

## Reflection for Secure IT UNIX 7.1 リリースノート

この度 Reflection for Secure IT (RSIT) バージョン 7.1 を国内リリースする運びとなりました。以下 RSIT UNIX クライアントおよびサーバの新機能について、その概要をご案内申し上げます。

### 記

#### 1. 対象製品

- 1) Reflection for Secure IT UNIX サーバ バージョン 7.1
- 2) Reflection for Secure IT UNIX クライアント バージョン 7.1

#### 2. バージョン 7.1 の主な新機能

##### 2.1 サーバ/クライアント 共通の新機能

- 1) "Reflection PKI Services Manager" を用いた外部 PKI 環境と連携した PKI 証明書認証。  
"Reflection PKI Services Manager" は、RSIT とは独立した無償プログラムで、RSIT UNIX サーバと RSIT UNIX クライアント内に実装した "PKI Services Manager Client" からの要求に対し、外部認証局 (CA) 等と連携して確認結果を返します。  
詳細は下記参照。
  - Tech Note 2425 (英文) <<http://support.attachmate.com/techdocs/2425.html>>
  - User Guide (英文)  
<[http://docs.attachmate.com/reflection/PKI/1.0/en/pki\\_manager\\_user\\_guide.pdf](http://docs.attachmate.com/reflection/PKI/1.0/en/pki_manager_user_guide.pdf)>
- 2) Solaris および Linux において、インストール先を指定可
- 3) 旧バージョン構成定義 (ssh2\_config、sshd2\_config) からの設定内容の移行を支援するスクリプトを用意
- 4) 新規プラットフォームに対応
  - a) AIX 6.1 (POWER)
  - b) Red Hat Enterprise Linux 5 (Itanium)

##### 2.2 サーバの新機能

- 1) sftp、scp によるファイルアクセス/操作許可を詳細に指定可
  - a) "ChrootSftpUsers"、"ChrootSftpGroups" パラメータにより、ユーザ、グループ単位のアクセス範囲の指定
  - b) "AllowSftpCommands" パラメータにより、ファイル操作の許可に関して {"all"、"none"、"browse"、"download"、"upload"、"delete"、"rename"} の中から一つあるいは複数を指定可。
  - c) b) の内容と "UserSpecificConfig"、"HostSpecificConfig" 指定組合せにより、ユーザ、グループ、ホスト単位のファイル操作許可を指定可。
- 2) ファイル転送に関するログを "SftpSyslogfacility" と "LogLevel" 指定により採取
- 3) Solaris において、最小特権 (Least Privilege) 機能に対応

##### 2.3 クライアントの新機能

- 1) Solaris 10 SPARC において、PKCS#11 スマートカードに対応

#### 3. バージョン 6.1 互換機能のサポート

バージョン 7.0 更新時に未サポートとなっていたバージョン 6.1 の機能に改めて対応しました。

##### 3.1 サーバ/クライアント 共通の機能

- 1) SFTP、scp によるファイル転送において、途中中断後の再コマンド発行時に中断点からの再開機能をサポート。

- 2) SFTP、scp において、転送先に転送ファイルと同一内容/同一名称のファイルが存在する時に転送を省略する Smart Copy 機能をサポート。  
注記：ASCII モード転送時は、Smart Copy 機能は無効になります。
- 3) ユーザ認証として、PKI 証明書認証と RADIUS 認証に対応し、サーバ認証として、PKI 証明書認証に対応。
- 4) ssh-certtool ユーティリティにより、PKCS#10 証明書要求や PKCS#12 形式パッケージの作成。
- 5) ssh-certview ユーティリティにより X.509 証明書、CRL リスト、PKCS#10 証明書要求を参照可。
- 6) メッセージ認証コード(MAC)アルゴリズムとして、より強固な hmac-sha256 と hmac-sha512 を追加し、MD5 署名の使用を拒否指定可。
- 7) 下記プラットフォームに再対応。
  - a) Red Hat Enterprise Linux 3 (x86、x86-64 )
  - b) Red Hat Enterprise Linux 4 (zLinux 64 ビット)
  - c) SUSE Linux Enterprise Server 9 (zLinux 32 ビット)

### 3.2 サーバの機能

- 1) "LogCertificateSubject"パラメータにより、システムログへのログイン成功/失敗記録の際に、認証用証明書の Serial Number と Subject 追記有無を指定可。
- 2) Message of the Day ファイル(/etc/motd) に記述したメッセージをユーザログイン時に表示可。

### 3.3 クライアントの機能

- 1) scp コマンドにおいて、バッチモードに対応。
- 2) ASCII モード転送のために、特定拡張子の場合は明示的な ASCII モード指定を省略可。
- 3) authorization ファイル内の PUBLIC-KEY オプションにて、強制 command、allow-from および deny-from オプションを指定可。
- 4) 認証エージェントに対して、証明書の add をサポート。
- 5) "HostCertNameCheck" パラメータにより、サーバのホスト証明書内の Common Name (CN)または Subject Alternative Name (SAN) フィールドとホスト名の一致判定を指定可。

## 4. バージョン 7.1 の入手

- 1) ボリュームライセンス (VPA) 保守契約のお客様：  
お手元に控えのユーザ名とパスワードを使い 下記 Attachmate ダウンロードライブラリサイトにログイン後、対象ファイルをダウンロードし入手下さい。  
<https://download.attachmate.co.jp/Login.aspx>
- 2) シングルパッケージ購入のお客様 ならびに 保守契約をされていないお客様：  
バージョンアップをご希望される場合、下記弊社お問合せ先までメール連絡をお願いします。  
[j-info@attachmate.com](mailto:j-info@attachmate.com)

以上