

WatchGuard XCS™

ネットワーク・トラフィックのセキュリティを実現し、
プライバシーを保護するXCSアプライアンス



WatchGuard® **Extensible Content Security (XCS)** は、インバウンドとアウトバウンドのメールに対し、厳格なセキュリティとプライバシーを提供。XCSをWeb Securityサービスとバンドルすることによって、メールとウェブのトラフィックを包括的に管理し、強力な統合セキュリティを実現できます。

XCSソリューションのメリット

- 複数のプロトコル上で、コンテンツ・セキュリティと脅威管理を効率的に統合
- 全てのメールとウェブのトラフィックを可視化し、管理を実現
- 企業コンプライアンスに必要なツールと情報を提供
- 複数のポイント・ソリューションを導入する必要がなく、コストと管理の手間を大幅に削減

The XCS platform "...
dramatically reduced
our email volume &
exposure to malicious
email-based attacks."

Stan Prothero
Network Services Supervisor
Puget Sound Blood Center

迷惑メール対策

- XCSの中核である「クラウド」コンポーネントの**Reputation Authority**は、最大98%の迷惑メールをゲートウェイでブロックし、ネットワーク帯域の最適化を実現し、ネットワークを脅威から守ります。
- **アンチスパム・エンジン**は、送信者情報と画像、添付ファイル、埋め込まれたURLなどのコンテンツを検査。メッセージ・トラフィックのコンテンツ分析をカテゴリーとスコアによって自動的に行い、高度なセキュリティを実現します。
- **迷惑メールおよび疑わしいメールの検疫機能**は、迷惑メールをローカルの検疫サーバへ転送。ユーザーは、ウェブ・ベースのインターフェイスから容易に、検疫メッセージ、安全リスト、ブロック・リストを管理できます。

ウイルス、スパイウェア、マルウェアからの保護

- **Zero-Hour Threat Outbreak Response**は、攻撃が仕掛けられた時間とスキャン用フィルタが開発・配布されるまでのセキュリティホールを削減します。
- **先進的なコンテンツ・フィルタリングおよびマルウェア対策**は、インバウンドとアウトバウンドのメールをスキャンし、悪意のあるコンテンツからネットワークを守ります。

プライバシーとコンプライアンスを実現するDLP（情報漏洩対策）

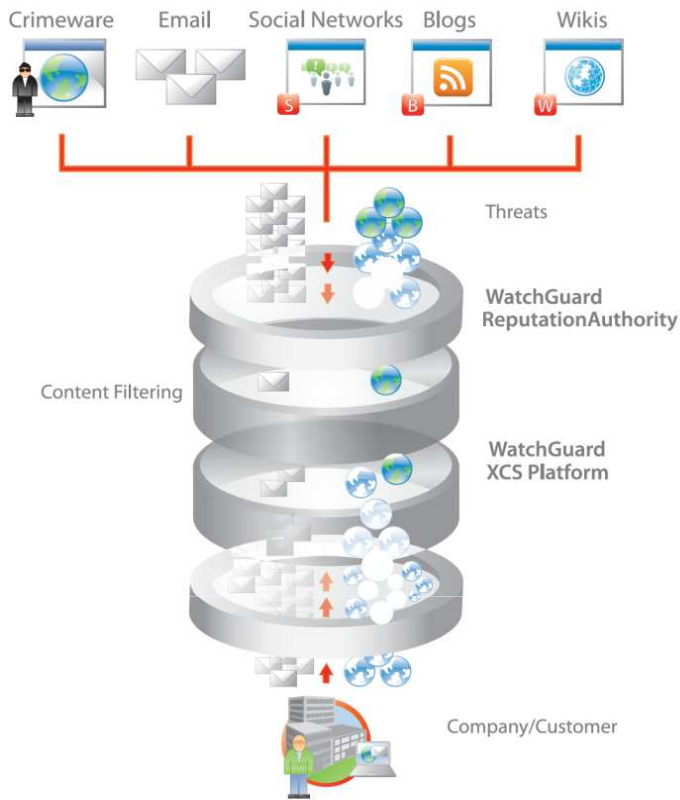
- **トランスペアレント修正機能**は、情報漏洩を防ぐために、ユーザ設定ポリシーに基づいて、メッセージを自動的にブロック、検疫、ルート変更、ブラインド・コピー、暗号化、または許可を行います。
- **コンプライアンス対応のための定義済みルール**は、リアルタイムでのデータロス対策と具体的な業界規制のポリシーに基づいており、カスタマイズ可能です。
- **シームレスなメール暗号化機能（オプション）**は、専用サーバ不要で、機密メッセージをセキュアに全ての受信者に配信可能。多くの暗号化技術に必要な高いコストを削減できます。
- **Eプロファイリングでのデータ検知と分類**によって、機密情報ファイルを分類し、同類の情報がアウトバウンド通信に含まれた場合、どのような情報を検知し、アクションを実行するかシステムに設定することが可能です。
- **一元的なDLP管理**によって、複数のプロトコル上に一つのポリシーを適用し、通信中のデータを消失およびポリシー違反から保護できます。

高い信頼性を実現するメール・セキュリティ

- **ダイナミックなオンデマンド・クラスタリング機能**は、複数のシステムへ簡単にシステム設定とメッセージング・キューを複製し、冗長性とスケーラビリティを実現し、最大限のアップタイムを提供できます。
- **メッセージ・レベルの冗長性**によって、通信が消失せずに、メール・セキュリティが常に稼働し実行されていることを保証します。

Web Securityサービスでセキュリティをウェブ・トラフィックへ拡張

- **利用許可とアプリケーション管理機能**によって、ユーザおよびグループに対して詳細なポリシーを設定し、インターネットとアプリケーション利用を一元的に管理・制限することができます。
- **URLフィルタリングとカテゴリ機能**は、コンテンツとポリシーに基づいてウェブサイトへのアクセスを動的に分析・ブロック。悪意のある不適切なサイトへのアクセスを遮断します。
- **ダイナミック・インスペクション機能**によって、コンテンツ検査をリアルタイムに行い、ネットワークに入ってくる全てのウェブ・ページを分析し、リスク・レベルを判断。ダイナミックに個々のページ、または一部をブロックします。
- **ウェブ・トラフィック拡張機能**は、ウェブ・キャッシング、拡張HTTPスキャン、大きなファイルのダウンロード、ストリーミング・メディアのサポートなどを含み、バンド幅帯域、サーバ負荷、ウェブ・トラフィックの遅延時間を削減します。



98%の不要なトラフィックをネットワーク上でブロック

WatchGuard ReputationAuthorityを活用し、悪意のある送信者を特定し、リアルタイムの振る舞いに基づいて98%以上の脅威をブロックします。複数のプロトコル上でデータをクロス参照・分析することにより、悪意のある不要なトラフィックが決してネットワークに入り込まないようにします。

ディープな防御を行うコンテンツ・フィルタリング

インバウンドとアウトバウンドのメールとウェブのトラフィックに対して、複数レイヤーのディープインスペクションを実行。コンテンツ、画像、送信者情報を徹底的に検査・分析し、誰が送信しているか、メッセージに何が含まれているか、どのようにメッセージが構成されているか、受信者の動作をどこに導くかによって、コンテキスト・ベースでウェイトの付いたスコアを提供。脅威レベルを設定し、安全な通信だけがネットワークを通ります。

リアルタイムDLP

ユーザが設定したポリシーに基づいて、複数のプロトコル上で、進行中のデータをブロック・検疫・許可・暗号化あるいは別の経路に切り替えることができるリアルタイムのソリューションを提供。リスク管理およびポリシー執行範囲の拡張機能を実現し、ポイント・ソリューション製品の導入なしで、プライバシーの保護とコンプライアンスの実現を可能にします。

一元管理とレポーティング

優れた管理機能によって、複数のプロトコル上のインバウンドとアウトバウンドのトラフィックに対して一つのポリシーを適用可能。管理時間を短縮し、他のITプロジェクトに集中する時間を増やすことができます。

複数のプロトコル上でのネットワークの出入りを可視化することによって、セキュリティの隙間をなくし、ポイント・ソリューションで必要とされる管理業務を削減することができます。

統合システムレポートに容易にアクセスし、指定の間隔や様々なフォーマットでカスタマイズ可能。時間、機能、グループなどをベースにレポートを作成・出力し、監査要件を満たすことができます。

管理者が複数のプロトコルにわたるポリシーを一つのビューから作成・管理・実行することができます。メールとウェブの包括的なレポートにより、自社ネットワークへの出入りを網羅的に把握することが可能です。

さまざまな規模の企業ネットワークに、最適なコンテンツ・セキュリティ・ソリューションを提供します。

ユーザ数 500 1000 4000 7000 10000 →

XCS170
最大500ユーザまでのメール・セキュリティ・ソリューション

XCS370
最大1,000ユーザまでのメール・セキュリティ・ソリューション

XCS570
最大1,000ユーザまでのエンタープライズ・メール・セキュリティ・ソリューション

XCS770
中規模エンタープライズ向けコンテンツ・セキュリティ・ソリューション

XCS970
大規模エンタープライズ向けコンテンツ・セキュリティ・ソリューション

XCS1170
Fortune500/Global 2000企業を含む大規模エンタープライズ向けコンテンツ・セキュリティ・ソリューション

安心サポート

全てのXCSアプライアンスは、WatchGuardのサポート&メンテナンス・プログラムであるLiveSecurity Serviceがバンドルされています。※

LiveSecurity Service内容 ■ハードウェア保証 ■テクニカル・サポート ■ソフトウェア・アップデート ■脅威レポート

※ 1年、2年、または3年のサービスから選択。

ウォッチガード・テクノロジー・ジャパン株式会社

〒150-8512 東京都渋谷区桜丘町26-1 セルリアンタワー15階 Tel.03-5456-7880 Fax.03-5456-5511
http://www.watchguard.co.jp info-jp@watchguard.com