脆弱性ツール診断

Powered by SCT SECUREクラウドスキャン

サイバートラスト株式会社

なんらかの脆弱性を抱えるWebサイト

脆弱性が検出されたWebサイト

98%

これまで脆弱性診断を実施したWebサイトのうちの約98%に
なんらかの脆弱性が発見されています。（当社調べ）

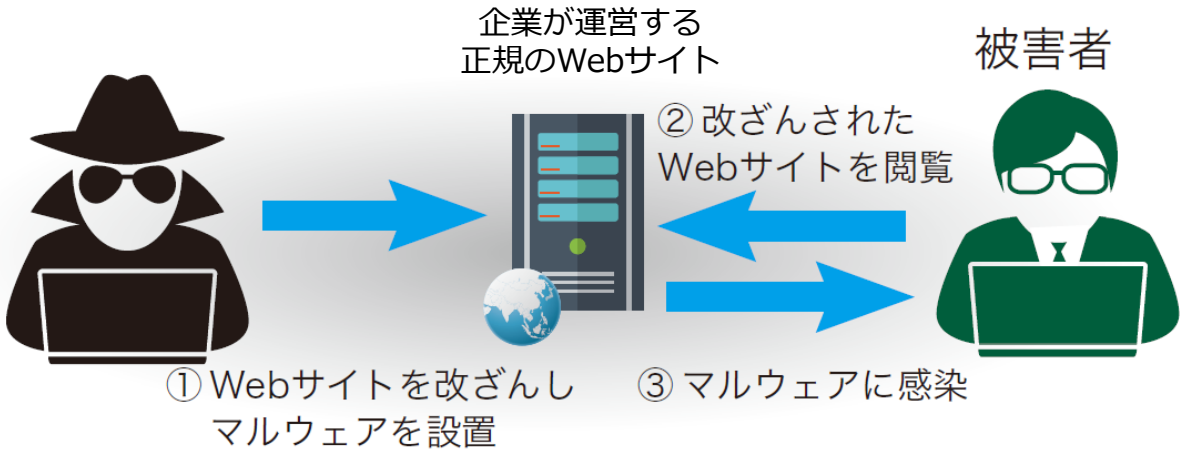
Webサイトの脆弱性はサイバー攻撃の入口となります

Webサイトへのハッキング攻撃の多くは、Webサイトに潜在する脆弱性を利用して行われます。

Webサイトの脆弱性を放置することは、ハッキングによる情報漏えいや改ざんのリスク抱えることになります。

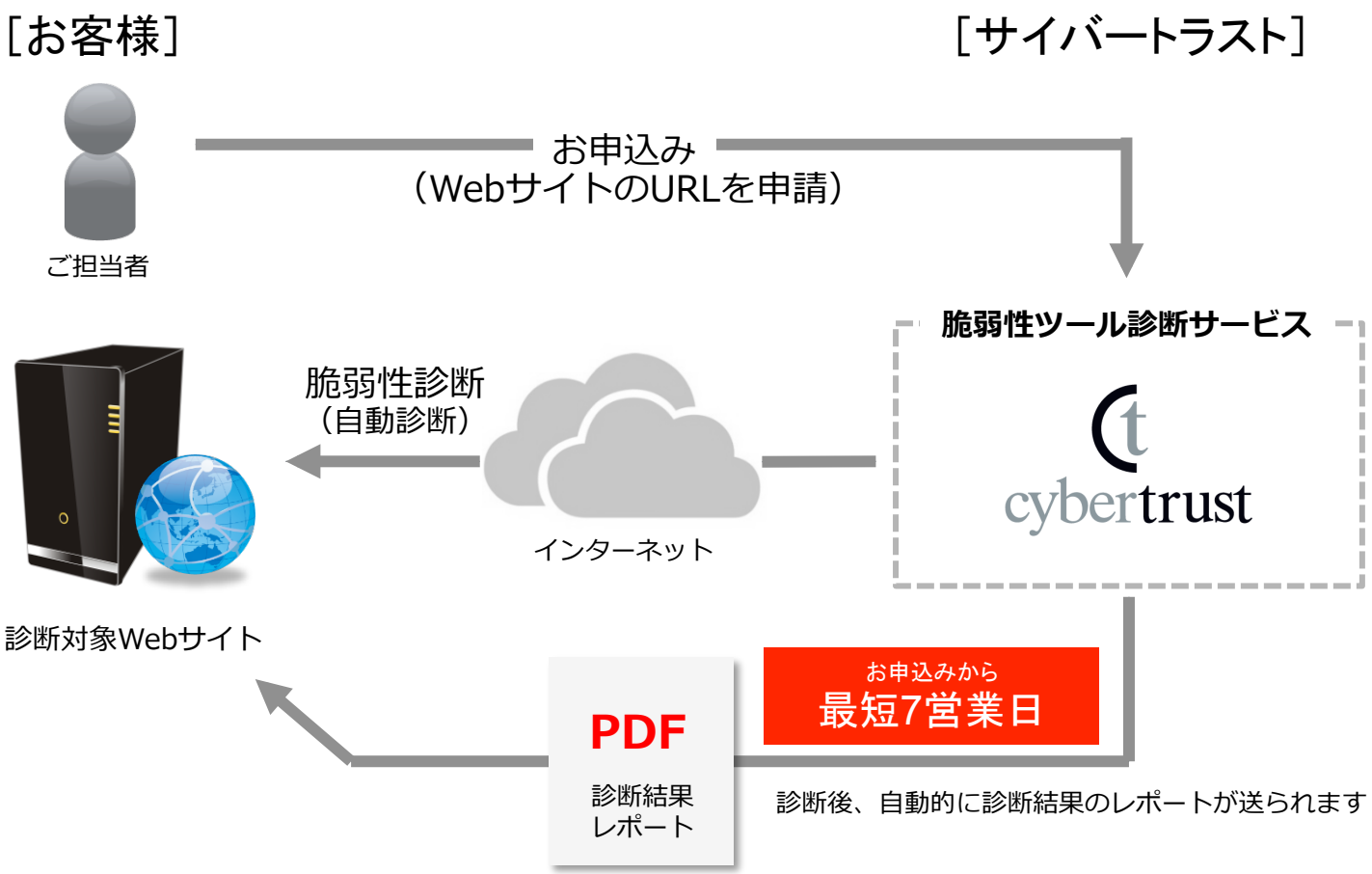
標的型攻撃の水飲み場型攻撃では、企業が運営する正規のWebサイトが改ざんされ、マルウェアが設置されます。

知らぬ間に、自社のWebサイトが他社の攻撃の踏み台として利用される場合があります。



脆弱性ツール診断の仕組み

完全自動のクラウド型の脆弱性診断サービスであるため、ユーザーは Web サイトのURL を申請するだけで、手軽に脆弱性診断を実施することができます。また、ツールによる自動診断であるため、比較的低コストで診断がおこなえることもメリットの一つとなっています。



脆弱性ツール診断の特長

お手軽

FQDNの申請だけで簡単に診断できます

クラウドサービスであるため、Webサーバーへのアプリケーションのインストールや、専用ハードの設置などは一切不要です。FQDNの申請だけで最新のセキュリティ情報に基づいた診断を、今すぐに始めることができます。

スピード

お申し込みから1週間で診断実施できます

お申し込みから1週間程度で脆弱性診断を実施します。診断結果はPDF形式のレポートにまとめられ、メールで3営業日後に納品されます。

低コスト

ツール診断なので低コストで診断できます

専門スタッフによる本格的な脆弱性診断に比べると、診断にかかる費用を大きく削減できます。

脆弱性ツール診断は、ツールによる自動診断ですので、複雑なWebアプリケーションの場合、探索・診断できるページに限界があります。
複雑なWebアプリケーションの場合は、経験豊かなセキュリティ技術者が個別に対応する脆弱性診断サービスをおすすめしています。ご判断に迷う場合は、まずはお気軽にご相談ください。

このようなお客様に最適な診断サービスです

- **コーポレートサイト**（企業ホームページ）の脆弱性診断を実施したい。
- 脆弱性診断を実施するための**予算が不足**している。
- サービスインまで**時間的な余裕がなく**、本格的な脆弱性診断が行えない。
- 開発途中のWebアプリケーション・Webサービスに対して**簡易的に**脆弱性診断を実施したい。
- **継続的**（1年ごと、半年ごと）に脆弱性診断を実施したい。

診断内容について

安全な検査

- ネットワーク・プラットフォーム・Webアプリケーションの脆弱性を自動検査
- ネットワークに影響を与えない非侵襲的(非破壊的)検査のみを実行

世界的に信頼性の高い診断エンジンを採用

- PCI-DSS(※)の認定ベンダーが提供する診断エンジンを採用
- セキュリティーに厳格なカード業界品質の診断サービス

※PCI DSS（Payment Card Industry Data Security Standard：PCIデータセキュリティスタンダード）は、クレジットカード情報および取り引き情報を保護するために2004年12月、JCB・American Express・Discover・マスターカード・VISAの国際ペイメントブランド5社が共同で策定した、クレジット業界におけるグローバルセキュリティ基準です。

最高水準の脆弱性データベースに基づき診断

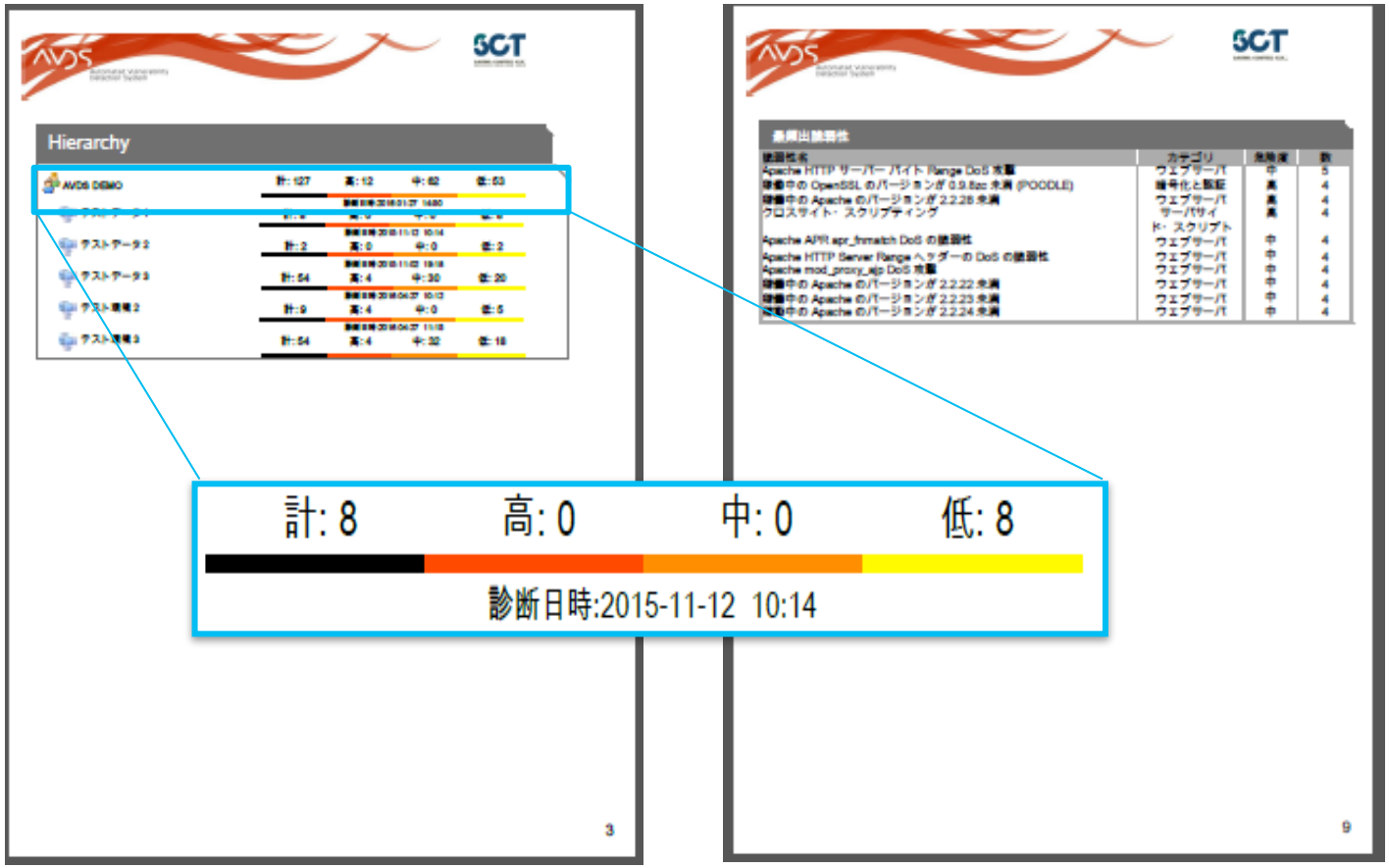
- 13,000項目の脆弱性と、5000以上の攻撃スクリプトを集積
- ITセキュリティ情報のポータルSecuriteam.com等の情報を元に、日々検査パターンを作成・更新

診断項目について

カテゴリー	検査項目例	検査項目数
DNSサーバー	BINDのバージョン取得など	約150項目
FTPサーバー	FTP平文認証など	約300項目
Mailサーバー	SMTP認証など	約300項目
NFSサービス	不必要なNFS Serverなど	約20項目
Proxyサーバー	F5 BIP-IPの永続クッキーなど	約150項目
RPCサービス	RPCポートマッパ検出など	約70項目
SQLサーバー	パスワードのないMySQLなど	約400項目
SSHサーバー	SSHサーバーバックポートセキュリティパッチなど	約100項目
Webmailサーバー	IlohaMail検出など	約100項目
ウェブサーバー	サポート対象外のウェブサーバーソフトウェア検出など	約1000項目
サーバーサイド・スクリプト	クロスサイト・スクリプティングなど CGIとFORM処理の脆弱性（SQLインジェクションを含む）	約4200項目
ネットワークサービス	PPTPの検出など	約1200項目
ネットワークデバイス	TTL Anomaly 検知など	約700項目
バックドア	Windows Terminal Serviceの検出など	約200項目
ファイアウォール	DNSによるファイアウォールルールの通過(UDP 53番)など	約50項目
ポリシーチェック	Officeのファイル一覧など	約4000項目
情報収集	GETリクエストによる稼動サービス確認	約90項目
暗号化と認証	自己署名SSL証明書など	約250項目

脆弱性診断の結果をレポートで報告

PCI-DSSの基準に基づき検出した脆弱性を3段階に分類してレポートします。
発見された脆弱性については、脆弱性の内容説明に加え、対応策（次のアクション）についても提案します。



脆弱性のレベルについて

検出後72時間以内に修正が必要	**高リスク脆弱性**
	バックドア、ファイルに対する読み込み/書き込み権限、遠隔コマンド実行、トロイの木馬、パスワードなど機密情報の開示等
	中リスク脆弱性
	ホストのファイルに対する限定的なアクセス権限、ディレクトリー・ブラウジング/トラバーサル、フィルタールールやセキュリティー機構等のセキュリティー関連情報の開示、DoS(サービス妨害攻撃)、メール中継等の不正なサービス利用等
緊急性なし	**低リスク脆弱性**
	サーバー設定とテストから収集した情報レベルの項目 ホスト情報：診断対象ホストについての情報、脆弱性には含まれない。 推測されるプラットフォーム：TCP/IP、 スタックフィンガープリンティング経由で情報を収集し、OSを推測等