clearswift

ARgonソリューションガイド

ARgon ～　適応型DLP戦略の基盤となるもの

ガイ バンカー博士

目次

はじめに

クリアスウィフトは、これまで20年に渡りディープコンテンツ分析検査技術をリードし続けてきました。10年前には、電子メールのためのDLP (情報漏洩防止)ソリューションを投入した最初の企業の一つとなっています。現在は情報リスクを低減するユニークな「アダプティブ リダクション」技術をお客様に提供し、数多くの賞を受賞しています。そして、ARgonのビジョンが生まれました。アダプティブ リダクションは、どの組織においても、適応型情報漏洩防止戦略の基盤として使えるようになったのです。

クリアスウィフトにとっての課題は、最小の運用コストと間接コストで最大の防御効果を上げるという、アダプティブ リダクションの利点を、いかにしてClearswift SECURE Gateway製品を導入されていないお客様にもお届けできるかという点にありました。この課題をクリアし、最初に市場に投入された製品がARgon for Emailです。ARgonファミリーは、今後さらに拡充される予定です。

ビジネス上のリスクとニーズ

DLPソリューションの必要性が認識されたのは、それほど遠い昔のことではありません。その初期段階においては、不注意による個人情報流出を防止するのが主な導入理由でした。これは会社の信用問題にも発展しかねない問題です。時が移り、情報の盗み取り、特にクレジットカード番号などの財務的な情報を地下マーケットで換金することを目的とした、悪意ある攻撃が仕掛けられる時代となりました。

業務プロセスの改善や社員教育と一体となった技術的ソリューションが強く求められるようになり、時を同じくして法令が改定され、ソリューションの導入に弾みがつきました。歴史的に見ると、これまでのDLPは、組織に託された情報を的確に防御し、ビジネスリスクを抑えるためのものでした。今日においても、その根本は変わっていません。しかし、脅威の様相は進化し続けており、単にビジネスリスクを抑えるだけでなく、生産性の低下とそれによる経済的悪影響をも同時に防止するための技術革新をも求められるようになってきています。

コラボレーションとクラウド

ここ数年の間に、クラウドコラボレーションと私有IT機器の業務利用(BYOD)が普及したことにより、DLPソリューションに対する要求事項に変化が起きています。ビジネスプロセスに変化が起こりつつあることを理解することは、たとえそれがIT部門にとって好ましくないものであれ、どのような形でソリューションを導入できるかを知る上で大切なことです。どのようなセキュリティソリューションであれ、最も強固だと思われる部分が、同時に最も脆弱な部分となります。頻繁に異なった処理を行うように覚えていなければならないものは、特にそうなる傾向にあります。問題は、個人は日常業務を遂行するためにフレキシブルであらねばならず、また、頻繁に起こる変更に対応しなければならないという点にあります。例えば、ノートパソコンを考えてみましょう。ノートパソコンをわざと紛失するような人は（新しい機種を支給してもらうための悪巧みを除いて）いませんが、たとえ紛失したとしても、新聞の一面に載るような事態にはなりませんでした。IT部門にとってこれは、代わりのパソコンを手配して、必要なソフトウェアとデータをインストールするという、単なる不快な出来事の一つに過ぎませんでした。しかし、この状況は2000年を境に大きく変わりました。紛失が起こり得るノートパソコンでは、そこに保存された重要情報を暗号化して保護することが法令で義務付けられたためです。もし暗号化したことを証明できなければ、罰金が課せられてしまいます。こうして、企業のノートパソコンに求められる「標準セキュリティ機能」のリストには、暗号化が追加されました。ノートパソコンを紛失してしまったとしても、それに伴うリスクは小さくなりました。情報に対する防御が、その情報が保存された機器の物理的な防御機能として導入されたわけです。

狙われているのは財務情報だけではない

独ボーダフォン[1]や韓国市民[2]、そして米ターゲットグループ[3]のケースとは異なり、2014年のソニー・ピクチャーズ[4]や米コミュニティ・ヘルス・システムズ[5]に対するサイバー攻撃では、サイバー犯罪者はいまやクレジットカードや銀行口座情報だけでなく、ありとあらゆる換金可能な情報を狙っていることが浮き彫りにされました。

映画「ザ・インタビュー」を公開中止に至らしめたソニー・ピクチャーズからのデータ流出をめぐる報道をみますと、より長期的な損害を与えたのが、後に企業とその経営陣の信用を失墜させるのに利用された特定情報へのターゲティングだったことが分かります。一方では、例えば掃除機メーカーのダイソンのロイヤルティカードのような一見無害そうな情報でありながら、しかしフィッシング攻撃に利用できるような知的財産が攻撃の目標となっています。

また、オーストラリア連邦警察[6]やベルギー国鉄[7]の事例のように、文書に含まれた明らかにセキュリティ違反に該当する情報ではなく、「隠れた」情報が見逃されたために起きた違反事例もあります。コラボレーションを行う必要のある範囲がますます広がってきたことが、共有して良いものといけないものを認識しきれていない従業員のミスを増やしています。さらに、一見無害に見えますが実は有害なアクティブコンテンツを埋め込んだ文書が、APT攻撃やランサムウェアの主要な送付手段になっています。外部組織とのコラボレーションニーズの高まりがここでも影響を及ぼし、無害そうに見える文書がもたらす脅威について認識の浅い受信者が、感染率を引き上げているのです。

既存DLPの弱点

DLPソリューションの導入には、試行錯誤がつきものです。理論的には、「何かリスクを減らしてくれるものを導入する」というたいへんシンプルなものです。しかし、これまでのDLPソリューションでは、減るのはリスクだけではなく、同時にコラボレーションも犠牲にすることになります。これは、誤検出が起こることで、本来通過させられるべき情報が「止めてブロック」され、隔離エリアで足止めされるためです。そもそも、情報の発信者が送信前に削除すべきものを削除しておけば、誤検出は避けられるのです。しかし、社員の大多数にとって、これを覚えておくことは容易なことではありません。情報セキュリティが本来の業務ではない社員にとって、これは最重要事項ではないのです。

コミュニケーションのブロックは、業務をスローダウンさせるだけでなく、フラストレーションも生み出します。送信者は送りたい情報が送信されないというフラストレーションを、受信者は受取るべき情報を受け取れないというフラストレーションを感じます。さらに、IT部門（やコンプライアンス部門）は、送信した電子メールは無害なものだから早くリリースせよ、と訴える社員の電話に忙殺され、やはりフラストレーションを溜め込みます。DLPソリューションがもたらすこのようなリスクは、メリットよりも大きくなってしまうことが少なくありません。その結果、そのソリューションはスイッチが切られるか、意味のある防御効果を発揮できないまでに動作を制限されてしまいます。

ブロックされたコミュニケーションのほとんどは、ある特定の情報さえ削除されていれば問題なく通過させて良いものであり、フラストレーションを引き起こさずに済んだはずです。クリアスウィフトは、既存DLPの問題点と誤検出の悪影響を、独自技術の「アダプティブ リダクション」によって解決しました。

[1] http://www.ft.com/cms/s/0/d0f7608c-1bae-11e3-94a3-00144feab7de.html#axzz3QbJ9GCBo
[2] http://www.securityweek.com/20-million-people-fall-victim-south-korea-data-leak
[3] http://www.reuters.com/article/2013/12/19/us-target-breach-idUSBRE9BH1GX20131219
[4] http://www.bbc.co.uk/news/technology-30692105
[5] http://www.reuters.com/article/2014/08/18/us-community-health-cybersecurity-idUSKBN0GI16N20140818
[6] http://www.theguardian.com/world/2014/aug/28/federal-police-mistakenly-publish-metadata-from-criminal-investigations
[7] http://www.flanderstoday.eu/business/nmbs-data-leak-was-breach-privacy

アダプティブ リダクション

アダプティブ リダクションは、「ポリシーに違反する情報だけを除去し、残りの部分の送信先への通過を妨げない」という、概念上とてもシンプルなものです。実際に、このソリューションはとても洗練されています。なぜならば、コンテンツを理解するだけでは十分でなく、そのコンテンツが使われている前後の文脈をも理解する必要があるためです。

コンテンツ

コンテンツという観点から見ると、アダプティブ リダクションを機能させるための独自のディープコンテンツ分析検査（DCI)技術を利用しているという点で、クリアスウィフトは他のDLPソリューションベンダーと一線を画しています。これは、電子メールとそれに添付された圧縮ファイルや文書ファイルをばらばらに分解するだけでなく、ポリシーに違反する情報を割愛して再び組み立てる能力があることを意味します。この能力を持つアダプティブ リダクションには3つの主要な機能があり、そのすべてがARgonソリューションに搭載されています。

- **データリダクション（秘匿化）**
- **ドキュメント サニタイゼーション**
- **構造サニタイゼーション**

データリダクション（秘匿化）

データリダクションを分かりやすく説明するために、一つの例を取ってみましょう。ある企業にお客様から注文メールが届き、そこにはクレジットカード番号が含まれていました。（皆さんのようなセキュリティのプロにとってこれは馬鹿げた話に聞こえるかもしれませんが、実はこんなことはしょっちゅう起きているのです。）企業のカスタマーサポート担当者は、注文確認のために「返信」ボタンをクリックしますが、このメールはブロックされます。なぜなら、そこにはクレジットカード番号が含まれているからです。ARgonでは、データリダクション機能がクレジットカード番号部分を秘匿化し、その「修正」されたメールが送信されます（図1）。

メッセージの内容が変更されると、送信者／受信者双方に通知が届けられます。また、セキュリティ事案として報告が上げられ、必要な場合はIT部門がアクションを取れるようにします。セキュリティ事案の95%は、このように個人が起こした無自覚なミスであり、特に調査を行う必要はありません。

ARgonでは、通知メール中に示されたURLをクリックすることで、元のメッセージをすみやかにリリースさせることができます。メッセージのリリースは、権限保持者や送信者の上司、あるいは他の人物や部門に限るよう設定することが可能です。

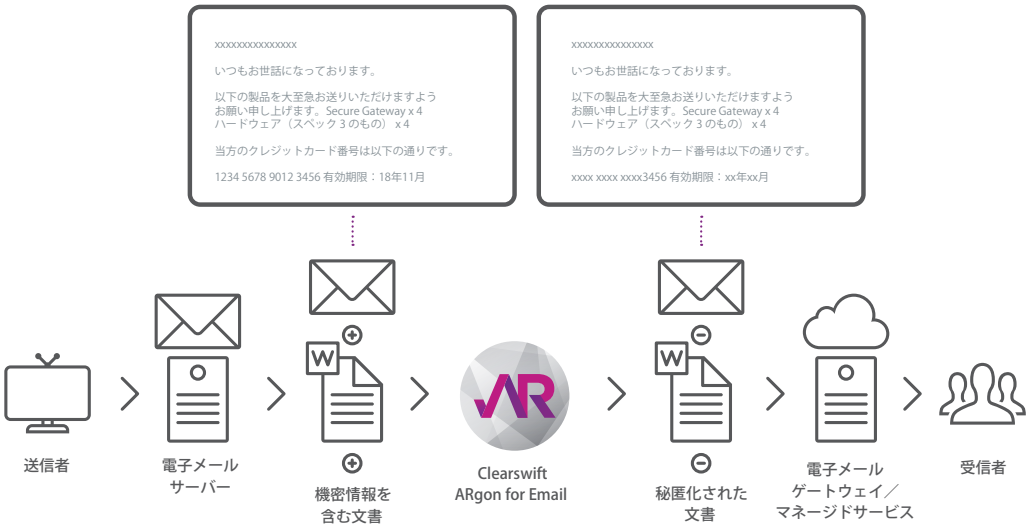

図 1：データリダクション（秘匿化）

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では、ドキュメントプロパティや変更履歴についてのポリシーを簡単に設定できます。多くの場合、ポリシーはシンプルなもので、組織外に送信される文書の全てに対して適用され、ユーザー名などの機密情報を含むドキュメントプロパティや変更履歴は除去されます。（図2）

クリアスウィフトのディープコンテンツ分析検査における、過去20年あまりに渡る経験により、ドキュメントプロパティなどの除去では、きめ細かな処理レベル設定が可能です。例えば、ドキュメントプロパティにプロテクトマークやクラスが付加されたものを残し、その他を除去するといった処理です。変更履歴と合わせて、高速保存によって残された情報も一緒に除去することが可能です。この機能によって、実際に送信されるものと、送信者が送っているつもりのものが一致します。

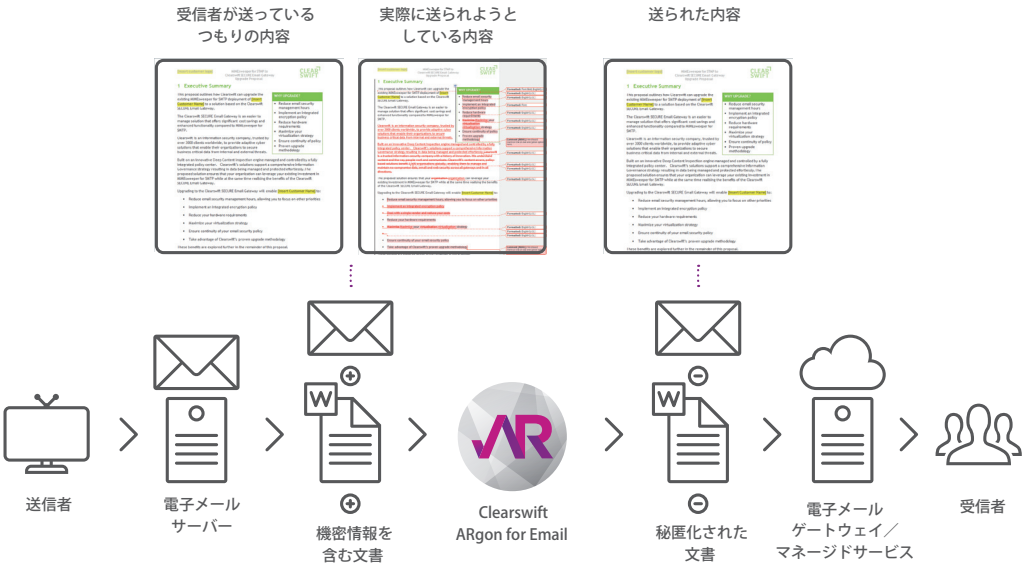

図 2：ドキュメント サニタイゼーション

構造サニタイゼーション

今日のAPT攻撃の最大のソースは、埋め込まれたアクティブコンテンツです。この攻撃は特定の個人や組織を標的としているため、既存のアンチウイルスソリューションでは普通は止めることができません。しかし、どれほどAPT攻撃の検出が難しかろうとも、単純にすべてのアクティブコンテツを除去してしまうことが、多くの組織にとってこの最も陰湿な攻撃に対する唯一の防御法となります。（図3）もし間違ったものを除去すれば、それは誤検出となりますが、その場合は権限保持者や送信者の上司、あるいはその他の個人や部門によってすみやかにリリースする機能が提供されています。

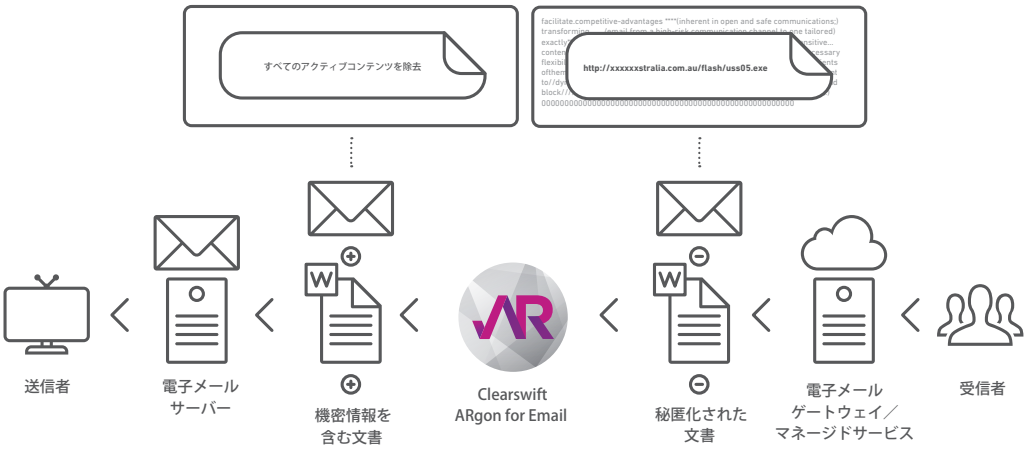

図 3：構造サニタイゼーション

コンテキスト

コンテキスト（背景、状況）は、さまざまな要素によって決定しなければなりませんが、情報の送信者と受信者、そして情報の通信方法が鍵となります。この場合、「誰」については、ディレクトリサービス（Microsoft Active Directoryやその他のLDAP準拠ソリューション）を利用して組織構造を調べることで特定できます。例えば、CEOは財務部門の社員よりもより大きな自由度を与えられるようポリシーを定義することができます。

さらに、アダプティブ リダクション機能においては、その名が示す通りに「適応（adaptive）」します。コンテンツとコンテキストを複合的に判断することで、異なる処理を実行させられるのです。したがって、ある文書を送信したのがたとえ企業の最高経営責任者であったとしても、受信者や通信手段に応じて異なった防御手段を取ることができます。例えば、電子メールなら暗号化し、Webサイトへのアップロードなら秘匿化を行い、USBスティックへのコピーならブロックする、といったことが可能です。

双方向性

これまでのDLPは、重要情報の組織外への流出を防ぐために考案されたものです。しかし、情報サプライチェーンの拡大により、より柔軟性が求められるようになりました。インバウンド（外部からの受信）だけでなくアウトバウンド（外部への発信）に対する防御も必要になってきたのです。しかも、埋め込まれたアクティブコンテンツを除去し、マルウェアを取り除くだけでなく、場合によってはデータリダクション（秘匿化）の実行も必要とされます。

例えば、PCI DSS (Payment Card Industry Data Security Standard)に準拠していないネットワークを持つ企業の場合、外部の決済会社がクレジットカード情報が載っている文書ファイルが添付された電子メールをこの企業に送信すると問題となります。（これは例外的な状況において起こるものですが、実際には毎月数回の割合で起きています。）受信側ネットワークが規格に準拠していないため、監査官庁の介入を防ぐためにはネットワークから情報を除去するプロセスが必要です。データリダクション（秘匿化）が導入されていれば、問題の情報は不適合ネットワークに到達する前に除去されますが、問題のない部分には手が付けられないため、コミュニケーションは成立します。

同様に、アクティブコンテンツの除去は、外部へ送信されるアウトバウンド通信に対しても実行可能です。例えば、投資ブローカーが配信するスプレッドシートに含まれたマクロという形の知的財産を守る場合などです。

ARgon ソリューション

アダプティブ リダクションは、速やかに情報リスクの低減効果が現れることから、クリアスウィフトのお客様の間では瞬く間にスタンダードとなりました。当社のパートナーや、購入を検討されているお客様からお話を伺った結果、このユニークな機能は、他の電子メールやWebソリューションと組み合わせて利用できるようにもするべきであることが明らかになりました。ARgon製品ファミリーは、この目的のために作られたものです。

ARgon for EmailはARgonファミリーとして投入される最初の製品です。今後もより多くのコミュニケーションチャネルと組み合わせるための製品がリリースされる予定です。

ARgon for Emailは、既存のあらゆる電子メールゲートウェイに対して直接方式、またはサイドカー（横付け）方式でのデプロイメントが可能です。既に投資を行った資産をムダにせず、アダプティブ リダクション機能を追加してリスクを低減することができるのです（図4）。

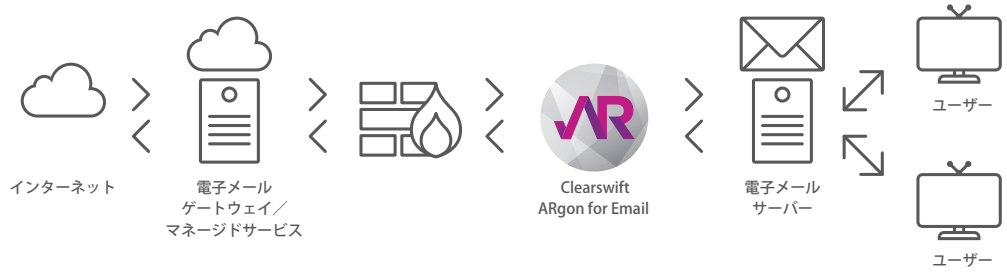

図 4：ARgon for Emailのデプロイメント

迅速なデプロイメントとリスクの即時低減を実現するために、ARgonにはさまざまなデフォルトポリシーやポリシーアクション、そして各種レポートが用意されています。もちろん、必要に応じてカスタマイズを行うことも可能です。

ARgon for Emailに含まれるデフォルトポリシーには次のようなものがあります。

- 組織外に送信される電子メール／添付ファイルに含まれるすべてのクレジットカード番号を秘匿化する
- 組織外に送信される電子メール／添付ファイルから、すべてのメタデータ、変更履歴、および高速保存データを除去する
- 組織外から受信する電子メール／添付ファイルから、すべてのアクティブコンテンツを除去する

デフォルトの設定では、すべてのポリシー違反はIT部門に通知が送られます。所属長への通知の設定や、SIEM（セキュリティ情報およびイベント管理）ソリューションとの統合も簡単に行えます。

その他のポリシー、例えば国民保険番号や社会保障番号などの標準トークンを秘匿化するポリシーなどは、容易に有効化することができます。

ARgon for Emailのビジネスケースを構築する

今日ITに投資する際には、購入を正当化するためのビジネスケースを構築する必要があります。これは、特にセキュリティソリューションを購入する場合には、困難な作業になるかもしれません。

つまるところ、セキュリティソリューションの多くは、ハッカーが内部システムにアクセスして損害を引き起こした場合に備える保険です。情報漏洩防止ソリューションは、セキュリティ侵害が起きて規制当局や立法機関から処罰されないよう、組織を守る目的で作られたものです。FUD（恐怖、不安、疑念）戦術に基づいたソリューションは、今日の企業が必要とするものではありません。多国籍グローバル企業であるか地元企業であるかにかかわらず、今日の企業には業務遂行と規制順守の両面において、業務プロセスに柔軟に対応でき、変化するニーズに適応できるソリューションが必要です。セキュリティソリューションは、攻撃が起きた時に役立つだけでなく、「日常的に価値」を提供してくれるものでなくてはなりません。さらに最も重要なのは、個人や組織の生産性を阻害してはならないということです。

ビジネス上のリスクは、起きる可能性と起きた場合の結果の重大さで判断することができます。ARgonのためにビジネスケースを構築する場合も、同じことを検討する必要があります。実際には、次のような点を含めた結果の重大性評価から始めると判断しやすいでしょう。　（しかし、これが検討すべき項目すべてということではありません。）

- 金融行動監視機構(FCA)やHIPAAなどの規制対象事業者ですか？
- 製品の設計仕様など、競合他社から守らなければならない知的財産をお持ちですか？
- 新規契約や製品購買の入札情報など、間違った人物の手に渡った場合に損害が発生する可能性のある営業情報をお持ちですか？
- PCI準拠事業者であり、外部からネットワークに受信するクレジットカード情報が貴社のCIO、CISO、あるいはコンプライアンス部門や監査部門にとって頭痛のタネとなっていますか？
- 国家最重要基盤を支えるデータを扱っていますか？
- 顧客や従業員の個人情報を保管していますか？

次の段階では、起きる可能性を検討します。これについては、現実にセキュリティ侵害が起こりうる確率はほぼ100%と考えるべきでしょう。セキュリティ侵害は、もはや「もし」ではなく、「いつ」起こるかの問題なのです。そこで、次のような特定の事案が起こる可能性を考えた方が良いでしょう。

- 過去にデータ侵害がありましたか？それはいつのことですか？
- 機密情報を含む電子メールが間違った宛先に誤送信されたことがありますか？
- 機密情報が記載された電子メールを誤送信されたことがありますか？
- 文書に埋め込まれたアクティブコンテンツが原因で、ネットワーク内部でマルウェア感染が発生したことがありましたか？
- 文書中に残った変更履歴が、それを見るべきではない人物に見られてしまって困ったことはありませんか？（こうした事例は、営業部門で起こりがちです。過去に作成した提案書を元に修正した提案書を新規顧客に送付した際、古い情報がまだ文書中に残っていて、それを新規顧客に見られてしまったというケースです。）
- 組織内で働いている従業員がいますか？

上記の質問の一つ以上に「はい」と回答された場合は、その項目でのデータ侵害に伴う費用を算出した方が良いでしょう。費用は年ごとに異なります。こういった数字は、不安を煽って購入を正当化するために利用されることもありますが、ビジネスケースを定量化する上でたいへん役立ちます。

データ侵害に至る可能性のある事案を検討したら、そのうち悪意ではなく不注意によるものがどれくらいの割合かを考慮するのも大切です。最近の調査によると、データ侵害の大部分が、実は外部からではなく内部から起きているということです。[8]これは、外部からのデータ侵害が減少しているという意味ではなく、内部脅威に対する備えが企業により一層求められていることを意味しています。

検討すべきパズルの最後のピースは、既存のセキュリティ資産に目を向けることです。ARgonは、「Rip and replace(完全な置き換え)」を前提として作られた製品ではありません。既存のソリューションを補強し、新しい世代の脅威に対処するためのものです。リプレース方式の製品に比較して、コスト効果と業務効率が高く、いつでも追加できる方式なのです。

[8] http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis

クリアスウィフトとARgonの未来

クリアスウィフトは、長年に渡ってディープコンテンツ分析検査のリーディングカンパニーであり、適応型（アダプティブ）DLPソリューションを電子メール、Web、エンドポイント向けに販売しています。ARgon for Emailは、アダプティブ リダクション機能を適用するARgonファミリー製品としてクリアスウィフトが最初に市場導入する電子メール向け製品です。電子メールが現在のところ主要な通信手段であるため最初に選ばれましたが、しかし、時代は変わりつつあり、アダプティブ リダクション機能に対するニーズもこれ以外のチャネルに拡大しています。

クリアスウィフトの全製品は、中核となる同じ技術の上に構築されており、異なる通信チャネルで同一のポリシーが適用できます。ARgonにおいても、これは同じです。情報を脅かす新たなリスクに対処するため、さらに多くのARgonファミリー製品が今後導入される予定です。ARgon for Emailと同様に、これらの製品も既存のセキュリティソリューションや電子メールソリューションを補完するために作られています。その結果、連携させて使用できるARgonソリューションのセットが生まれます。（図5）

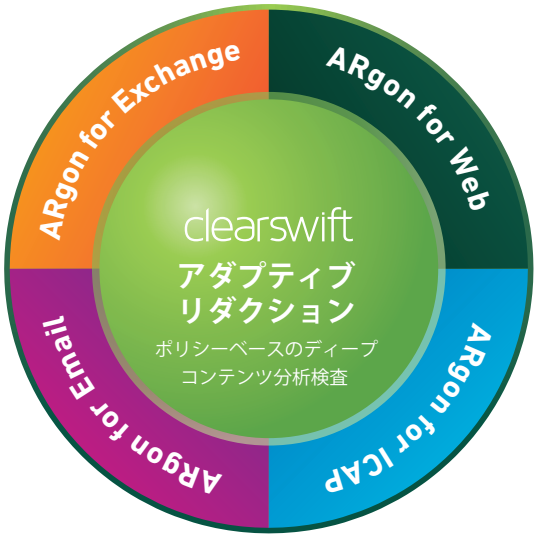

図 5：ARgon製品ファミリー

ARgon for Webは、ARgon for Emailと同様の機能をWeb環境において提供します。この製品は、HTTPおよびHTTPSトラフィックの両方と連動して使用可能です。ICAPベースのWebプロキシをお持ちのお客様にアダプティブリダクション機能を提供するのは、ARgon for ICAPです。ARgon for Exchangeは、内部脅威への対処として、内部電子メールにアダプティブ リダクション機能を付加するための製品です。

まとめ

かつて古代ギリシャの哲学者であるヘラクレイトスはこう言いました。『この世で唯一変わらないものは、変化するという事実だ。』今日のビジネスも同じであり、常に変化し続けています。セキュリティに関して言えば、やはりあらゆる変化が起きています。新しい脅威と新しい法規制が、重要情報の防御に関して新たな義務を生み出しました。

クリアスウィフトが提供するARgon製品ファミリーは、組織が直面する新しい脅威に、悪意によるものと不注意によるもののどちらにも対処しています。既に購入済みの既存のセキュリティソリューションと連動して機能するよう作られたソリューションは、これまでのDLPソリューションが対処できなかった問題の多くを解決できます。アダプティブ リダクション機能を搭載したARgonはポリシー違反の情報のみを除去し、残りの部分は手付かずのまま通過させますので、誤検出を減らし、生産性を高めます。

また、受信する文書に埋め込まれたアクティブコンテンツを除去し、今日外部からもたらされる最も大きな脅威であるAPT攻撃から組織を防御します。

クリアスウィフトは、電子メールやWebゲートウェイにどのようなセキュリティ製品を既に購入していたとしても、アダプティブ リダクション機能をすべての組織で活用いただけることを目指しておりましたが、ARgon製品の投入によってその願いが実現しました。

クリアスウィフトについて

クリアスウィフトは組織のビジネスクリティカルな情報を保護し、セキュアなコラボレーションの実現とビジネスの成長を推進する、世界から信頼を受けている情報セキュリティ企業です。

クリアスウィフトの革新的技術は、アダプティブ（適応型）DLP（情報漏洩防止）への迅速な移行をサポートし、ビジネスの阻害要因となるリスクを除去し、組織の機密データの常時100%の可視化を実現いたします。

クリアスウィフト株式会社

clearswift

〒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/