AX260A

Secure Shell (SSH)
ソフトウェアマニュアル

2020 年 4 月 発行（第 2 版）

はじめに

■ 対象製品

このマニュアルは，SecureShell(SSH)機能についての内容を記載しています。対象製品は，AX260A シリーズについて記載しています。また，ソフトウェアは，OS-L2F でサポートする機能について記載します。
Ver.4.17 以降のソフトウェアをご利用の場合は，以下マニュアルを参照してください。
「AX260A Secure Shell (SSH) ソフトウェアマニュアル (AX26A-SOFT-007)」

■ 輸出・取り扱い時の注意

本製品を輸出される場合には，外国為替および外国貿易法ならびに米国の輸出管理関連規則など外国の輸出関連法規をご確認のうえ，必要な手続きをお取りください。

また，本マニュアルを使用・閲覧される方(以下，利用者)は，次の条件を承諾し，同意するものとします。本マニュアルは，日本国およびアメリカ合衆国の輸出管理法等の輸出規制において，ソフトウェア(暗号)の使用に必要な技術として，輸出規制の対象となっております。
本マニュアルまたは本マニュアルから得た技術情報を，直接的または間接的に輸出，再輸出，非居住者に提供・開示を行うには，別途手続きが必要です。ご利用者は，本マニュアルまたは本マニュアルから得た技術情報の取り扱いに関して，日本国内の法ならびに，日本国およびアメリカ合衆国の輸出管理法等の輸出規制に従うことに同意するものとします。

なお，不明な場合は，弊社担当営業にお問い合わせください。

■ 商標一覧

Ethernet は，富士ゼロックス株式会社の登録商標です。
イーサネットは，富士ゼロックス株式会社の登録商標です。
Microsoft は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Windows は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Mac OS，Macintosh は，Apple Computer，Inc.の商標です。
ssh は SSH Communications Security Corp (www.ssh.com) の登録商標です。
RSA，RSA SecurID は，RSA Security Inc.の米国およびその他の国における商標または登録商標です。
そのほかの記載の会社名，製品名は，それぞれの会社の商標もしくは登録商標です。

■ マニュアルはよく読み，保管してください。

製品を使用する前に，安全上の説明をよく読み，十分理解してください。
操作を行う前にこのマニュアルをよく読み，書かれている指示や注意を十分に理解してください。また，このマニュアルは必要な時にすぐ参照できるよう使いやすい場所に保管してください。

なお，このマニュアルでは特に断らないかぎり SecureShell(SSH)機能についてだけ記載しています。その他の機能につきましては，対応する本装置のマニュアルをご覧ください。

■ ご注意
このマニュアルの内容については，改良のため，予告なく変更する場合があります。

■マニュアルの構成
このマニュアルは，次に示す 6 つの編と付録から構成されています。

［解説編］
本装置の SSH 機能について解説しています。

［コンフィグレーションガイド編］
本装置の SSH サーバ機能を使用する場合のコンフィグレーションコマンド例について解説しています。

［運用ガイド編］
本装置の SSH サーバの管理運用について説明しています。

［コンフィグレーションコマンドレファレンス編］
本装置のコンフィグレーションコマンドについて詳細を説明しています。

［運用コマンドレファレンス編］
本装置の運用コマンドについて詳細を説明しています。

［メッセージ・ログレファレンス編］
本装置の SSH 機能に関連するメッセージ・ログについて説明しています。

［付録］
用語解説，準拠規格，謝辞（Acknowledgments）を掲載しています。

■ 発行
２０２０年４月（第２版）　ＡＸ２６Ａ－ＳＯＦＴ－００４_Ｒ１

■ 著作権
All Rights Reserved, Copyright(C), 2015, 2020, ALAXALA Networks, Corp.

■ 変更履歴

【第 2 版】変更内容

項番	章・節・項・タイトル	追加・変更内容
1	はじめに	• Ver.4.17 以降のマニュアルを分離しました。
2	4.1　SSH サーバへの接続ユーザ数	• スタック動作時のログイン数について追加しました。【4.12 以降】
3	6.3　SSH サーバのホスト鍵ペアの変更をする	• MC 運用モード機能，ゼロタッチプロビジョニング機能について追加しました。【4.9 以降】
4	6.4　SSH サーバのホスト鍵ペアを保存・復元する	• MC 運用モード機能，ゼロタッチプロビジョニング機能について追加しました。【4.9 以降】
5	C.準拠規格	• 準拠規格を変更しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

目　次

用語略称の表記

■ 用語略称一覧

略称	用語
AES	Advance Encryption Standard
CA	Certificate Authority
CBC	Cipher Block Chaining
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
FTP	File Transfer Protocol
HMAC	Hash Message Authentication Code
IP	Internet Protocol
IPv6	Internet Protocol version 6
MAC	Message Authentication Code
MD5	Message Digest 5
PC	Personal Computer
PGP	Pretty Good Privacy
PP	Program Product
RADIUS	Remote Authentication Dial In User Service
rcp	Remote Copy
RSA	Rivest，Shamir，Adleman
SCP	Secure Copy
SFTP	Secure File Transfer Protocol
SHA1	Secure Hash Algorithm 1
S/W	Software
SSH	Secure Shell
TACACS+	Terminal Access Controller Access Control System Plus

解説編

1. SecureShell(SSH)概要

本章では SSH の機能概要を示します。

1.1　概要

1.1.1　特徴

SSH 機能は，クライアント端末からサーバへ，安全でないネットワークを介して接続する際に使用します。SSH を使用することで，通信路は暗号化され，認証も厳しく行えるため，ネットワーク上の悪意のある第三者の盗聴・改ざん・なりすましから保護できます。SSH を使用することで，TELNET 接続(図 1.1-1)の脅威であった，運用情報の流出，データの改ざん，不正なりすましサーバへの誤接続などから保護された，セキュアな運用管理を実現できます(図 1.1-2)。

図 1.1-1　TELNET での接続による脅威(盗聴)

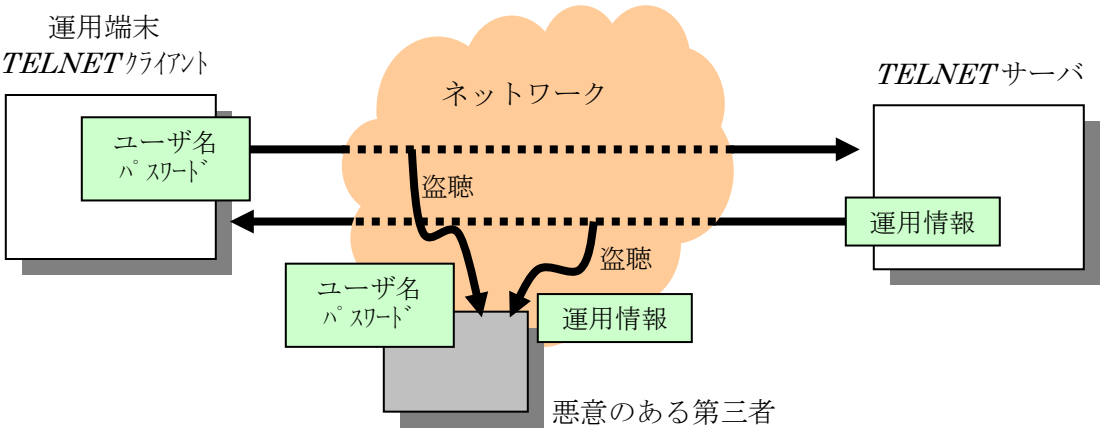
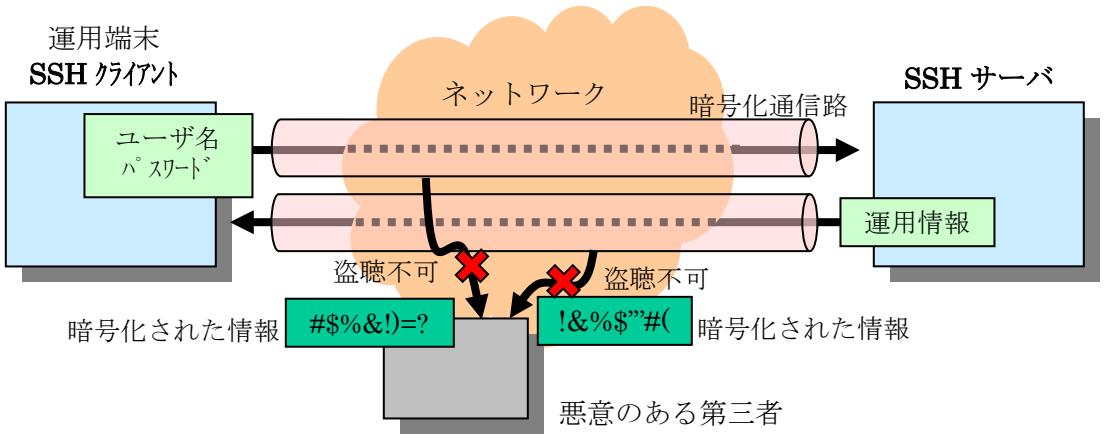


図 1.1-2　SSH での接続によるセキュアな運用管理



1.1.2　プロトコルバージョン

SSH にはプロトコルとしてバージョン 1(SSHv1)とバージョン 2(SSHv2)があります。SSHv2 では，SSHv1 と同様に，通信を暗号化して各種機能を提供しますが，加えてファイル転送(sftp)機能も提供します。

また，SSHv2 は鍵の交換に Diffie-Hellman 鍵交換プロトコルを使用し，暗号通信データの完全性を保護するためにメッセージ認証コード(MAC)を採用しています。そのため，SSHv2 は SSHv1 に比べセキュリティが向上しています。

本装置では，SSHv1 と SSHv2 の SSH サーバをサポートしています。運用の際は，上記セキュリティ上の理由からできるだけ SSHv2 をお使いください。

また，本マニュアルでは，以下の SSHv2 クライアントソフトウェアとの接続を例として示しました。

・OpenSSH　　「OpenSSH_4.3p2」

SSH はセキュリティソフトですので，古いバージョンのクライアントソフトウェアをご利用にならず，上のようなできるだけ最新の物をご利用ください。

その他のクライアントソフトウェアでも，「付録 B. 準拠規格」に適合していれば基本的に接続可能ですが，事前に十分な接続テストを行ってください。

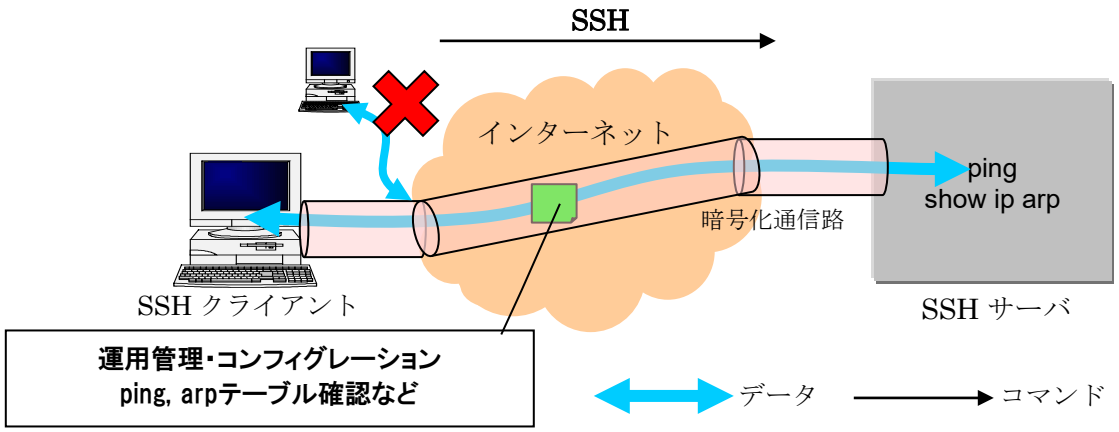
1.2　機能概要

1.2.1　セキュアリモートログイン機能

通常，SSH(SecureShell)と呼ばれる機能です。この機能を用いると，インターネットを介しても，安全に管理運用端末から，SSH サーバへログインすることができます。また，通信内容を他者に見られることがありませんので，安全な管理運用を実現できます(図 1.2-1)。

本装置運用の際，インターネットを介しても運用端末から本装置へ安全にログインすることができます。

図 1.2-1　セキュアリモートログイン機能



SSH サーバへログインするためのユーザの認証方法は，telnet で用いられていたパスワード認証の他，より安全な公開鍵認証を利用できます。公開鍵認証を利用することで，パスワードの秘密情報が漏洩し他者に利用されることを防ぐことができます。

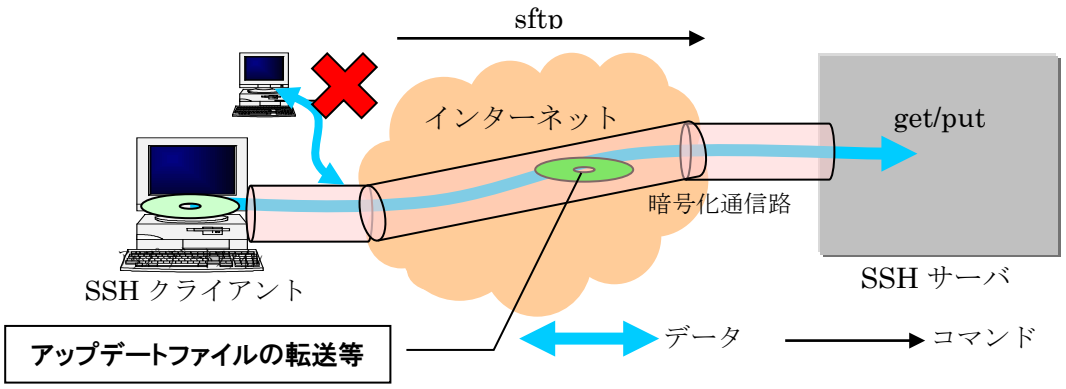
本装置上で公開鍵認証を利用するには，あらかじめユーザ公開鍵の登録をおこないます。

1.2.2　セキュアファイル転送機能

セキュア FTP(sftp)と呼ばれる機能です。この機能を用いると，管理運用端末と SSH サーバ間でファイルを転送することができます。また，通信内容を他者に見られたり，改ざんされたりすることがありませんので，安全な管理運用を実現できます。セキュア FTP は FTP と同様のインタフェースで使用できます。

本装置運用の際，アップデート実施時のファイルアップロードなどを安全に行うことができます(図 1.2-2)。

図 1.2-2　セキュアファイル転送機能



1.3　サポート機能一覧

本装置サポートする機能一覧を表 1.3-1に示します。

表 1.3-1　SSH 機能サポート一覧

項番	機能名		SSH プロトコル バージョン	本装置	説明
1	SSH サーバ		v1/v2	○	SSH のサーバ機能です
(1)		セキュアリモートログイン	v1/v2	○	SSH のリモートログイン(telnet 相当)機能です
(2)		セキュアコピー	v1/v2	×	SSH を利用したファイルコピー(rcp 相当)機能です
(3)		セキュアファイル転送	v2	○	SSH を利用したファイル転送(ftp 相当)機能です
2	SSH クライアント		v1/v2	×	SSH のクライアント機能です
(1)		セキュアリモートログイン	v1/v2	×	SSH のリモートアクセス(telnet 相当)機能です
(2)		セキュアコピー	v1/v2	×	SSH を利用したファイルコピー(rcp 相当)機能です
(3)		セキュアファイル転送	v2	×	SSH を利用したファイル転送(ftp 相当)機能です
3	認証エージェント		v1/v2	×	認証エージェント機能です
4	ポート転送		v1/v2	×	ポート転送(TCP トンネリング)機能です
5	X11 プロトコル自動転送		v1/v2	×	X11 を自動転送する機能です
6	データ圧縮		v1/v2	×	通信のデータ圧縮をおこなう機能です
7	IPv6		v1/v2	○	IPv6 を用いて通信可能です

実装：　○ … サポート　△…一部サポート　× … 未サポート

本装置でサポートする詳細機能一覧を表 1.3-2に示します。

表 1.3-2　SSH 詳細機能サポート一覧

項番	機能名				SSH ﾌﾟﾛﾄｺﾙﾊﾞｰｼﾞｮﾝ	本装置	説明
1	ユーザ認証方法				v1/v2	○	ユーザ認証を行う方法です
(1)		公開鍵認証	RSA	サーバ機能	v1/v2	○	RSA 公開鍵を用いたユーザ認証鍵をサーバ側に登録できます
				ｸﾗｲｱﾝﾄ機能		×	
(2)			DSA	サーバ機能	v2	○	DSA 公開鍵を用いたユーザ認証鍵をサーバ側に登録できます
				ｸﾗｲｱﾝﾄ機能		×	
(3)			PGP		v2	×	PGP 鍵を用いた認証です
(4)			CA 認証		v2	×	CA 認証を用いた認証です
(5)		パスワード認証	ローカル	サーバ機能	v1/v2	○	ローカルパスワード認証です
				ｸﾗｲｱﾝﾄ機能		×	
(6)			RADIUS/TACACS+		v1/v2	△	RADIUS/TACACS+連携のパスワード認証です。本装置は RADIUS 認証と連携します
(7)		ホストベース/RSARhost 認証			v1/v2	×	ホストベース認証です
(8)		Rhost 認証			v1	×	SSHv1 の Rhost 認証です
2	共通鍵暗号方式				v1/v2	○	通信路の暗号化に用います
(1)		aes128-cbc	128 bit		v2	○	-
(2)		aes192-cbc	192 bit		v2	○	-
(3)		aes256-cbc	256 bit		v2	○	-
(4)		3des-cbc	168 bit		v1/v2	○	-
(5)		blowfish-cbc	128 bit		v1/v2	×	-
(6)		twofish128-cbc	128 bit		v2	×	-
(7)		その他			v1/v2	×	上記だけサポートします
3	メッセージ認証コード(MAC)方式				v2	○	データの改ざん防止に用います
(1)		hmac-sha1			v2	○	-
(2)		hmac-sha1-96			v2	○	-
(3)		hmac-md5			v2	○	-
(4)		hmac-md5-96			v2	○	-
(5)		その他			v2	×	上の 4 種類だけサポートします
4	ログインメッセージ表示機能				v1/v2	×	
(1)		ログイン前メッセージ表示機能			v2	×	
(2)		ログイン後メッセージ表示機能			v1/v2	×	

実装：　　○ … サポート　　△…一部サポート　　× … 未サポート

2. SSH 詳細

本章では SSH の接続手順や暗号方式などの詳細な説明をします。

2.1　SSH 接続手順

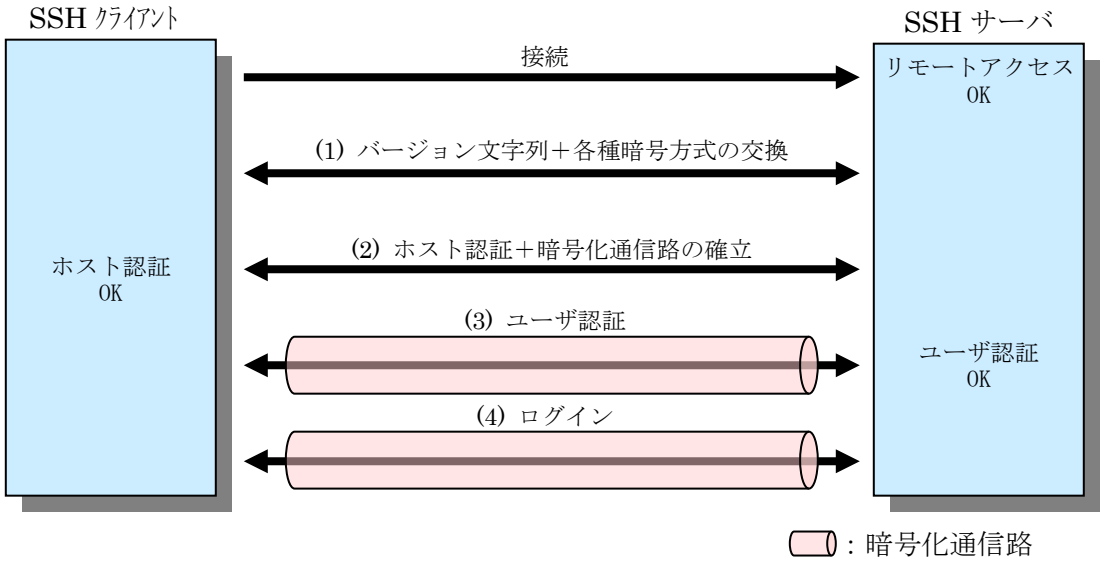
次に，SSH の接続からログインまでの流れを説明します。また，説明中の暗号方式や MAC 方式については，「2.2暗号化技術」および「2.3メッセージ認証コード(MAC)」の説明をご覧ください。

2.1.1　接続からログインまでの流れ

SSH クライアントから，ネットワークを介して接続されている SSH サーバへ接続する場合の流れを図 2.1-1 に示します。SSHv1 と SSHv2 では詳細な接続手順が異なりますが，基本的な流れは同じです。

まず接続すると，バージョン文字列と各種暗号方式の交換(1)の後，クライアント側で，接続相手が正しい接続相手であるか認証(ホスト認証)を行い，同時に，SSH クライアントーSSH サーバ間を流れるデータを暗号化する通信路を確立します(2)。暗号化通信路が確保された後，暗号化通信上でユーザ認証を行い(3)，認証が成功するとログインします(4)。

図 2.1-1　SSH 接続の流れ



以下，SSH 接続の流れの各手順をそれぞれ説明します。

(1) バージョン文字列＋各種暗号方式の交換

接続後，サーバとクライアントの間で SSH バージョン文字列を交換し，SSHv1 で接続するのか，SSHv2 で接続するのかを決定します。

1. SSHv1

サーバは，クライアントへ使用できる共通鍵暗号方式のリスト，ホスト公開鍵とサーバ公開鍵を送ります(これらの鍵の用途は(2)で説明します)。クライアントでは，そ

のリストから可能な共通鍵暗号方式を決定します。

2. SSHv2

サーバ・クライアント間で，可能な鍵交換方式，希望する公開鍵暗号方式，共通鍵暗号方式，MAC，圧縮アルゴリズムの各リストを交換します。

(2) ホスト認証＋暗号化通信路の確立

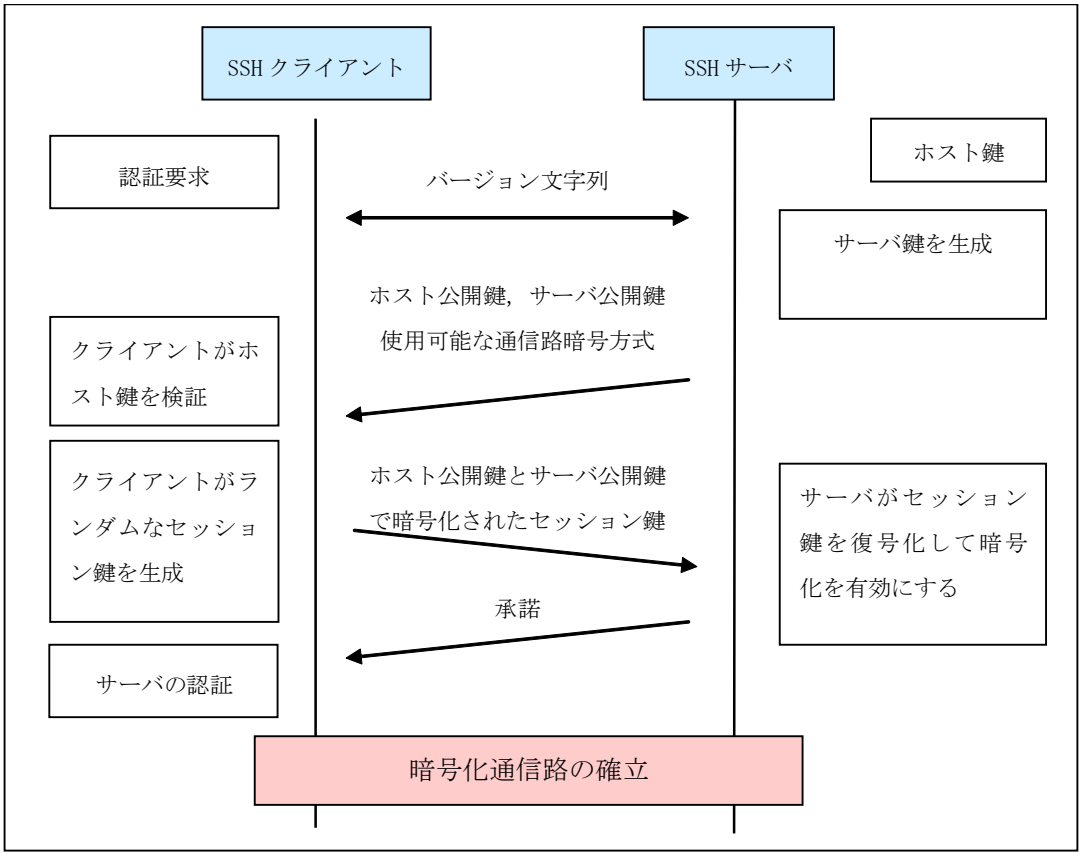
各 SSH サーバは各々異なるホスト鍵ペア(ホスト公開鍵とホスト秘密鍵)に変更してから運用します（工場出荷時にはデフォルトのホスト鍵ペアが設定されています。運用コマンド set ssh hostkey によるホスト鍵ペアの変更を強くお勧めします)。

クライアントはサーバの正当性確認のためこれらの鍵を用います。

1. SSHv1

クライアントは，(1)で送られてきたホスト公開鍵を各ユーザが保持しているホスト公開鍵のデータベースと照合してホスト認証を行います。その後，暗号化通信で用いるセッション鍵を生成します。このセッション鍵を，ホスト公開鍵と(1)で同時に送られてきたサーバ公開鍵とを用いて暗号化し，サーバに送付します。サーバ側では自身の秘密鍵でセッション鍵を復号できれば，暗号化した承諾メッセージを送り，正しいホストであることを証明します。また同時に，暗号化通信路が確立されます(図 2.1-2)。

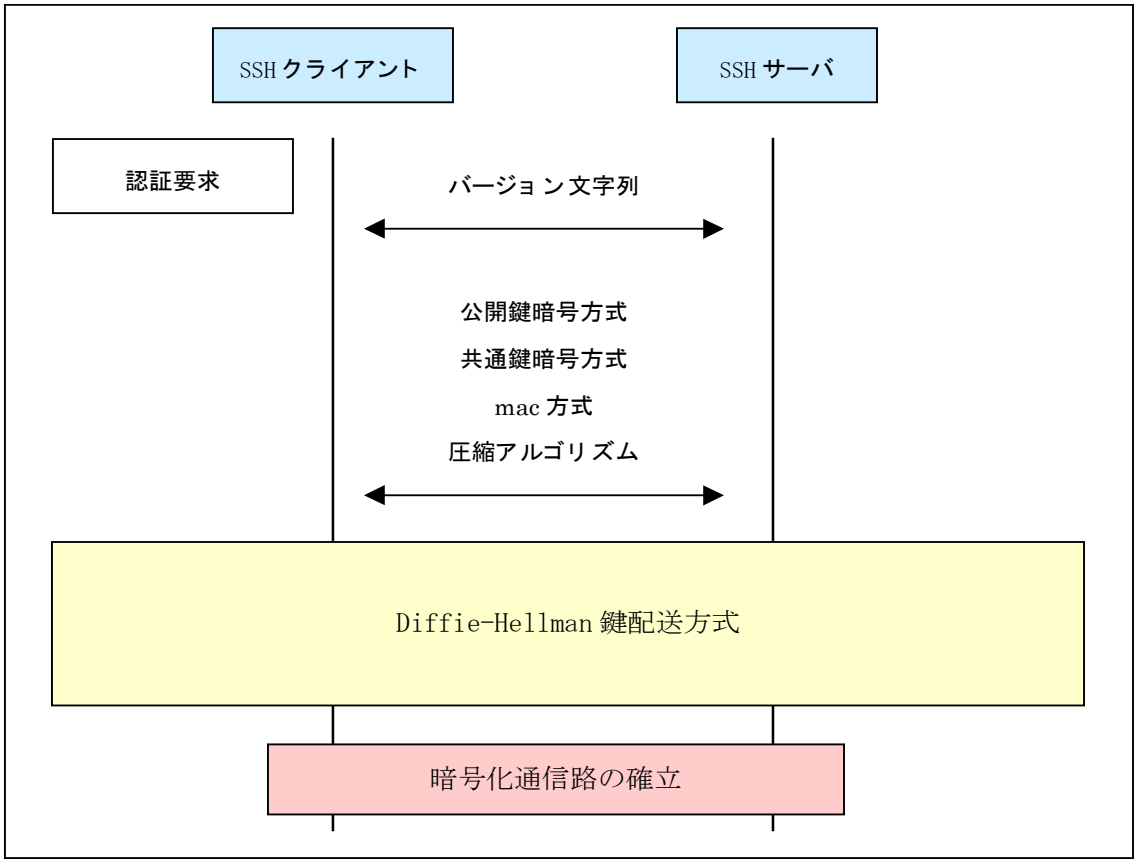
図 2.1-2　SSHv1 でのホスト認証と暗号化通信路の確立



2. SSHv2

サーバ・クライアント両者は，(1)で交換した共通鍵暗号や MAC のアルゴリズムリスト中から，使用するアルゴリズム方式を決定します。その後，Diffie-Hellman 鍵交換方式で暗号化通信路に用いる共通鍵を交換し，その鍵交換の途中，サーバのホスト公開鍵はクライアント側で保持しているホスト公開鍵のデータベースと照合してホスト認証も行います(図 2.1-3)。Diffie-Hellman 鍵交換方式は，交換する鍵を直接送ることなく両者で鍵を得ることができるアルゴリズムです。

図 2.1-3　SSHv2 でのホスト認証と暗号化通信路の確立



(3) ユーザ認証

ホスト認証後，暗号化通信路が確立されると，次の(a)(b)いずれかのユーザ認証を行います。（ユーザ認証の種類は本装置のコンフィグレーションコマンド ip ssh authentication で設定が可能です。）

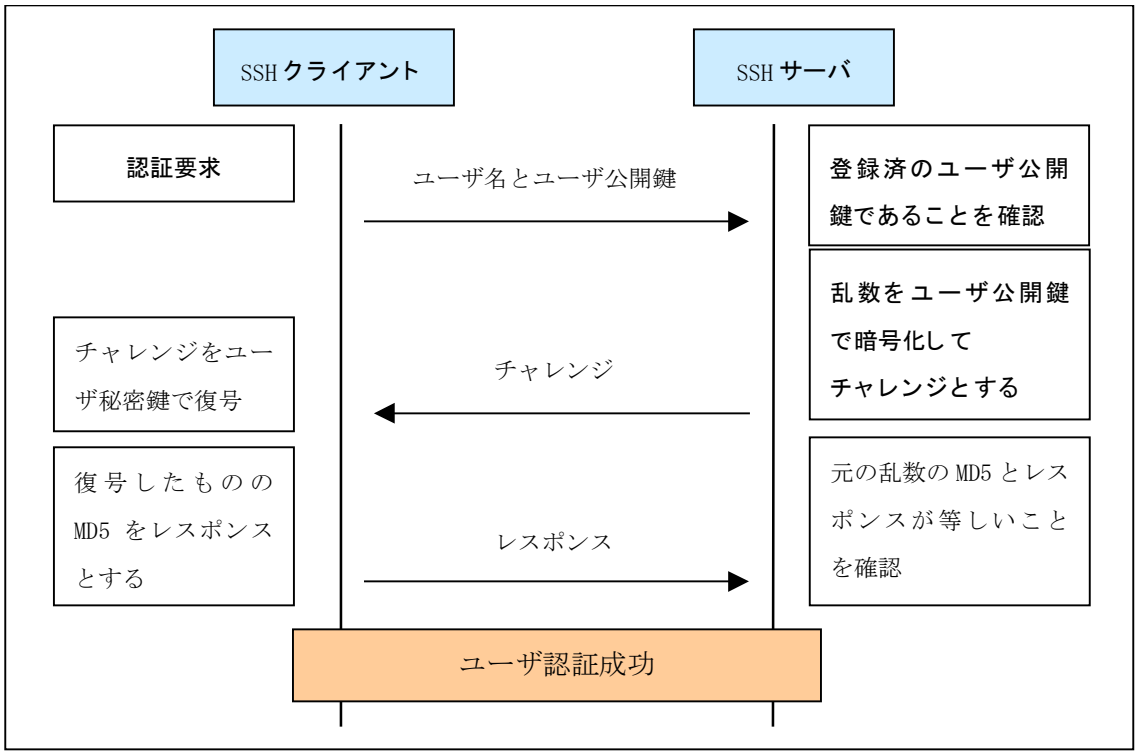
(a) 公開鍵暗号方式によるユーザ認証

サーバ側ではあらかじめユーザの公開鍵を登録しておきます。クライアントユーザは，登録されているユーザ公開鍵に対応する秘密鍵を所持していることで認証を行います。

1. SSHv1

SSHv1 では，”チャレンジ＆レスポンス"という方法を用います。まずサーバでは，ユーザから送られてきたユーザ公開鍵があらかじめ登録されているか確認します。その後，乱数を発生させ，それをユーザ公開鍵で暗号化し，クライアントに返します(チャレンジ)。クライアントではチャレンジを秘密鍵で復号し，元の乱数に戻してから，ハッシュ(MD5)をかけ，それをサーバに返送します(レスポンス)。サーバでは，元の乱数にハッシュをかけたものとクライアントから送られてきたものを照合し，等しければユーザ認証成功とします(図 2.1-4)。

図 2.1-4　SSHv1 でのユーザの公開鍵認証の流れ

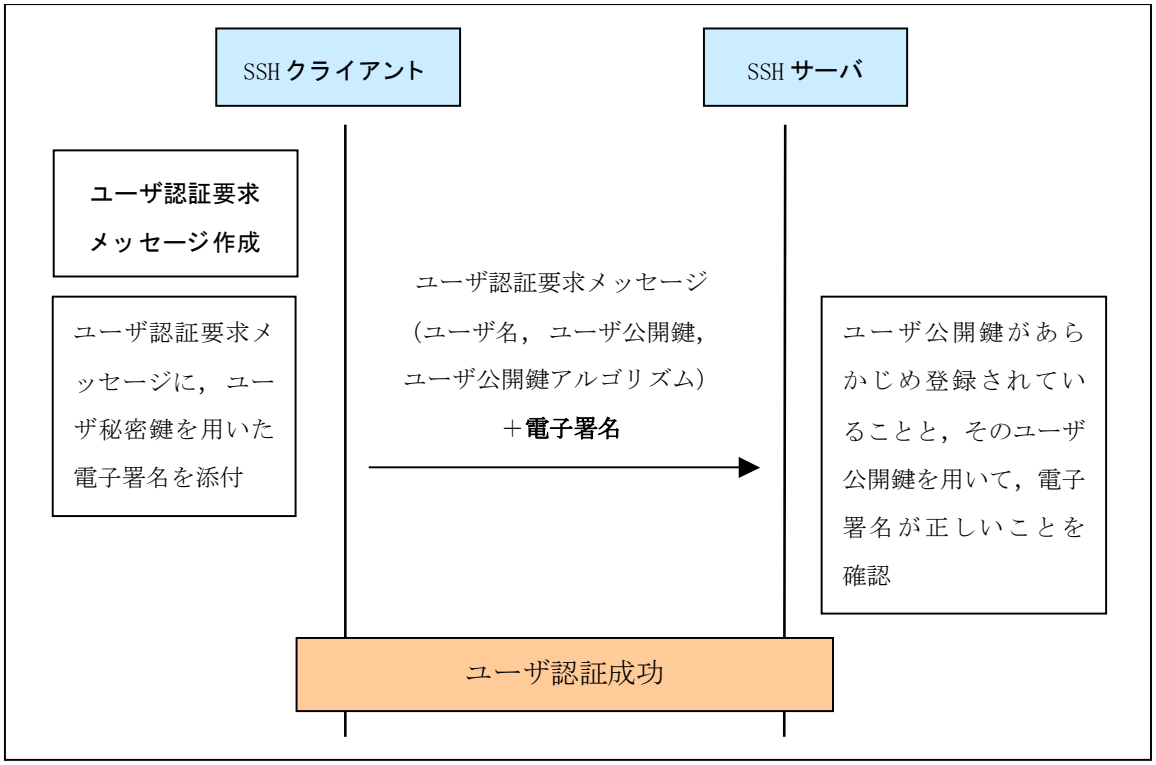


2. SSHv2

SSHv2 では，電子署名という方法を用いてユーザ認証を行います。まず，クライアントは，ユーザ名，ユーザの公開鍵，ユーザの公開鍵アルゴリズムを記述した認証要求メッセージを作成します。そして，作成した認証要求メッセージに対して，ユーザの秘密鍵を用いて電子署名を作成します。最後に，サーバに対して，認証要求メッセージに電子署名を付けたものを送付します。

サーバでは，送付された認証要求メッセージから，ユーザ名とユーザ公開鍵を取り出し，あらかじめ登録されているユーザとユーザの公開鍵であることを確認します。また，登録されているユーザの公開鍵を用いて，送られてきた電子署名を審査し，正しいユーザの電子署名であることを確認できると，ユーザ認証成功とします(図 2.1-5)。

図 2.1-5　SSHv2 でのユーザの公開鍵認証の流れ



(b) ローカルパスワードによるユーザ認証

telnet と同様にサーバ側でローカルに設定されたパスワードを用いてユーザ認証を行います。しかし，パスワードは暗号化されたチャネルを通るため，第三者には見えません。

(4) ログイン

ユーザ認証が成功すると，セッションが確立し，ユーザはログインとなります。ここで，通常はターミナルのセッションが開始されます。sftp で接続の場合は，サーバ側で sftp-server コマンドが実行され，ファイル転送が行われます。

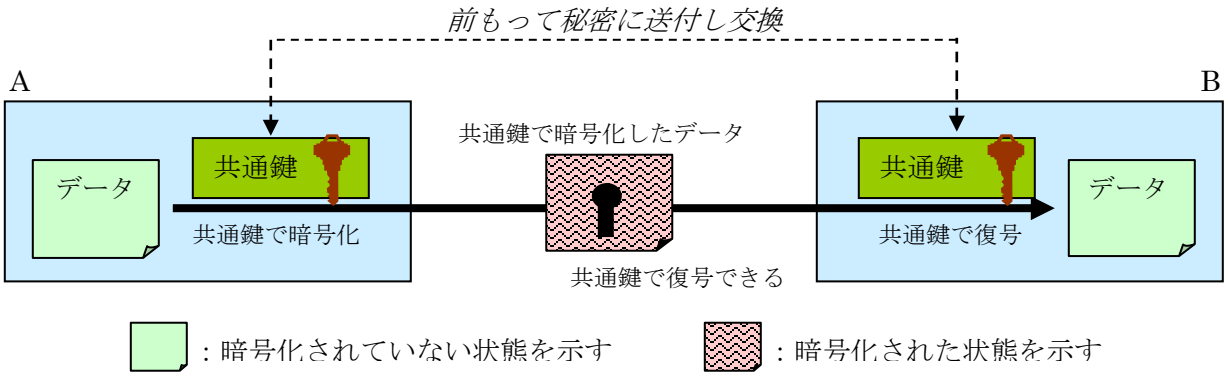
2.2　暗号化技術

SSH プロトコルでは，次の二種類の暗号方式(暗号化技術)を利用して，認証と暗号化通信を行っています。それぞれの暗号方式はさまざまなアルゴリズムによって実現されますが，基本的には元のデータに対して，ある特定のデータである「鍵」を使用し，特定の処理を行って暗号化を実現し，暗号化されたデータはある「鍵」を使用して処理し，復号します。

2.2.1　共通鍵暗号方式

A と B で共通の鍵である「共通鍵」を使用することで，暗号化と復号をおこないます。そのため，この「共通鍵」は暗号化通信を行う前に，前もって秘密に送付しておくことが必要となります。

図 2.2-1　共通鍵暗号方式での暗号化通信



共通鍵暗号方式は，(2)の公開鍵暗号方式に比べ，演算の処理量が少ないという利点があります。そのため，SSH プロトコルでは，通信の暗号化にはこの共通鍵暗号方式を採用しています。

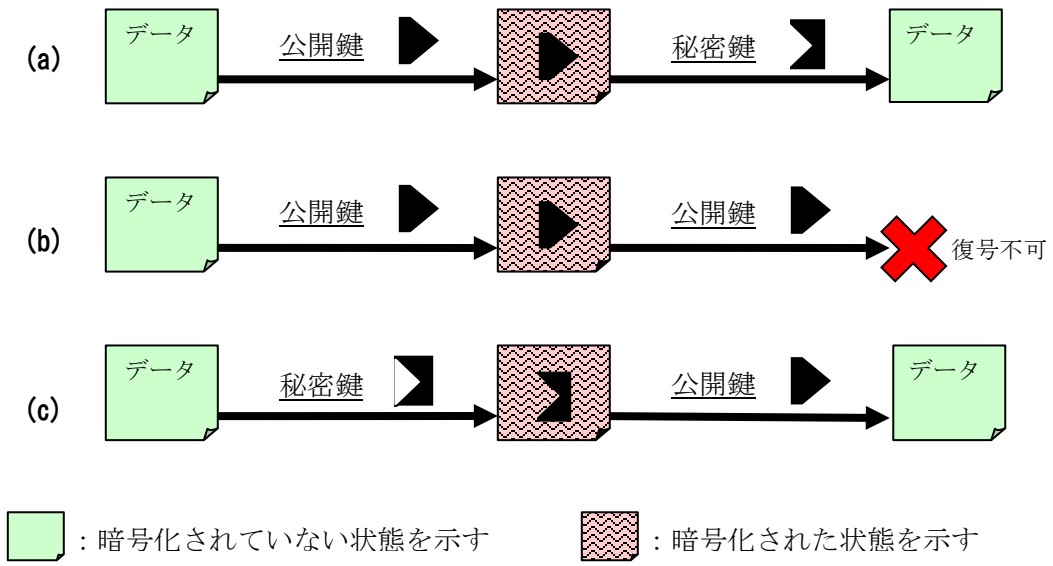
本装置では，使用する共通鍵暗号方式の種類はコンフィグレーションコマンド ip ssh ciphers で設定可能です。

2.2.2　公開鍵暗号方式

公開鍵暗号方式は，二種類の鍵「公開鍵」と「秘密鍵」をペアで使用します。この「公開鍵」と「秘密鍵」には以下の性質があり，公開鍵暗号方式はこれらの性質を利用して暗号化や署名を実現しています。

(a) 「公開鍵」で暗号化されたデータは「秘密鍵」で復号できる（図 2.2-2(a)）
(b) 「公開鍵」で暗号化されたデータは「公開鍵」では復号できない（図 2.2-2(b)）
(c) 「秘密鍵」で暗号化したデータは「公開鍵」で復号できる（図 2.2-2(c)）
(d) 「公開鍵」から「秘密鍵」を生成することはできない

図 2.2-2　公開鍵と秘密鍵の関係

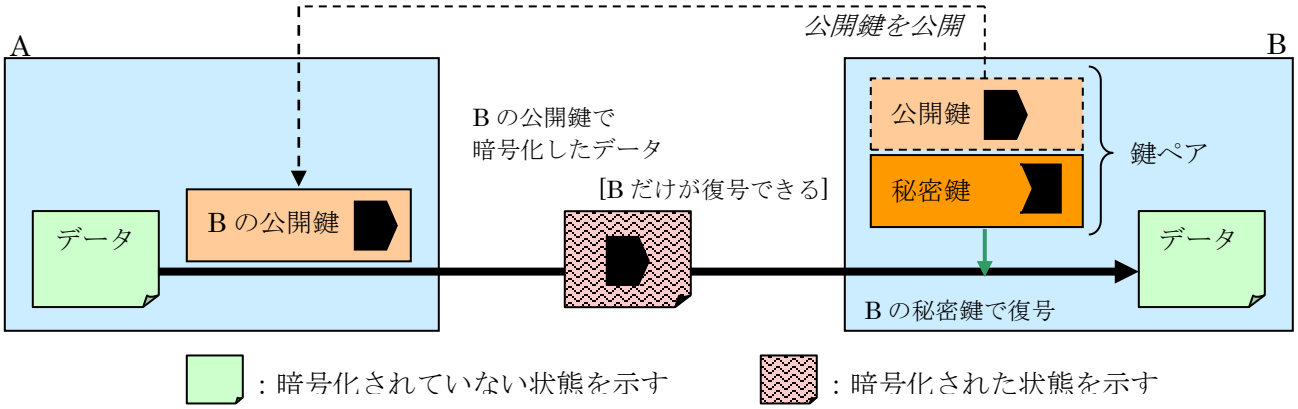


通常，鍵ペアを作成した側は「秘密鍵」を任意のパスフレーズで暗号化して手元に保管し，「公開鍵」を相手に公開します。相手は，送信する相手の「公開鍵」を用いて，データを暗号化し送信します。

また，自身の「秘密鍵」を用いて，暗号化したデータを相手に送り，相手が「公開鍵」で復号できることを確かめることで，電子署名とすることができます。

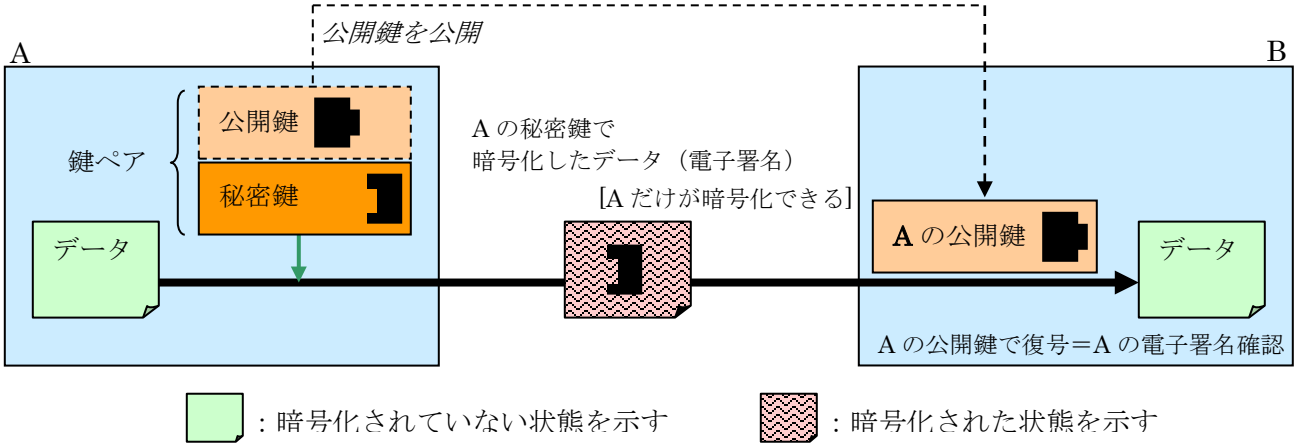
以下の図 2.2-3 は，鍵ペアを作成したＢが「公開鍵」を相手Ａに公開しています。相手Ａは公開されたＢの「公開鍵」を用いて，データを暗号化して，Ｂへ送付しています。送付されたデータはＢ自身の秘密鍵でだけ復号できます。

図 2.2-3　公開鍵暗号方式での暗号化



また図 2.2-4 は，鍵ペアを作成したＡが「公開鍵」を相手Ｂへ公開しています。Ａは自身の「秘密鍵」で暗号化したデータを相手Ｂへ送付し，ＢはＡの「公開鍵」で復号できることを確認することで，Ａが送付したデータであることを確認できます(電子署名)。

図 2.2-4　公開鍵暗号方式での署名



公開鍵暗号方式は，(1)の共通鍵暗号方式に比べ，秘密に鍵を送付する必要がないため便利ですが，演算の処理量が大きいという欠点があります。そのため，SSH プロトコルでは，共通鍵の送付(SSHv1)または交換(SSHv2)と，ホスト認証・ユーザ認証にこの公開鍵暗号方式を採用しています。

本装置では，ユーザの公開鍵認証用に使用するユーザ公開鍵はコンフィグレーションコマンド ip ssh authkey で設定(登録)が可能です。

2.3　メッセージ認証コード(MAC)

SSHv2 では，メッセージ認証コードを利用して通信内容の改ざんの検出を行っています。メッセージ認証コードとは元の情報から固定長のコードを作成し，通信中に元の情報が改ざんされた場合にはそのコードも異なるようになっています。

本装置では, 使用する MAC はコンフィグレーションコマンド ip ssh macs で設定可能です。

3. 構成

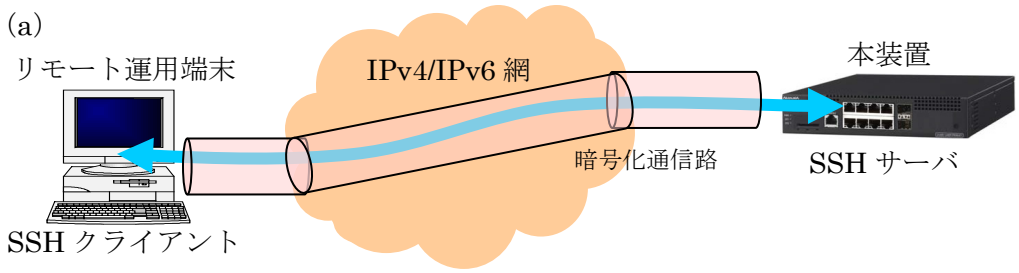
本章では SSH の接続構成を示します。

3.1　SSH の接続構成

本装置の SSH 機能を利用するための接続構成例を図 3.1-1に示します。

(a)　リモート運用端末から SSH クライアントを使用して本装置へ接続する例

図 3.1-1　SSH 機能利用のネットワーク構成例



各端末間は暗号化通信路が生成されますので，安全な通信が可能です。安全な通信路上で，「1.2 機能概要」で紹介しました SSH の各種機能がご利用になれます。

4. 収容条件

本章では SSH 固有の収容条件を示します。

4.1 SSH サーバへの接続ユーザ数

SSH サーバへの接続ユーザ数の最大数は，コンフィグレーションコマンド line vty で設定する最大ログインユーザ数となります。また，最大ログインユーザ数は，SSH サーバへの接続数(SSH セキュアリモートログインでの接続数)だけでなく，telnet で接続しているユーザ数も合わせた数となります。

表 4.1-1 各リモートアクセスの接続条件

項目		リモートアクセス種別					
		ssh		sftp		telnet	ftp
		パスワード	公開鍵	パスワード	公開鍵		
最大ログインユーザ数		16 ※1		1 ※2		16 ※1	1 ※2
ユーザアカウント	ローカル	○	○	○	○	○	○
	RADIUS	○	×	○	×	○	○
ユーザパスワード		必須	－	必須	－	△	△
ワンタイムパスワード認証		×		×		○	×
ログインタイムアウト時間		60 分		※3		60 分	30 分

（凡例）○：接続可　×：接続不可　－：対象外　△：未指定でも接続可

※１：最大ログインユーザ数は ssh と telnet の総和

※２：sftp と ftp は同時接続可能

※３：未サポート

［注意事項］

SSH クライアント側から Rekey 要求が送信されても，本装置は拒否します。SSH クライアント側で Rekey 要求を送信しないように設定してください。

(1) スタック動作時のログイン数について

スタック動作時のログイン数は，マスタ以外のメンバスイッチのコンソールログイン数も含めてスタック全体で最大 4 となります。ログイン数の範囲を次の表に示します。

表 4.1-2 スタック動作時のログイン数の範囲

ログイン種別	コンフィグレーションコマンド line vty で設定したログイン数	スタック全体のログイン数（最大４）
telnet/ssh によるリモートログイン	含まれる	含まれる
マスタ以外のメンバスイッチのコンソールログイン	含まれない	
マスタスイッチのコンソールログイン	含まれない	含まれない
ftp/sftp によるリモートログイン		

4.2 SSH サーバへのユーザ公開鍵の登録

本装置の SSH サーバへ接続するユーザが公開鍵認証を利用する場合は，ユーザ名と，該当ユーザのユーザ公開鍵の登録を行ってください。

公開鍵認証を用いる際の登録できるユーザ数，ユーザ公開鍵数，ユーザ公開鍵の種類を以下に示します。

(1) 登録が有効になる公開鍵認証ユーザ数
装置あたり 10 ユーザ

(2) 登録可能なユーザ公開鍵数
1 ユーザあたり 10 個

表 4.2-1に，登録できるユーザ公開鍵の種類を示します。

表 4.2-1 登録可能なユーザ公開鍵の種類

SSHプロトコル	公開鍵アルゴリズム ※1	bit数 ※2	公開鍵種別
SSHv1	RSA	512～2560	SSHv1形式
SSHv2	RSA (ssh-rsa)	512～5120	SECSH形式 ※3
			OpenSSH形式
	DSA (ssh-dss)	512～1536	SECSH形式 ※3
			OpenSSH形式

※1 ：公開鍵アルゴリズム: draft-ietf-secsh-transport-15.txt
※2 ：鍵にコメントが含まれない場合の bit 数です。
(コメントと鍵の部分を合わせて 900 文字までの鍵が登録できます。)
※3 ：SECSH 形式: draft-ietf-secsh-publickeyfile-03.txt

4.3　運用時の注意事項

4.3.1　　多国語 SSH クライアントの制限

一部の多国語(日本語など)クライアントでは，サーバへ ASCII 文字以外(日本語文字など)でエラーメッセージを送付する場合がありますので，できるだけ ASCII 文字でエラーメッセージを送付するクライアントをご利用ください。

コンフィグレーションガイド編

5. SSH サーバ機能の設定ガイド

本章では SSH のサーバ機能のコンフィグレーション設定例を示します。

5.1　SSH サーバの基本設定（ローカルパスワード認証）

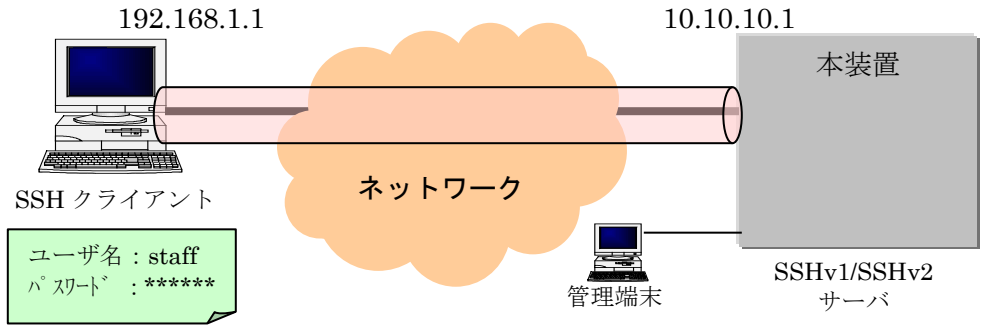
(1) 設定内容の概要

もっとも手軽に SSH を利用して暗号化通信を行うには, telnet と同じパスワード認証を利用します。この場合でも，telnet と違い，ユーザ名やパスワードは暗号化されて送付されますので，外部に漏洩することはありません。ここでは，ローカルパスワード認証を使用した場合の SSH サーバの設定例を示します。

(2) 構成図と設定条件

SSH クライアントからネットワークを介して本装置へ接続する構成とします(図 5.1-1)。

図 5.1-1　SSH サーバの基本設定 構成図



［設定条件］

本装置の SSH サーバ
- IP アドレス　　10.10.10.1
- SSHv1 と SSHv2 で接続可能とする（デフォルト動作）
- パスワード認証を使用し，公開鍵認証も許可する（デフォルト動作）

SSH クライアント
- IP アドレス　　192.168.1.1

ログインのための情報
- ユーザ名　　staff
- パスワード　　******

なお，本装置－SSH クライアント間はあらかじめ通信設定を行い，通信できることとします。

(3) ユーザの登録

管理端末上から，装置管理者モードの運用コマンド adduser を使用して，ユーザ staff とパスワードを設定し，ログインユーザアカウントを作成してください。なお，パスワードを設定していないユーザは SSH のパスワード認証でログインできません。

```
> enable
```

```
# adduser staff
User(empty password) add done. Please setting password.
Changing local password for staff.
New password:******
Retype new password:******
#
```

(4) コンフィグレーション設定

管理端末から，コンフィグレーションコマンドで SSH サーバを動作させる設定を行います。

［コマンド設定例］

解説番号　　入力コマンド

```
1    (config)# ip ssh
2    (config)# line vty 0 1
```

表 5.1-1　本装置の設定解説

解説番号	解説
1	SSH サーバの動作を開始させます。
2	本装置へログインするユーザ数を２とします。

［設定内容の表示］

```
(config)# show
 (中略)
line vty 0 1
!
 (中略)
ip ssh
!
```

(5) 動作確認

SSH クライアントから，本装置(10.10.10.1)へ接続し，ユーザ：staff，パスワード：******で認証されログインできることを確認してください。

5.2　SSHv2 サーバで公開鍵認証を行う設定（SECSH 鍵－方法 1）

(1) 設定内容の概要

パスワード認証より安全に，SSH を利用して認証を行うには，公開鍵認証を利用します。これはパスワード認証と違い，パスワード自体がネットワーク上を流れません。従って，たとえ，暗号が解読されたとしてもパスワードが外部に漏洩することはありません。

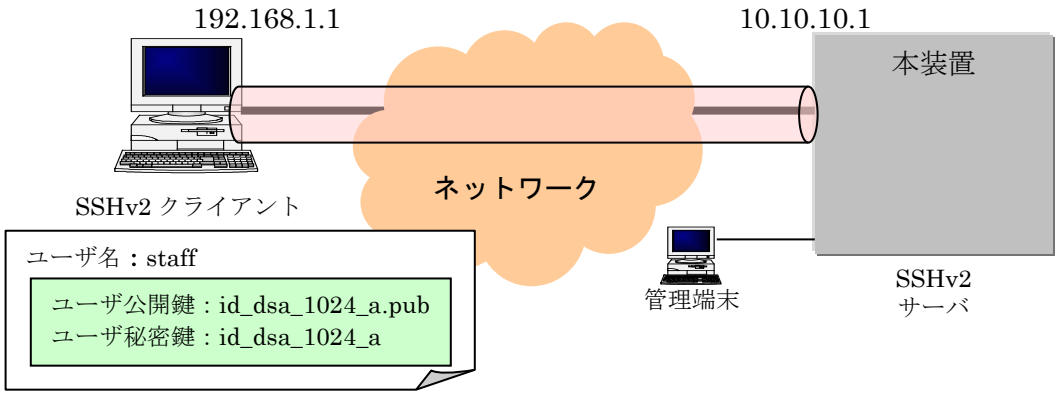
ここでは，クライアントで作成したユーザ鍵ペアのうち，ユーザ公開鍵を本装置の SSH サーバへ登録し公開鍵認証を行う設定を行います。ユーザ公開鍵の登録はコンフィグレーションコマンドで行いますが，方法 1 では，あらかじめクライアントより，ユーザ公開鍵ファイルを本装置へ転送しておきます。そして，そのユーザ公開鍵ファイルをコンフィグレーションコマンドで読み込み登録します。

本例では SECSH 形式の SSHv2 DSA のユーザ公開鍵で説明していますが，SECSH 形式の SSHv2 RSA のユーザ公開鍵も同様な方法で登録ができます。

(2) 構成図と設定条件

SSH クライアントからネットワークを介して本装置へ接続する構成とします(図 5.2-1)。

図 5.2-1　SSHv2 サーバで公開鍵認証を行う設定（SECSH 鍵－方法 1）構成図



［設定条件］

本装置の SSH サーバ
- IP アドレス　　10.10.10.1
- SSHv2 でだけ接続可能とする
- 公開鍵認証を使用し，パスワード認証も許可する（デフォルト動作）
- SECSH 形式の SSHv2 DSA のユーザ公開鍵を登録する

SSHv2 クライアント
- IP アドレス　　192.168.1.1

ログインのための情報
- ユーザ名　　staff
- ユーザ公開鍵　　id_dsa_1024_a.pub
- ユーザ秘密鍵　　id_dsa_1024_a

} ユーザ鍵ペア(クライアント側で予め作成し，公開鍵認証に使えるように登録する)

なお，本装置－SSH クライアント間はあらかじめ通信設定を行い，通信できることとします。

(3) ユーザの登録

管理端末から，装置管理者モードの運用コマンド adduser を使用して，ユーザ staff とパスワードを設定し，ログインユーザアカウントを作成してください。

```
> enable
# adduser staff
User(empty password) add done. Please setting password.
Changing local password for staff.
New password:******
Retype new password:******
#
```

(4) ユーザ公開鍵の転送

クライアント側でユーザ鍵ペアをあらかじめ用意します[ご使用の SSH クライアントソフトの鍵生成ツール(UNIX 系の SSH ソフトでは ssh-keygen コマンド)を用いて生成します]。本装置で,「5.1 SSHサーバの基本設定（ローカルパスワード認証)」の SSH 基本設定を行い，本装置の SSH サーバにクライアントからパスワード認証で接続可能に設定します。

5.1章の設定例：

```
(config)# ip ssh
(config)# line vty 0 1
```

クライアントから sftp で本装置にユーザ公開鍵(id_dsa_1024_a.pub)を転送します。転送したファイルは本装置の RAMDISK に一時保存されます。

```
$ sftp staff@10.10.10.1
Connecting to 10.10.10.1...
staff@10.10.10.1's password:  *** パスワード認証 ***
sftp> put id_ietf_dsa.pub
Uploading id_ietf_dsa.pub to /ramdisk/id_ietf_dsa.pub
id_ietf_dsa.pub                               100%  693     x.xKB/s   00:00
sftp> ls
id_ietf_dsa.pub
sftp> bye      ***  転送完了 ***
```

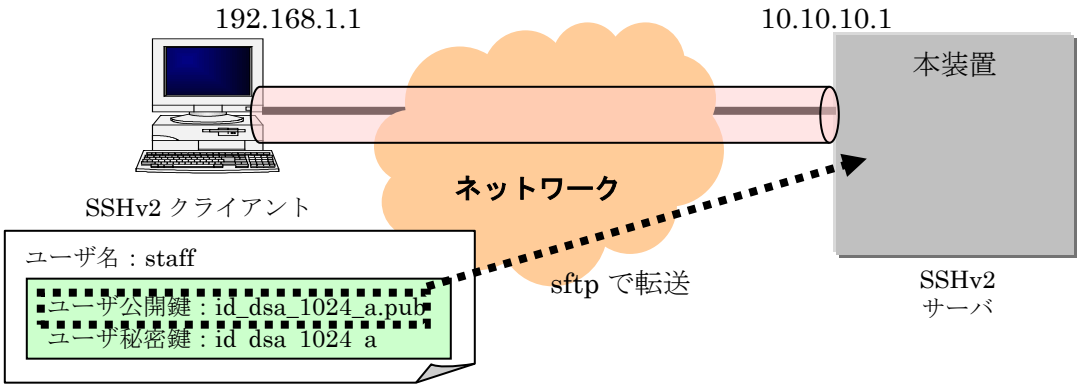
[ご参考]

ユーザ公開鍵の転送は ftp を用いても可能ですが，通信途中での改ざん等セキュリティ上好ましくありませんので，sftp を使用することをお勧めします。

[注意事項]

転送先の RAMDISK は一時保存エリアです。装置の再起動で RAMDISK 上のファイルは消去されますのでご注意ください。

図 5.2-2　ユーザ公開鍵（SECSH 鍵）の転送



(5) コンフィグレーション設定

管理端末から，コンフィグレーションコマンドで SSH サーバの設定変更と，ユーザ公開鍵の登録を行います。

［コマンド設定例］

解説番号　　入力コマンド

```
1    (config)# ip ssh version 2
2    (config)# ip ssh authkey staff client-v2 load-key-file id_dsa_1024_a.pub
```

表 5.2-1　本装置の設定解説

解説番号	解説
1	SSH サーバのプロトコルバージョン 2 だけサポートとします。
2	ユーザ: staff の SSHv2 のユーザ公開鍵を RAMDISK 上のファイル id_dsa_1024_a.pub から読み込みます。この時，この鍵の名前(インデックス名)を client-v2 とします。コンフィグレーションにはユーザ公開鍵の内容が設定されます。

［設定内容の表示］

```
(config)# show
line vty 0 1
!
 (中略)
ip ssh
ip ssh version 2
ip ssh authkey staff client-v2 "AAAAB3NzaC1kc3MAAACBAPQX4hUjicV2cuSbbOeYug3
```

```
Zwe1wdveLixNAcRX15dh8XDDIv1drKW6LnxTDiM8wfsEPDoOCOZwae9VOLgpBFXqdNAHlBSPeKV
EUvSBah+romEWRuPgBHIkJWg3FbzkHV8cYiQxzAZT87RunikN9j2kq+ftoJIs7IWR4gHXby/JTA
AAAFQDTl3fYwEZaZEF1ZATkUeLsaBnn/wAAAIEAhy3mVaF87Pjjbaq+XY+l2mjIOptqGb7KcTKv
bfb2JZVscidxzOaKnNWRMJtsZSyMXkpdEjaWNmQvbV6MDGn3PYX63CLomIsWUPxdo7bcOJFyx1G
vZ4bef7JTP9xO48/lFSwQTL7bKeXZ9cidgGXMmch8Tz15WSu8rP+t3m/yS7gAAACAZ/yWFB1rl8
BeNkvcsmilupce2hb2uaef/4I7ymPT9irDQsfRY3RxiG5KOUh7g84j9WFtx/y9KtFk46hUizNYn
kkVcEwjo1uTbhtRpehFObUYPyQu+ZxFDHZ3vB1oONOfaOU4xME18RC4CHax+Fm/OUMdPzpzAD6F
ZHS+9zkdi7k="
!
（中略）
```

(6) 動作確認

SSHv2 クライアントから，本装置(10.10.10.1)へ接続し，ユーザ名 staff，秘密鍵(id_dsa_1024_a)にパスフレーズを入力して，公開鍵認証で認証されログインできることを確認してください。

5.3　SSHv2 サーバで公開鍵認証を行う設定（SECSH 鍵－方法 2）

(1) 設定内容の概要

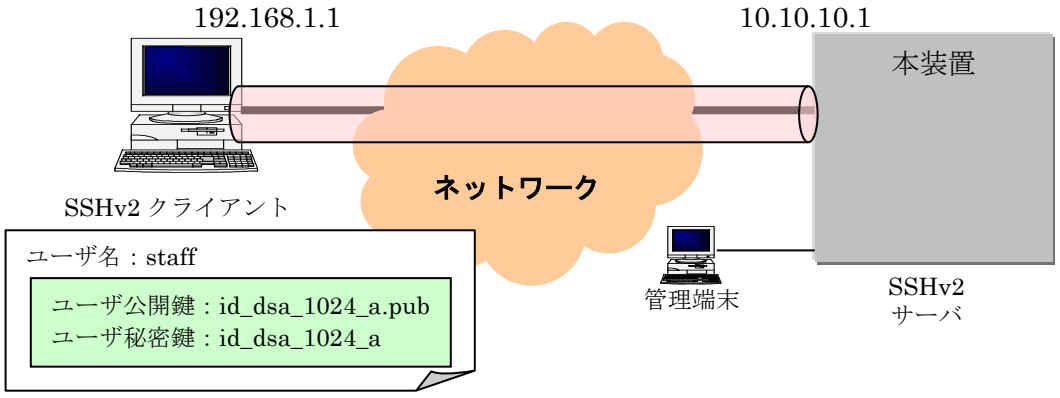
ここでは，公開鍵認証を行うために，クライアントで作成したユーザ鍵ペアのうち，ユーザ公開鍵を本装置の SSH サーバへ登録します。ユーザ公開鍵の登録はコンフィグレーションコマンドで行いますが，方法 2 では，ユーザ公開鍵ファイルの内容をコンフィグレーションコマンドで直接入力し，設定登録します。

本例では SECSH 形式の SSHv2 DSA のユーザ公開鍵で説明していますが，SECSH 形式の SSHv2 RSA のユーザ公開鍵も同様な方法で登録ができます。

(2) 構成図と設定条件

SSHv2 クライアントからネットワークを介して本装置へ接続する構成とします(図 5.3-1)。

図 5.3-1　SSHv2 サーバで公開鍵認証を行う設定(SECSH 鍵－方法 2）構成図



［設定条件］

本装置の SSH サーバ
- IP アドレス　　10.10.10.1
- SSHv2 でだけ接続可能とする
- 公開鍵認証だけを使用する
- SECSH 形式の SSHv2 DSA のユーザ公開鍵を登録

SSHv2 クライアント
- IP アドレス　　192.168.1.1

ログインのための情報
- ユーザ名　　staff
- ユーザ公開鍵　id_dsa_1024_a.pub
- ユーザ秘密鍵　id_dsa_1024_a

} ユーザ鍵ペア(クライアント側で予め作成し，公開鍵認証に使えるように登録する)

なお，本装置－SSH クライアント間はあらかじめ通信設定を行い，通信できることとします。

(3) ユーザの登録

管理端末から，装置管理者モードの運用コマンド adduser を使用して，ユーザ staff とパスワードを設定し，ログインユーザアカウントを作成してください。

```
> enable
# adduser staff
User(empty password) add done. Please setting password.
Changing local password for staff.
New password:******
Retype new password:******
#
```

(4) ユーザ公開鍵の準備

クライアント側でユーザ鍵ペアをあらかじめ用意します[ご使用の SSH クライアントソフトの鍵生成ツール(UNIX 系の SSH ソフトでは ssh-keygen コマンド)を用いて生成します]。まず，管理端末上でクライアントのユーザ公開鍵内容を準備します(図 5.3-2)。本例では，SECSH 形式の SSHv2 DSA ユーザ公開鍵を例に説明します。

図 5.3-2　準備したユーザ公開鍵（SECSH 鍵）内容

```
---- BEGIN SSH2 PUBLIC KEY ----
Subject: staff
Comment: "1024-bit dsa, staff@client1-pc, Tue Oct 22 2002 16:21:35 +09¥
00"
AAAAB3NzaC1kc3MAAACBAPQX4hUjicV2cuSbb0eYug3Zwe1wdveLixNAcRX15dh8XDDIv1
drKW6LnxTDiM8wfsEPDoOC0Zwae9V0LgpBFXqdNAHlBSPeKVEUvSBah+romEWRuPgBHIkJ
Wg3FbzkHV8cYiQxzAZT87RunikN9j2kq+ftoJIs7IWR4gHXby/JTAAAAFQDTl3fYwEZaZE
F1ZATkUeLsaBnn/wAAAIEAhy3mVaF87Pjjbaq+XY+l2mjIOptqGb7KcTKvbfb2JZVscidx
zOaKnNWRMJtsZSyMXkpdEjaWNmQvbV6MDGn3PYX63CLomIsWUPxdo7bcOJFyx1GvZ4bef7
JTP9x048/lFSwQTL7bKeXZ9cidgGXMmch8Tz15WSu8rP+t3m/yS7gAAACAZ/yWFB1rl8Be
NkvcsmilupCe2hb2uaef/4I7ymPT9irDQsfRY3RxiG5K0Uh7g84j9WFtx/y9KtFk46hUiz
NYnkkVcEwjo1uTbhtRpehF0bUYPyQu+ZxFDHZ3vBlo0NOfa0U4xME18RC4CHax+Fm/OUMd
PzpzAD6FZHS+9zkdi7k=
---- END SSH2 PUBLIC KEY ----
```

(5) コンフィグレーション設定

次に，管理端末から，先ほど準備したユーザ公開鍵の内容をコンフィグレーションコマンドで入力(コピーアンドペースト)します。コンフィグレーションコマンドでユーザ公開鍵の内容を直接入力する場合は，SECSH 形式のユーザ公開鍵のヘッダ(Comment:コメント等)，開始・終了マーカおよび改行コードを含めないよう，登録するユーザ公開鍵内容の形式は次のようにします。

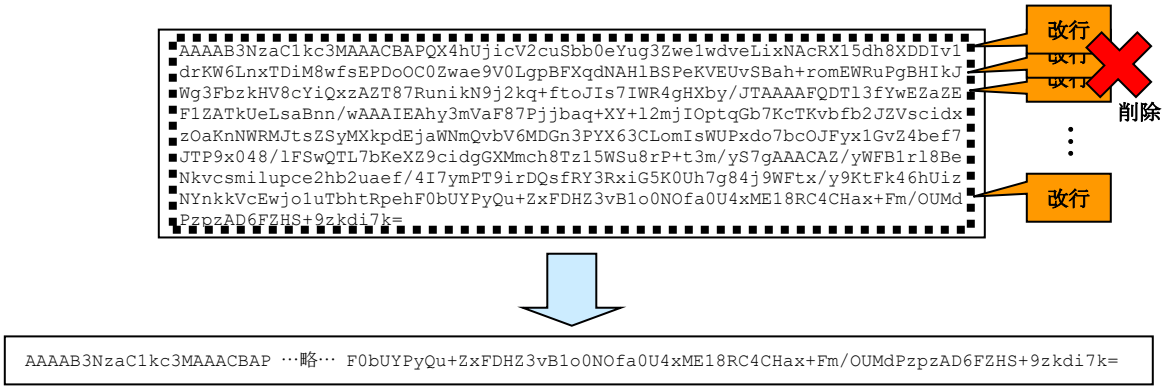
1．ヘッダ，開始･終了マーカを除いた，鍵の部分だけを取り出します(図 5.3-3 点線部分)。

図 5.3-3　ユーザ公開鍵（SECSH 鍵）の入力部分

```
---- BEGIN SSH2 PUBLIC KEY ----
Subject: staff
Comment: "1024-bit dsa, staff@client1-pc, Tue Oct 22 2002 16:21:35 +09¥
00"
AAAAB3NzaC1kc3MAAACBAPQX4hUjicV2cuSbb0eYug3Zwe1wdveLixNAcRX15dh8XDDIv1
drKW6LnxTDiM8wfsEPDoOC0Zwae9V0LgpBFXqdNAHlBSPeKVEUvSBah+romEWRuPgBHIkJ
Wg3FbzkHV8cYiQxzAZT87RunikN9j2kq+ftoJIs7IWR4gHXby/JTAAAAFQDTl3fYwEZaZE
F1ZATkUeLsaBnn/wAAAIEAhy3mVaF87Pjjbaq+XY+l2mjIOptqGb7KcTKvbfb2JZVscidx
zOaKnNWRMJtsZSyMXkpdEjaWNmQvbV6MDGn3PYX63CLomIsWUPxdo7bcOJFyx1GvZ4bef7
JTP9x048/lFSwQTL7bKeXZ9cidgGXMmch8Tz15WSu8rP+t3m/yS7gAAACAZ/yWFB1rl8Be
NkvcsmilupCe2hb2uaef/4I7ymPT9irDQsfRY3RxiG5K0Uh7g84j9WFtx/y9KtFk46hUiz
NYnkkVcEwjo1uTbhtRpehF0bUYPyQu+ZxFDHZ3vBlo0NOfa0U4xME18RC4CHax+Fm/OUMd
PzpzAD6FZHS+9zkdi7k=
---- END SSH2 PUBLIC KEY ----
```

２．SECSH 形式のユーザ公開鍵は改行コードを含んでいるため，すべての改行を取り除き 1 行形式にします(図 5.3-4)。

図 5.3-4　ユーザ公開鍵（SECSH 鍵）の改行除去



注意事項：変換後のユーザ公開鍵の部分に空白を含めないでください。空白の後はコメントとみなされます。

登録するユーザ公開鍵を準備できましたら，管理端末から，コンフィグレーションコマンドで SSH サーバの諸設定と，ユーザ公開鍵の登録を行います。

［コマンド設定例］

解説番号	入力コマンド
1	(config)# ip ssh
2	(config)# ip ssh version 2
3	(config)# ip ssh authentication publickey
4	(config)# ip ssh authkey staff client-v2 “AAAAB3NzaC1kc3MAAACBAPQX4hUjicV2cuSbb0eYug3Zwe1wdveLixNAcRX15dh8XDDIv1drKW6LnxTDiM8wfsEPDoOC0Zwae9V0LgpBFXqdNAHlBSPeKVEUvSBah+romEWRuPgBHIkJWg3FbzkHV8cYiQxzAZT87RunikN9j2kq+ftoJIs7IWR4gHXby/JTAAAAFQDTl3fYwEZaZEF1ZATkUeLsaBnn/wAAAIEAhy3mVaF87Pjjbaq+XY+l2mjIOptqGb7KcTKvbfb2JZVscidxzOaKnNWRMJtsZSyMXkpdEjaWNmQvbV6MDGn3PYX63CLomIsWUPxdo7bcOJFyx1GvZ4bef7JTP9x048/lFSwQTL7bKeXZ9cidgGXMmch8Tz15WSu8rP+t3m/yS7gAAACAZ/yWFB1rl8BeNkvcsmilupce2hb2uaef/4I7ymPT9irDQsfRY3RxiG5K0Uh7g84j9WFtx/y9KtFk46hUizNYnkkVcEwjo1uTbhtRpehF0bUYPyQu+ZxFDHZ3vB1o0NOfa0U4xME18RC4CHax+Fm/OUMdPzpzAD6FZHS+9zkdi7k=”
5	(config)# line vty 0 1

表 5.3-1　本装置の設定解説

解説番号	解説
1	SSH サーバの動作を開始させます。
2	SSH サーバのプロトコルバージョン 2 だけサポートとします。
3	許可するユーザ認証方式を公開鍵認証だけとします。
4	ユーザ:staff の準備した SECSH 形式の SSHv2 ユーザ公開鍵を途中で改行しないように，””で囲んで入力します。この時，このユーザ公開鍵の名前(インデックス名)を client-v2 とします。
5	本装置へログインするユーザ数を２とします。

［設定内容の表示］

```
(config)# show
 (中略)
line vty 0 1
!
 (中略)
ip ssh
ip ssh version 2
ip ssh authentication publickey
ip ssh authkey staff client-v2 "AAAAB3NzaC1kc3MAAACBAPQX4hUjicV2cuSbbOeYug3
Zwe1wdveLixNAcRX15dh8XDDIv1drKW6LnxTDiM8wfsEPDoOCOZwae9VOLgpBFXqdNAHlBSPeKV
EUvSBah+romEWRuPgBHIkJWg3FbzkHV8cYiQxzAZT87RunikN9j2kq+ftoJIs7IWR4gHXby/JTA
AAAFQDTl3fYwEZaZEF1ZATkUeLsaBnn/wAAAIEAhy3mVaF87Pjjbaq+XY+l2mjIOptqGb7KcTKv
bfb2JZVscidxzOaKnNWRMJtsZSyMXkpdEjaWNmQvbV6MDGn3PYX63CLomIsWUPxdo7bcOJFyx1G
vZ4bef7JTP9xO48/lFSwQTL7bKeXZ9cidgGXMmch8Tz15WSu8rP+t3m/yS7gAAACAZ/yWFB1rl8
BeNkvcsmilupce2hb2uaef/4I7ymPT9irDQsfRY3RxiG5KOUh7g84j9WFtx/y9KtFk46hUizNYn
kkVcEwjo1uTbhtRpehFObUYPyQu+ZxFDHZ3vB1oONOfaOU4xME18RC4CHax+Fm/OUMdPzpzAD6F
ZHS+9zkdi7k="
!
```

(6) 動作確認

SSHv2 クライアントから，本装置(10.10.10.1)へ SSHv2 で接続し，ユーザ名 staff，ユーザ秘密鍵(id_dsa_1024_a)にパスフレーズを入力して，公開鍵認証で認証されログインできることを確認してください。

5.4　SSHv2 サーバで公開鍵認証を行う設定（OpenSSH 鍵ー方法 1）

(1) 設定内容の概要

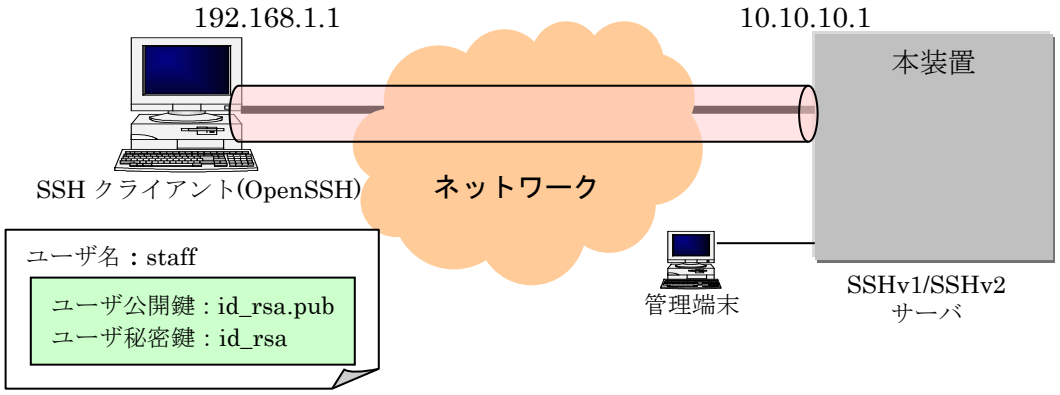
ここでは, OpenSSH クライアントで作成したユーザ鍵ペアのうち, ユーザ公開鍵を本装置の SSH サーバへ登録し公開鍵認証を行う設定を行います。ユーザ公開鍵の登録はコンフィグレーションコマンドで行いますが，方法 1 では，あらかじめクライアントより，ユーザ公開鍵ファイルを本装置へ転送しておきます。そして，そのユーザ公開鍵ファイルをコンフィグレーションコマンドで読み込み，登録します。

本例では OpenSSH の SSHv2 RSA ユーザ公開鍵で説明していますが, OpenSSH の SSHv2 DSA ユーザ公開鍵も同様の手順で登録できます。

(2) 構成図と設定条件

OpenSSH クライアントからネットワークを介して本装置へ接続する構成とします(図 5.4-1)。

図 5.4-1　SSHv2 サーバで公開鍵認証を行う設定（OpenSSH 鍵ー方法 1）構成図



［設定条件］

本装置の SSH サーバ
- IP アドレス　10.10.10.1
- SSHv1 と SSHv2 で接続可能とする（デフォルト動作）
- 公開鍵認証を使用し，パスワード認証も許可する（デフォルト動作）
- OpenSSH 形式の SSHv2 RSA ユーザ公開鍵を登録する

SSHv1 クライアント
- IP アドレス　192.168.1.1

ログインのための情報
- ユーザ名　staff
- ユーザ公開鍵　id_rsa.pub
- ユーザ秘密鍵　id_rsa

} ユーザ鍵ペア(クライアント側で予め作成し，公開鍵認証に使えるように登録する)

なお，本装置ーSSH クライアント間はあらかじめ通信設定を行い，通信できることとします。

(3) ユーザの登録

サーバ側で，管理端末から，装置管理者モードの運用コマンド adduser を使用して，ユーザ staff とパスワードを設定し，ログインユーザアカウントを作成してください。

```
> enable
# adduser staff
User(empty password) add done. Please setting password.
Changing local password for staff.
New password:******
Retype new password:******
#
```

(4) ユーザ公開鍵の転送

クライアント側でユーザ鍵ペアをあらかじめ用意します[ご使用の SSH クライアントソフトの鍵生成ツール(UNIX 系の SSH ソフトでは ssh-keygen コマンド)を用いて生成します]。本装置で,「5.1 SSHサーバの基本設定（ローカルパスワード認証)」の SSH 基本設定を行い，本装置の SSH サーバにクライアントからパスワード認証で接続可能に設定します。

5.1章の設定例：

```
(config)# ip ssh
(config)# line vty 0 1
```

クライアントから sftp で本装置にユーザ公開鍵(id_rsa.pub)を転送します。転送したファイルは本装置の RAMDISK に一時保存されます。

```
$ sftp staff@10.10.10.1
Connecting to 10.10.10.1...
staff@10.10.10.1's password:  *** パスワード認証 ***
sftp> put id_rsa.pub
Uploading id_rsa.pub to /ramdisk/id_rsa.pub
id_rsa.pub                                    100%  224     x.xKB/s   00:00
sftp> ls
id_rsa.pub
sftp> bye      ***  転送完了 ***
```

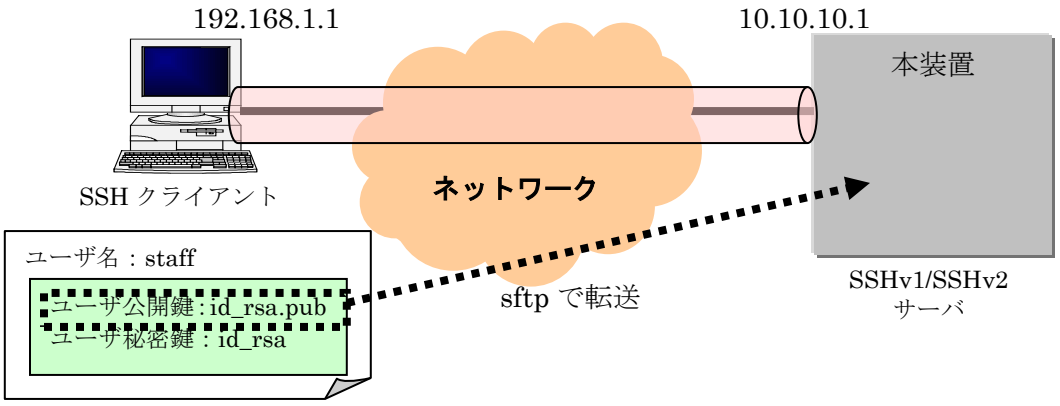
[ご参考]

ユーザ公開鍵の転送は ftp を用いても可能ですが，通信途中での改ざん等セキュリティ上好ましくありませんので，sftp を使用することをお勧めします。

[注意事項]

転送先の RAMDISK は一時保存エリアです。装置の再起動で RAMDISK 上のファイルは消去されますのでご注意ください。

図 5.4-2　ユーザ公開鍵（OpenSSH 鍵）の転送



(5) コンフィグレーション設定

管理端末から，コンフィグレーションコマンドでユーザ公開鍵の登録を行います。

［コマンド設定例］

解説番号　　入力コマンド

1　(config)# ip ssh authkey staff client-0 load-key-file id_rsa.pub

表 5.4-1　本装置の設定解説

解説番号	解説
1	ユーザ:staff の SSHv2 のユーザ公開鍵を RAMDISK 上のファイル id_rsa.pub から読み込みます。この時，この鍵の名前(インデックス名：任意文字列)を client-0 とします。OpenSSH 形式のユーザ公開鍵の場合でも，SECSH 形式のユーザ公開鍵と同様に登録することが可能です。なお，コンフィグレーション情報にはユーザ公開鍵の鍵内容が設定されます。

［設定内容の表示］

```
(config)# show
 (中略)
line vty 0 1
!
 (中略)
ip ssh
ip ssh authkey staff client-0 "AAAAB3NzaC1yc2EAAAABIwAAAIEAnvn2OcoFEScIfM4S
5q8T6/IN+ZzNpWE9q+mgpTB7OAMy6nOVhoi5ovQKyAwn44E4n1CrXY6dPIB9HfHkwPOBK3F6xsP
wu66rpQ8CNkZdo4TiAiAqJgORlUZsHZWi1pcVg4eGY+R31fPFCmbGSxask97cCWCRwhNoffsjHR
nn5hE= staff@OpenSSH-Client"
!
```

(6) 動作確認

OpenSSH クライアントから，本装置(10.10.10.1)へ接続し，ユーザ名 staff，秘密鍵(id_rsa)にパスフレーズを入力して，公開鍵認証で認証されログインできることを確認してください。

5.5　SSHv2 サーバで公開鍵認証を行う設定（OpenSSH 鍵ー方法 2）

(1) 設定内容の概要

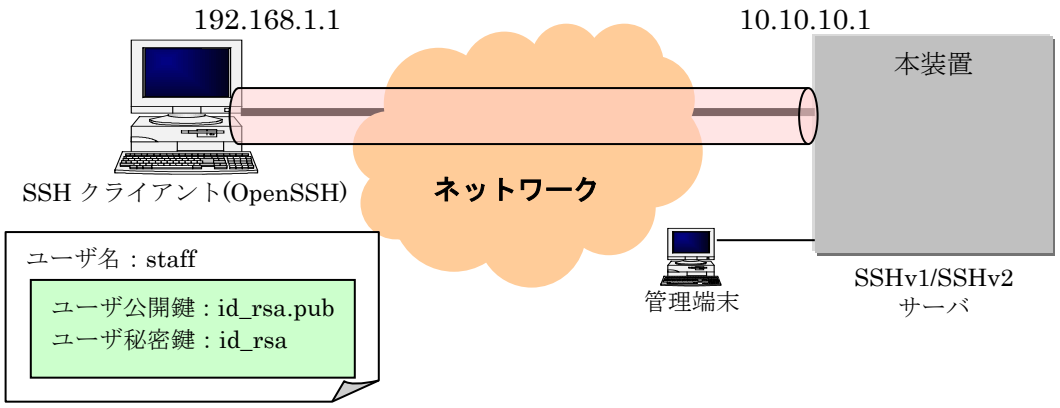
ここでは，公開鍵認証を行うために，OpenSSH クライアントで作成したユーザ鍵ペアのうち，ユーザ公開鍵を本装置の SSH サーバへ登録します。ユーザ公開鍵の登録はコンフィグレーションコマンドで行いますが，方法 2 では，ユーザ公開鍵ファイルの内容をコンフィグレーションコマンドで直接入力し，設定登録します。

本例では OpenSSH の SSHv2 RSA ユーザ公開鍵で説明していますが，OpenSSH の SSHv2 DSA ユーザ公開鍵も同様の手順で登録できます。

(2) 構成図と設定条件

SSH クライアントからネットワークを介して本装置へ接続する構成とします(図 5.5-1)。

図 5.5-1　SSHv2 サーバで公開鍵認証を行う設定（OpenSSH 鍵ー方法 2）構成図



［設定条件］

本装置の SSH サーバ
- IP アドレス　　10.10.10.1
- SSHv1 と SSHv2 で接続可能とする（デフォルト動作）
- 公開鍵認証を使用し，パスワード認証も許可する（デフォルト動作）
- OpenSSH 形式の SSHv2 RSA ユーザ公開鍵を登録する

SSHv2 クライアント
- IP アドレス　　192.168.1.1

ログインのための情報
- ユーザ名　　staff
- ユーザ公開鍵　id_rsa.pub
- ユーザ秘密鍵　id_rsa

} ユーザ鍵ペア(クライアント側で予め作成し，公開鍵認証に使えるように登録する)

なお，本装置ーSSH クライアント間はあらかじめ通信設定を行い，通信できることとします。

(3) ユーザの登録

サーバ側で，管理端末から，装置管理者モードの運用コマンド adduser を使用して，ユーザ staff とパスワードを設定し，ログインユーザアカウントを作成してください。

```
> enable
# adduser staff
User(empty password) add done. Please setting password.
Changing local password for staff.
New password:******
Retype new password:******
#
```

(4) ユーザ公開鍵の準備

クライアント側でユーザ鍵ペアをあらかじめ用意します[ご使用の SSH クライアントソフトの鍵生成ツール(UNIX 系の SSH ソフトでは ssh-keygen コマンド)を用いて生成します]。

まず,管理端末上でクライアントのユーザ公開鍵内容を準備します(図 5.5-2)。本例では,OpenSSH 形式の SSHv2 RSA ユーザ公開鍵を例に説明します。

図 5.5-2　準備したユーザ公開鍵（OpenSSH 鍵）の内容

```
ssh-rsa AAAAB3NzaC1yc2EA…略…31fPFCmbGSxask97cCWCRwhNoffsjHRnn5hE= staff@OpenSSH-Client
```

(5) コンフィグレーション設定

次に，管理端末から，先ほど準備したユーザ公開鍵の内容をコンフィグレーションコマンドで入力(カットアンドペースト)しますが，コンフィグレーションコマンドで OpenSSH のユーザ公開鍵の内容を直接入力する場合は，先頭の”ssh-rsa”または”ssh-dss”を取り除いて，改行コードを含めないようにします(破線の部分)。

図 5.5-2　入力するユーザ公開鍵（OpenSSH 鍵）の内容

```
ssh-rsa AAAAB3NzaC1yc2EA…略…31fPFCmbGSxask97cCWCRwhNoffsjHRnn5hE= staff@OpenSSH-Client
```

注意事項：ユーザ公開鍵に空白や改行を追加しないように，そのまま 1 行で入力してください。

登録するユーザ公開鍵を準備できましたら，管理端末から，コンフィグレーションコマンドで SSH サーバの諸設定と，ユーザ公開鍵の登録を行います。

[コマンド設定例]

解説番号	入力コマンド
1	(config)# ip ssh
2	(config)# ip ssh authkey staff client-0 “AAAAB3NzaC1yc2EAAAABIwAAAIEAnvn2OcoFEScIfM4S5q8T6/IN+ZzNpWE9q+mgpTB7OAMy6nOVhoi5ovQ

```
                    KyAwn44E4n1CrXY6dPIB9HfHkwPOBK3F6xsPwu66rpQ8CNkZdo4TiAiAqJgORl
                    UZsHZWi1pcVg4eGY+R31fPFCmbGSxask97cCWCRwhNoffsjHRnn5hE= staff@
                    OpenSSH-Client"
3                   (config)# line vty 0 1
```

表 5.5-1　本装置の設定解説

解説番号	解説
1	SSH サーバの動作を開始させます。
2	ユーザ staff の準備した OpenSSH 形式の SSHv2 のユーザ公開鍵を途中で改行しないように，""で囲んで入力します。この時，このユーザ公開鍵の名前(インデックス名：任意文字列)を client-O とします。
3	本装置へログインするユーザ数を 2 とします。

［設定内容の表示］

```
(config)# show
 (中略)
line vty 0 1
!
 (中略)
ip ssh
ip ssh authkey staff client-O "AAAAB3NzaC1yc2EAAAABIwAAAIEAnvn2OcoFESclfM4S
5q8T6/IN+ZzNpWE9q+mgpTB7OAMy6nOVhoi5ovQKyAwn44E4n1CrXY6dPIB9HfHkwPOBK3F6xsP
wu66rpQ8CNkZdo4TiAiAqJgORlUZsHZWi1pcVg4eGY+R31fPFCmbGSxask97cCWCRwhNoffsjHR
nn5hE= staff@OpenSSH-Client"
!
```

(6) 動作確認

OpenSSH クライアントから，本装置(10.10.10.1)へ SSHv2 で接続し，ユーザ名 staff，ユーザ秘密鍵(id_rsa)にパスフレーズを入力して，公開鍵認証で認証されログインできることを確認してください。

5.6　SSHv1 サーバで公開鍵認証を行う設定（方法 1）

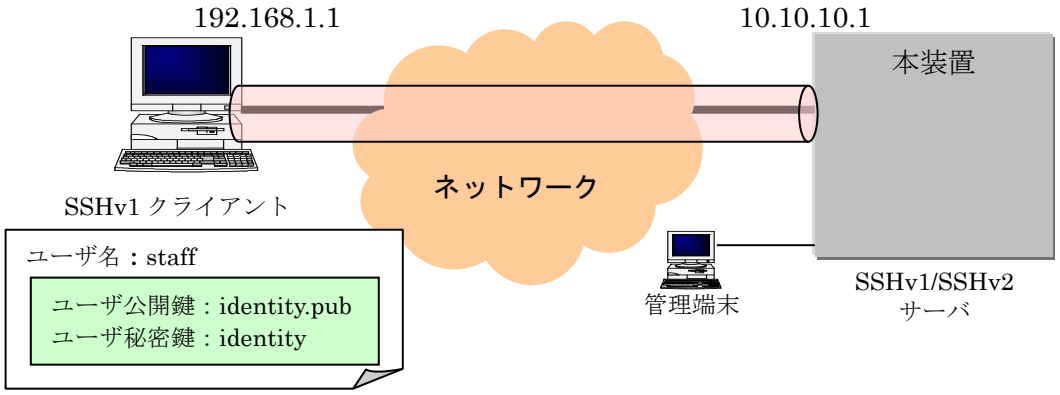
(1) 設定内容の概要

ここでは，SSHv1 クライアントで作成したユーザ鍵ペアのうち，ユーザ公開鍵を本装置の SSH サーバへ登録し公開鍵認証を行う設定を行います。ユーザ公開鍵の登録はコンフィグレーションコマンドで行いますが，方法 1 では，あらかじめクライアントより，ユーザ公開鍵ファイルを本装置へ転送しておきます。そして，そのユーザ公開鍵ファイルをコンフィグレーションコマンドで読み込み，登録します。

(2) 構成図と設定条件

SSHv1 クライアントからネットワークを介して本装置へ接続する構成とします(図 5.6-1)。

図 5.6-1　SSHv1 サーバで公開鍵認証を行う設定（方法 1）　構成図



［設定条件］

本装置の SSH サーバ
- IP アドレス　10.10.10.1
- SSHv1 と SSHv2 で接続可能とする（デフォルト動作）
- 公開鍵認証だけを使用する
- SSHv1 のユーザ公開鍵を登録する

SSHv1 クライアント
- IP アドレス　192.168.1.1

ログインのための情報
- ユーザ名　staff
- ユーザ公開鍵　identity.pub
- ユーザ秘密鍵　identity

} ユーザ鍵ペア(クライアント側で予め作成し，公開鍵認証に使えるように登録する)

なお，本装置－SSH クライアント間はあらかじめ通信設定を行い，通信できることとします。

(3) ユーザの登録

サーバ側で，管理端末から，装置管理者モードの運用コマンド adduser を使用して，ユーザ staff とパスワードを設定し，ログインユーザアカウントを作成してください。

```
> enable
# adduser staff
User(empty password) add done. Please setting password.
Changing local password for staff.
New password:******
Retype new password:******
#
```

(4) ユーザ公開鍵の転送

クライアント側でユーザ鍵ペアをあらかじめ用意します[ご使用の SSH クライアントソフトの鍵生成ツール(UNIX 系の SSH ソフトでは ssh-keygen コマンド)を用いて生成します]。本装置で,「5.1 SSHサーバの基本設定（ローカルパスワード認証)」の SSH 基本設定を行い，本装置の SSH サーバにクライアントからパスワード認証で接続可能に設定します。

5.1章の設定例：

```
(config)# ip ssh
(config)# line vty 0 1
```

クライアントから sftp で本装置にユーザ公開鍵(identity.pub)を転送します。転送したファイルは本装置の RAMDISK に一時保存されます。

```
$ sftp staff@10.10.10.1
Connecting to 10.10.10.1...
staff@10.10.10.1's password:  *** パスワード認証 ***
sftp> put identity.pub
Uploading identity.pub to /ramdisk/ identity.pub
identity.pub                                  100%  335     x.xKB/s   00:00
sftp> ls
identity.pub
sftp> bye      ***  転送完了 ***
```

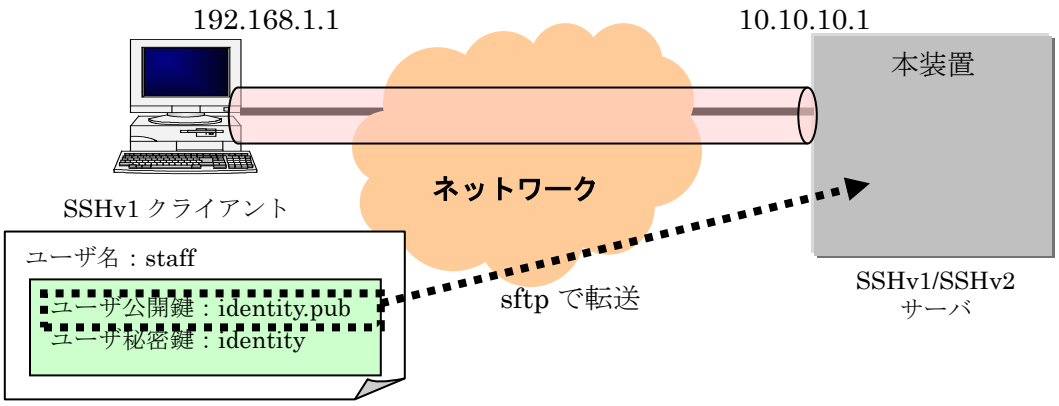
[ご参考]

ユーザ公開鍵の転送は ftp を用いても可能ですが，通信途中での改ざん等セキュリティ上好ましくありませんので， sftp を使用することをお勧めします。

[注意事項]

転送先の RAMDISK は一時保存エリアです。装置の再起動で RAMDISK 上のファイルは消去されますのでご注意ください。

図 5.6-2　ユーザ公開鍵（SSHv1 鍵）の転送



(5) コンフィグレーション設定

管理端末から，コンフィグレーションコマンドで SSH サーバの諸設定変更と，ユーザ公開鍵の登録を行います。

［コマンド設定例］

解説番号　　入力コマンド

```
1    (config)# ip ssh authentication publickey
2    (config)# ip ssh authkey staff client-v1 load-key-file identity.pub
```

表 5.6-1　本装置の設定解説

解説番号	解説
1	許可するユーザ認証方式を公開鍵認証だけに変更します。
2	ユーザ staff の SSHv1 のユーザ公開鍵を RAMDISK 上のファイル identity.pub から読み込みます。この時，この鍵の名前(インデックス名：任意文字列)を client-v1 とします。コンフィグレーションにはユーザ公開鍵の内容が設定されます。

［設定内容の表示］

```
(config)# show
 (中略)
line vty 0 1
!
 (中略)
ip ssh
ip ssh authentication publickey
ip ssh authkey staff client-v1 "1024 37 14753365671206614340722622503227471
```

```
48858464605875741379265771406286026202204808066000898184833007576341412085743012017278333255926087503938106389842066406013975523053044505527699048923555275901272201283612361649060403839474378666756881926343498797135872452602693184152404875769073183479505294230209903141313 97 staff@client"
!
```

(6) 動作確認

SSHv1 クライアントから，本装置(10.10.10.1)へ接続し，ユーザ名 staff，秘密鍵(identity)にパスフレーズを入力して，公開鍵認証で認証されログインできることを確認してください。

5.7　SSHv1 サーバで公開鍵認証を行う設定（方法 2）

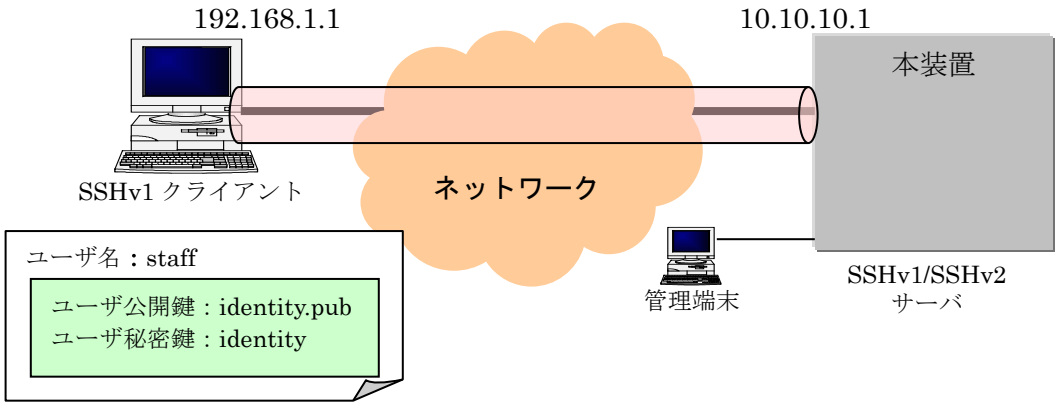
(1) 設定内容の概要

ここでは，公開鍵認証を行うために，SSHv1 クライアントで作成したユーザ鍵ペアのうち，ユーザ公開鍵を本装置の SSH サーバへ登録します。ユーザ公開鍵の登録はコンフィグレーションコマンドで行いますが，方法 2 では，ユーザ公開鍵ファイルの内容をコンフィグレーションコマンドで直接入力し，設定登録します。

(2) 構成図と設定条件

SSH クライアントからネットワークを介して本装置へ接続する構成とします(図 5.7-1)。

図 5.7-1　SSHv1 サーバで公開鍵認証を行う設定（方法 2）　構成図



［設定条件］

本装置の SSH サーバ
- IP アドレス　10.10.10.1
- SSHv1 と SSHv2 で接続可能とする（デフォルト動作）
- 公開鍵認証だけを使用する
- SSHv1 ユーザ公開鍵を登録する

SSHv1 クライアント
- IP アドレス　192.168.1.1

ログインのための情報
- ユーザ名　staff
- ユーザ公開鍵　identity.pub
- ユーザ秘密鍵　identity

} ユーザ鍵ペア(クライアント側で予め作成し，公開鍵認証に使えるように登録する)

なお，本装置－SSH クライアント間はあらかじめ通信設定を行い，通信できることとします。

(3) ユーザの登録

サーバ側で，管理端末から，装置管理者モードの運用コマンド adduser を使用して，ユーザ staff とパスワードを設定し，ログインユーザアカウントを作成してください。

```
> enable
# adduser staff
User(empty password) add done. Please setting password.
Changing local password for staff.
New password:******
Retype new password:******
#
```

(4) ユーザ公開鍵の準備

クライアント側でユーザ鍵ペアをあらかじめ用意します[ご使用の SSH クライアントソフトの鍵生成ツール(UNIX 系の SSH ソフトでは ssh-keygen コマンド)を用いて生成します]。

まず，管理端末上でクライアントの SSHv1 ユーザ公開鍵内容を準備します(図 5.7-2)。

図 5.7-2　準備したユーザ公開鍵（SSHv1 鍵）の内容

```
1024 37 14753365671206…略…184152404875769073183479505294230209903141313 97 staff@client
```

(5) コンフィグレーション設定

次に，管理端末から，先ほど準備したユーザ公開鍵の内容をコンフィグレーションコマンドで入力(カットアンドペースト)しますが，コンフィグレーションコマンドで SSHv1 のユーザ公開鍵の内容を直接入力する場合は，改行コードを含めないようにします。

[注意事項]

ユーザ公開鍵に空白や改行を追加しないように，そのまま 1 行で入力してください。

登録するユーザ公開鍵を準備できましたら，管理端末から，コンフィグレーションコマンドで SSH サーバの諸設定と，ユーザ公開鍵の登録を行います。

[コマンド設定例]

解説番号	入力コマンド
1	(config)# ip ssh
2	(config)# ip ssh authentication publickey
3	(config)# ip ssh authkey staff client-v1 “1024 37 147533656712 066143407226225032274714885846460587574137926577140628602620 2 048080660008981848330075763414120857430120172783332559260875 039381063898420664060139755230530445055276990489235552759012 7 220128361236164906040383947437866675688192634349879713587245 2 602693184152404875769073183479505294230209903141313 97 staff@c

```
lient"
4               (config)# line vty 0 1
```

表 5.7-1　本装置の設定解説

解説番号	解説
1	SSH サーバの動作を開始させます。
2	許可するユーザ認証方式を公開鍵認証だけとします。
3	ユーザ staff の準備した SSHv1 のユーザ公開鍵を途中で改行しないように，””で囲んで入力します。この時，このユーザ公開鍵の名前(インデックス名：任意文字列)を client-v1 とします。
4	本装置へログインするユーザ数を２とします。

［設定内容の表示］

```
(config)# show
（中略）
line vty 0 1
!
（中略）
ip ssh
ip ssh authentication publickey
ip ssh authkey staff client-v1 "1024 37 14753365671206614340722622503227471
48858464605875741379265771406286026202204808066000898184833007576341412085 7
43012017278333255926087503938106389842066406013975523053044505527699048923 5
55275901272201283612361649060403839474378666756881926343498797135872452602 6
93184152404875769073183479505294230209903141313 97 staff@client"
!
```

(6) 動作確認

SSHv1 クライアントから，本装置(10.10.10.1)へ SSHv1 で接続し，ユーザ名 staff，ユーザ秘密鍵(identity)にパスフレーズを入力して，公開鍵認証で認証されログインできることを確認してください。

5.8　SSH サーバの暗号アルゴリズム関連の設定変更

(1) 設定内容の概要

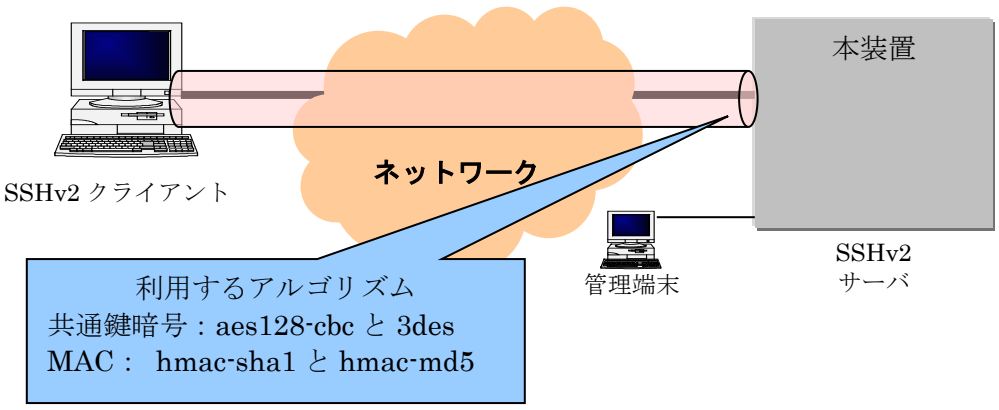
SSH の暗号化通信では共通鍵暗号とメッセージ認証コードが用いられます。本装置の SSH サーバ機能の共通鍵暗号(Cipher)とメッセージ認証コード(MAC)は，複数の種類のアルゴリズムをサポートしています。

ここでは，サポートしている複数のアルゴリズムの中で，使用するアルゴリズムの指定を変更します。使用するアルゴリズムはコンフィグレーションコマンドで設定します。(これらのアルゴリズム指定は SSHv2 でのサポートです。SSHv1 では固定です。)

(2) 構成図と設定条件

SSHv2 クライアントからネットワークを介して本装置へ接続する構成とします(図 5.8-1)。

図 5.8-1　SSHv2 サーバの暗号アルゴリズム関連の設定変更 構成図



［設定条件］

本装置の SSH サーバ

・Cipher(共通鍵暗号)は aes128-cbc と 3des を使用する

・MAC(ﾒｯｾｰｼﾞ認証ｺｰﾄﾞ)は hmac-sha1 と hmac-md5 を使用する

なお，本装置－SSH クライアント間はあらかじめ通信設定を行い，通信できることとします。

また，アカウント作成やパスワード認証(公開鍵認証)の SSHv2 サーバ設定はすでに完了(5.1章， 5.2章，5.3章参照)し，SSHv2 でクライアントからログインできることとします。

(3) コンフィグレーション設定

コンフィグレーションコマンドでアルゴリズムの設定(変更)を行います。

［コマンド設定例］

解説番号　　入力コマンド

```
1    (config)# ip ssh ciphers aes128-cbc 3des
2    (config)# ip ssh macs hmac-sha1 hmac-md5
```

表 5.8-1　本装置の設定解説

解説番号	解説
1	SSH サーバの共通鍵暗号アルゴリズムとして aes128-cbc と 3des だけをサポートします。
2	SSH サーバのメッセージ認証コードアルゴリズムとして hmac-sha1 と hmac-md5 だけをサポートします。

［設定内容の表示］

```
(config)# show
（中略）
ip ssh
ip ssh ciphers aes128-cbc 3des
ip ssh macs hmac-sha1 hmac-md5
!
（中略）
```

(4) 動作確認

SSHv2 クライアントで aes128-cbc または 3des，hmac-sha1 または hmac-md5 を有効にして，本装置へ SSHv2 で接続し，その時に暗号方式が aes128-cbc または 3des であること，MAC 方式が hmac-sha1 または hmac-md5 であることを確認してください。

5.9　RADIUS 認証と連携した SSH サーバの設定

(1) 設定内容の概要

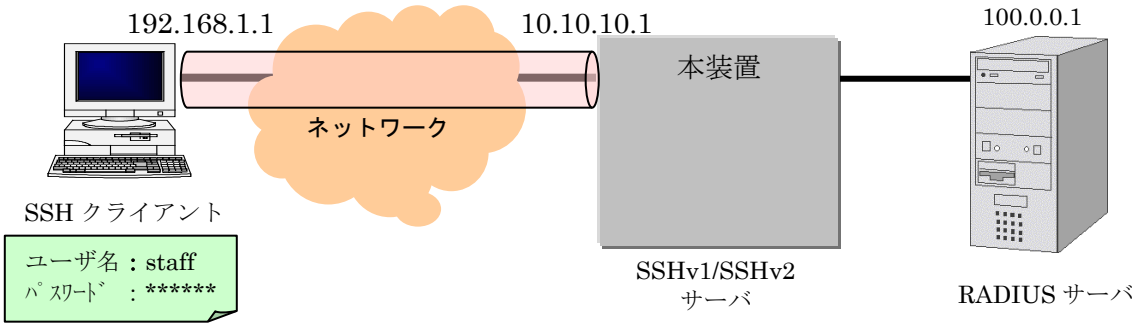
SSH を利用して本装置にログインする際のパスワード認証を RADIUS サーバで管理することができます。

ここでは，RADIUS 認証とローカルパスワード認証を使用した場合の SSH サーバの設定例を示します。RADIUS 認証に使用するサーバを 1 台指定し，RADIUS 認証に失敗した場合には本装置によるローカル認証を行うように設定します。また，RADIUS 接続情報としてタイムアウト時間 2 秒を設定します。

(2) 構成図と設定条件

SSH クライアントからネットワークを介して本装置へ接続する構成とします(図 5.9-1)。

図 5.9-1　RADIUS 認証と連携した SSH サーバの設定 構成図



［設定条件］

本装置の SSH サーバ
- IP アドレス　　10.10.10.1
- SSHv1 と SSHv2 で接続可能とする（デフォルト動作）
- 公開鍵認証を使用し，パスワード認証も許可する（デフォルト動作）
- RADIUS 認証を使用する

SSH クライアント
- IP アドレス　　192.168.1.1

RADIUS サーバ
- IP アドレス　　100.0.0.1
- 共有鍵(key)　　“RADIUSKEY”

ログインのための情報
- ユーザ名　　staff
- パスワード　　******

※なお，本装置－SSH クライアント間，本装置－RADIUS サーバ間はあらかじめ通信設定を行い，通信できることとします。

(3) ユーザの登録

管理端末上から，装置管理者モードの運用コマンド adduser を使用して，ユーザ staff とパスワードを設定し，ログインユーザアカウントを作成してください。アカウントにはパスワードの設定を行ってください。SSH では認証時にパスワードを省略すると，ログインできません。

```
> enable
# adduser staff
User(empty password) add done. Please setting password.
Changing local password for staff.
New password:******
Retype new password:******
#
```

(4) コンフィグレーション設定

管理端末から，コンフィグレーションコマンドで SSH クライアントに対するリモートアクセス許可設定と，SSH サーバを動作させる設定を行います。

［コマンド設定例］

```
解説番号          入力コマンド
    1    (config)# ip ssh
    2    (config)# line vty 0 1
    3    (config)# aaa authentication login default group radius local
    4    (config)# radius-server host 100.0.0.1 key “RADIUSKEY”
    5    (config)# radius-server timeout 2
```

表 5.9-1　本装置の設定解説

解説番号	解説
1	SSH サーバの動作を開始させます。
2	本装置へログインするユーザ数を 2 とします。
3	使用するログイン認証方式を RADIUS 認証およびローカル認証に設定します。
4	RADIUS 認証に使用するサーバのホスト名と共有鍵を設定します。
5	RADIUS サーバからの応答タイムアウト時間を 2 秒に設定します。

［設定内容の表示］

```
(config)# show
 (中略)
aaa authentication login default group radius local
!
 (中略)
radius-server timeout 2
radius-server host radius-server1 key “RADIUSKEY”
```

```
!
 (中略)
line vty 0 1
!
 (中略)
ip ssh
!
 (中略)
```

(5) 動作確認

SSH クライアントから，本装置(10.10.10.1)へ接続し，ユーザ名 staff と RADIUS サーバ上のパスワードで認証されログインできることを確認してください。

［注意事項］

RADIUS サーバからの応答タイムアウト時間はネットワーク環境に合わせて調整してください。またタイムアウトが発生した場合のリトライ回数の設定も変更することができます。詳しくは「コンフィグレーションコマンドレファレンス　ログインセキュリティと RADIUS」を参照してください。

5.10 SSHv2 サーバ機能だけを使いセキュリティを高める

(1) 設定内容の概要

本装置は，装置の運用管理のために，TELNET(TCP ポート番号 23)・FTP(TCP ポート番号 21)の各サーバ機能をサポートしています。これらのサーバ機能はコンフィグレーションにより使用できる状態になっていることがあります。

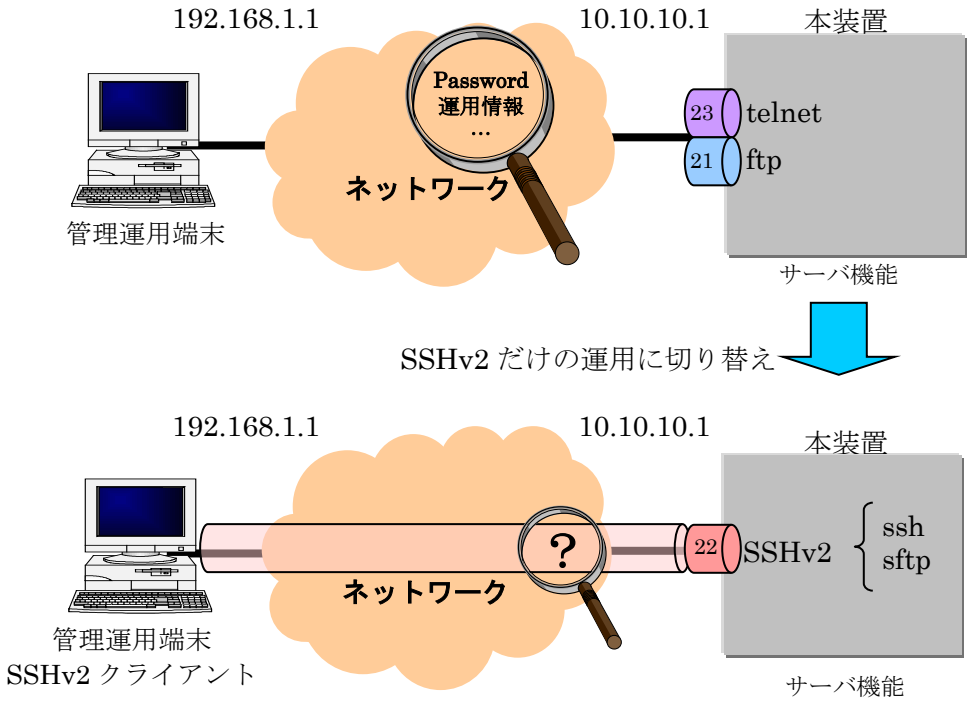
ここでは，上記のサーバ機能を使用せず SSH サーバ機能だけを使用し，セキュアな運用管理を行う設定をします。SSH サーバ機能は，TELNET や FTP と同等の運用管理機能をサポートしていますので，SSH サーバ機能での運用管理に移行し，不要なサーバ機能を停止することをお勧めします。また，SSH サーバ機能はセキュリティの高い SSHv2 だけを使用します。

さらにアクセスリストを適用し，接続できる運用端末の制限を行います。

(2) 構成図と設定条件

管理運用端末からネットワークを介して本装置へ接続する構成とします(図 5.10-1)。

図 5.10-1 SSHv2 サーバ機能だけを使いセキュリティを高める 構成図



［設定条件］

本装置のサーバ

・SSHv2 だけを使用する
・telnet, ftp 機能を使用しない
・ネットワーク 192.168.1.0/24 の端末からだけのアクセスを許可する。

なお，本装置－SSH クライアント間はあらかじめ通信設定を行い，通信できることとします。

(3) コンフィグレーション設定

コンフィグレーションコマンドで SSH サーバ機能とシステム管理情報の設定(変更)を行います。

［コマンド設定例］

解説番号	入力コマンド
1	(config)# ip ssh
2	(config)# ip ssh version 2
3	(config)# no ftp-server
4	(config)# ip access-list standard REMOTE
	(config-std-nacl)# permit 192.168.1.0 0.0.0.255
	(config-std-nacl)# exit
5	(config)# ipv6 access-list REMOTE6
	(config-ipv6-acl)# deny ipv6 any any
	(config-ipv6-acl)# exit
6	(config)# line vty 0 1
7	(config-line)# transport input ssh
8	(config-line)# ip access-group REMOTE in
9	(config-line)# ipv6 access-class REMOTE6 in
	(config-line)# exit

表 5.10-1 本装置の設定解説

解説番号	解説
1	SSH サーバの動作を開始させます。
2	SSH サーバのプロトコルバージョン 2 だけサポートします。
3	FTP サーバを無効にします。（デフォルト設定）
4	本装置へログインを許可するリモート運用端末のアドレス 192.168.1.0/24 のアクセスリストを作成します。
5	IPv6 アドレスのリモート運用端末からのログインを拒否するアクセスリストを作成します。
6	本装置へログインするユーザ数を 2 とします。
7	リモート運用端末から SSH プロトコルだけアクセスを許可します。
8	192.168.1.0/24 のリモート運用端末だけアクセスを許可します。
9	IPv6 アドレスのリモート運用端末からのアクセスを拒否します。

表 5.10-2　本装置の設定解説

解説番号	解説
1	SSH サーバの動作を開始させます。
2	SSH サーバのプロトコルバージョン 2 だけサポートします。
3	FTP サーバを無効にします。（デフォルト設定）
4	本装置へログインを許可するリモート運用端末のアドレス 192.168.1.0/24 のアクセスリストを作成します。
5	本装置へログインするユーザ数を 2 とします。
6	リモート運用端末から SSH プロトコルだけアクセスを許可します。
7	192.168.1.0/24 のリモート運用端末だけアクセスを許可します。

［設定内容の表示］

```
(config)# show
(中略)
line vty 0 1
 transport input ssh
 ip access-group REMOTE in
 ipv6 access-class REMOTE6 in
!
(中略)
ip ssh
ip ssh version 2
!
(中略)
ip access-list standard REMOTE
 10 permit 192.168.1.0 0.0.0.255
!
ipv6 access-list REMOTE6
 10 deny ipv6 any any
!

(中略)
```

(4) 動作確認

SSHv2 クライアントから本装置へ接続できることを確認してください。また，ftp， telnet や 192.168.1.0/24 以外の SSH 端末から接続できないことを確認してください。

運用ガイド編

6. SSH サーバ運用コマンドの利用ガイド

本章では SSH サーバの運用コマンドの例を示します。

6.1　SSH サーバのログを確認・消去する

(1) 概要

SSH サーバのログを確認することができます。SSH サーバログには，SSH サーバにログインしたユーザ名やその時に利用したユーザ認証の種類などが表示されます。ユーザがログインできない時の SSH サーバ側での状態の把握にも役立ちます。

なお，SSH サーバのログは本装置の電源を切ったり，再起動をしたりすると消去されます。

(2) 確認方法

本装置で SSH ログ確認コマンドを入力します。

```
> show ssh logging

Date 20XX/09/19 19:32:59 UTC
(ア)
20XX/09/19 19:32:48 sshd Closing connection to 192.168.10.100.
20XX/09/19 19:32:48 sshd Disconnecting: Too many authentication failures for staff1.
20XX/09/19 19:32:48 sshd Failed password for staff1 from 192.168.10.100 port 2174.
20XX/09/19 19:32:47 sshd Failed password for staff1 from 192.168.10.100 port 2174.
20XX/09/19 19:32:47 sshd Failed password for staff1 from 192.168.10.100 port 2174.
20XX/09/19 19:32:46 sshd Failed password for staff1 from 192.168.10.100 port 2174.
20XX/09/19 19:32:45 sshd Failed password for staff1 from 192.168.10.100 port 2174.
20XX/09/19 19:32:36 sshd Sent 768 bit server key and 1024 bit host key.
20XX/09/19 19:32:36 sshd RSA key generation complete.
20XX/09/19 19:32:35 sshd Generating 768 bit RSA key.
20XX/09/19 19:32:35 sshd Client protocol version 1.5; client software version TTSSH/2.45.
(イ)
20XX/09/19 19:32:35 sshd Connection from 192.168.10.100 port 2174.
20XX/09/19 19:31:30 sshd Entering interactive session for SSH2.
20XX/09/19 19:31:30 sshd Accepted publickey for staff1 from 192.168.10.100 port 2173 ssh2.
20XX/09/19 19:31:30 sshd Found matching DSA key: 16:0b:6c:cb:12:83:f2:25:69:1b:c4:73:8e:37:9f:c0.
20XX/09/19 19:31:30 sshd Failed none for staff1 from 192.168.10.100 port 2173 ssh2.
20XX/09/19 19:31:23 sshd kex: server->client aes256-cbc hmac-sha1.
20XX/09/19 19:31:22 sshd kex: client->server aes256-cbc hmac-sha1.
20XX/09/19 19:31:22 sshd Client protocol version 2.0; client software version TTSSH/2.45.
20XX/09/19 19:31:22 sshd Connection from 192.168.10.100 port 2173.

>
```

ログ表示は最新のものが上に表示されます。

(ア) SSHv1(protocol version 1.5)でユーザ staff1 が 192.168.10.100 から接続し，
パスワード認証に失敗したことがわかります。

(イ) SSHv2 でユーザ staff1 が 192.168.10.100 から接続し，
公開鍵認証(DSA)でログインしたことがわかります。

(3) 注意事項

クライアントからのメッセージを表示するログ部分では，送られた文字が ASCII 文字以外(日本語文字など)の場合，ASCII 表示可能な文字にエンコード変換されて表示します。

なるべく，ASCII 文字でエラーメッセージを送付するクライアントをご利用ください。

(4) 消去方法

装置管理者モードの SSH ログ消去コマンドを入力します。

```
> enable
# clear ssh logging
Would you wish to CLEAR the SSH server's log? (y/n): y

Clear Complete.
#
```

消去の確認です。y を入力します。

6.2　SSH サーバのホスト公開鍵の確認をする

(1) 概要

SSH クライアントが SSH サーバを確認できるように，各々の SSH サーバは異なるホスト鍵ペアに変更してから運用します（工場出荷時にはデフォルトのホスト鍵ペアが設定されています。運用コマンド set ssh hostkey によるホスト鍵ペアの変更を強くお勧めします)。

SSH クライアント側では，SSH サーバに初めて接続する時や，ホスト公開鍵が変更された場合，そのサーバの Fingerprint の確認を行うよう警告・承認確認メッセージが表示されます。この時に，あらかじめ接続先のサーバの Fingerprint（またはホスト公開鍵）を入手しておき，接続時に目視確認することでより安全な接続が行えます。

本コマンドでは，SSHv1/SSHv2 のホスト公開鍵とその Fingerprint の確認が可能です。

(2) 確認方法

運用コマンドでホスト公開鍵の表示を行います。

```
> show ssh hostkey

Date 20XX/09/11 09:32:06 UTC

******* SSHv1 Hostkey *******

1024 65537 112676670827222279613762898147415720811259820741286658557999554110106264702311 3
943120729117808345272300056975789401190169610484301410980604870962889893279169871308556619
653902343314040484345625244656741164451968702730151969974584171941799596068373366303944657
053583545620694390204035676242785567125465544918 63

Fingerprint for key:
xifik-kigez-mogot-zysom-pidyg-kutop-holam-rudib-negof-lilyk-lyxax
Fingerprint(HEX) for key:
7a:79:c1:da:db:69:27:42:e4:48:ab:5c:86:18:a6:04

******* SSHv2 Hostkey *******

MIHxMIGpBgcqhkjOOAQBMIGdAkEA/UNXOgmhyXWRcOBZLun6hspiuS/Q/N/KuOstYrD5kQr7vTcNrCNZDYDnCVFfrC
6/xyBQGPOfhUBpRUc7eoJpMwIVAOLUu3B5ClDwieTcsYqmu517ABBXAkEAgTfPLQcVxAiqkTowSvA/tVyXwCPovs3n
BBK8S9nFW+ZzGm9oR2RccrbfulnOAkaoUVmacGBxvD+z9qhhHgiNjQNDAAJAeBvdcIgYEly7EUlObb1KxTGe97hxdM
31vhJnzGkgrzlyEhf2+d1V756AOmArKvnkq1MKlaFj4vxnqqGVypRfng==

Fingerprint for key:
xemos-tibod-rukys-zekos-puvel-nufet-tihin-leroz-cufis-zaruc-daxox
Fingerprint(HEX) for key:
6e:3c:a1:10:ab:02:7f:73:d8:aa:7e:40:d0:51:6e:f8

>
```

本装置の SSH サーバでは，bubblebabble 形式と HEX 形式の Fingerprint をサポートしています。クライアント・サーバの実装によっては SSHv1 での Fingerprint のサポートはありません。より安全に接続を行うためにも SSHv2 で接続されることをお勧めいたします。

6.3　SSH サーバのホスト鍵ペアの変更をする

(1) 設定内容の概要

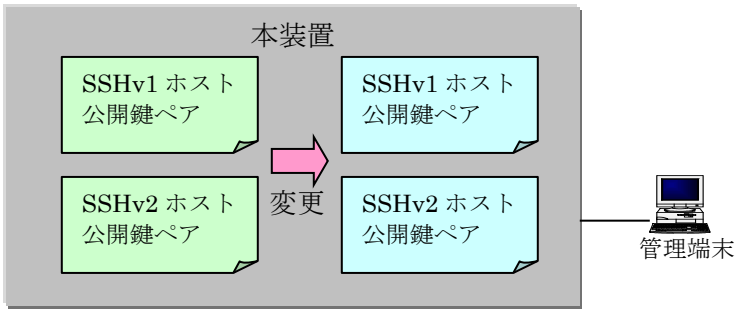
SSH クライアントが SSH サーバを確認できるように, 各々の SSH サーバは異なるホスト鍵ペアに変更してから運用します。工場出荷時にはデフォルトのホスト鍵ペアが設定されています。運用コマンド set ssh hostkey によるホスト鍵ペアの変更を強くお勧めします。一度変更を実施すれば, 通常変更の必要はありません。

本操作は SSH サーバの管理組織の変更など, 何らかの理由でホスト鍵ペアを変更したい場合に行います。

(2) 構成図と設定条件

本装置の SSH サーバは，SSHv1 のホスト鍵ペアと SSHv2 のホスト鍵ペアに変更してから運用します(図 6.3-1)。

図 6.3-1　SSH サーバのホスト鍵ペア変更 構成図



［設定条件］

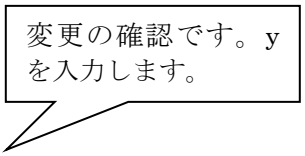
本装置の SSH サーバ

・SSHv1 ホスト鍵ペア，SSHv2 ホスト鍵ペアを再生成し変更します。

(3) 運用コマンド設定

装置管理者モードの運用コマンドでホスト鍵ペアの変更を行います。

```
> enable
# set ssh hostkey

WARNING!!
Would you wish to change the SSH (v1 and v2) Hostkeys? (y/n): y

*** Changing the SSHv1 Hostkey, Please wait a minute ***
Generating public/private rsa1 key.
The key fingerprint is:
ee:c7:94:9e:fc:11:0d:6d:c0:e7:f8:5b:9e:ed:c0:b6 1024-bit rsa1 hostkey

*** Changing the SSHv2 Hostkey, Please wait a minute ***
Generating public/private dsa key.
The key fingerprint is:
8d:2f:48:95:94:c6:2d:d1:8b:3d:98:7a:21:ba:79:9f 1024-bit dsa hostkey

Your identification has been saved.
The Hostkeys (SSHv1 and SSHv2) were generated Completely.
Please execute the reload command,
because the new hostkeys becomes effective after reboot.

#
```



変更したホスト鍵ペアは，本装置の再起動後に有効となります。運用コマンド reload で本装置を再起動してください。

MC 運用モード機能使用時は，運用コマンド update mc-configuration で MC にソフトウェアおよび装置情報と一括で保存後に，運用コマンド reload を実行してください。

ゼロタッチプロビジョニング機能を使用時は，AX-Network-Manager でソフトウェアおよび装置情報と一括で保存後に，運用コマンド reload を実行してください。

(4) 動作確認

本装置を再起動後，SSH サーバのホスト公開鍵確認コマンド(show ssh hostkey)を実行(6.2章を参照)し，ホスト公開鍵が変更されていることを確認してください。(ホスト秘密鍵はセキュリティの都合上，見ることはできません。)

また，SSH クライアントから，本装置へ SSHv1 もしくは SSHv2 で接続し，ホスト公開鍵が変更されていることを確認してください。

サーバのホスト鍵ペアを変更した場合は，クライアント側で接続時にそのホスト公開鍵が変更された旨の警告が表示されます。クライアントユーザには，変更したホスト公開鍵またはその Fingerprint を通知し，ユーザのホスト公開鍵データベースの変更（または変更の承認）を行っても

らうようにしてください。（クライアントでホスト公開鍵データベースの変更・承認を行う方法は，各クライアントのマニュアルやトラブルシュートをご覧ください。）

6.4　SSH サーバのホスト鍵ペアを保存・復元する

(1) 概要

SSH クライアントが SSH サーバを確認できるように, 各々の SSH サーバは異なるホスト鍵ペアに変更してから運用します（工場出荷時にはデフォルトのホスト鍵ペアが設定されています。運用コマンド set ssh hostkey によるホスト鍵ペアの変更を強くお勧めします)。

本操作は SSH サーバの装置障害または交換時など，何らかの理由でホスト鍵ペアを保存・復元したい場合に行います。

(2) 保存・復元方法

本装置の SSH サーバは，SSHv1 のホスト鍵ペアと SSHv2 のホスト鍵ペアで運用しますが，保存・復元方法には，以下の手段があります。

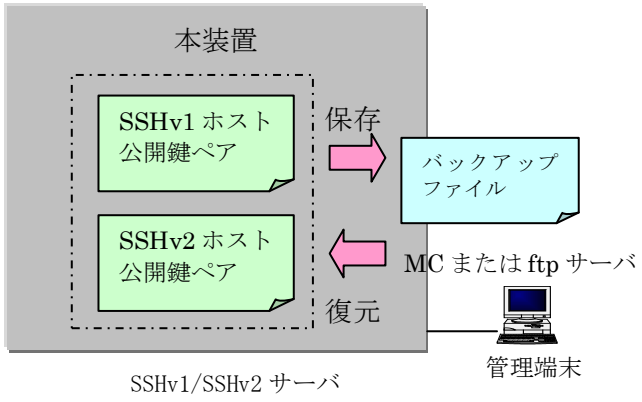
・バックアップ・リストア
・MC 運用モード機能
・ゼロタッチプロビジョニング機能

(a) バックアップ・リストア

本装置に設定したホスト鍵ペアをバックアップファイルとして保存・復元できます。（図 6.4-1）

なお，SSH に関する情報以外に保存対象となる装置情報は,「コンフィグレーションガイド Vol.1 装置情報のバックアップ・リストア」を参照してください。

図 6.4-1　SSH サーバのホスト鍵ペア保存・復元 概念図



保存は運用コマンド backup，復元は運用コマンド restore を使用します。これら運用コマンドの詳細は「運用コマンドレファレンス」を参照してください。

(b) MC 運用モード機能

MC 運用モード機能でホスト鍵ペアを含む装置情報を MC に保存し，MC から復元できます。

MC 運用モード機能の詳細は，「コンフィグレーションガイド Vol.1　MC 運用モード機能」を参照してください。

MC 運用モード機能は運用コマンド set mc-configuration を設定します。保存は運用コマンド update mc-configuration，復元は保存した MC を挿入して本装置を起動することで可能です。ホスト鍵ペアを変更した場合は，装置を再起動する前に運用コマンド update mc-configuration で MC にソフトウェアおよび装置情報を一括で保存してください。これら運用コマンドの詳細は「運用コマンドレファレンス」を参照してください。

(c) ゼロタッチプロビジョニング機能

ゼロタッチプロビジョニング機能でホスト鍵ペアを含む装置情報を AX-Network-Manager に保存し，AX-Network-Manager から復元できます。

ゼロタッチプロビジョニング機能の詳細は，「コンフィグレーションガイド Vol.1　ゼロタッチプロビジョニング機能」を，AX-Network-Manager の詳細は，AX-Network-Manager のマニュアルを参照してください。

本装置のソフトウェアと装置情報は AX-Network-Manager で定期的にバックアップしています。

ゼロタッチプロビジョニング機能は本装置を起動したときに動作し，AX-Network-Manager からバックアップファイルを取得して，装置情報を復元します。

ホスト鍵ペアを変更した場合は，装置を再起動する前に AX-Network-Manager でソフトウェアおよび装置情報を一括で保存してください。

(3) 動作確認

装置情報の復元を行った場合，自動的に装置が再起動します。このとき通信が一時的に中断します。装置再起動後，SSH サーバのホスト公開鍵確認コマンド（show ssh hostkey）を実行し，ホスト公開鍵が復元されていることを確認してください。（ホスト秘密鍵はセキュリティの都合上，見ることはできません。）

また，SSH クライアントから，本装置へ SSHv1 または SSHv2 で接続し，ホスト公開鍵が変更されていないことを確認してください。

7. トラブルシュート

本章ではSSH機能が正常に動作しない，または通信が出来ないといったトラブルが発生した場合の対処方法を説明します。

7.1　他装置から本装置に対して SSH で接続できない

他装置 SSH クライアントから本装置に対して ssh，sftp で接続できない場合には以下の手順で確認してください。

7.1.1　リモート接続経路の確立を確認する

本装置と管理端末間の通信経路が確立できていない可能性があります。ping コマンドを使用して通信経路を確認してください。

7.1.2　本装置のリモートアクセス制御を確認する

本装置のリモートアクセス制御により接続できない可能性があります。以下をご確認ください。

- コンフィグレーションコマンド ip ssh と line vty を設定していること。
- コンフィグレーションコマンド line vty の階層で，transport input を設定している場合，
  そのパラメータに ssh または all 以外を設定していないこと。
- コンフィグレーションコマンド line vty の階層で，アクセスリストを指定している場合，
  許可された IPv4 アドレスまたは IPv6 アドレスの端末から接続していること。

詳細は「コンフィグレーションガイド Vol.1　ログインセキュリティの設定」を参照してください。

図 7.1-1　本装置でリモートアクセスコンフィグレーションを確認する

```
(config)# show line
line vty 0 1
  transport input ssh
!
```

line vty が設定されているか？
transport を設定している場合，ssh または all 以外を設定していないか？

7.1.3　SSH サーバのコンフィグレーションを確認する

SSH サーバに関するコンフィグレーションが下記のどれかに該当するような場合は，本装置に対して SSH で接続できません。

- 本装置に SSH サーバに関するコンフィグレーションが未設定の場合
- 本装置の SSH サーバの設定と，他装置の SSH クライアント側の設定で認証方式などが一致しない場合
- 運用コマンド format flush が実行されて，SSH サーバに関するコンフィグレーションが消去されてしまった場合

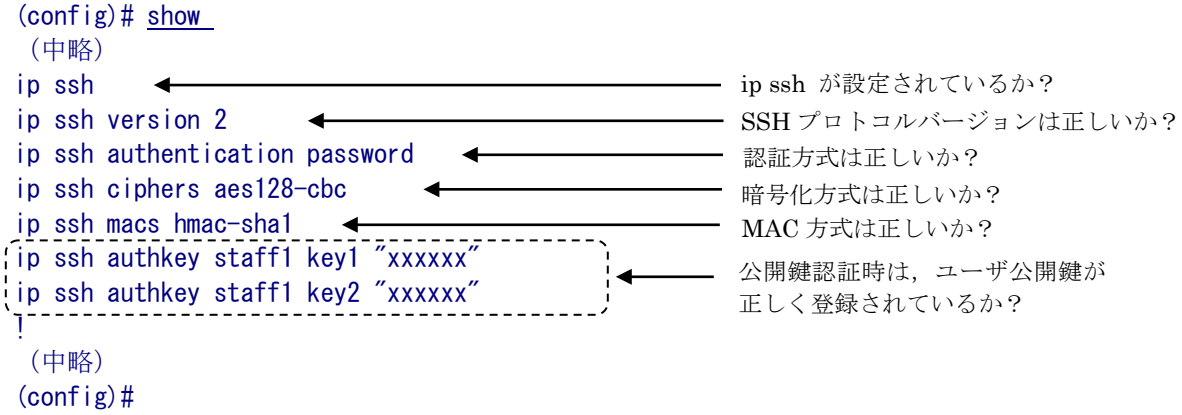
コンフィグレーションに SSH サーバの情報が正しく設定されているか確認してください。SSH コンフィグレーションコマンドの詳細については「5.SSHサーバ機能の設定ガイド」と「8.コンフィグレーション」を参照してください。

他装置の SSH クライアントの設定については，ご使用の SSH クライアントのマニュアルを参照してください。

表 7.1-1　本装置のコンフィグレーションで設定する SSH サーバ情報

項番	SSH コンフィグレーション 設定項目	内容
1	SSH 使用・未使用フラグ	SSH 使用・未使用を指定します。
2	SSH プロトコルバージョン	SSH プロトコルバージョン 1 または 2 を指定します。
3	認証方式	公開鍵認証，パスワード認証を指定します。
4	暗号方式	共通鍵暗号方式を指定します。
5	MAC	MAC 方式を指定します。
6	ユーザ公開鍵	ユーザ公開鍵を登録します。

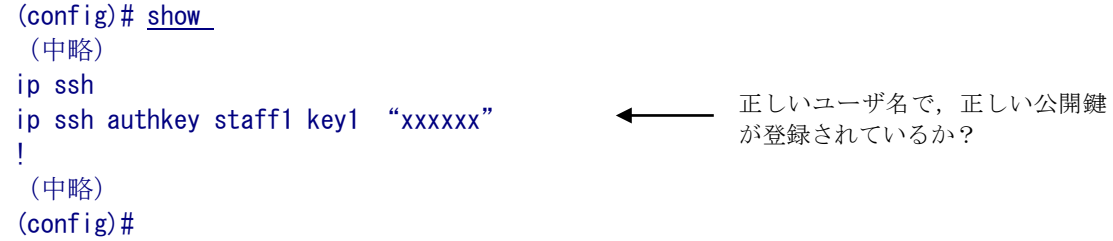
図 7.1-2　本装置で SSH コンフィグレーションを確認する



7.1.4　本装置に登録したユーザ公開鍵が正しいか確認する

本装置に公開鍵認証でログインする場合は，本装置のコンフィグレーションに登録したユーザ公開鍵が本当に正しい鍵であるかをもう一度確認してください。

図 7.1-3　本装置でユーザ公開鍵を確認する



7.1.5　本装置にアカウントが存在するか確認する

本装置に存在しないアカウントではローカル認証でログインできません。SSH でローカル認証を使用して本装置にログインできるアカウントは，運用コマンド show users で「*local(users)」に表示されるユーザだけです。アカウントにはパスワードの設定を行ってください。SSH では認証時にパスワードを省略すると，ログインできません。

図 7.1-4　本装置でのユーザアカウント確認例

```
> show users

(中略)

 * local (users)
  No   Name              Password
   1   operator          ****
   2   admin             ****
   3   user              not set

(中略)

>
```

SSH で使用するユーザ名が存在しているか？

7.1.6　ログインユーザ数を確認する

本装置にログインできる最大ユーザ数を超えてログインされ以下のログがでていないかを運用コマンド show logging で確認してください。詳細は「コンフィグレーションガイド Vol.1 ログインセキュリティの設定」を参照してください。

図 7.1-5　本装置で最大ログイン数を超えている場合の例

```
> show logging

EVT 05/20 14:09:25 E3 SESSION Login refused for too many users logged in.
```

7.2　ローカルパスワード認証時のユーザ名やパスワードを忘れてしまった

本装置でのユーザ名やローカルパスワードを忘れてしまった場合には，以下の手順で対応してください。

(1) 装置管理者モードに遷移できるユーザ名とパスワードがある場合

本装置にログイン後，装置管理者モードに変更して当該ユーザのパスワードの変更（password コマンド），もしくは削除（clear password コマンド）を行います。

図 7.2-1　ユーザのパスワードを変更

```
# password staff1
Changing local password for staff1.
New password:******
Retype new password:******
#
```

図 7.2-2　ユーザのパスワードを削除

```
# clear password staff1
Changing local password for staff1.
Password cleared.
#
```

(2) 装置管理者モードに遷移できるユーザ名とパスワードがない場合

本装置にログインできるユーザ名がない場合は，以下の手順で対応してください。

1. 本装置を再起動し，コンソールに”login”が表示されるまで，[CTRL＋N]キーを同時に押下し続けてください。
2. このとき，スタートアップコンフィグレーションファイルおよびログインユーザ情報は読み込まれません。
3. 本装置起動後は，ログインユーザ名：operator でログインできます。
4. ログイン後，ログインユーザ名とパスワードを変更してください。
   ・ログイン後，ログインユーザ名とパスワードを登録してください。登録については，「5.1 SSHサーバの基本設定（ローカルパスワード認証)」を参照してください。
   パスワード（password コマンド）を設定してください。パスワードの設定は「9.運用・保守機能」を参照してください。

5. 本装置を再起動してください。
   スタートアップコンフィグレーションファイルおよび変更したログインユーザ情報が読み込まれます。

7.3　公開鍵認証時のパスフレーズを忘れてしまった

本装置に対して SSH 公開鍵認証でログインする際に入力するパスフレーズを忘れてしまった場合は，そのユーザ公開鍵・秘密鍵の鍵ペアは使用することができません。次の手順に従って対応してください。

(1) 本装置の SSH コンフィグレーションからユーザ公開鍵を削除する

本装置の SSH コンフィグレーションコマンドで,パスフレーズを忘れてしまったユーザのユーザ公開鍵を削除してください。

図 7.3-1　本装置の SSH コンフィグレーションからユーザ公開鍵を削除

```
(config)# show
 (中略)
ip ssh
ip ssh version 2
ip ssh authentication publickey
ip ssh authkey staff1 key1 "xxxxxxxxxx"
ip ssh authkey staff1 key2 "xxxxxxxxxx"
!
 (中略)
(config)# no ip ssh authkey staff1 key1

(config)# show
 (中略)
ip ssh
ip ssh version 2
ip ssh authentication publickey
ip ssh authkey staff1 key2 "xxxxxxxxxx"
!
 (中略)
```

(2) SSH クライアント側端末のユーザ鍵ペアを削除する

SSH クライアント側端末にてパスフレーズを忘れてしまったユーザのユーザ公開鍵・秘密鍵の鍵ペアを削除して，登録も解除してください。あらためて，公開鍵認証を使用される場合は，ご使用の SSH クライアントにて鍵ペアを再作成後，本装置の SSH コンフィグレーションコマンドにてユーザ公開鍵登録をやり直してください。SSH コンフィグレーションコマンドでのユーザ公開鍵登録方法は「5.SSHサーバ機能の設定ガイド」と「8. コンフィグレーション」を参照してください。

7.4　SSH で接続した時にホスト公開鍵が変更されている警告が表示される

SSH 接続したときに，以前接続したサーバとホスト鍵が異なると，SSH クライアントによっては警告メッセージを表示する場合があります。

これは悪意ある第 3 者が本装置になりすましている可能性もありますので以下の手順に従って充分に確認を行ってから SSH 接続を行ってください。

7.4.1　本装置の装置管理者への問い合わせと対応

本装置の装置管理者モードで，運用コマンド set ssh hostkey を使用して意図的にホスト鍵ペアを変更，もしくは装置構成の変更等をしていないか問い合わせ確認してください。本装置で装置管理者がホスト鍵ペアの変更を行っていない場合は，なりすまし攻撃にあっている（または他のホストへ接続）危険性がありますので SSH 接続を中断し，ネットワーク管理者に連絡してください。

なりすましの危険性が無く，単に本装置のホスト公開鍵が変更されていた場合，以下に従って再接続してください。

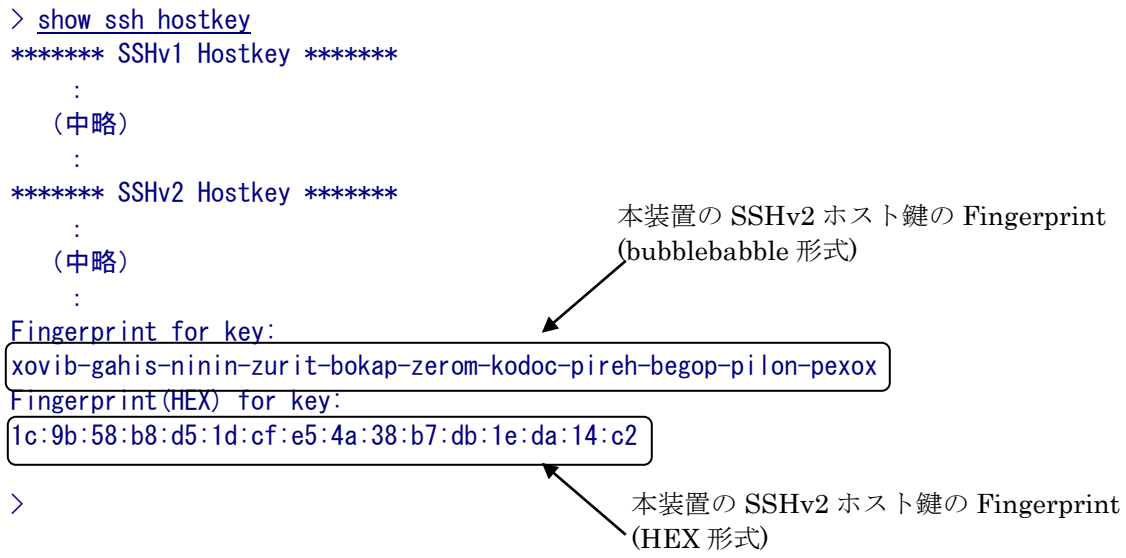
7.4.2　ホスト公開鍵が変更された場合の再接続

SSH クライアントから SSHv2 プロトコルを使用して，ホスト鍵ペアが変更された本装置の SSH サーバに接続します。より安全に接続するために，以下の手順に従って Fingerprint により，接続しようとしている本装置の SSH サーバが正しい接続対象のホストであることを確認します。

(1) Fingerprint の事前確認

あらかじめ，本装置側にログインして show ssh hostkey コマンドで Fingerprint を確認します。（コンソール接続などネットワーク経由でない安全な方法で確認されるとより安全です。）

図 7.4-1　ホスト公開鍵の Fingerprint の事前確認



(2) Fingerprint をクライアントユーザ側へ通知

確認した Fingerprint を SSH クライアントユーザに通知します。(ネットワーク経由以外の安全な方法「郵送，電話等」で通知するとより安全です。)

(3) Fingerprint を確認して SSH 接続

クライアント側では，本装置の SSH サーバに対して SSH 接続した際に表示される Fingerprint が(2)で通知されたものと同じであることを確認した後，接続します。

クライアントによっては Fingerprint が HEX 形式で表示されるものと bubblebabble 形式で表示されるものがあります。また，SSHv 1 では Fingerprint をサポートしていないものあります。クライアントに合った形式で確認するようにしてください。

7.4.3 ユーザのホスト公開鍵データベースの登録削除

ご使用の SSH クライアントによっては，ユーザのホスト公開鍵データベースに登録された，本装置の SSH サーバのホスト公開鍵が自動で削除されず，接続のたびに警告が表示される，または接続できない場合があります。このような場合は手動でファイルを編集・削除し再接続してください。

コンフィグレーションコマンドレファレンス編

8. コンフィグレーション

本章は SSH サーバのコンフィグレーションコマンドレファレンスです。

8.1　コンフィグレーションコマンド一覧

SSH のコンフィグレーションコマンド一覧を次表に示します。

表 8.1-1　コンフィグレーションコマンド一覧

項目	コンフィグレーションコマンド名称	概要	本装置のマニュアルからの変更事項
1	ip ssh	SSH サーバを動作させます。	新規
2	ip ssh version	SSH サーバの SSH プロトコルバージョンの制限を行います。	新規
3	ip ssh authentication	SSH サーバのユーザ認証方式の制限を行います。	新規
4	ip ssh ciphers	SSHv2 サーバで使用する暗号方式の制限を行います。	新規
5	ip ssh macs	SSHv2 サーバで使用する MAC 方式の制限を行います。	新規
6	ip ssh authkey	SSH サーバで公開鍵認証に使用するユーザ公開鍵の登録を行います。	新規
7	transport input	リモート運用端末から各種プロトコルを使用してのアクセスを制限するために使用します。	パラメータ ssh を追加しました。

8.2　コンフィグレーションコマンド

8.2.1　ip ssh

本装置へ SSH でリモートログインするための，SSH サーバを動作させます。本設定と line vty の設定を行うと，すべてのリモート運用端末から SSH プロトコルでのリモートアクセスを受け付けるようになります。アクセスを制限する場合は，line vty モードで ip access-group，ipv6 access-class や，transport input を設定してください。

［入力形式］

情報の設定
　ip ssh

情報の削除
　no ip ssh

［入力モード］
(config)

［パラメータ］
なし

［コマンド省略時の動作］
SSH サーバは動作していませんので，本装置へ SSH でリモートログインできません。

［通信への影響］
なし

［設定値の反映契機］
設定値変更後，すぐに運用に反映されます。

［注意事項］

- 本設定だけでは SSH でログインできません。line vty でログインユーザ数の設定が必要です。
- 本設定と line vty の設定を行うと，すべてのリモート運用端末から SSH プロトコルでのリモートアクセスを受け付けるようになります。アクセスを制限する場合は，line vty モードで ip access-group，ipv6 access-class や，transport input を設定してください。
- ローカルパスワード認証を使用する場合は，運用コマンド password でログインパスワードの設定が必要です。
- 他の SSH 情報コマンド(ip ssh version など)を設定しても，本コマンドを設定していない場合

は，SSH サーバは動作していませんので，本装置へ SSH でリモートログインできません。

［関連コマンド］

line vty
ip ssh authentication
password

8.2.2 ip ssh version

SSH サーバで使用する SSH プロトコルバージョンの制限を行います。

本設定がない場合は SSH プロトコルバージョン 1 と 2 いずれの接続も許可します。

[入力形式]

情報の設定
ip ssh version { 1 | 2 }

情報の削除
no ip ssh version

[入力モード]
(config)

[パラメータ]

{ 1 | 2 }

本パラメータ省略時の初期値

省略できません。

値の設定範囲

1：プロトコルバージョン 1 だけ接続を許可します。

2：プロトコルバージョン 2 だけ接続を許可します。

[コマンド省略時の動作]
SSH プロトコルバージョン 1 と 2 いずれの接続も許可します。

[通信への影響]
なし

[設定値の反映契機]
次回のログインから運用に反映されます。

[注意事項]

- SSH サーバを動作させるために，ip ssh と line vty の設定が必要です。
- セキュリティ確保のためにプロトコルバージョン 2 だけを使用することをお勧めします。

[関連コマンド]
line vty
ip ssh

8.2.3 ip ssh authentication

SSH サーバのユーザ認証方式の設定を行います。

本装置の SSH サーバで許可するユーザ認証方式(publickey 公開鍵認証，password ローカルパスワード認証)を指定します。

[入力形式]

情報の設定

ip ssh authentication { publickey | password }

情報の削除

no ip ssh authentication

[入力モード]

(config)

[パラメータ]

{ publickey | password }

本パラメータ省略時の初期値

省略できません。

値の設定範囲

publickey： 公開鍵認証だけ許可します。

password： ローカルパスワード認証だけ許可します。

[コマンド省略時の動作]

認証方式は公開鍵認証，パスワード認証いずれも許可します。

[通信への影響]

なし

[設定値の反映契機]

次回のログインから運用に反映されます。

[注意事項]

- SSH サーバを動作させるために，ip ssh と line vty の設定が必要です。
- ローカルパスワード認証を使用する場合は，運用コマンド password でログインパスワードの

設定が必要です。

［関連コマンド］

line vty
ip ssh
ip ssh authkey
password

8.2.4 ip ssh ciphers

SSHv2 サーバで使用する暗号方式の制限を行います。

本装置の SSHv2 サーバで許可する共有鍵暗号方式を，並べて指定します。

［入力形式］

情報の設定

ip ssh ciphers <Encryption algorithm> [<Encryption algorithm> […]]

情報の削除

no ip ssh ciphers

［入力モード］

(config)

［パラメータ］

<Encryption algorithm>

本パラメータ省略時の初期値

省略できません。

値の設定範囲

以下の暗号方式名を指定します。

表 8.2-1 共通鍵暗号方式

項番	暗号方式名
1	aes128-cbc
2	aes192-cbc
3	aes256-cbc
4	3des

［コマンド省略時の動作］

SSHv2 サーバで許可する共有鍵暗号方式は，aes128-cbc，aes192-cbc，aes256-cbc，3des です。

［通信への影響］

なし

［設定値の反映契機］

次回のログインから運用に反映されます。

［注意事項］

- SSH サーバを動作させるために，ip ssh と line vty の設定が必要です。
- 本設定の有無に関係なく，SSHv1 では 3des だけサポートとなります（その他の共通鍵暗号方式は入力できますが無効となります）。

［関連コマンド］

line vty
ip ssh
ip ssh version

8.2.5 ip ssh macs

SSHv2 サーバで使用する MAC 方式の制限を行います。

本装置の SSHv2 サーバで許可する MAC 方式を，並べて指定します。

［入力形式］

情報の設定

ip ssh macs <MAC algorithm> [<MAC algorithm> […]]

情報の削除

no ip ssh macs

［入力モード］

(config)

［パラメータ］

<MAC algorithm>

本パラメータ省略時の初期値

省略できません。

値の設定範囲

以下の MAC 方式名を指定します。

表 8.2-2 MAC 方式

項番	MAC 方式名
1	hmac-md5
2	hmac-md5-96
3	hmac-sha1
4	hmac-sha1-96

［コマンド省略時の動作］

SSHv2 サーバで許可する MAC 方式は，hmac-md5，hmac-md5-96，hmac-sha1，hmac-sha1-96 です。

［通信への影響］

なし

［設定値の反映契機］

次回のログインから運用に反映されます。

［注意事項］

- SSH サーバを動作させるために，ip ssh と line vty の設定が必要です。
- 本設定は，SSHv1 ではプロトコル上無効となります(入力できますが無効となります)。

［関連コマンド］

line vty
ip ssh
ip ssh version

8.2.6 ip ssh authkey

SSH サーバで公開鍵認証に使用するユーザ公開鍵の登録を行います。

公開鍵を登録できるユーザは装置全体で 10 人までですが，有効となるユーザは運用コマンド adduser で登録されたログインユーザ名と一致するユーザだけです。

登録できる公開鍵は 1 ユーザ当たり最大 10 個，装置全体で最大 10 個です。

［入力形式］

情報の設定

ip ssh authkey <user name> <authentication key name>
{ “<publickey>” | load-key-file <file name> }

情報の削除

no ip ssh authkey <user name> <authentication key name>

［入力モード］

(config)

［パラメータ］

<user name>

SSH サーバ機能で公開鍵を登録するユーザ名を設定します。

本装置のログインユーザ名と同じユーザ名を設定したときに，有効なユーザとなります。

本パラメータ省略時の初期値

省略できません。

値の設定範囲

ユーザ名(16 文字以下)。

１文字目は英字，２文字目以降は英数字です。

<authentication key name>

ユーザ公開鍵のインデックスのために任意の名称を設定します。

鍵はユーザ毎に 10 個まで登録できます。他の鍵と名称が重複しないように設定してください。

本パラメータ省略時の初期値

省略できません。

値の設定範囲

鍵名称：英数字とアンダースコア（_）とハイフン（－）で 14 文字以下

{”<publickey>”| load-key-file <file name>}

公開鍵認証を行うユーザ公開鍵内容を登録します。

本パラメータ省略時の初期値

省略できません。

値の設定範囲

ダブルクォート（”）で囲んだユーザ公開鍵の内容を直接入力します。

公開鍵は最大 900 文字まで入力可能です。

または，load-key-file に続けて RAMDISK 上のユーザ公開鍵ファイル名を設定します。

ファイル名にはパスを指定できます。

ファイル名は最大 64 文字までで数字と英大文字が入力可能です。

・登録できる公開鍵の種類

SSHv1 形式の RSA 公開鍵または, SECSH 形式の DSA と RSA, OpenSSH 形式の DSA と RSA 公開鍵を登録できます。

鍵のコメント部分を含めて 900 文字まで入力可能です。登録可能な鍵の bit 長は以下の表になります。

900 文字以内で登録可能な公開鍵の bit 長

公開鍵の種類		登録可能 bit 長
SSHv1	RSA	512～2560
SSHv2	DSA	512～1536
	RSA	512～5120

※コメント部分なしの場合

（コメント部分の文字数によっては，登録可能 bit 長が減少します）

なお，コンフィグレーション上に表示される鍵形式は，

”鍵内容 コメント”となります。

・コメントの内容

コメントの文字は，英数字と特殊文字が入力可能です。詳細は「コンフィグレーションコマンドレファレンス　文字コード一覧」を参照してください。

ただし，次の文字は使用できないのでご注意ください。

・大カッコ始め（{）

・大カッコ終わり（}）

・シングルクォート（’）

・セミコロン（;）

・ドル（$）

・逆シングルクォート（ ‘）

・バックスラッシュ文字（¥）

使用できない文字がコメントとして設定されている場合は，ピリオド（.）に変換して読み込まれます。

・公開鍵内容を直接ダブルクォート（”）で囲んで登録する場合

入力する鍵の部分に改行や空白を含めず 1 行で入力してください。空白の後はコメントとみなされます。

SECSH 形式の公開鍵は改行を含んでいるため，すべての改行を取り除いて入力してください。なお，ヘッダ(Comment:コメント等)，開始・終了マーカを除いた，鍵の部分だけを入力してください(次図点線部分)。ヘッダ(Comment:コメント等)，開始・終了マーカは入力できません。

図 8.2-1 SECSH 形式の公開鍵の手入力範囲

```
---- BEGIN SSH2 PUBLIC KEY ----
Subject: gr4000
Comment: "1024-bit dsa, gr4000, Tue Oct 22 2002 16:21:35 +0900"
AAAAB3NzaC1kc3MAAACBAPQX4hUjicV2cuSbb0eYug3Zwe1wdveLixNAcRX15dh8XDDIv1
drKW6LnxTDiM8wfsEPDoOC0Zwae9V0LgpBFXqdNAHlBSPeKVEUvSBah+romEWRuPgBHIkJ
Wg3FbzkHV8cYiQxzAZT87RunikN9j2kq+ftoJIs7IWR4gHXby/JTAAAAFQDTl3fYwEZaZE
F1ZATkUeLsaBnn/wAAAIEAhy3mVaF87Pjjbaq+XY+l2mjIOptqGb7KcTKvbfb2JZVscidx
zOaKnNWRMJtsZSyMXkpdEjaWNmQvbV6MDGn3PYX63CLomIsWUPxdo7bcOJFyx1GvZ4bef7
JTP9x048/lFSwQTL7bKeXZ9cidgGXMmch8Tz15WSu8rP+t3m/yS7gAAACAZ/yWFB1rl8Be
Nkvcsmilupce2hb2uaef/4I7ymPT9irDQsfRY3RxiG5K0Uh7g84j9WFtx/y9KtFk46hUiz
NYnkkVcEwjo1uTbhtRpehF0bUYPyQu+ZxFDHZ3vB1o0NOfa0U4xME18RC4CHax+Fm/OUMd
PzpzAD6FZHS+9zkdi7k=
---- END SSH2 PUBLIC KEY ----
```

OpenSSH 形式の鍵においては，”ssh-rsa”や”ssh-dss”部分をのぞいた鍵部分だけをコメント部分を含めて途中で改行が入力されないようにして，1 行で入力してください(次図点線部分)。

図 8.2-2 OpenSSH 形式の公開鍵の手入力範囲

```
ssh-rsa AAAAB3NzaC1yc2EA…略…31fPFCmbGSxask97cCWCRwhNoffsjHRnn5hE= staff@OpenSSH-Client
```

・load-key-file でファイル名を指定する場合

ユーザ公開鍵はあらかじめ sftp, ftp 等で本装置の RAMDISK へ転送してそのファイル名を指定してください。

［コマンド省略時の動作］
公開鍵認証を使用してのログインはできません。

［通信への影響］
なし

［設定値の反映契機］
設定値変更後，すぐに運用に反映されます。

［注意事項］
- SSH サーバを動作させるために，ip ssh と line vty の設定が必要です。
- 本設定にてユーザ公開鍵を設定したユーザ名が，本装置のログインアカウントに登録されていない場合は，運用コマンド adduser でアカウントを新規登録した時点で，当該アカウントのユーザ公開鍵が自動的に有効になります。

［関連コマンド］
line vty
ip ssh

8.2.7 transport input

リモート運用端末から各種プロトコルを使用してのアクセスを制限するために使用します。

telnet または SSH のうち，指定されたプロトコルでだけアクセスを許可し，指定されていないプロトコルはアクセスを制限します。

［入力形式］

情報の設定

transport input {telnet | ssh | all | none}

情報の削除

no transport input

［入力モード］

(config-line)

［パラメータ］

{ telnet | ssh | all | none }

telnet : telnet プロトコルでのリモートアクセスを受け付けます。

ssh : SSH プロトコルでのリモートアクセスを受け付けます。

all : すべてのプロトコルでのリモートアクセスを受け付けます(telnet と SSH)。

none : すべてのプロトコルでのリモートアクセスを受け付けません。

本パラメータ省略時の初期値

省略できません。

値の設定範囲

telnet，ssh，all，または none

［コマンド省略時の動作］

telnet と SSH(ip ssh 設定時)プロトコルでのリモートアクセスを受け付けます。

［通信への影響］

なし

［設定値の反映契機］

設定値変更後，すぐに運用に反映されます。

［注意事項］

- SSH を使用する場合は，グローバルコンフィグレーションモードの ip ssh 設定が必要です。
- ftp 接続を許可/制限する場合は，グローバルコンフィグレーションモードの ftp-server で設定

してください。

［関連コマンド］

line vty
ip ssh

8.3　コンフィグレーションコマンドのエラーメッセージ

表 8.3-1　SSH コンフィグレーションコマンドエラーメッセージ

メッセージ	内容
ssh: Can’t execute.	実行できません。
ssh: ’<File name>’ file open error.	指定ファイルがオープンできません。
	<File name>：指定ファイル
ssh: input file is bad format.	入力ファイルが不正な形式です。
ssh: The public key is too long.	公開鍵が長すぎます。
ssh: The public key is bad format.	公開鍵が不正な形式です。
ssh: Can not delete it because data is not corresponding.	公開鍵がありません。
ssh: Public keys are a maximum of 10 entries.	公開鍵は最大 10 エントリです。

運用コマンドレファレンス編

9. 運用・保守機能

本章はSSHサーバの運用・保守機能についての運用コマンドレファレンスです。

9.1　運用コマンド一覧

本機能は, 本装置から他の装置に対して SSH で接続を実施する場合や, SSH サーバに関する, ホスト鍵ペアの再生成やサーバの状態確認などを運用コマンドにより実行します。本装置でサポートする機能一覧を表 9.1-1に示します。

表 9.1-1 運用コマンドサポート機能一覧

項番	分類	コマンド	機能
9.2.1	ホスト鍵管理	show ssh hostkey	ホスト公開鍵 表示コマンド
9.2.2		set ssh hostkey	ホスト鍵ペア 変更コマンド
9.2.3	サーバ保守	show ssh logging	SSH サーバトレース情報 表示コマンド
9.2.4		clear ssh logging	SSH サーバトレース情報 消去コマンド
9.2.5	ログインユーザ管理	show sessions (who)	ログインユーザ情報　表示コマンド

9.2　運用コマンド詳細

9.2.1　show ssh hostkey

［機能］
本装置の SSHv1/SSHv2 ホスト公開鍵と Fingerprint の表示を行うコマンドです。

［入力形式］
show ssh hostkey

［パラメータ］
なし
本装置の SSHv1/SSHv2 のホスト公開鍵と Fingerprint を表示します。

［入力モード］
一般ユーザモード

［実行例］
SSHv1/SSHv2 ホスト公開鍵と Fingerprint を表示します。

```
> show ssh hostkey

Date 20XX/06/11 09:32:06 UTC

******* SSHv1 Hostkey *******

1024 65537 112676670827222279613762898147415720811259820741286658557999554110106264702311394312072911780834527230005697578940119016961048430141098060487096288989327916987130855661965390234331404048434562524465674116445196870273015196997458417194179959606837336630394465705358354562069439020403567624278556712546554491863

Fingerprint for key:
xifik-kigez-mogot-zysom-pidyg-kutop-holam-rudib-negof-lilyk-lyxax
Fingerprint(HEX) for key:
7a:79:c1:da:db:69:27:42:e4:48:ab:5c:86:18:a6:04

******* SSHv2 Hostkey *******

MIHxMIGpBgcqhkjOOAQBMIGdAkEA/UNXOgmhyXWRcOBZLun6hspiuS/Q/N/KuOstYrD5kQr7vTcNrCNZDYDnCVFfrC6/xyBQGPOfhUBpRUc7eoJpMwIVAOLUu3B5ClDwieTcsYqmu517ABBXAkEAgTfPLQcVxAiqkTowSvA/tVyXwCPovs3nBBK8S9nFW+ZzGm9oR2RccrbfulnOAkaoUVmacGBxvD+z9qhhHgiNjQNDAAJAeBvdcIgYEly7EUlObb1KxTGe97hxdM31vhJnzGkgrzlyEhf2+d1V756AOmArKvnkq1MKlaFj4vxnqqGVypRfng==

Fingerprint for key:
xemos-tibod-rukys-zekos-puvel-nufet-tihin-leroz-cufis-zaruc-daxox
Fingerprint(HEX) for key:
6e:3c:a1:10:ab:02:7f:73:d8:aa:7e:40:d0:51:6e:f8
```

>

［応答メッセージ］

メッセージ	内容
ssh: Can't execute.	ホスト鍵が異常で実行できません。もしくはコマンド実行エラーです。 ［対応］ 1. set ssh hostkey でホスト鍵を作り直してください。 2. コマンドを再実行してください。

［注意事項］

・ご使用のクライアントによってサポートされている Fingerprint の形式が異なりますので，本装置では bubblebabble 形式と HEX 形式の両方を表示します。

9.2.2 set ssh hostkey

［機能］
本装置の SSHv1/SSHv2 ホスト鍵ペア(公開鍵・秘密鍵)の変更を行うコマンドです。
変更後のホスト鍵を有効にするために，本装置の再起動が必要です。
工場出荷時にはデフォルトのホスト鍵ペアが設定されています。本コマンドによるホスト鍵ペアの変更を強くお勧めします。一度変更を実施すれば，通常変更の必要はありません。

［入力形式］
set ssh hostkey

［パラメータ］
なし
　本装置の SSHv1/SSHv2 ホスト公開鍵ペアの変更を行います。

［入力モード］
装置管理者モード

［実行例］
SSHv1/SSHv2 のホスト鍵ペアを変更します。

```
# set ssh hostkey

WARNING!!
Would you wish to change the SSH (v1 and v2) Hostkeys? (y/n): y

*** Changing the SSHv1 Hostkey, Please wait a minute ***
Generating public/private rsa1 key pair.
The key fingerprint is:
42:13:3c:08:3f:1e:96:11:3c:be:86:c8:39:f5:48:d9 1024-bit rsa1 hostkey

*** Changing the SSHv2 Hostkey, Please wait a minute ***
Generating public/private dsa key pair.
The key fingerprint is:
d6:b4:17:37:1b:8f:8c:1c:6d:bf:d0:ae:11:c7:5d:85 1024-bit dsa hostkey

The Hostkeys (SSHv1 and SSHv2) were generated Completely.
Please execute the reload command,
because the new hostkeys becomes effective after reboot.

#
```

［応答メッセージ］

メッセージ	内容
The Hostkeys (SSHv1 and SSHv2) were generated Completely.	SSHv1 と SSHv2 ホスト鍵の変更生成が完了しました。
ssh:Can't execute.	コマンドが実行できませんでした。 ［対応］ コマンドを再実行してください。

［注意事項］

・工場出荷時にはデフォルトホスト鍵が設定されています。本コマンドによるホスト鍵の変更を強くお勧めします。一度変更を行うと，その後の変更は通常必要ありません。
・変更後のホスト鍵を有効にするために，本装置の再起動が必要です。
・ホスト鍵の作成中断は出来ません（本コマンド実行中の[CTRL+C]は未サポートです）。

9.2.3 show ssh logging

[機能]
SSH サーバの運用状態のトレースログを表示します。

[入力形式]
show ssh logging

[入力モード]
一般ユーザモード

[パラメータ]
なし

[実行例]

```
> show ssh logging

Date 20XX/05/31 19:32:59 UTC
20XX/05/31 19:32:48 sshd Closing connection to 192.168.10.100.
20XX/05/31 19:32:48 sshd Disconnecting: Too many authentication failures for operator.
20XX/05/31 19:32:48 sshd Failed password for operator from 192.168.10.100 port 2174.
20XX/05/31 19:32:47 sshd Failed password for operator from 192.168.10.100 port 2174.
20XX/05/31 19:32:47 sshd Failed password for operator from 192.168.10.100 port 2174.
20XX/05/31 19:32:46 sshd Failed password for operator from 192.168.10.100 port 2174.
20XX/05/31 19:32:45 sshd Failed password for operator from 192.168.10.100 port 2174.
20XX/05/31 19:32:36 sshd Sent 768 bit server key and 1024 bit host key.
20XX/05/31 19:32:36 sshd RSA key generation complete.
20XX/05/31 19:32:35 sshd Generating 768 bit RSA key.
20XX/05/31 19:32:35 sshd Client protocol version 1.5; client software version TTSSH/2.45.
20XX/05/31 19:32:35 sshd Connection from 192.168.10.100 port 2174.
20XX/05/31 19:31:30 sshd Entering interactive session for SSH2.
20XX/05/31 19:31:30 sshd Accepted publickey for operator from 192.168.10.100 port 2173 ssh2.
20XX/05/31 19:31:30 sshd Found matching DSA key: 16:0b:6c:cb:12:83:f2:25:69:1b:c4:73:8e:37:9f:c0.
20XX/05/31 19:31:30 sshd Failed none for operator from 192.168.10.100 port 2173 ssh2.
20XX/05/31 19:31:23 sshd kex: server->client aes256-cbc hmac-sha1.
20XX/05/31 19:31:22 sshd kex: client->server aes256-cbc hmac-sha1.
20XX/05/31 19:31:22 sshd Client protocol version 2.0; client software version TTSSH/2.45.
20XX/05/31 19:31:22 sshd Connection from 192.168.10.100 port 2173.

>
```

[応答メッセージ]

メッセージ	内容
ssh: Can't execute.	コマンドが実行できませんでした。 ［対応］ コマンドを再実行してください。
There is no logging data.	表示情報がありません。

[ログフォーマット]

yy/mm/dd hh:mm:ss イベント発生部位 message

1 2 3

1.時刻 … 採取年，月，日，時，分，秒を表示します。
2.プロセス番号 … サーバのプロセス番号を表示します。
3.ログメッセージ … メッセージ部分が表示されます。

[ログメッセージ]

メッセージ	内容
Generating 768 bit RSA key.	RSA サーバ鍵を生成しています。
RSA key generation complete.	RSAサーバ鍵を生成しました。
Sent 768 bit server key and 1024 bit host key.	サーバ鍵とホスト鍵を送信しました。
Connection from <host> port <port>	<host>の<port>から接続されています。 <host>：リモートホスト <port>：リモートホストのポート
Failed <authentication method> for <user> from <host> port <port> [ssh2]	ユーザ認証に失敗しました。 <authentication method>：認証方式 <user>：ユーザ名 <host>：リモートホスト <port>：リモートホストのポート [ssh2]：SSHv2の場合に表示します
Found matching <key type> key: <fingerprint>	登録されているユーザ公開鍵が見つかりました。 <key type>：公開鍵の種類 <fingerprint>：公開鍵のフィンガープリント
Accepted <authentication method> for <user> from <host> port <port> [ssh2]	ユーザ認証に成功しました。 <authentication method>：認証種類 <user>：ユーザ名 <host>：リモートホスト <port>：リモートホストのポート [ssh2]：SSHv2の場合に表示します
Did not receive identification string from <host>	<host>からバージョン識別子を受信できませんでした。 <host>：リモートホスト
Client protocol version <version>; client software version <software version>	クライアントのプロトコルバージョンとソフトウェアバージョンを表示します。

	<version>：プロトコルバージョン <software version>：ソフトウェアバージョン
kex: client->server <cipher> <mac>	クライアントからサーバへ鍵交換ネゴシエーションしています。 <cipher>：共通鍵暗号方式名 <mac>：MAC方式名
kex: server->client <cipher> <mac>	サーバからクライアントへ鍵交換ネゴシエーションしています。 <cipher>：共通鍵暗号方式名 <mac>：MAC方式名
Entering interactive session for SSH2.	SSHv2のセッションを開始しました。
Entering interactive session.	SSHv1のセッションを開始しました。
fatal: no matching cipher found: client <client ciphers> server <server ciphers>	サーバとクライアントで適合する共通鍵暗号方式がありませんでした。 <client ciphers>：クライアント側の暗号方式リスト <server ciphers>：サーバ側の暗号方式リスト
fatal: no matching mac found: client <client macs> server <server macs>	サーバとクライアントで適合するMAC方式がありませんでした。 <client macs>：クライアント側のMAC方式リスト <server macs>：サーバ側のMAC方式リスト
Received disconnect from <host>:	リモートホストによって切断されました。(理由無しの場合) <host>：リモートホスト
Disconnecting: Too many authentication failures for <user>	<user>は何度も認証失敗したため，切断しました。 <user>：ユーザ名
fatal: Read from socket failed: Connection reset by peer	コネクションが切断されました。
Connection closed by <host>	<host>との接続が切れました。 <host>：リモートホスト
Closing connection to <host>	<host>との接続を終了しました。 <host>：リモートホスト

［注意事項］
・ログは最大 1024 件まで保存されます。これを超えた場合，古いログから自動的に消去されます。
・SSH サーバのログは本装置の電源を切ったり，再起動をしたりすると消去されます。

9.2.4 clear ssh logging

［機能］
SSH サーバの運用状態のトレースログを消去します。

［入力形式］
clear ssh logging

［入力モード］
装置管理者モード

［パラメータ］
なし

［実行例］
```
# clear ssh logging
Would you wish to CLEAR the SSH server's log? (y/n): y

Clear complete.
```

［応答メッセージ］

メッセージ	内容
Clear complete.	ログの消去が完了しました。
ssh: Can't execute.	コマンドが実行できませんでした。 ［対応］ コマンドを再実行してください。

［注意事項］
なし

9.2.5 show sessions (who)

[機能]
本装置にログインしているユーザを表示します。

[入力形式]
show sessions
who

[入力モード]
一般ユーザモードおよび装置管理者モード

[パラメータ]
なし

[実行例]
```
> show sessions

Date 20XX/05/31 21:09:13 UTC
 Username          Type     Login                Source
*staff             console  20XX/05/31 20:33:43  -
 staff             vty0     20XX/05/31 20:26:19  192.168.1.246
 staff             vty1     20XX/05/31 20:27:54  192.168.1.240
 staff             ftp      20XX/05/31 20:34:40  192.168.1.241
 staff             sftp     20XX/05/31 20:03:27  192.168.1.203

>
```

[表示説明]

項目	意味	詳細
Username	ユーザ名称	コマンドを実行しているユーザは，ユーザ名称の前にアスタリスク（*） を表示します。
Type	接続タイプ	console：ローカル接続 vty0：telnet/ssh 接続 vty1：telnet/ssh 接続 ftp：ftp 接続 sftp：sftp 接続
Login	ログイン時間	－
Source	IP アドレス	telnet / ftp / ssh / sftp クライアントを実行している装置の IP アドレスです。 console はハイフン（－）固定です。

[注意事項]
なし

メッセージ・ログレファレンス編

10. ログメッセージ

本章はSSHに関する本装置のログメッセージ一覧です。

10.1 ログメッセージ一覧

表 10.1-1 ログメッセージ一覧(イベント発生部位＝SESSION)

項番	イベントレベル	イベント発生部位	メッセージ識別子	メッセージテキスト
	内容			
1	E3	SESSION	00e00000	Authentication login xxxxxxxx RADIUS accept.
	RADIUS 認証に成功しました。 xxxxxxxx：ユーザ名 [対応] なし。			
2	E3	SESSION	00e00001	Authentication login xxxxxxxx RADIUS reject.
	RADIUS 認証に失敗しました。 xxxxxxxx：ユーザ名 [対応] 1.本装置に対してコンフィグレーションで許可されたリモートホストから不正なアクセスが行われた可能性があります。リモートホストの運用状況を確認してください。 2.このログは正規のユーザがログイン時に誤った操作（パスワード入力間違いなど）をした場合にも収集されます。 従って，このログが収集されてもリモートホストの運用状況に問題がない場合もあります。 3. RADIUS サーバの設定を確認してください。			
3	E3	SESSION	00e00002	Authentication login xxxxxxxx RADIUS no response.
	RADIUS 認証で，RADIUS サーバから応答がありませんでした。 xxxxxxxx：ユーザ名 [対応] 1.RADIUS サーバの IP アドレスが誤っていないか，コンフィグレーションを確認してください。 2.RADIUS サーバのポート番号が誤っていないか，コンフィグレーションを確認してください。			
4	E3	SESSION	00e00003	Authentication login xxxxxxxx RADIUS server configuration is not defined.
	RADIUS 認証用の RADIUS サーバが設定されていません。 xxxxxxxx：ユーザ名 [対応] RADIUS コンフィグレーションが設定されているか確認してください。			

5	E3	SESSION	00e00004	Authentication login xxxxxxxx RADIUS over request.
	RADIUS 認証で，RADIUS サーバへの同時最大送信数（256）を超過しました。 xxxxxxxx：ユーザ名 [対応] RADIUS 認証の要求負荷が高くなっています。 一時的な場合は，再度ログインを実施してください。 継続的に発生する場合は，システム構成を見直してください。			
6	E3	SESSION	00e00006	Authentication login xxxxxxxx RADIUS invalid server specified.
	RADIUS 認証で内部エラーが発生しました。 xxxxxxxx：ユーザ名 [対応] なし。			
7	E3	SESSION	00e00007	Authentication login xxxxxxxx RADIUS return error. code = xx
	RADIUS 認証で内部エラーが発生しました。 xxxxxxxx：ユーザ名 code = xx：原因コード（メーカ解析用情報） [対応] なし。			
8	E3	SESSION	00e00008	Authentication login xxxxxxxx RADIUS time out.
	RADIUS 認証でタイムアウトが発生しました。 xxxxxxxx：ユーザ名 [対応] 再度ログインを実施してください。			
9	E3	SESSION	00e00100	"users file' is corrupted. Started by default.
	'users file'が壊れています。デフォルトユーザで起動しました。 [対応] なし。			
10	E3	SESSION	00e00101	Failed to write 'users file'.
	'users file'ファイルの書き込みに失敗しました。 [対応] 運用コマンド format flush を実行してください。			

11	E3	SESSION	00e02000	Unknown host address <ip address>
	SSH で本装置に接続しようとしましたが，<ip address>からの接続を許可しませんでした。 <ip address>：SSH で接続しようとした IPv4 アドレスまたは IPv6 アドレス [対応] 1.本装置に対して不正なアクセス（コンフィグレーションで許可された以外のリモートホストからのアクセスが行われた可能性があります。<ip address>のリモートアクセスを確認してください。 2. <ip address>からのリモートアクセスを許可している場合は，コンフィグレーションに誤りがある可能性があります。コンフィグレーションの設定内容を確認してください。 3. <ip address>からのリモートアクセスを許可したい場合は，コンフィグレーションでアクセス許可の設定してください。			
12	E3	SESSION	00e02001	Login incorrect xxxxxxxx.
	ログインに失敗しました。 xxxxxxxx：ユーザ名 [対応] 1.本装置に対してコンソールまたはコンフィグレーションで許可されたリモートホストから不正なアクセス（アカウント，パスワード認証で失敗）が行われた可能性があります。 2.コンソールまたはコンフィグレーションで許可したリモートホストの運用状況を確認してください。このログは正規のユーザがログイン時に誤った操作をした場合にも収集されます。従って，このログが収集されてもリモートホストの運用状況に問題がない場合もあります。 3.本装置に運用コマンド adduser により登録済みのアカウントかどうかを確認してください。（確認方法：運用コマンド show users で確認）			
13	E3	SESSION	00e02002	Login refused for too many users logged in.
	SSH で接続しようとしましたが，ログインユーザ数をオーバーしたため，接続を許可しませんでした。 [対応] 1.現在ログインしているユーザ数を確認してください。 2.必要であれば，コンフィグレーションでログインできるユーザ数の制限を増加させてください。			
14	E3	SESSION	00e02003	Login xxxxxxxx from <ip address> (vtynn).
	SSH(vtynn)でユーザ(xxxxxxxx from <ip address>)がログインしました。 xxxxxxx：ユーザ名 from <ip address>：リモートログインしたユーザの IPv4 アドレスまたは IPv6 アドレス vtynn：0～15 [対応] なし。			
15	E3	SESSION	00e02003	Login xxxxxxxx from <ip address> (sftp).
	sftp でユーザ(xxxxxxxx from <ip address>)がログインしました。 xxxxxxx：ユーザ名 from <ip address>：リモートログインしたユーザの IPv4 アドレスまたは IPv6 アドレス [対応] なし。			

16	E3	SESSION	00e02004	Logout xxxxxxxx from <ip address> (vtynn).
	SSH(vtynn)のユーザ(xxxxxxxx from <ip address>)がログアウトしました。 xxxxxxx：ユーザ名 from <ip address>：リモートログアウトしたユーザの IPv4 アドレスまたは IPv6 アドレス vtynn：0～15 [対応] なし。			
17	E3	SESSION	00e02004	Logout xxxxxxxx from <ip address> (sftp).
	sftp のユーザ(xxxxxxxx from <ip address>)がログアウトしました。 xxxxxxx：ユーザ名 from <ip address>：リモートログアウトしたユーザの IPv4 アドレスまたは IPv6 アドレス [対応] なし。			
18	E3	SESSION	00e02100	Connection reset by xxxxxxxx (sftp).
	sftp のセッションが切断されました。 xxxxxxxx：ユーザ名 [対応] なし。			
19	E9	SESSION	00e00002	Authentication login xxxxxxxx RADIUS message queue error. errno=xx
	RADIUS 認証で内部エラー（メッセージ queue 異常応答）が発生しました。 xxxxxxxx：ユーザ名 errno=xx：メーカ解析用情報 [対応] なし。（自動的に装置が再起動されます。）			

付録

A. 用語解説

英字

- **3des(Triple Data Encryption Standard)**
  共通鍵暗号方式の DES を 3 回適用して強度を増したものです。
- **AES(Advanced Encryption Standard)**
  米国商務省標準技術局(NIST)が制定した，次世代標準暗号化方式です。
- **blowfish**
  Bruce Schneier 氏が考案した 448bit 可変長キー暗号化アルゴリズムです。
- **bubblebabble 形式**
  Fingerprint の表示形式の 1 つです。
  例
  xoriv-socym-demed-cylam-fyhum-davep-dusal-koras-hyfep-pecyt-roxyx
- **Diffie-Hellman 鍵交換**
  鍵交換アルゴリズムで，第三者に盗聴される可能性のある通信路上で安全に鍵の交換を行います。
- **DSA(Digital Signature Algorithm)**
  デジタル署名アルゴリズムの 1 つです。
- **Fingerprint**
  鍵の指紋です。公開鍵に対してある特別の計算を行った結果であり，公開鍵が変わると Fingerprint も変わります。
- **FTP(File Transfer Protocol)**
  ネットワーク上のクライアントとサーバとの間で，ファイルの転送を行なうためのプロトコル(コマンド)のことです。
- **HEX 形式**
  Fingerprint の表示形式の 1 つです。
  例 19:46:78:28:ca:03:23:61:4c:09:b4:4b:06:97:8b:9d
- **hmac-sha1, hmac-sha1-96**
  MD4 アルゴリズムを改良した,160 ビットメッセージダイジェストアルゴリズムです。

- **hmac-md5, hmac-md5-96**
  現在,もっとも広く用いられているメッセージ要約関数で,任意長メッセージから 128 ビットの一方向ハッシュ値を生成します。
- **IPsec**
  IP パケットレベルでの暗号化と認証を行なうセキュリティ技術です。
- **IPv6**
  128 ビットの IP アドレスを持つ新しいインターネットプロトコルです。
- **HTTP(Hyper Text Transfer Protocol)**
  GET などの ASCII 文字コマンドを用いて WWW 情報をやり取りするプロトコルです。
- **OpenSSH**
  SSH の実装のひとつで，フリーに実装が行われているものです。
- **RADIUS(Remote Authentication Dial In User Service)**
  NAS(Network Access Server)に対して認証・課金機能を提供するプロトコルです。NAS は RADIUS のクライアントとして動作するリモートアクセスサーバ，ルータなどの装置のことです。
- **RLOGIN**
  ネットワーク経由でコンピュータを遠隔利用する際に使うプロトコルです。
- **RSA**
  公開鍵暗号アルゴリズムの一つです。
- **SECSH**
  SSH プロトコルの標準化を進めている，IETF の Secure Shell ワーキンググループのことです。
- **TCP ラッパー**
  サーバで各サービスを提供する際に，サービス要求を別のプログラムで受けて，アクセス制御やロギングを行う仕組みです。
- **TELNET**
  ネットワーク経由でコンピュータを遠隔利用する際に使うプロトコルです。
- **twofish**
  128bit のブロックサイズをもち，256bit までのキーを受け入れます。Blowfish の改良版です。
- **VPN(Virtual Private Network)**
  オープンネットワーク上で仮想的なクローズドネットワークを実現したものです。

あ行

- **アルゴリズム**
  ここでは，暗号化や復号する手順や方式のことです。
- **暗号化**
  データをある鍵によって組み替え，第三者に解読できないようにすることです。

か行

- **改ざん**
  ネットワーク上のクライアントーサーバ間の通信内容を第三者が変更し，不正な情報をやり取りさせることです。

・ **仮想端末**
　　コンピュータと端末間で通信プロトコルに依存しないアクセス制御手段を提供するための機能です。
・ **公開鍵**
　　公開鍵暗号方式での鍵ペアの一方で，相手に公開する鍵のことです。
・ **公開鍵認証**
　　パスワードを用いず，公開鍵で認証を行う方法です。ネットワーク上にはユーザの秘密情報が流れません。

た行

・ **ダイジェスト**
　　要約です。ある文字列の内容を短い文字列で表現したものです。
・ **データ圧縮**
　　データを圧縮しながら通信します。ただし，あらかじめ圧縮されたファイル (アップデートファイル等) には効果がありません。
・ **チャレンジ＆レスポンス**
　　サーバからのチャレンジメッセージに対して，正しいレスポンスを返すことで認証を行うことです。
・ **電子署名**
　　公開鍵暗号方式で，あるユーザの秘密鍵で変換したダイジェストは，そのユーザの公開鍵でだけ確認できることを利用した署名です。
・ **盗聴**
　　ネットワーク上の第三者が，通信の内容を盗み見することです。

な行

・ **なりすまし**
　　巧みにネットワークを操作し，偽者のホストが正規のホストに替わって接続を受け付けることです。

は行

・ **ハッシュ**
　　ある文字列の内容を短い文字列で表現するためのアルゴリズム・方法です。
・ **パスフレーズ**
　　公開鍵暗号方式で，鍵ペアを作成した際に，秘密鍵に対して暗号化するための鍵のことです。パスフレーズは，パスワードより長く設定できるという意味もあります。
・ **秘密鍵**
　　公開鍵暗号方式での鍵ペアの一方で，自身で秘密に保持しておく鍵のことです。
・ **ファイヤーウォール**
　　防火壁です。外部からの不正なパケットを遮断する仕組みです。
・ **フォールバック**
　　SSHv1 と SSHv2 を同じ TCP ポートで接続できるようにするために，自動的に切り替える仕組みのことです。
・ **復号**
　　暗号化されたデータを元のデータに戻すことです。

- **プロトコル**
  接続や通信の手順・方法です。

ま行

- **メッセージ認証コード(MAC)**
  データが通信中に改ざんされていないことを確かめるために，暗号化時に計算されてデータに添付されてくるコードです。

ら行

- **リモートコピーコマンド(rcp)**
  他のホストへファイルをコピーするコマンドです。
- **ローカルパスワード認証**
  サーバが保持しているユーザ名とパスワードのデータベースを基に，ユーザの認証を行う方法です。認証時，ユーザはユーザ名とパスワードをサーバに送る必要があります。

B. 準拠規格

表 B-1 SSH 規格

項番	規格	名称
1	RFC4251(2006 年 1 月)	The Secure Shell (SSH) Protocol Architecture
2	RFC4252(2006 年 1 月)	The Secure Shell (SSH) Authentication Protocol
3	RFC4253(2006 年 1 月)	The Secure Shell (SSH) Transport Layer Protocol
4	RFC4254(2006 年 1 月)	The Secure Shell (SSH) Connection Protocol
5	draft-ylonen-sshprotocol-00 (1995 年 11 月)	The SSH (Secure Shell) Remote Login Protocol
6	draft-ietf-secsh-publickeyfile-03 (2002 年 10 月)	SSH Public Key File Format
7	draft-ietf-secsh-filexfer-13 (2006 年 7 月)	SSH File Transfer Protocol

C. 謝辞(Acknowledgments)

LICENSE ISSUES
==============

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of
the OpenSSL License and the original SSLeay license apply to the toolkit.
See below for the actual license texts. Actually both licenses are BSD-style
Open Source licenses. In case of any license issues related to OpenSSL
please contact openssl-core@openssl.org.

OpenSSL License

```
/* ====================================================================
 * Copyright (c) 1998-2016 The OpenSSL Project.    All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *       notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *       notice, this list of conditions and the following disclaimer in
 *       the documentation and/or other materials provided with the
 *       distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *       software must display the following acknowledgment:
 *       "This product includes software developed by the OpenSSL Project
 *       for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *       endorse or promote products derived from this software without
 *       prior written permission. For written permission, please contact
```

```
 *       openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *       nor may "OpenSSL" appear in their names without prior written
 *       permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *       acknowledgment:
 *       "This product includes software developed by the OpenSSL Project
 *       for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.    IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).    This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */

 Original SSLeay License
 -----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.    The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.    The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
```

```
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
*       notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*       notice, this list of conditions and the following disclaimer in the
*       documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*       must display the following acknowledgement:
*       "This product includes cryptographic software written by
*        Eric Young (eay@cryptsoft.com)"
*       The word 'cryptographic' can be left out if the rouines from the library
*       being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*       the apps directory (application code) you must include an acknowledgement:
*       "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED.    IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed.    i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/
```