Reflection for Secure IT のご紹介

2011年 7月26日

NetIQ 株式会社 Attachmate事業部

Attachmate

1. 会社紹介

The Attachmate Group, Inc.

Attachmate	NetIQ	Novell	SUSE
Terminal Emulation	Identity, Security and Compliance Management	Collaboration	Enterprise Linux Servers
Legacy Modernization	Systems Management	File and Networking Services	Software Appliances
Managed File Transfer	Resource Management	Endpoint Management	Linux Desktops
Enterprise Fraud Management			

ネットアイキュー(株)　　ノベル(株)

Attachmate

2. Reflection for Secure IT の概要

Reflection for Secure IT（RSIT） は、

Attachmate 社 が開発/ 販売/ サポート する

商用版 SSH（Secure SHell）製品です。

【製品】

- UNIX/Linux, Windows 環境に 統一製品仕様を提供
- 高品質、高信頼
  （＝10年の国内稼働実績/200社以上の国内顧客基盤）
- 安全な暗号ライブラリを使用
  - FIPS 140-2 取得、
  - “暗号2010年問題”対応
- 相互接続性
  - IETF SecSH 標準規格準拠
  - OpenSSH scp1(非標準)接続、公開鍵(非標準)変換

【サポート】

- お問合せサポート窓口
- ドキュメント, ナレッジ(FAQ)の提供
- 専用サイトからの最新版の提供(保守ユーザ様)

【お勧めポイント】

- セキュアな導入/運用支援
- TCOの削減

Attachmate

3. 要件4への対応

PCI Security Standards Council

要件 4:　　オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する

ネットワークには悪意のある人々が容易にアクセスできるため、機密情報をネットワーク経由で伝送する場合は暗号化する必要があります。誤って構成されたワイヤレスネットワーク、および従来の暗号化や認証プロトコルの脆弱性は、こうした脆弱性につけこんでカード会員データ環境への特権アクセスを取得する、悪意のある人々の標的となります。

PCI DSS 要件	テスト手順
4.1 オープンな公共ネットワーク経由で機密性の高いカード会員データを伝送する場合、強力な暗号化とセキュリティプロトコル（SSL/TLS、IPSEC、SSH など）を使用して保護する。 *PCI DSS の範囲内であるオープンな公共ネットワークの例として以下が挙げられる。* ▪ インターネット ▪ ワイヤレステクノロジ ▪ Global System for Mobile Communications （GSM） ▪ General Packet Radio Service （GPRS）	**4.1** カード会員データがオープンな公共ネットワーク経由で送受信される場合、セキュリティプロトコルが使用されていることを確認する。 以下のように、データ伝送時に強力な暗号化が使用されていることを確認する。
	4.1.a 受信時のトランザクションのサンプルを選択してトランザクションを監視し、カード会員データが送信時に暗号化されていることを確認する。
	4.1.b 信頼できるキーまたは証明書（あるいはその両方）のみが受け付けられていることを確認する。
	4.1.c プロトコルの安全な構成のみが使用され、安全でないバージョンまたは構成がサポートされないことを確認する。
	4.1.d 使用中の暗号化手法に、適切な強度の暗号化が実装されていることを確認する （ベンダの推奨事項/ベストプラクティスを確認する）。

【 RSITによる対応 】

- ・SSH による保護
- ・鍵ペアの作成/登録と運用
- ・外部認証局(CA)との連携
- ・FIPS 140-2 取得ライブラリ使用
- ・FIPSモード運用指定
- ・SSHサーバ設定による運用
  - -”暗号2010年問題”対応
  - -脆弱アルゴリズムの除外

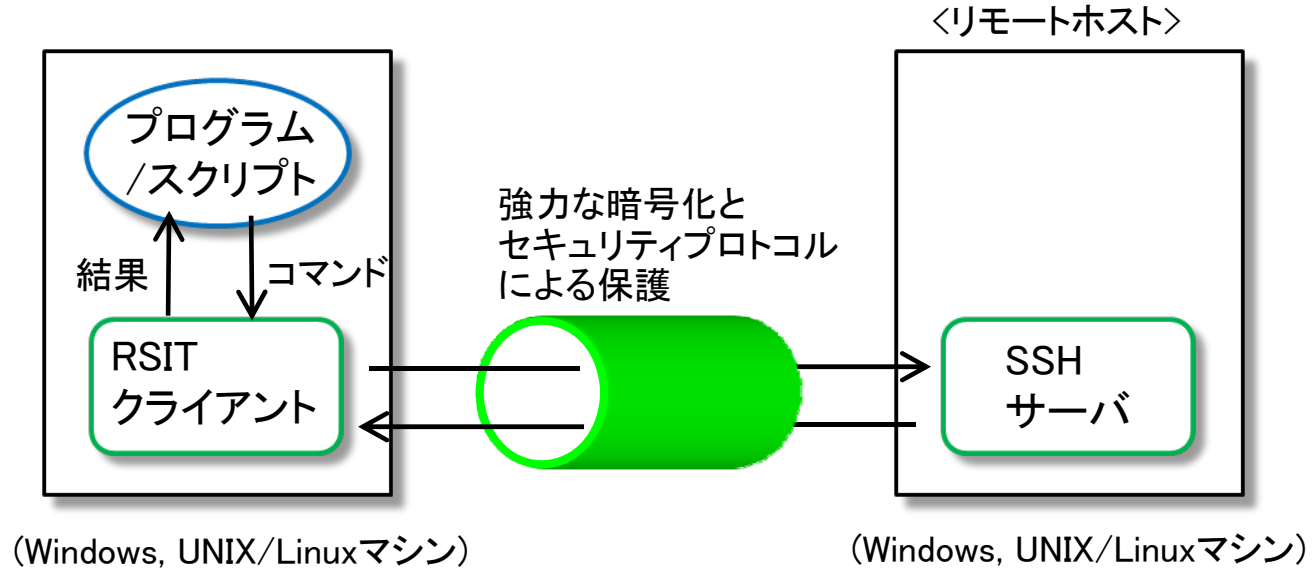
Attachmate

4. RSIT との連携補完による要件への対応

・他アプリケーションと連携し、組込み部品的に要件4の補完製品として対応可
　～プログラム/スクリプトからの自動実行（コマンド発行とリターンコード自動判定）

【対象となる機能 例】

a) ファイル転送 と リモートファイル操作
b) リモートコマンド実行
c) アプリケーション通信の暗号化トンネリング

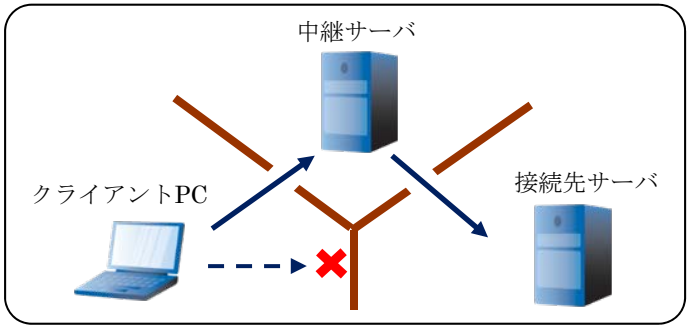


Attachmate

5. RSIT の特徴的な機能　1/2

1. マルチホップ接続

～クライアントから直接接続できない遠隔の接続先サーバへ中継サーバを経由しSSH多段接続

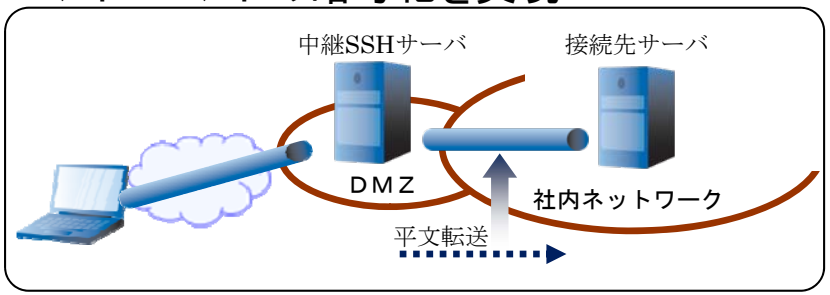


【実現仕様/特徴】

a) 経路指定はクライアント設定による
b) 中継サーバはSSHサーバ ポート転送機能で対応
c) 複数台の中継サーバ経由も可
d) ユーザ認証はクライアントと各サーバ間で実施

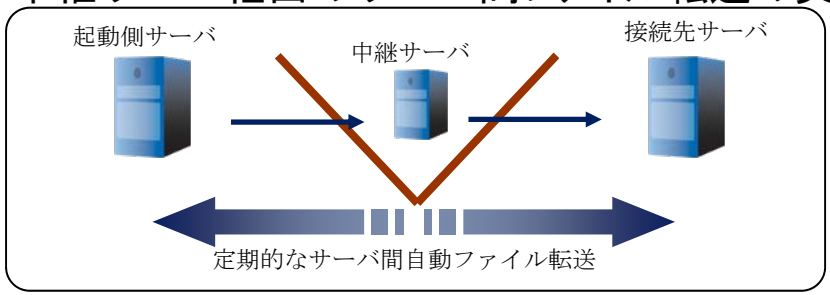
【事例1】

・エンドtoエンドの暗号化を実現



【事例2】

・中継サーバ経由のサーバ間ファイル転送の実現



2. 通信帯域/時間のムダを削減するファイル転送

1) Resume 機能 ～ 転送途中に切断しリトライ後、中断点の分割パケットから再開
　・転送成功部分を再送するムダを削減。大容量ファイルの制限時間内転送に効果的。

2) Skip 機能 ～転送先に同一ファイル存在時、転送処理を省略しタイムスタンプのみ更新
　・サーバ/クライアント間で連携し、ハッシュ関数で同一判定。

Attachmate

5. RSIT の特徴的な機能　2/2

3. サーバ保護重視の設定 ～ ユーザへは必要最低限の権限のみ付与

1) 提供機能の制限

①リモートログイン、②リモートコマンド、③ファイル転送、④トンネリング

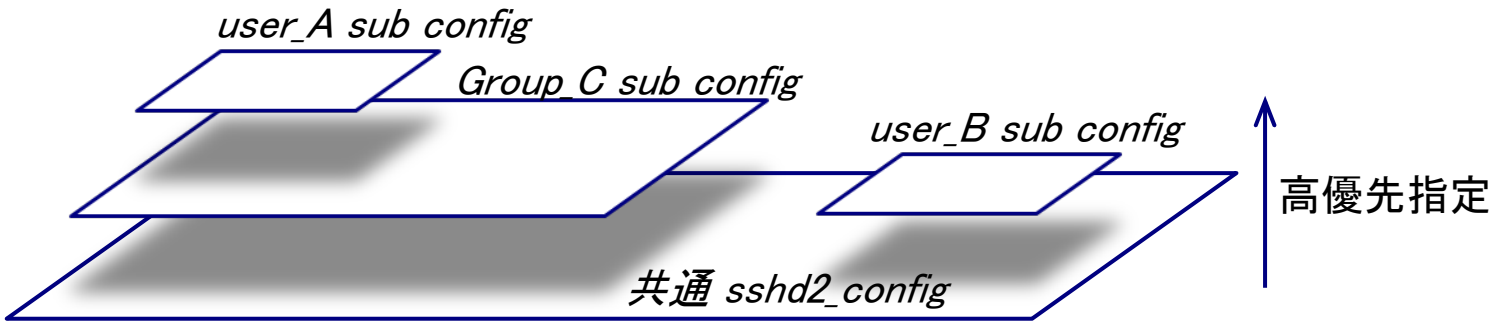
2) アクセス権限の制限

a) ファイル転送アクセス範囲

b) sftp コマンド制限：

{Browse/Download/Upload/Delete/Rename} 選択指定

3) ユーザ/グループ/クライアント端末　単位の個別設定



4. 重要ファイル(=秘密鍵) 隠ぺい による流出リスクの低減

・クライアント秘密鍵〔公開鍵認証/証明書認証用〕の保存先とファイル名を変更(*)

(*) config 設定 又は コマンドオプションにより指定

Attachmate

6. 事例紹介

機能	代表的な 用途 と 事例
ファイル転送 と リモートファイル操作 （sftp, scp）	・サーバ間のファイル転送、ファイルの同期化 ・ファイル（バックアップ, ログ情報）の自動収集
	《事例》・A銀行/構築システム標準採用、・B銀行/ネット決済インフラ採用 ・C社 /地銀向けアウトソースサービス ・ISP D社 /コンテンツ作成業者からのコンテンツアップロード用 ・旅行業 E社 /Webサービスインフラ ・製造業 F社 /国内外取引先との受発注情報の送受 ・海外小売業G社 /全店舗・配送センタ・オフィスに導入
リモートコマンド	・リモートホスト上の処理起動
	《事例》 ・H社 /電子マネーインフラサーバ機 正常稼動確認
アプリ通信の 暗号化トンネリング	・社内ネットワーク アプリケーションサーバへの社外からのVPNアクセス 〔メールサーバ、ファイルサーバ、Webサーバ 等〕
	《事例》 ・I社 /イントラ内メールサーバへのVPNアクセス
リモートログイン	・人手操作によるサーバの遠隔保守 ・社内サーバアクセス厳格運用（パスワード盗聴防止 等）
	《事例》 ・J社, K社 /データセンタに採用

Attachmate