

メール暗号化

Clearswift SECURE Email Gatewayは、いくつかの暗号化技術によるオプションを提供し、インターネット回線で送信される電子メールの安全を保ちます。

メール暗号化を行うことで、Eメールメッセージが確実に保護されます。

- **機密性** – メール内容が意図しない相手に読まれてしまうことはほとんどの場合ありません。
- **完全性** – メール内容が損なわれることなく、送信者から受信者に渡るまでの間に誰にも改変されることなく配信されます。
- **否認防止** – メールの内容と誰が送信したかについての情報を、起こったこと、あるいは起こらなかったことを法的に証明するために利用できます。

Clearswift SECURE Email Gatewayは、他社製品と比較してビジネスコミュニケーションを安全にするためのより広範な機能に対応しています。

機能	Clearswift	Cisco	Forcepoint	Barracuda	Microsoft	Google	Symantec	Mimecast	Fortinet	Proofpoint
暗号化	あり	あり	あり	あり	あり	あり	あり	あり	あり	あり
TLS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
パスワード	✓	×	×	×	×	×	×	×	×	×
プッシュ/プル	✓	✓	✓	✓	✓	✓	✓	✓	×	✓
S/MIME	✓	✓	×	×	×	×	×	×	✓	×
PGP	✓	×	×	×	×	×	×	×	×	×
PDF	×	×	×	×	×	×	✓	×	×	×
レコード管理	×	×	×	×	✓	×	×	×	×	×
IBE	×	×	✓	×	×	×	×	×	✓	×

Clearswift SECURE Email Gatewayは、通信方向やポリシーに応じてメールの暗号化を設定できます。(例: クレジットカード番号を添付ファイル中に発見した場合など)

ユーザーコミュニティ、メールの頻度、暗号化の必要性 (デスクトップへ、デスクトップから、インターネット回線上) に応じた様々な暗号化手法があります。

Transport Layer Security (TLS)

TLSは送信者のデスクトップから受信者のデスクトップに至るまでの全経路に渡ってメールを保護するものではありませんが、インターネット上のサーバー間のメール通信を保護します。エンドユーザーに対して完全に透明性があるため、広く利用されています。TLSはClearswift ARgon for Emailでも利用可能です。

パスワード

メール本文と添付ファイルはパスワード保護されたZipファイルに圧縮されて受信者に送信されます。送信者は受信者にパスワードを届ける必要があり、それには通常SMSや別アカウントへの電子メールが使用されます。

ポータル ブッシュアップ

ホスト型電子メールポータルでは、電子メールの受信者は着信メールをWebメールスタイルのクライアントを使用して開き、送信者への返信も安全な方法で行うことができます。この技術はメールのトランザクションが少ない、あらゆるレベルのユーザーを対象としています。上級ユーザーは、安全なWebメールポータルにログインせずに直接自分の企業メールクライアントで暗号化メールを受け取れるように設定を調整することも可能です。

Secure MIME (S/MIME)

S/MIMEは電子メールを安全に送信するために用いられる国際規格であり、ヨーロッパで広く使われています。S/MIMEでは公開鍵暗号化方式が用いられます。ユーザーは数学的にリンクされた公開鍵と秘密鍵の両方を持っており、公開鍵を使用して暗号化されたメッセージは、対応する秘密鍵を持つ受信者によってのみ開くことができます。Clearswift SECURE Email Gatewayでは、サーバーとユーザー間の通信暗号化にこの技術が使われています。

Pretty Good Privacy (PGP)

PGPはS/MIMEと類似のメカニズムを持っており、ユーザーは公開鍵と秘密鍵の両方を持ちますが、異なるアルゴリズムが用いられます。

Portable Document Format (PDF)

これはメール本文と添付ファイルをパスワード保護付きのPDFファイルに埋め込むもので、パスワード保護付きのメールが作成されるのと同様の方法です。パスワードは安全な方法で配布される必要があります。

レコードマネージメント (DRM)

DRMでは、受信者がデータをEメールまたはハイパーリンクで受領でき、受信者のみがデータにアクセスすることができます。受信者のデータ操作については制限（転送や印刷など）を設けられる上、データはいつでも取り消し可能です。

IDベース暗号 (IBE)

IBEは受信者が鍵や証明書を持つ必要のない暗号化方式です。

送信者は受信者に対し、受信者の姓名または電子メールアドレスから生成された鍵によって暗号化されたメールを送信できます。

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 Clearswift Ltd. 本内容の無断転載を禁じます。

Clearswiftのロゴ、Clearswiftの製品名は、Clearswift Ltd.の登録商標です。

記載の製品および会社名は各社の商標または登録商標です。

製品仕様、デザインは予告なく変更することがあります。