アンチウイルス

アンチウイルス ソフトウェアの使用に関する問題がある場合は、次の表のトラブルシューティングのヒントを参照してください。

該当する状況	参照先
アンチウイルス機能が使用できない	262 ページの「アンチウイルス機能のインストールに関する問題」
アンチウイルス モニタリング機能が使用できない	262 ページの「アンチウイルス モニタリング警告」
製品の競合に関する警告が表示される	263 ページの「アンチウイルス製品同士の競合の解決」
アンチウイルス機能、または IM セキュリティ機能を有効にできない	263 ページの「メール スキャンまたは IM セキュリティが使用できない」

表 C-5: Zone Labs アンチウイルスの問題に関するトラブルシューティング

アンチウイルス機能のインストールに関する問題

インストール時に問題が生じた場合、インストール後にアンチウイルス機能が使用できないことがあります。この問題は、インストール時に av.dll ファイルが正常に登録されなかった場合、または、アンチウイルスのアップデート・オペレーション中にエラーが発生した場合に起こります。このような場合は、「必要な操作: ZoneAlarm Security Suite (または ZoneAlarm Anti-virus) の再インストール」というメッセージが表示されます。

この問題を解決するには、Zone Labs セキュリティ ソフトウェアを終了して、インストール プログラムを再度実行してください。インストール時には、**[クリーン インストール]** ではなく、**[アップグレード]** を選択します。製品の再インストール後も [アンチウイルス] パネルが正常に動作しない場合は、製品をアンインストールしてからクリーン インストールを試行してください。これらの方法を使用してもこの問題が解決できない場合は、Zone Labs のカスタマ サポートにお問い合わせください。

アンチウイルス モニタリング警告

アンチウイルス モニタリング警告は、お使いのコンピュータにおいてアンチウイルス保護が不十分であることをユーザに通知します。アンチウイルス機能がオフになっている場合や、アンチウイルス署名ファイルが最新ではない場合、または、いかなるアンチウイルス ソフトウェアも実行していない場合に、この警告が表示されます。

すべてのアンチウイルス製品が監視されるわけではないため、この警告が表示されなければアンチウイルス保護に問題はない、とは限りません。保護の状態を確認するには、アンチウイルス ソフトウェアがインストールさ

れている場合はそれを開いて、アップデートを実行します。有効期限が切れている場合は、使用契約を更新します。

アンチウイルス製品同士の競合の解決

他のアンチウイルス製品がインストールされている状態で ZoneAlarm Security Suite を使用すると、Zone Labs Antivirus を使用する前に他のアンチウイルス製品をアンインストールする必要があることを示す競合の警告が表示されます。警告には、検出されたアンチウイルス ソフトウェア製品が表示されるほか、ZoneAlarm Security Suite がそれらのソフトウェアを自動的にアンインストールできるかどうか、または手動でアンインストールする必要があるかどうかが表示されます。表示された製品を自動的にアンインストールできない場合は、各ソフトのベンダのマニュアルで、製品をアンインストールする方法について確認してください。

メール スキャンまたは IM セキュリティが使用できない

Zone Labs Antivirus ソフトウェアのメール スキャン オプション、または IM セキュリティ機能を有効にすることができない場合は、ZoneAlarm Security Suite と互換性のない Layered Service Provider (LSP) テクノロジを使用する製品がインストールされている可能性があります。この問題を解決するには、競合している製品をアンインストールする必要があります。

競合が発生すると、C:¥Windows¥Internet Logs ディレクトリに lspconflict.txt というファイルが作成されます。このファイルには、競合の原因となった製品の名前が含まれています。原因となった製品を手動で削除、または、lsupport@zonelabs.com にこのファイルを添付したメールを送信してください。各製品のアンインストール方法については、それぞれのベンダのマニュアルを参照してください。

サードパーティのソフトウェア

多くの頻繁に使用されるプログラムでは、インターネット アクセスが自動的に設定されます。インターネット アクセスは自動的に設定できても、サーバ アクセス権も必要になるプログラムは少なくありません。

Zone Labs セキュリティ ソフトウェア が自動的に認識して設定できないプログラムを使用している場合は、手動で許可を設定する必要があります。Zone Labs セキュリティ ソフトウェア . Zone Labs セキュリティ ソフトウェアとともに使用するプログラムの設定方法については、次のセクションを参照してください。

アンチウイルス

アンチウイルス ソフトウェアがアップデートを受信するためには、トラスト ゾーンのアクセス許可が必要になります。

自動アップデート

アンチウイルス ソフトウェアのベンダから自動的にアップデートを受信するには、アップデートを含むドメイン（たとえば、update.avsupdate.com）をトラスト ゾーンに追加します。53 ページの「トラスト ゾーンへの追加」を参照してください。

メール保護

Zone Labs セキュリティ ソフトウェアの MailSafe 機能が、アンチウイルス ソフトウェアのメール保護機能と競合する場合があります。このような場合、Zone Labs セキュリティ ソフトウェアとアンチウイルスの設定を調整し、アンチウイルスと Zone Labs セキュリティ ソフトウェアの両方の保護を受けられるようにします。

アンチウィルス ソフトウェアを設定するには：

1. アクセスする全ファイルをスキャンし、メールのスキャン オプションは無効にするようにアンチウイルス プログラムを設定します。
2. Zone Labs セキュリティ ソフトウェア で、インバウンド MailSafe 保護を有効にします。

   129 ページの「インバウンド MailSafe 保護の有効化」を参照してください。

3. 隔離された MailSafe 添付ファイルに対する警告表示を無効にします。

178 ページの「特定の警告の表示または非表示」を参照してください。

この設定を使用すると、MailSafe は疑いのあるメールの添付ファイルを隔離し、そのファイルを開こうとした際に警告を表示します。添付ファイルを開くことを選択した場合に、アンチウィルス ソフトウェアがスキャンを行ないます。

ブラウザ

ブラウザが正常に機能するには、インターネット ゾーンおよびトラスト ゾーンのアクセス許可が必要となります。アクセス許可を与える前に、ブラウザのセキュリティをどのように設定すれば最適な保護機能が実現されるかを理解し、さらに、ブラウザに最新のサービス パックがインストールされていることを確認してください。

ブラウザにアクセス許可を与えるには、次のいずれかの操作を行います。

- プログラムに直接アクセス許可を与えます。89 ページの「プログラムのインターネット アクセスの許可」を参照してください。
- ブラウザのプログラム警告が表示されたら、[**許可**] をクリックします。

Internet Explorer

Windows 2000 を使用している場合、サービスおよびコントローラ アプリケーション（一般的なファイル名は、services.exe）に、インターネットへのアクセス権限を与える必要が生じることがあります。

サービスとコントローラ アプリケーションにインターネット アクセス許可を与えるには、次のようにします。

1. [**プログラム コントロール**]|[**プログラム**] を選択します。
2. [プログラム] カラムで、[**サービスおよびコントローラ アプリケーション**] を選択します。
3. [アクセス] カラムで、ショートカット メニューから [**許可**] を選択します。

Netscape

バージョン 4.73 以降の Netscape Navigator は、Zone Labs セキュリティ ソフトウェア と一緒に実行しても通常は何の問題も起きません。バージョン 4.73 以降の Navigator を使用していて、Zone Labs セキュリティ ソフトウェア がアクティブな際に Web サイトへのアクセスに問題が生じる場合

は、ブラウザの設定でプロキシ アクセスが設定されていないことを確認します。

チャット プログラムおよびインスタント メッセージング プログラム

チャットおよびインスタント メッセージング プログラム（たとえば、Instant Messenger など）は、正常に動作するためにサーバ許可を必要とする場合があります。

チャット プログラムにサーバ許可を与えるには、次のようにします。

- プログラムにより生成されたサーバ プログラム警告に対して［許可］を選択します。
- プログラムにサーバ許可を与えます。

90 ページの「プログラムのサーバ動作の許可」を参照してください。

チャット ソフトウェアを設定して、確認メッセージが表示されないファイル転送を拒否することをお勧めします。チャット プログラムでのファイル転送は、ワーム、ウイルス、およびトロイの木馬などの悪意のあるプログラムを配布する手段となります。チャット プログラムで最大限のセキュリティを実現する設定方法については、チャット ソフトウェアのベンダのヘルプ ファイルを参照してください。Zone Alarm Security Suite を使用している場合は、IM セキュリティ レベルを「高」に設定して、ファイル転送をブロックします。

メール プログラム

メール プログラム（たとえば、Microsoft Outlook）を使用してメールの送受信を行うには、メール サーバが含まれるゾーンに対するアクセス許可をプログラムに与える必要があります。さらに、メール クライアント ソフトウェアのなかには、サーバ許可を必要とする複数のコンポーネントを含むものもあります。たとえば、Microsoft Outlook では、ベース アプリケーション（OUTLOOK.EXE）とメッセージ サブシステム スプーラ（MAPISP32.exe）の両方にサーバ許可が必要となります。

メール サーバをインターネット ゾーンへ含み、メール プログラムにインターネット ゾーンに対してアクセス許可を与えることもできますが、メールサーバをトラスト ゾーン含んでトラスト ゾーンに対してのみアクセス許可を制限するとより安全です。メール クライアントにトラスト ゾーンへの

アクセス許可を付与したら、リモート メール サーバ（ホスト）をトラスト ゾーンに追加します。

プログラムにトラスト ゾーンへのアクセス許可またはサーバ許可を与える方法については、75 ページの「手動によるプログラム許可の設定」を参照してください。

ホストをトラスト ゾーンに追加する方法については、52 ページの「通信ソースの管理」を参照してください。

インターネット留守番電話プログラム

インターネット留守番電話プログラム（CallWave など）を Zone Labs セキュリティ ソフトウェア とともに使用するには、次の操作を行います。

- プログラムにインターネット ゾーンへのサーバ許可およびアクセス許可を与えます。
- ベンダ サーバの IP アドレスをトラスト ゾーンへ追加します。

サーバの IP アドレスは、ベンダのテクニカル サポートに問い合わせてください。

- インターネット ゾーンのセキュリティ レベルを［中］に設定します。

ファイル共有プログラム

Napster、Limewire、AudioGalaxy、または Gnutella クライアント ソフトウェアなどのファイルの共有プログラムを Zone Labs セキュリティ ソフトウェア とともに使用するには、インターネット ゾーンのサーバ許可が必要となります。

FTP プログラム

FTP（ファイル転送プロトコル）プログラムを使用するには、FTP クライアント プログラムおよび Zone Labs セキュリティ ソフトウェア で、以下の設定変更が必要となる場合があります。

- FTP クライアントの passive モードまたは PASV モードを有効にする

  これにより、双方向のコミュニケーションに同じポートが使用されます。PASV が有効でない場合、Zone Labs セキュリティ ソフトウェア は、データ転送のために新しいポートに接続しようとする FTP サーバをブロックする場合があります。

- 使用する FTP サイトをトラスト ゾーンに追加する

■ FTP クライアント プログラムにトラスト ゾーンに対するアクセス許可を与える

トラスト ゾーンへの追加方法およびプログラムにアクセス許可を付与する方法の詳細については、47 ページの「アドバンス セキュリティ オプションの設定」を参照してください。

ゲーム

Zone Labs セキュリティ ソフトウェア を使用している場合にインターネット上でゲームを行うには、次の設定の変更が必要となる場合があります。

プログラム許可

インターネット ゲームが正常に機能するには、インターネット ゾーンへのアクセス許可やサーバ許可が必要となります。

ゲーム プログラムを原因とするプログラム警告で［許可］を押すと、簡単にアクセス許可を付与することができます。しかし、多くのゲームで「排他的な」フル スクリーン モードが使用されているため、警告に気付かないことがあります。次のいずれかの方法で、この問題を解決できます。

■ ウィンドウ表示でゲームを行う

このようにすれば、デスクトップよりも小さいウィンドウでゲームを実行している場合に、警告に気付くことができます。警告が表示されてもマウスがゲームにロックされていて応答できない場合は、キーボードの Windows ロゴ キーを押します。

ゲーム プログラムにインターネット アクセスを付与した後、ゲームをリセットし、フル スクリーンで実行します。

■ ソフトウェア レンダリング モードの使用

レンダリング モードを「ソフトウェア レンダリング」に変更すると、ゲーム画面の前面に警告を表示することができます。ゲームにインターネット アクセスを許可した後で、最適なレンダリング デバイスに設定を戻すことができます。

■ Alt+Tab を使用する

Alt+Tab を押して、画面を Windows に戻します。これにより、ゲームを実行したまま、警告に応答することができます。インターネット アクセスを許可したら、**Alt+Tab** を押してゲームを再開します。

ノート 最後のメソッドは、特に Glide または OpenGL を使用している場合に、いくつかのアプリケーションをクラッシュさせる可能性があります。しかし、この問題は次にゲームを実行する際には発生しません。Alt+Tab の代わりに Alt+Enter を使用できる場合もあります。

セキュリティ レベル／ゾーン

インターネット ゲーム、特に、Java、アプレット、またはその他の Web ベースのポータル機能を使用するインターネット ゲームは、インターネット ゾーンのセキュリティ レベルを「高」に設定すると、正確に動作しない場合があります。また、「高」セキュリティ設定では、リモート ゲーム サーバがご使用のコンピュータを「認識」できなくなります。この問題を解決するには、次の操作を行います。

- インターネット ゾーンのセキュリティを「中」に変更する。または
- 接続するゲーム サーバの IP アドレスをトラスト ゾーンに追加します。ゲーム メーカーのマニュアルにはサーバの IP アドレスやホスト名が記載されています。

ホストまたは IP アドレスをトラスト ゾーンへ追加する方法は、53 ページの「トラスト ゾーンへの追加」を参照してください。

ゲーム サーバを信頼するということは、ゲームをしている他のプレイヤーを信頼するということです。Zone Labs セキュリティ ソフトウェア は、信頼された環境内のゲーム プレイヤーによるアタックからは、ご使用のコンピュータを保護しません。最適な保護を得るために、ブラウザのセキュリティ設定を理解し、ブラウザに最新のサービス パックがインストールされていることを確認してください。

リモート コントロール プログラム

ご使用のコンピュータが、PCAnywhere または Timbuktu などのリモート アクセス システムのホストまたはクライアントである場合、次のようにします。

- 接続するホストまたはクライアントの IP アドレスをトラスト ゾーンに追加します。53 ページの「トラスト ゾーンへの追加」を参照してください。
- リモートでアクセスしているネットワークのサブネットをトラスト ゾーンに追加します。53 ページの「トラスト ゾーンへの追加」を参照してください。

■ 動的な IP アドレスがリモート マシンに割り当てられている場合、DHCP サーバ アドレスまたはアドレス範囲をトラスト ゾーンに追加します。

コントロールすることができないネットワーク（企業や大学の LAN）上にリモート コントロール クライアントまたはホストがある場合、ネットワーク周辺のファイアウォールまたはその他の機能によって接続が妨げられることがあります。上記の操作を行っても接続できない場合は、ネットワーク管理者に問い合わせてください。

VNC プログラム

VNC および Zone Labs セキュリティ ソフトウェア をともに使用するには、次の操作を行います。

1. サーバとビューア（クライアント）マシンの両方で、次のいずれかの操作を行います。

   ← リモート アクセスに使用するビューア（クライアント）の IP アドレスまたはサブネットが分かっていて、それらが常に同じである場合は、トラスト ゾーンにその IP またはサブネットを追加します。53 ページの「トラスト ゾーンへの追加」を参照してください。

   ビューアの IP アドレスが分からない、または IP アドレスが今後変更されることがある場合は、プログラムにトラスト ゾーンとインターネット ゾーンのアクセス許可およびサーバ許可を与えます。83 ページの「新しいプログラムのアクセス許可の設定」を参照してください。

   ビューア マシン上で VNCviewer により指示されたら、サーバ マシン名または IP アドレスを入力し、次にパスワードを入力します。接続が可能になります。

サーバ許可およびアクセス許可を与えて VNC アクセスを有効にする場合は、セキュリティを維持するため、VNC パスワードを設定して使用するようにします。アプリケーションにインターネット ゾーンへの許可を与えるのではなく、可能であればサーバおよびビューアの IP アドレスをトラスト ゾーンに追加することをお勧めします。

2. ビューア（クライアント）マシン上で、VNCviewer を実行し、サーバ マシンに接続します。「待ち受けモード」として実行しないでください。

Telnet

Telnet を介してリモート サーバにアクセスするには、サーバの IP アドレスをトラスト ゾーンに追加します。

ストリーミング メディア プログラム

RealPlayer、Windows Media Player、QuickTime など、オーディオおよびビデオのストリーミングを行うアプリケーションを Zone Labs セキュリティ

ソフトウェア とともに使用するには、インターネット ゾーンのサーバ許可が必要となります。

プログラムにサーバ許可を付与する方法については、90 ページの「プログラムのサーバ動作の許可」を参照してください。

Voice over IP プログラム

Voice over IP (VoIP) プログラムと Zone Labsセキュリティ ソフトウェアをともに使用するには、次の操作の一方または両方を行います。これは、プログラムにより異なります。

1. VoIP アプリケーションにサーバ許可およびアクセス許可を与えます。
2. VoIP プロバイダのサーバをトラスト ゾーンに追加します。サーバの IP アドレスについては、VoIP プロバイダのカスタマ サポートにお問い合わせください。

Web 会議プログラム

Microsoft NetMeeting などの Web 会議プログラムで問題が生じる場合は、次の操作を行ってください。

1. 会議の開催時に接続するドメインまたは IP アドレスをトラスト ゾーンに追加します。53 ページの「トラスト ゾーンへの追加」を参照してください。
2. 会議プログラムの「リモート デスクトップ共有 (Remote Desktop Sharing)」オプションを無効にします。

付録 D
プログラム動作

この付録では、疑わしい動作または危険な動作を実行するプログラムに対する許可または拒否を判断するためのガイダンスを提供します。

- 274 ページの「疑わしい動作」
- 275 ページの「危険な動作」

疑わしい動作

次の表は、疑わしい動作の警告が表示された場合の対処法に役立つ情報を提供します。ここにリストされた情報は参照専用です。正当なプログラムを使用し、次に表示されるアクションを実行する必要があります。疑わしいプログラム動作を許可または拒否するかは、個々の状況に応じて判断する必要があります。

検出された動作	動作の意味	対応方法
スタートアップ ディレクトリの変更	プログラムはコンピュータが起動するたびに自分自身を実行するように設定しています。	プログラムをインストールしていない場合は、悪意のあるプログラムの可能性があるため、このアクションを拒否する必要があります。
ブラウザの検索デフォルトの変更	デフォルトのブラウザ検索が変更されています。	現在、ブラウザの検索機能を変更していない場合は、このアクションを拒否する必要があります。
ブラウザのページ デフォルトの変更	デフォルトのホーム ページが変更されています。	ホーム ページを変更していない場合は、このアクションを拒否する必要があります。
ドライバのアンロード	あるプログラムが別のプログラムのドライバをアンロードしようとしています。	この動作が行われる正当な理由はありません。このアクションを拒否する必要があります。

表 D-1: 疑わしい動作のガイド

危険な動作

次の表は、危険な動作の警告が表示された場合の対処法に役立つ情報を提供します。ここにリストされた情報は参照専用です。正当なプログラムを使用し、次に表示されるアクションを実行する必要があります。

検出された動作	動作の意味	対応方法
DDE (Dynamic Data Exchange) 入力の伝送	プログラムが別のプログラムに DDE 入力を送信しようとしています。これにより、プログラムがインターネットにアクセスできるようになったり、情報が漏洩したりする可能性があります。	この動作は多くの場合、URL を Internet Explorer で開くために使用されます。この動作を実行しているアプリケーションが既知で信頼できる場合、動作を許可しても安全と考えられます。そうでない場合は、[拒否] をクリックしてください。
Windows メッセージの送信	あるプログラムが別のプログラムにメッセージを送信しようとしています。	あるプログラムが、別のプログラムに特定の機能を実行させようとしている可能性があります。別のプログラムとの通信を必要とするソフトウェアをインストールしている場合を除き、このアクションを拒否する必要があります。
あるプログラムが別のプログラムを抹消しようとしています。	あるプログラムが別のプログラムを終了させようとしています。	あるプログラムが、信頼できるプログラムを抹消しようとしている可能性があります。タスク マネージャを使用してプログラムやプロセスを終了させた直後である場合や、コンピュータの再起動を必要とするソフトウェアをインストールした直後である場合を除き、このアクションを拒否する必要があります。
オープンされたプロセス / スレッドの呼び出し	あるプログラムが別のプログラムを制御しようとしています。システム アプリケーションがこの動作を行うことは、正当な動作です。	この動作を実行しているプログラムを信頼できる場合を除き、このアクションを拒否する必要があります。

表 D-2: 危険な動作のガイド

検出された動作	動作の意味	対応方法
キーボードとマウスの入力のモニタリング	あるプログラムが、キーボードとマウスの入力をモニタリングしようとしています。	ナレーション ソフトウェアなどを機能させるために、このアクティビティのモニタリングを必要とする特殊なプログラムを実行していない場合は、このアクションを拒否する必要があります。
キーボードとマウスの入力のリモート コントロール	プログラムはキーボードとマウスのリモート コントロールを試みています。	PC Anywhere または VNC などのリモート アクセス ソフトウェアを実行していない場合は、このアクションを拒否する必要があります。
ドライバのインストール	プログラムは *ドライバ* をロードしようとしています。ドライバがロードされると、プログラムはコンピュータ上で任意の処理を実行できるようになります。	アンチウイルス、アンチスパイウェア、ファイアウォール、VPN、その他のシステム ツールをインストールしていない場合は、このアクションを拒否する必要があります。
*物理メモリ*の変更	プログラムは別のプログラムが所有する情報の変更または読み取りを試みている可能性があります。	ゲーム、ビデオ、またはシステム ユーティリティ ソフトウェアを実行していない場合は、このアクションを拒否する必要があります。
プログラムまたはシステム サービスへのコードの挿入	プログラムやサービスを無効にする可能性のあるコードを、他のプログラムに挿入しようとしています。	プログラムの形式や動作を変更する高度に特殊化されたソフトウェアを実行していない場合は、このアクションを拒否する必要があります。
ネットワーク パラメータの変更	プログラムはネットワーク設定を変更しようとしています。危険な Web サイトへの誘導および Web トラフィックのモニタリングを行う可能性があります。	TCP/IP チューニング ソフトウェアを実行していない場合は、このアクションを拒否する必要があります。
適切なプログラムからの不明または不正プログラムの起動	プログラムは別のプログラムを変更しようとしています。	使用中のプログラムが別のプログラムを開始する理由（ブラウザへのリンクを含む Word 文書や他のプログラムへのリンクを含む IM プログラムなど）がない場合は、このアクションを拒否する必要があります。

表 D-2: 危険な動作のガイド

検出された動作	動作の意味	対応方法
システム レジストリへのアクセス	プロセスがレジストリ設定を書き替えようとしています。	通常、この動作は自動的にブロックされます。プログラム コントロールを手動モードに設定している場合は、このアクションを拒否してください。
ランキーの削除	プログラムがランキー エントリを削除しようとしていました。	プログラムがスタートアップ時に起動するように設定されていて、それがキャンセルされた場合、このプログラムはランキーを削除します。これ以外の場合、このアクションを拒否する必要があります。
ZoneAlarm プログラムの変更	あるプログラムが ZoneAlarm プログラムを変更して、おそらく ZoneAlarm プログラムの実行や製品のアップデートを阻止ようとしています。	ZoneAlarm クライアントのアップグレード中である場合を除き、このアクションを拒否してください。

表 D-2: 危険な動作のガイド

用語集

3DES
Triple Data Encryption Standard（三重のデータ暗号化規格）の略。168 ビット キーを使用する標準化された対称キー暗号化形式。3DES は、以前の 56 ビット DES 暗号化規格をさらに強化したものです。

ACTIVEX コントロール
Microsoft が開発した、Web ブラウザによって自動的にダウンロードされ実行される一連のテクノロジー。ActiveX コントロールは、Windows オペレーティング システムのすべてにアクセスできるため、ユーザのマシン上にあるソフトウェアやデータを破損する可能性があります。

BLUE COAT
Blue Coat はソフトウェア開発およびアプリケーション サービス会社で、インターネット利用とアクティビティのフィルタ、監視、報告を行います。ZoneAlarm Pro のペアレント コントロール機能は、Blue Coat のコンテンツ カテゴリを使ってユーザが訪問する Web サイトへのアクセスを許可するか、ブロックするかを決定します。

COOKIE
コンテンツのカスタマイズ、ユーザ情報の保存、ユーザのインターネット アクティビティの記録を行うため、Web サイトで使用される小規模なデータ ファイル。多くの場合 Cookie は正当な目的で使用されますが、Cookie によってはユーザの許可なく個人情報が漏洩することもあります。

COOKIE コントロール
コンピュータ上に Cookie が保管されるのを防ぐプライバシー機能。

DES
データ暗号化規格の略。56 ビット キーを使用する一般的な対称キー暗号化形式。DES からより強力な 3DES に変更されました。

DHCP（動的ホスト構成プロトコル）
動的 IP アドレスをサポートするプロトコル。ISP は静的 IP アドレスを提供する代わりに、ユーザがログオンするたびに異なる IP アドレスを割り当てることがあります。これにより、比較的少数の IP アドレスで多くのカスタマにサービスを提供することができま

す。

DHCP（動的ホスト構成プロトコル）ブロードキャスト / マルチキャスト
動的 IP アドレスを使用しているネットワーク上のクライアント コンピュータにより使用されるメッセージの一種。コンピュータがオンラインになり IP アドレスが必要な場合、コンピュータはブロード キャスト メッセージをネットワーク上の DHCP サーバに送信します。DHCP サーバがブロードキャスト メッセージを受信すると、コンピュータに IP アドレスを割り当てます。

DLL（ダイナミック リンク ライブラリ）
Windows アプリケーションが動的に（すなわち必要に応じて）アクセスできる、関数のライブラリ。

DNS（ドメイン ネーム サーバ）
ホスト名またはドメイン名（例、www.yoursite.com）をインターネット アドレス（例、123.456.789.0）に変換するためにインターネット上で通常使用されるデータ クエリ サービス。

HTTP REFERRER ヘッダ フィールド
「参照元ドキュメント」についての情報を含む Web ページを表示する、メッセージのオプション フィールド。適切に使用すると、Web サイトの管理者がサイトを管理する上で役立ちます。誤った使い方をすると、IP アドレス、ワークステーション名、ログイン名、また場合によっては（ずさんな運営の E コマース サイトなどにおいて）クレジット カード番号の漏洩につながります。[Cookie] タブで［プライベート ヘッダ情報を削除する］を選択することにより、このヘッダ フィールドで個人情報が転送されるのを防ぐことができます。

ICMP（インターネット制御メッセージ プロトコル）
エラー コントロールおよび情報メッセージをサポートする、インターネット プロトコルの拡張。「ping」メッセージは、インターネット接続をテストするために使用される一般的な ICMP メッセージです。

ICS（インターネット接続共有）
ICS とは Windows オペレーティング システムで提供されているサービスで、ネットワークに接続している複数のコンピュータが単一の接続を共有してインターネットに接続できるようにするものです。

INDEX.DAT
Index.dat ファイルには Temporary Internet、Cookies、および History フォルダ内の全ファイルのコピーが保管されます。これらのファイルを削除した後も、コピーは保管されます。

IP アドレス
電話ネットワーク上の電話を識別するために電話番号が使用されるように、インターネット上でコンピュータを識別するために使用さ

れる数字。通常、ピリオドで区切った 0 ～ 255 の 4 組の数字で表示されるアドレスです。たとえば、172.16.100.100 のような形式になります。

IP アドレスが常に同じ場合もありますが、インターネット サービス プロバイダ（ISP）が、動的ホスト構成プロトコル（DHCP）を使用して、インターネットに接続するたびにコンピュータへ異なる IP アドレスを割り当てる場合もあります。ただし、インターネット サービス プロバイダ（ISP）が、Dynamic Host Configuration Protocol（DHCP）を使用して、インターネットに接続するたびにコンピュータへ異なる IP アドレスを割り当て場合もあります。

ISP（インターネット サービス プロバイダ）
インターネットへのアクセスを提供する会社。ISP は、ダイヤルアップ（モデムによる標準電話線を介した接続）、高速デジタル加入者線（DSL）、およびケーブル モデムを含む、さまざまなインターネット接続を消費者および企業に提供します。

JAVA アプレット
Java で記述されたインターネット ベースの小規模なプログラムで、Web サイトの HTML ページに埋め込まれており、ブラウザ上で実行することができます。

JAVASCRIPT
Web サイト上でよく見られるインタラクティブ コンテンツを可能にする、一般的なスクリプト言語。最も広く使用されている JavaScript 機能には、［戻る］や［履歴］リンク、マウスでポイントすると変化する画像、ブラウザ ウィンドウの開閉などがあります。JavaScript は非常に一般的であり、その用途の大半は無害なことから、Zone Labs セキュリティ ソフトウェアのデフォルト設定では、JavaScript は許可されています。

キーロガー
スパイウェアの形態の 1 つで、コンピュータ上のキーストロークを記録し、多くの場合、データをリモート サーバに送信します。クレジット カード番号やその他の重要な個人情報など、キーボードを使用して入力されたテキストがキーロギング プログラムによって収集され、ID 盗用される可能性があります。

MD5 署名
ファイルの整合性の確認に使用される、デジタルな「フィンガープリント」。何らかの方法でファイルが変更された場合（たとえば、ハッカーによりプログラムが改変された場合）、MD5 署名も変更されます。

MIME オブジェクト
メール メッセージに統合された、画像、サウンド ファイル、またはビデオ ファイルなどのオブジェクト。MIME は、Multipurpose Internet Mail Extensions（多目的インターネット メール拡張仕

様）の略です。

NetBIOS（ネットワーク基本入出力システム）
ローカル ネットワーク内で、異なる複数のコンピュータ上のアプリケーションが通信することを可能にするプログラム。デフォルトでは、Zone Labs セキュリティ ソフトウェア は、トラスト ゾーンでの NetBIOS 通信を可能にし、インターネット ゾーンではこれをブロックします。これにより、インターネット上で攻撃を受けやすい NetBIOS の脆弱性から保護しながら、ローカル ネットワーク上ではファイルの共有を可能にします。

OpenSSL
OpenSSL は、Eric A. Young と Tim J. Hudson によって開発された SSL ライブラリに基づく、オープン ソースのセキュリティ プロトコルです。

PING
特定のコンピュータがインターネットに接続しているかどうかを確認するために使用される ICMP メッセージ（正式には「ICMP エコー」）の一種。小さいユーティリティ プログラムが、単純な「エコー要求」メッセージを目的の IP アドレスに送信し、応答を待ちます。そのアドレスのコンピュータは、メッセージを受信すると「エコー」を送り返します。インターネット プロバイダによっては、カスタマが接続しているかどうか確認するために定期的に「ping」を送信する場合があります。

SHA1
データのハッシュを生成するために使用されるアルゴリズム。

SmartDefense Advisor
Zone Labs SmartDefense Advisor は、警告の原因を即座に分析するオンライン ユーティリティで、プログラム警告に対して［許可］または［拒否］のどちらの答えを選択すべきか決定する際に役立ちます。SmartDefense Advisor を使用するには、警告のポップアップで［詳細情報］ボタンをクリックします。Zone Labs セキュリティ ソフトウェア によって、その警告に関する情報が SmartDefense Advisor に送信されます。SmartDefense Advisor は、警告に関する説明、およびセキュリティの確保に必要な対策についてのアドバイスなどを返信します。

TCP（伝送制御プロトコル）
TCP/IP ネットワークで使用される主要プロトコルの 1 つ。これにより、データが確実に配信されるようになり、パケットは送信された順序のまま配信されます。

TrueVector セキュリティ エンジン
Zone Labs セキュリティ ソフトウェア セキュリティの主要なコンポーネント。TrueVector エンジンは、インターネット通信を調査

し、セキュリティ ルールを施行します。

UDP（ユーザ データグラム プロトコル）
IP ネットワーク上で実行されるコネクションレスのプロトコルで、主にネットワークを介したメッセージの配信に使用されます。

WEB バグ
通常 1x1 ピクセルのイメージ ファイル。このファイルを含んだページ（または HTML 形式のメール）への訪問をモニタリングします。Web バグはユーザがどの広告や Web ページにアクセスしたかを調査するために使用されます。プライバシー コントロールを使用して Web バグをブロックすると、Web バグの場所には空白のボックスが表示されます。

アクセス許可
アクセス許可は、コンピュータ上のプログラムが他のコンピュータと接続することを許可するものです。プログラムが他のコンピュータからの接続要求を「待ち受ける」ことを許可するサーバ許可とは異なります。トラスト ゾーン、インターネット ゾーン、またはその両方について、プログラムのアクセス許可を設定することができます。

アドバンス プログラム コントロール
アドバンス プログラム コントロールは、未知のプログラムが信頼できるプログラムを使用してインターネットにアクセスすることを防ぐ、高度なセキュリティ機能です。

アニメーション広告
動く画像を含む広告。

暗号化
このプロセスは、スクランブルされたデータを送信するため、許可された受信者だけが解読することができます。たとえば、インターネット上で購買が行われたときなど、クレジット カード情報は暗号化を使用してスクランブルされます。

インターネット ゾーン
インターネット ゾーンには、トラスト ゾーンまたはブロックするゾーンに追加されているコンピュータを除く、世界中のすべてのコンピュータが含まれます。

Zone Labs セキュリティ ソフトウェア は、ハッカーからコンピュータを守るために、最も厳しいセキュリティをインターネットゾーンに適用します。一方、トラスト ゾーンの ″中″ セキュリティ設定では、既知および信頼できるコンピュータまたはネットワーク（たとえば、家庭用ネットワーク コンピュータ、またはビジネス ネットワーク）と簡単に通信することが可能となります。

埋め込みオブジェクト
Web ページに組み込まれるサウンド ファイルまたは画像ファイル

などのオブジェクト。

永続 COOKIE
アクセスした Web サイトによってユーザのハードドライブに保存される Cookie。これらの Cookie は、次回同じ Web サイトにアクセスする際に読み出されます。これは便利な機能ですが、同時に、個人情報、コンピュータ情報またはインターネット使用に関する情報がテキスト ファイルで保管されるため、危険性も増加します。

外国語フィルタ
Zone Labs セキュリティ ソフトウェアの迷惑メール フィルタの機能の 1 つ。外国語フィルタは、ヨーロッパ言語以外の言語を含むメールをブロックします。

拡散性
拡散性とは、ウイルスが拡散する可能性を示します。手動によるフロッピー ディスクの共有で拡散するブート セクタ ウイルスには、低レベルの拡散性が割り当てられていますが、自分自身を多数の対象に送信することが可能なワームには、高レベルの拡散性が割り当てられています。

隔離
Zone Labs セキュリティ ソフトウェアの MailSafe は、自動実行コードの可能性があるファイル名の拡張子（たとえば .EXE や .BAT）を持つ受信メールの添付ファイルを隔離します。ファイル名拡張子を変更することで、隔離機能は添付ファイルが検査されずに開かれることを防ぎます。これにより、ハッカーがメールの添付ファイルとして配布するワームやウイルスなどの悪意のあるプログラムから保護されます。

キャッシュ クリーナ
コンピュータから不要なファイルや Cookie の削除を可能にするプライバシー機能です。必要に応じて実行することも、スケジュールを設定して実行することもできます。

協調フィルタ
Zone Labs セキュリティ ソフトウェアの迷惑メール フィルタの機能の 1 つ。協調フィルタリングでは、自分と自分以外の Zone Labs セキュリティ ソフトウェア ユーザから報告された迷惑メールから抽出した情報を使って、不明の発信元からの新しいメッセージがスパムである可能性が判断されます。

ゲートウェイ
ネットワーク上で 2 つの異なる種類のネットワークをリンクするための、ハードウェアとソフトウェアの組み合わせ。たとえば、家庭用または企業内のローカル エリア ネットワーク（LAN）上のコンピュータから、ゲートウェイを使用してインターネットに接続する

ことができます。

広告ブロック
バナー、ポップアップおよびその他の種類の広告をブロックするための Zone Labs セキュリティ ソフトウェアの機能。

高レベルの警告
ハッカー活動が疑われる場合などに生成される警告。高レベルのファイアウォール警告は、上部に赤い帯の付いた警告ポップアップとして表示されます。[ログ ビューア] では、[レベル] カラムから警告の危険レベルが高いかどうかを確認することができます。

コンポーネント
特定のタスクを実行するために大規模なプログラムが必要とする、小規模なプログラムや関数のセット。同時に複数のプログラムによって使用されるコンポーネントもあります。Windows オペレーティング システムでは、さまざまな Windows アプリケーションで使用される多くのコンポーネント DLL (Dynamic Link Libraries) が提供されています。

コンポーネントの学習モード
インストール後、プログラム コントロールが「中」に設定される期間。コンポーネントの学習モードでは、Zone Labs セキュリティ ソフトウェア は、多数の警告を表示してユーザの作業を中断することなしに、頻繁に使用される各コンポーネントの MD5 署名をすばやく学習します。

サードパーティ COOKIE
永続 Cookie の一種で、アクセスした Web サイトではなく、広告主その他のメサードパーティによってコンピュータ上に保存されます。ｷ この Cookie は、一般的にユーザのインターネット動向をサードパーティに報告するために使用されます。追跡 Cookie ともいいます。

サーバ許可
サーバ許可は、コンピュータ上のプログラムが他のコンピュータからの接続要求を「待ち受ける」ことを許可します。これにより、他のコンピュータがご使用のコンピュータとの接続を開始できるようになります。これは、プログラムが他のコンピュータとの通信セッションを開始することを許可するアクセス許可とは異なります。

サーバとして動作
プログラムが他のコンピュータからの接続要求を「待ち受ける」とき、そのプログラムはサーバとして動作します。チャット プログラム、メール クライアント、およびインターネット キャッチホン プログラムなど、いくつかの一般的なプログラムは、正常に動作するためにサーバとして動作する必要が生じることがあります。ただし、一部のハッカー プログラムは、その作者からの指示を待ち受けるためのサーバとして動作します。Zone Labs セキュリティ ソフトウェアは、ユーザがサーバ許可を与えない限り、コンピュータ上

のプログラムがサーバとして動作することを防止します。

自己署名証明書
公開キー証明書。公開キーをバインドする証明書と、証明書に署名するために使用されるプライベート キーは、署名者に所属する同一のキー ペアのコンポーネントです。

情報警告
Zone Labs セキュリティ ソフトウェア がセキュリティ設定に一致しない通信をブロックした際に表示される警告の種類。情報警告に対して、ユーザは対応する必要はありません。

スカイスクレイパー広告
Web ページの側面に沿って垂直に掲載される広告。

スクリプト
ユーザの介入なしで自動的に実行される一連のコマンド。多くの場合、バナー、マウスでポイントすると変化するメニュー、およびポップ-アップ広告などで使用されます。

ステルス モード
Zone Labs セキュリティ ソフトウェア がコンピュータをステルス モードにすると、予期しない通信に対して応答しなくなります。さらに、ユーザのコンピュータの存在が認識されることもありません。これにより、コンピュータ上で許可を持つプログラムが接続を始めるまで、ユーザのコンピュータはインターネット上で他のコンピュータから見えなくなります。

スパム
不特定多数を対象として要求されていないメッセージを送信するなど、メーリング リストや USENET、またはその他のネットワーク通信機能をブロードキャスト媒体であるかのように不適切な方法で使用すること。

製品のアップデート サービス
Zone Labs セキュリティ ソフトウェアの無料アップデートを提供する Zone Labs のサービス。Zone Labs セキュリティ ソフトウェアの購入後 1 年間は無料でご利用いただけます。

セキュリティ レベル
高、中、低の各設定により、ご使用のコンピュータ上で許可される通信の種類を指定します。

セッション COOKIE
ブラウザのメモリ キャッシュに保存される Cookie で、ブラウザ ウィンドウを閉じると同時に消去されます。有効時間が短いため、最も安全な Cookie と言えます。

ダイヤルアップ接続
モデムおよびアナログ電話線を使用したインターネット接続。モデ

ムは、インターネット サービス プロバイダのサイトの電話番号をダイヤルしてインターネットへ接続します。この接続方法は、アナログ モデムを使用せず、電話番号をダイヤルしないデジタル加入者線などの接続方法とは異なります。

中レベルの警告
ハッカーの攻撃ではなく、害のないネットワーク アクティビティが原因と思われる警告。

ドライバ
デバイスをコントロールするプログラム Windows 環境ではたいてい、ドライバに DRV 拡張があります。ドライバはデバイスと、そのデバイスを使用するプログラムのトランスレータの機能を果たします。各デバイスには、自身のみが知る一連の特殊なコマンドがあります。しかし、プログラムがデバイスにアクセスする場合にはたいてい、標準コマンドを使用します。プログラムによる標準コマンドを受けたドライバは、それらのコマンドを該当デバイス用の特殊なコマンドに変換します。

トラスト ゾーン
トラスト ゾーンには、信頼でき、リソースを共有するコンピュータが含まれます。

たとえば、3 台の家庭用 PC が Ethernet ネットワークでリンクしている場合、個々のコンピュータまたはネットワーク アダプタ サブネット全体を Zone Labs セキュリティ ソフトウェアのトラスト ゾーンに含めることができます。トラスト ゾーンのデフォルトである「中」セキュリティでは、ファイルやプリンタなどのリソースをホーム ネットワーク上で安全に共有することができます。そして、「高」セキュリティ設定となっているインターネット ゾーンにハッカーをとどめておくことができます。

トロイの木馬
スクリーン セーバのような便利で害のないプログラムを装った、悪意のあるプログラム。トロイの木馬の中には、コンピュータ上でサーバになりすまし、外部からの接続要求を待ち受けるものがあります。ハッカーがトロイの木馬プログラムへの接続に成功すると、そのコンピュータはハッカーにコントロールされる可能性があります。そのため、信頼できる既知のプログラムに限ってサーバ許可を与えることが重要になります。自動的にリモート アドレスに接続しようとするトロイの木馬もあります。

ハートビート メッセージ
インターネット サービス プロバイダ（ISP）が、ダイヤルアップ接続が使用されていることを確認するために送信するメッセージ。カスタマが不在であると判断すると、ISP はそのカスタマとの接続を切断し、その IP アドレスを他のカスタマに提供します。

破壊性
ウイルスが原因となる破損の程度を示します。破壊性のレベルは、

どの程度、破損を元通りにできるかを示すものです。破壊性が低レベルの場合は、割り込みの度合いは小さく、発生した破損もすべて元通りにできます。破壊性が中レベルまたは高レベルの場合、発生した破損を元通りにすることは不可能であるか、広範囲の割り込みを発生させることを示します。

パケット
ネットワーク通信の単位。インターネットのような「パケット交換方式」のネットワークでは、外部へのメッセージは小さい単位に分けられて送信され、送信先で再度組み立てられます。各パケットには、発信元の IP アドレス、送信先の IP アドレス、およびポート番号が含まれています。

パスロック
インターネット ロックが適用されている場合でも、パスロック許可が与えられているプログラムはインターネットへのアクセスを続けることができます。その他すべてのプログラムに対するアクセス許可およびサーバ許可は、ロックが開かれるまで無効となります。

ハッシュ
ハッシュとは、文字列から計算式によって生成された数値のことで、他のテキストから同一の値が生成される可能性はほとんどありません。ハッシュは、送信されたメッセージが不正に変更されていないことを確認するために使用されます。

バナー広告
Web ページに水平バナーで掲載される広告。

パブリック ネットワーク
ISP と関連するネットワークなどの比較的大きなネットワーク。デフォルトでは、パブリック ネットワークは*インターネット ゾーン* に追加されます。

ブート セクタ ウイルス
コンピュータのハード ドライブ、またはディスク ドライブの一番目のセクタやはじめの数個のセクタに感染する種類のコンピュータウイルスで、ウイルスがドライブやディスクのブートとして動作することを可能にします。

フィッシング
正当な企業または機関になりすまし虚偽のメールを送る行為のこと。フィッシング メールは、不正な目的で使用するために、受信者をだまして個人情報を提供させようとします。

物理メモリ
コンピュータにインストールされたメモリ ハードウェア（通常は RAM）

プライバシー アドバイザ
Zone Labs セキュリティ ソフトウェア が Cookie やモバイル コー

ドをブロックしたことを示す小さな表示。この表示から、特定のページについてこれらをブロックしないように設定できます。

プライベート ネットワーク
家庭用または企業内のローカルエリア ネットワーク (LAN)。デフォルトでは、プライベート ネットワークは*トラスト ゾーン* に加えられます。

プログラム一覧
インターネット アクセスおよびサーバ許可を割り当てることができるプログラムの一覧。一覧は、[プログラム コントロール] パネルの [プログラム] タブに表示されます。プログラムを一覧に追加したり、一覧から削除したりできます。

ブロック ゾーン
ブロック ゾーンには、接触したくないコンピュータが含まれます。Zone Labs セキュリティ ソフトウェア は、お使いのコンピュータとブロック ゾーン内のコンピュータとの通信を阻止します。

プロトコル
データの送受信の標準フォーマット。異なるプロトコルは、異なる目的に使用されます。たとえば、SMTP（簡易メール転送プロトコル）はメール メッセージの送信に使用され、FTP（ファイル転送プロトコル）は各種の大型ファイルの送信に使用されます。各プロトコルは特定のポートに関連付けられています。たとえば、FTP メッセージはポート 21 番を使用します。

平文
クリア テキストは *プレーン テキスト* とも呼ばれ、暗号化されないテキスト形式で送信されるデータです。このデータは暗号化されないため、送信中に傍受されたり、読み取られたりする可能性があります。

ポート
チャネルは TCP または UDP の使用に関連します。ポートの中には標準ネットワーク プロトコルに割り当てられているものがあります。たとえば、HTTP (Hypertext Transfer Protocol) は一般的にポート 80 番を使用します。ポート番号は、0 から 65535 の範囲内です。

ポート スキャン
ハッカーが使用する、インターネット上の保護されていないコンピュータを検索するためのテクニック。ハッカーは自動ツールを使用して指定した IP アドレス範囲のすべてのコンピュータ上のポートをスキャンし、保護されていない「開かれた」ポートを検索します。開かれたポートが見つかると、ハッカーはそのポートを、保護されていないコンピュータに侵入するためのアクセス ポイントとして使用することができます。

ポップ アンダー広告
表示中のウィンドウの背面で、新規のブラウザ ウィンドウに表示される広告。これは、表示中のブラウザ ウィンドウを閉じるまで前面に表示されません。

ポップアップ広告
表示しているウィンドウの前面に「ポップアップ」する新規のブラウザ ウィンドウ内に表示される広告。

メール サーバ
コンピュータ上のメール プログラムがアクセスするリモート コンピュータで、ここからユーザ宛に送信されたメール メッセージが読み出されます。

メッセージ フィルタ
Zone Labs セキュリティ ソフトウェアの迷惑メール フィルタの機能の 1 つ。メッセージ フィルタは発見的ルールを使って、さまざまな種類の迷惑メールに共通した特徴について、メールを分析します。

モバイル コード
Web ページまたは HTML 形式のメールに組み込むことができる実行可能コンテンツ。モバイル コードによりインタラクティブな Web サイトを提供できるようになります。しかし、データの盗難や改変、その他不当な目的のために悪質なモバイル コードが使用されることもあります。

モバイル コード コントロール
アクセスした Web サイト上のアクティブ コントロールおよびスクリプトをブロックすることができる Zone Labs セキュリティ ソフトウェアの機能。モバイル コードはインターネットでは一般的なもので、多くは正当な目的で使用されますが、ハッカーにより悪用される場合もあります。

ワイルド
通常の日常的な操作によって、無防備なユーザのコンピュータ上や、そのようなコンピュータ間で拡散しているウイルスのことです。ワイルド レベルは、そのウイルスに関するカスタマ レポートの数によって示されます。ワイルド レベルが低い場合はカスタマ レポートの数が少ないことを示し、ワイルド レベルが中程度か高い場合は、多数のカスタマ レポートがあることを示します。

索引

コード挿入。危険な動作*を参照*
  種類 276
物理メモリ、変更。危険な動作*を参照*
  種類 276

シンボル

.zl6 ファイル拡張子 147

A

Alt 67
Amazon 保護ファイル、作成 26
AOL
  インスタント メッセージ、使用 266
  エキスパート ルール 67
  プライバシー サイト一覧 156
AOL インスタント メッセンジャ 208
Authentication Header (AH) Protocol（認証ヘッダ プロトコル）37

B

Blue Coat 198, 199
Blue Coat、前述 199

C

Cerberian、前述 198
Cookie 120
  ブロック 150, 157–158
  保持および削除 165
  有効期限日の設定 158
Cookie コントロール
  概要 150
Cookie の保持 166
CreateProcess 91

D

DefenseNet 7
DHCP（動的ホスト構成プロトコル）メッセージ
  デフォルトのポート許可 56
  曜日 / 時間グループ 67
  リモート コントロール プログラム 270
Dynamic Real-time Rating (DRTR) 200

E

eBay 保護ファイル、作成 26
eBay、ブロック 203
Encapsulating Security Payload (ESP) protocol（暗号ペイロード プロトコル）
  VPN プロトコル 37, 49
Eudora、感染したメール 147

F

FireWire 49
FTP
  プログラム、使用 267
  プロトコル、エキスパート ルールへの追加 66

G

Generic Routing Encapsulation (GRE) protocol（ルーティングのカプセル化プロトコル）
  VPN プロトコル 37, 40
  前述 49

H

Hotmail、特別なフォルダ 135, 144
Hypertext Transfer Protocol (HTTP)
  エキスパート ファイアウォール ルール 67

I

ID ロック 187–196
  myVAULT も*参照*
  概要 188
  ステータスのモニタリング 190
ID ロック警告 239
ie3.proxy.aol.com 156
IGMP
  エキスパート ルール 59, 97
  デフォルトのポート許可 56
IMAP4
  エキスパート ルール 66
IM セキュリティ
  概要 208–214
Index.dat ファイル、削除

Internet Explorer
アクセス許可の付与 265
キャッシュ、削除 166
削除オプションの設定 165
プライバシー保護 152
Internet Key Exchange (IKE) protocol (インターネット鍵交換プロトコル)
VPN プロトコル 37
IP Security (IPSec) protocol (IP セキュリティ プロトコル)
VPN プロトコル 37
IP アドレス
Zone Labs への送信時の非表示 25
エキスパート ルール 59
通信ソースの一覧 52
トラスト ゾーンへの追加 35, 36, 53
ネットワークの種類の判別 32, 33
IP アドレスの範囲
エキスパート ファイアウォール ルール 63
トラスト ゾーンへの追加 53
isafe.exe 147
ISP (インターネット サービス プロバイダ)
警告の詳細 172
通信ソースの一覧 52
ハートビート メッセージ 14, 259

J

JavaScript
メール保護 128
Java アプレット、ブロック 162

L

Layer 2 Tunneling protocol (L2TP) (Layer 2 トンネリング プロトコル)
VPN プロトコル 37
Lightweight Directory Access protocol (LDAP: 簡易ディレクトリ アクセス プロトコル)
VPN プロトコル 37
lsass.exe 20

M

MailFrontier 138
MailSafe
外部への保護
送信者のアドレス、確認 28
MailSafe 警告 128, 223
MD5 署名 77, 89
定義 281
MIME オブジェクト
定義 281
ブロック 163
MP3 サイト、ブロック 203
MSN メッセンジャ 208
myVAULT 191–193
データの追加 191
データの編集および削除 193

N

NetBIOS
エキスパート ファイアウォール ルール 66
「高」セキュリティ設定 46
定義 288
デフォルトのポート許可 56
ネットワークの認識 256
ハートビート メッセージ 259
ファイアウォール警告 222
Netscape
Cookie の削除 167
キャッシュ、削除 167
削除オプションの設定 165
バージョン 4.73 265
Network News Transfer Protocol (NNTP) 66

O

OpenGL
システム クラッシュ 268
OpenProcess 91
OSFirewall イベント
種類 82
Outlook、迷惑メール フィルタ 135

P

pay-to-surf sites、ブロック 203
PC Anywhere
危険な動作 276
PCAnywhere。リモート コントロール プログラムを*参照*、使用
ping メッセージ
インターネット ゾーンでの許可 259
警告 222
デフォルトのポート許可 56
Point-to-Point Tunneling protocol (PPTP: ポイント ツー ポイント トンネリング プロトコル)
VPN プロトコル 37
POP3
エキスパート ファイアウォール ルール 66

R

Real Networks
エキスパート ファイアウォール ルール 67
RTSP 67

S

Secure Hypertext Transfer Protocol (HTTPS) 67
services.exe 20
SKIP 37

SmartDefense 87
SmartDefense Advisor 222
  警告の送信 172, 174
  定義 282
  ブラウザのアクセス許可 233
  レベルの設定 79
  概要 186
SMTP
  エキスパート ファイアウォール ルール 67
spoolsv.exe 20
svchost.exe 20

T

Telnet 66, 270
TFTP 67
Timbuktu。リモート コントロール プログラムを*参照*、使用
TrueVector セキュリティ エンジン 83, 258

U

UDP
  エキスパート ファイアウォール ルール 59
  デフォルトのポート許可 56
URL 履歴、削除
URL、ブロック 217

V

VNC
  危険な動作 276
VNC プログラム、使用 270
VoIP プログラム、使用 271

W

Web 会議プログラム、使用 271
Web コンテンツのフィルタリング 201
Web コンテンツ、フィルタリング 92
[Who Is] タブ。Hacker ID *参照*
Windows 98 147
Windows ファイアウォール、無効 49
Windows メディア
  エキスパート ルール 67
  履歴の削除 165
winlogon.exe 21

Y

Yahoo! Messenger 208

Z

Zone Alarm 偽物メール確認
Zone Alarm 迷惑メール、迷惑メール フィルタ、特殊な Outlook フォルダを参照
Zone Labs セキュリティ ソフトウェア アプリケーションの終了 15
Zone Labs セキュリティ ソフトウェアのインストール 1–5
Zone Labs セキュリティ ソフトウェア 4
  FTP プログラム 267
  アップデート 17, 22
  アプリケーションの終了 15
  インストール 1–5
  概要 15
  スタートアップ時に起動 24
  ファイル共有プログラム 267
ZoneAlarm チャレンジ メール、迷惑メール フィルタ
ZoneAlarm、インストール 4

あ

アーカイブ ファイル
  ウイルス 112
アウトバウンド MailSafe 保護
  カスタマイズ ??–134
  送信者のアドレス、確認 28
  有効化 129
  カスタマイズ 133–134
アクション
  エキスパート ルール 62, 71
  ログ ビューア 55, 182
アクセス許可
  FTP プログラム 268
  アンチウイルス ソフトウェア 264
  ゲーム 268
  トラスト ゾーン 19
  パスワード 83
  ブラウザ ソフトウェア 265
  プログラムの設定 7
  プログラムへの付与 40, 75
  ポートの設定 57
  メール プログラム 266
アクセス コントロール
  オプションの設定 216
  概要 208
[アクティブなプログラム] エリア 14
アスタリスク、使用 192
新しいネットワーク警告 240
新しいプログラム警告 228, 237, 238
アップデートの確認の設定 22
アドウェア 120
アドバンス プログラム警告 234
アドレス解決プロトコル、有効化 49
アドレス マスク応答および要求 67
アニメーション広告
  スペースの表示方法 160
  ブロック 151
アプリケーション対話 91
アプリケーション対話コントロール 78
暗号化 208
  オプションの設定 216
  概要 212
  有効化と無効化 213
  例 212–213

アンチウイルス ソフトウェア
メール保護 264, 265
アンチウイルス保護
状況、表示 121
アンチウイルス保護機能 99–125

い

イベントのログ
オンとオフ 177
概要 176
カスタマイズ 179
インスタント メッセージング サービス
アクセスのブロック 208
トラフィックの暗号化 212
インストール
ZoneAlarm 4
インターネット オークション サイト、ブロック 203
インターネット制御メッセージ プロトコル (ICMP)
インターネット接続に関するトラブルシューティング 259
エキスパート ファイアウォール ルール 59
デフォルトのポート許可 56
メッセージの種類 67
インターネット接続共有 (ICS)
セキュリティ オプションの設定 47–48
警告オプション 227
有効化 36
インターネット ゾーン 14
許可 19
ネットワークの自動的な追加 50
ネットワーク、自動的な追加 32
インターネット リレー チャット、ブロック 217
インターネット ロック 14, 15
アイコン 15
インターネット ロック警告 225
インテリジェント クイック スキャン 108

う

ウイルス
アーカイブ ファイル 112
署名ファイルのアップデート 102
処理 107, 112
スキャン 110–113
ウイルスの処理 107
ウイルスのスキャン 110–113
疑わしいプログラム動作
種類 274–??
埋め込みオブジェクト、ブロック 163
疑わしい動作の警告 237

え

永続 Cookie 151
有効期限日の設定 158
エキスパート ファイアウォール ルール
概要 59
トラッキング オプション 71
プログラム 96
編集 71
ランク付け 71
管理 70–72
作成 62–63
適用 59–61
エキスパート ファイアウォール ルールのランク付け 60, 71
エコー要求
エキスパート ルール 67
鉛筆のアイコン 155

お

オートコンプリート フォーム、データの削除
音声伝送
ブロック 209
例 210
音声伝送、ブロック 216

か

外国語フィルタ 139
外部から / 外部への通信インジケータ 13
外部からの保護
オプションの設定 216
概要 210–212
前述 208
[外部への保護] エリア 16
学習モード 77, 78
隔離
アイコン 224
インバウンド MailSafe 保護 128
添付ファイルの種類の設定、変更 130
添付ファイルを開く 131, 265
カスタム ポート、追加 57
仮想プライベート ネットワーク (VPN)
警告 37, 235
自動設定警告 235
手動操作の要求警告 236
接続の設定 37–41, 254
接続のトラブルシューティング 254
活動家サイト、ブロック 203
カテゴリ 204
許可およびブロック 199, 201–204
感染のリスク評価 111, 117
感染ファイル
リスク評価 111, 117

き

キーボードとマウス
モニタリング 276
キーボードのショートカット 245–252
キーロガー 120

危険な動作
種類 275–??
危険な動作の警告 237
機能コントロール
オプションの設定 216
概要 209–210
前述 208
偽物メールの提供 139
偽物メール フォルダ 139
偽物メール確認
キャッシュ クリーナ
概要 150, 164
手動での実行 164
ハード ドライブの削除オプション、設定 165
164–167
ブラウザの削除オプション、設定 165–167
協調フィルタ 139
許可
サーバ 19
パスロック 14, 79
パスワード 23

く

グラマーおよびライフスタイル、ブロック 203
繰り返されたプログラム警告 76, 229
ログ オプション 180
グループ
エキスパート ルールへの追加 65–69
軍事サイト、ブロック 203

け

警告
ID ロック 239
OSFirewall 237
新しいネットワーク 240
インターネット ロック 225
高レベル 222
情報 222
設定 84
対応 20, 37
中レベル 222
プログラム
MailSafe 128
新しいプログラム 228, 237, 238
アドバンス プログラム警告 234
繰り返されたプログラム警告 76, 180
サーバ プログラム警告 76, 180, 225, 266
自動 VPN 設定警告 37, 235
手動操作の要求警告 236
ブロックされたプログラム 224
変更されたプログラム警告 229
リファレンス 221–241
ログ 176
警告への対応 20, 37, 170
ゲートウェイ
インターネット接続共有 (ICS) 36
デフォルトのポート許可 56
警告の転送または抑制 47
セキュリティの施行 47
トラスト ゾーンへの追加 53
場所の種類 65
ゲーム
Zone Labs セキュリティ ソフトウェアの使用 268–269
オンライン、アクセスのブロック 202
ゲーム ソフトウェア
危険な動作 276
[検索] ボタン 65

こ

広告ブロック
概要 150
「高」セキュリティ設定
Cookie コントロール 151
ID ロック 190
一般的でないプロトコルの許可 40
インターネット ゾーン 45
概要 18
広告ブロック 151
トラスト ゾーン 45
表示される警告イベント 177
ファイアウォール保護 45
ファイルおよびプリンタの共有 35
プライバシー保護 151
プログラム コントロール 77
ログ オプション 177
高レベルの警告 222
コントロール センタ 12
コントロール センタ、概要 12–14
コンポーネント
MD5 署名 77
VPN 関連 37
管理 94
認証 78
コンポーネント一覧 94

さ

サードパーティ Cookie、ブロック 158
サーバ許可
VoIP プログラム 271
エキスパート ルール 96
警告 232
ゲーム 268
ストリーミング メディア プログラム 271
ゾーン 19
チャット プログラム 266
通信の種類のデフォルト 56
ファイル共有プログラム 267
プログラム一覧のカラム 89
プログラムへの付与 90
メール プログラム 266

サーバとして機能 19
　定義 285
サーバ プログラム警告 76, 83, 225, 266
　ログ オプション 180
サブネット
　VPN 設定 39
　項目の種類 52
　トラスト ゾーンへの追加 53

し

自己署名証明書 214
[システム] エリア 14
実行イベント 82
自動 VPN 設定警告 235
自動ロック
　オプションの設定 80
　有効化 79
[状況] タブ 16
詳細検査スキャン 108
[詳細情報] ボタン 171, 172, 174, 175, 176, 233
　キーボードのショートカット 248, 252
情報応答 67
情報警告 171, 222
情報要求 67
ショートカット メニュー 15

す

スーパー アクセス 88
スカイスクレイパー広告
　スペースの表示方法 160
スキャンのスケジューリング 101
スクリーンロガー 120
スクリプト、ブロック 162
ステルス モード
　「高」セキュリティ設定 46
　定義 286
スパイ Cookie 120
スパイウェア
　種類 120
　スキャン 108
　防止 85
スマート フィルタリング
　概要 198
　タイムアウト オプションの設定 200
　有効化 199

せ

成人向けコンテンツ、ブロック 201
政府サイト、ブロック 203
セキュリティ イベント、ロギング 218
セキュリティ コンポーネント
　カスタマイズ 216
　管理 215
セキュリティ設定
　バックアップとリストア 23
　Zone Labs との共有。DefenseNet を*参照*
セキュリティ設定のバックアップとリストア 23
セキュリティ設定のリストア 23
セッション Cookie
　「高」セキュリティ設定 151
　ブロック 157
設定
　キーボードのショートカット 250
　スタートアップ時に起動 258
　ファイアウォール保護 47
　プログラム コントロール 84
　ペアレント コントロール 200
設定、指定 24
全システム スキャン 108

そ

送信先
　エキスパート ルール 59, 62, 63
ゾーン
　概要 18
　ファイアウォール保護 52
　キーボードのショートカット 246
　追加 53–54
ソフトウェアのアップデート 22
ソフトウェア レンダリング モード 268

た

タイムスタンプ、タイムスタンプ応答 67
ダイヤラ 120
ダイヤルアップ接続
　設定 241
ダッシュボード
　キーボードのショートカット 248
　使用 13

ち

チャット会話、保護 208
チャット プログラム
　サーバ プログラム警告 266
　使用 266
チャレンジ メール 142

「中」セキュリティ設定
ID ロック 190
一般的でないプロトコル 49
インターネット ゾーン 45, 260, 267
概要 18
学習モード 77, 78
カスタマイズ 19
警告 222, 232
警告イベント 177
広告ブロック 151
トラスト ゾーン 45, 53, 256
ネットワーキング 36
ファイルおよびプリンタの共有 35
プライバシー保護 151
プログラム コントロール 78, 267
ポート アクセス 57
リソースの共有 257
ログ オプション 177
「中」セキュリティ設定、定義 215
中レベルの警告 222
超過時間 67

つ

追加
インターネット ゾーンへのワイヤレス ネットワーク 50
カスタム ポート 57
トラスト ゾーン 53
ネットワークをトラスト ゾーンへ 49
プログラム一覧へのプログラム 89
プログラム用のエキスパート ルール 96
ブロック ゾーン 54
通信ソース
一覧 52
管理 52
デフォルトのポート許可 56
ツール バー、メール フィルタ 135

て

[停止] ボタン 15
概要 14
キーボードのショートカット 247
クリックする時期 14
システム トレイ アイコン 15
「低」セキュリティ設定
学習モード 78
ゾーン 45
[頻繁に変更] オプション 89
ファイルおよびプリンタの共有 45
プログラム コントロール 78
デフォルト設定のリストア 216
デフォルトのセキュリティ設定 215, 216
電子メール
偽物、報告 139
迷惑、報告 137
伝送制御プロトコル (TCP)
エキスパート ファイアウォール ルール 59
デフォルトのポート許可 57
添付ファイル一覧
アクセス 130
編集 130

と

ドメイン ネーム サーバ (DNS)
エキスパート ルール 67
外部へのメッセージ
送信先の確認 55
デフォルトのポート許可 56
インターネット接続に関するトラブルシューティング 259
外部からのメッセージ
発信元の確認 181
外部へのメッセージ
送信先の確認 182
定義 280
必要な VPN リソース 39
ドライバ イベント 82
ドライバ、ロード 276
トラスト アクセス 88
トラスト サイト リスト 194–196
トラスト ゾーン
VPN リソース、追加 37
インターネット接続共有 (ICS) 36
許可 19
追加 53
ネットワーク インジケータ 14
ネットワークの自動的な追加 49
ネットワーク、自動的な追加 32
トラスト レベル 87, 88
トラッキング オプション
エキスパート ファイアウォール ルール 62, 71
トラブルシューティング 253–260
トレースルート 67
トロイの木馬 76
Zone Labs セキュリティ ソフトウェアの保護 83
プログラム コントロール 90
120
メール保護 128

に

ニュースとメディアのサイト、ブロック 203

ね

ネットワーク リソース、共有 32
ネットワーク インジケータ 13, 14
ネットワーク セキュリティ オプション、設定 49
ネットワーク設定
設定 49

ネットワーク設定ウィザード
概要 32
無効 33, 34

は

ハード ドライブ、削除 165
ハートビート メッセージ
許可 259
ダイヤルアップ接続、トラブルシューティング 259
定義 287
配色、変更 24, 26
パケット
エキスパート ファイアウォール ルール 59
警告 171
タイプ、ブロック 48
定義 288
発信元
確認 184
場所
エキスパート ファイアウォール ルールへの追加 63
グループの作成 65
パスロック許可
プログラムへの付与 93
パスワード
VNCviewer 270
キャッシュからの削除 166
作成 22
プログラム コントロール 83
ハッカー ID
概要 186
発信元
Cookie の保持 166
エキスパート ファイアウォール ルール 59
通信、確認 52, 176
バナー広告
スペースの表示方法 160
ブロック 151
パブリック ネットワーク
定義 288
ネットワーク設定ウィザード 32
パラメータ問題
エキスパート ルール 67

ひ

日付 / 時間
ログ ビューア 182
ビデオ ソフトウェア
危険な動作 276
ビデオ伝送、ブロック 216, 242
表示設定、指定 24
平文パスワード 239
頻繁に変更 89

ふ

ファイアウォール警告 171
対応 222
発信元の確認 223
ログ 179
ファイアウォール保護 43–72
アドバンス セキュリティ オプション 47–54
エキスパート ルール 59–61
概要 44
セキュリティ レベルの設定 45–46
ポートのブロックおよびブロック解除 56
ファイル イベント 82
ファイルおよびプリンタの共有
サーバ アクセス 232
トラブルシューティング 267
ネットワーク セキュリティ 49
有効化 35, 240
ファイル断片、削除 165
ファイルの転送、ブロック 242
フィッシング 138
フィルタ オプション、設定 92
フォーム データ、キャッシュからの削除
物理メモリ イベント 82
プライバシー アドバイザ
使用 153
プライバシー サイト一覧 154
AOL 156
Web サイトの追加 155
アクセス 154
広告ブロック ソフトウェア 155
プライバシー保護
Cookie コントロール
レベルの設定 151
キャッシュ クリーナ
手動での実行 164
広告ブロック
レベルの設定 151
プログラムごとの有効化 152
モバイル コード コントロール
カスタマイズ 162
有効化と無効化 151
レベルの設定 151
Cookie コントロール 157–159
カスタマイズ 157–159
キャッシュ クリーナ 164–167
広告ブロック
カスタマイズ 160–161
プライベート ネットワーク
仮想。仮想プライベート ネットワーク (VPN) を*参照*
定義 289
ネットワーク設定ウィザード 32
ブラウザ キャッシュ、削除 166, 167, 205
ブラウザ ソフトウェア、使用 265
ブラウザのデフォルト、変更 274
ブラウザ ヘルプ オブジェクト 120
フラグメント、ブロック 48
プリンタ。ネットワーク リソース、共有を参照

プロキシ サーバ
インターネット接続に関するトラブルシューティング 258
回避システム、アクセスのブロック 203
プログラム
エキスパート ルールの作成 96
停止 88
トラスト レベル 88
プログラム一覧への追加 89
プログラム アクセスの制限 88
プログラム一覧
アクセス 85
プログラムの追加および削除 89
プログラム許可 87
プログラム警告 228–235
対応 79
プログラム コントロール 73–269
インターネット ロック 79
概要 74
ゾーン 19
「中」セキュリティ設定 77
レベルの設定 77
プログラム コンポーネント
管理 94–95
プログラム コンポーネント警告 230
プログラムの抹消 88
プロセス イベント 82
ブロック
埋め込みオブジェクト 163
実行可能 URL 242
スクリプト 162
パケットのフラグメント 48
ビデオ伝送 242
ファイルの転送 242
プログラム 48
Cookie 157–159
カテゴリ別 Web コンテンツ 199–204
広告 160–161
不適切な Web コンテンツ 201–204
ポート 56–58
メールの添付ファイル 128–129
ブロックされたプログラム警告 224
[ブロックした侵入] エリア 16
ブロック ゾーン
概要 18
追加 54
プロトコル
VPN 37, 40
エキスパート ファイアウォール ルール 59
エキスパート ルール 49
グループの作成 66
デフォルトの許可 56
ファイアウォール保護 48
メール 35

へ

ペアレント コントロール 197–205
概要 198
カテゴリの許可およびブロック 201–??
許可およびブロック ??–204
スマート フィルタリング 199
設定の指定 200
タイムアウト オプションの設定 200
有効化 199
変更されたプログラム警告 229

ほ

報告
偽物メール 139
迷惑メール 137
暴力コンテンツ、ブロック 204
ポート
1394 49
エキスパート ファイアウォール ルール 59
「高」セキュリティ設定 45
追加 57
デフォルトの許可 56
ファイアウォール保護 44
ブロックおよびブロック解除 56–57
ホーム ネットワーク
ファイアウォール警告 222
保護されていないワイヤレス ネットワーク
ワイヤレス ネットワーク設定ウィザード 33
保護されているワイヤレス ネットワーク
ワイヤレス ネットワーク設定ウィザード 33
保護レベル
カスタマイズ 216
設定 215
ホスト ファイル、ロック 49
ホスト名
通信ソースの一覧 52
トラスト ゾーンへの追加 257
プライバシー サイト一覧 156
ポリシー 79

ま

マイ コンピュータ 62

む

無効
Windows ファイアウォール 49

め

迷惑メールの提供 137

迷惑メール フィルタ
レポート 145
Hotmail 135, 144
外国語フィルタ 139
会社名のブロック 136
偽物メールの報告 138, 139, 143
偽物メール フォルダ 139
協調フィルタ 139
自動報告オプション 143
送信者のブロック 135
[チャレンジ メール] フォルダ 142
ツール バー 135
特別な Outlook フォルダ 135–145
プライバシー 142
プライバシーの保護 138, 139
迷惑メールの提供 137
迷惑メールの報告 137
迷惑メール フォルダ 138
メール リストのブロック 137
メッセージ フィルタ 139
メッセージ フィルタリング オプション 139
ワイヤレス デバイス サポート 143
迷惑メール フィルタ、迷惑メール フィルタを参照 135
迷惑メール フォルダ 138
迷惑メール防止
オプションの設定 216
概要 209
前述 208
メール サーバ、接続 35
メール送信許可
アウトバウンド MailSafe 保護 129
90
[メール フィルタ] ツール バー 135
メール保護 127–??
アウトバウンド 129
インバウンド 128, 129
概要 128
ステータス 264
添付ファイル一覧 130
??–134
メール用ごみ箱、削除
メッセージ イベント 82
メッセージの暗号化 208
メッセージ フィルタ 139

も

モジュール イベント 82
モバイル コード コントロール
概要 150
カスタマイズ 156, 162

ゆ

有害なリンク、削除 242
有効期限
Cookie の設定 158
アップデート サービス 17
ユーモア サイト、ブロック 203

よ

曜日 / 時間
エキスパート ルールへの追加 63
範囲、グループの作成 68

ら

ライセンス キー
アップデート 28

り

リダイレクト 67
リモート ホスト コンピュータ
VPN 設定 39
リモート アクセス プログラム
トラブルシューティング 24
リモート コントロール プログラム、使用 269

る

ルータ勧誘 67
ルータ広告 67
ループバック アダプタ
トラスト ゾーンへの追加 38
留守番電話プログラム 267

れ

レジストリ イベント 82

ろ

ローカル サーバ、ブロック 48
ログ エントリ
エキスパート ルール 96
アーカイブ 184–185
オプション 179
概要 176
形式の設定 179
表示 180, 182
フィールド 183
プログラム 180
プログラム警告 180
ログ ビューア
アクセス 180
使用 218
ログ ファイル形式の設定 179
ロック アイコン
システム トレイ 15
ロックモード、指定 80

わ

ワーム 120

ワイヤレス ネットワーク設定
設定 50
ワイヤレス ネットワーク セキュリティ オプション、設定 50

「高」セキュリティ設定
デフォルトのポート許可 56–57
「中」セキュリティ設定
デフォルトのポート許可 56–57
「低」セキュリティ設定
デフォルトのポート許可 56–57