News Release

HITACHI
Inspire the Next

2011年11月21日
株式会社日立ソリューションズ

標的型サイバー攻撃への対策を実現
サイバー攻撃（APT）対策診断サービスと情報漏洩防止ソリューション「秘文」により攻撃を防御

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、昨今、情報漏えい事件が相次いでいる標的型サイバー攻撃への対策として、現状のセキュリティ対策の対応度合いを診断する「サイバー攻撃（APT）対策診断サービス」と、特に対策が急がれる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」の提供を、12月1日より開始します。現状のセキュリティ対策の不足部分を明確にし、標的型メール攻撃へ対応することで、外部からの脅威を低減し、企業内からの情報漏えい防止を実現します。

ここ最近、特定の企業や公的機関の機密情報を標的にしたサイバー攻撃による情報漏えい事件が相次いでいます。このような攻撃は標的型サイバー攻撃と呼ばれています。その中でも、APT（Advanced Persistent Threat)や「新しいタイプの攻撃」と呼ばれる攻撃は、人間の心理的な隙やまだ公表されていないコンピュータシステムの脆弱性を利用しているため、一定のセキュリティ対策を行っている企業であっても被害を受けるケースがあり、従来の情報漏えい事件と比べ被害が深刻化しています。

標的型サイバー攻撃に対抗するためには、現状のセキュリティ対策がどの程度実施できているかを見極めたうえで、APTを想定した新しい観点での対策を実施することが重要です。

日立ソリューションズでは、標的型サイバー攻撃への対策として、現状のセキュリティ対策状況を診断、分析し、必要となるセキュリティ要件を整理する「サイバー攻撃（APT）対策診断サービス」と、標的型メール攻撃に対しては企業の入口、出口、社内の3ポイントで対策を実施する「秘文 標的型メール攻撃対策ソリューション」を提供します。また、日立ソリューションズでは、セキュリティシステムの導入に向けたコンサルティングから、「秘文」に代表される独自の情報漏えい防止ソリューションや導入・運用が容易なアプライアンスを活用したソリューションの提供まで、企業の情報セキュリティに関するライフサイクルを全てカバーしており、今回提供を開始するサービス、ソリューションを組み合わせることで、効果的に標的型サイバー攻撃対策が実現できます。さらに、標的型サイバー攻撃の入口対策、出口対策、情報の窃取対策を行う関連ソリューションを今後販売していく予定です。

■ 「サイバー攻撃（APT）対策診断サービス」の主な特長

1. 実事案をもとにした分析

標的型サイバー攻撃の実例をベースに分析された、独立行政法人 情報処理推進機構（IPA）発行の『「新しいタイプの攻撃」の対策に向けた設計・運用ガイド（第1版）』に、日立ソリューションズがこれまで企業や公共機関など業種・業態を問わずネットワーク・セキュリティ関連のソリューションを提供してきたノウハウを加えて作成したテンプレートに基づき、専門の技術者が従来のセキュリティ対策の実施度合いを評価・分析します。

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　ﾎｰﾑﾍﾟｰｼﾞ:http://www.hitachi-solutions.co.jp/

日立ソリューションズ

2. 短期間で診断結果を報告

サービス開始から約1ヶ月で診断結果を報告します（標準的な構成の場合）。短期間で診断結果が出るため、世の中の脅威に素早く対応できます。

3. 豊富な経験に基づいたセキュリティ要件の整理

ネットワーク・セキュリティや「秘文」を中心としたエンドポイントセキュリティなどのソリューション提供における豊富な経験に基づいて、専門の技術者が必要となるセキュリティ要件を整理します。

■「秘文 標的型メール攻撃対策ソリューション」の主な特長

1. 入口対策

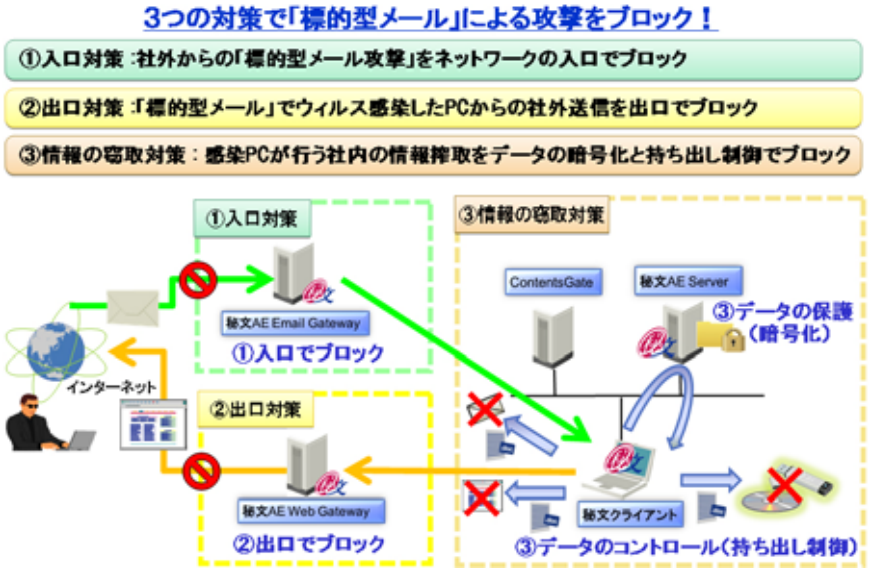
疑わしいメールを受信しないようにネットワークの入口でブロックします。「秘文AE Email Gateway」によって、送信元サーバーの信頼度や添付ファイルタイプをチェックし、ウイルス感染など危険性のあるメールは社員のPCに配信せずに一時的に専用サーバーに保留します。

2. 出口対策

ウイルス感染したPCから社外に情報を流出できないように社外送信を出口でブロックします。多くのウイルスは不正な社外サイトにアップロードする方法で情報を盗み出そうとします。「秘文AE Web Gateway」によって、PCからアクセスする社外サイトの危険性をチェックし、社外サイトへの機密情報のアップロードを制限します。さらに、「秘文AE Web Gateway」とコンテンツ承認基盤「ContentsGate」を連携させることで承認を受けていない文書の社外サイトへの持ち出しを防止します。

3. 情報の窃取対策

暗号化と持ち出し制御によりウイルスが情報を盗み出そうとする動作からデータを保護します。「秘文シリーズ」とその関連製品によって、ファイルサーバー上のデータを暗号化し、機密情報の窃取ができないようにします。また持ち出し制御機能のコントロールにより、許可されていない機密ファイルのメール送信、アップロード、外部記録媒体へのコピーを禁止します。



図：秘文「標的型メール攻撃」対策ソリューションの概要

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/

■ **価格**

1. **サイバー攻撃（APT）対策診断サービス**

サービス名	価格（税込）
サイバー攻撃（APT）対策診断サービス	個別見積

2. **秘文 標的型メール攻撃対策ソリューション**

製品名			価格（税込）
入口対策		秘文AE Email Gateway	577,500円
出口対策		秘文AE Web Gateway	892,500円
情報の窃取対策	データ保護	秘文AE Server	1,365,000円
	データコントロール	ContentsGate Base	2,520,000円

※ 秘文「標的型メール攻撃」対策ソリューションは100ユーザーで利用する場合の価格です。

※ データコントロールを入口対策、出口対策と連携する場合には、制御したい内容に応じて関連製品のライセンスが必要になります。

■ **販売開始時期**：2011年12月1日

■ **製品紹介URL**

サイバー攻撃（APT）対策診断サービス

http://www.hitachi-solutions.co.jp/security_consul/sp/apt_assess.html

秘文「標的型メール攻撃」対策ソリューション

http://www.hitachi-solutions.co.jp/hibun/sp/product/gatewaysol.html

＜商品・サービス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：槇田、鈴木

Tel：03－5479－5013　Fax：03－5780－6455　E-mail：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。

- -

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もありますので、あらかじめご了承ください。

- -

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 ﾎｰﾑﾍﾟｰｼﾞ:http://www.hitachi-solutions.co.jp/