

SecureAge

# SecureEmail



暗号化メールをもっと気軽に

いつものメールソフトでシームレスに送信、受信、保存

# SecureEmailとは？

SecureEmailは、ITセキュリティ上の最大の弱点である、Emailへの攻撃や情報漏洩からの防御を行う、業界最高水準の暗号化メールソフトウェアです。

メールプラットフォーム上で効果的かつ完全な鍵管理を行うことで、今までの効率を失うことなく信頼性とプライバシーを保持しながら、シームレスな送受信および保存を可能にしています。



## Emailの分類とセキュリティの選択

ポリシーベースのセキュリティ制御で、「分類なし」「制限あり」「親展」といった、Emailの機密分類化を簡単に設定できます。

このメール分類ラベルの機密性によって、セキュリティ（「署名」「暗号化」「署名と暗号化」「DRM署名と暗号化」など）の選択肢が決まります。また、送信後の保存や転送、返信の扱いまで管理することができます。

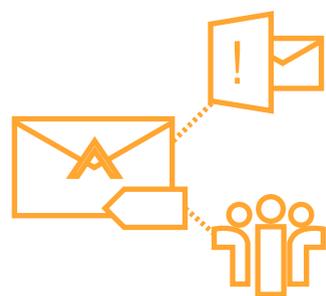
分類ラベルは、「機密」や「極秘」など種類やセキュリティレベルに応じて、カスタマイズすることも可能です。

## お任せ鍵管理

SecureAgeは、暗号化に PKI(Public Key Infrastructure: 公開鍵基盤)を使用しています。

メールの暗号化に使用する秘密鍵および公開鍵は自動管理されますので、ユーザは鍵管理を気にすることなく、作業を続けることができます。

SecureEmailは、無制限のRSA鍵長をサポートするとともに、無制限に鍵ヒストリーを保存するため、メールアーカイブへのアクセスも簡単です。



## 各種メールソフトとのシームレスな統合

SecureEmailは、多くの企業が利用している主要なメールプラットフォームの Microsoft OutlookやIBM Notesなどのプラグインを搭載していますので、今までの作業効率を妨げることなく、メールの暗号化が行えます。

また、SecureEmailは、上記の分類ラベルやポリシールールなどのロジックを、カスタマイズして導入することもできます。

## 暗号化アルゴリズムのカスタマイズ

SecureEmailは、RSA, Triple-DES, AESなどの暗号化アルゴリズムをサポートしていますが、カスタマイズを行い、独自のアルゴリズムを採用するなど、更にセキュリティレベルをあげることも可能です。



# SecureEmailの特徴と技術



## ポリシーベースのセキュリティ

セキュリティに応じたメールの分類を事前定義またはカスタマイズすることで、簡単にメールを暗号化します。



## 自動送信エージェント

数の多い受信者に対し、定期的に安全かつ自動的にメールを送信できる機能です。



## デジタル著作権管理 (DRM)

メール受信者のリストに制限をかけ、印刷、スクリーンキャプチャ、転送、コピー有効期限などの機能を制御します。



## 受信者のデジタル証明書を自動取得

将来使用の目的で、受信者の証明書を自動検索し、インポートします。



## デジタル証明書の自動管理

デジタル証明書を自動的に認証、削除、更新します。



## SecureAge管理サーバとの互換性

SecureEmailユーザの集中型ポリシー管理、ログ管理、鍵管理を簡単に行えます。



## メールヘッダーの整合性保護

ヘッダとメール内容の両方を署名暗号化し、それぞれの整合性を検証、保護します。



## S/MIME メールサポート

SecureEmailを利用していない第三者へも追加ソフトなどを必要とせず、暗号化メールの送信が可能です。



## メールアーカイブの再暗号化

古い鍵から新しい鍵へ移行するツールも備え、アーカイブされた古いメールも、新しい鍵で常に暗号化されています。



## SecureEmailから第三者(サードパーティEmailクライアント)への送信について



SecureEmailは、S/MIME標準(Microsoft Outlook、IBM Notes、Apple Mail、Thunderbirdなど)のEmailクライアントソフトウェアと暗号化されたEmailを交換することで、公開鍵(デジタル証明書)を自動インポートし、暗号化メールを送信することができます。

### 1. 暗号化して送信

S/MIME標準を利用しているEmailクライアントとは、すべての電子メールコンテンツと添付ファイルを暗号化して、送信が可能です。ただし、受信者は事前に公開鍵をSecureEmailユーザに送信する必要があります。公開鍵の送信方法はクライアントソフトにより異なりますが、作業はとても簡単です。

(例えば、受信者がMicrosoft Outlookをご利用の場合、下記を参照してください。

Microsoft ホーム > サポート > Outlook > メール > デジタル署名 > デジタル署名を追加してメッセージを保護する)

### 2. 平文で送信

すべての電子メールコンテンツと添付ファイルは、暗号化されていない単純なメールとしても送信できます。

ただし、SecureEmailユーザは、SecureAge管理者が作成したオンラインおよびオフラインのポリシー内で、平文のEmailを送信する権利が必要です。

# ゲートウェイEmailセキュリティとの比較

メールへの脅威は、送信者や受信者を直接襲うだけでなく、時にはメールサーバへも及ぶことがあります。

ゲートウェイEmailセキュリティでは、一度マシンが侵されてしまうと、暗号化されていない平文のメールコンテンツを、保護することはできません。



## ゲートウェイEmailセキュリティ

移動データのみを暗号化  
ユーザPCや企業サーバ内において  
データは平文状態です



## SecureAge SecureEmail

エンドツーエンド保護  
停止中でも、使用中でも、移動中でも  
メールは常に暗号化状態を保ちます

SecureEmailは、すでにご利用中のメールプラットフォームを変更すること無く、ゲートウェイ以上のメールセキュリティをお約束します。

メールは常に暗号化を保ち、認証されていないユーザのアクセスを許さず、エンドツーエンドのメールセキュリティを提供します。

### ソフトウェアの仕様と要件

#### 製品情報

製品名: SecureAge SecureEmail  
表示言語: 日本語、英語  
ライセンス: 標準およびボリュームライセンス  
サポート: 1年(以降別途SMS更新)  
付属品: 各種管理者ガイド、ユーザガイド

#### インストール要件

プロセッサ: OSで推奨された x86/x64ビットプロセッサ  
※AES-NIに対応したプロセッサを推奨  
OS: Windows 10, 8.1, 8, 7, Vista, XP  
Windows Server 2012, 2008, 2003  
メモリ: OSで推奨された容量  
HDD: 50MB以上の空き容量

※仕様と要件は予告なく変更される場合がありますので、予めご了承ください。



セキュアエイジ株式会社 〒105-0001 東京都港区虎ノ門1-16-6 UCF7F ☎03-6869-7269



[www.secureage.co.jp](http://www.secureage.co.jp)



[contactus@secureage.co.jp](mailto:contactus@secureage.co.jp)