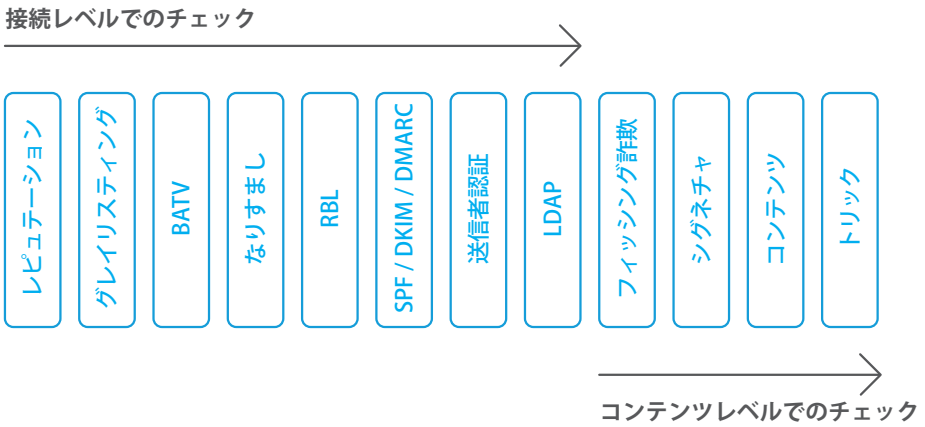
clearswift
RUAG Cyber Security

スパム対策

Clearswift SECURE Email Gatewayは、マルチレイヤーのウイルス対策ソリューションを搭載。99%の検出率を達成し、誤検出を最小に抑えます。



スパム対策機能がスパムやフィッシング詐欺、メールマガジン（ニュースレター）と判定した電子メールに対して、システム管理者はポリシーを構成して、ブロック、サニタイズ、保留、タグ付け、配信といったアクションを取ることができます。

- **レピュテーション** – TRUSTmanagerを利用。外部からのメールはすべて、数百万のIPアドレスのレピュテーションを網羅したリアルタイムのデータベースに照らしてチェックされます。送信元IPアドレスが"BAD"に分類されている場合、そのメールは即座にブロックされます。
- **グレイリスティング** – 送信者のレピュテーションが疑わしい場合、最初は接続を拒否し、送信者にメールの再送信を要求できます。これによりスパムのボットネットを取り除くことが可能となると同時に、システムが受信するマルウェアの数を減らすこともできます。
- **BATV** – システムが受信した配達不能レポートスパムを検出します。これは、社員の電子メールアドレスに偽装したスパムメールによって引き起こされるもので、そのメールの配達不能レポートが生成されると、偽装された送信者に送り返されます。
- **なりすまし対策** – なりすましメールを検出するため、システムには幾重ものアルゴリズムが組み込まれています。この機能は、SPF、DKIM、DMARCを使用することでさらに強化されています。
- **RBL** – 一体型のリアルタイム ブロックリストは、Spamhaus、Protected Sky、IBM、SORBSなど複数のRBLで強化することができます。これは、送信元IPアドレスがスパム行為に関わったことがあるかどうかをチェックするために作られた別個のシステムです。
- **メッセージ認証サービス** – Clearswift SECURE Email Gatewayは次の3つのメール認証機能を備えています。
  - **SPF** – 送信元IPアドレスを、公開されたDNS内送信IPアドレスのリストに照らしてチェックします。
  - **DKIM** – DKIMヘッダーが送信者によって追加されたかどうかを受信側がチェックします。これは、送信者のDNSレコードと同じ鍵ペアを使用して作成されたものです。
  - **DMARC** – SPFチェックとDKIMチェックの両方または一方の結果を使用して、メールの正当性をさらにチェックするものです。
- **送信者認証** – 送信元のドメインが存在するかどうかをチェックします。
- **LDAP** – Active Directoryと統合され、メールを受領する前に受信者が存在するかどうかをチェックします。
- **フィッシング詐欺** – フィッシング詐欺に特有のURLや添付ファイルの有無をチェックし、通常のバルクスパムやバルクメルマガではないことを確認します。これにより、フィッシング詐欺メールをその他の"通常のスパム"と区別できます。
- **シグネチャ** – バルクメールを識別します。
- **コンテンツ** – 攻撃的な内容のコンテンツを識別します。
- **トリック** – スパム対策ソリューションを迂回してしまうような形式や送信方法を取るメールを見つけ出します。

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/