

2012 年 1 月 20 日  
株式会社日立ソリューションズ

## ファイアウォールログ解析製品の最新版を販売開始 標的型サイバー攻撃によって外部へ情報を漏えいさせるバックドア通信を早期に発見

株式会社日立ソリューションズ(本社:東京都品川区、取締役社長:林 雅博/以下、日立ソリューションズ)は、ファイアウォールのログ解析製品の最新版で、バックドア(\*1)通信による外部への不正なアクセスの遮断ログをレポートできる「FIREWALLstaff(ファイアウォールスタッフ)01-05」の販売を 1 月 23 日から開始します。本製品をファイアウォールと組み合わせることで、標的型サイバー攻撃によって、情報を外部に漏えいさせるバックドア通信を早期に把握することができ、企業における「出口対策」を強化します。

(\*1)バックドア:クラッカーがコンピューターをウイルスに感染させる際に、次回も気づかれずに侵入できるように設置する裏口

昨今、政府機関や特定企業を狙った標的型サイバー攻撃による情報漏えい事故が相次いでいます。これまで企業のサイバー攻撃への対策は、ファイアウォールやマルウェア(\*2)対策ソフトによって外部からの侵入を防ぐ「入口対策」が主流でした。しかし、マルウェアも多様化しており、ウイルスに感染した PC に設置されたバックドアなどを經由して、外部に重要な情報が漏えいするのを防ぐ「出口対策」が求められています。

(\*2)マルウェア:コンピューターに侵入し、感染活動や破壊活動を行ったり、情報を外部に漏えいさせたりする有害なソフトウェア

ファイアウォールによる「出口対策」の1つとして、バックドア通信を遮断し、外部への情報漏えいを防止する方法があります。バックドア通信を遮断するには、外部へのアクセスは必ず認証が必要となるプロキシサーバーを經由するようネットワーク設定を行い、さらに、プロキシサーバーを經由していない外部へのアクセスは遮断するようにファイアウォールの設定を行うことが第一の対策です。その上で、遮断すると同時に、ファイアウォールの遮断ログからバックドア通信が発生したことを早期に把握し、対策を施すことが重要です。

今回、販売を開始する「FIREWALLstaff」は、ポート番号単位でファイアウォールが外部へのアクセスを遮断した通信の接続元と接続先を集計できる機能を追加しました。これにより、バックドア通信で利用されることが多いポート番号であるWebアクセスのHTTPや個人情報などを入力するHTTPSなどのレポートを集中的にチェックすることで、接続先情報から攻撃者を特定したり、接続元情報からバックドアを仕掛けられたPCを早期に発見することで、標的型サイバー攻撃対策の出口対策を強化します。また、「FIREWALLstaff」のログ解析レポートは、日本語でわかりやすく記載されているため、専門知識がなくても、チェックを行うことが可能です。

日立ソリューションズは、標的型サイバー攻撃への対策として、以下の製品・サービスを組み合わせ、「標的型攻撃防御ソリューション」として提供します。

1. お客様のセキュリティ対策レベルを診断する「サイバー攻撃(APT)対策診断サービス」
2. 標的型メール攻撃へ対応する「秘文 標的型メール攻撃対策ソリューション」、「Sendmail」、「Messaging Gear」
3. 「出口対策」のための「パロアルトPAシリーズ」、「FIREWALLstaff 01-05」

## ■ 「FIREWALLstaff」について

FIREWALLstaff は、ファイアウォール／UTM のログ解析製品です。ファイアウォールのログを解析して、通信の方向別／通過した通信と遮断された通信別／プロトコル(ポート番号)別に『どのマシンが何処に、どのくらいアクセスしているか』を集計することができます。

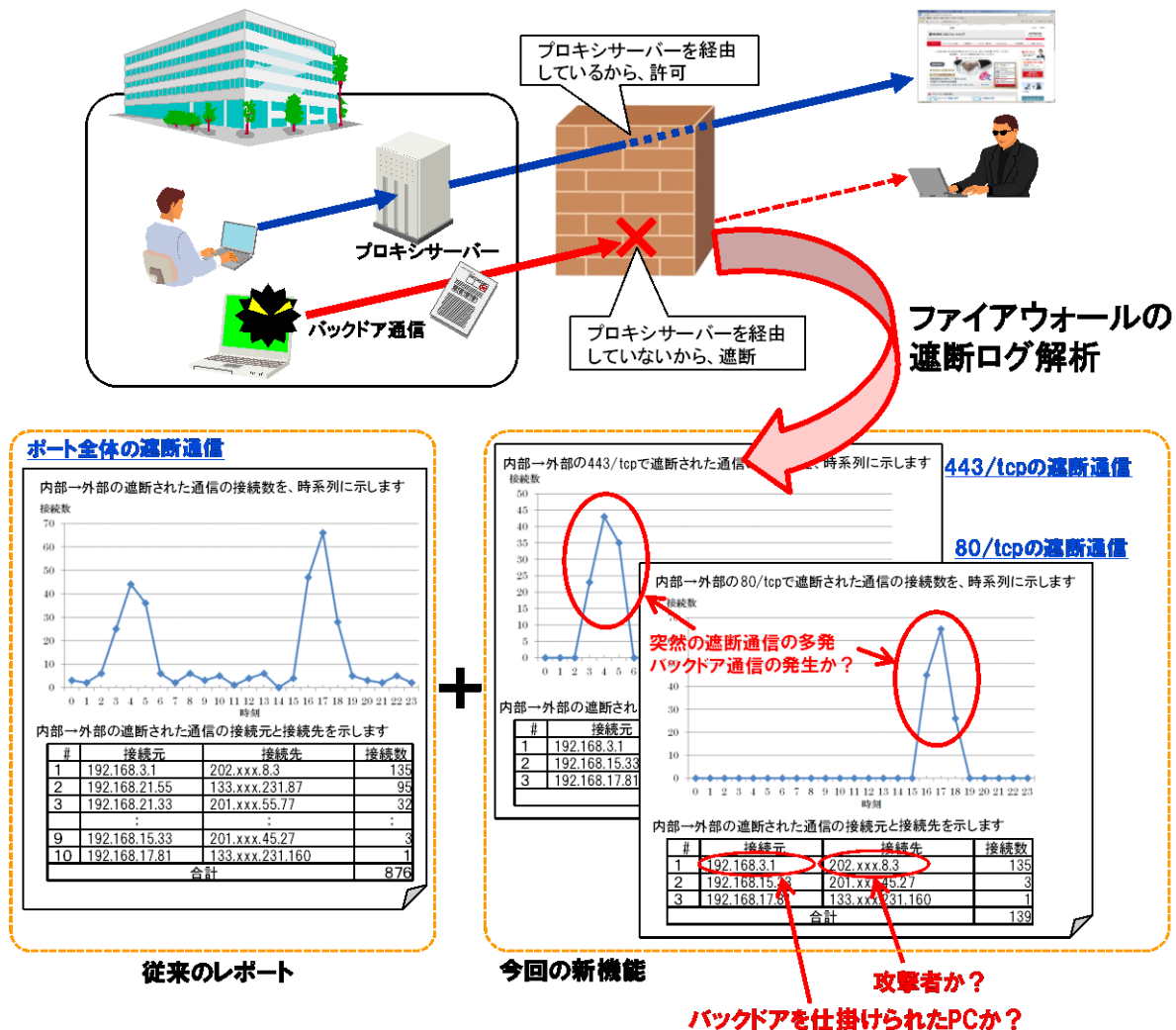


図. 「FIREWALLstaff」の遮断された通信の分析イメージ

## ■ 価格

製品名	価格(税込)
FIREWALLstaff 01-05 ライセンス	630,000円～756,000円

※ FIREWALLstaffは、ファイアウォール台数のライセンスが必要です

## ◎ 株式会社 日立ソリューションズ

本社 〒140-0002 東京都品川区東品川四丁目12番7号  
 本社別館 〒108-8250 東京都港区港南二丁目18番1号  
 Tel:03-5780-2111 ホームページ: <http://www.hitachi-solutions.co.jp/>

日立ソリューションズ

■ 対応ファイアウォール

- Juniper Networks NetScreen/SSG
- Juniper Networks SRX
- 富士通 IPCOM EX
- Check Point
- Fortinet FortiGate
- Palo Alto Networks PA

■ 販売開始時期:2012年1月23日

■ 製品紹介URL: <http://www.hitachi-solutions.co.jp/firewallstaff/sp/>

<商品に関するお問い合わせ先>

ホームページ: <https://www.hitachi-solutions.co.jp/inquiry/> Tel:0120-571-488

<報道機関からのお問い合わせ先>

担当部署: コーポレート・コミュニケーション本部 広報・宣伝部

担当者: 宮本、廣納(ひろのう)

Tel:03-5479-5013 Fax:03-5780-6455 E-mail: [koho@hitachi-solutions.com](mailto:koho@hitachi-solutions.com)

日立ソリューションズは、お客様の業務ライフサイクルにわたり、オンプレミス・クラウド連携を始めとする豊富なソリューションを全体最適の視点で組み合わせ、ワンストップで提供する『ハイブリッドインテグレーション』を実現します。

- ※ FIREWALLstaff、Messaging Gear は、株式会社日立ソリューションズの登録商標です。
- ※ Sendmail は、センドメール社の登録商標です。
- ※ NETSCREEN、JUNIPER NETWORKS はそれぞれジュニパーネットワークス社の登録商標です。
- ※ IPCOM は、富士通株式会社の登録商標です。
- ※ Check Point は、Check Point Software Technologies Ltd.の登録商標です。
- ※ FORTIGATE はフォーティネット社の登録商標です。
- ※ PALO ALTO NETWORKS はパロアルトネットワークス社の登録商標です。
- ※ 記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

---

◎ 株式会社 日立ソリューションズ

本社 〒140-0002 東京都品川区東品川四丁目12番7号  
本社別館 〒108-8250 東京都港区港南二丁目18番1号  
Tel:03-5780-2111 ホームページ: <http://www.hitachi-solutions.co.jp/>

日立ソリューションズ



-----  
このニュースリリース記載の情報(製品価格、製品仕様、サービスの内容、発売日、お問い合わせ先、URL等)は、発表日現在の情報です。予告なしに変更され、検索日と情報が異なる可能性がありますので、あらかじめご了承ください。  
-----

