HITACHI
Inspire the Next

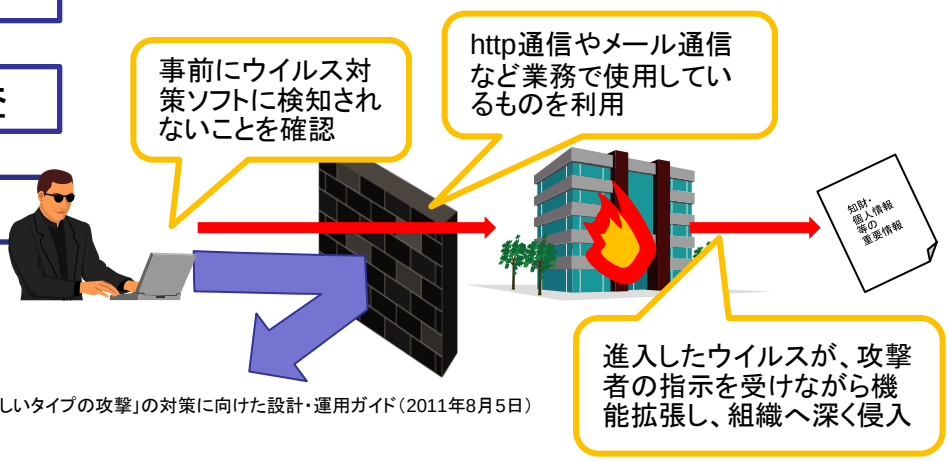
サイバー攻撃(APT)対策診断サービス

日立ソリューションズは、標的型サイバー攻撃であるAPT(Advanced Persistent Threats)に対して、どの程度の対策が実施されているかを診断し、追加のセキュリティ要件を明確にする「サイバー攻撃(APT)対策診断サービス」を提供します。

APT(Advanced Persistent Threats)とは

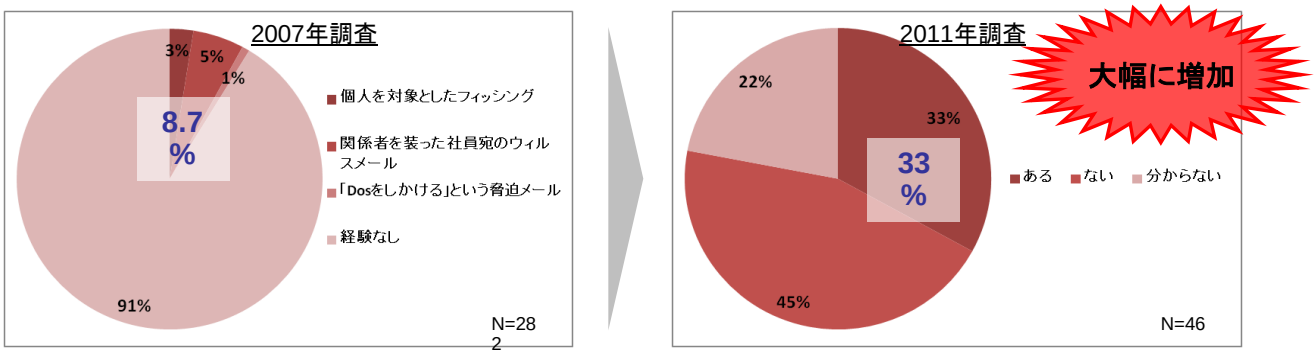
1)標的組織に感染
2)自己更新・拡張
3)標的システムを調査
4)本攻撃

「新しいタイプの攻撃」とも呼ばれ、対策の状況に合わせて持続的に攻撃が続けられ、少しづつ目的の情報に迫るため、従来の対策をすり抜けて重要な情報を盗み出したり、重要システムを破壊するような攻撃。



参考:IPA「新しいタイプの攻撃」の対策に向けた設計・運用ガイド(2011年8月5日)

組織名	概要	発生月
某原子力関連施設(イラン)	Stuxnet(スタクスネット)により、ウラン濃縮施設に侵入し、設置されている遠心分離機9,000基のうち、約1,000基を破損	2010年7月
某銀行	ネットバンキングにおいて、預金の不正な引き出しや不正アクセスなどの被害が発生	2011年8月
某製造業	本社、工場、研究所など国内11拠点にあるサーバーおよびパソコン83台がウィルス感染し、一部パソコンのシステム情報(ネットワークアドレスなど)の情報が流出	2011年8月
某政府機関	某政府機関所属の3人に標的型メールが送付され1人がメールを開き感染、ネットワーク上の他の端末のID/パスワードを取得、サーバー上の情報を外部から閲覧可能な状態に変更	2011年10月



出典:経済産業省 サイバーセキュリティと経済 研究会報告書中間とりまとめ(2011年8月5日)

サイバー攻撃(APT)対策診断サービスにより、自社の対策状況と必要な追加の対策内容が整理できます。

株式会社 日立ソリューションズ

情報漏洩防止ソリューション～サイバー攻撃（APT）対策診断サービス～

● 日立ソリューションズのサイバー攻撃（APT）対策診断サービス

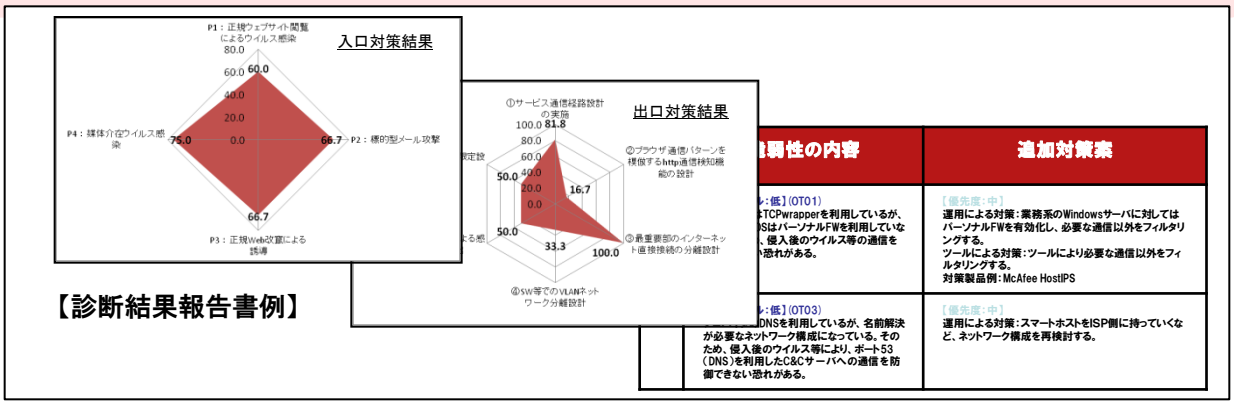
お客様においてAPTの脅威が現実のものとなった場合を想定し、現状のネットワーク構成等に問題点がないかを確認します。また、問題点がある場合はその対策方針について検討します。

STEP1. 現状の確認

STEP2. 漏洩シナリオ検討

STEP3. ヒアリング実施

STEP4. 報告会実施



● サイバー攻撃（APT）対策診断サービスの特徴

■ 実事案をもとにした分析

過去に実際に起きたAPTの事案をベースに分析された、
IPA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）をもとに
評価・分析致します。

■ 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。

■ 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・セキュリティのソリューション提供における豊富な経験に基づいて
必要となるセキュリティ要件を整理します。

商品・サービスに関するお問い合わせ

【電話による受付】

0120-421-126［通話料無料］

受付時間 10:00～17:30　月曜日～金曜日（祝日、弊社休業日を除く）

【WEBによる受付】

https://www.hitachi-solutions.co.jp/inquiry/

株式会社 日立ソリューションズ

http://www.hitachi-solutions.co.jp/