

Reflection for Secure IT Windows サーバは、SSH 通信を使い易く高機能化した、Windows 環境で動作するセキュリティ製品です。転送データの暗号化と完全性保証、サーバ/ユーザ相互認証、更にはロギング機能等により、お客様データの安全な転送、重要なサーバのリモート管理、企業内アプリケーションへのセキュアなアクセスを実現します。そして、盗聴/改ざん/なりすましなどの不正行為による脅威から、企業の重要な情報とサーバ/ネットワーク環境を保護します。近年、業界等でセキュリティ諸規制順守が求められていますが、データ通信の観点からその要件を満たす信頼ある製品に仕上がっています。

### バージョン 7.2 の特長

- Microsoft Windows Server 2008 R2 (x86-64) に対応。
- Microsoft Cluster Service に対応。
- リモート端末接続により定義ネットワークドライブへアクセス可。
- 1ユーザ当たりの同時接続数上限値を指定可。
- ネットワーク上に定義したSFTP ディレクトリ およびネットワークドライブに対しアクセスユーザの認証情報を指定可。
- サーバ構成ファイルの保存場所を指定可。
- ドメインユーザ名の認証時間を改善。

## 主な機能と仕様

### 安全なリモートアクセス

- リモート端末接続:
  - コマンドラインシェル (cmd.exe など) を指定可
  - デフォルトのログオンディレクトリを指定可
- NEW** - リモート端末接続中に定義済みネットワークドライブ下のディレクトリにアクセス可
- リモートコマンド実行

### 安全なファイル転送

- SCP および SFTP
- 特長的な機能:
  - Smart Copy (同一ファイルの重複転送処理を回避)
  - 中断点再開機能
- SCP1 に対応 (OpenSSH との相互接続性)
- 仮想ディレクトリおよび chroot 環境に対応

### アクセス制御

- 稼働サービスの指定:
  - リモート端末接続
  - リモートコマンド実行
  - ローカルポート転送
  - リモートポート転送
  - SCP1 アクセス
  - SFTP/SCP2 アクセス
  - SFTP 操作 (参照、ダウンロード、アップロード、削除、名前の変更)
- 構成設定の指定単位 (サブコンフィグによる個別指定):
  - 共通指定
  - グループ個別指定
  - ユーザ個別指定
  - クライアント個別指定 (IP アドレスまたはドメイン名)
- Windows の対話型アクセス権がないユーザの接続を拒否

- NEW** - 1ユーザ当たりの同時接続上限値を指定可
- NEW** - ネットワーク上に定義したSFTP ディレクトリ およびネットワークドライブに対しアクセスユーザの認証情報を指定可

### トンネリング

- TCP ポート転送 (ローカルおよびリモート)
- FTP プロトコル (アクティブモードおよびパッシブモード)
- RDP プロトコル

### 標準規格

- IETF SecSH インターネット標準規格準拠 (RFC 4250 ~ 4254, 4256, 4462, 4344, 4345, 4716)

### 暗号ライブラリ

- 米国標準技術局(NIST)暗号モジュール認定基準 FIPS 140-2 レベル 1 取得 (証明書番号 1027)

### 暗号アルゴリズム

- 共通鍵暗号アルゴリズム:
  - AES (128, 192, および 256 ビット CTR)
  - AES (128, 192, および 256 ビット CBC)
  - 3DES (56 ビット×3 EDE)
  - Blowfish (128 ビット)
  - CAST (128 ビット)
  - Arcfour (128, 256 ビット)
- 公開鍵暗号アルゴリズム:
  - RSA (生成はデフォルト2048 bit, 範囲512~8192 bit)
  - DSA (生成はデフォルト2048 bit, 範囲512~8192 bit)

- メッセージ認証コード:
  - HMAC-MD5 (オプションにて MD5 拒否指定可)
  - HMAC-MD5-96
  - HMAC-SHA1
  - HMAC-SHA1-96
  - HMAC-SHA256
  - HMAC-SHA512
  - RIPEMD160
- 鍵交換アルゴリズム:
  - diffie-hellman-group1-sha1
  - diffie-hellman-group14-sha1
  - diffie-hellman-gex-sha1
  - gss-group1-sha1 with Kerberos 5
  - gss-gex-sha1 with Kerberos 5

### 認証

- サーバ認証:
  - 公開鍵 (RSA および DSA)
  - PKI X.509 証明書
  - GSSAPI/Kerberos
- ユーザ認証:
  - パスワード認証 (ローカルユーザおよび Windows ドメインユーザ)
  - 公開鍵認証:
    - RSA および DSA ユーザ鍵
    - OpenSSH 公開鍵の相互運用性
  - キーボード対話形式:
    - RSA SecurID
    - RADIUS
    - パスワード
  - PKI X.509 証明書
  - GSSAPI/Kerberos
- Reflection PKI サービスマネージャ (外付けオプション):
  - 複数の Reflection for Secure IT 製品を対象に、PKI 機能の構成と管理を集中化
- NEW** - DoD PKI 認定

## 主な機能と仕様 (続き)

- FIPS 140-2 レベル 1 取得 (証明書番号 1048)
- RFC 2253、2560、および 3280
- サーバおよびクライアント認証用の X.509 証明書 (X.509 バージョン 1 ~ 3)
- X.509 CRL (バージョン 2)
- OCSP の失効確認
- NEW** - HSPD-12 に対応
- LDAP および HTTP 証明書、CRL リポジトリに対応
- Microsoft Windows 証明書ストア
- 対応している証明書の拡張機能:
  - CDP、IDP、AIA、ポリシー制約、基本制約、名前制約、拡張鍵の使用
- 信頼アンカー単位構成のカスタマイズ
- 証明書への SSH ユーザアカウント名割り当てカスタマイズ

- NEW** - SOCKS プロキシに対応
- NEW** - PKI クライアントのコマンドラインユーティリティ (サービスの可用性と証明書の有効期間をクエリー)

### 監査

- Windows イベントログレベルの指定
- デバッグログ (ローカル あるいは UTC タイムスタンプ指定)
- パスワード認証リトライアウト時のイベント記録

### 管理ツール

- NEW** • サーバ構成ファイルの保存場所を変更可
- 構成ユーティリティが米国セクション 508 に対応

### オペレーティングシステム

- NEW** • Microsoft Windows Server 2008 R2 (x86-64)
- Microsoft Windows Server 2008 (x86 および x86-64)
- Microsoft Windows Server 2003 (x86 および x86-64)
- NEW** • Microsoft Cluster Service に対応

### システム要件

- Microsoft Windows オペレーティングシステムの最低限の要件を満たすシステム

## Attachmate社について

Attachmate社は、企業のIT投資の拡大、管理、セキュリティ保護のお手伝いをいたします。当社は、端末エミュレーション、ホストシステムとの統合、セキュアな管理されたファイル転送、および企業内の不正行為監視ツール等 先進ソフトウェアとソリューションを提供しております。世界中で 65,000 社を超える顧客企業が、Attachmateの技術によりIT資産の新たな有効活用をはかっています。詳細については、[www.attachmate.jp](http://www.attachmate.jp) をご覧ください。



日本支社  
NetIQ 株式会社 Attachmate 事業部  
〒162-0845 東京都新宿区市谷本村町1-1  
住友市ヶ谷ビル 9階  
TEL 03-3513-5111 FAX 03-3513-5112  
E-mail [j-info@attachmate.com](mailto:j-info@attachmate.com)  
URL [www.attachmate.jp](http://www.attachmate.jp)

米国本社  
1500 Dexter Avenue North  
Seattle, WA 98109 USA  
TEL +1 206-217-7500  
FAX +1 206-217-7515  
URL [www.attachmate.com](http://www.attachmate.com)

\*NetIQ 株式会社は米国 Attachmate Corporation の 100% 子会社です。