2016 年 6 月 15 日
株式会社セキュアソフト

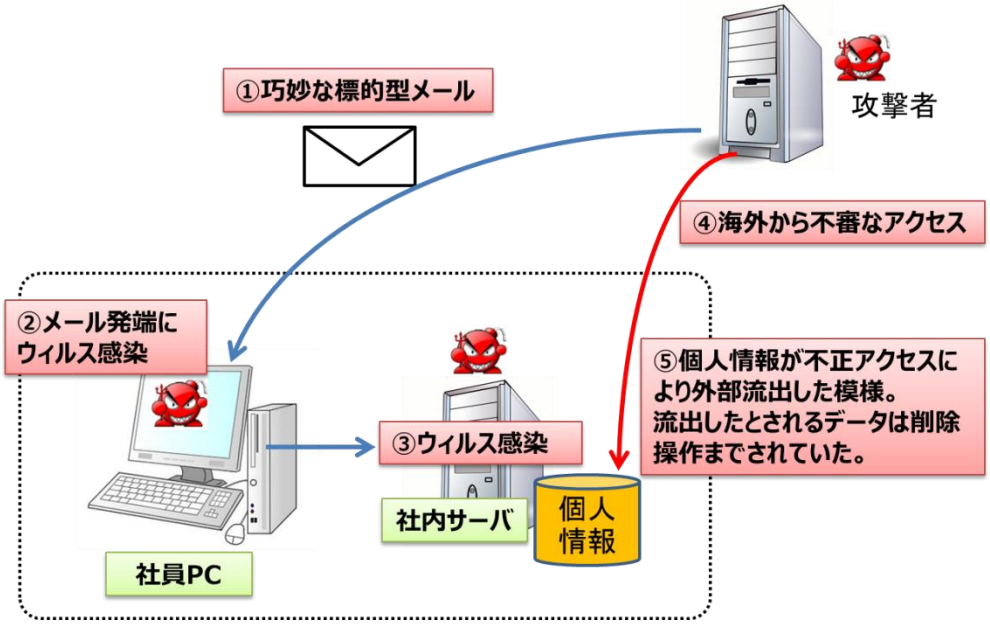
大手旅行会社の情報漏えい事件にみる標的型攻撃への分離ソリューションの必要性

2016 年 6 月 14 日、大手旅行会社のインターネット販売を主とする子会社において約 793 万人分の大量の個人情報が流出した恐れがあるとの発表があり、各種報道機関でも取り上げられております。報道機関の情報などから、2015 年上半期、国内における情報セキュリティ関連インシデントとして注目された日本年金機構における基礎年金番号などの個人情報漏えい事件と同様の手口です。今回も巧妙な標的型メールが発端となった事案ですが、アンチウィルスソフトなどでは検出できない未知脅威への対策が必要です。セキュアソフトでは、このようなセキュリティ事故を防止するために、2016 年 3 月より「SecureSoft コンテナ」を発売しております。SecureSoft コンテナのソリューションによって、個人情報をはじめとする重要情報と社外とのメールやインターネット通信を分離することで、万が一ウイルスに感染しても重要情報を守ることができる事をご紹介いたします。
なお、弊社は当事件に一切関与しておりません。

1.事件の概要（報道機関の情報から弊社推定）

各報道機関からの情報より、以下図の段階を踏んで、情報が漏えいしたと推定されます。

① 社員に取引先の航空会社を装ったメールが届く
② 添付ファイルを開いてパソコンがウイルスに感染
③ 他のパソコンやサーバに 2 次感染
④ 外部からの攻撃者による海外から不審なアクセス
⑤ 個人情報データが流出した可能性、データは社内サーバから削除



2.今回の事件を防止する当社のセキュリティ対策ソリューションについて

2015 年に発生した年金機構での情報漏えい事件以降、未知脅威対策ソリューションが注目されていますが、完全な防止対策となっていないことが指摘されています。そこで、セキュアソフトは、1 台のパソコンの中で重要情報と外部からのアクセスを分離する次世代 VDI ソリューション 「SecureSoft コンテナ」をリリースし、エンドポイントでの情報漏えい対策に力を入れています。そして、現在多くの企業、団体様よりお問い合わせを頂いております。

3.SecureSoft コンテナについて

「SeureSoft コンテナ」は独自開発したコンテナ技術を利用し、パソコン上で重要業務データの利用環境とインターネット利用環境を 100%分離する情報漏えい対策ソリューションです。利用環境を 100%分離することで、APT 攻撃やウイルス感染などのあらゆる攻撃からお客様の重要なデータが漏えいすることを完全に防ぐことができます。

【製品販売の背景】

昨年明るみに出た日本年金機構をはじめとする個人情報流出事件は、業務用 PC がインターネットに接続したことにより標的型攻撃を受けてウイルス感染し、同 PC 内に基幹システムから摘出して保存していた大量の個人情報が外部に送信されたものです。この問題を解決するためにはインターネットアクセス専用 PC と業務用 PC に分ける方法がありますが、効率性が悪くコストもかかります。また、別の対策として VDI などの画面転送方式が検討されていますが、導入コストが高く再検討を余儀なくされています。セキュアソフトでは、このようなお客様のニーズにお応えするために安価で簡単に構築できる独自技術の 100%分離ソリューションであるセキュリティコンテナシリーズを開発・販売することとなりました。

【コンテナ技術とは】

1 台の Windows PC 上に保護されたコンテナ環境を生成し、メモリ、ファイル、ネットワークの各リソースをローカル環境と完全分離する技術です。コンテナ環境で作成したデータは PC 内に暗号化して安全に保存されます。このコンテナ技術により、業務を物理的に 2 台の PC に分ける必要がなくなります。また、Windows 上でさらに別の仮想システムを動作させる仕組みと違い、すでにインストールされている Windows OS を使用し、アプリケーションもコンテナ環境で動作させるため追加ライセンスを購入する必要はありません。

図. Securesoft i-コンテナ上でウイルスに感染しても通常業務環境のデータにアクセスできない

このコンテナ技術により、たとえば SecureSoft i-コンテナ上でインターネットから標的型メールで添付ファイルにあるウイルスが不正な動きをしても通常業務環境のデータが分離されているために個人情報などの重要データアクセスを防止することが可能です。SecureSoft コンテナについての詳しい内容は、下記 URL をご参照ください。
https://www.securesoft.co.jp/products/#container

【対策例①】

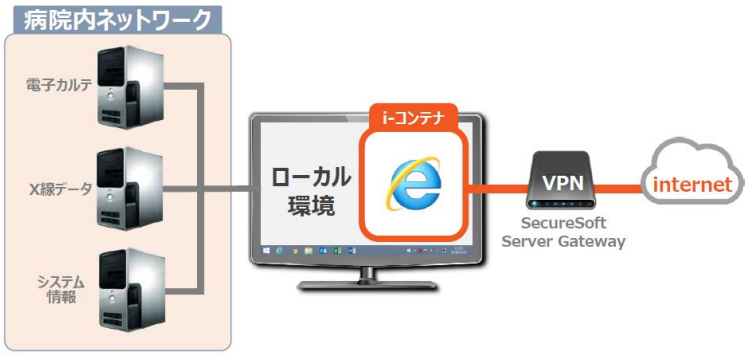
SecureSoft i-コンテナでインターネットアクセス環境の隔離を行い、万が一のウイルス感染も通常環境の重要データにはアクセスできないことで標的型攻撃による情報漏えいを防ぐことができます。

（課題例）

病院では診察の際に電子カルテが開かれているが、診察する先生は薬や医療に関する情報をインターネットで検索する必要がある。病院のルール上、電子カルテを開いている端末では個人情報漏えい対策によりインターネットアクセスを禁じている。インターネットアクセスの必要がある場合は、別の場所に置いてあるインターネットアクセス専用端末で操作する必要があり、業務効率が悪い。

（解決手段）

クライアント PC にインターネットアクセス専用ソフト SecureSoft i-コンテナを導入し、通常業務環境と 100%分離する。
そのことにより、万が一、インターネット経由でウイルスに感染した場合でもそのウイルスはコンテナ環境内に閉じ込められ、電子カルテ等の通常業務環境に影響を及ぼさない。



【対策例②】

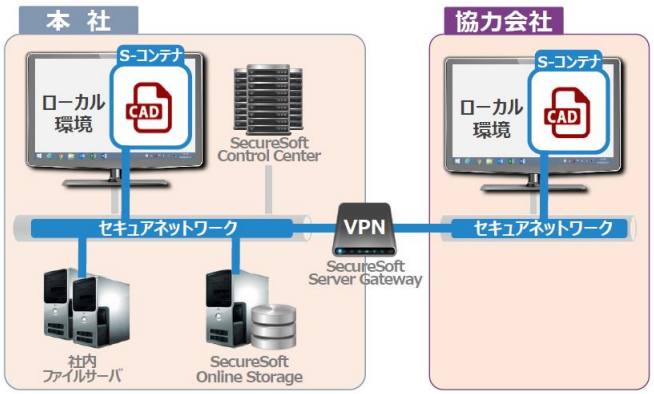
SecureSoft S-コンテナで顧客情報を扱う業務とインターネットやメールのやりとりを行う業務の論理分離を行うことで、標的型攻撃による情報漏えいを防ぐことができます。

（課題例）

本社と国内外の協力会社などと個人情報、機密情報を含む重要データのやり取りを行っており、その重要データの情報漏えいを防止したい。

（解決手段）

全クライアント PC に SecureSoft S-コンテナを導入、本社と国内外の協力会社との間は VPN 通信を利用し、重要データ用の隔離された環境を構築。また、すべてのクライアント PC は SecureSoft Control Center（管理サーバ）により USB などの外部メディア等の制御、ファイルの持ち込み/持ち出しが管理でき、人的要因を含めた情報漏えいを防止。



以上