clearswift
RUAG Cyber Security

マルウェア対策

Clearswift SECURE Gatewayは、マルウェアが組織内に侵入増殖するリスクを除く幾重もの手段を提供します。

マルウェアはまず、SophosおよびKasperskyのアンチウイルスで検出されます。
独立の調査機関によるアンチウイルス（AV）試験「Webおよび電子メール脅威を含むマルウェアのゼロデイ攻撃に対する防御」において、SophosとKasperskyの両社は、ゼロデイ攻撃に対して完璧なスコアを収めています。

アンチウイルス	1月	2月	業界平均
SOPHOS	100%	100%	99%
KASPERSKY lab	100%	100%	99%

両社ともに違いは無いように見えますが、両社のアンチウイルスを一緒にデプロイすることで、著しく大きな効果が得られます。2017年3月に実施したクリアスウィフト社内での試験では、どちらのアンチウイルスも同時に72%のトラフィックを検出しましたが、一方のアンチウイルスが見逃したものを他方が検出した場合がいくつかありました。

こうした結果は、ほとんどのアンチウイルス ベンダーが採用している数々の機能によってもたらされたものです。

- シグネチャ – 最新のアンチウイルス定義に定期的に更新されます。
- クラウド検索 – 新たに発見されたマルウェアと一致するかどうかをリアルタイムにチェックします。
- ヒューリスティック – アンチウイルスエンジンが既知の悪質なファイルとの類似点を検査します。
- 振る舞い分析 – ファイルをエミュレーター内で短時間実行し、アプリケーションが何をするかを分析します。これが「サンドボックス」の動作原理ですが、アプリケーションはより長時間（ファイルのスキャンのために最長15分）実行されます。

Clearswift SECURE Gateway製品は、悪質なオブジェクトを検出するため、さらに多くの機能を搭載しています。

高度なファイル検査技術で拡張子偽装に対応

高精度なコンテンツフィルタリング技術を持つClearswift SECURE Gateway製品は、ファイル名に惑わされることなく、200種以上のファイル形式をそのファイルの構造から突き止めることができます。たとえば、「危険なウイルス.exe」というファイルが「安全なファイル.txt」というファイル名に拡張子偽装されていたような場合でも、Clearswift SECURE Gateway製品が実行ファイルをブロックするように設定されていれば、このファイルもブロックされます。

アクティブコードの検出

Clearswift SECURE Gateway製品はHTML、PDF、Office、OpenOffice形式のファイルについて、システムへの攻撃に使用されるアクティブコード（アクティブコンテンツ）への参照がないかどうかを調べることができます。アクティブコードへの参照があると判断されたファイルは、通常ブロックされます。

構造サニタイゼーション

アクティブコード検出機能の拡張として、意図したユーザーや受信者にファイルを「サニタイズ（無害化）」してクリーンなデータのコピーを届ける機能です。この機能はHTML、PDF、Office、OpenOffice形式に対して実行でき、SECURE Email Gatewayでは元のメッセージを保存することも可能です。

結合データの検出

ディープコンテンツ分析検査エンジンを使ってファイル形式を検証します。たとえば、画像ファイルにテキストファイルが結合されていたとしても、Clearswift SECURE Gateway製品では検出可能であり、あらかじめ設定しておけば、こうしたファイルの送信をブロックできます。

メッセージ サニタイゼーション

マルウェアが社内に侵入する可能性を排除するために、SECURE Email Gatewayでは次のようなアクションの実行を設定できます。

- 添付ファイルの削除
- URLの削除
- メール本文中のアクティブスクリプトの削除
- HTML形式のメールを単純なテキスト形式に変換して配信

感染発生フィルター

SECURE Email Gateway は感染発生検出機能も備えており、アンチウイルス防御が補強されています。マルウェアに感染しているメールを検出します。

クリアスウィフト株式会社

clearswift
RUAG Cyber Security

〒163-1030
東京都新宿区西新宿3-7-1　新宿パークタワーN30階
tel. 03-5326-3470（代表）
fax: 03-5326-3001
Email: sales.jp@clearswift.co.jp
Web: http://www.clearswift.co.jp/