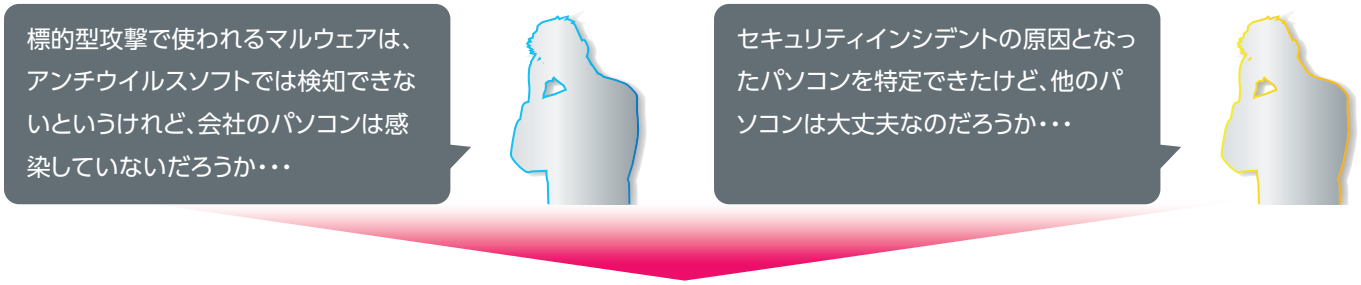
WIDE ANGLE
INFORMATION SECURITY AND RISK MANAGEMENT

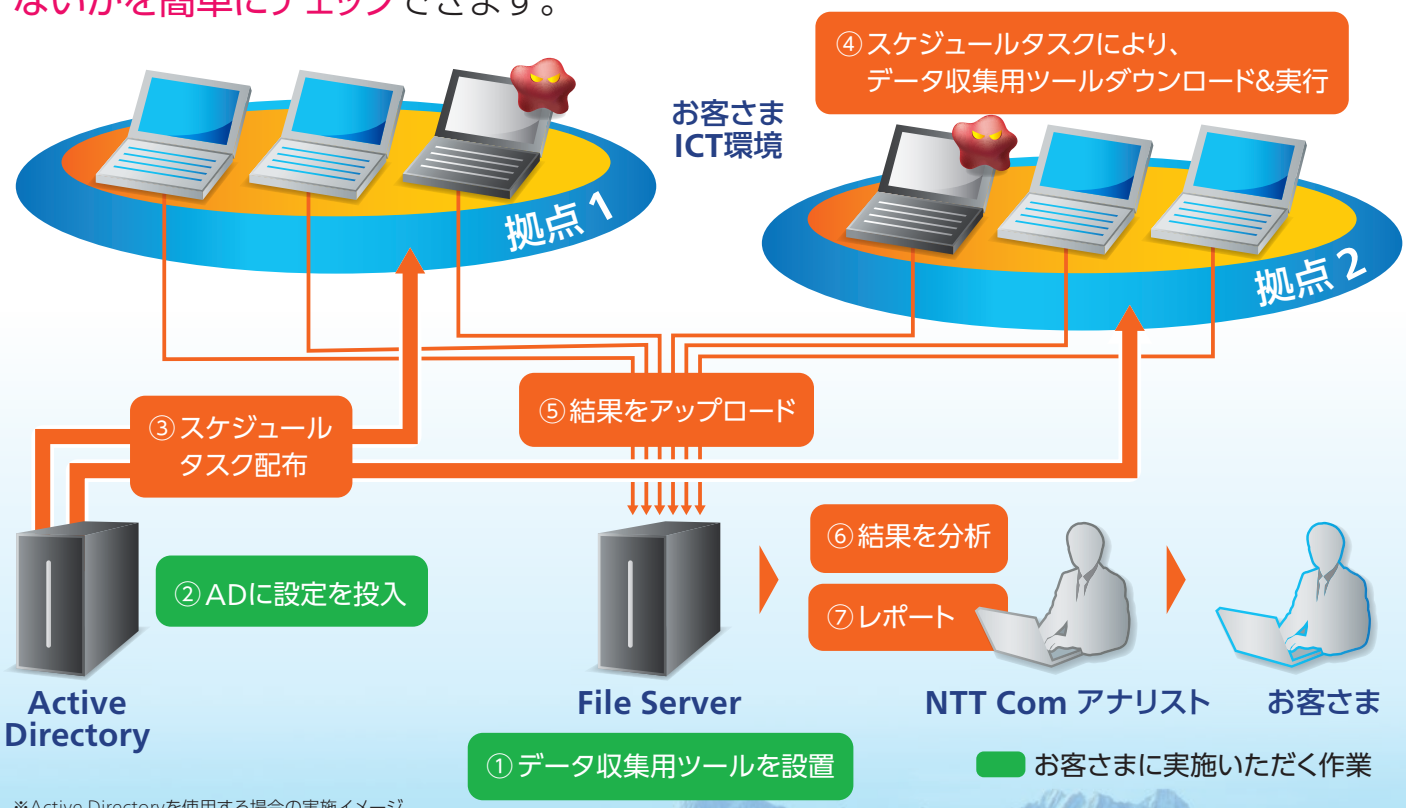
NTT Communications
Transform. Transcend.

インシデントレスポンス
標的型マルウェア感染端末調査

標的型攻撃などで使われる、アンチウィルスソフトでは
検出できないマルウェアに端末が感染していないか、
お客さまのICT環境の健康診断ができます。



弊社にて独自に開発した調査ツールをお客さまのICT環境上にある端末で実行していただくだけで、**アンチウイルスソフトでは検出できない不審なプログラムが潜んでいないかを簡単にチェック**できます。



※Active Directoryを使用する場合の実施イメージ

NTT Com はここが違う！

機械的なマルウェア検出ではなく、弊社インシデントレスポンスサービスで得られた知見に基づいたフォレンジックアナリストによるマルウェア検出サービスです。

特徴1　ディスクフォレンジックにおけるマルウェア特定技術を応用

インシデントレスポンスでは、ディスクフォレンジックによりアンチウイルスソフトやセキュリティ機器で検知できないマルウェアを見つけることができます。そこで利用される技術のうち、特にマルウェアの検知実績が多い手法を応用しています。

特徴2　多数の自動起動設定から不審なものを洗い出すテクニック

端末上で自動起動するプログラムは、1台あたり300を超えることもあります。インシデントレスポンスで日々蓄積しているテクニック・ノウハウを活用し、大量の自動起動プログラムの中からマルウェアを検出します。

特徴3　アンチウイルスソフトでは検出できないマルウェアの検出実績多数

発見されにくい標的型マルウェアや、ファイルをもたないマルウェア（ファイルレスマルウェア）の検出実績が多数あります。いずれもアンチウイルスソフトでは検出できなかったマルウェアを、本手法により検出しています。

サービス内容

■ 価格（参考）
500台まで　100万円（税別）　※500台以上についてはお問い合わせください

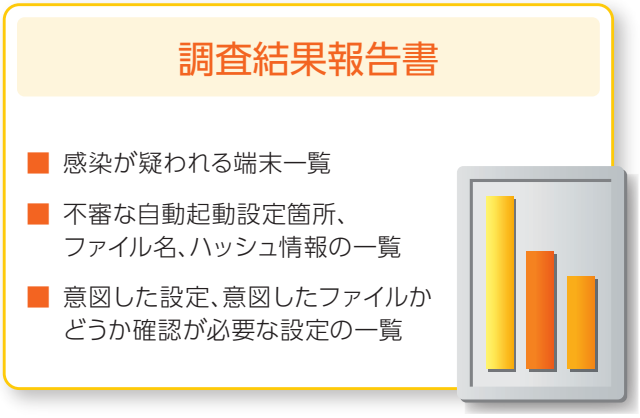
■ 提供内容
Windows端末で取得した自動起動設定およびその他揮発性情報*1の分析によるマルウェア感染端末有無の判定

■ 調査期間
解析にかかる時間は調査対象数に依存します。
※調査対象端末が500台の場合、ツール実行結果を弊社に送付いただいてから約1週間

■ 成果物
調査結果報告書を電子ファイルにて提出します。

■ 情報の管理
ツールの実行結果、報告書等、調査に使用したデータは報告1か月で破棄します。

■ 調査期間
解析にかかる時間は調査対象数に依存します。



【提供条件】（抜粋）

・調査対象端末に弊社指定ツールをローカル管理者権限またはシステム権限にて、Active Directory（AD）や資産管理ソフトなどで配布、実行することが可能であること
- ADを使用する場合、ADで必要な設定をお客さまにて実施頂けること
- 資産管理ソフトを使用する場合、ツールの配布、実行、データ回収をお客さまにて実施頂けること

・調査におけるネットワーク負荷に同意いただけること
- 調査対象1台に対し発生する通信量は最大約3MBです
- 許容される帯域に応じて同時実行端末数を制御します

*1 揮発性情報：キャッシュやメモリ上にある消えやすいデータ

お問い合わせ先
NTTコミュニケーションズ株式会社
ホームページ　www.ntt.com/business/services/security/security-management/wideangle.html

2016.12