clearswift
RUAG Cyber Security

Clearswift SECURE ICAP Gateway

サードパーティ製WebプロキシとICAPプロトコルで連携するWebコンテンツ検査ソリューション

Clearswift SECURE ICAP Gatewayは、高性能コンテンツ分析検査エンジンを搭載し、サードパーティ製WebプロキシとICAPプロトコルで連携するWebコンテンツ検査ソリューションです。既存のプロキシサーバー環境を活用して、高度な情報漏洩防止やフィルタリング機能など幅広い機能を提供し、お客様のWebセキュリティインフラを強化します。さらに、リバースプロキシ環境と連携することで、クラウドアプリケーションへのフィルタリング機能も提供します。

Clearswift SECURE ICAP Gateway の導入により、ディープコンテンツ分析検査、アダプティブ リダクション、情報漏洩防止技術を既存のWebセキュリティアーキテクチャに適用できます。既存のインフラに混乱を与えることがないため、情報の流れをお客様のインフォメーション ガバナンス ポリシーに適合させ、コンプライアンスの徹底を最小のリスクで推進できます。

情報漏洩防止

情報漏洩防止 (DLP) ツールの導入は、正確性の欠如やデプロイメントの複雑さ、または必要な運用コストといった問題で失敗することがよくあります。クリアスウィフトはこういった運用上の課題を、無許可の情報共有を制限する最新の双方向機能により抑え込み、同時に業務の生産性を阻害する誤検出の発生を最小限にとどめました。

既存のデータソースとの結合と柔軟な語彙分析により、Clearswift SECURE ICAP Gatewayは情報漏洩の可能性を、実際に起こる前に正確に検出します。Clearswift Information Governance Serverと統合することで、コンテンツ（フィンガープリント）の検出だけでなく、Gatewayを通過する情報のすべての断片を追跡することが可能となり、情報保護をより高いレベルに引き上げることができます。

デプロイメントは極限まで簡素化されており、ICAPの利用によって既存のインフラに統合されます。

ポリシー違反が生じた場合には、特定のワークフローを実行したり、コンプライアンスに適合するようコンテンツを修正してコラボレーションを継続したりと、柔軟なアクションを取ることが可能です。

ディープコンテンツ分析検査

クリアスウィフトの優れたディープコンテンツ分析検査エンジンが情報の流れを完全に分解して理解し、機密情報のやり取りを阻止します。Web 2.0アプリケーションに適用が可能で、ユーザーや組織内の役割や部門に応じて個別に設定することができます。

コンテキスト認識型スキャンは制限されている情報のアップロードを防止し、情報の分析結果に応じて、ユーザー（正規、非正規とも）に個別のポリシーを適用するといったきめ細かな対応を取ることが可能です。

機密情報の不正なやり取りについてはあまり認識が広まっていないため、クリアスウィフト製品ではモニターモードでの柔軟なポリシー適用や、実施前の微調整ができるようになっています。

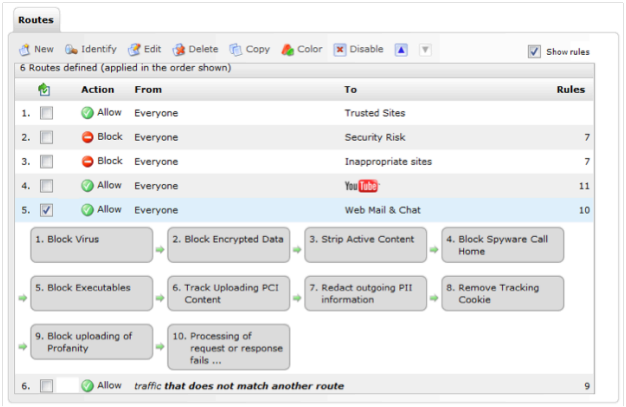
アダプティブ リダクション (Adaptive Redaction)

Clearswift SECURE ICAP Gatewayは、お客様の既存のセキュリティインフラにアダプティブ リダクション技術を追加するために開発された製品です。アダプティブ リダクションでは分析されたコンテンツにリアルタイムで修正を加えることが可能で、交換される情報がセキュリティポリシーに従ったものとなるようにします。

メタデータ、更新履歴、プロパティなどに加え、実行可能ファイルなどの隠された情報や通常チェックされない情報もシームレスに除去されるため、お客様の機密情報の安全を確実に保護します。

不明な攻撃やAPT攻撃による組織の資産へのアクセスを防止するため、埋め込み実行ファイル、スクリプト、マクロといったアクティブコンテンツは検出、除去されます。アダプティブ リダクションを情報分析ルールと連携させることにより、機密コンテンツや攻撃的なコンテンツをアップロード／ダウンロードされた時点で除去、置換することも可能です。

図1 Web管理インターフェースによる簡素化されたルール強制定義



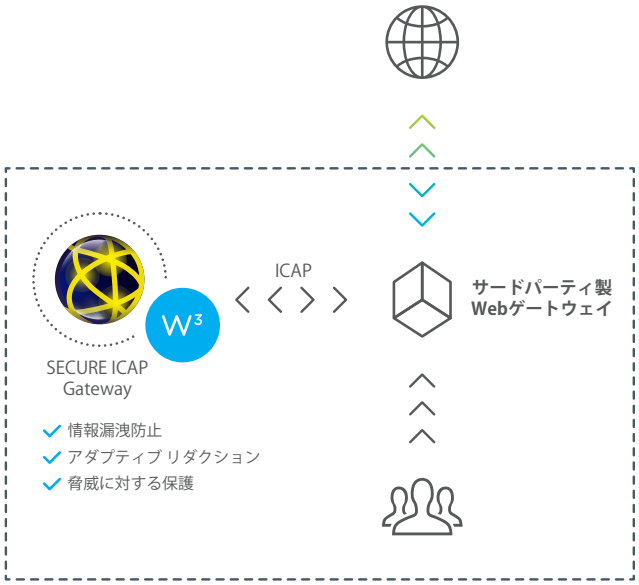
管理とコンプライアンス

管理上必要なタスクは強力で直感的に操作可能なユーザーインターフェイスによって簡素化されていますので、エラーが起こりにくく、導入後の運用コストも最小限に抑えられます。Clearswift SECURE ICAP Gatewayの柔軟で設定の容易なポリシーには、総合的レポート機能と監査機能が付いています。

Clearswift SECURE ICAP Gatewayには、現在と将来の法規制に対するコンプライアンスを確保し、情報漏洩防止対策をより容易なものとするための標準テンプレートや、規制対象の情報や秘匿を要する知的財産の漏洩につながる危険性のある単語を集めた定義済みエンティティが付属しています。

豊富なレポート機能

誰がいつ、どこのサイトにアクセスしたかの詳細なレポートが取れます。また、スケジュール設定によるレポートの自動生成や、対話型でのドリルダウンレポートも可能です。



柔軟なポリシー管理

Clearswift SECURE ICAP Gatewayでは、Facebook、LinkedIn、Twitter、YouTubeという最も人気の高い4つのソーシャルネットワークサイトに特化したポリシールートが用意されています。ユーザーや部門ごとに異なるポリシーの設定が可能で、各ルートにはWebサイトの種類によってコンテンツルールが予め設定されています。

FacebookやWebメール、またはその他の類似サイト経由でのデータ流出の心配がある場合でも、サイトへのアクセスは許可し、アウトバウンド方向のデータの流れを制御することが可能です。YouTubeには不適切なコンテンツが含まれている可能性がありますが、アクセスを許可した動画だけに制限することができます。Clearswift SECURE ICAP Gatewayのきめ細かなポリシーにより、データ漏洩や法的リスクや組織の評判に関わるリスクを低減し、規制順守を履行できます。

外部からの脅威への対応

Clearswift SECURE ICAP Gatewayでは、カスペルスキー社あるいはソフォス社製のウイルス／マルウェア／スパイウェア保護のライセンスをオプションで追加できます。

クリアスウィフトのコンテンツ分析検査とアダプティブ リダクション技術によってセキュリティはさらに強化されています。疑わしいスクリプトやその他の高リスクのコンテンツ（実行ファイルなど）のダウンロードを防止します。さらに、ファイルやWebページに含まれるアクティブコンテンツは、コミュニケーションに遅滞を招くことなくリアルタイムでサニタイズ（除去）されます。

マイナンバー対応とテキスト検索

マイナンバーを検出する機能も搭載しています。テキスト検索式の作成と設定を行う場合、日本のマイナンバーはもちろん、異なる地域のID番号（IDカード、運転免許証、パスポート）、標準日付形式などの幅広いグループオプションから選択できます。

高度なURLフィルタリング

Clearswift SECURE ICAP Gatewayには、84のカテゴリーに分類されたURLデータベースが含まれています。このデータベースは数百万のWebサイト、または数十億のWebページをカバーしています。

データベースにはセキュリティリスクのカテゴリーが含まれており、悪質なマルウェアやフィッシング詐欺を防止します。データベースは、セキュリティ保護をより一層強固にするため継続的に更新されています。

ウェブサイトのカテゴライズ設定

毎年5千万もの新しいWebサイトが現れる今日、ユーザーがまだ分類されていないWebサイトを訪れてしまう可能性は極めて高いものと考えなければなりません。Clearswift SECURE ICAP Gatewayには、悪意のある既知のURLデータベースが搭載され、営業日内に定期的に更新されています。不適切サイトへのアクセスを防止し、最新のオンライン脅威からお客様の組織を安全に保護します。

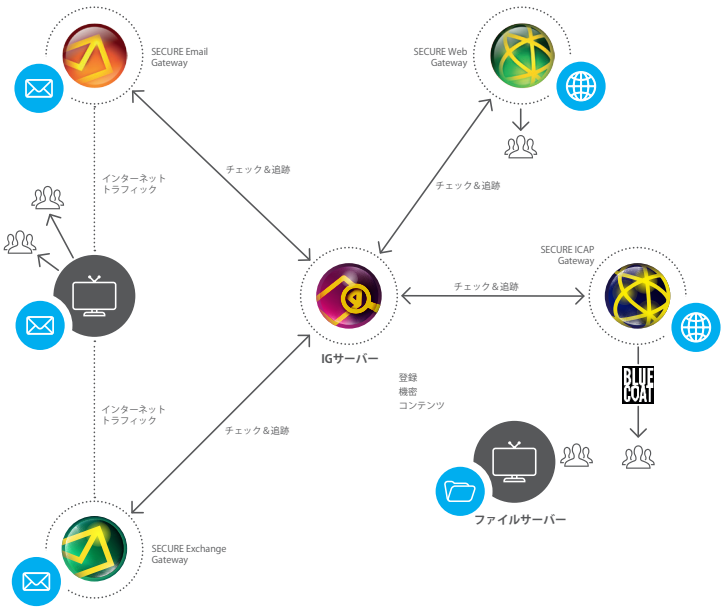
フレキシブルな導入オプション

ソフトウェアをインストール済みのハードウェア アプライアンス版、お客様選択のハードウェアプラットフォームにインストールできるソフトウェア版、仮想環境へインストールできるバーチャルソフトウェア版(仮想プラットフォーム対応)から選択できます。

IGサーバーとの統合

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、機密情報が容易に分類できない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、機密部分を新規の未分類文書に切り貼りした場合はどうなるでしょうか？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することが可能になります。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することが可能で、IGサーバーは文書全体や、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を保存します。IGサーバーに接続した場合、Clearswift SECURE ICAP Gatewayは通過する機密コンテンツの検出に使用可能となり、セキュリティポリシーに違反する場合は適切なアクションを取ることができます。

また、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、特定ファイルや文書の一部を閲覧できるのは誰かを知ることできるため、必要に応じた修正アクションを取ることができます。



特長	メリット
プラットフォーム	
ICAPサーバー	インフラ内で既存のICAPクライアントに接続します。対応ICAPクライアント: Blue Coat Proxy SG / F5 BIG-IP / Barracuda NextGen Firewall / Squid
フレキシブルな導入オプション：ハードウェア、ソフトウェアイメージ、VMware vSphere	お客様のIT戦略に適合する柔軟性を提供します。
Active Directory (AD) / LDAP の統合	柔軟なポリシーとグループ／個人別のレポート、監査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。
ポリシー	
柔軟できめ細かなポリシー管理	リスクを最小に抑えながらWeb 2.0 の利用を可能にするポリシーを容易に定義できます。
Facebook、LinkedIn、Twitter、YouTube用ポリシー	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。
ポリシーの方向性による制限	特定の種類のファイル（スプレッドシート等）のアップロードを禁止し、一方でダウンロードを許可することが可能です。
カスタマイズ可能なブロックページ	ユーザーのアクションに応じたフィードバックを提供して指導を行うことができます。
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 *	コンテンツから機密情報を検出、＊（アスタリスク）にリアルタイムに置き換えて秘匿化します。ビジネスプロセスに遅延を生じさせずに秘匿を要する情報を保護します。
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 *	文書中の隠れた情報（メタデータ、プロパティ、高速保存データ、など）を除去して漏洩を防止します。
アダプティブ リダクション：構造サニタイゼーション *	文書やHTMLページのアクティブコンテンツを検出、除去し、APT攻撃やその他の脅威から保護します。
Clearswift Information Governance Serverの統合**	ファイルの全部または一部のアップロード／ダウンロードを検出し、SECURE ICAP Gatewayを通過するあらゆる情報の追跡が可能になります。
外部データソースの接続	送信中に発見されたデータをデータベースから正確に特定します。
語彙分析および正規表現ルール	ファイルのコンテンツを、シンプルまたは複雑なパターン一致によるキーワードやフレーズで検索し、秘匿を要するデータを特定します（200以上の文字エンコードに対応）。
定義済みの機密データ用テンプレート	クレジットカード、銀行口座、社会保障番号などを容易に検出できます。
コンプライアンス辞書	GLBA、HIPAA、SEC、SOX、PCI、PII用を含む多言語対応の編集可能な辞書により、企業の評判と用語上のリスクを最小化します。
事前定義トークン	複数：クレジットカード番号、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、SWIFTコード
MIMEsweeperによる真の「バイナリ形式ファイル」の特定	バイナリベースの正確な検出を行います。独自のファイルシグネチャも定義可能です。
検疫	
双方向のウイルス／マルウェアスキャン**	既知／未知のマルウェアのネットワークへの出入りを阻止します。
双方向のスパイウェアスキャン	スパイウェア、アドウェア、キーロガー、感染したマシンからのスパイウェアによるコールホームをブロックします。
84のカテゴリーに分類されたURLフィルター用データベース	不適切なサイトへのアクセスを防止し、Webレポートに追加情報を提供します。
マルウェア、フィッシング詐欺、およびスパイウェアのカテゴリー	既知の高リスクURL／サイトへのアクセスを防止します。（1時間毎に更新）
リアルタイムの分類エンジン	不適切なコンテンツを持つ新しいサイトや未分類のサイトへのアクセスを防止します。
コンテンツ認識型巡回検査	リクエストの分解と応答を行い、コンテンツに見える実行ファイル（別のファイル形式内や圧縮コンテナに埋め込まれたものを含む）を正確に検出します。
管理、レポート作成	
Webベースの直感的なインターフェイス	簡単に操作が可能で、複雑な構文やLinuxのコマンドを学習する必要がありません。
事前定義されたカスタマイズも可能なレポート	直感的なドリルダウンで視覚的なレポートを容易に修正、実行、共有できます。
定期的なレポート作成	一度作成したレポートを繰り返し実行し、電子メール経由で配布できます。
複数のGateway製品を統合したレポート作成	ユーザーのアクティビティを統合したレポートにより、管理データの分析や共有が容易になります。
SNMP、SMTP警告	SNMPまたはSMTP管理警告を使用し、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。

* 2つ目以降はコストオプション
** コストオプション

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、安全なコラボレーションとビジネスの成長の実現を推進する、世界中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、現在900を超えるリセラーと共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: salesjp@clearswift.co.jp
Web: http://www.clearswift.co.jp/

2017年 12月