

ファイルを格納するだけで 簡単に暗号・復号化！

データの**全自動署名暗号化**を実現

世界標準

世界178ヶ国 11万社が導入している
「公開鍵暗号化方式」のデファクトスタンダード
PGP暗号システムを簡単に導入できます。



スムーズ導入



既存のシステムへの影響を
最小限に抑え、
迅速かつ柔軟な導入が可能。
汎用性もバツグンです。



データ保護

日本版SOX法・個人情報保護法への対応。
暗号化・電子署名、ファイルの完全削除など、
機能が充実しています。



PGP自動暗号サーバ

PGP自動暗号サーバのメリット

1

簡単操作でファイルを暗号化

複雑なCommand Lineパラメータを理解しなくても簡単に導入可能です。
また、フォルダを周期監視するため、特定フォルダにファイルを格納するだけで暗号、復号が実現可能です。

世界標準のPGP暗号システムを簡単導入

世界標準でかつ強力なPGP暗号システムを簡単に導入できます。
PGP Desktopとの連携も可能で、PGP DesktopのGUIを使って鍵管理を行うことができるため、管理作業が軽減されます。

2

3

多数のユーザを一台のサーバでカバー

一台のサーバを設置するだけで、多くのユーザがファイルの暗号化、復号化を行うことが可能です。




電子署名対応

保管書類を暗号及び電子署名して保存すれば、万一の流出や不正な参照を防ぐことができるだけでなく、改ざん防止にも役立ちます。
このような暗号化・電子署名も単に特定のフォルダへファイルをコピーするだけで行うことができます。

4

PGP自動暗号サーバの機能

PGP自動暗号サーバの共有フォルダへファイルを格納するだけで、

-  ファイルの暗号化
-  ファイルの復号化
-  ファイルの電子署名

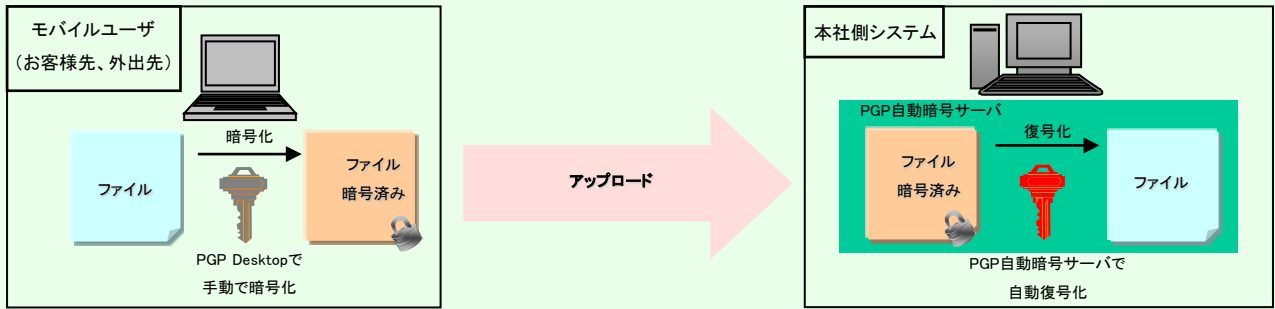
を行うことができます。



PGP自動暗号サーバ導入例

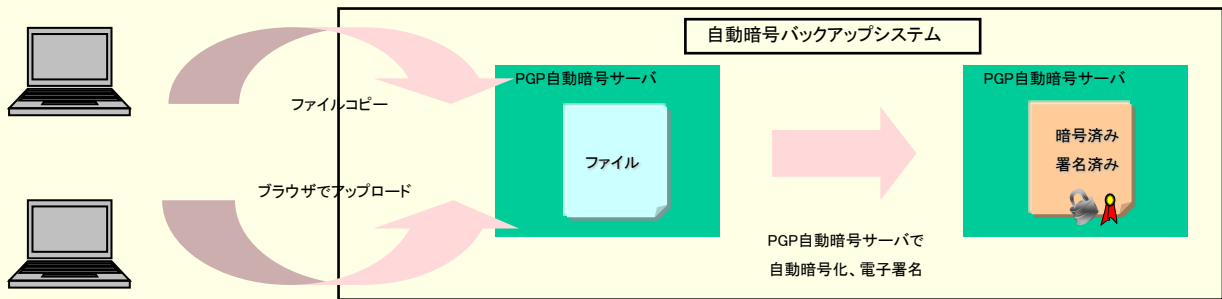
暗号ファイルWEB転送システム

ファイルを暗号化してから転送することで、インターネットでの重要ファイルのアップロードを実現します。



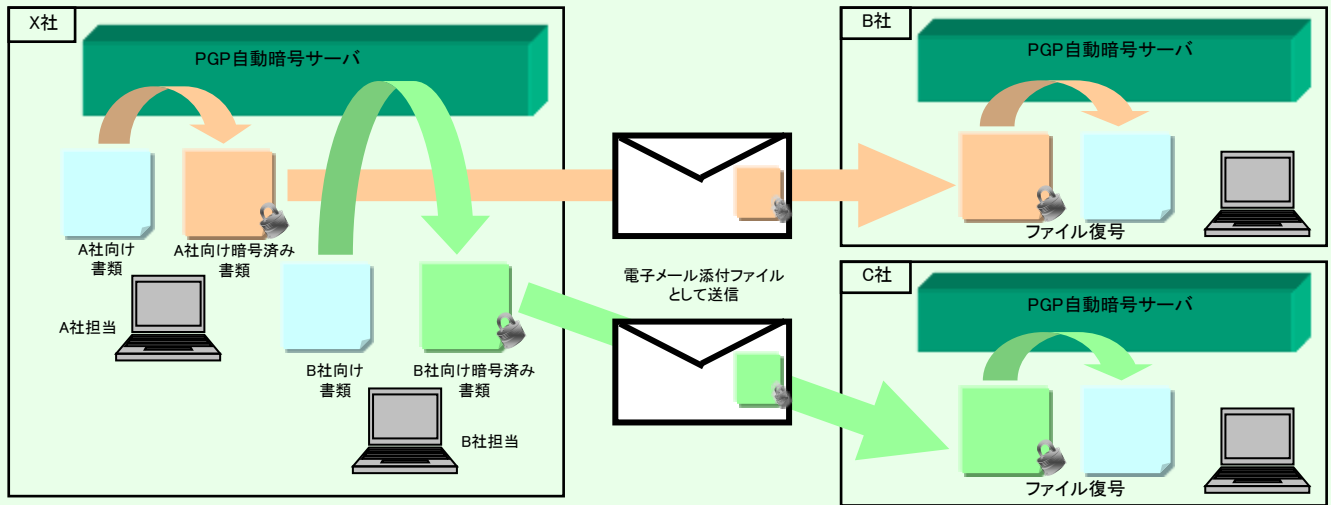
重要ファイルバックアップシステム

重要ファイルをファイルサーバへコピーまたはアップロードするだけで、自動で暗号化しセキュアに保存します。署名付与により、改ざん防止もあわせて実施できます。



暗号ファイル企業間送受信

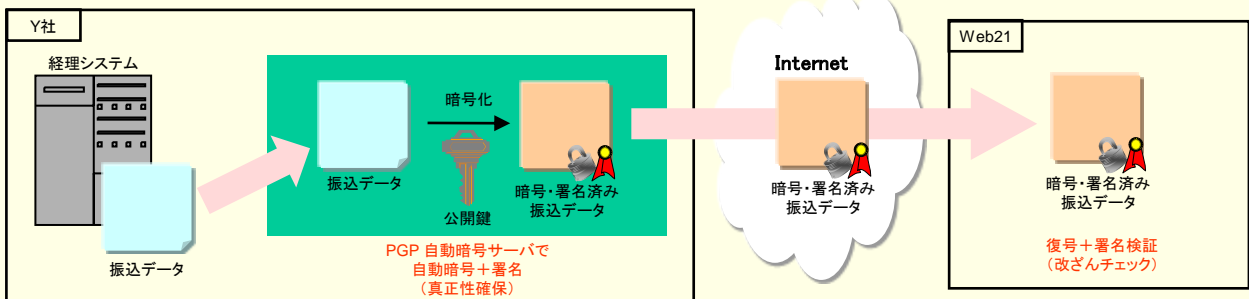
重要ファイルをやり取りする企業間でのインターネットメールを使った簡易な暗号ファイル送受信システムです。



WEB21 振込データ改ざん防止システム

「Web21」は、三井住友銀行様の法人向けのインターネットバンキングサービスです。振込、給与支払、残高や明細照会などの経理業務をパソコンから行うことができます。PGP暗号データのアップロードに対応しています。

PGP自動暗号サーバを用いて振込データ出力時に暗号、署名を行うことで、振込データの真正性を確保(第三者への漏洩がなく、途中改ざんがないことを確認)できます。





PGPについて

【PGPとは】

PGP (Pretty Good Privacy) はフィル・ジマーマン (Philip Zimmermann) が開発した公開鍵方式を利用した暗号ソフトウェアです。電子メールで利用されることが多いPGPですが、ファイルの暗号及び復号を行うことができます。

暗号方式としては大変広く利用されており、世界標準の暗号システムといえます。

秘密鍵・公開鍵のペアを利用し、公開鍵を交換することで誰でも、あなただけが解読できる暗号ファイルを作成することができます。また電子署名にも対応しているので、ファイルの改ざん防止にも利用することができます。

【PGPのメリット】

鍵の交換が簡単

公開鍵を渡すだけです。公開鍵が漏洩してもセキュリティ上の脅威は小さいです。

秘密鍵はパスフレーズで保護

秘密鍵は漏洩してはならないものなので、パスフレーズを付与することで保護可能です。またUSB型のセキュリティトークンに格納しておく方法もあります。(オプション)

世界標準(デファクト・スタンダード)

デファクト・スタンダードとして世界でもっとも広く活用されている暗号方式といえるでしょう。企業間でのデータ交換に使用するには、独自方式ではなく世界標準の方式を採用するのがよいでしょう。

豊富なツール

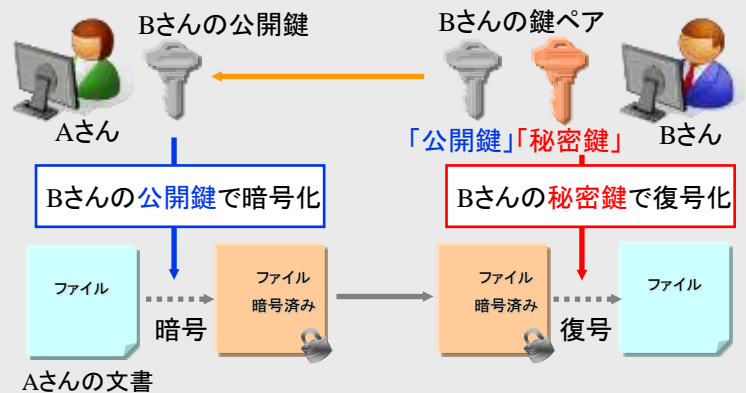
PGPをサポートする豊富なツールがPGP社より提供されています。

公開鍵と秘密鍵

公開鍵暗号方式で使用する鍵ペアには、「公開鍵」と「秘密鍵」があります。

「公開鍵」・・・データの暗号化のみを行います。公開鍵で暗号化されたデータは対となる秘密鍵でしか復号することはできません。

「秘密鍵」・・・対となる公開鍵で暗号化されたデータの復号化を行います。対となる公開鍵以外で暗号化されたデータは、復号化することはできません。



技術仕様

動作環境

- Windows Server 2008*
- Windows Server 2003 (SP2)*
- * Microsoft .NET Framework 3.5のインストール要

公開鍵形式

- OpenPGP (RFC 4880)
- X.509 v3

共通鍵暗号アルゴリズム

- AES (最大256ビット鍵) / •CAST5 / •TripleDES
- IDEA / •Twofish / •Blowfish* / •Arc4 (128ビット鍵)
- * Blowfishのサポートは、Blowfish で暗号化されたメッセージの復号化、または、優先する暗号としてBlowfishが指定された鍵に対する暗号化に限定されます。

ハッシュ

- SHA-1, SHA-256, SHA-384, SHA-512
- MD5 / •RIPEMD-160

公開鍵暗号アルゴリズム

- Diffie-Hellman (最大 4096 ビット鍵)
- DSA (1024 ビット鍵のみ、最大 3072 ビットまで検証可能)
- RSA (最大 4096 ビット鍵)

圧縮アルゴリズム

- Zip / •BZip2 / •ZLib



〒163-0777 東京都新宿区西新宿2-7-1 新宿第一生命ビル
ソリューションビジネス本部 ソリューション営業1部

TEL : 03-3342-1411 FAX : 03-3342-0453

※カタログに記載されている会社名及び製品名は、各社の商標または登録商標です。