



コンテンツレベルで情報漏洩を防止する セキュアコンピューティングのソリューション

ネットワーク経由の情報漏洩再び

昨今、官公庁や企業から機密情報の漏洩事件が相次ぎ、テレビや新聞をにぎわせている。これらの情報漏洩事件に共通しているのは、ネットワーク経由で感染したウイルスによってパソコンに保管されていた情報がインターネットに流れたというものである。

数年前、メールやFTP経由の情報漏洩の危機が盛んに叫ばれ、一部の官公庁や企業ではメール内容をチェックする仕組みを導入、或いはメールの使用を厳格化する規定を定めたところが見られた。しかし、その後に相次いだ紙媒体やリムーバブルメディアによる情報漏洩事件によって、対策の主眼はこれらのいわゆるオフライン媒体に移り、昨年4月に施行された個人情報保護法対策でも、このようなオフライン媒体に主眼を置いたソリューションが主流であった。

その意味で、最近起こった一連の情報漏洩は「古くて新しい事件」とも言うことができる。

意外に重要な ゲートウェイ・セキュリティ

一連の情報漏洩事件の直接の引き金を引いたのがウイルスであったことを

考えると、ウイルスに感染したパソコンを持ち込ませない、アンチ・ウイルスをインストールしてパターンファイルを常に最新のものに保つ、などの対策は非常に重要である。しかし、万が一、感染して情報が漏洩しつつあるときにそれを最後の一线で留めるゲートウェイにも注目する必要がある。

セキュアコンピューティングの UTM (統合脅威管理) ・ TM (脅威管理) ソリューション

セキュアコンピューティングが開発・販売しているUTM (統合脅威管

理)「Sidewinder G2」とTM (脅威管理)「Cyber Guard TSP」は、いずれも、10年以上前の開発当初からアプリケーション・プロキシ方式を採用し、その後のネットワークの高速化の流れの中で、ボトルネックとならないように製品の改良を重ねてきた。

これらの製品を通過しようとするTCP/UDPのトラフィックは、全てデータのレベルまでチェックされ、正常と判断されたものだけが中継される。したがって、HTTPのポートを悪用した情報漏洩に対しては、その内容が不適切であるということでトラフィックを遮断することが可能である。また、

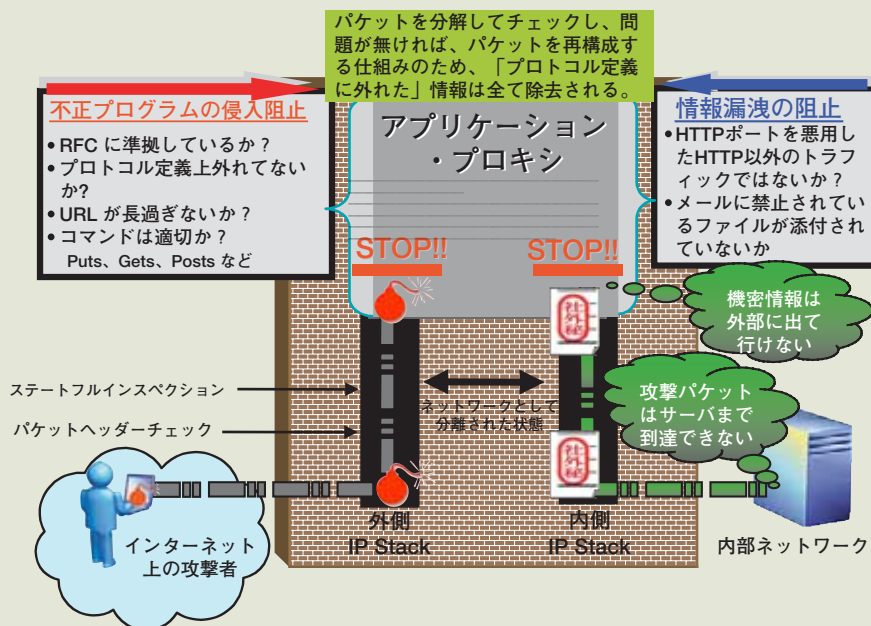


図1 アプリケーション・ゲートウェイの仕組み

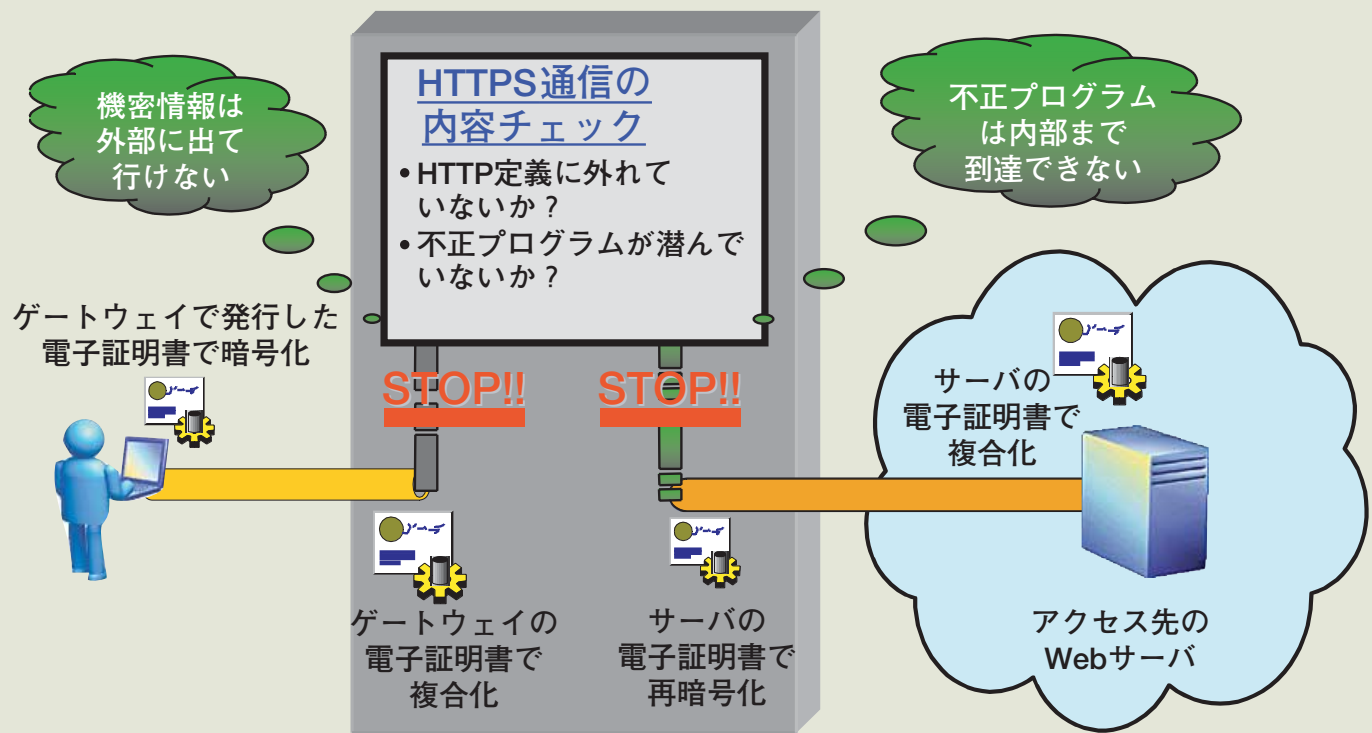


図2 HTTPS内容チェックの仕組み

メールの添付ファイルの拡張子や本文の内容などについても詳しくチェックすることができるので、メールを悪用した情報漏洩も防ぐことができる。

それを悪用した不正プログラムの侵入や機密情報の漏洩などが起こり得るのである。

トに接続を許可する。そして、クライアントには自ら発行した電子証明書を使って認証させるので、HTTPS接続が確立した後もその内容を常に把握することができる。

WebWasherは、他にもアンチ・ウイルスやアンチ・スパム、そして、Webフィルタリング機能も備え、一台であらゆる種類のコンテンツを詳しくチェックして情報の漏洩を防ぐ。

見逃されがちなHTTPSの脅威

HTTPSはWebのトラフィックを手軽に暗号化できるプロトコルとして、インターネット上での買い物や決済、そして、パスワードをはじめとした会員情報の入力などに必要不可欠なものになっている。しかしながら、この手軽さと暗号化機能は諸刃の剣である。つまり、暗号化されているため、通信の内容はチェックすることができず、

HTTPSトラフィックに本格対応したWebWasher

セキュアコンピューティングが開発・販売している「WebWasher」は、世界で始めてゲートウェイレベルのHTTPS内容チェックを実現した製品だ。

WebWasherは、プロキシとしてクライアントからのHTTPS接続要求に対して、クライアントの代わりにサーバに対する接続要求を行う。そして、サーバ側の証明書が正しいものであることを確認した後に初めてクライアン

お問い合わせ先

セキュアコンピューティング
ジャパン(株)

TEL : 03-5114-8224

E-mail : japan_info@securecomputing.com

URL : <http://www.securecomputing.co.jp/>