SonicOS 7.0

AppFlow 監視

管理者ガイド

SONICWALL®

目次

1

AppFlow 報告

「**監視 | AppFlow > AppFlow 報告**」ページには、以下のレポートが表示されます。

ⓘ **補足:** 「**監視 | AppFlow > AppFlow 報告**」ページは、SonicWall TZ、NSv、NSsp シリーズ装置でサポートされます。

「**監視 | AppFlow > AppFlow 報告**」ページでは、現在ネットワーク上で発生していることを示す上位レベルの集計レポートを表示し、次のような事柄を一目で把握することが可能です。

- ネットワーク上で頻繁に使用されるアプリケーション
- セッションとバイト総数に関して、ネットワーク帯域幅を消費しているアプリケーション
- ウイルス、侵入およびスパイウェアを含むアプリケーション
- ユーザが訪問しているウェブサイト種別

報告データは、システムを最後に再起動した時点からか、データが最後にリセットされた時点からかのいずれかで見ることができます。

報告を有効にして構成するには、『**SonicOS/X ログ**』技術文書の「**フロー報告の統計の管理**」に従ってください。「**監視 | AppFlow > AppFlow 報告**」ページの上部にある緑色のチェック マーク アイコンは、「**デバイス | AppFlow 設定 > フロー報告**」ページへのリンクを示します。これは、報告を構成するためのページです。

ページの最上部には、以下の設定と情報が表示されます。

- **IP バージョン** – 「IPv4」、「IPv6」、または「IPv4 & IPv6」を選択し、そのトラフィックに関するレポートを表示します。
- **表示** – レポートの表示種別を、ファイアウォールを再起動した後の合計アクティビティ、ユーザが最後にリ

セットした後のアクティビティ、または、構成されたスケジュールによるアクティビティより選択します。スケジュールの場合、レポートのエクスポート先を FTP または電子メールのいずれかより構成できます。エクスポート先は、「構成」ボタンで設定します。「**スケジュールどおり**」の場合、FTP/電子メールによりレポートをエクスポートするよう構成できます。設定するには「**構成**」をクリックします。

次のいずれかを選択します。

- 「**再起動以降**」 – 装置の最後の再起動から集計した統計が表示されます。
- 「**最後のリセット以降**」 – 統計をクリアした時間以降に集計された統計が表示されます。
- 「**スケジュールどおり**」 – FTP/電子メールによりレポートをエクスポートするよう構成できます。

- **制限** – 結果の項目数を制限します。
- **チェック マーク** – クリックするか、マウス カーソルを重ねると、「**デバイス | AppFlow 設定 > フロー報告**」へのリンクが表示されます。
- **再表示** – クリックすると、報告データが更新されます。

トピック:

上位アプリケーション

「**表示**」ドロップダウン リストで、「**再起動以降**」、「**最後のリセット以降**」、または「**スケジュールどおり**」を選択します。

これらの選択肢は、以下のように定義されます。

- **セッション** – 接続数/フロー数
- **始動者バイト** – 始動者が送信したバイト数
- **応答者バイト** – 応答者が送信したバイト数

報告には、以下の情報が表示されます。

- **アプリケーション名** – アプリケーションの名前 – シグネチャ ID
- **アプリケーション割合** – そのアプリケーションの使用頻度を、全アプリケーション数に対する比率として表示します
- **アクセス ルール** – ファイアウォール ルールにより遮断された接続数/フロー数
- **アプリケーション ルール** – DPI エンジンによって遮断された接続/フローの数
- **位置遮断** – 地域強制により遮断された接続数/フロー数
- **ボットネット遮断** – ボットネット強制により遮断された接続数/フロー数
- **ウイルス** – ウイルスを伴う接続数/フロー数
- **侵入** – 脅威として検知された接続数/フロー数
- **スパイウェア** – スパイウェアを伴う接続数/フロー数

上位ユーザ

「**表示**」ドロップダウン リストで、「**再起動以降**」、「**最後のリセット以降**」、または「**スケジュールどおり**」を選択します。

これらの選択肢は、以下のように定義されます。

- **セッション** – 開始/応答したセッション/接続の数
- **受信バイト数** – ユーザが受信したバイト数
- **送信バイト数** – ユーザが送信したデータ量（バイト）

報告には、以下の情報が表示されます。

- **ユーザ名** – ユーザの名前、または「不明」
- **ユーザ割合** – そのユーザのアクティビティを、全ユーザのアクティビティに対する比率として表示します。
- **遮断** –遮断された接続/セッション
- **ウイルス** – ウイルスを伴う接続数/フロー数
- **スパイウェア** – スパイウェアが検知されたセッション数/接続数
- **侵入** – 侵入として検知されたセッション数/接続数
- **ボットネット** – ボットネットが検知されたセッション/接続

上位 IP アドレス

「**表示**」ドロップダウン リストで、「**再起動以降**」、「**最後のリセット以降**」、または「**スケジュールどおり**」を選択します。

これらの選択肢は、以下のように定義されます。

- **セッション** – 開始/応答したセッション/接続の数
- **受信バイト数** – ユーザが受信したバイト数
- **送信バイト** – ユーザが送信したデータ量（バイト）

報告には、以下の情報が表示されます。

IP アドレス – IP アドレス

IP アドレス割合 – その IP アドレスに関する接続/フローの頻度を、全 IP アドレスに対する全接続/フローとの比率として表示します。

- **遮断** –遮断された接続/セッション
- **ウイルス** – ウイルスを伴う接続数/フロー数
- **スパイウェア** – スパイウェアが検知されたセッション数/接続数
- **侵入** – 侵入として検知されたセッション数/接続数
- **ボットネット** – ボットネットとして検知されたセッション/接続

上位ウイルス

「**表示**」ドロップダウン リストで、「**再起動以降**」、「**最後のリセット以降**」、または「**スケジュールどおり**」を選択します。

報告には、以下の情報が表示されます。

- **セッション** – このウイルスを含むセッション数/接続数

報告には、以下の情報が表示されます。

- **ウイルス名** – ウイルスの名前、または「不明」
- **ウイルス割合** – そのウイルスの頻度を、全ウイルスの合計数に対する比率として表示します

上位侵入

「**表示**」ドロップダウン リストで、「**再起動以降**」、「**最後のリセット以降**」、または「**スケジュールどおり**」を選択します。

報告には、以下の情報が表示されます。

- **セッション** – このウイルスを含むセッション数/接続数

報告には、以下の情報が表示されます。

- **侵入名** – 侵入の名前、または「不明」
- **侵入割合** – その侵入の頻度を、全侵入の合計数に対する比率として表示します

上位スパイウェア

「**表示**」ドロップダウン リストで、「**再起動以降**」、「**最後のリセット以降**」、または「**スケジュールどおり**」を選択します。

報告には、以下の情報が表示されます。

- **セッション** – このウイルスを含むセッション数/接続数

報告には、以下の情報が表示されます。

- **スパイウェア名** – スパイウェア シグネチャの名前、または「不明」
- **スパイウェア割合** – そのスパイウェアの頻度を、全スパイウェアの合計数に対する比率として表示します

上位位置

「**表示**」ドロップダウン リストで、「**再起動以降**」、「**最後のリセット以降**」、または「**スケジュールどおり**」を選択します。

これらの選択肢は、以下のように定義されます。

- **セッション** – 開始/応答したセッション/接続の数
- **受信バイト数** – ユーザが受信したバイト数
- **送信バイト** – ユーザが送信したデータ量（バイト）

報告には、以下の情報が表示されます。

- **国名** – ロケーションまたは国の名前
- **ロケーション割合** – そのロケーションに関する接続/フローの頻度を、全ロケーションに対する全接続/フローとの比率として表示します
- **破棄** – 破棄されたセッション数/接続数

上位ボットネット

「**表示**」ドロップダウン リストで、「**再起動以降**」、「**最後のリセット以降**」、または「**スケジュールどおり**」を選択します。

報告には、以下の情報が表示されます。

- **ボットネット名** – ボットネットの名前
- **回数** – ボットネットが検知されたセッション/接続

上位ウェブ種別

「**表示**」ドロップダウン リストで、「**再起動以降**」、「**最後のリセット以降**」、または「**スケジュールどおり**」を選択します。

報告には、以下の情報が表示されます。

- **セッション** – セッション数/接続数

報告には、以下の情報が表示されます。

- **格付け名** – URL 種別名
- **ウイルス割合** – その格付け種別の URL へのアクセス頻度を、全 URL アクセス合計数に対する比率として表示します

2

AppFlow 監視

「**監視 | AppFlow > AppFlow 監視**」ページには、以下のレポートが表示されます。

ⓘ **補足:** 「**監視 | AppFlow > AppFlow 監視**」ページは、SonicWall TZ、NSv、NSsp シリーズ装置でサポートされます。

「**監視 | AppFlow > AppFlow 監視**」ページでは、現在ネットワーク上で発生していることを示す上位レベルの集計レポートを監視し、次のような事柄を一目で把握することが可能です。

- ネットワーク上で頻繁に使用されるアプリケーション
- セッションとバイト総数に関して、ネットワーク帯域幅を消費しているアプリケーション
- ウイルス、侵入およびスパイウェアを含むアプリケーション
- ユーザが訪問しているウェブサイト種別

報告を有効にして構成するには、『**SonicOS/X ログ**』技術文書の「**フロー報告の統計の管理**」に従ってください。「**監視 | AppFlow > AppFlow 監視**」ページの上部にある緑色のチェック マーク アイコンは、「**デバイス | AppFlow 設定 > フロー報告**」ページへのリンクを示します。これは、報告を構成するためのページです。

ページの最上部には、以下の設定と情報が表示されます。

- **+作成** – クリックすると、インシデントに関するフィルタが作成されます。
- **+フィルタに追加** – クリックすると、選択したアプリケーションにフィルタ条件が追加されます。
- **IP バージョン** – 「IPv4」、「IPv6」、または「IPv4 と IPv6」を選択し、そのトラフィックに関するレポートを表示します。
- **スライダー** – スライダーを使用して最新 60 秒、2 分、10 分、15 分、30 分、60 分、3 時間、6 時間、12 時間、24 時間、7 日、15 日、30 日のフロー結果を絞り込むか、すべてのフロー結果を表示します。
- **グループ別** – **アプリケーション**、**種別**、または**シグネチャ**に基づいてフローをグループ化して結果を絞り込みます

- **チェック マーク** – クリックすると、監視状況と「**デバイス | AppFlow 設定 > フロー報告**」へのリンクが表示されます。
- **再表示** – クリックすると、報告データが更新されます。

トピック:

上位アプリケーション

アプリケーション別にフローにフィルタを適用できます。アプリケーションは、**アプリケーション**、**種別**、**シグネチャ**ごとにグループ化できます。

これらの選択肢は、以下のように定義されます。

- **アプリケーション** – アプリケーション名 – シグネチャ ID
- **セッション** – 接続数/フロー数
- **合計パケット** – パケット数
- **合計バイト** – 始動者が送信したバイト数
- **平均速度 (KBPS)** – 現在の平均速度 (接続の存続期間にわたって計算)
- **脅威** – 侵入/スパイウェア/ウイルスとして検知されたセッション数/接続数

上位ユーザ

ユーザ別にフローにフィルタを適用できます。ユーザは、**ユーザ名**、**IP アドレス**、**ドメイン名**、**認証種別**ごとにグループ化できます。

これらの選択肢は、以下のように定義されます。

- **ユーザ** – ユーザの名前 – シグネチャ ID
- **セッション** – 接続数/フロー数
- **合計パケット** – パケット数
- **合計バイト** – 始動者が送信したバイト数
- **平均速度 (KBPS)** – 現在の平均速度 (接続の存続期間にわたって計算)
- **脅威** – 侵入/スパイウェア/ウイルスとして検知されたセッション数/接続数

上位ウェブ利用状況

ウェブ アクティビティ別にフローにフィルタを適用できます。ウェブ URL は、**ドメイン名**、**URL**、**格付け**ごとにグループ化できます。

これらの選択肢は、以下のように定義されます。

- **ドメイン名** – ウェブドメインの名前
- **エントリをフィルタに追加する** – アイコンが表示され、特定のドメイン名をフィルタに追加できます
- **セッション** – 接続数/フロー数
- **合計パケット** – パケット数
- **合計バイト** – 始動者が送信したバイト数
- **平均速度 (KBPS)** – 現在の平均速度 (接続の存続期間にわたって計算)
- **脅威** – 侵入/スパイウェア/ウイルスとして検知されたセッション数/接続数

上位始動者 IP

始動者 IP 別にフローにフィルタを適用できます。始動者 IP は、**IP アドレス**、**インターフェース**、**国**ごとにグループ化できます。

これらの選択肢は、以下のように定義されます。

- **始動者** – 始動者 IP アドレスの名前
- **エントリをフィルタに追加する** – アイコンが表示され、特定の始動者 IP アドレスをフィルタに追加できます
- **セッション** – 接続数/フロー数
- **合計パケット** – パケット数
- **合計バイト** – 始動者が送信したバイト数
- **平均速度 (KBPS)** – 現在の平均速度 (接続の存続期間にわたって計算)
- **脅威** – 侵入/スパイウェア/ウイルスとして検知されたセッション数/接続数

上位応答者 IP

応答者 IP 別にフローにフィルタを適用できます。応答者 IP は、**IP アドレス**、**インターフェース**、**国**ごとにグループ化できます。

これらの選択肢は、以下のように定義されます。

- **応答者** – 応答者 IP アドレスの名前
- **エントリをフィルタに追加する** – アイコンが表示され、特定の応答者 IP アドレスをフィルタに追加できます
- **セッション** – 接続数/フロー数
- **合計パケット** – パケット数
- **合計バイト** – 始動者が送信したバイト数
- **平均速度 (KBPS)** – 現在の平均速度 (接続の存続期間にわたって計算)
- **脅威** – 侵入/スパイウェア/ウイルスとして検知されたセッション数/接続数

上位脅威

脅威別にフローにフィルタを適用できます。脅威は、**すべて、侵入、ウイルス、スパイウェア、アンチスパム、ボットネット**としてグループ化できます。

これらの選択肢は、以下のように定義されます。

- **脅威** – 脅威の名前
- **エントリをフィルタに追加する** – アイコンが表示され、特定の脅威をフィルタに追加できます
- **セッション** – 接続数/フロー数
- **合計パケット** – パケット数
- **合計バイト** – 始動者が送信したバイト数
- **平均速度 (KBPS)** – 現在の平均速度 (接続の存続期間にわたって計算)
- **脅威** – 侵入/スパイウェア/ウイルスとして検知されたセッション数/接続数

上位 VoIP

VoIP 別にフローにフィルタを適用できます。VoIP は、**メディア種別**または**発信者 ID** ごとにグループ化できます。

これらの選択肢は、以下のように定義されます。

- **VoIP** – VoIP の名前
- **エントリをフィルタに追加する** – アイコンが表示され、特定の VoIP データをフィルタに追加できます
- **セッション** – 接続数/フロー数
- **合計パケット** – パケット数
- **合計バイト** – 始動者が送信したバイト数
- **平均速度 (KBPS)** – 現在の平均速度 (接続の存続期間にわたって計算)
- **脅威** – 侵入/スパイウェア/ウイルスとして検知されたセッション数/接続数

上位 VPN

VPN 別にフローにフィルタを適用できます。VPNは、**リモート IP アドレス、ローカル IP アドレス、名前**ごとにグループ化できます。

これらの選択肢は、以下のように定義されます。

- **VPN** – VPN の名前
- **エントリをフィルタに追加する** – アイコンが表示され、特定の VPN データをフィルタに追加できます
- **セッション** – 接続数/フロー数
- **合計パケット** – パケット数
- **合計バイト** – 始動者が送信したバイト数
- **平均速度 (KBPS)** – 現在の平均速度 (接続の存続期間にわたって計算)
- **脅威** – 侵入/スパイウェア/ウイルスとして検知されたセッション数/接続数

上位デバイス

デバイス の IP アドレス別にフローにフィルタを適用できます。デバイスは、**IP アドレス**、**インターフェース**、**名前**、**ベンダー**ごとにグループ化できます。

これらの選択肢は、以下のように定義されます。

- **デバイス** – デバイスの名前
- **エントリをフィルタに追加する** – アイコンが表示され、特定のデバイスデータをフィルタに追加できます
- **セッション** – 接続数/フロー数
- **合計パケット** – パケット数
- **合計バイト** – 始動者が送信したバイト数
- **平均速度 (KBPS)** – 現在の平均速度 (接続の存続期間にわたって計算)
- **脅威** – 侵入/スパイウェア/ウイルスとして検知されたセッション数/接続数

上位内容

コンテンツ別にフローにフィルタを適用できます。コンテンツは、**ファイル種別**または**電子メール アドレス**ごとにグループ化できます。

これらの選択肢は、以下のように定義されます。

- **内容** – コンテンツの名前
- **エントリをフィルタに追加する** – アイコンが表示され、特定のコンテンツ データをフィルタに追加できます
- **セッション** – 接続数/フロー数
- **合計パケット** – パケット数
- **合計バイト** – 始動者が送信したバイト数
- **平均速度 (KBPS)** – 現在の平均速度 (接続の存続期間にわたって計算)
- **脅威** – 侵入/スパイウェア/ウイルスとして検知されたセッション数/接続数

上位ポリシー

セキュリティ **ポリシー**別にフローにフィルタを適用できます。セキュリティポリシーは、**アクセス ルール**、**NAT ルール**、**始動者ルート ポリシー**、**応答者ルート ポリシー**ごとにグループ化できます。

これらの選択肢は、以下のように定義されます。

- **ポリシー** – 監視対象のセキュリティ ポリシーの名前
- **エントリをフィルタに追加する** – アイコンが表示され、特定のポリシー データをフィルタに追加できます
- **セッション** – 接続数/フロー数
- **合計パケット** – パケット数
- **合計バイト** – 始動者が送信したバイト数
- **平均速度 (KBPS)** – 現在の平均速度 (接続の存続期間にわたって計算)
- **脅威** – 侵入/スパイウェア/ウイルスとして検知されたセッション数/接続数

3

CTA レポート

「キャプチャ脅威評価（CTA）レポート」を使用して、ダウンロードおよびキャプチャ脅威評価サービスへの投稿ができる SonicFlow レポート（SFR）を生成します。

CTA レポートの生 成 およびダウンロード

SonicFlow レポート（SFR）を生成およびポストするには、以下の手順に従います

1. 「**監視 | AppFlow > CTA レポート**」ページの「キャプチャ脅威評価」画面に移動します。
2. 「**CTA レポートの生成とダウンロード**」タブで、「**レポートの生成**」をクリックします。
3. レポートが生成されると、そのレポートをダウンロードしたり、新しいレポートを生成したりすることができます。

4. レポートをダウンロードするには、「**レポートのダウンロード**」を選択します。

詳細オプション

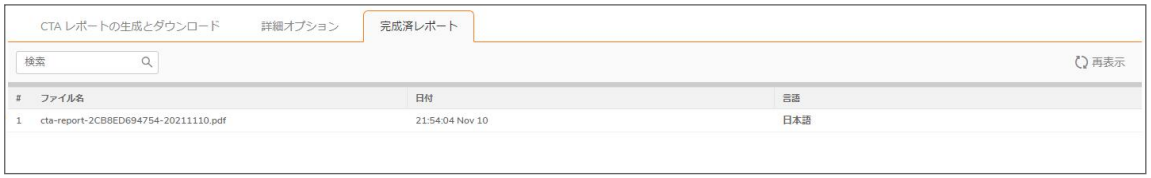
「**詳細オプション**」タブの値はファイアウォールに保存されません。ログアウトするか、ブラウザのキャッシュをクリアすると、ユーザ定義データは消去されます。

詳細 CTA レポート オプションを構成するには、以下の手順に従います

1. 「**監視 | AppFlow > CTA レポート**」ページに移動します。
2. 「**詳細オプション**」タブをクリックします。

3. テキスト オプション、レポート種別、表示する目的のセクションを使用して、CTA レポート用にデータをカスタマイズするか、ユーザ定義 レポート ロゴを含めます。
4. ユーザ定義データの入力を完了したら、「**CTA レポートの生成およびダウンロード**」に戻り、「**レポートの生成**」をクリックします。ユーザ定義レポートが「**完成済レポート**」タブで提供される PDF に表示されます。

完成済レポート



生成されたレポートがテーブルに表示され、レポートの PDF バージョンをダウンロード、表示、削除できます。

4

SonicWall サポート

有効なメンテナンス契約が付属する SonicWall 製品をご購入になったお客様は、テクニカル サポートを利用できます。

サポート ポータルには、問題を自主的にすばやく解決するために使用できるセルフヘルプ ツールがあり、24 時間 365 日ご利用いただけます。サポート ポータルにアクセスするには、次の URL を開きます:
https://www.sonicwall.com/ja-jp/support

サポート ポータルでは、次のことができます。

- ナレッジ ベースの記事や技術文書を閲覧する。
- 次のサイトでコミュニティ フォーラムのディスカッションに参加したり、その内容を閲覧したりする:
  https://community.sonicwall.com/technology-and-support
- ビデオ チュートリアルを視聴する。
- https://mysonicwall.com にアクセスする。
- SonicWall のプロフェッショナル サービスに関して情報を得る。
- SonicWall サポート サービスおよび保証に関する情報を確認する。
- トレーニングや認定プログラムに登録する。
- テクニカル サポートやカスタマー サービスを要請する。

SonicWall サポートに連絡するには、次の URL を開きます: https://www.sonicwall.com/ja-jp/support/contact-support

このドキュメントについて

補足: メモ アイコンは、補足情報があることを示しています。

重要: 重要アイコンは、補足情報があることを示しています。

ヒント: ヒント アイコンは、参考になる情報があることを示しています。

注意: 注意アイコンは、手順に従わないとハードウェアの破損やデータの消失が生じる恐れがあることを示しています。

警告: 警告アイコンは、物的損害、人身傷害、または死亡事故につながるおそれがあることを示します。

SonicOS AppFlow 監視 管理者ガイド
更新日 – 2021 年 4 月
ソフトウェア バージョン – 7.0
232-005637-10 Rev B

エンド ユーザ製品利用規約

SonicWall エンド ユーザ製品利用規約を参照する場合は、次に移動してください: https://www.sonicwall.com/ja-jp/legal

オープン ソース コード

SonicWall Inc. では、該当する場合は、GPL、LGPL、AGPL のような制限付きライセンスによるオープン ソース コードについて、コンピュータで読み取り可能なコピーをライセンス要件に従って提供できます。コンピュータで読み取り可能なコピーを入手するには、「SonicWall Inc.」を受取人とする 25.00 米ドルの支払保証小切手または郵便為替と共に、書面によるリクエストを以下の宛先までご送付ください。

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035