AX260A

Secure Shell（SSH）
ソフトウェアマニュアル

AlaxalA

■はじめに

このマニュアルは，Secure Shell(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 より前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-004）」

■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。
Internet Explorer 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。
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。
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。
ssh は SSH Communications Security Corp (www.ssh.com) 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。
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 つの編から構成されています。

第 1 編　コンフィグレーションガイド

本装置の SSH 機能の解説，SSH 機能を使用する場合のコンフィグレーション例，SSH サーバの管理運用について説明しています。

第 2 編　コンフィグレーションコマンドレファレンス

本装置に SSH 機能に関するコンフィグレーションコマンドについて説明しています。

第 3 編　運用コマンドレファレンス

本装置の SSH 機能に関する運用コマンドについて説明しています。

第 4 編　メッセージ・ログレファレンス

本装置の SSH 機能に関するログメッセージについて説明しています。

第 5 編　トラブルシューティングガイド

本装置の SSH 機能を運用中のトラブルシュートについて説明しています。

第 6 編　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１版）

■著作権

変更内容

■第 1 版の変更内容

表　変更内容

マニュアル名	追加・変更内容
全体	Ver.4.17 以降用に分離して新規作成

目次

第1編　コンフィグレーションガイド

1　SecureShell（SSH）

1.1 解説

1.1.1 概要

SSH は，クライアントからサーバへ，安全ではないネットワーク上で，セキュアに接続する機能です。

SSH を使用すると，クライアントとサーバが相互に認証し，通信内容を暗号化し，メッセージ認証によって通信内容が変更されていないことを確認します。このため，ネットワーク上の悪意ある第三者によるなりすまし，盗聴，改ざんから通信を保護できます。SSH を使用することで，telnet 接続の脅威（不正なりすましサーバへの誤接続，運用情報の流出，データの改ざんなど）から保護された，セキュアな運用管理を実現できます。telnet 接続による脅威および SSH 接続によるセキュアな運用管理を次の図に示します。

図 1-1 telnet 接続による脅威

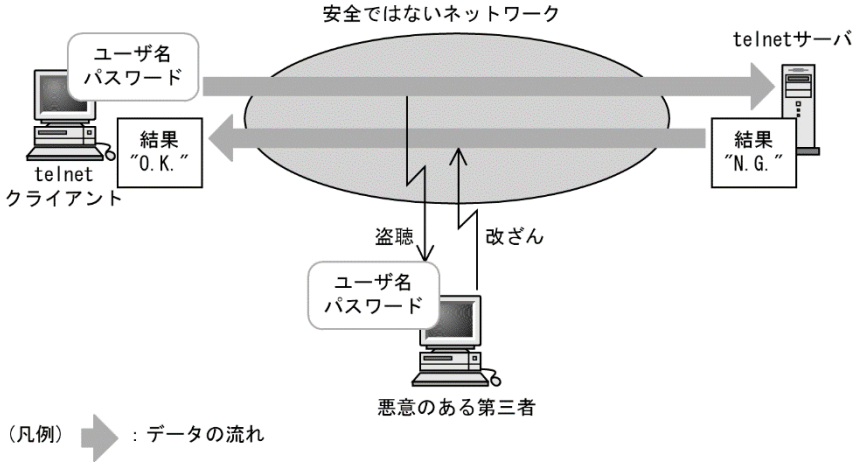
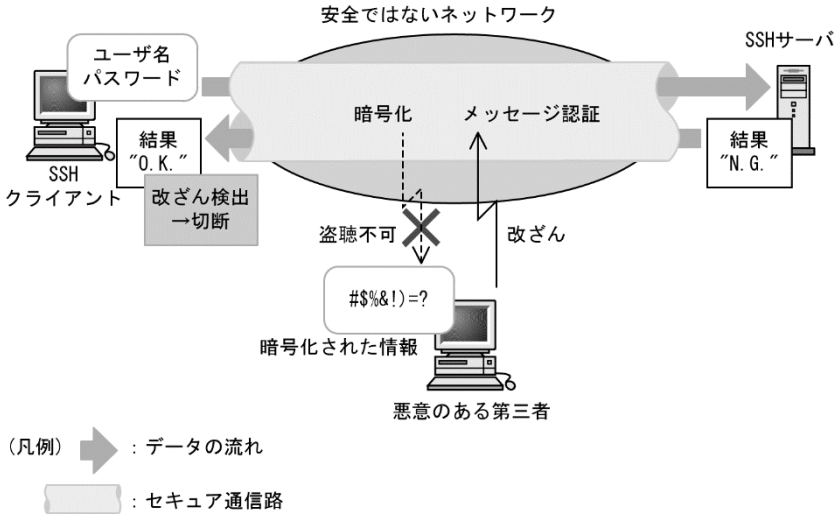


図 1-2 SSH 接続によるセキュアな運用管理



SSH サーバへ接続するユーザの認証方法として，telnet や FTP で使用されていたパスワード認証のほかに，より安全な公開鍵認証を使用できます。公開鍵認証を使用することで，パスワードが漏洩して他者に利用されることを防ぎます。

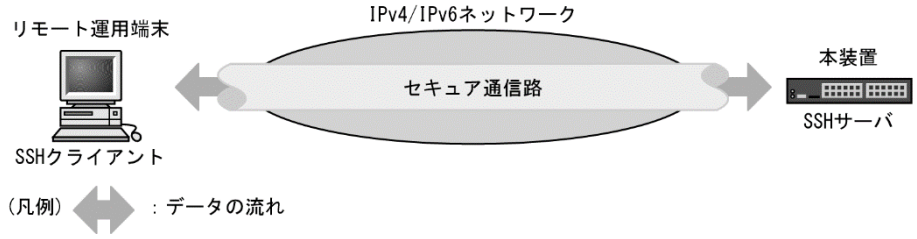
SSH にはバージョン 1（SSHv1）とバージョン 2（SSHv2）があります。本装置は SSHv1 と SSHv2 の両方をサポートしています。

しかし，できるだけ SSHv2 に限定して運用することを推奨します。理由は，SSHv2 が SSHv1 に比べてセキュリティが向上しているためです。SSHv2 ではメッセージ認証によって通信の改ざんを防ぎます。また，SSHv2 は SSHv1 よりも進歩した暗号技術を採用しています。

本装置の SSH 機能は，IPv4 ネットワークと IPv6 ネットワークのどちらでも使用できます。本装置は SSH サーバ機能をサポートしています。

本装置の SSH サーバ機能によって，セキュア通信路上でリモート運用端末から本装置へのログインやファイル転送を実現できます。リモート運用端末から本装置への SSH の接続例を次の図に示します。

図 1-3 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



1.1.2 SSH の基本機能

(1) セキュアリモートログイン

SSH が提供するセキュア通信路をリモートログインに使用する機能です。セキュアリモートログインを使用すると，インターネット経由でも安全に，運用端末から SSH サーバへログインできます。また，通信内容を他者に見られないため，安全な運用管理を実現できます。

本装置の運用にセキュアリモートログインを使用することで，インターネット経由でも運用端末から本装置へ安全にログインし運用できます。

(2) セキュア FTP（SFTP）

SSH が提供するセキュア通信路を使用して，FTP と同様の会話型インタフェースを使用し，クライアントとサーバ間でファイルを転送する機能です。ファイル転送のほかに，ファイル名を確認したりファイルを削除したりできます。

本装置の運用にセキュア FTP を使用することで，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実行できます。

1.1.3 サポート機能

本装置がサポートする SSH のサーバの役割，SSH プロトコルバージョン，SSH 接続に使用できるプロトコルを次の表に示します。

表 1-1 SSH サーバ・プロトコルバージョン・接続プロトコルサポート一覧

機能名		サポート有無
SSH サーバ		○
SSH クライアント		×
SSH プロトコルバージョン	バージョン 1（SSHv1）	○
	バージョン 2（SSHv2）	○
SSH 接続に使用できるプロトコル	IPv4	○
	IPv6	○

（凡例）○：サポート　×：未サポート

SSH の基本機能とサポート状況を次の表に示します。

表 1-2 SSH 機能サポート一覧

機能名	説明	サポート有無
セキュアリモートログイン	SSH を使用したリモートログイン	○
セキュアコマンド実行	SSH を使用したコマンド実行	×
セキュアコピー（SCP）	SSH を使用したファイルコピー	×
セキュア FTP（SFTP）	SSH を使用したファイル転送	SSHv1：× SSHv2：○
認証エージェント	認証エージェント機能	×
ポート転送	TCP 転送機能	×
X11 プロトコル自動転送	X11 を自動転送する機能	×
データ圧縮	通信のデータを圧縮する機能	×

（凡例）○：サポート　×：未サポート

SSHv1 のセキュリティ機能の方式別サポート状況を次の表に示します。

表 1-3 SSHv1 セキュリティ機能の方式別サポート一覧

機能名	方式		サポート有無
ホスト認証	公開鍵認証	RSA	○
ユーザ認証	公開鍵認証	RSA	○
	パスワード認証		○
	RHOSTS 認証		×
	RHOSTS + RSA 認証		×
暗号化	共通鍵暗号	3des-cbc	○
	その他の方式		×

（凡例）○：サポート　×：未サポート

SSHv2 のセキュリティ機能の方式別サポート状況を次の表に示します。

表 1-4 SSHv2 セキュリティ機能の方式別サポート一覧

機能名	方式		サポート有無
ホスト認証	公開鍵認証	RSA，DSA	○
	証明局証明書による公開鍵認証		×
	PGP 証明書による公開鍵認証		×
ユーザ認証方法	公開鍵認証	RSA，DSA	○
	証明局証明書による公開鍵認証		×
	PGP 証明書による公開鍵認証		×
	ホストベース認証		×
	パスワード認証		○
鍵交換	diffie-hellman-group1-sha1，diffie-hellman-group14-sha256		○
	その他の方式		×
共通鍵暗号	aes128-ctr，aes192-ctr，aes256-ctr，aes128-cbc，aes192-cbc，aes256-cbc		○
	3des-cbc		○
	blowfish-cbc		×
	twofish128-cbc		×
	その他の方式		×
メッセージ認証コード	hmac-sha2-512，hmac-sha2-256，hmac-sha1，hmac-md5，hmac-sha1-96，hmac-md5-96		○
	その他の方式		×

（凡例）○：サポート　×：未サポート

SSH サーバのログインセキュリティと RADIUS 対応のサポート状況を次の表に示します。（本装置は TACACS＋未サポートです。）

表 1-5 SSH サーバのログインセキュリティ機能サポート一覧

機能名		サポート有無
同時にログインできるユーザ数の設定		○
リモート運用端末の IP アドレスによる制限		○
ログインメッセージ	ログイン前	×
	ログイン後	×
RADIUS	認証	○

（凡例）○：サポート　×：未サポート

1.1.4 SSH のセキュリティ機能

SSH には，セキュリティを確保するために暗号技術を使用する機能が五つあります。

1. ホスト認証
2. ユーザ認証
3. セッション鍵の共有
4. 暗号化
5. メッセージ認証（SSHv2 だけ）

以降，各機能について説明します。

(1) ホスト認証

ホスト認証は，SSH クライアントが SSH サーバを認証する機能です。

各 SSH サーバはそれぞれ異なるホスト鍵ペアを保持しています。SSHv1 では，ホスト公開鍵を使用してクライアントからサーバへ公開鍵暗号で通信することによって，サーバを認証します。SSHv2 では，サーバがホスト秘密鍵でデジタル署名を作成し，クライアントがホスト公開鍵で署名を確認することによりサーバを認証します。

本装置がサポートするホスト鍵ペアの公開鍵アルゴリズムとサイズを次の表に示します。

表 1-6 本装置がサポートするホスト鍵ペアの公開鍵アルゴリズムとサイズ

SSH バージョン	公開鍵アルゴリズム	鍵のサイズ
SSHv1	RSA	1024bit
SSHv2	RSA	1024bit,, 2048bit, 3072bit
	DSA	1024bit

本装置の SSH サーバ機能では，デフォルトで SSHv1 用 RSA 1024bit と SSHv2 用 DSA 1024bit のホスト鍵ペアを生成します。デフォルト以外の鍵ペアを使用する場合や鍵ペアを生成し直す場合は，運用コマンド set ssh hostkey を使用してください。SSHv2 の不要なアルゴリズムの鍵ペアを削除する場合は，運用コマンド erase ssh hostkey を使用してください。なお，SSHv1 の RSA ホスト鍵ペアは削除できません。

SSH クライアントでは，過去に接続したサーバのホスト公開鍵を保持しています。SSH クライアントでは，SSH サーバへ初めて接続するときやサーバのホスト公開鍵が変更されたときに，公開鍵のフィンガープリント（ハッシュ値）を表示して，ユーザに正しい公開鍵かどうか確認を要求します。事前にユーザへ告知したサーバのホスト公開鍵のフィンガープリントと，ユーザが接続したときに表示されたフィンガープリントを比較することで，サーバのなりすましを防げます。

本装置の SSH サーバ機能のホスト公開鍵およびホスト公開鍵のフィンガープリントを確認するには，運用コマンド show ssh hostkey を使用してください。表示内容と表示形式を次の表に示します。

表 1-7 SSH サーバ機能のホスト公開鍵およびフィンガープリント表示形式

SSH バージョン	表示内容	表示形式
SSHv1	公開鍵	SSHv1 形式
	フィンガープリント	SECSH（MD5）形式（RFC4716）
	フィンガープリント	SHA256 形式
SSHv2	公開鍵	OpenSSH 形式
	フィンガープリント	SECSH（MD5）形式（RFC4716）
	フィンガープリント	SHA256 形式

(2) ユーザ認証

ユーザ認証は，SSH サーバが SSH クライアントを認証する機能です。本装置では，ユーザ認証方式として次に示す二つの方式をサポートしています。

- 公開鍵認証
- パスワード認証

本装置の SSH サーバが使用するユーザ認証方式は，コンフィグレーションコマンド ip ssh authentication で設定できます。

(a) 公開鍵認証

公開鍵アルゴリズムを使用してユーザを認証する機能です。各ユーザは，それぞれ鍵ペアを用意します。SSH サーバには，ユーザの公開鍵を設定しておきます。SSHv1 では，サーバから公開鍵暗号で通信することによってユーザを認証します。SSHv2 では，クライアントがユーザの秘密鍵でデジタル署名を作成し，サーバが署名を確認することでユーザを認証します。

本装置の SSH サーバ機能は公開鍵認証をサポートします。

本装置の SSH サーバがユーザ認証でサポートする，公開鍵アルゴリズムと公開鍵のサイズを次の表に示します。

表 1-8 本装置の SSH サーバがサポートするユーザ公開鍵のアルゴリズムとサイズ

SSH バージョン	公開鍵アルゴリズム	ユーザ公開鍵のサイズ
SSHv1	RSA	512bit ~ 2560bit
SSHv2	RSA	512bit ~ 5120bit
	DSA	512bit ~ 1536bit

本装置の SSH サーバでは，ユーザ公開鍵の登録にコンフィグレーションコマンド ip ssh authkey を使用します。登録に使用できる公開鍵の形式を以下に示します。

表 1-9 登録できる公開鍵の形式

SSH バージョン	表示形式
SSHv1	SSHv1 形式の公開鍵ファイル
	SSHv1 形式の公開鍵を示す数字列
SSHv2	SECSH（RFC4716）形式の公開鍵ファイル
	OpenSSH 形式の公開鍵ファイル
	SECSH 形式または OpenSSH 形式の公開鍵を示す文字列

(b) パスワード認証

SSH クライアントがユーザ名とパスワードを送信し，SSH サーバがサーバ内のユーザアカウント情報と照合するか，または RADIUS などによって認証サーバへユーザ名とパスワードが正しいかどうか問い合わせることで，ユーザ名とパスワードを確認します。SSH では，ユーザ認証情報は暗号化されるため，盗聴によってパスワードが漏洩する危険はありません。

本装置の SSH サーバ機能はパスワード認証をサポートしています。ただし，本装置の SSH サーバでは，パスワードを設定していないユーザはパスワード認証できません。本装置への SSH 接続のユーザ認証方式としてパスワード認証を使用する場合は，ユーザアカウントにパスワードを設定してください。

(3) セッション鍵の共有

セキュア通信路の暗号化やメッセージ認証に共通鍵として使用するセッション鍵を，サーバとクライアントで共有する機能です。SSHv1 では，クライアントがセッション鍵を作成し，ホスト認証時の RSA 公開鍵暗号によってクライアントからサーバへセッション鍵を送付します。SSHv2 では鍵交換方式によってサーバとクライアントの両方に同じセッション鍵を生成します。

本装置では SSHv2 サーバが使用する鍵交換方式を選択できます。鍵交換方式を選択するには，コンフィグレーションコマンド ip ssh key-exchange を使用してください。

(4) 暗号化

セキュア通信路を暗号化する機能です。暗号化には共通鍵暗号を使用します。

本装置では，コンフィグレーションコマンド ip ssh ciphers を設定することで，SSHv2 サーバの暗号化方式を制限できます。

(5) メッセージ認証

セキュア通信路のデータを認証する機能で，SSHv2 だけに存在する機能です。メッセージ認証では，メッセージ認証コードを使用します。

本装置ではコンフィグレーションコマンド ip ssh macs を設定することで，SSHv2 サーバのメッセージ認証コードを制限できます。

1.1.5 SSH が使用する暗号技術

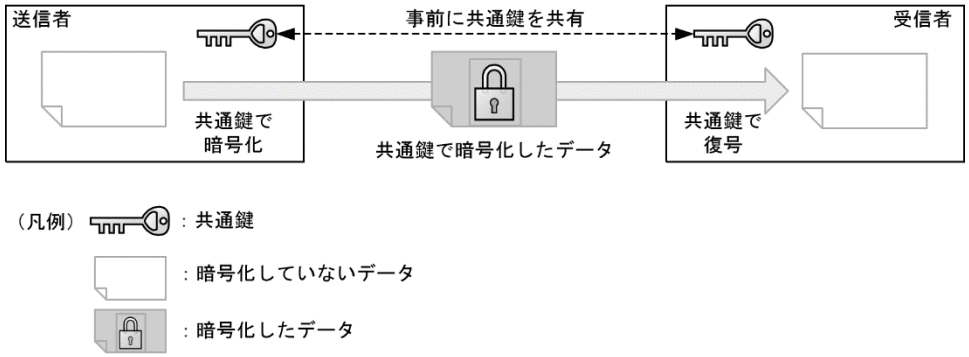
SSH では，次に示す暗号技術を使用して，セキュアな通信を実現します。

- 共通鍵暗号
- メッセージ認証コード
- 公開鍵アルゴリズム
- 鍵交換

(1) 共通鍵暗号

送信者と受信者で同じ鍵（共通鍵）を使用します。共通鍵暗号は，送信者と受信者とで共通鍵を共有し，送信者はその鍵で暗号化し，受信者はその鍵で復号する技術です。共通鍵暗号による暗号化通信の例を次の図に示します。

図 1-4 共通鍵暗号による暗号化通信の例

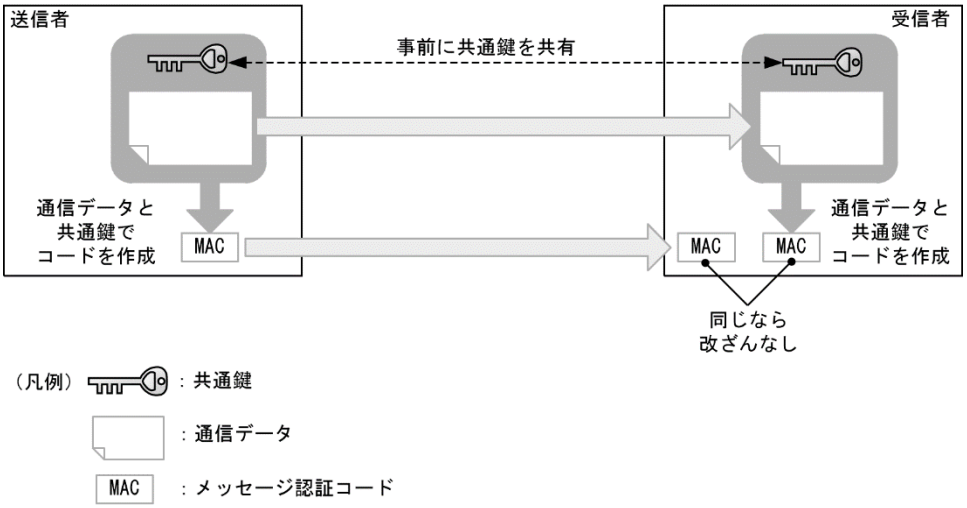


(2) メッセージ認証コード

メッセージ認証コードは，共通鍵を使用して，送信者が送信した通信データが改ざんされていないことを確認する技術です。また，改ざんされていないことを確認するために使用する固定長のデータのことも，メッセージ認証コードと呼びます。

送信者は通信データと共通鍵を組み合わせてメッセージ認証コードを作成し，通信データと同時に送信します。受信者でも通信データと共通鍵を組み合わせてメッセージ認証コードを作成し，受信したメッセージ認証コードと比較します。比較した結果が同じであれば，通信データが改ざんされてないことが確認できます。メッセージ認証コードによる改ざん確認の例を次の図に示します。

図 1-5 メッセージ認証コードによる改ざん確認の例



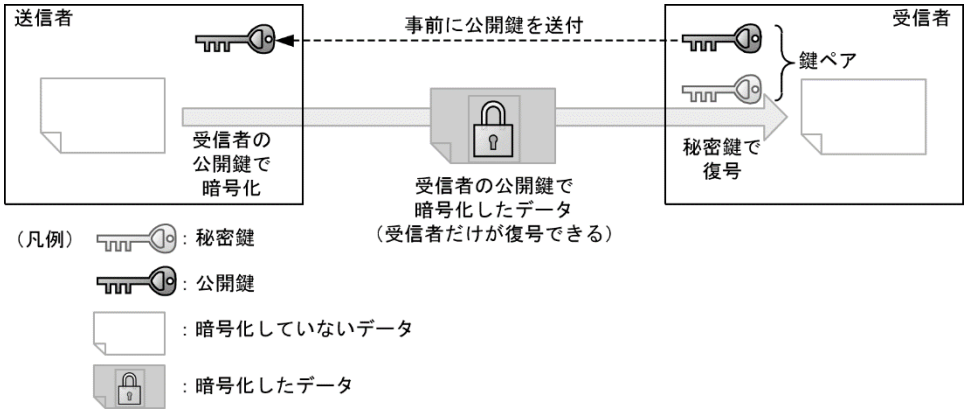
(3) 公開鍵アルゴリズム

公開鍵アルゴリズムは，二種類の鍵である公開鍵と秘密鍵を，ペアで使用するアルゴリズムです。ペアになる公開鍵と秘密鍵の組み合わせを鍵ペアと呼びます。

(a) 公開鍵暗号

公開鍵暗号は，公開鍵で暗号化し，秘密鍵で復号する暗号化技術です。受信者が鍵ペアを作成して公開鍵だけを送信者へ送付します。送信者は，受信者の公開鍵でデータを暗号化して送信します。このように，秘密鍵を保持する受信者しか復号できない暗号化通信を実現します。公開鍵暗号による暗号化通信の例を次の図に示します。

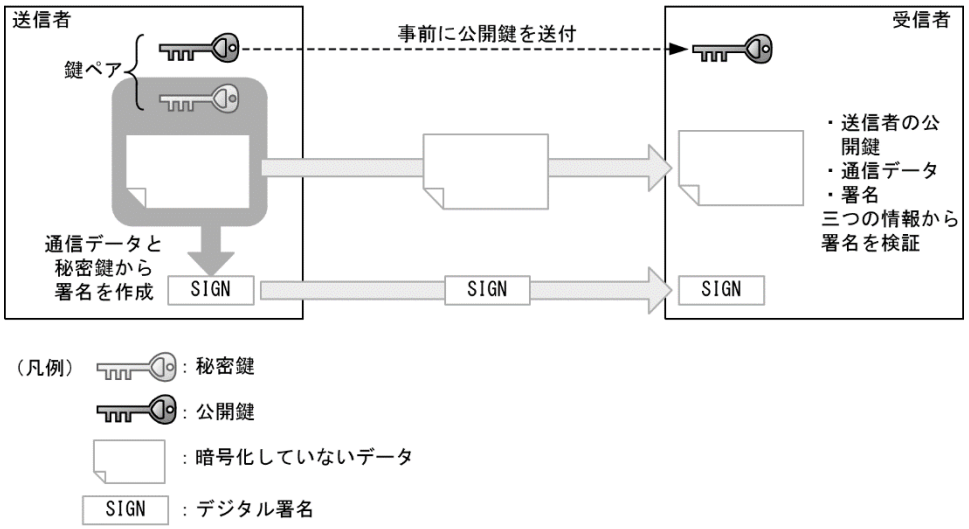
図 1-6 公開鍵暗号による暗号化通信の例



(b) デジタル署名

デジタル署名は，通信データが改ざんされていないか，送信者が正しいかを確認する技術です。送信者は，あらかじめ公開鍵を受信者へ公開しておき，通信データと秘密鍵から署名を作成します。受信者は，通信データと署名と公開鍵から，署名が正しいことを確認します。署名が正しければ，通信データが改ざんされていないこと（通信データの認証），および送信者が秘密鍵の保有者であること（送信者の認証）が確認できます。デジタル署名の例を次の図に示します。

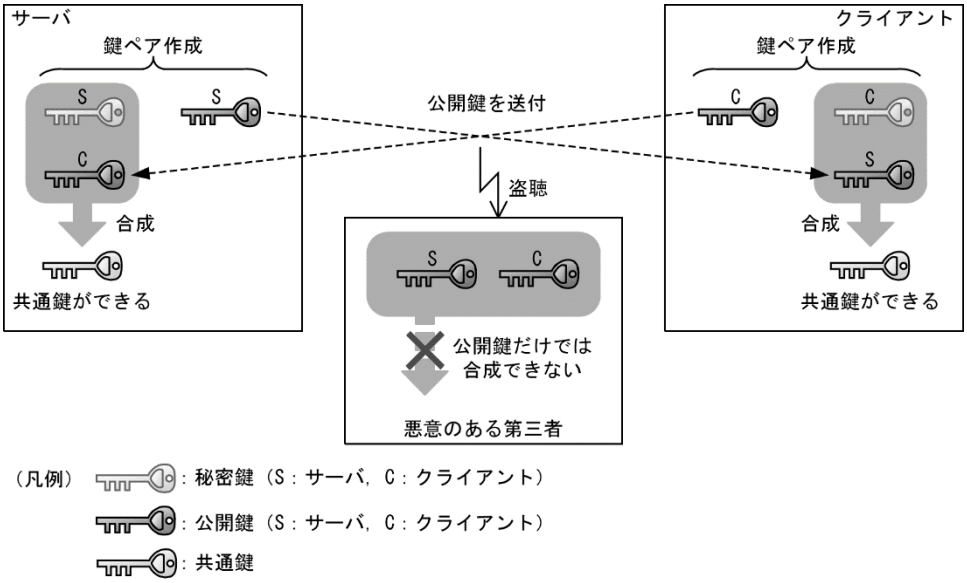
図 1-7 デジタル署名の例



(5) 鍵交換

鍵交換は，通信の両端が交換した情報を基に共通鍵を作成する方式です。サーバとクライアントは，それぞれ鍵ペアを生成し，互いに公開鍵を送付します。自装置の秘密鍵と対向装置の公開鍵を合成すると，サーバとクライアントで同じ共通鍵が生成されます。悪意ある第三者が盗聴してサーバとクライアントの公開鍵を入手しても，公開鍵だけでは共通鍵を作成できません。このため，サーバとクライアントの間で安全に共通鍵を共有することができます。鍵交換例を次の図に示します。

図 1-8 鍵交換の例



1.1.6　ログイン制御機能のサポート

(1)　リモート運用端末からのログインの許可および同時にログインできるユーザ数

本装置の SSH サーバを使用する場合は，コンフィグレーションコマンド line vty を設定する必要があります。また，セキュアリモートログインは，リモートログインのユーザ数としてカウントされ，ユーザ数の制限対象となります。

(2)　リモート運用端末の IP アドレスによる制限

リモート運用端末から本装置の SSH サーバへのアクセスは，リモート運用端末の IP アドレスによる制限対象となります。

1.1.7　RADIUS のサポート

本装置の SSH サーバは，RADIUS による認証をサポートしています。ただし，RADIUS によるログイン認証を使用できるのはパスワード認証だけです。

詳細は「コンフィグレーションガイド Vol.1　RADIUS 認証の適用機能および範囲」を参照してください。

1.1.8　SSH 使用時の注意事項

(1)　多国語 SSH クライアントの制限

日本語などの一部の多国語クライアントでは，ASCII 文字以外の文字（日本語など）でサーバへエラーメッセージを送付することがありますので，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使用してください。

1.2 コンフィグレーション

1.2.1 コンフィグレーションコマンド一覧

SSH サーバ機能のコンフィグレーションコマンド一覧を次の表に示します。

表 1-10 コンフィグレーションコマンド一覧

コマンド名	説明
ip ssh	SSH サーバを動作させます。
ip ssh authentication	SSH サーバのユーザ認証方式を制限します。
ip ssh authkey	SSH サーバで公開鍵認証に使用するユーザ公開鍵を登録します。
ip ssh ciphers	SSHv2 サーバで使用する暗号方式を制限します。
ip ssh key-exchange	SSHv2 サーバで使用する鍵交換方式を制限します。
ip ssh macs	SSHv2 サーバで使用するメッセージ認証コード方式を制限します。
ip ssh version	SSH サーバの SSH プロトコルバージョンを制限します。
transport input※1	リモート運用端末から本装置へのアクセスに使用できるプロトコルを制限するために使用します。
ip access-group※2	リモート運用端末から本装置へのアクセスを，端末の IPv4 アドレスによって制限するために使用します。
ipv6 access-class※2	リモート運用端末から本装置へのアクセスを，端末の IPv6 アドレスによって制限するために使用します。

注※1

「コンフィグレーションコマンドレファレンス　運用端末接続」を参照してください。

注※2

「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。

1.2.2 SSH サーバの基本設定（ローカルパスワード設定）

本装置の SSH サーバ機能を利用するために必要な設定を示します。ユーザ認証方式は，telnet と同じパスワード認証を使用します。

［設定のポイント］

SSH 接続に使用するユーザアカウントへのパスワードの設定例と，SSHv2 サーバを動作させる設定例を示します。セキュリティのため SSHv1 が不要な場合は，動作させる SSH のバージョンを SSHv2 に制限してください。

ログインユーザの作成時にパスワードを設定するように注意してください。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ないためです。ログインユーザの作成については，「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と RADIUS」を参照してください。

SSH クライアントが本装置へ初めて接続するとき，SSH クライアントはホスト公開鍵のフィンガープリントを表示して正しいかどうか確認を要求します。本装置のホスト公開鍵とフィンガープリントの表示方法については，後述の「1.3.2　SSH サーバのホスト公開鍵の確認」を参照してください。

［コマンドによる設定］

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

#

装置管理者モードで運用コマンド adduser を実行します。ユーザ名（staff）とパスワードを設定して，ログイン用のユーザアカウントを作成します。

2. (config)# ip ssh version 2

SSH サーバが動作するバージョンを SSHv2 に制限します。

3. # configure
(config)# ip ssh

SSH サーバの動作を開始させます。

4. (config)# line vty 0 1
(config-line)# exit

本装置へのリモートログインを許可します。この設定例では，ログインできるユーザ数を 2 に設定します。

5. (config)# save

設定内容を保存します。

1.2.3 ユーザ認証に公開鍵認証を使用する設定

(1) ユーザ公開鍵を転送する場合

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，公開鍵認証をする設定例を示します。

［設定のポイント］

あらかじめ，クライアントでユーザ公開鍵ファイルを作成し，本装置へ転送しておいてください。ユーザ公開鍵の転送には ftp を使用できますが，よりセキュリティを確保できる SFTP を使用することをお勧めします。

ここでは SECSH 形式の SSHv2 DSA のユーザ公開鍵で説明していますが，SSHv2 RSA のユーザ公開鍵，OpenSSH 形式や SSHv1 形式の公開鍵も同様の方法で登録できます。

［ユーザ認証鍵の転送］

```
$ 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 ***
```

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。

［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。

［コマンドによる設定］

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

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-O 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

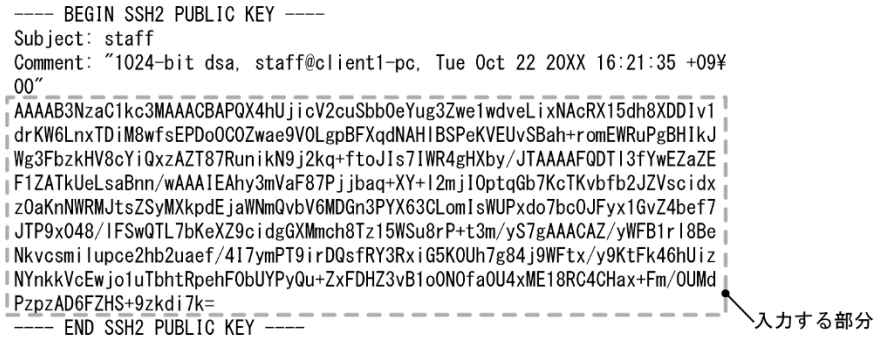
ション情報にはユーザ公開鍵の鍵内容が設定されます。

(2) SSHv2 ユーザ公開鍵（SECSH 形式）を直接入力する場合

公開鍵認証をするために，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。

クライアントで，あらかじめ SECSH 形式のユーザ公開鍵を作成します。ip ssh authkey コマンドで SECSH 形式のユーザ公開鍵の内容を直接入力する場合は，ヘッダ（Comment:コメントなど），開始マーカ，終了マーカ，および改行コードを除いた，鍵の部分だけを入力してください。ユーザ公開鍵（SECSH 形式）の入力部分を次の図に示します。

図 1-9 SSHv2 ユーザ公開鍵（SECSH 形式）の入力部分



［設定のポイント］

この例では，ユーザ公開鍵ファイルの内容を ip ssh authkey コマンドで直接入力して，ユーザ公開鍵を登録します。

ここでは SECSH 形式の SSHv2 DSA のユーザ公開鍵で説明していますが，SSHv2 RSA のユーザ公開鍵も同様の方法で登録できます。

［コマンドによる設定］

1.(config)# ip ssh authkey staff client-v2 "AAAAB3NzaC…S+9zkdi7k="

SSHv2 クライアントであらかじめ作成したユーザ（staff）のユーザ公開鍵（SECSH 形式）の内容を，途中で改行しないようにダブルクォート（"）で囲んで入力します。このとき，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。

［注意事項］

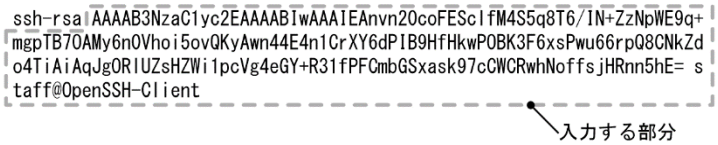
SECSH 形式のユーザ公開鍵には改行コードが含まれているため，すべての改行を取り除いて 1 行の形式にしてください。

(3) SSHv2 ユーザ公開鍵（OpenSSH 鍵）を直接入力する場合

公開鍵認証をするために，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。

クライアントで，あらかじめ OpenSSH 形式のユーザ公開鍵を作成します。ip ssh authkey コマンドで OpenSSH 形式のユーザ公開鍵の内容を直接入力する場合は，先頭にある「ssh-rsa」，または「ssh-dss」を取り除いた部分を，改行コードを含めないでそのまま 1 行で入力してください。ユーザ公開鍵（OpenSSH 鍵）の入力部分を次の図に示します。

図 1-10 SSHv2 ユーザ公開鍵（OpenSSH 鍵）の入力部分



［設定のポイント］

この例では，ユーザ公開鍵ファイルの内容を ip ssh authkey コマンドで直接入力して，ユーザ公開鍵を登録します。

ここでは OpenSSH の SSHv2 RSA ユーザ公開鍵で説明していますが，SSHv2 DSA のユーザ公開鍵も同様の方法で登録できます。

［コマンドによる設定］

1.(config)# ip ssh authkey staff client-O "AAAAB…n5hE= staff@OpenSSH-Client"

あらかじめ作成したユーザ（staff）の SSHv2 のユーザ公開鍵（OpenSSH 形式）を，途中で改行しないようにダブルクォート（"）で囲んで入力します。このとき，このユーザ公開鍵の名前（インデックス名）を client-O とします。

［注意事項］

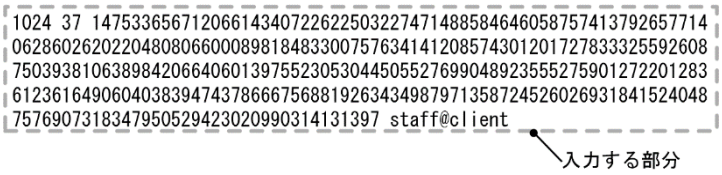
ユーザ公開鍵はすべての改行を取り除いて 1 行の形式にしてください。

(4) SSHv1 ユーザ公開鍵を直接入力する場合

公開鍵認証をするために，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。

クライアントで，あらかじめ SSHv1 ユーザ公開鍵を作成します。ユーザ公開鍵の入力部分を次の図に示します。

図 1-11 SSHv1 ユーザ公開鍵の入力部分



［設定のポイント］

この例では，ユーザ公開鍵ファイルの内容を ip ssh authkey コマンドで直接入力して，ユーザ公開鍵を登録します。

［コマンドによる設定］

1.(config)# ip ssh authkey staff client-v1 "1024 37 14753…31397 staff@client"

あらかじめ作成したユーザ（staff）の SSHv1 のユーザ公開鍵を，途中で改行しないようにダブルクォート（"）で囲んで入力します。このとき，このユーザ公開鍵の名前（インデックス名）を client-v1 とします。

［注意事項］

ユーザ公開鍵はすべての改行を取り除いて 1 行の形式にしてください。

1.2.4 SSH サーバの暗号アルゴリズム関連の設定変更

SSHv2 のセキュリティ機能では，ホスト認証とユーザ認証のほかに，鍵交換，暗号化，メッセージ認証を使用します。本装置の SSHv2 サーバ機能では，鍵交換，暗号化，メッセージ認証についても，複数の種類のアルゴリズムをサポートしています。

［設定のポイント］

サポートしている複数のアルゴリズムのうちから，使用するアルゴリズムを設定します。

［コマンドによる設定］

1. (config)# ip ssh key-exchange diffie-hellman-group14-sha256

   SSHv2 サーバの鍵交換アルゴリズムとして，diffie-hellman-group14-sha256 だけを使用するように設定します。

2. (config)# ip ssh ciphers aes128-ctr

   SSHv2 サーバの暗号化アルゴリズムとして，共通鍵暗号の aes128-ctr だけを使用するように設定します。

3. (config)# ip ssh macs hmac-sha2-256 hmac-sha1

   SSHv2 サーバのメッセージ認証コードアルゴリズムとして，hmac-sha2-256 と hmac-sha1 だけを使用するように設定します。

1.2.5 リモート運用端末からの SSH 接続を許可する IP アドレスの設定

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。

［設定のポイント］

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

［コマンドによる設定］

1. # configure

   (config)# ip ssh

   SSH サーバの動作を開始させます。

2. (config)# ip ssh version 2

   SSH サーバが動作するバージョンを SSHv2 に制限します。

3. (config)# no ftp-server

FTP サーバを無効にします。（デフォルト設定）

4.(config)# ip access-list standard REMOTE

(config-std-nacl)# permit 192.168.1.0 0.0.0.255

(config-std-nacl)# exit

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.(config)# ipv6 access-list REMOTE6

(config-ipv6-acl)# deny ipv6 any any

(config-ipv6-acl)# exit

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.(config)# line vty 0 1

本装置へログインするユーザ数を 2 とします。

7.(config-line)# transport input ssh

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.(config-line)# ip access-group REMOTE in

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.(config-line)# ipv6 access-class REMOTE6 in

(config-line)# exit

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。

10.(config)# save

設定内容を保存します。

1.2.6 RADIUS 認証と連携した SSH サーバの設定

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。

［設定のポイント］

ログイン用のユーザアカウントの作成，および SSH サーバを動作させる設定例を示します。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。

［コマンドによる設定］

1.> enable

adduser staff

User(empty password) add done. Please setting password.

Changing local password for staff.

New password:******

Retype new password:******

#

装置管理者モードで運用コマンド adduser を実行します。ユーザ名（staff）とパスワードを設定して，ログイン用のユーザアカウントを作成します。

2.# configure

(config)# ip ssh

SSH サーバの動作を開始させます。

3.(config)# line vty 0 1

(config-line)# exit

本装置へのリモートログインを許可し，ログインできるユーザ数を 2 に設定します。

4.(config)# aaa authentication login default group radius local

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。

5.(config)# radius-server host 100.0.0.1 key “RADIUSKEY”

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。

6. (config)# radius-server timeout 2

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。

7.(config)# save

設定内容を保存します。

［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。詳細は「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。

1.3 オペレーション

1.3.1 運用コマンド一覧

SSH サーバ機能の運用コマンド一覧を次の表に示します。

表 1-11 運用コマンド一覧

コマンド名	説明
show ssh hostkey	ホスト公開鍵とフィンガープリントを表示します。
set ssh hostkey	ホスト鍵ペアを変更します。
erase ssh hostkey	SSH ホスト鍵ペアを削除します。
show ssh logging	SSH サーバのトレースログを表示します。
clear ssh logging	SSH サーバのトレースログを消去します

1.3.2 SSH サーバのホスト公開鍵の確認

SSH クライアントが SSH サーバを確認できるように，各 SSH サーバは異なるホスト鍵ペアを保持しています。SSH クライアント側では，SSH サーバに初めて接続する場合や，ホスト公開鍵が変更された場合に，そのサーバのフィンガープリントを確認するようにメッセージが表示されます。このとき，あらかじめ接続先サーバのフィンガープリント（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に接続できます。

運用コマンド show ssh hostkey で，SSHv1/SSHv2 のホスト公開鍵およびフィンガープリントが確認できます。

図 1-12 ホスト公開鍵およびフィンガープリントの確認

```
> show ssh hostkey

Date 20XX/03/03 15:14:27 UTC

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

1024 65537 112676670827222279613762898147415720811259820741286658557999554110106264702311394312
072911780834527230005697578940119016961048430141098060487096288989327916987130855661965390234331
404048434562524465674116445196870273015196997458417194179959606837336630394465705358354562069 4
390204035676242785567125465544918631024-bit rsa1 hostkey

Fingerprint for key:
  MD5     7a:79:c1:da:db:69:27:42:e4:48:ab:5c:86:18:a6:04
  SHA256  F8mpx5e/zGBXM2cRUfCtJNjickLJY0QMsL+DEziYOiw

******* SSHv2 DSA Hostkey *******

ssh-dss AAAAB3NzaC1kc3MAAACBAJfYQUaSgxBHDKJdiYLapbj9kizj7JG4OV5D3O4OQsM6VXSIWLtskOyKEJv7LJLaeIA
CT4O5vNZNzQ+sweAwfIEIiuqhPquHijDOSgBp6YfsNz/R9Dr3IcBEt9bOFM7TQ+nzUs7AD7Obb9b8PljETvNlqjpDW7wy+H
OGGu3aiyQ/AAAAFQCJu21YQ8/tinWLjnoUABrKvQWNQQAAAIEAhgrGjsCqIRGb4FqMkjOi3qGNvofORqiuuWg+kDnFP4spD
6OzOW9X+X83mpTPXkWBNbcv2ZVI/lgtY3uHm8vv4t1rfe1GLYzyHU9KGGbqnJaCbJF1Fi2RWj1YsHwQggUX1mlREYStLKHG
htK6KIRK11zwkUGAEOhSHgVuZCELKd4AAACAO9bR4nOceMPKaZLMXkBhYtjV4O8JEYjSAsWRpi697EXWUuxKVWpqUOvOOOU
k9xk6afjZ56qcsPMTbEa6BONkEd7eIL7DIQbsy7WSVOdj/6rwpkVqVvnZt9d1UtbBfyO+qFf1v2gEjtW3DO/i4OFPu1n2KC
nfKfknRtrZ/ALI66M= 1024-bit dsa hostkey

Fingerprint for key:
  MD5     b2:72:be:9a:e0:06:71:6b:ba:fc:2d:47:93:94:b1:dd
```

```
  SHA256  zKnyAcYg3MGmNmbLM9nxMjU4Q5oRq6CjRcd8w9luHXE

>
```

1.3.3 SSH サーバのホスト鍵ペアの変更

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。

本装置を別の用途へ転用する場合も，SSH のホスト鍵ペアを変更することをお勧めします。SSH のホスト鍵ペアを変更する場合は，運用コマンド set ssh hostkey コマンドを実行します。

また，SSHv2 のホスト鍵としてデフォルトの DSA 1024bit 以外のホスト鍵ペアを使用する場合にも，運用コマンド set ssh hostkey を実行します。デフォルトの DSA ホスト鍵ペアを使用しない場合には，運用コマンド erase ssh hostkey を実行して DSA ホスト鍵ペアを削除してください。

図 1-13 ホスト鍵ペア（SSHv1 RSA と SSHv2 DSA）の変更

```
> 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. (1024 bits)
Fingerprint for key:
  MD5     4b:fa:d5:cf:ea:d1:bc:d1:dd:87:0c:45:55:f8:48:6e
  SHA256  FiNJZoi7oSUX+dVg3dufB6aKwN8AA8u7IyIZOy8soKs

*** Changing the SSHv2 Hostkey, Please wait a minute ***
Generating public/private dsa key. (1024 bits)
Fingerprint for key:
  MD5     ad:1c:49:f8:0b:5e:10:ff:32:14:1c:56:5b:53:ca:4a
  SHA256  nzVQjVu9qVM3J3ndRKQVWGH+eQpxCQUe8kop8jKpiIk

The Hostkeys were generated Completely.
The change will be effective on the next reload.
#
```

図 1-14 SSHv2 RSA3072bit ホスト鍵ペアの作成および SSHv2 DSA ホスト鍵ペアの削除

```
> enable
# set ssh hostkey rsa 3072

WARNING!!
Would you wish to change the SSHv2 RSA Hostkeys? (y/n): y

*** Changing the SSHv2 Hostkey, Please wait a minute ***
Generating public/private rsa key. (3072 bits)
Fingerprint for key:
  MD5     c0:4e:81:fb:c2:6e:f7:19:70:32:0f:5b:00:da:d9:e4
  SHA256  lv+Gyu78KdwngLAXUqlLlenl9I+jLcPXLk9C3GNXorU

The Hostkeys were generated Completely.
The change will be effective on the next reload.
# erase ssh hostkey dsa
```

```
WARNING!!
Would you wish to erase the SSHv2 DSA Hostkeys? (y/n): y

The SSHv2 DSA Hostkey was erased.
The change will be effective on the next reload.
#
```

ホスト鍵ペアの変更（作成，削除も含む）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。

1.3.4 SSH サーバのホスト鍵ペアを保存・復元する

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。

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

(1) 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。

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。

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。

(2) 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。

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。

(3) 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。

1.3.5 SSH サーバのログを確認・消去する

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。

(1) ログを確認する

運用コマンド show ssh logging でログを確認できます。ログ表示は最新のものが上に表示されます。

図 1-15　SSH サーバのログを確認

```
> show ssh logging

Date 20XX/09/19 19:32:59 UTC
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.    |1.
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. ┘
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.                                    |2.
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.          ┘
>
```

1. 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。
2. 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。

［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。

(2) ログを消去する

装置管理者モードに移行し，運用コマンド clear logging でログを消去できます。

図 1-16 SSH サーバのログを消去

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

Clear Complete.
#
```

2　収容条件

2.1 リモートアクセス

本装置へのリモートアクセスでの収容条件を示します。

(1) リモートログインできるユーザ数

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です。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。リモートアクセスの接続条件を次の表に示します。

表 2-1 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		
最大ログイン数		16／4 ※1		1 ※2		16／4 ※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		未サポート		60 分	30 分

（凡例）○：接続可　×：接続不可　－：対象外　△：未指定でも接続可

注※1：最大ログインユーザ数は ssh と telnet の総和　１６／４（スタンドアロン動作時／スタック動作時）

注※2：sftp と ftp は同時接続可能

［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。

(2) 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 2-2 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		

(3) 本装置へのユーザ公開鍵の登録

SSH によって本装置へ接続するユーザが公開鍵認証を使用する場合は，ユーザ名と，該当ユーザのユーザ公開鍵を登録してください。公開鍵認証を使用する場合に登録できるユーザ数およびユーザ公開鍵数を次の表に示します。

表 2–3 登録できるユーザ数およびユーザ公開鍵数

項目	最大数
登録できる公開鍵認証ユーザ数	10 ユーザ／装置
登録できるユーザ公開鍵数	10 個／ユーザ

第2編　コンフィグレーションコマンドレファレンス

1　SecureShell（SSH）

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。

本コマンドと line vty コマンドを設定すると，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］

- 本コマンドの設定だけでは 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。
- 本コマンドと line vty コマンドを設定すると，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

ip ssh authentication

SSH サーバで許可するユーザ認証方式を指定します。

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 }

本装置の SSH サーバで許可するユーザ認証方式を指定します。

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

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，パスワード認証のどちらも許可します。

［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

ip ssh authkey

SSH サーバで公開鍵認証に使用するユーザ公開鍵を登録します。

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

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。

表 1-1　900 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。

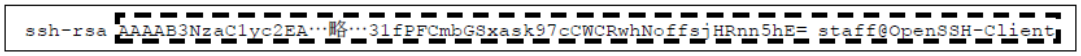
SECSH 形式の公開鍵は改行を含んでいるため，すべての改行を取り除いて入力してください。なお，ヘッダ（Comment:コメント等），開始・終了マーカを除いた，鍵の部分だけを入力してください（次図点線部分）。ヘッダ（Comment:コメント等），開始・終了マーカは入力できません。

図 1-1　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
drKW6LnxTDiM8wfsEPDoOC0Zwae9V0LgpBFXqdNAH1BSPeKVEUvSBah+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 1-2　OpenSSH 形式の公開鍵の手入力範囲



・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

ip ssh ciphers

SSHv2 サーバで使用する暗号方式を制限します。

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>

共通鍵暗号方式を指定します。同一の<encryption algorithm>は複数設定できません。

本パラメータ省略時の初期値

省略できません。どれか一つは設定する必要があります。

値の設定範囲

次の表に示す共通鍵暗号方式名を指定します。

表 1-2 共通鍵暗号方式

項番	暗号方式名
1	3des
2	aes128-cbc
3	aes128-ctr
4	aes192-cbc
5	aes192-ctr
6	aes256-cbc
7	aes256-ctr

［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，3des，aes128-cbc，aes128-ctr，aes192-cbc，aes192-ctr，aes256-cbc，aes256-ctr 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

ip ssh key-exchange

SSHv2 サーバで使用する鍵交換方式を制限します。

本装置の SSHv2 サーバで許可する鍵交換方式を，並べて指定します。

［入力形式］

情報の設定

ip ssh key-exchange < key-exchange algorithm> [<key-exchange algorithm> [...]]

情報の削除

no ip ssh key-exchange

［入力モード］

(config)

［パラメータ］

< key-exchange algorithm> [<key-exchange 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

以下の鍵交換方式を指定します。

表 1-3 鍵交換方式

項番	鍵交換方式名
1	diffie-hellman-group1-sha1
2	diffie-hellman-group14-sha256

［コマンド省略時の動作］

SSHv2 サーバで許可する鍵交換方式は，diffie-hellman-group1-sha1，diffie-hellman-group14-sha256 です。

［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］

本コマンドの設定は，SSHv1 ではプロトコル上無効となります（設定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

transport input

ip ssh macs

SSHv2 サーバで使用するメッセージ認証コード方式を制限します。

本装置の SSHv2 サーバで許可するメッセージ認証コード方式を，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>

メッセージ認証コード方式を指定します。同一の<mac algorithm>は複数設定できません。

本パラメータ省略時の初期値

省略できません。どれか一つは設定する必要があります。

値の設定範囲

次の表に示すメッセージ認証コード方式名を指定します。

表 1-4 メッセージ認証コード方式

項番	メッセージ認証コード方式名
1	hmac-md5
2	hmac-md5-96
3	hmac-sha1
4	hmac-sha1-96
5	hmac-sha2-256
6	hmac-sha2-512

［コマンド省略時の動作］

SSHv2 サーバで許可するメッセージ認証コード方式は，hmac-md5，hmac-md5-96，hmac-sha1，hmac-sha1-96，hmac-sha2-256，hmac-sha2-512 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

ip ssh version

本装置の SSH サーバで使用する SSH プロトコルバージョンを制限します。

本コマンドの設定がない場合は，SSH プロトコルバージョン 1 と 2 どちら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 どちら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

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

2　コンフィグレーション編集時のエラーメッセージ

2.1　コンフィグレーション編集時のエラーメッセージ

2.1.1　SSH

表 2-1　SSH のエラーメッセージ

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。

第3編　運用コマンドレファレンス

1　SecureShell（SSH）

show ssh hostkey

本装置の SSHv1/SSHv2 ホスト公開鍵とフィンガープリントの表示を行うコマンドです。

［入力形式］

show ssh hostkey

［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］

図 1-1　SSHv1/SSHv2 ホスト公開鍵とフィンガープリントの表示

```
> show ssh hostkey

Date 20XX/03/03 15:14:27 UTC

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

1024 65537 112676670827222279613762898147415720811259820741286658557999554110106264702311394312
072911780834527230005697578940119016961048430141098060487096288989327916987130855661965390234331
404048434562524465674116445196870273015196997458417194179959606837336630394465705358354562069 4
390204035676242785567125465544918 63 1024-bit rsa1 hostkey

Fingerprint for key:
  MD5     7a:79:c1:da:db:69:27:42:e4:48:ab:5c:86:18:a6:04
  SHA256  F8mpx5e/zGBXM2cRUfCtJNjickLJY0QMsL+DEziY0iw

******* SSHv2 DSA Hostkey *******

ssh-dss AAAAB3NzaC1kc3MAAACBAJfYQUaSgxBHDKJdiYLapbj9kizj7JG40V5D3O4OQsM6VXSIWLtskOyKEJv7LJLaeIA
CT4O5vNZNzQ+sweAwfIEIiuqhPquHijDOSgBp6YfsNz/R9Dr3IcBEt9bOFM7TQ+nzUs7AD7Obb9b8PljETvNlqjpDW7wy+H
OGGu3aiyQ/AAAAFQCJu21YQ8/tinWLjnoUABrKvQWNQQAAAIEAhgrGjsCqIRGb4FqMkjOi3qGNvofORqiuuWg+kDnFP4spD
6OzOW9X+X83mpTPXkWBNbcv2ZVI/lgtY3uHm8vv4t1rfe1GLYzyHU9KGGbqnJaCbJF1Fi2RWj1YsHwQggUX1mlREYStLKHG
htK6KIRK11zwkUGAEOhSHgVuZCELKd4AAACAO9bR4nOceMPKaZLMXkBhYtjV4O8JEYjSAsWRpi697EXWUuxKVWpqUOvOOOU
k9xk6afjZ56qcsPMTbEa6BONkEd7eIL7DIQbsy7WSVOdj/6rwpkVqVvnZt9d1UtbBfyO+qFf1v2gEjtW3DO/i4OFPu1n2KC
nfKfknRtrZ/ALI66M= 1024-bit dsa hostkey

Fingerprint for key:
  MD5     b2:72:be:9a:e0:06:71:6b:ba:fc:2d:47:93:94:b1:dd
  SHA256  zKnyAcYg3MGmNmbLM9nxMjU4Q5oRq6CjRcd8w9luHXE

>
```

［表示説明］

なし

［通信への影響］

なし

［応答メッセージ］

表 1-1　show ssh hostkey コマンドの応答メッセージ

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］

使用するクライアントによってサポートされているフィンガープリントのハッシュアルゴリズムが異なるため，本装置では MD5 アルゴリズムと SHA256 アルゴリズムの両方を表示します。

set ssh hostkey

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 [{rsa1 | dsa | rsa {1024 | 2048 | 3072}}]

［入力モード］

装置管理者モード

［パラメータ］

{rsa1 | dsa | rsa {1024 | 2048 | 3072}}

作成するホスト鍵ペアの種類を指定します。

rsa1

SSHv1 向けの RSA ホスト鍵ペアを作成します。

dsa

SSHv2 向けの DSA ホスト鍵ペアを作成します。

rsa {1024 | 2048 | 3072}

SSHv2 向けの RSA ホスト鍵ペアを作成します。ホスト鍵の長さは，1024bit, 2048bit,3072bit から選択します。

本パラメータ省略時の動作

SSHv1 向けの RSA ホスト鍵ペアと SSHv2 向けの DSA ホスト鍵ペアを作成します。

［実行例］

図 1-2　SSHv1/SSHv2 のホスト鍵ペアを変更

```
# 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. (1024 bits)
Fingerprint for key:
  MD5     4b:fa:d5:cf:ea:d1:bc:d1:dd:87:0c:45:55:f8:48:6e
  SHA256  FiNJZoi7oSUX+dVg3dufB6aKwN8AA8u7IyIZOy8soKs

*** Changing the SSHv2 Hostkey, Please wait a minute ***
Generating public/private dsa key. (1024 bits)
Fingerprint for key:
  MD5     ad:1c:49:f8:0b:5e:10:ff:32:14:1c:56:5b:53:ca:4a
  SHA256  nzVQjVu9qVM3J3ndRKQVWGH+eQpxCQUe8kop8jKpiIk

The Hostkeys were generated Completely.
The change will be effective on the next reload.
#
```

図 1-3 SSHv1 の RSA ホスト鍵ペアを変更

```
# set ssh hostkey rsa1

WARNING!!
Would you wish to change the SSHv1 RSA Hostkeys? (y/n): y

*** Changing the SSHv1 Hostkey, Please wait a minute ***
Generating public/private rsa1 key. (1024 bits)
Fingerprint for key:
  MD5     0c:5b:fa:87:f8:9d:c9:3f:d5:1b:d6:95:d9:23:a6:07
  SHA256  ORPQvhBrVAkBgoo98ututxfhAmrnyVpEVetAbgOvWKc

The Hostkeys were generated Completely.
The change will be effective on the next reload.
#
```

図 1-4 SSHv2 の RSA ホスト鍵ペアを変更

```
# set ssh hostkey rsa 3072

WARNING!!
Would you wish to change the SSHv2 RSA Hostkeys? (y/n): y

*** Changing the SSHv2 Hostkey, Please wait a minute ***
Generating public/private rsa key. (3072 bits)
Fingerprint for key:
  MD5     c0:4e:81:fb:c2:6e:f7:19:70:32:0f:5b:00:da:d9:e4
  SHA256  lv+Gyu78KdwngLAXUqlLlenl9I+jLcPXLk9C3GNXorU

The Hostkeys were generated Completely.
The change will be effective on the next reload.
#
```

[表示説明]

なし

[通信への影響]

なし

[応答メッセージ]

表 1-2 set ssh hostkey コマンドの応答メッセージ

メッセ―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。
The change will be effective on the next reload.	設定状態は再起動後に反映されます。
The Hostkeys were generated Completely.	SSHv1 と SSHv2 ホスト鍵の変更生成が完了しました。

［注意事項］

1. 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。
2. 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。
3. 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）。

erase ssh hostkey

本装置の SSHv2 ホスト鍵ペア（公開鍵および秘密鍵）を削除します。

削除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。

［入力形式］

erase ssh hostkey {dsa | rsa}

［入力モード］

装置管理者モード

［パラメータ］

{dsa | rsa}

削除するホスト鍵ペアの種類を指定します。

dsa

SSHv2 DSA ホスト鍵ペアを削除します。

rsa

SSHv2 RSA ホスト鍵ペアを削除します。

本パラメータ省略時の動作

省略できません。

［実行例］

図 1-5　SSHv2 DSA ホスト鍵ペアの削除

```
# erase ssh hostkey dsa

WARNING!!
Would you wish to erase SSHv2 DSA Hostkey? (y/n): y

The SSHv2 DSA Hostkey was erased.
The change will be effective on the next reload.
#
```

図 1-6　SSHv2 RSA ホスト鍵ペアの削除

```
# erase ssh hostkey rsa

WARNING!!
Would you wish to erase SSHv2 RSA Hostkey? (y/n): y

The SSHv2 RSA Hostkey was erased.
The change will be effective on the next reload.
#
```

［表示説明］

なし

［通信への影響］

なし

［応答メッセージ］

表 1-3　erase ssh hostkey コマンドの応答メッセージ

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。
The change will be effective on the next reload.	設定状態は再起動後に反映されます。

［注意事項］

なし

show ssh logging

本装置の 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］

一般ユーザモードおよび装置管理者モード

［パラメータ］

なし

［実行例］

図 1-7　SSH サーバのトレースログの表示

```
> show ssh logging

Date 20XX/06/15 19:32:59 UTC
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 operator.
20XX/09/19 19:32:48 sshd Failed password for operator from 192.168.10.100 port 2174.
20XX/09/19 19:32:47 sshd Failed password for operator from 192.168.10.100 port 2174.
20XX/09/19 19:32:47 sshd Failed password for operator from 192.168.10.100 port 2174.
20XX/09/19 19:32:46 sshd Failed password for operator from 192.168.10.100 port 2174.
20XX/09/19 19:32:45 sshd Failed password for operator 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.
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 operator 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 operator 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.

>
```

［表示説明］

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。

表 1-4　SSH サーバのトレースログ

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>：メッセージ認証コード方式名
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>：メッセージ認証コード方式名
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メッセージ認証コード方式がありませんでした。 <client macs>：クライアント側のメッセージ認証コ

	ード方式リスト <server macs>：サーバ側のメッセージ認証コード方式リスト
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

［通信への影響］

なし

［応答メッセージ］

表 1-5 show ssh logging コマンドの応答メッセージ

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。

［注意事項］

1. 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。
2. 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。

clear ssh logging

本装置の 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］

図 1-8　SSH サーバのトレースログのクリア

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

Clear complete.
#
```

［表示説明］

なし

［通信への影響］

なし

［応答メッセージ］

表 1-6　clear ssh logging コマンドの応答メッセージ

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

show sessions（who）

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］

図 1-9　本装置にログインしているユーザの表示

```
> show sessions

Date 20XX/02/15 21:09:13 UTC
 Username          Type     Login                Source
*staff             console  20XX/02/15 20:33:43  -
 staff             vty0     20XX/02/15 20:26:19  192.168.1.246
 staff             vty1     20XX/02/15 20:27:54  192.168.1.240
 staff             ftp      20XX/02/15 20:34:40  192.168.1.241
 staff             sftp     20XX/02/15 20:03:27  192.168.1.203

>
```

［表示説明］

表 1-7　show sessions の表示説明

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。

［通信への影響］

なし

［応答メッセージ］

なし

［注意事項］

なし

第4編　メッセージ・ログレファレンス

1　装置関連の障害およびイベント情報

1.1 装置

1.1.1 イベント発生部位＝SESSION

イベント発生部位=の装置関連の障害およびイベント情報を次の表に示します。

表 1-1 イベント発生部位=SESSION の装置関連の E3 情報

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。			

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			
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			

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			
	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。			

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			
	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。）			

第5編　トラブルシューティングガイド

1　SSH 接続のトラブルシュート

1.1 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，次に示す手順で確認してください。

(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。

(2) 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未設定の以下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。

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 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

SSH コンフィグレーション設定項目	内容
SSH 使用・未使用フラグ	SSH 使用・未使用を指定します。
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。
認証方式	公開鍵認証，パスワード認証を指定します。
暗号方式	共通鍵暗号方式を指定します。
鍵交換	鍵交換方式を指定します。
メッセージ認証コード	メッセージ認証コード方式を指定します。
ユーザ公開鍵	ユーザ公開鍵を登録します。

図 1-1 本装置で SSH コンフィグレーションを確認する

```
(config)# show
（中略）
ip ssh                                          1.
ip ssh version 2                                2.
ip ssh authentication password                  3.
ip ssh ciphers aes128-cbc                       4.
ip ssh key-exchange diffie-hellman-group14-sha256   5.
ip ssh macs hmac-sha1                           6.
ip ssh authkey staff1 key1 "xxxxxx"             7.
ip ssh authkey staff1 key2 "xxxxxx"             7.
!
（中略）
(config)#
```

1.ip ssh が設定されていることを確認

2.SSH プロトコルバージョンが正しいか確認

3.認証方式が正しいか確認

4.暗号化方式が正しいか確認

5.鍵交換方式が正しいか確認

6.メッセージ認証コード方式が正しいか確認

7.公開鍵認証時は，ユーザ公開鍵が正しく登録されているか確認

(3) 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 1-2　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                              1.
  transport input ssh                     2.
!     :
```

1.line vty が設定されているか確認

2.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確認

(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 1-3　本装置でユーザ公開鍵を確認する

```
(config)# show
（中略）
ip ssh
ip ssh authkey staff1 key1 "xxxxxx"                    1.
!
（中略）
(config)#
```

1.正しいユーザ名で，正しい公開鍵が登録されているか確認

(5) ログインアカウントの存在およびパスワードが設定済か確認する

本装置に存在しないアカウントではパスワード認証でログインできません。SSH でパスワード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 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          ****                 │1.
   2   admin             ****                 │
   3   user              not set              ┘

(中略)

>
```

1.正しいユーザ名で，正しい公開鍵が登録されているか確認

(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しようとして，次の図に示す運用ログが出力されていないかを，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 1-5　本装置で最大ログイン数を超えている例

```
> show logging

(中略)

EVT 01/20 14:09:25 E3 SESSION Login refused for too many users logged in.

(中略)

>
```

1.2 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た

本装置でのユーザ名やローカルパスワードを忘れた場合に，次に示す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 1-6 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 1-7 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。

   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。

2. 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。
3. 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，本書「第 1 編 コンフィグレーションガイド 1.2.2 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。

4. 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。

1.3 公開鍵認証時のパスフレーズを忘れた

本装置に対して SSH 公開鍵認証でログインするときに入力するパスフレーズを忘れた場合は，そのユーザ鍵ペア（ユーザ公開鍵とユーザ秘密鍵）は使用できません。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

本装置のコンフィグレーションコマンド ip ssh authkey を使用して，パスフレーズを忘れてしまったユーザのユーザ公開鍵を削除してください。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例を次の図に示します。

図 1-8 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で，パスフレーズを忘れてしまったユーザの鍵ペア（ユーザ公開鍵とユーザ秘密鍵）を削除して，登録も解除してください。再度，公開鍵認証を使用する場合は，使用する SSH クライアントでユーザ鍵ペアを再作成したあと，本装置の SSH コンフィグレーションコマンドであらためてユーザ公開鍵を登録してください。

1.4 接続時にホスト公開鍵変更の警告が表示される

他装置から本装置に対して 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。

このメッセージが表示されたときは，悪意のある第三者が本装置になりすましているおそれもあるため，次の手順に従って十分に確認してから SSH で接続してください。

(1) 本装置の装置管理者へ問い合せる

次の内容について装置管理者へ問い合わせて確認してください。

- 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していないか
- 装置構成の変更などをしていないか

本装置で装置管理者がホスト鍵ペアを変更していない場合は，なりすまし攻撃にあっている危険性，またはほかのホストへ接続しているおそれ があるため，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なく，本装置のホスト公開鍵が変更されていた場合は，以降の手順に従って再接続してください。

(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，次の手順に従って，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フィンガープリントで確認します。

1. フィンガープリントの事前確認
   あらかじめ，本装置側にログインして show ssh hostkey コマンドでフィンガープリントを確認します。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。

2. フィンガープリントをクライアントユーザ側へ通知
   確認したフィンガープリントを SSH クライアントユーザに通知します。郵送や電話など，ネットワーク経由以外の安全な方法で通知するとより安全です。

3. フィンガープリントを確認して 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フィンガープリントが手順 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フィンガープリントが MD5 形式で表示されるものと SHA256 形式で表示されるものがあります。また，SSHv1 ではフィンガープリント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。

(3) ユーザのホスト公開鍵データベースを登録または削除する

使用する 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ないで，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・削除して，再接続してください

付録

付録 A.準拠規格

表 A-1 SSH の準拠規格

項番	規格番号（発行年月）	規格名
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	RFC4344(2006 年 1 月)	The Secure Shell (SSH) Transport Layer Encryption Modes
6	RFC8268(2017 年 12 月)	More Modular Exponentiation (MODP) Diffie-Hellman (DH) Key Exchange (KEX) Groups for Secure Shell (SSH)
7	draft-ylonen-sshprotocol-00 (1995 年 11 月)	The SSH (Secure Shell) Remote Login Protocol
8	draft-ietf-secsh-filexfer-13 (2006 年 7 月)	SSH File Transfer Protocol

付録 B.謝辞(Acknowledgments)

［OpenSSL］

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.]
*/
```