2017 年 10 月 17 日

キヤノンマーケティングジャパングループ

NEWS RELEASE

キヤノン IT ソリューションズ株式会社

「GUARDIANWALL Web ファミリー」の新バージョン 「GUARDIANWALL WebFilter」Ver1.1 を提供開始 ～外部攻撃対策機能を強化し、より安全な Web 通信を実現～

キヤノンマーケティングジャパングループのキヤノン IT ソリューションズ株式会社（本社：東京都品川区、代表取締役社長：神森晶久、以下キヤノン ITS）は、Web 情報漏えい対策・フィルタリングソリューション「GUARDIANWALL Web ファミリー」の新バージョン、「GUARDIANWALL WebFilter」Ver1.1 を、2017 年 10 月 30 日より提供開始します。標的型攻撃などの外部攻撃対策機能を大幅に強化しました。

GUARDIANWALL WebFilter

巧妙化、高度化した標的型攻撃が日々増加しており、「情報漏えい対策」は企業にとって大きな課題となっています。また、働き方改革による業務環境の多様化やクラウドサービスの本格普及に伴い Web を利用した業務の重要度は増しています。一方で、Web アクセスの制御においては業務に支障を与えず適切かつ柔軟な管理を要求され、ユーザーが意識することなく最新の脅威に対応することが急務となっています。

「GUARDIANWALL WebFilter」は、Web サイトへのアクセスをカテゴリごとに制御し、業務外の Web 利用の抑制に加え、外部へ送信される情報（Web メールや SNS などに添付されるファイル内のテキスト情報を含む）を検査する機能により、Web からの情報漏えいを防ぐソリューションです。

新バージョンでは、既知の脅威である危険な Web サイトへのアクセスを防ぎつつ、未知の脅威となるマルウェアによる不正通信を検知／遮断し、かつその通信を可視化する、外部攻撃対策機能の強化を行いました。業務の流れやクラウドサービスの利便性はそのままに、マルウェアの感染予防から、情報流出の抑止、感染拡大の阻止と、多層型の外部攻撃対策により、安全な Web 通信を実現します。

＜ 外部攻撃対策の機能強化項目 ＞

- 6 億人が利用する URL 情報を用い危険なサイトへのアクセスを遮断し、マルウェア感染を予防
- 独自解析技術を用いて、マルウェア感染端末特有の不正通信を検知／遮断し、情報流出を抑止
- 不正通信履歴から自動学習することで、類似する通信を遮断し、感染拡大を阻止
- 通信ログの管理機能強化により、監視負荷を軽減、マルウェア潜伏予見を支援

キヤノン ITS は、今後も増加する標的型攻撃への対応など、ユーザーからの要望に応えた製品強化を進めます。また、国内外のベンダーと積極的に「共創」を進め、総合情報漏えい対策ソリューション「GUARDIANWALL シリーズ」のラインアップ拡充を図ることで、より広範囲の情報漏えい対策を提供いたします。

- **報道関係者のお問い合わせ先：キヤノン IT ソリューションズ株式会社**
  企画本部 事業推進部 コミュニケーション推進課　03-6701-3603
- **一般の方のお問い合わせ先　：キヤノン IT ソリューションズ株式会社**
  基盤・セキュリティソリューション企画センター　03-6701-3336
- **「GUARDIANWALL シリーズ」ホームページ：　https://www.canon-its.co.jp/products/guardianwall/**

＜GUARDIANWALL WebFilter 新バージョン概要図＞

＜機能強化項目詳細＞

■外部攻撃対策の強化

・6 億人が利用する URL 情報を用い危険なサイトへのアクセスを遮断し、マルウェア感染を予防

全世界 6 億人以上の利用実績がある URL フィルタリングデータベースを用い、Web アクセスの都度、最新の URL カテゴリを判定する方式を採用しました。世界の 200 を超える収集源からリアルタイムに更新される「URL 情報」をもとに、外部攻撃や犯罪に多く用いられる、特に海外の危険な Web サイトへのアクセス遮断精度を向上し、マルウェアへの感染予防対策を実現します。また、Web サイトのカテゴリ判定率・更新率の大幅な向上により、既知の URL のほぼ全てをカテゴライズします。これにより、カテゴリごとの厳密な Web アクセス制御を実現するとともに、カテゴリ未登録の不審な URL へはアクセスを禁止した場合、より安全に Web を利用いただけます。

登録URL 1.4億以上　　利用人数 6億人以上

・独自解析技術を用いて、マルウェア感染端末特有の不正通信を検知／遮断し、情報流出を抑止

マルウェアに感染した端末が外部と不正に通信する際の、特有の通信を検知し、遮断します。フィルタリング技術に基づく独自の解析により、Web ブラウザーからの通常の Web アクセスと、不正通信との差異を検知します。外部との不正な長時間接続を遮断するコネクトバック通信検知機能※に加え、通信先が未知の URL であった場合の不正通信遮断のさらなる強化を実現し、情報漏えいを未然に防ぎます。

・不正通信履歴から自動学習することで、類似する通信を遮断し、感染の拡大を阻止

過去に検知／遮断した不正通信の通信先 URL や認証名、User-Agent を学習しブラックリストへ自動登録することで、類似通信を検知した際にあらかじめ指定したアクセス制御を即座に適用します。特にコネクトバック通信検知機能の検知から遮断まで一定の時間を必要とする点を補い、同じ感染端末から繰り返される不正通信や、新たに感染した別端末からの不正通信の自動かつ迅速な遮断を実現し、情報漏えい被害の拡大を防げます。

・通信ログの機能強化により、監視負荷を軽減、マルウェア潜伏予見を支援

一見では判読が困難な不審な通信ログを、Web アクセスの統計情報メニューから容易に確認ができるようになりました。不審な通信を可視化することで、システム管理者による Web 通信の監視負荷を低減させ、マルウェア感染の早期発見を支援します。

・危険な URL カテゴリと判定された Web サイトへのアクセス統計情報
・存在しない IP アドレス／URL へのアクセスなど、通信の確立に失敗したアクセス統計情報
・一般的にマルウェアでは対応していないプロキシ認証への失敗の統計情報

■その他強化機能

・Web メールやメッセンジャーのログ閲覧機能の対象サービスを更新（Outlook.com など）
・ユーザー要望に基づくユーザーインターフェースの改善（オンラインヘルプの充実 など）
・送信データのファイル形式やファイル内キーワードの検査機能が Office 2016 形式に対応

※ コネクトバック通信の検知機能について

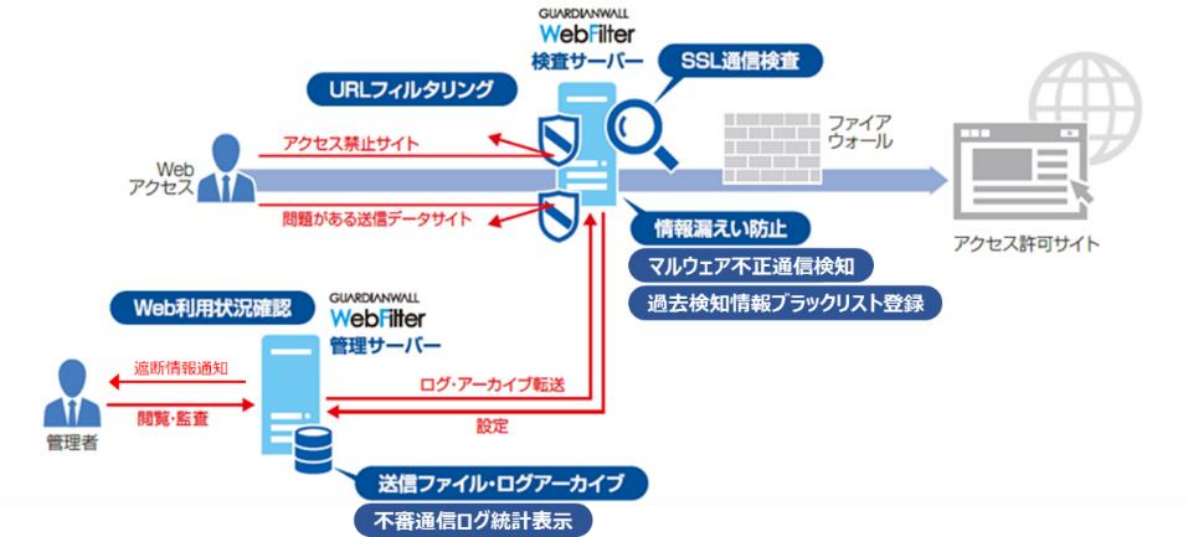
コネクトバック通信とは、マルウェアに感染した端末側から外部へ発信を行い、攻撃者に接続する通信方式です。
コネクトバック通信検知機能では、指定時間を超えて接続する同一通信を自動で遮断します。

＜初年度一般向け Linux 版ライセンス 価格例＞

製品名	価格（税別）	提供開始日
GUARDIANWALL WebFilter	150,000 円（25 ユーザー）	2017 年 10 月 30 日

＜GUARDIANWALL WebFilter について＞

GUARDIANWALL WebFilter 概要図



＜稼働環境＞

■Linux 版

プログラムバージョン		GUARDIANWALL WebFilter Ver 1.1.00
マシンスペック	CPU	インテル32bit・マイクロプロセッサー（Pentium以上） / インテル64bit・マイクロプロセッサー（Itanium 2は非対応） 1.0 GHz 1 コア以上（推奨：2.0 GHz 4 コア以上）
	メモリー	1 GB 以上（推奨：4 GB以上）
OS		Red Hat Enterprise Linux 5 / 6 / 7（32bit/64bit対応） ※Red Hat Enterprise Linux 5 は、Red Hat Enterprise Linux Desktop未対応
仮想環境		上記対応OSの動作を保証している仮想環境
IaaS環境		AWS（Amazon Web Services） Azure（Microsoft Azure）

■仮想アプライアンス版　（2017 年 11 月リリース予定）

プログラムバージョン	GUARDIANWALL WebFilter Ver 1.1.00
仮想環境	VMware ESXi 6.0 Hyper-V（Microsoft Windows Server 2012 R2 / 2016）
CPU	2 コア
メモリー	4 GB以上

＜GUARDIANWALL シリーズについて＞

「GUARDIANWALL シリーズ」は、「GUARDIANWALL Mail ファミリー」、「GUARDIANWALL Cloud ファミリー」、「GUARDIANWALL Web ファミリー」から構成する、総合情報漏えい対策ソリューションです。企業活動に欠かせないメールと Web、利用拡大しているクラウドサービスにおいて、重大なセキュリティ事故につながる情報漏えいを防止する、ソリューション群を提供しています。