clearswift
RUAG Cyber Security

GDPR（一般データ保護規則）コンプライアンスの推進：情報の可視化、保護、ガバナンス

EU一般データ保護規則 (GDPR) は、EU市民のデジタル権利を強化し、企業の所在地やデータ処理の場所に関わらずEU域内の保護規則を簡素化することにより、個人データのプライバシーのレベルを引き上げます。組織の規模に関わらず、個人データを新しい基準で管理することが求められています。個人情報の保存場所や共有時期を明確にした上で、規制の意味を理解し、所定のセキュリティ対策を実施しなければなりません。

業務の中断によりコストを発生させずにGDPRコンプライアンスを効果的に実施することが重要です。そのためにはリアルタイム でのこれらの実施が求められています。

データの可視化	適応型（Adaptive）セキュリティ
インテリジェントなポリシー適用	ガバナンス

データの可視化

目に見えないものを守ることはできません。

クリアスウィフトの製品は、組織内でやり取りされ、また潜んでいる個人データを見つけ出すと同時に、それらの情報が電子メールやWeb、ソーシャルメディア、クラウドアプリなどを通して組織外に流出しないように監視できます。リムーバブルストレージや、企業Webサイトでの文書公開といった見落とされがちなプロセスについても、注意を怠らないようにしなければなりません。獲得したデータの可視化は、初期段階においてはプライバシー監査の難易度評価の一環として、その後の段階においては、データ保護影響評価の一環として活用できます。さらに、「忘れられる権利」を要求された際には、エンドポイントやファイルサーバー上にある非構造化ファイル内の情報の発見にも利用できます。その後の削除は自動でも手動でも実行可能です。

インテリジェントなポリシー適用

すべてのデータ、アクセス権限、共有権限を平等に扱うことはできません。ポリシーは、すべてのチャネルで一貫していなければなりません。しかもGDPRの適用地域、データタイプ（国家安全保障、児童保護、医療など）、処理目的、要求されるセキュリティ措置に応じて、インテリジェントに適用する必要があります。

クリアスウィフトのインテリジェントなポリシー適用では、インバウンドとアウトバウンド双方のポリシーの選択にコンテンツだけではなくコンテキストも利用されます。コンテキストとは送信者および受信者（またはターゲットのアップロードサイト）であり、また、通信メカニズム（電子メール、Web、エンドポイントなど）も含まれます。単一の共有ポリシーにより一貫性が確保され、同時に展開や利用が容易になります。たとえば、文書ファイルを会社に電子メールで送付する際に取るべきアクションとして、通信の暗号化が利用できます。しかし、同じ文書ファイルをクラウドサイトにアップロードする場合には、取るべきアクションは秘匿を要する機密情報の自動除去、さらに、ユーザーが同じ文書をUSBドライブにコピーしようとした際には、システムにブロックさせることができます。

クリアスウィフト製品にはGDPRの対象となる情報を発見保護するためのポリシー構築に役立つシンプルなインターフェースが用意されています。さらに、処理をより容易に実行するため、次のようなテンプレートもあらかじめ用意されています。

PII（個人識別情報）とPCI（クレジットカード業界）用の事前定義正規表現

- 国民保険、ID番号
- IPアドレス
- クレジットカード番号
- 社会保障番号
- 国際銀行口座番号 (IBAN)

編集可能なコンプライアンス辞書

- 個人識別情報 (PII)
- 医療保険の携行性と責任に関する法律 (HIPAA)
- グラム・リーチ・ブライリー法 (GLBA)
- 証券取引委員会 (SEC)
- SOX法 (サーベンス・オクスリー法)

ソーシャルネットワークとクラウドコラボレーションサイト用のコンテキスト ポリシールール

- インバウンド防御
- コンプライアンス違反防御 (インバウンド)
- データ漏洩防御 (アウトバウンド)
- 適応型 (Adaptive) セキュリティ

適応型 (Adaptive) セキュリティ

クリアスウィフトのGDPRソリューションは、企業内から外部のクラウドに至るまであらゆる領域を保護するために作られています。社員のうっかりミス、悪意ある社員や悪質な外部からの攻撃による個人データの流出や漏洩を防ぐには、情報が保存されているストレージと出口ポイント (図1参照) の防御が不可欠です。適応型 (Adaptive) セキュリティでは、GDPRポリシーに基づいた自動秘匿化、暗号化、ブロック、移動、削除をリアルタイムに行います。

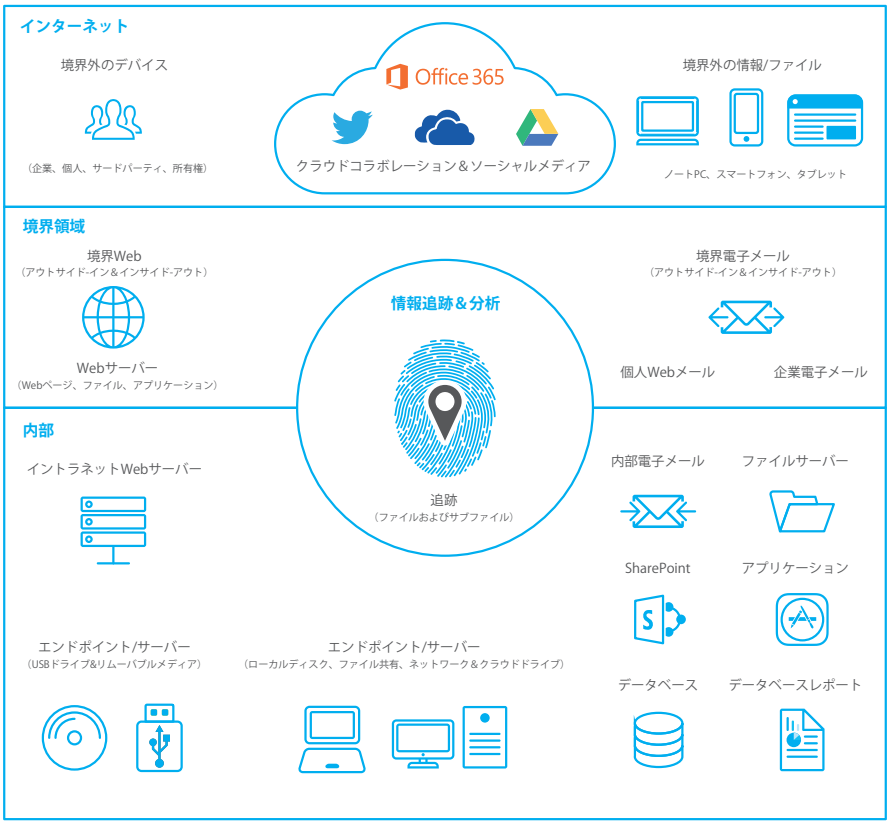

図 1:クリアスウィフトのソリューションは企業のあらゆる領域を保護します。

クリアスウィフト独自の「アダプティブ リダクション」技術によって、多くの組織でGDPR順守が実現できます。特定の個人データだけを削除して共有を防ぎます。その間他のデジタルアクティビティは継続して使用可能で、業務を阻害することも、誤検出を出すこともありません。完全な保護が、エンドユーザーに気付かれずに実施され、組織とビジネスパートナー、そして顧客を守ります。

ガバナンス

データ保護官(DPO)、コンプライアンス部長、ITセキュリティ担当者は、レポート、ポリシー違反、隔離データ、ログに関して完全な可視性を必要としています。クリアスウィフトのGDPRガバナンス追跡機能は、ポリシーや適応型 (Adaptive) セキュリティをリアルタイムに適用するだけでなく、報告に必要な紛失個人データ、ソース、リスクを特定するための違反・侵害分析も可能にします。

さらに、ファイルとその下位レベル (情報) のきめ細かな追跡により、サードパーティに渡った情報をも監視し、GDPR順守に役立てることができます。情報来歴レポートは、どの情報がどのサードパーティに渡ったのかを特定するのに役立ちます。したがって、GDPRで制定されることになっている「忘れられる権利」に基づいた要求が起こされても、適切な外部組織にコンタクトすることが可能です。

GDPRコンプライアンスのためのクリアスウィフトのソリューション

クリアスウィフトは、重要情報保護のための事業を展開してきました。あらゆる規模の組織が、電子メールで送信される情報、インターネット上を流れる情報、エンドポイント上の情報などを保護する上で、クリアスウィフトの比類のない水準のセキュリティに依存しています。その鍵となっているのが、ソリューションの中心に据えられたディープコンテンツ分析検査エンジンです。電子メールやインターネット上のトラフィック、文書は、分析のために構成要素に分解され、それぞれの要素に対してコミュニケーションの内容とコンテキストに応じたポリシーが適用されます。ポリシーの選択プロセスにコンテキストを含めることはたいへん重要です。コミュニケーションを取ろうとしているのは誰か、どこに送ろうとしているのか、どのように送られるのかといった点を理解することで、コンプライアンス上どのようなアクションを取るべきかが決定されます。

クリアスウィフトのより深部に至るまでの分析とサニタイゼーションは他の追随を許さないものであり、分析対象の圧縮化/暗号化、ファイルサイズ、分析タイミングの遅延、仮想環境回避技術や文書の複合埋め込みレイヤーによって制限されることはありません。その結果は最高の検出率と低負担（誤検出のほぼゼロ化など）として現れており、GDPRコンプライアンスに準拠するために費用対効果の高いアプローチです。

ピアリング

GDPRソリューションの展開に際しては、すべてを一度に行うのではなく、リスク優先度や部門/リソースの利用可能度に応じたデプロイメントができるよう、数段階に分かけた計画が立てられます。企業電子メールで流れる情報の初期調査は、すべての出口ポイントにおける同様の情報を見つけ出すために、Web/クラウド上の分析とサニタイゼーションを追加して拡張することも可能です。ピアリングを行うことで、すべてのチャンネルでポリシーが共有され、あらゆる変更がすべてのコミュニケーションフローに対して遅滞なく一貫して適用されます。異なるソリューションが追加されて新しいオプションが利用可能になっても、1台のコンソールで集中管理できます。

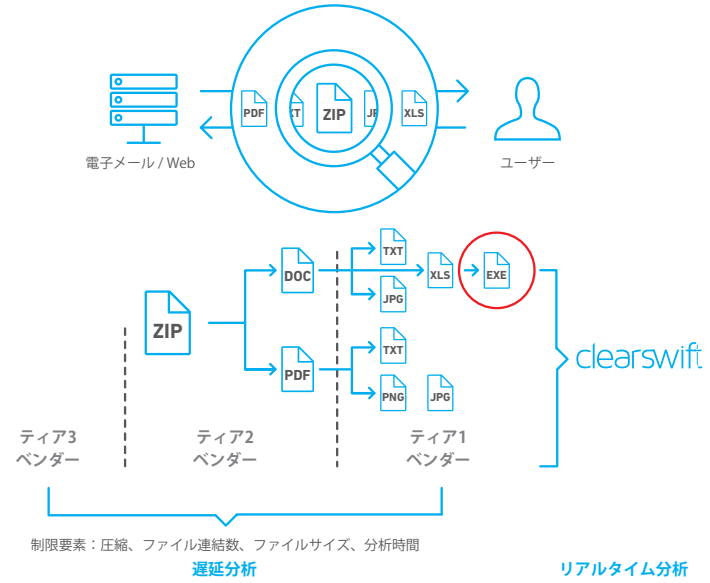

図 2：最もきめ細かなレベルのディープ分析：ファイル/サブファイル、カプセル化データ/非表示データ/メタデータ

フレキシブルな導入オプション

クリアスウィフトのGDPRソリューションは、現行のClearswift Gateway製品（およびエンドポイント用製品Clearswift Critical Information Protection）上でアクティベートできます。

あるいは、既に投資済みの既存のITセキュリティツール（シスコ、シマンテック、マイクロソフト、ソフォス、F5、ブルーコート等）を拡張するプラグインとして、より深部のレイヤーの分析検査、GDPR用インテリジェントポリシー、適用型(Adaptive)セキュリティを追加することもできます。

特徴	メリット
	可視性
保存データの検索	ノートPC、サーバー、ネットワーク/クラウドドライブ上の機密情報を検索し、リスクを軽減します。
移動中データの監視と管理	電子メール/Webトラフィック上の重要情報の監視と管理を行います。アダプティブ リダクション、暗号化、ブロックといった制御が可能です。
利用中データの監視と管理	エンドポイント上のリムーバブルメディアの監視と管理を行います。リムーバブルメディア（USBドライブ、CD/DVD ROM等）への複製の暗号化または複製防止が可能です。
双方向性ポリシー	インバウンド、アウトバウンド双方においてコンプライアンス侵害を防御します。
	適応型（Adaptive）セキュリティ
標的型攻撃に対する防御（インバウンド）	情報を媒介とする脅威が問題を起こす前に無力化します。
データ漏洩防御（アウトバウンド）	あらゆるコミュニケーションチャネル（電子メール、Web、エンドポイント等）において不注意や意図的なデータ漏洩を防御します。
アダプティブ リダクション	事前定義のキーワード/トークンに基づき、よく使用されるアプリケーションからテキストを自動除去します。望ましくない、または秘匿を要するファイル履歴情報を削除します。（カスタムプロパティや「予期せぬ」（または不正な）プロパティを含む。）アクティブコンテンツを検出し、すべての痕跡を完全に除去します。
適応型の暗号化	コンテキストに基づく複数の暗号化により、セキュアな情報コミュニケーションを実現します。
	インテリジェントなポリシー適用
柔軟できめ細かなポリシー管理	複数のコミュニケーションチャネルにわたるポリシーを容易に定義可能。検索に一貫性が確保され、取るべきアクションに柔軟性が与えられます。
テキスト分析と正規表現ルール	簡単な表現による単語/フレーズ検索、より複雑な正規表現を使用したパターン検索、またはブール検索/位置検索により、機密データのパターンを検出できます。カスタムトークンを作成してのより緻密な検索により誤検出を低減し、また、構造化データソースのチェックも可能です。
クラウドコラボレーションポリシー	クラウドとの間で送受信される情報を保護します。また、クラウドドライブ上の保存データのスキャンも可能です。
バイナリ形式ファイルの特定	独自のファイルシグネチャを定義可能なシグネチャベースの正確な検出により、ファイル形式のなりすましに対処します。
ファイル/サブファイル上の情報監視と統制	機密文書の登録が可能。電子メールとWebの出口ポイントにおけるファイル/サブファイルレベルでの情報監視とコントロールを行います。
	ガバナンス
事前定義のガバナンス辞書	GDPRで要求される情報（クレジットカード番号、銀行口座番号、社会保障番号、個人ID、国民保険番号を含む）を容易に検出できます。迅速な実装が可能です。
カスタマイズ可能なレポート	コンプライアンス担当責任者やIT管理者に最適な視覚的レポートを直感的なドリルダウンで容易に修正、実行、共有できます。
完全なSMTP、HTTP、HTTP/S分析検査	暗号化されたトラフィックの内容を検査し、アウトバウンド/インバウンド双方で機密データの侵害を防ぎます。
ソーシャルメディア管理（Facebook、LinkedIn、Twitter、YouTubeを含む）	Web 2.0サイトへのアクセスを、ポリシーによって許可されたコンテンツや機能に限定できます。
Active Directory (AD) / LDAP の統合	柔軟なポリシーとグループ/個人別の監査レポート作成を可能にする完全ユーザーベースのポリシー管理が可能です。
SNMP、SMTP、SYSLOG警報	SNMPまたはSMTP管理警告により、データセンターにおける「ライトアウト」でのデプロイメントを容易にします。ログファイルはSYSLOGを使用して自動的に統合されます。

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/
2017年 9月