Vol. 10
2012.4

日立ソリューションズ

Newsletter

株式会社日立ソリューションズ　http://www.hitachi-solutions.co.jp/

今月号のキーワード　情報漏洩を防止するには出口対策が重要

特集　日立ソリューションズの「標的型サイバー攻撃対策ソリューション」

近年、政府や企業の情報システムに不正に侵入し、情報を盗み出す「標的型サイバー攻撃」が相次いで発生しています。「標的型サイバー攻撃」の対策には、外部への情報漏洩を防止するための出口対策、社内の情報システムへの侵入を防止するための入口対策があります。ここでは、それぞれの対策の概要と日立ソリューションズが提供する製品・サービスを紹介します。

此内　優

システムプラットフォーム事業部
プロダクト拡販支援センタ
センタ長

■「標的型サイバー攻撃」とその対策について

「標的型サイバー攻撃」は、ソフトウェアの脆弱性などを悪用し、複数の攻撃を組み合わせ、政府や企業の情報システムに不正に侵入し、ソーシャル・エンジニアリング（人間の心理的な隙や、行動のミスにつけ込んで秘密情報を入手する手法）により情報を盗み出すことを目的とした攻撃と定義されています。その対策として、日立ソリューションズは、多様化するセキュリティリスクに対応した情報漏洩防止ソリューション「秘文シリーズ」と最新のネットワーク機器を組み合わせた多層防御、ならびにセキュリティ診断サービスを含めたトータルセキュリティソリューション（図1）を提供しています。

標的型サイバー攻撃対策には、社内の情報システムから外部への情報漏洩を防ぐ出口対策と外部からの侵入を防ぐ入口対策があります。近年外部からの情報システムへの攻撃が多様化していることから、入口対策で完全に侵入を防ぐことは難しくなっています。そのため万が一、侵入されても外部への情報漏洩を防止できる出口対策が重要となります。出口対策を次の4つに分け、多層防御を実現することで情報漏洩リスクを軽減することができます。

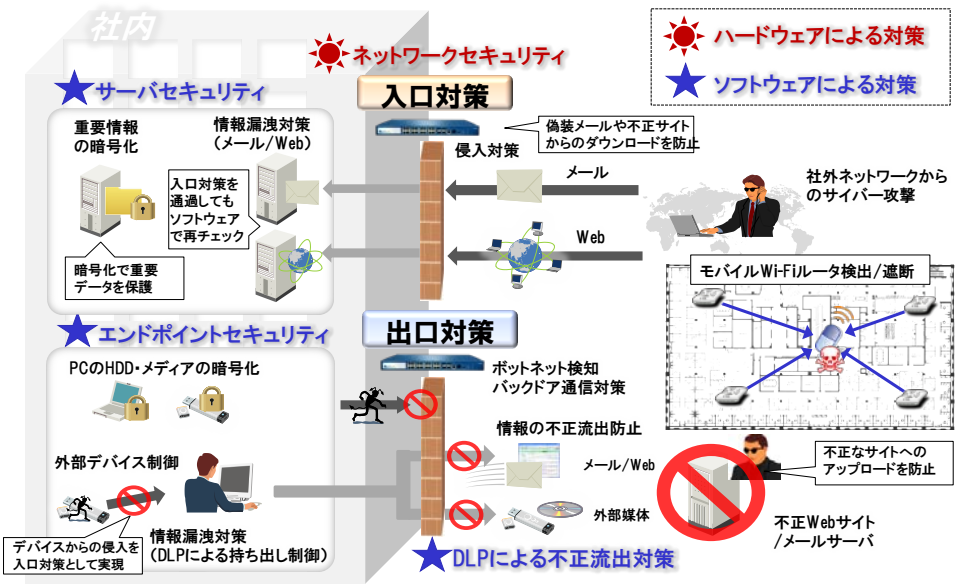

図1　標的型サイバー攻撃対策ソリューションの全体像

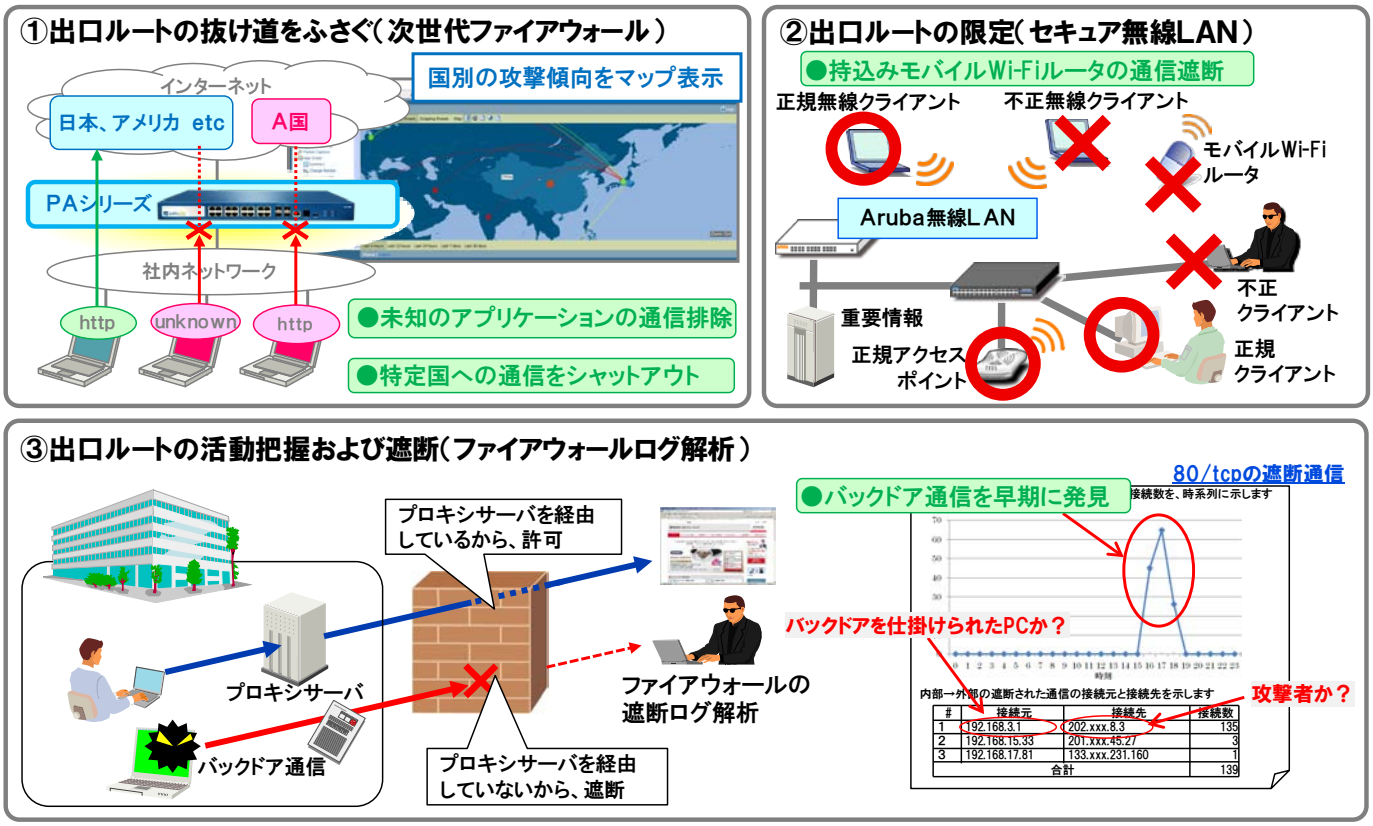

図2　標的型サイバー攻撃の出口対策（ネットワーク機器）

① 出口ルートの抜け道をふさぐ
② 出口ルートの限定
③ 出口ルートの活動把握および遮断
④ 情報の不正流出防止

■ネットワーク機器による出口対策

「①出口ルートの抜け道をふさぐ」の対策（図2の①）では、日立ソリューションズが販売する米パロアルトネットワークス社の次世代ファイアウォール「PAシリーズ」を利用します。同製品では、使用しているアプリケーション単位で通信を識別し、未知のアプリケーションの通信を排除することで従来のファイアウォールでは検知できなかった抜け道をふさぐことが可能となります。また、「標的型サイバー攻撃」で利用されることが多い特定国への通信も遮断できます。

「②出口ルートの限定」対策（図2の②）については、ウェブアクセスを正規ルート（プロキシ経由）に限定し、参照するだけでウィルスに感染するような悪質サイトへの通信を遮断するというのが一般的な対策です。ところが意外と見落としがちなのが、最近普及の著しいモバイルWi-Fiルータ経由の出口です。スマートフォン、タブレット端末用に私物のモバイルWi-Fiルータを社内に持ち込めば、管理外の出口ができてしまうので非常に危険です。米アルバネットワークス社のセキュア無線LANシステム「Arubaシリーズ」であれば、無線空間を監視し、私物で持ち込まれたモバイルWi-Fiルータの場所を把握することはもちろん、遮断パケット送信して通信を遮断することができます。

「③出口ルートの活動把握および遮断」（図2の③）については、限定した出口の正規ルートのログを取得して、普段と違った活動が行われていないかなどを分析することで、バックドア通信の予兆を把握することができます。日立ソリューションズのファイアウォールログ解析製品「FIREWALLstaff」は、ファイアウォールがポート番号単位で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することで、情報を外部に漏洩しようとする通信を早めに把握できます。また、一時的に通信の遮断が多くなるなど平常時と異なる状態を時系列のグラフによって可視化して把握できるため、管理者が標的型サイバー攻撃を受けているか見極めるための判断材料を提供します。

■秘文シリーズによる出口対策

日立ソリューションズは、長年、情報漏洩防止ソリューション「秘文シリーズ」にて、従業員の過失事故や悪意ある内部犯行などを阻止するさまざまな対策を提供してきました。「秘文シリーズ」による対策は、ユーザー認証や暗号化などにより情報コンテンツを厳密に保護する仕組みであるため、標的型サイバー攻撃の特徴である巧妙な情報詐欺は難しく、偽装されにくいといえます。「④情報の不正流出防止」（図3）

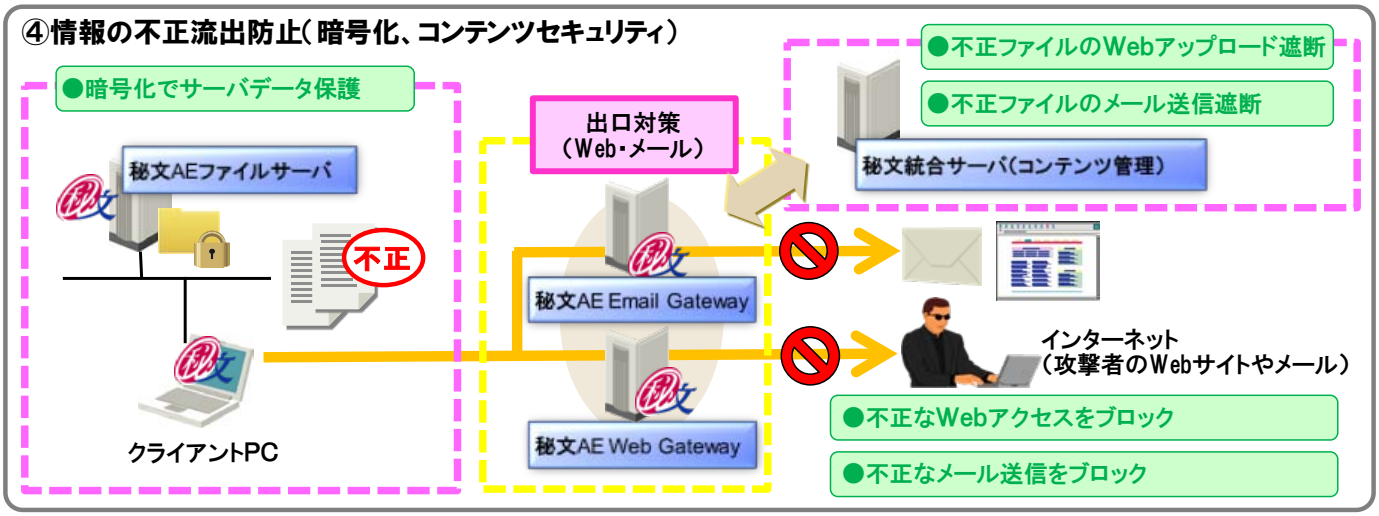

図3　標的型サイバー攻撃の出口対策(秘文シリーズ)

の対策としては、「秘文AEファイルサーバ」で利用したサーバ上の重要情報を暗号化することで不正な情報詐取があった場合でも情報漏洩を防止できます。また、「秘文統合サーバ(秘文 Server Extension)」の厳密なコンテンツ管理により、許可されていない情報(ファイル)が社外へ流出することを防止できます。また、対策可能な情報漏洩経路は、バックドア通信として使われることが多いウェブ経路を「秘文AE Web Gateway」で監視し、メールでの情報流出に備えては「秘文AE Email Gateway」での対策が可能となっています。

■3つの侵入経路の入口対策

出口対策同様に重点を置くのが以下の3つの侵入経路からのウィルス感染などの脅威を防ぐ入口対策です。

① メールからの侵入防止
② ウェブサイトからの侵入防止
③ 外部デバイスからの侵入防止

出口対策で紹介した「秘文AE Email Gateway」ならびに「秘文AE Web Gateway」は、入口対策として「①メールからの侵入防止」と「②ウェブサイトからの侵入防止」にも利用できます。具体的なメール侵入対策は、偽装した添付ファイルをブロックする機能、マルウェアの危険性のあるメールは一時保留とし安全を確認後にコンピューターで受信する機能などがあります。ウェブ侵入対策は、悪意のあるサイトからウィルス付きファイルをダウンロードすることを阻止したり、信頼できないサイトへの接続防止やダウンロードできるサイトを制限することができます。

また、「③外部デバイスからの侵入防止」は、外部デバイスを制御する「秘文AE Information Fortress」と拡張オプションソフトウェアにより、許可されていないデバイスを一切利用できなくする設定や、利用する場合は利用者への警告や管理者への通報などにより、ウィルス感染リスクの高い私物USBメモリなどの持ち込み利用を防止できます。

■ウィルス拡散防止と診断サービス

最後に、ウィルスが内部に侵入してしまった後の拡散防止として、社内に接続されたコンピュータが最新の脆弱性情報に対応しているかを管理することも重要です。また、企業のセキュリティ対策状況を専門家が診断し、どのような対策を追加すべきか提示する「診断サービス」も提供しています。日々巧妙化している「サイバー攻撃等」との闘いに終わりはありません。日立ソリューションズは、今後もあらゆる脅威に対応して、安全・安心の製品・サービスを提供していきます。

■これまでの関連リリース

・多様化するセキュリティリスクに対応した「秘文 V10」を販売開始(2012年4月23日)
http://www.hitachi-solutions.co.jp/company/press/news/2012/0423.html

・ファイアウォールログ解析製品「FIREWALLstaff」の最新版を販売開始(2012年1月20日)
http://www.hitachi-solutions.co.jp/company/press/news/2012/0120.html

・次世代ファイアウォールパロアルトPAシリーズに対応する標的型サイバー攻撃対策を強化(2011年12月20日)
http://www.hitachi-solutions.co.jp/company/press/news/2011/1220.html

・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 (2011年11月21日)
http://www.hitachi-solutions.co.jp/company/press/news/2011/1121.html

最近のニュースリリース

当社の発信したニュースリリースの詳細は、当社ホームページの以下URL
http://www.hitachi-solutions.co.jp/company/press/　でご覧いただけます。

■リメディアル教育向け学習支援システム「学習ワンダーランド」を販売開始
ゲーム感覚のインターフェースにより学生の学習意欲を向上

■画像に埋め込んだ二次元コードからWebサイトへ誘導する「活文　Photocode」をSaaS型で提供
デザイン性を維持することで、効果的な広告宣伝活動を実現

■次世代コラボレーションシステムをマイクロソフト テクノロジー センターに設置
実機による利用体験が可能に

TOPICS

国際協力機構の研修生と農業IT化への取り組みに関する研修を開催

日立ソリューションズは、2012年3月28日に本社にて農業IT化への取り組みに関する研修を行いました。本研修は、独立行政法人 国際協力機構（JICA）の活動の一環として、ガーナ、レソト、ナイジェリア、タンザニア、ウガンダ、スーダンの「農業のITシステム化技術研修生」として来日した農業関連政府機関の方々8名を対象に、自国の農業の発展に寄与できる人材を育成することを目的に開催したものです。各種農業における情報システムを理解し活用することで、農産物の生産性向上と適切な政策決定につなげ、開発途上国における食料の安定供給や農産物の高付加価値化、および、市場対応力強化を図るものです。

昨年に続き当社が本研修の講義を担当し、研修生は日本における導入事例を参考に、各国でどのように地理情報システム（GIS）を導入できるかなどの議論や発表を行いました。

GISを利用した農業IT化について議論を行う様子

商　号	株式会社日立ソリューションズ
本社事務所	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（大代表）
URL	http://www.hitachi-solutions.co.jp/
設立年月日	1970年9月21日
従業員数	13，367名（2012年3月31日現在、連結）
事業内容	業務コンサルティング、ITコンサルティング、システム設計、保守、システム運用、システム開発のライフサイクルを一括してサポートするワンストップサービスを提供
主要製品	機密情報漏洩防止ソリューション「秘文」、就業管理システム「リシテア」、指静脈認証システム「静紋」、 Juniper Networks製品、電子ドキュメントトータルソリューション「活文」、インタラクティブ電子ボード「StarBoard」、 エンタープライズ型地理情報システム「GeoMation」、統制IT基盤提供サービス「SecureOnline」、JP1ソリューションサービス他
認証取得	ISO9001、ISO14001、ISO27001
主な子会社および関連会社	日立ビジネスソリューション（株）、（株）日立東日本ソリューションズ、（株）日立中国ソリューションズ、 （株）日立ソリューションズバリュー、（株）日立ソリューションズデザイン、（株）日立ソリューションズサービス、 （株）日立ソリューションズ九州、（株）DACS、（株）アイネス、（株）ビジネスブレイン太田昭和

＊ 記載されている会社および製品名は各社の商標または登録商標です。

ニュースレター、転載、取材に関するお問い合わせ
Tel:03-5479-5013［広報・宣伝部：廣納・宮本］
E-mail:koho@hitachi-solutions.com

発行日　2012年4月27日