clearswift

Clearswift SECURE Exchange Gateway

社内メール環境での適切な情報制御を提供するメールソリューション

Clearswift SECURE Exchange Gateway (SXG) は、不適切な情報や機密情報が組織内で流布され、組織外へ流出してしまうのを防ぎ、ポリシーとコンプライアンス要件徹底をサポートします。マルウェアや不適切なファイル形式を検出し、柔軟なポリシー設定によりルール定義を容易に実現し、メールのやり取りをスキャンして違反事項を特定します。

DLP (情報漏洩防止)

Clearswift SECURE Exchange Gateway (SXG)は、電子メールの機密を保持し、組織のコンプライアンスポリシーに合致したものにします。違反要素を含むメッセージは、人手による検査のために隔離されるか、違反コンテンツが「アダプティブ リダクション」機能によって自動的に除去されます。添付されたPDFやMicrosoft Officeファイルに対してキーワード検索を実施すれば、特定のキーワードやフレーズをアスタリスクなどの文字にダイナミックに置換可能です。機密に該当するフレーズは自動的に除去され、脅威となるのを未然に防止します。また、Microsoft OfficeやPDFファイル内に残っている許可されていない機密データの痕跡が組織内で共有され、最終的に組織外に流出してしまうことのないよう、ドキュメント サニタイゼーション機能がドキュメントプロパティや変更履歴を除去しますので、不注意による情報漏洩事故を防ぐことができます。

きめ細やかなポリシー設定でコンプライアンスを強化

電子メールメッセージと添付ファイルは、そのサイズやメッセージの内容、または添付ファイルの内容によってフィルターを適用できます。部門間でやり取りされるメッセージを制御するポリシーの作成も可能です。メッセージの拒否または隔離処理については、許可を与えられた管理者による手動リリースの他に、所属長に転送してリリースするか削除するかの判断を委ねることもできます。これにより、業務の効率化とIT部門の負担軽減が実現します。

ディープ コンテンツ フィルタリングとカスタマイズ可能なキーワード検索

電子メールメッセージと添付ファイルに対するディープ コンテンツ フィルタリング機能は、不適切なコンテンツや機密情報を確実に検出します。150以上のファイル形式と200言語以上の文字セット認識に対応しており、標準辞書やカスタマイズ辞書を活用してキーワード検索を行うことで、好ましくないコンテンツや秘匿を要するコンテンツを検出します。キーワード検索では、コンテンツ違反の検出にワード、フレーズ、ユーザー定義のトークンやテキストエンティティ（マイナンバー、クレジットカード番号等）、正規表現が使用可能です。

キーワード検索に加え、ファイルサイズ、ファイル形式制御、ファイル名によるブロックなどを併用できるため、業務に関係のないファイルや、あるいは単にサイズが大きすぎるためにExchangeのインフラに影響を及ぼしそうなファイルの検出や削除もできます。

包括的なマルウェアコントロール

メッセージスキャンには、Sophos か Kaspersky のいずれかのアンチウイルスエンジンから選択可能です。最高で2つまでのエンジンを使用できますので、Exchangeサーバーに余分な処理サイクルを負わせることはありません。ファイルの先頭や後尾にデータを付加して検出を避けようとする試みに対処するため、構造検証をファイル形式に適用することもできます。また、構造サニタイゼーションによってPDFやMicrosoft Office、HTMLファイルからアクティブコードを除去することも可能で、APT攻撃が企業メッセージサービス内に侵入するリスクを低減させます。

ポリシーベースのルール

社内メールやインターネットの電子メールをカバーするために、AD／LDAPを統合してルールを簡単に定義することができます。ポリシーの作成は、個人ベースでも部門ベースでも、コンテンツベースでも可能です。これは、銀行や軍事組織、研究組織、あるいは特定の輸出規制を順守する必要のある多国籍企業など、お互いに情報が分離、遮断される必要がある組織内の部門間でメールをやり取りしなければならない組織にとってはとりわけ重要な要件です。

モニターモード
モニターモードでは、メッセージの流れを阻害することなくお客様のDLPポリシーをテストすることができます。メッセージのコピーはSXGプラットフォームによって処理され、その結果によって電子メールコンテンツのどこかに問題があるか、あるいは誤検出を避けるためにDLPポリシーを調整する必要があるかを判断できます。

スキャンプラットフォーム
他社の多くのExchangeスキャン製品とは異なり、クリアスウィフトはExchangeサーバーの負担を軽減するためのオフボックスソリューションを提供しています。このプラットフォームはハードニングされたLinux上で動作し、物理ハードウェアでのデプロイメントに加え、vSphereやHyper-Vへの仮想的な展開も可能です。Exchange上では軽量なインターセプターを使用するだけなので、メッセージの配信所要時間に影響を与えません。
ExchangeTransportサーバーに展開されるSXGインターセプターは、メッセージのコピーをSXGの処理ノードに転送します。メッセージが危険と判断された場合には、そのメッセージを拒否、改変、あるいは手動での承認のために隔離できます。

導入オプション
SXGプラットフォームの導入は、現在お持ちのセキュリティ インフラに依存しません。マネージド サービス モデルをアウトソースしている場合（図1）でも、オンプレミスのレイヤード セキュリティ モデルを使用している場合（図 2）のどちらでも動作可能です。

管理とレポート作成
SXGは、耐障害性を備えた処理エンジンとのグループ化が可能で、Web UIによって管理できます。これにより、異なる権限を持つシステム管理者でも、統一されたポリシーの定義やメッセージ管理、レポート作成、システム監視などの、システムタスクを実行できます。
ExchangeのインターセプターはPowerShellで設定され、組織へのデプロイメントにおいて他のインターセプターと共有できるようにActive Directory LDSに保存されます。

図 1：検疫マネージドサービスモデル

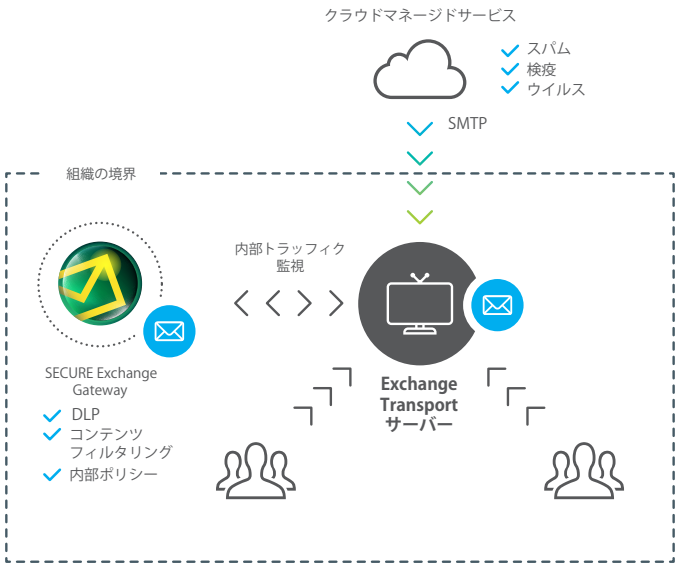
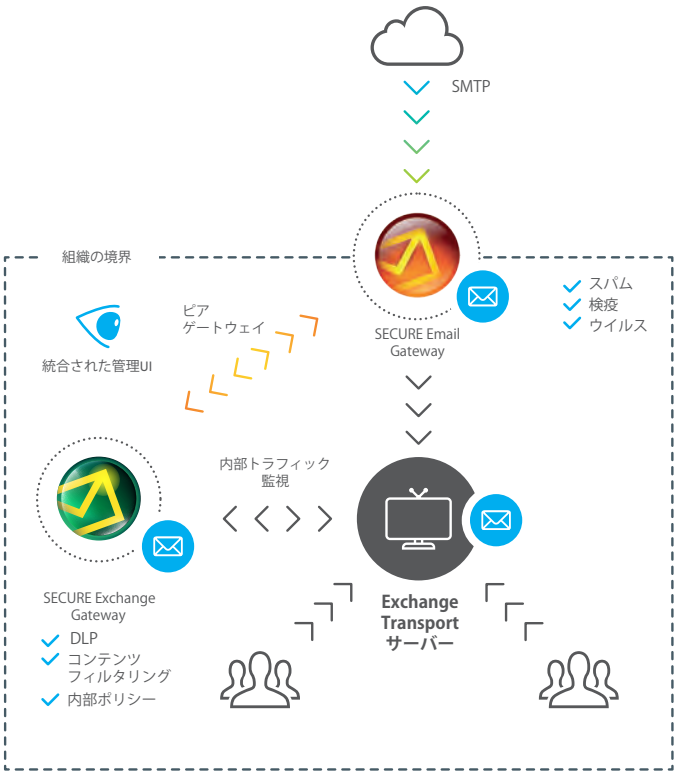


図 2：オンプレミスのレイヤードセキュリティ



クリアスウィフトの他のGateway製品、IGサーバーとの統合

SXGはSECURE Email GatewayやWeb Gatewayとピアを形成して、ポリシーやレポートデータの共有が可能です。
SXGをSECURE Email Gatewayと併用した場合、システム管理者は単一のダッシュボードからメッセージポリシーを管理できます。

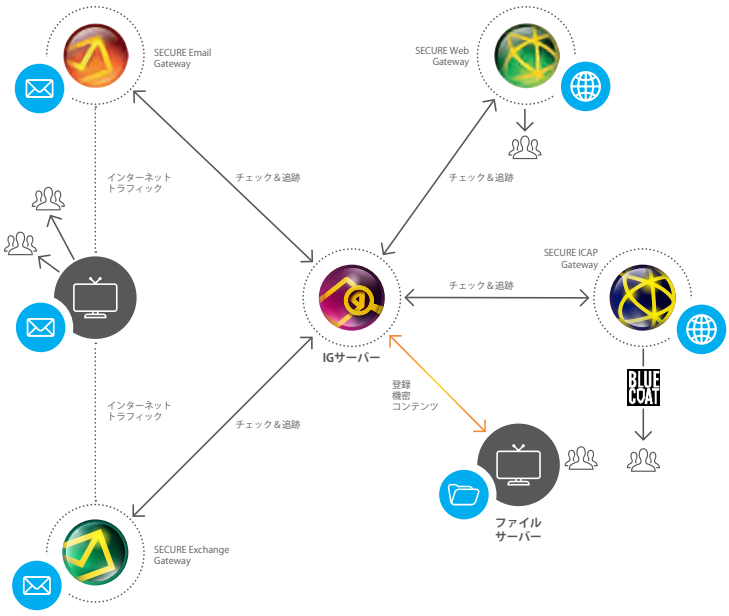
図 3：ピアゲートウェイの管理：システム管理者は境界と社内メールのメッセージポリシーを単一のダッシュボードから管理可能

情報漏洩防止は、一般的には既知のキーワードやフレーズによって管理されます。しかし、容易に分類できない機密情報の場合はどうすればよいでしょうか。たとえば、「トップシークレット」とヘッダーに記された文書から、誰かが機密セクションを新規の未分類文書に切り貼りした場合どうなるでしょう？ここで高度フィンガープリントアルゴリズムが威力を発揮し、機密文書をその一部分だけであっても検出できます。インフォメーション　ガバナンス(IG)サーバーには、組織内のユーザーが機密データを登録でき、IGサーバーには文書全体の他、段落、画像、その他の埋め込みコンテンツなどの構成要素のデジタル表現も保存できます。

IGサーバーは、SECURE Exchange Gateway（SXG）、SECURE Email Gateway、SECURE Web Gatewayといったクリアスウィフトの他製品と共同して、企業全体の情報漏洩防止を同時に提供するよう設計されています。

また、IGサーバーに接続した場合、SXGはユーザー間で配信される機密コンテンツの検出に使って、ポリシーに違反するメッセージや添付ファイルをブロックすることがでます。

さらに、IGサーバーはデータ追跡サービスを提供しています。管理者は誰が特定のファイルや文書の一部を閲覧できるかを把握できますので、必要に応じた修正アクションを取ることができます。



クリアスウィフトについて

クリアスウィフトは、ビジネスクリティカルなデータを保護して安全なコラボレーションとビジネスの成長を実現することで、世界中のお客様に信頼されている情報セキュリティ企業です。クリアスウィフト独自の技術は、直接的で「適応型」の情報漏洩防止をサポートし、業務の中断を防ぎ、クリティカルな情報に対する完全な可視性の常時確保を可能にします。
クリアスウィフトはヨーロッパ、オーストラリア、日本、アメリカに拠点を置き、900社を超えるリセラーとともに世界各地でビジネスを展開しています。
クリアスウィフトおよび製品、サービスに関する詳しい情報は以下のホームページをご覧ください。

www.clearswift.co.jp

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: http://www.clearswift.co.jp/

特長	Clearswift SECURE Exchange Gateway
プラットフォーム	
対応プラットフォーム	Exchange 2007 / 2010 / 2013 / 2016
モニターモード（電子メールの流れを阻害せずにメッセージのコピーを処理）	○
AD/LDAPとの統合	○
デプロイメント オプション	N+1 オフボックス負荷分散処理エージェント（フィルタリングはExchangeサーバーの負荷処理に影響を及ぼしません）
DBメンテナンス	自動
検疫	
アンチウイルスエンジン	KasperskyまたはSophos
ファイル検出方法	ファイルのシグネチャ / 拡張子 / チェックサム
カスタムファイル形式の認識	○
画像スキャン	○
アクティブコンテンツ検出フィルター	○
情報漏洩防止	
アダプティブ リダクション：データリダクション（秘匿化）	あり※
アダプティブ リダクション：ドキュメント サニタイゼーション	あり※
アダプティブ リダクション：構造サニタイゼーション	あり※
テキスト分析：重み付けワード、正規表現、論理演算子、辞書	○
事前定義キーワードによる検索リスト	複数：PCI、SEC、SOX、機密性、不敬語リストなど
事前定義トークン	複数：クレジットカード番号、日本マイナンバー、米社会保障番号、IBAN、英国民保険番号、豪納税申告番号、独納税者ID番号、BIC (SWIFT)コード など
カスタムトークン	○
キーワード検索言語	200以上の文字コードをサポート
システム管理	
組み込みレポート作成	○
レポートの自動配信	○
エンドユーザー メッセージリリース／ポータル	○
エンドユーザーリリースのブランド化設定	○
エンドユーザーリリースシステム用iPhoneアプリ	○
権限委譲	○
パッチの自動ダウンロード	○
仮想化対応	VMwareおよびMicrosoft Hyper-V
通知機能の送信対象	送信者 / 受信者 / 指名管理者 / 所属長
通知によるメッセージのリリース	○
メッセージリリース時点での監査担当へのコピー送信	○
アラーム通知方法	UI / 電子メール / SNMP
SYSLOGの一元化	○
ポリシーのロールバック	○
ポリシーの変更履歴	○

※アダプティブ リダクションには、3つの機能がありますが、導入に際しては少なくとも1つの機能が必要となります。
残りの2つはオプション機能として追加できます。

clearswift