

Reflection® for Secure IT Windows クライアントは、グラフィカルユーザインタフェースとコマンドラインインタフェースの両方で安全なファイル転送機能と端末アクセス機能を提供する SSH クライアントです。このクライアントは、Windows および用の SSH クライアント/サーバを提供する Reflection for Secure IT 製品ファミリに含まれる製品で、これらの製品はすべて、通信/転送されるデータを保護するように設計されています。

バージョン 7.2 の特長

- Microsoft® Windows 7 に対応
- Attachmate FileXpress 転送管理機能との連携対応強化
- スマートカードへの対応を強化
- 画面メニューからリンクされた Web 上 日本語オンラインヘルプガイドを参照可
- Reflection FTP クライアントユーティリティ: ~SFTP プロトコル、FTP over SSH, FTP over SSL/TLS, Kerberos-ftp に対応
- PKI 証明書への対応強化: ~PKCS #11, 米国防総省CAC(Common Access Card), OCSP, CRL, LDAPを介した中間CA証明書

技術仕様

技術仕様

接続性

- SSH2 プロトコル: IETF SecSh インターネット標準規格準拠 (RFC 4250, 4254, 4256, 4462, 4344, 4345, 4716)
- SSH1 プロトコル (旧式 SSH 1 プロトコルサーバとの相互接続用)
- SCP1 (OpenSSH サーバ相互接続用)

認定暗号ライブラリ

- FIPS 140-2 レベル 1 取得 (証明書 #1027)

使いやすいインタフェース

- 使い慣れたグラフィカルユーザインタフェース
- ssh, sftp, scp コマンドラインによるバッチ処理/スクリプト処理

- NEW** • マルチホップ接続用簡易設定画面

安全なファイル転送

- SCP:
 - rcp コマンドの置き換え
 - SCP1 に対応
- SFTP:
 - FTP プロトコルの置き換え
 - draft-ietf-secsh-filexfer に準拠
- Reflection FTP クライアントユーティリティ:
 - SFTP プロトコル、FTP over SSHの他、FTP over SSL/TLS, Kerberos-ftp に対応
- NEW** • SFTP 転送時のタイムスタンプおよびファイル属性の保持を指定可

トンネリング

- TCP ポート転送 (ローカルリモート)
- FTP プロトコル (デュアルチャネル)
- X11 転送
- ゲートウェイポート
- RDP プロトコル (Microsoft リモートデスクトップアクセスを保護)

暗号化アルゴリズム

- 暗号:
 - AES (128, 192, 256 ビット; CTR および CBC)
 - 3DES (3 つの 56 ビット鍵による CBC)
 - Blowfish (128 ビット CBC)
 - CAST (128 ビット)
 - Arcfour (128 および 256 ビット)
- MAC:
 - HMAC-SHA1 および HMAC-SHA1-96
 - HMAC-SHA256 および HMAC-SHA512
 - HMAC-MD5 および HMAC-MD5-96
 - RIPEMD160
- 鍵交換:
 - Diffie-Hellman
 - RSA

認証

- サーバ認証:
 - 公開鍵認証 (RSA および DSA)
 - PKI X.509 証明書認証
 - GSSAPI
- ユーザ認証:
 - パスワード認証
 - 公開鍵認証
 - PKI X.509 証明書認証
 - キーボード対話型認証
 - GSSAPI/Kerberos認証
- パスワード認証:
 - ローカル
 - Windows ドメイン (Active Directory) 認証
- 公開鍵認証:
 - RSA
 - DSA
 - エージェント転送
- NEW** • スマートカードに対応)
 - キーボード対話型認証:
 - パスワード
 - RSA SecurID
 - RADIUS

- PKI X.509 証明書認証:
 - Reflection 証明書マネージャ
 - Windows 証明書マネージャ (MSCAPI)
 - オンライン証明書ステータスプロトコル
 - 証明書失効リスト (CRL)
 - CRL および中間 CA 証明書の LDAP/Active Directory による検索
 - PKCS #12 鍵および証明書の保存
 - PKCS #11 スマートカードに対応
- NEW** • 信頼済み証明書の共有保存場所
- GSSAPI/Kerberos認証:
 - Reflection Kerberos クライアント
 - Microsoft SSPI ログオン資格情報

多言語対応

- 英語
- 日本語
- フランス語
- ドイツ語

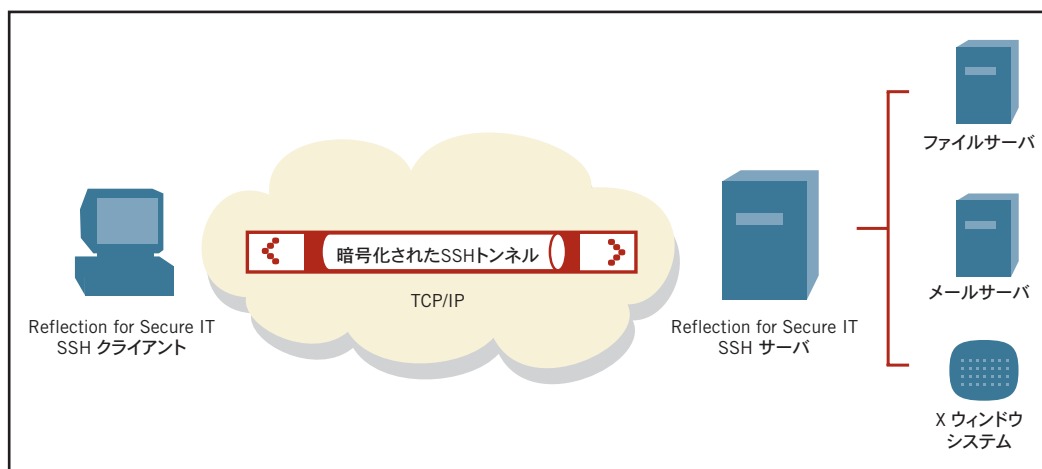
オペレーティングシステム

- NEW** • Microsoft Windows 7
- Microsoft Windows Vista (Service Pack 2)
- Microsoft Windows XP (Service Pack 3)
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008 (R2 を含む)
- Windows Terminal Server
- Citrix XenApp

技術仕様

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
- ディスク容量は、インストールされている機能によって異なります
- ネットワークインタフェースカード



SSH クライアントと SSH サーバの両方が一緒になって、すべての通信経路全体で安全な「トンネル」を構築します。

Attachmate について

Attachmate は、端末エミュレーション、既存アプリケーションと最新技術の統合、および安全なファイル転送を実現するために先進のソフトウェアをお届けします。また、当社の NetIQ 事業では、IT プロセスの自動化と性能管理、セキュリティ、および分散 IT 環境の法令遵守に対するソリューションを提供しています。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 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 jinfo@attachmate.com
 URL 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

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