

# 業務を止めずに 自動でセキュリティリスクを排除！ 情報資産を確実に守る 「アダプティブ リダクション」とは

## 標的型攻撃と内部不正の二大脅威に対処するには

大規模な情報漏洩事件が相次ぐなか、もはや業種や規模を問わずすべての企業には、情報資産を守るための適切な対策が求められるようになってきている。

そして情報漏洩を引き起こすきっかけとして特に警戒しなければならないのが、標的型攻撃と内部の人員による不正だ。

これらの脅威の拡大を受けて、多層防御によるセキュリティ強化に取り組む企業も増えている。その際のポイントとなるのが、特定のセキュリティ機能に頼り過ぎないことだ。ある特定の攻撃手法に大きな効果を発揮する機能であっても、わずか半年後には期待するほどの効果を上げられなくなる可能性も高い。なぜならば、情報セキュリティ上の脅威の変化の速度と大きさは、一般的な IT 施策の常識をはるかに超えたレベルにあるからである。

そのため情報漏洩対策のためのソリューション選定時のポイントは、特定のセキュリティ機能を備えるかどうかではなく、「情

報資産を守る」というポリシーに立脚した機能を備えたソリューションであることとなる。その代表的なものの 1 つが、クリアスウィフトが提供する入口／出口対策の製品群だ。同社は、企業が最も力を入れて守るべきメール、Web のポイントにおいて情報資産を守るソリューションを提供。そこで活用されているのが、「アダプティブ リダクション」と呼ばれる一連の “機能群” だ。

## ポリシーに応じて異なる保護アクションを実施

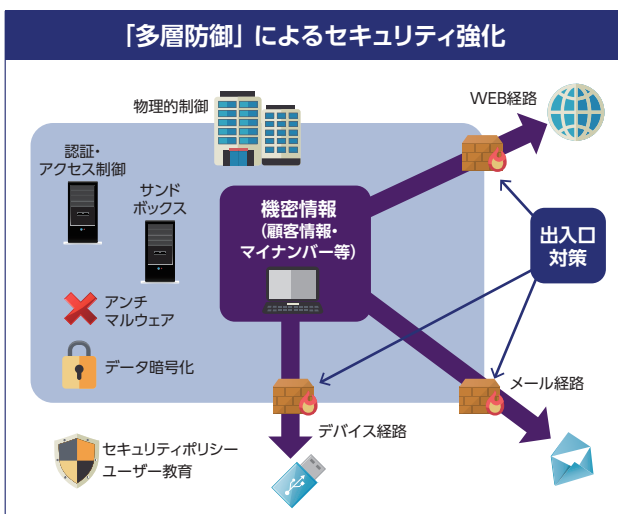
「ポリシーに違反する情報を除去し、残りの部分の宛先への通過を妨げない」というのがアダプティブ リダクションの基本的な概念だ。「アダプティブ (適応型)」とは、ポリシーに応じて異なるアクションが実施されることを指しており、アダプティブ リダクションには「構造サニタイゼーション」、「データ リダクション」、「ドキュメント サニタイゼーション」の 3 つの機能がある。

## 標的型攻撃対策にも有効な無害化機能 「構造サニタイゼーション」



構造サニタイゼーションは、受信した文書からマクロなどのアクティブコンテンツを自動的に検知、除去して無害化する機能である。これにより潜在的に有害なアクティブコンテンツを従業員がうっかり開いてしまう前に、埋め込まれた文書からアクティブコンテンツだけを削除することが可能となる。標的型攻撃では、取引先などを偽った巧妙な文面と合わせて、マルウェアが添付されたメールを送りつけることが多いが、構造サニタイゼーションは、こうしたマルウェアを検知、除去することで、標的型攻撃を初期の段階で防御するのである。

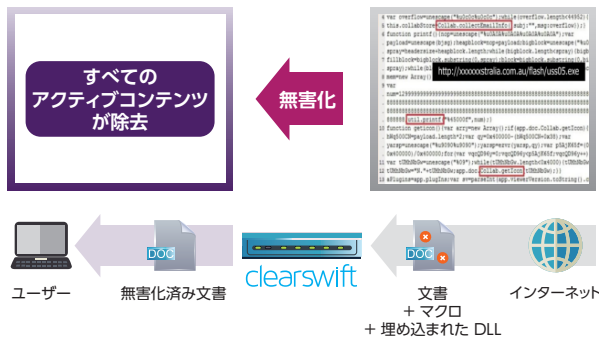
地方自治体のマイナンバー対応にも、構造サニタイゼーションは大きな効果を発揮すると期待されている。総務省が推奨する「自治体情報システム強靱性向上モデル」では、標的型攻撃対策などの観点から、マイナンバーによる情報連携に活用される



企業の情報資産を守るためには、特定のセキュリティ機能のみによらない多層防御が必要となる

## 構造サニタイゼーションによるファイル無害化

- 外部から送られるファイル(メールの添付ファイルやWEBダウンロード)に含まれるプログラムコードを無条件に削除する
- 標的型攻撃を初期の段階で防御する



構造サニタイゼーションの概念図。受け取った文書からマクロなどのアクティブコンテンツを自動的に検知、除去して無害化を行う

LGWAN 系の業務用ネットワーク / システムと、メールや Web などのインターネット系を分割することが求められている。具体的には、両者の通信経路を分けると同時に、両システム間で通信する場合には、ウイルス等の感染のない無害化通信を図らねばならない。この無害化を構造サニタイゼーションで実施することで、現場の自治体職員の利便性を一切損なうことなく、自動的かつ確実な対策が実現できることになる。

## 機密情報を秘匿する「データ リダクション」

データ リダクションは、電子メールと添付ファイル中の表示コンテンツから、ポリシーに違反している情報を除去する機能だ。これにより、内部の不正だけでなくうっかりミスによる情報漏洩も防ぐことが可能となる。除去の対象となる情報は、クレジットカード番号や顧客情報、電話番号、さらには特定の文字列など、事前にノンプログラミングで任意に設定することができる。

データ リダクションであれば、メールの本文や添付されている Microsoft Office 文書などからマイナンバーだけを見つけ出して意味のない情報へと置き換えてしまうため、利便性を保ちながら、漏洩や悪用を未然に防ぐことが可能となる。クリアスウィフトでは、米国の社会保障番号制度をはじめ、各国の共通番号制度への対応ノウハウを蓄積してきており、それらが機能に反映されているのも強みの 1 つとなっている。

## 見落としがちなメタデータでの情報漏洩を防ぐ「ドキュメント サニタイゼーション」

ドキュメント サニタイゼーションは、Microsoft Office や PDF などの一般的な文書に含まれるメタデータや更新履歴などの「隠れた」情報を、ポリシーに従って自動で除去することで、望まぬ情報の公開、漏洩を防止する機能である。例えば Office 文書の「プロパティ」には、作成者情報や更新履歴などが含まれており、正しく使う分には便利な機能ではあるものの、十分なりテラシーを持たないユーザーが誤った使い方をすれば機密情報の漏洩にもつながりかねない。

そこでドキュメント サニタイゼーションでは、Web やメールを介して社内と外部を行き来する文書に対して、あらかじめ設定したポリシーに合致したメタデータや隠れた情報のみを自動的に除去する。これにより、使いたいメタ情報は残したまま、機密情報の漏洩を未然に防ぐことが可能となる。

## 高い情報資産保護技術が評価され、世界3,000社700万ユーザーが利用

アダプティブ リダクションをはじめとしたクリアスウィフトの高い情報資産保護の技術力は世界中の企業や組織で高く評価されており、特に豊富な採用実績を誇るのが、軍事機関や政府機関、金融機関といった極めてミッションクリティカルな組織である。

国内でも、クリアスウィフトのソリューションは金融業界を筆頭に広く導入されている。そのうちの 1 つ、ある大手金融会社では、グループ全体の共通メール基盤として運用を開始した後、大幅に利用範囲を拡大。現在は約 20,000 ユーザーが利用中だ。同社では、外部宛てメールの添付ファイルの自動暗号化や、センシティブ情報や個人情報の検知と保留などを実施するとともに、グループ各社単位、役職単位、送信 / 受信者属性などの組み合わせに応じたきめ細かなアクションを適用。これにより、ビジネス上のコミュニケーションや利便性を下げずに顧客情報を確実に守り、金融業界に求められる高いコンプライアンスも実現しているのである。

### ●製品に関するお問い合わせ●

## クリアスウィフト株式会社

〒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: <https://www.clearswift.co.jp/>

©2016 Clearswift Ltd. 製品仕様、デザインは予告なく変更することがあります。