

見せない

データの**全自動署名暗号化**を実現!

触らせない



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。

全自動
署名暗号化
||
PGP® Command
Line



178ヶ国
11万社

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です。

PGP® CommandLine

PGP® Command Lineは、信頼されたPGP®の暗号化エンジンを貴社のシステムに組み込むことができる暗号化ツールです。

①公開鍵を利用した暗号化と電子署名

世界標準のPGP公開鍵暗号化方式で、暗号化と電子署名を行います。

②公開鍵を利用した復号化と署名検証

PGP公開鍵暗号化方式で暗号署名されたファイルの復号化と署名検証(改ざん・なりすましチェック)を行います。

③自己復号形式での暗号化

共通鍵(パスメッセージ)を利用してPGP製品を持たないPC上でも復号化が可能な「自己復号形式」で暗号化を行います。

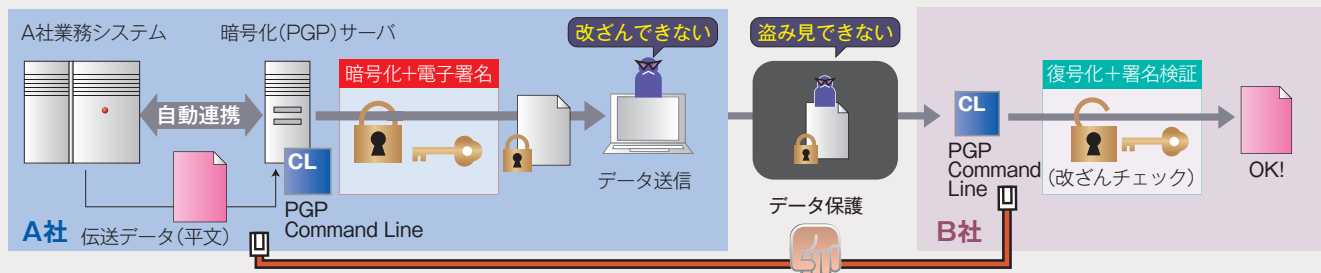
④ファイルやフォルダの完全削除

ファイルやフォルダの完全削除、ディスク空き領域の完全削除を行います。

Q 他社に送る重要情報、途中で改ざんされたり漏洩しない方法は？

活用例① システム間のデータ伝送におけるデータの機密性と完全性を確保する。

システム間の連携

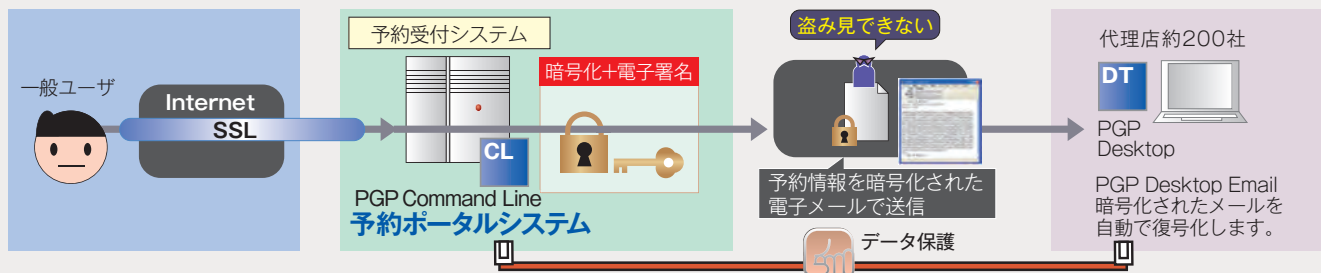


A PGP Command Lineを用いて、自動的に暗号化・電子署名を行うことで、相手に送ったデータの第三者への漏洩を防ぐことができます。また、途中で改ざんされていないことも確認できます。

Q お客様から預かった大切な情報を、安全に関係先に自動転送するには？

活用例② システムから自動配信されるデータの機密性を確保する。

自動一斉配信

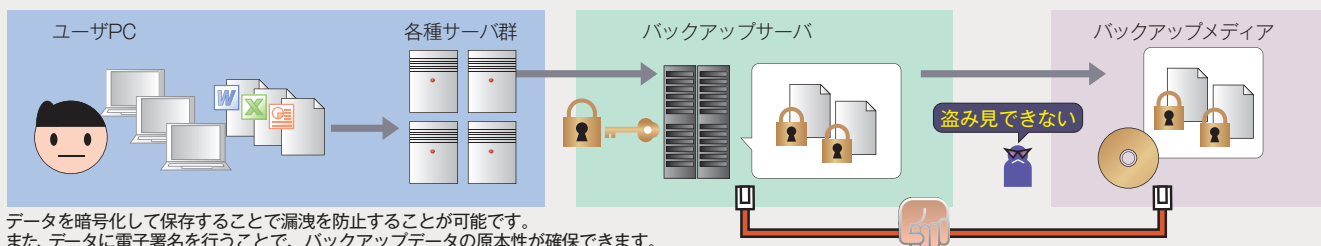


A 関係先への自動転送をする際に、PGP Command Lineで重要情報を自動的に暗号化することで、第三者への漏洩を防ぐことができます。関係先は、PGP Desktopを用いて、重要データを開くことができます。

Q バックアップサーバ内に重要データが蓄積されている、適切な漏洩・改ざん対策は？

活用例③ システムバックアップの機密性と完全性を確保する。

データバックアップ



データを暗号化して保存することで漏洩を防止することが可能です。また、データに電子署名を行うことで、バックアップデータの原本性が確保できます。

A PGP Command Lineでバックアップデータに自動的に暗号化・電子署名を施すことで、漏洩・改ざんのリスクを抑えることができます。暗号化されたバックアップデータは、メディアに移しても、漏洩の心配はありません。



「信頼性や普及率。要件を満たすのは、PGP®Command Line しかありませんでした」

三井住友銀行、パソコンバンク Web21の新オプションサービス「振込データ改ざん防止システム」

三井住友銀行様は、法人向けインターネットバンキング「パソコンバンクWeb21(以下 Web21)」で、PGP®Command Lineを活用した、振込データ改ざん防止のための新しいセキュリティ強化システムを開始しました。開発を担当した同行EC業務部商品企画第一グループ 部長代理 北谷展清氏にうかがいました。



-- 「Web21」と、新しく追加したセキュリティ強化システムについて教えてください。

「Web21」は、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、会社のパソコンから行うことができます。2008年現在、10万社を超えるお客さまに、ご利用いただいています。「Web21」は、利便性だけでなくセキュリティにも力を入れており、今回PGP Command Lineを使って「振込データ改ざん防止システム」を構築したのも、そうした取り組みの一環です。

「振込データ改ざん防止システム」は、Web21「エキスパート」のオプションサービスとしてご利用いただけるもので、お客さまが三井住友銀行に送信する振込依頼データが、お客さまの社内で改ざんされていないことを担保するためのシステムです。主に、内部統制報告書を提出する必要がある上場企業向けサービスとして開発しました。

-- 「振込データ改ざん防止システム」を使うと、何がどう良くなるのですか。

「振込データ改ざん防止システム」を使うことにより、振込の業務手順における社内不正(振込データの改ざん)を防止することが可能になると考えています。振込とは、「会社のお金が、会社の外に出て行くこと」であり、財務諸表とも直結する業務なので、内部統制報告書においては、特に重視されるポイントです。

振込業務では、担当者が振込依頼をし、承認者(上長)がそれを承認して、はじめて振込が実行されます。この承認手続きと、その他のセキュリティ機能により、通常はこのセキュリティレベルで十分であると思われる。しかし、内部統制報告書を監査する、

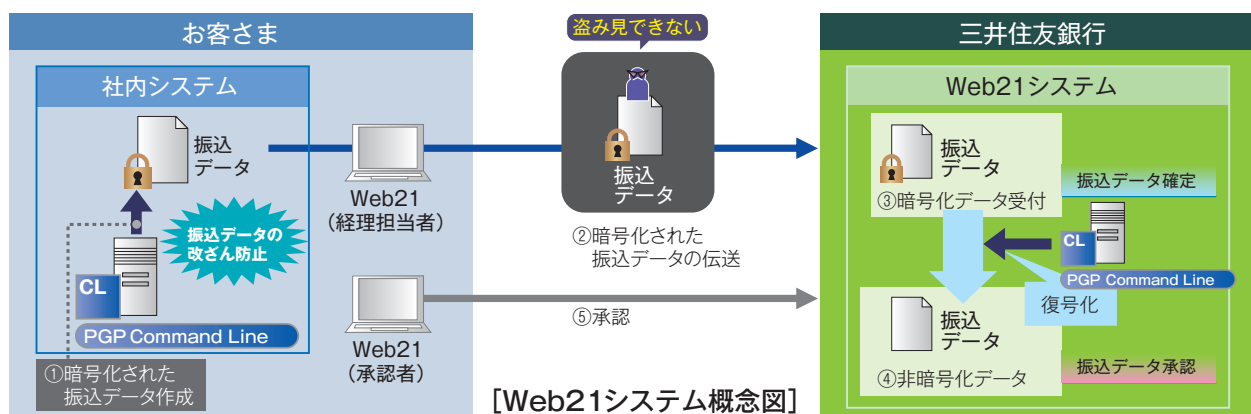
監査法人の視点からは、基幹システムから出力された振込データと実際に銀行に届いた振込データが完全に同一であることが担保されておらず、「業務手順の統制が不十分」と見えることがあります。「振込データ改ざん防止システム」では、お客さまのシステムで暗号化・電子署名を施された振込データを銀行に伝送することになるため、担当者による改ざんは不可能です。システム上で、(A)お客さまの経理システムから出力された振込依頼データと、(B)三井住友銀行に送信されたデータとの同一性を証明でき、「しくみとしての改ざん防止」を成しえるのです。

-- 改ざん防止に、なぜ暗号化が最適なのですか。

振込データが「改ざんされていない」ことを担保する手段としては、暗号化の他に、①(A)(B)の二つのデータを見比べる「徹底目視検査」、②お客さまと三井住友銀行のホストコンピュータどうしを専用線で直接つなぐ手法の2種類が考えられます。①は正確性と人的コストの問題があり、②は業務手順に人手を介在させないので、正確性は申し分ないのですが、膨大な費用がかかります。暗号化を用いると、正確性と費用の両面から最も現実的でしたし、導入後の、振込操作におけるお客さまの手数は通常の「Web21」と大して変わりません。

-- 暗号化エンジンにPGP®Command Lineを採用した理由は。

PGPIは、1991年に発表されて以来、公開鍵暗号を使用した暗号化ソフトウェアとして、世界中で広く使われています。また、PGP Command Lineは、ソースコードが公開されており、長年にわたって多くの技術者に「揉まれてきた」ソフトウェアなので、安全性・安定性があり、銀行業務に採用する暗号化エンジンとして信頼できます。「Web21」のお客さまでもPGP Command Lineを既に導入している会社があり、その事実も採用の後押しとなりました。



PGP® Command Line——ビジネスプロセスに暗号化エンジンを組み込んで重要情報を保護

製品概要

大量の情報を安全にやり取りする必要がある企業は、PGP Command Lineを導入することにより、既存のシステムへの影響を最小限に抑えつつ、自動的に重要情報の改ざんを防止し保護することができます。また、不正なアクセスから守ることができます。

豊富な実績を持つ暗号技術

PGP Command Lineは、自動化したビジネスプロセスで扱われる重要情報を保護し、法規制に対するコンプライアンス、プライバシーの保護、機密性の保持を助けます。また、情報の保護だけでなく、監査証跡のための電子署名もサポートします。

新規および既存のビジネスプロセスへ柔軟に統合

PGP Command Lineは、ほとんどすべてのビジネスプロセスへ統合できます。既存のビジネスアプリケーションへの影響を最小限に抑えつつ、セキュリティを追加できるため、そのアプリケーションのライフサイクルを伸ばすことができます。

PGP Encryption Platformに対応

PGP Command Lineは、ユーザ管理、ポリシー、プロビジョニングのための戦略的な暗号化フレームワークであるPGP Encryption Platformに対応することで、複数の暗号化アプリケーションを統合し、自動的な運用を実現します。導入およびシステムの管理を迅速に進めることができるほか、多層のセキュリティを提供します。

【使用例】 スクリプトに下記のコマンドを追加することにより、自動で暗号化できるプログラムです。

```
pgp --encrypt payment.csv --recipient "Corporate Key"
scp payment.csv.pgp archiveuser@192.168.0.100:~/
<current date>/ payment.csv
pgp --wipe payment.csv --wipe-passes 6
```

・ [payment.csv] を "Corporate Key" 鍵で暗号化して別ストレージに転送。
・ サーバに残った payment.csv ファイルは完全抹消する。

動作環境

対応するプラットフォーム

- ・ Windows 7 (32/64 ビット)
- ・ Windows Server 2008
- ・ Windows Vista SP2 (32/64 ビット)
- ・ Windows Server 2003 SP2 (32/64 ビット)
- ・ Windows XP SP3 (32/64 ビット)
- ・ HP-UX 11i 以降 (PA-RISC/Itanium)
- ・ IBM AIX 5.3/6.1
- ・ Red Hat Enterprise Linux 5.0 以降 (x86/x86_64)
- ・ SLES (SUSE Linux Enterprise Server) 9 SP4/10 SP2 (x86のみ)
- ・ Fedora Core 6 (x86_64のみ)
- ・ Sun Solaris 9 (SPARCのみ)/10 (SPARC x86/x86_64)
- ・ Apple Mac OS X 10.5.x/10.6.x (Intel のみ)

公開鍵形式

- ・ OpenPGP (RFC 4880)
- ・ X.509 v3

ディレクトリ サーバー

- ・ LDAP
- ・ PGP Universal Server
- ・ PGP Global Directory

共通鍵暗号アルゴリズム

- ・ AES (最大256 ビット) / CAST5 / TripleDES / IDEA / Twofish / Blowfish* / Arc4 (128 ビット)

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) / DSA (1024 ビットのみ、最大3072 ビットまで検証可能) / RSA (最大4096 ビット)

圧縮アルゴリズム

- ・ Zip / BZip2 / ZLib

* 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。

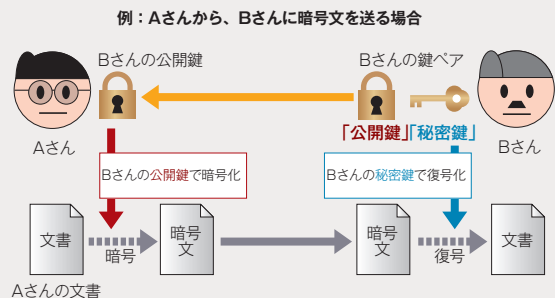
参考資料

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。

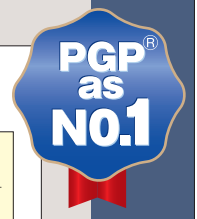
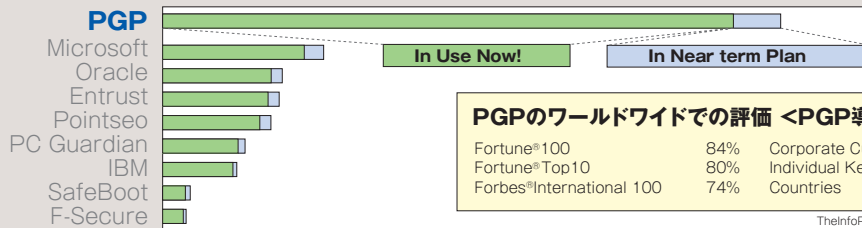
公開鍵… データの暗号化のみを行います。公開鍵で暗号化されたデータは対となる秘密鍵でしか復号化することはできません。

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。

PGPを利用して暗号化通信を行うのにお互いの公開鍵を交換し合うことが必要ですが、公開鍵自体は暗号化専用の鍵なので不特定多数に配布しても問題ありません。このように、公開鍵暗号方式のメリットは自分の秘密鍵(復号化用)さえ厳重に保管していれば良く、(危険性の無い)公開鍵をインターネット等を通じて第三者に容易に配布できることが挙げられます。また秘密鍵自体も暗号化されており、これを利用する(秘密鍵を復号化する)には秘密鍵に設定されたパスフレーズを知らなければ、秘密鍵ファイルだけを持っていたとしても使用することはできません。



PGPが米国のマーケットリサーチで暗号分野でナンバーワンリーダーに!



販売代理店

<東京>
〒163-0777 東京都新宿区西新宿2-7-1 小田急第一生命ビル
TEL:03-3342-1411 FAX:03-3342-0453

<大阪>
〒530-0003 大阪府大阪市北区堂島1-6-20 堂島アバンザ
TEL:06-6442-1314 FAX:06-6442-1316

<名古屋>
〒450-6213 愛知県名古屋市中村区名駅4-7-1 ミッドランドスクエア
TEL:052-563-0232 FAX:052-563-0233
Email: pgp@nsd.co.jp WEB: http://www.nsd.co.jp/pgp/

製品開発元: Symantec Corporation
※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。