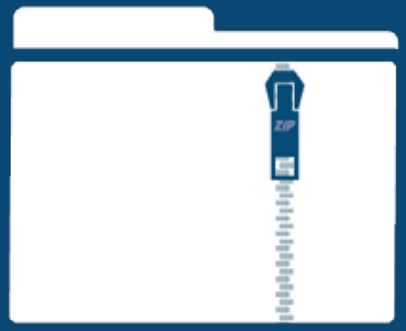
PCI DSS コンプラインスの達成とデータ セキュリティ ブリーチのリスクを軽減

エクセルソフト株式会社
営業部 PKWARE 製品担当
田淵 義人
2013/7



PKWARE
.ZIP ファイル形式の発案者

PKWARE 会社概要

名称	PKWARE, Inc.
設立	1986年
事業内容	• ZIP 形式の発案者として、PKZIP の開発･販売。 ZIP 標準の拡張を図り、データ圧縮の技術を革新。今日では、世界中でZIP ファイルが生成され、さまざまな場所で保管され、データ交換に使用されています。 • PKZIP にセキュリティ機能を強化した SecureZIP の開発･販売。 • SecureZIP によるデータ セキュリティ ソリューションの提供
販売製品	SecureZIP、PKZIP
導入実績	全世界で 30,000 社以上 (日本では 600 社以上) で採用 Fortune 100 の 90% の企業で採用 世界上位 25 の銀行のうち 23 行で採用 200 以上の連邦政府機関で採用

エクセルソフト会社概要

名称	エクセルソフト株式会社
設立	平成３年７月１日
所在地	東京都港区三田3-9-9
資本金	１０００万円
事業内容	ソフトウェアの開発･販売事業
主要取引先	伊藤忠テクノソリューションズ、インテル、HPCシステムズ、NTTデータ、シネックスインフォテック、ソニー、ソフトバンクBB、ダイワボウ情報システム、東芝、日本アイ･ビー･エム、日本SGI 、日本電気、日本ヒューレット･パッカード、ネットワールド、ビジュアルテクノロジー、日立製作所、日立電子サービス、富士通、マイクロソフト、松下電器産業、理経　等
関連会社	XLsoft Corporation アメリカ カリフォルニア州

「開発ツールはエクセルソフトで」をモットーに。

販売/サポートだけでなく、運用もお客様と一緒に考えます。

PCI DSS: 目的

“PCI DSS は堅牢なクレジットカード情報保護の処理を開発するための実用的なフレームワークを提供します – セキュリティの問題に対する予防、検知、および適切な対応など”

-PCI SECURITY STANDARDS COUNCIL

PCI は以下のコンプラインスに準拠して策定されています

American Express Data Security Operating Policy (DSOP)
Discover Information Security and Compliance (DISC)
MasterCard Site Data Protection (SDP) Security Certification
Visa Account Information Security (AIS)
Visa Cardholder Information Security Program (CISP)

PCI DSS コンプライアンス

6 のカテゴリの 12 の要件

- セキュアなネットワークの構築と維持
- 脆弱性の管理
- アクセス コントロールの実装
- ネットワークの監視とテスト
- 情報セキュリティ ポリシーの維持
- カード所有者データの保護

ガイドラインの可視化

PCI DSS コンプライアンス

カード所有者データの保護

- セクション 3 - 保存したカード所有者データを保護
- セクション 4 - オープンなパブリック ネットワーク間でのカード所有者データの転送を暗号化
- セクション 7 - カード所有者データへのアクセスをビジネス上知るべき範囲内に制限
- セクション 12 - 従業員および請負業者を含むすべての担当者に対して、情報セキュリティ対策のポリシーを維持

ガイドラインの可視化

- セクション 3.7 - 休止、使用していない VM を特定および監視して、適切なセキュリティ コントロールを適用

PCI の要件…

カード所有者情報および/またはトランザクション情報を処理、格納、または転送する事業者はその要件に準拠する必要があります。

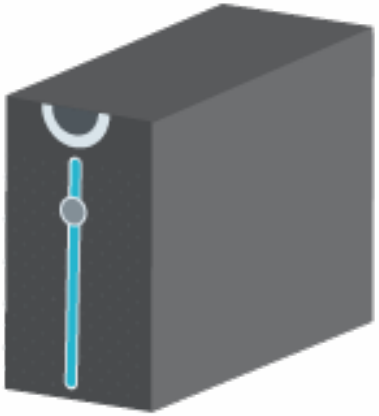
すべてのメンバー機関、加盟店、販売店、およびサービスプロバイダーが含まれます。

PCI の適用対象システム

システム
コンポーネント

ネットワーク
コンポーネント

サーバー



アプリケーション

PCI DSS コンプライアンス

多くの企業では、PCI の要件のほとんどに準拠するインフラを持っています

- ファイアウォール
- アクセス コントロール
- 監査ログ
- 攻撃の検知/予防

対応が遅れている対策が一つあります…カード所有者データの保護

非準拠のコスト

PCI に準拠できず、販売店サイト内のカード データのブリーチによって、莫大な罰金 (最大 $100,000 / 月)、ペナルティ、カード決済へのアクセスの禁止などが発生します。

ブリーチのコスト

Source: Lockton Companies.
2012 Cyber Risks Decoded Report

間接的なコスト

- ID の復旧
- 案内
- ID の監視
- 捜査
- 発見
- コール センター

直接的なコスト

- 訴訟
- 資金の損失
- 法的な罰金
- 賠償

米国でのブリーチのコスト:
$7.2 Million $214 per record

“組織は、データそのものをセキュアにすることをより一層重要視する必要があり、インフラを保護の第2のレイヤとして使用する必要があります。”

- PAUL STAMP, FORMER ANALYST, FORRESTER RESEARCH

データセントリック セキュリティと PCI

データセントリックのセキュリティへのアプローチは PCI の要件に対応

- 確認したデータや転送時のデータを保護
- 組織のセキュリティ ポリシーを強制
- 休止中の仮想マシンの保護

PCI のデータ セキュリティの利点

ポリシーの強制

- 組織全体で暗号化や認証に使用するポリシーを作成および強制

導入がスムーズ

- データセントリック セキュリティは既存のセキュリティの資産を補完

“ユーザー プルーフ”

- 組織内のユーザーが暗号化したファイルへの管理者アクセス

データセントリックのアプローチのビジネス上の利点

スケーラビリティ

- クロスプラットフォーム: プラットフォーム間を移動するデータを保護
- セキュリティや IT インフラの既存の資産を相互運用的に活用
- 使いやすく、展開しやすい

互換性

- 標準ベースでレガシー ファイル フォーマットを開くことが可能

データを暗号化する理由?

セキュリティ ブリーチのリスクを排除

- 企業ブランドや企業価値を保護

金銭的なペナルティを回避

Visa は準拠していない大規模な小売店に対して月 $10,000 から $100,000 の罰金を科します。

- CREDITCARDS.COM

事例 – グローバル小売店

顧客プロファイル

- 世界最大規模のデパートメント ストア
- 米国で 850 店以上

ビジネス ゴール

- PCI DSS とセキュリティ対策を実施
  - メインフレームで暗号化した機密データをセキュアに複数のハードウェアのプラットフォームに移動して復号化する
  - データをリムーバル メディアに転送または保存した際に情報を保護する

チャレンジ

- 社内外でのデータ交換に活用できるデータ暗号化ソリューションを探す
- PCI に準拠

ケース スタディ – グローバル小売店

PKWARE ソリューション: SecureZIP PartnerLink

顧客の利点:

- ビジネス パートナーとセキュアに情報交換が可能
- 操作効率が改善し、データをそのままディスクに保存するステージをなくし、データが常に保護された状態を確保

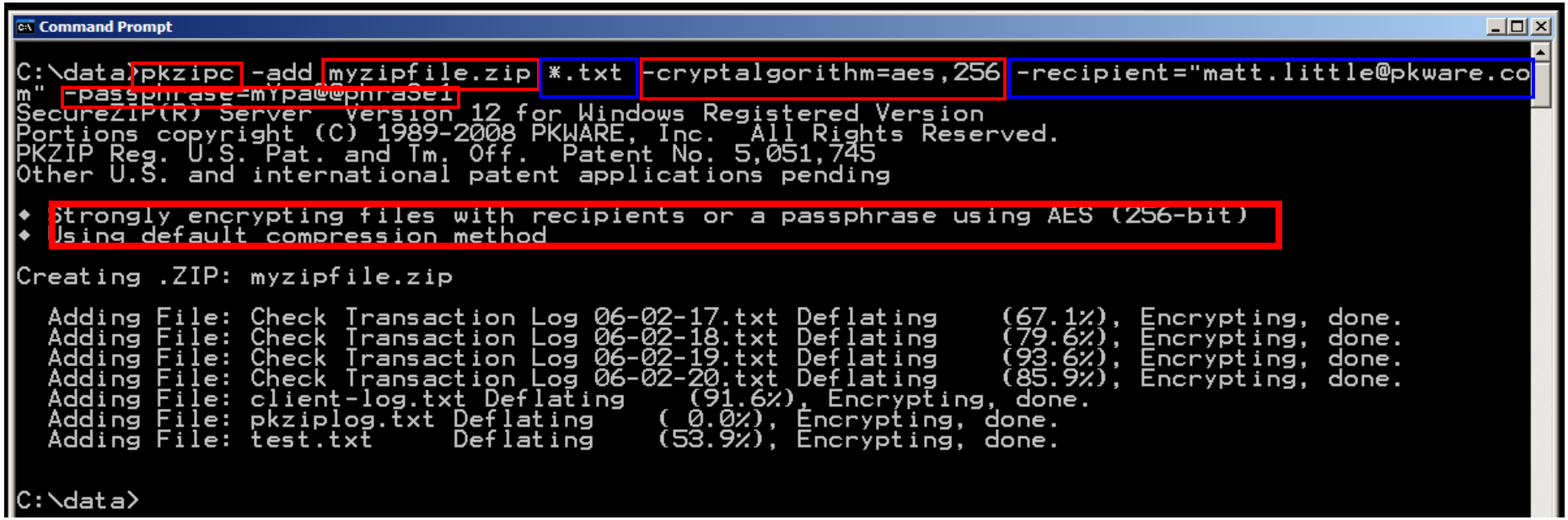
結果

- PCI コンプライアンスの達成
- 処理時間を最大 600% 短縮
- メインフレーム環境とターゲットの環境間で通信時間を 75% まで短縮

ポイントソリューション としての SecureZIP

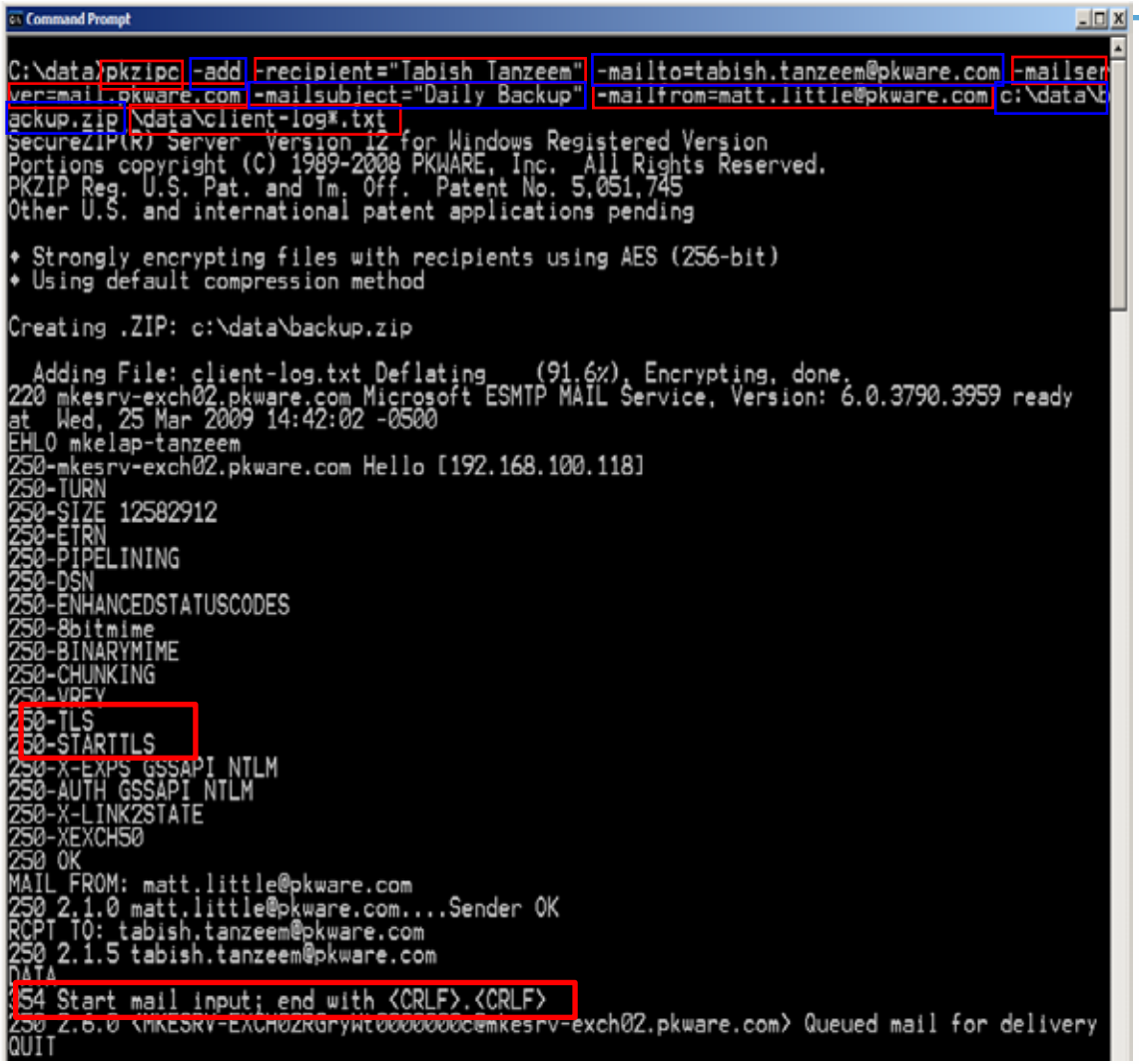
デモ

パスワードとデジタル証明書での暗号化



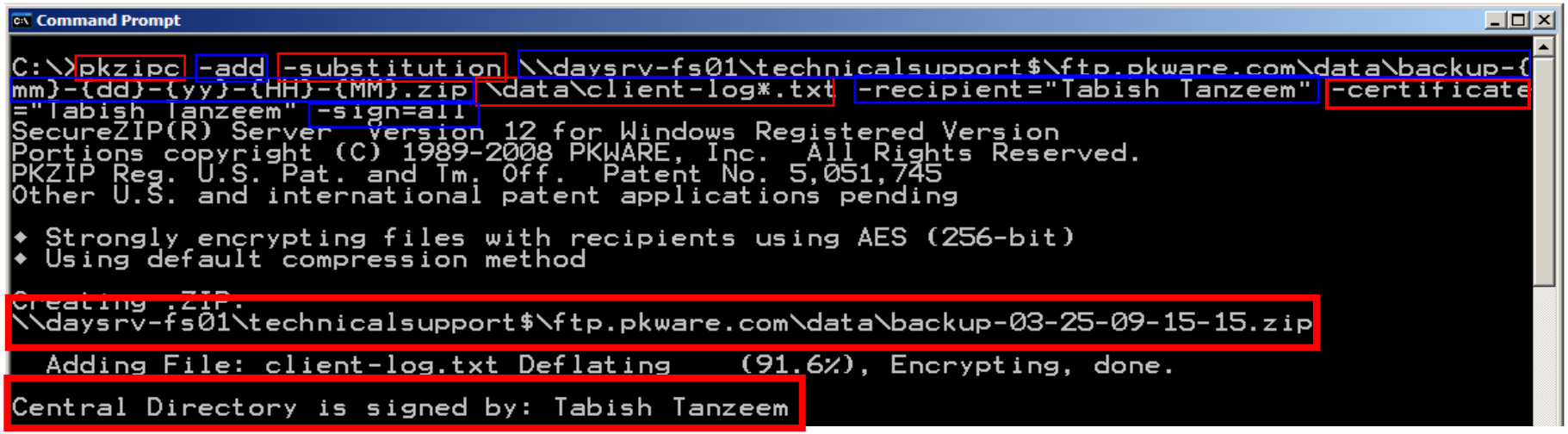
pkzipc	SecureZIP 呼び出しと初期化
-add	新規アーカイブ作成コマンド (必須パラメーター)
myzipfile.zip	新規 zip ファイル名 (必須パラメーター)
*.txt	アーカイブに追加するファイル名 (必須パラメーター)
-cryptalgorithm= aes,256	データの暗号化を行う際の暗号化アルゴリズムを定義。この例では、AES 256bit 暗号化アルゴリズムを使用。(デフォルトの動作として設定することができるオプションパラメーター)
-recipient = “matt.little @pkware.com”	データの暗号化を行う際の対象の方の公開鍵を使用するための Email アドレスを定義するフラグ。(暗号化をする際は -recipient か -passphrase が必須)
-passphrase	データの暗号化を行う際のパスワードを定義するフラグ。パスワードが設定ファイルで定義されている場合、SecureZIP は標準のパスワードを使用する。(暗号化をする際は -recipient か -passphrase が必須)

ZIP/暗号化/メールを 1ステップで



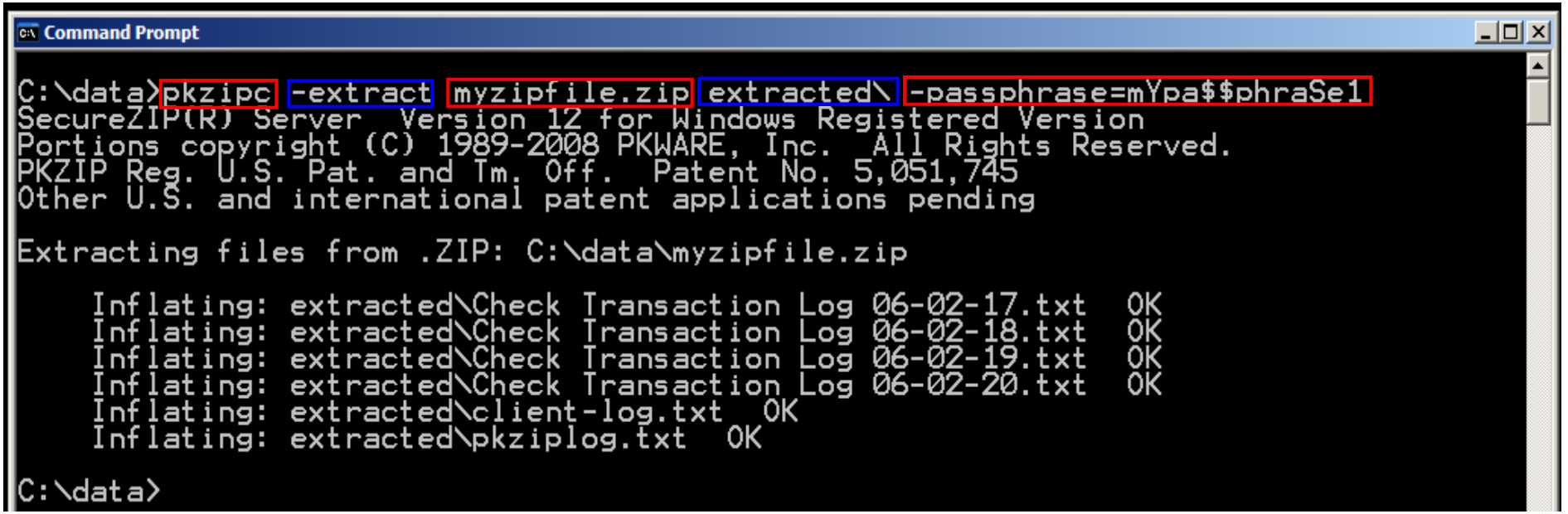
pkzipc	SecureZIP 呼び出しと初期化
-add	新規アーカイブ作成コマンド (必須パラメーター)
-recipient	暗号ファイル受信者の共通鍵の common name を定義するフラグ。(データ暗号化を行う場合は必須オプション)
-mailto	受信者の email アドレスを指定。複数の受信者がいる場合は、本オプションを複数使用する。
-mailserver	SMTP サーバーの IP アドレスを指定。
-mailsubject	email メッセージヘッダーのタイトルのテキストを指定。
-mailfrom	メッセージ送信者の email アドレスを指定。このアドレスは SMTP サーバーから許可されたものでなければいけない。
C:¥data¥backup.zip	新規 zip ファイル名 (必須パラメーター)
¥data¥client-log*.txt	アーカイブに追加するファイル名 (必須パラメーター)

デジタル署名された ZIP ファイルを作成



pkzipc	SecureZIP 呼び出しと初期化
-add	新規アーカイブ作成コマンド (必須パラメーター)
-substitution	新規 zip ファイルに変数トークンを指定するオプションのフラグ。様々な指定方法が可能。
¥¥daysrv-fs01¥technicalsupport$¥ftp.pkware.com¥data¥backup-{mm}-{dd}-{yy}-{HH}-{MM}.zip	新規 zip ファイル名 (必須パラメーター) この例では同じネットワークの別のサーバーの UNC パスを使用。substitution のトークンも ZIP ファイル名に使用しています。
¥data¥client-log*.txt	アーカイブに追加するファイル名 (必須パラメーター)
-recipient = “Tabish Tanzeem”	暗号ファイル受信者の共通鍵名を定義するフラグ。 (データ暗号化を行う場合は必須パラメーター)
-certificate = Tabish Tanzeem	提供されたデジタル証明書でアーカイブに署名する際に定義するフラグ。
-sign=all	データに署名するフラグ (署名する場合は必須パラメーター)

暗号化された zip ファイルを復号



pkzipc	SecureZIP 呼び出しと初期化
-extract	アーカイブ解凍コマンド (必須パラメーター)
myzipfile.zip	ZIPファイル名 (必須パラメーター)
extracted¥	解凍するファイルを配置するパス。ネットワークドライブ、ローカルドライブを指定可能。
-passphrase	データの解凍を行う際のパスワードを定義するフラグ。パスワードが設定ファイルで定義されている場合、SecureZIP は標準のパスワードを使用する。(暗号化をする際は -recipient か -passphrase が必須)

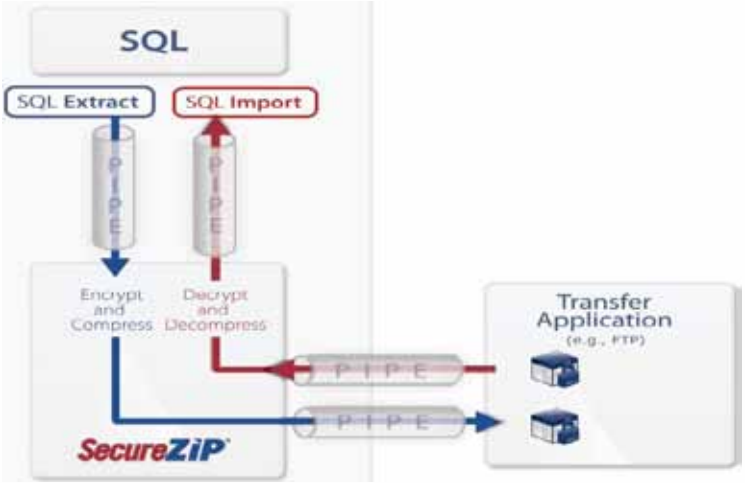
NOTE: If the ZIP file was encrypted using the certificate based encryption; SecureZIP will automatically look in to the certificate store to find the matching private key to decrypt the data

SecureZIP で FIFO パイプを使用する

SecureZIP Server は、FIFO パイプを使用して、OS の内部処理コミュニケーション機能を使用して、ファイルの読み書きができます。

FIFO パイプは、データの保存や転送の処理をスムーズに行い、またよりセキュアに処理します。

これによって、SecureZIP は、データを移動する際に、暗号化していないデータをディスクに書き込むことなく、アプリケーション間で直接 ZIP フォーマットでやりとりができます。



パイプの例 - STDIN/STDOUT を活用

以下は SecureZIP が処理を受け取る使用例:

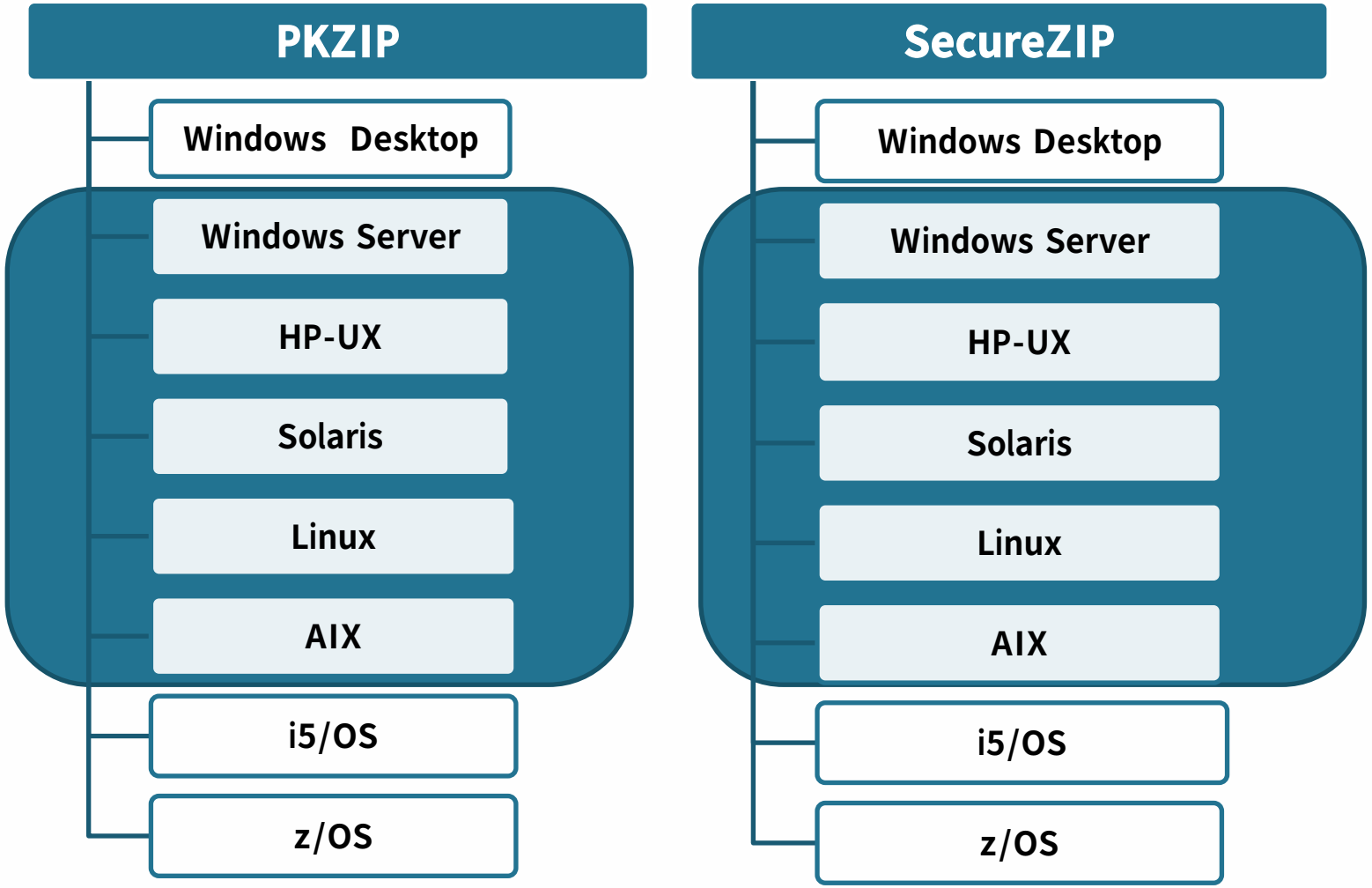
```
<SQLQuery application> | pkzipc –add
Report.zip –passphrase="Mypassphrase"
```

以下は SecureZIP が処理を投げる使用例:

```
pkzipc –console –silent=all –
passphrase="Mypassphrase" ImportData.zip |
<SQLImport Application>
```

ライセンスについて

PKWARE 製品ポートフォリオ



サーバーシステム要件

Windows Server 2003-2008 (drop 2000)

Linux: Ubuntu 10.4 (LTS)

SUSE 9-11, RHEL 4-6

AIX 5.3-7.1 (drop 5.2)

Microsoft Server

HPUX 11iv1-v3

Solaris Sparc 8-11

Solaris x86

redhat

IBM

hp

ORACLE

XLSOFT PKWARE

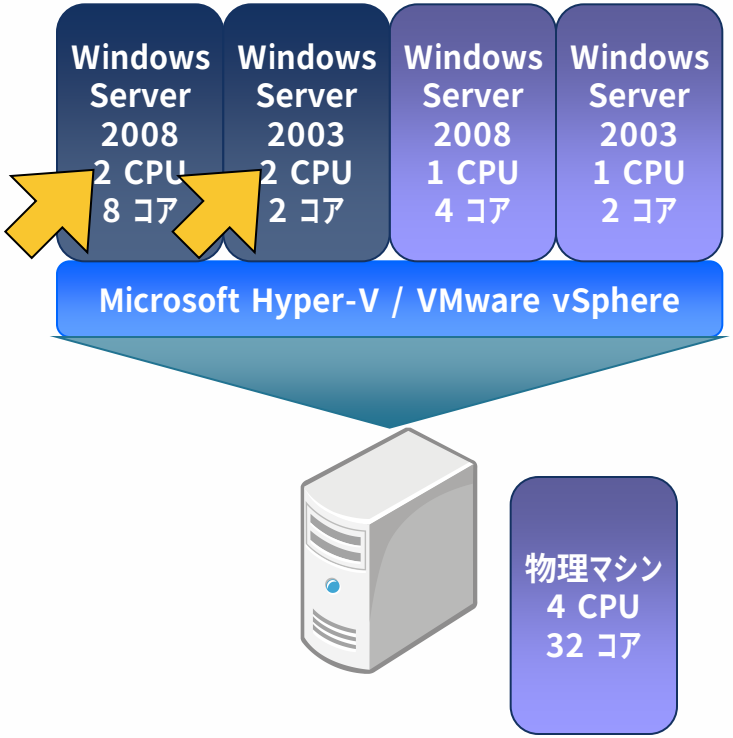
SecureZIP/PKZIP for Windows Server

SecureZIP/PKZIP for Windows Server は「インスタンスライセンス」です。

- ソフトウェアをインストールする各物理 OS および仮想 OS (インスタンス) に対して、1ライセンスが必要です。
- ライセンス単価はご購入時の合計ライセンス数で決まります。
- 保守はライセンス価格の 20% で、購入は任意ですが途中での加入および数量を変更しての更新はできません。

SecureZIP/PKZIP for Windows Server のライセンス算出方法

例：



物理サーバーにインストールされた Microsoft Hyper-V, VMware Server, VMware vSphere (ESX) などの仮想環境にインストールされた Windows Server 2008/2003 の 2台に SecureZIP/PKZIP がインストールされている場合

2インスタンスライセンスが必要です。

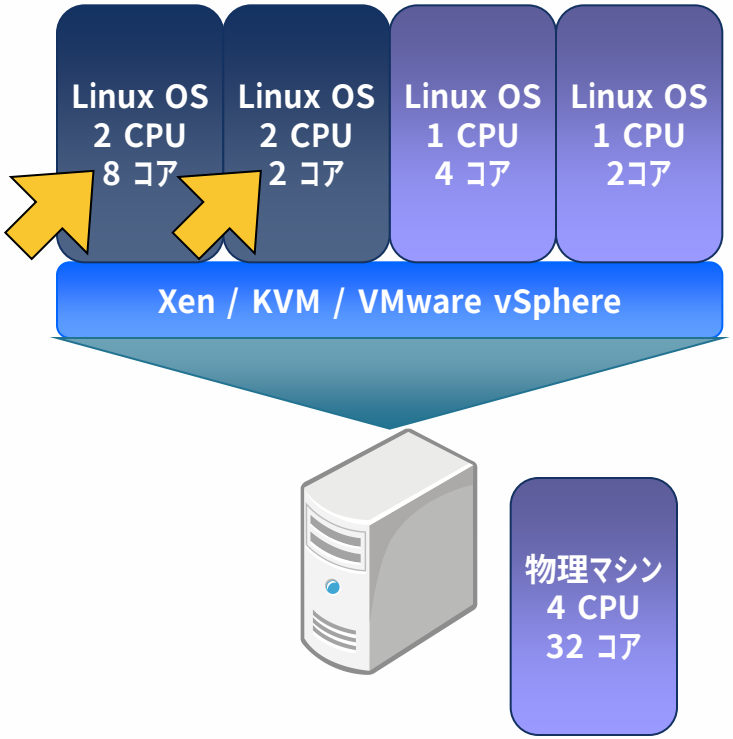
SecureZIP/PKZIP for Linux Server

SecureZIP/PKZIP for Linux Server は「CPU ライセンス」です。

- ソフトウェアをインストールする各物理/仮想マシンの CPU 2コアに対して、1ライセンスが必要です。4コアのマシンは 2 ライセンス必要です。
- ライセンス単価はご購入時の合計ライセンス数で決まります。
- 保守はライセンス価格の 20% で、購入は任意ですが途中での加入および数量を変更しての更新はできません。

SecureZIP/PKZIP for Linux Server のライセンス算出方法

例：



物理サーバーにインストールされた Xen, KVM, VMware Server, VMware vSphere などの仮想環境にインストールされた Linux 2台（2 CPU 8コアと 2 CPU 2 コア）に SecureZIP/PKZIP がインストールされている場合

4 CPU ライセンス＋2 CPU ライセンスの計 6 CPU ライセンスが必要です

- 仮想の場合も 1 CPU ライセンスで 2 コアまで
- 1 コアの CPU が 2 つの場合は、CPU が優先される

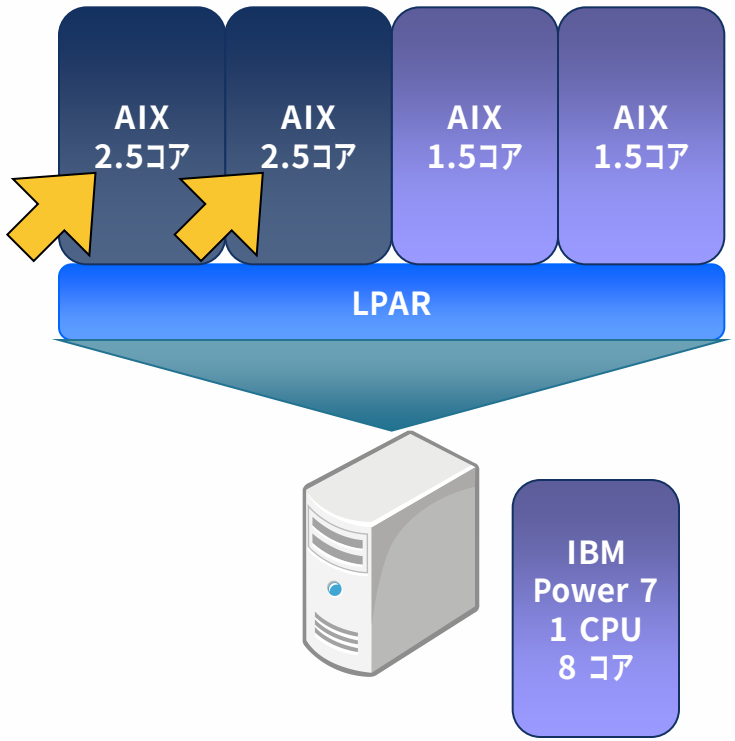
SecureZIP/PKZIP for UNIX Server

SecureZIP/PKZIP for UNIX Server は「CPU ライセンス」です

- ソフトウェアをインストールする各物理マシンの CPU 2コアに対して、1 ライセンスが必要です。4コアのマシンは 2ライセンス必要です。
- IBM LPAR / HP vPar など、論理パーティションによる仮想環境の場合、各区画の仮想環境 OS 毎に CPU 数分のライセンスが必要となります。
  - 小数点以下の CPU 数は、切り上げします。例えば、1 物理 CPU を 0.5コア、0.2コア、0.3コア と割り当て、各 AIX に SecureZIP/PKZIP Server をインストールする場合、それぞれ 1 ライセンスが必要で、合計 3 ライセンスが必要となります。
- ライセンス単価はご購入時の合計ライセンス数で決まります。
- 保守はライセンス価格の 20% で、購入は任意ですが途中での加入および数量を変更しての更新はできません。

SecureZIP/PKZIP for UNIX Server のライセンス算出方法

例：



IBM LPAR 上にインストールされた AIX 2台（2区画）に SecureZIP/PKZIP がインストールされている場合

4 CPUライセンスが必要です

- 1CPU ライセンスで 2コアまですが 2.5 の場合は切り上げで 3コア扱いのため、2CPU ライセンスが必要です。

質問