NWD-126044-001

PF5200 シリーズ

Secure Shell (SSH)
ソフトウェアマニュアル

NEC

■対象製品

このマニュアルは，PF5200 シリーズのソフトウェアの SecureShell(SSH) 機能について記載しています。ソフトウェア機能は，ソフトウェア OS-F3PA によってサポートする機能について記載します。

■輸出時の注意

本製品は，外国為替及び外国貿易法に基づくリスト規制の該当貨物ですので，輸出（又は非居住者への技術の提供あるいは外国において技術の提供をすることを目的とする取引）を行う場合には，経済産業大臣の輸出許可（又は役務取引許可）が必要となります。

また，本製品には米国の輸出関連法令の規制を受ける技術が含まれており，輸出する場合輸出先によっては米国政府の許可が必要です。

■商標一覧

Cisco は，米国 Cisco Systems, Inc. の米国および他の国々における登録商標です。
Ethernet は，米国 Xerox Corp. の商品名称です。
IPX は，Novell,Inc. の商標です。
Microsoft は，米国 Microsoft Corporation の，米国，日本およびその他の国における登録商標または商標です。
Octpower は，日本電気株式会社の登録商標です。
UNIX は，X/Open Company Limited が独占的にライセンスしている米国ならびに他の国における登録商標です。
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です。
ssh は SSH Communications Security Corp の登録商標です。
F-SecureSSH は F-Secure Corporation の商標です。
「プログラマブルフロー」および「ProgrammableFlow」は，日本電気株式会社の登録商標または商標です。
その他，各会社名，各製品名は，各社の商標または登録商標です。

■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。
このマニュアルは，いつでも参照できるよう，手近な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) 機能についてのみ記載しています。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。

■電波障害について

この装置は，情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

■高調波規制について

高調波電流規格 JIS C 61000-3-2 適合品
適合装置：

- PF5240F-48T4XW
- PF5240R-48T4XW

■発行

2011 年 10 月（初版）NWD-126044-001

■著作権

Copyright (C) 2010-2011, NEC Corporation. All rights reserved.

はじめに

■対象製品およびソフトウェアバージョン

このマニュアルはPF5200シリーズを対象に記載しています。ソフトウェア機能は，ソフトウェアOS-F3PAによってサポートする機能について記載します。
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とき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。

■このマニュアルの訂正について

このマニュアルに記載の内容は，ソフトウェアと共に提供する「リリースノート」および「マニュアル訂正資料」で訂正する場合があります。

■対象読者

本装置を利用したネットワークシステムを構築し，運用するシステム管理者の方を対象としています。
また，次に示す知識を理解していることを前提としています。

- ネットワークシステム管理の基礎的な知識

■マニュアルの読書手順

本装置の導入，セットアップ，日常運用までの作業フローに従って，それぞれの場合に参照するマニュアルを次に示します。

● 装置の開梱から，初期導入時の基本的な設定について知りたい

PF5200 シリーズ
クイックスタートガイド
(NWD-126031-001)

● ハードウェアの設備条件，取り扱い方法について知りたい

PF5200 シリーズ
ハードウェア取扱説明書
(NWD-126033-001)

● ソフトウェアの機能，コンフィグレーションの設定，運用コマンドについて知りたい

PF5200 シリーズ ソフトウェアマニュアル
コンフィグレーションガイド Vol.1
(NWD-126034-001)

PF5200 シリーズ ソフトウェアマニュアル
コンフィグレーションガイド Vol. 2
(NWD-126034-002)

PF5200 シリーズ ソフトウェアマニュアル
コンフィグレーションガイド Vol. 3
(NWD-126034-003)

● コンフィグレーションコマンドの 入力シンタックス，パラメータ詳細について知りたい

PF5200 シリーズ ソフトウェアマニュアル
コンフィグレーション コマンドレファレンス Vol.1
(NWD-126037-001)

PF5200 シリーズ ソフトウェアマニュアル
コンフィグレーション コマンドレファレンス Vol. 2
(NWD-126037-002)

● 運用コマンドの入力シンタックス，パラメータ詳細について知りたい

PF5200 シリーズ ソフトウェアマニュアル
運用コマンドレファレンス Vol.1
(NWD-126039-001)

PF5200 シリーズ ソフトウェアマニュアル
運用コマンドレファレンス Vol.2
(NWD-126039-002)

● メッセージとログについて知りたい

PF5200 シリーズ ソフトウェアマニュアル
メッセージ・ログレファレンス
(NWD-126041-001)

● MIB について知りたい

PF5200 シリーズ ソフトウェアマニュアル
MIB レファレンス
(NWD-126042-001)

● ソフトウェアアップデートを行う手順について知りたい

PF5200 シリーズ
ソフトウェアアップデートガイド
(NWD-126047-001)

● ネットワーク接続のセキュアな運用管理について知りたい

PF5200 シリーズ
Secure Shell (SSH) ソフトウェアマニュアル
(NWD-126044-001)

● トラブル発生時の対処方法について知りたい

PF5200 シリーズ
トラブルシューティングガイド
(NWD-126043-001)

● Secure Channel の TLS 接続について知りたい

PF5200 シリーズ
【別冊】OpenFlow 機能 TLS 対応編
(NWD-126045-001)

■このマニュアルでの表記

AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second *bpsと表記する場合もあります。
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
CC	Continuity Check
CDP	Cisco Discovery Protocol
CFM	Connectivity Fault Management
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
E-Mail	Electronic Mail
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode

LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LSP	Label Switched Path
LSP	Link State PDU
LSR	Label Switched Router
MA	Maintenance Association
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEP	Maintenance association End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol
NET	Network Entity Title
NLA ID	Next-Level Aggregation Identifier
NPDU	Network Protocol Data Unit
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OADP	Octpower Auto Discovery Protocol
OAM	Operations, Administration, and Maintenance
OFC	OpenFlow Controller
OFS	OpenFlow Switch
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PCI	Protocol Control Information
PDU	Protocol Data Unit
PFS	Programmable Flow Switch
PICS	Protocol Implementation Conformance Statement
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
PRI	Primary Rate Interface
PS	Power Supply
PSNP	Partial Sequence Numbers PDU
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSI	Real Switch Instance
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SELector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol

SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SPF	Shortest Path First
SSAP	Source Service Access Point
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
VLAN	Virtual LAN
VRRP	Virtual Router Redundancy Protocol
VSI	Virtual Switch Instance
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WoL	Wake on LAN
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web
XFP	10 gigabit small Form factor Pluggable

■常用漢字以外の漢字の使用について

このマニュアルでは，常用漢字を使用することを基本としていますが，次に示す用語については，常用漢字以外を使用しています。

- 溢れ（あふれ）
- 迂回（うかい）
- 筐体（きょうたい）
- 毎（ごと）
- 閾値（しきいち）
- 溜まる（たまる）
- 輻輳（ふくそう）
- 漏洩（ろうえい）

■ kB(バイト) などの単位表記について

1kB(キロバイト)，1MB(メガバイト)，1GB(ギガバイト)，1TB(テラバイト) はそれぞれ 1024 バイト，1024^2 バイト，1024^3 バイト，1024^4 バイトです。

■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

目次

第 1 編　解説編

1 SecureShell(SSH) 概要 1

1.1 概要 2

1.1.1 特徴 2

1.1.2 プロトコルバージョン 2

1.2 機能概要 4

1.2.1 セキュアリモートログイン機能 4

1.2.2 セキュアコピー機能 5

1.2.3 セキュアファイル転送機能 5

1.3 サポート機能一覧 6

2 SSH 詳細 9

2.1 SSH 接続手順 10

2.1.1 接続からログインまでの流れ 10

2.2 暗号化技術 15

2.2.1 共通鍵暗号方式 15

2.2.2 公開鍵暗号方式 15

2.3 メッセージ認証コード (MAC) 18

3 構成 19

3.1 SSH の接続構成 20

4 収容条件 21

4.1 SSH サーバへの接続ユーザ数 22

4.2 SSH サーバへのユーザ公開鍵の登録 23

4.3 運用時の注意事項 24

4.3.1 多国語 SSH クライアントの制限 24

第 2 編　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 25

5.1 SSH サーバの基本設定（ローカルパスワード認証） 26

5.2 SSHv2 サーバで公開鍵認証を行う設定（SECSH 鍵ー方法 1） 28

5.3 SSHv2 サーバで公開鍵認証を行う設定（SECSH 鍵ー方法 2） 32
5.4 SSHv2 サーバで公開鍵認証を行う設定（OpenSSH 鍵ー方法 1） 36
5.5 SSHv2 サーバで公開鍵認証を行う設定（OpenSSH 鍵ー方法 2） 39
5.6 SSHv1 サーバで公開鍵認証を行う設定（方法 1） 42
5.7 SSHv1 サーバで公開鍵認証を行う設定（方法 2） 46
5.8 SSH サーバの暗号アルゴリズム関連の設定変更 49
5.9 RADIUS 認証と連携した SSH サーバの設定 51
5.10 SSHv2 サーバ機能だけを使いセキュリティを高める 54

第 3 編　運用ガイド編

6 SSH クライアント機能の利用ガイド 57
6.1 SSH クライアントから SSH サーバにログインする 58
6.2 セキュアコピーで SSH サーバにファイルを転送する 62
6.3 セキュア FTP で SSHv2 サーバにファイルを転送する 64
6.4 SSH クライアントから本装置で運用コマンドを実行する 66

7 SSH サーバ運用コマンドの利用ガイド 69
7.1 SSH サーバのログを確認・消去する 70
7.2 SSH サーバのホスト公開鍵の確認をする 71
7.3 SSH サーバのホスト鍵ペアの変更をする 72
7.4 SSH サーバのホスト鍵ペアを保存・復元する 74

8 トラブルシュート 75
8.1 他装置から本装置に対して SSH で接続できない 76
8.1.1 リモート接続経路の確立を確認する 76
8.1.2 本装置のリモートアクセス制御を確認する 76
8.1.3 SSH サーバのコンフィグレーションを確認する 76
8.1.4 本装置に登録したユーザ公開鍵が正しいか確認する 77
8.1.5 本装置にアカウントが存在するか確認する 77
8.1.6 ログインユーザ数を確認する 78
8.1.7 本装置に対して不正なアクセスが無いか確認する 78
8.2 本装置から他装置に対して SSH で接続できない 79
8.2.1 リモート接続経路の確立を確認する 79
8.2.2 他装置のリモートアクセス制御を確認する 79
8.2.3 SSH サーバとクライアントの認証方式などが一致するか確認する 80
8.2.4 他装置にアカウントが存在するか確認する 80
8.3 他装置から本装置に対して SSH リモートコマンド実行できない 81

8.3.1 SSH クライアントの指定オプションの確認 81
8.3.2 実行するコマンドの入力モードの確認 82
8.3.3 y/n 確認メッセージが必要なコマンドを実行していないか確認 82
8.4 他装置から本装置に対して SCP 実行できない 83
8.4.1 SCP クライアントの確認 83
8.5 ローカルパスワード認証時のパスワードを忘れてしまった 84
8.5.1 パスワードの変更，または削除 84
8.6 公開鍵認証時のパスフレーズを忘れてしまった 85
8.7 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 86
8.7.1 本装置の装置管理者への問い合わせと対応 86
8.7.2 ホスト公開鍵が変更された場合の再接続 87
8.7.3 ユーザのホスト公開鍵データベースの登録削除 88

第 4 編 コンフィグレーションコマンドレファレンス編

9 コンフィグレーション 89
9.1 コンフィグレーションコマンド一覧 90
9.2 コンフィグレーションコマンド 91
9.2.1 ip ssh 91
9.2.2 ip ssh version 93
9.2.3 ip ssh authentication 95
9.2.4 ip ssh ciphers 97
9.2.5 ip ssh macs 99
9.2.6 ip ssh authkey 101
9.2.7 transport input 106
9.3 コンフィグレーションコマンドのエラーメッセージ 107

第 5 編 運用コマンドレファレンス編

10 運用・保守機能 109
10.1 運用コマンド一覧 110
10.2 運用コマンド詳細 111
10.2.1 ssh コマンド 111
10.2.2 sftp コマンド 117
10.2.3 scp コマンド 121
10.2.4 show ssh hostkey コマンド 125
10.2.5 set ssh hostkey コマンド 127

10.2.6　show ssh logging コマンド　129
10.2.7　clear ssh logging コマンド　134

第 6 編　メッセージ・ログレファレンス編

11 ログメッセージ　135
11.1　ログメッセージ一覧　136

付録　141

付録 A　用語解説　142
付録 B　準拠規格　145
付録 C　謝辞 (Acknowledgments)　146

1 SecureShell(SSH) 概要

本章では SSH の機能概要を示します。

1.1　概要

1.2　機能概要

1.3　サポート機能一覧

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，「図 1-1　TELNET での接続による脅威 (盗聴)」の脅威であった，運用情報の流出，データの改ざん，不正な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 1-2　SSH での接続によるセキュアな運用管理)。

図 1-1　TELNET での接続による脅威 (盗聴)

図 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 サーバと SSH クライアント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・サーバソフトウェアとの接続を例として示しました。

・OpenSSH　　「OpenSSH_4.3p2」

・F-Secure 社　　「F-SecureSSH 3.2.3」

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・サーバ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・サーバソフトウェアでも，「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 1-3　セキュアリモートログイン機能)。また，ログインせずにコマンドのみを実行させることができます。

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。また，ログインせずに arp テーブルの確認や，ping 疎通確認テストなどを安全に行うことができます。

図 1-3　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，あらかじめユーザ毎にユーザ公開鍵の登録をおこないます。

1.2.2　セキュアコピー機能

セキュアコピー (scp) 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。セキュアコピーは UNIX リモートコピーコマンド (rcp) と同様のインタフェースで使用できます (図 1-4　セキュアコピー機能)。

本装置運用の際，コンフィグレーションのバックアップなどを安全に行うことができます (図 1-4　セキュアコピー機能)。

図 1-4　セキュアコピー機能

1.2.3　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アップデートファイル取得などを安全に行うことができます (図 1-5　セキュアファイル転送機能)。

図 1-5　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 1-1　に示します。

表 1-1　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× … 未サポート

本装置でサポートする詳細機能一覧を表 1-2　に示します。

表 1-2　SSH 詳細機能サポート一覧

項番	機能名				SSH プロトコルバージョン	本装置	説明
1	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。本装置の RADIUS/TACACS+ 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-ctr	128 bit		v2	○	-
(2)		aes192-ctr	192 bit		v2	○	-
(3)		aes256-ctr	256 bit		v2	○	-
(4)		arcfour256	256 bit		v2	○	-
(5)		arcfour128	128 bit		v2	○	-
(6)		arcfour	128 bit		v2	○	-
(7)		aes128-cbc	128 bit		v2	○	-
(8)		aes192-cbc	192 bit		v2	○	-
(9)		aes256-cbc	256 bit		v2	○	-
(10)		3des-cbc	168 bit		v1/v2	○	-
(11)		blowfish-cbc	128 bit		v1/v2	○	-
(12)		twofish128-cbc	128 bit		v2	×	-
(13)		その他			v1/v2	×	上記のみサポートします
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 種類のみサポートします

項番	機能名	SSH プロトコルバージョン	本装置	説明
4	ログインメッセージ表示機能	v1/v2	○	ログイン前後にコンフィグレーションコマンド banner login/motdで設定されたメッセージを表示します。 なお , SSH/sftp/scp の各ログインでメッセージは共通となります (login-ftp/motd-ftp の設定は使用しません)。
(1)	ログイン前メッセージ表示機能	v2	○	ログインプロンプトの前に表示します。プロトコル上 , SSHv2 でのみサポートです。SSHv1 の接続では表示されません。
(2)	ログイン後メッセージ表示機能	v1/v2	○	ログイン後に表示します。なお , ログインしない接続 (scp, sftp または ssh -t にてコマンド実行された場合) には表示されません。

実装：○ … 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

2.2　暗号化技術

2.3　メッセージ認証コード (MAC)

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　SSH 接続の流れ」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－ 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　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) を持っています。これらはインストール時に生成されています。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 2-2　SSHv1 でのホスト認証と暗号化通信路の確立)。

図 2-2　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 2-3　SSHv2 でのホスト認証と暗号化通信路の確立)。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 2-3　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 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 2-4　SSHv1 でのユーザの公開鍵認証の流れ)。

図 2-4　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 2-5　SSHv2 でのユーザの公開鍵認証の流れ)。

図 2-5　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。クライアントが接続時にコマンド実行を指定していた場合は，指定コマンドが実行されます。scp や sftp で接続の場合は，サーバ側で scp や 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 2-6　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 で設定およびクライアントコマンドのパラメータ -c で指定が可能です。

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 2-7　(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 2-7　(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 2-7　(c))

（d）「公開鍵」から「秘密鍵」を生成することはできない

図 2-7　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 2-8　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 自身の秘密鍵でのみ復号できます。

図 2-8　公開鍵暗号方式での暗号化

また図 2-9　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 2-9　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 で設定および，クライアントコマンドのパラメータ -m で指定が可能です。

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

3.1　SSH の接続構成

SSH 機能を利用するための接続構成例を「図 3-1　SSH 機能利用のネットワーク構成例」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

(b)　本装置の SSH クライアントからリモートにある SSH サーバへ接続する例

(c)　本装置の SSH クライアントからリモートにあるもう一台の本装置へ接続する例

図 3-1　SSH 機能利用のネットワーク構成例

いずれも，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。

また，SSH サーバ (SSHv1/SSHv2) や SSH クライアント (SSHv2) は，現在普及が進められている IPv6 にも対応していますので，今後拡大する IPv6 ネットワーク環境下においても利用できます。

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

4.2　SSH サーバへのユーザ公開鍵の登録

4.3　運用時の注意事項

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。

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）　登録可能な公開鍵認証ユーザ数

装置あたり 20 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 4-1　に，登録できるユーザ公開鍵の種類を示します。

表 4-1　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。

本装置の SSH サーバでログを表示させる際に，クライアントからのエラーメッセージを表示する部分では，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。

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。なお SSH クライアント機能は，コンフィグレーションを設定する必要はありません。

5.1　SSH サーバの基本設定（ローカルパスワード認証）

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

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

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

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

5.6　SSHv1 サーバで公開鍵認証を行う設定（方法 1）

5.7　SSHv1 サーバで公開鍵認証を行う設定（方法 2）

5.8　SSH サーバの暗号アルゴリズム関連の設定変更

5.9　RADIUS 認証と連携した SSH サーバの設定

5.10　SSHv2 サーバ機能だけを使いセキュリティを高める

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。

なお，本装置のクライアントはローカルパスワード認証のみをサポートしていますので，本装置間で SSH 接続を行う場合は，ローカルパスワード認証を使用する必要があります。

（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　SSH サーバの基本設定 構成図）。

図 5-1　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 2

表 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	本装置へログインするユーザ数を 3 とします。

[設定内容の表示]

```
(config)# show ip ssh
ip ssh
!
(config)# show line
line vty 0 2
!
```

(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。したがって，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　SSHv2 サーバで公開鍵認証を行う設定（SECSH 鍵－方法 1）構成図）。

図 5-2　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 でのみ接続可能とする
- 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 2
```

クライアントから scp にて本装置のユーザ staff ホームディレクトリにユーザ公開鍵 (id_dsa_1024_a.pub) を転送します。

```
SSHv2ｸﾗｲｱﾝﾄ> scp id_dsa_1024_a.pub staff@10.10.10.1:.
*** パスワード認証 ***
*** 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，scp または sftp を使用することをお勧めします。

[注意事項]

各ユーザホームディレクトリ配下に，”.ssh”ディレクトリを作成しないでください。さらに，この”.ssh”ディレクトリ配下にファイルを転送したり，ファイルをコピー・生成したりしないでください。このディレクトリは，本装置の SSH サーバ機能が自動的に生成し，使用します。ユーザがファイルを置いた場合，削除されたり上書きされたりします。

図 5-3　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 /usr/home/staff/id_dsa_1024_a.pub

表 5-2　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 のみサポートとします。
2	ユーザ：staff の SSHv2 のユーザ公開鍵をファイル /usr/home/staff/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
line vty 0 2
!
(config)# show ip ssh
ip ssh
ip ssh version 2
ip ssh authkey staff client-v2
"AAAAB3NzaC1kc3MAAACBAPQX4hUjicV2cuSbb0eYug3Zwe1wdveLixNAcRX15dh8XDDIv1drKW6Lnx
TDiM8wfsEPDoOC0Zwae9V0LgpBFXqdNAHlBSPeKVEUvSBah+romEWRuPgBHIkJWg3FbzkHV8cYiQxzA
ZT87RunikN9j2kq+ftoJIs7IWR4gHXby/JTAAAAFQDTl3fYwEZaZEF1ZATkUeLsaBnn/wAAAIEAhy3m
```

VaF87Pjjbaq+XY+l2mjIOptqGb7KcTKvbfb2JZVscidxzOaKnNWRMJtsZSyMXkpdEjaWNmQvbV6MDGn
3PYX63CLomIsWUPxdo7bcOJFyx1GvZ4bef7JTP9x048/lFSwQTL7bKeXZ9cidgGXMmch8Tz15WSu8r
P+t3m/yS7gAAACAZ/yWFB1rl8BeNkvcsmilupce2hb2uaef/4I7ymPT9irDQsfRY3RxiG5K0Uh7g84j
9WFtx/y9KtFk46hUizNYnkkVcEwjo1uTbhtRpehF0bUYPyQu+ZxFDHZ3vB1o0NOfa0U4xME18RC4CHa
x+Fm/OUMdPzpzAD6FZHS+9zkdi7k="
!

(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，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 5-4　SSHv2 サーバで公開鍵認証を行う設定 (SECSH 鍵ー方法 2) 構成図)。

図 5-4　SSHv2 サーバで公開鍵認証を行う設定 (SECSH 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
- SSHv2 でのみ接続可能とする
- 公開鍵認証のみを使用する
- 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 5-5　準備したユーザ公開鍵（SECSH 鍵）内容)。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 5-5　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
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 ----
```

(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。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 5-6　ユーザ公開鍵（SECSH 鍵）の入力部分」の点線部分)。

図 5-6　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+ZxFDHZ3vB1o0NOfa0U4xME18RC4CHax+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 5-7　ユーザ公開鍵（SECSH 鍵）の改行除去)。

図 5-7　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+romEWRuPgBHIkJWg3FbzkHV8cYiOxzAZT87RunikN9j2kq+ftoJIs7IWR4gHXby/JTAAAAFQDTl3fYwEZaZEF1ZATkUeLsaBnn/wAAAIEAhy3mVaF87Pjjbaq+XY+l2mjIOptqGb7KcTKvbfb2JZVscidxzOaKnNWRMJtsZSyMXkpdEjaWNmQvbV6MDGn3PYX63CLomIsWUPxdo7bcOJFyx1GvZ4bef7JTP9x048/lFSwQTL7bKeXZ9cidgGXMmch8Tz15WSu8rP+t3m/yS7gAAACAZ/yWFB1rl8BeNkvcsmilupce2hb2uaef/4I7ymPT9irDOsfRY3RxiG5K0Uh7g84j9WFtx/y9KtFk46hUizNYnkkVcEwjo1uTbhtRpehF0bUYPyQu+ZxFDHZ3vB1o0NOfa0U4xME18RC4CHax+Fm/OUMdPzpzAD6FZHS+9zkdi7k=”
5	(config)# line vty 0 2

表 5-3　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 のみサポートとします。
3	許可するユーザ認証方式を公開鍵認証のみとします。
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 3 とします。

［設定内容の表示］

```
(config)# show ip ssh
ip ssh
ip ssh version 2
ip ssh authentication publickey
ip ssh authkey staff client-v2
"AAAAB3NzaC1kc3MAAACBAPQX4hUjicV2cuSbb0eYug3Zwe1wdveLixNAcRX15dh8XDDIv1drKW6Lnx
TDiM8wfsEPDoOC0Zwae9V0LgpBFXqdNAHlBSPeKVEUvSBah+romEWRuPgBHIkJWg3FbzkHV8cYiQxzA
ZT87RunikN9j2kq+ftoJIs7IWR4gHXby/JTAAAAFQDTl3fYwEZaZEF1ZATkUeLsaBnn/wAAAIEAhy3m
VaF87Pjjbaq+XY+l2mjIOptqGb7KcTKvbfb2JZVscidxzOaKnNWRMJtsZSyMXkpdEjaWNmQvbV6MDGn
3PYX63CLomIsWUPxdo7bcOJFyx1GvZ4bef7JTP9x048/lFSwQTL7bKeXZ9cidgGXMmch8Tz15WSu8rP
+t3m/yS7gAAACAZ/yWFB1rl8BeNkvcsmilupce2hb2uaef/4I7ymPT9irDQsfRY3RxiG5K0Uh7g84j9
WFtx/y9KtFk46hUizNYnkkVcEwjo1uTbhtRpehF0bUYPyQu+ZxFDHZ3vB1o0NOfa0U4xME18RC4CHax
+Fm/OUMdPzpzAD6FZHS+9zkdi7k="
!
(config)# show line
line vty 0 2
!
```

(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 5-8　SSHv2 サーバで公開鍵認証を行う設定（OpenSSH 鍵ー方法 1）構成図）。

図 5-8　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－ 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 2
```

クライアントから scp にて本装置のユーザ staff のホームディレクトリにユーザ公開鍵 (id_rsa.pub) を転送します。

```
SSHクライアント> scp id_rsa.pub staff@10.10.10.1:.
*** パスワード認証 ***
*** 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，scp または sftp を使用することをお勧めします。

[注意事項]

各ユーザホームディレクトリ配下に，”.ssh”ディレクトリを作成しないでください。さらに，この”.ssh”ディレクトリ配下にファイルを転送したり，ファイルをコピー・生成したりしないでください。このディレクトリは，本装置の SSH サーバ機能が自動的に生成し，使用します。ユーザがファイルを置いた場合，削除されたり上書きされたりします。

図 5-9　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-O load-key-file /usr/home/staff/id_rsa.pub

表 5-4　本装置の設定解説

解説番号	解説
1	ユーザ :staff の SSHv2 のユーザ公開鍵をファイル /usr/home/staff/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。

[設定内容の表示]

```
(config)# show ip ssh
ip ssh
ip ssh authkey staff client-O "AAAAB3NzaC1yc2EAAAABIwAAAIEAnvn20coFESclfM4S5q8T
6/IN+ZzNpWE9q+mgpTB7OAMy6n0Vhoi5ovQKyAwn44E4n1CrXY6dPIB9HfHkwPOBK3F6xsPwu66rpQ8
CNkZdo4TiAiAqJgORlUZsHZWi1pcVg4eGY+R31fPFCmbGSxask97cCWCRwhNoffsjHRnn5hE= staff
@OpenSSH-Client"
!
(config)# show line
line vty 0 2
!
```

(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－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 5-10　SSHv2 サーバで公開鍵認証を行う設定（OpenSSH 鍵－方法 2）構成図)。

図 5-10　SSHv2 サーバで公開鍵認証を行う設定（OpenSSH 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
- 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－ 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 5-11　準備したユーザ公開鍵（OpenSSH 鍵）の内容)。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 5-11　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-dsa”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 5-12　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-O “AAAAB3NzaC1yc2EAAAABIwAAAIEAnvn20coFESclfM4S5q8T6/IN+ZzNpWE9q+mgpTB7OAMy6n0Vhoi5ovQKyAwn44E4n1CrXY6dPIB9HfHkwPOBK3F6xsPwu66rpQ8CNkZdo4TiAiAqJgORlUZsHZWi1pcVg4eGY+R31fPFCmbGSxask97cCWCRwhNoffsjHRnn5hE= staff@OpenSSH-Client”
3	(config)# line vty 0 2

表 5-5 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 3 とします。

[設定内容の表示]

```
(config)# show ip ssh

ip ssh
ip ssh authkey staff client-O "AAAAB3NzaC1yc2EAAAABIwAAAIEAnvn20coFESclfM4S5q8T
6/IN+ZzNpWE9q+mgpTB7OAMy6n0Vhoi5ovQKyAwn44E4n1CrXY6dPIB9HfHkwPOBK3F6xsPwu66rpQ8
CNkZdo4TiAiAqJgORlUZsHZWi1pcVg4eGY+R31fPFCmbGSxask97cCWCRwhNoffsjHRnn5hE= staff
@OpenSSH-Client"
!
(config)# show line
line vty 0 2
!
```

(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 5-13　)。

図 5-13　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）
- 公開鍵認証のみを使用する
- 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 2
```

クライアントから scp にて本装置のユーザ staff のホームディレクトリにユーザ公開鍵 (identity.pub) を転送します。

```
SSHv1クライアント> scp identity.pub staff@10.10.10.1:.
*** パスワード認証 ***
*** 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，scp または sftp を使用することをお勧めします。

[注意事項]

各ユーザホームディレクトリ配下に，”.ssh”ディレクトリを作成しないでください。さらに，この”.ssh”ディレクトリ配下にファイルを転送したり，ファイルをコピー・生成したりしないでください。このディレクトリは，本装置の SSH サーバ機能が自動的に生成し，使用します。ユーザがファイルを置いた場合，削除されたり上書きされたりします。

図 5-14　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 /usr/home/staff/identity.pub

表 5-6　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のみに変更します。
2	ユーザ staff の SSHv1 のユーザ公開鍵をファイル /usr/home/staff/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 ip ssh
ip ssh
ip ssh authentication publickey
ip ssh authkey staff client-v1 "1024 37  147533656712066143407226225032274714885
846460587574137926577140628602620220480806600089818483300757634141208574301201
727833325592608750393810638984206640601397552305304450552769904892355527590127 2
2012836123616490604038394743786667568819263434987971358724526026931841524048757
690731834795052942302099031413139 7 staff@client"
!
(config)# show line
line vty 0 2
!
```

(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 5-15　SSHv1 サーバで公開鍵認証を行う設定（方法 2）構成図）。

図 5-15　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）
- 公開鍵認証のみを使用する
- 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 5-16　準備したユーザ公開鍵（SSHv1 鍵）の内容)。

図 5-16　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 14753365671206 61434072262250322747148858464605875741379265771406286026202204808 06600089818483300757634141208574301201727833325592608750393810638 98420664060139755230530445055276990489235552759012722012836123616 49060403839474378666756881926343498797135872452602693184152404875 76907318347950529423020990314131397 staff@client”
4	(config)# line vty 0 2

表 5-7　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のみとします。

解説番号	解説
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 3 とします。

［設定内容の表示］

```
(config)# show ip ssh
ip ssh
ip ssh authentication publickey
ip ssh authkey staff client-v1 "1024 37
147533656712066143407226225032274714885846460587574137926577140628602620220480 8
066000898184833007576341412085743012017278333255926087503938106389842066406013 9
755230530445055276990489235552759012722012836123616490604038394743786667568819 2
634349879713587245260269318415240487576907318347950529423020990314131397 staff@
client"
!
(config)# show line
line vty 0 2
!
```

（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 5-17　SSHv2 サーバの暗号アルゴリズム関連の設定変更 構成図)。

図 5-17　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 blowfish を使用する
- MAC(メッセージ認証コード) 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 blowfish`
2	`(config)# ip ssh macs hmac-sha1 hmac-md5`

表 5-8 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 blowfish のみをサポートします。
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 のみをサポートします。

[設定内容の表示]

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

(4) 動作確認

SSHv2 クライアントで aes128-cbc または blowfish，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 もしくは blowfish であること，MAC 方式が hmac-sha1 もしくは 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 5-18　RADIUS 認証と連携した SSH サーバの設定 構成図）。

図 5-18　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

- ホスト名　　radius-server1
- 共通鍵 (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:******
```

なお，RADIUS/TACACS+ 認証では本装置上にユーザアカウントが作成されていない場合，共通のユーザ remote_user としてログインします。RADIUS/TACACS+ 認証全般や remote_user の扱いについては，「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/TACACS+」をご覧ください。

(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 2
3	(config)# aaa authentication login default group radius local
4	(config)# radius-server host radius-server1 key “RADIUSKEY”
5	(config)# radius-server timeout 2

表 5-9　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 3 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通鍵を設定します。
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 aaa
aaa authentication login default group radius local
!
(config)# show line
line vty 0 2
!
(config)# show ip ssh
ip ssh
!
(config)# show radius-server
radius-server timeout 2
radius-server host radius-server1 key “RADIUSKEY”
!
```

(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 Vol.1　ログインセキュリティと RADIUS ／ TACACS+」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 サーバ機能のみを使用し，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 のみを使用します。

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 5-19　SSHv2 サーバ機能だけを使いセキュリティを高める 構成図)。

図 5-19　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 SSH サーバ

- SSHv2 のみを使用する
- telnet，ftp 機能を使用しない
- ネットワーク 192.168.1.0/24 の端末からのみ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 2
7          (config-line)# transport input ssh
8          (config-line)# ip access-group REMOTE in
9          (config-line)# ipv6 access-class REMOTE6 in
```

表 5-10　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 のみサポートします。
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 3 とします。
7	リモート運用端末から SSH プロトコルのみ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のみ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。

[設定内容の表示]

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

(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。

6 SSH クライアント機能の利用ガイド

本章では SSH クライアント機能の利用例を示します。

6.1　SSH クライアントから SSH サーバにログインする

6.2　セキュアコピーで SSH サーバにファイルを転送する

6.3　セキュア FTP で SSHv2 サーバにファイルを転送する

6.4　SSH クライアントから本装置で運用コマンドを実行する

6.1　SSH クライアントから SSH サーバにログインする

（1）　概要

本装置は SSH クライアント機能をサポートしており，SSHv2 および SSHv1 サーバに接続できます。ただし，本装置の SSH クライアント機能はパスワード認証のみをサポートしていますので，SSHv2 および SSHv1 サーバ側ではパスワード認証を有効にする必要があります。

（2）　構成図と条件

本装置の SSH クライアントからネットワークを介して SSHv2 サーバへ接続する構成とします (図 6-1 本装置の SSH クライアントから SSHv2 サーバへ接続 構成図)。

図 6-1　本装置の SSH クライアントから SSHv2 サーバへ接続 構成図

[設定条件]

SSHv2 サーバ

※サーバ・クライアント間の通信の基本設定は完了しているものとします。

- 以下のユーザを作成し，SSH でパスワード認証を許可する。
  ユーザ名：staff,　パスワード：******
- SSH プロトコルバージョンは 2 のみサポート
- クライアントから SSH ポート (TCP22 番) へ接続できるように，ファイヤーウォール，リモートアクセス制限の設定をする。
- 共通鍵暗号は aes128-cbc を使う。
- MAC は hmac-sha1 を使う。

SSH クライアント

- 共通鍵暗号は aes128-cbc を使う。
- MAC は hmac-sha1 を使う。

（3）　SSHv2 サーバの設定例

(a) SSHv2 サーバが本装置の場合

- 運用コマンドでユーザ staff のアカウントを作成します。

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

- コンフィグレーションコマンドで SSHv2 サーバ機能を設定します。

```
(config)# ip ssh
(config)# ip ssh version 2
(config)# ip ssh authentication password
(config)# ip ssh ciphers aes128-cbc
(config)# ip ssh macs hmac-sha1
```

詳細は,「5　SSH サーバ機能の設定ガイド」をご覧ください。

(b) SSHv2 サーバが SSH 社，F-SecureSSH 社製品の場合

- ユーザ staff を作成します。(adduser など)
- sshd2_config に以下を設定 (追加・確認) します。

Port	22
AllowedAuthentications	password
Ciphers	aes128
MACs	hmac-sha1

- sshd2 を直接起動している場合は sshd2 を再起動し，設定を反映します。
- ファイヤーウォールや TCP ラッパーなどのアクセス制限を適宜設定します。
  (具体的には 10.10.10.1 からの TCP 22 番ポートアクセスを許可します。)

(c) SSHv2 サーバが OpenSSH の場合

- ユーザ staff を作成します。(adduser など))
- sshd_config に以下を設定 (追加・確認) します。

  Port 22
  Protocol 2
  PasswordAuthentication yes
  Ciphers aes128-cbc
  MACs hmac-sha1

- sshd を直接起動している場合は sshd を再起動し，設定を反映します。
- ファイヤーウォールや TCP ラッパーなどのアクセス制限を適宜設定します。
  (具体的には 10.10.10.1 からの TCP 22 番ポートアクセスを許可します。)

(4) 接続方法

本装置で，SSH クライアントコマンドを入力します。

```
> ssh -c aes128-cbc -m hmac-sha1 staff@192.168.1.1  ①
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established.
DSA key fingerprint is 75:c0:fa:9e:ec:4f:1d:98:1f:d5:59:1c:fc:35:07:b2.
Are you sure you want to continue connecting (yes/no)? yes  ②
Warning: Permanently added '192.168.1.1' (DSA) to the list of known hosts.
staff@192.168.1.1's password: ******  ③
***ログイン***
```

[解説]

①運用コマンド ssh を使用して，SSH サーバ 192.168.1.1 へユーザ staff として接続します。また，その際，共通鍵暗号方式として aes128 を，MAC 方式として hmac-sha1 を使います。

② SSHv2 サーバに最初に接続する際には，クライアントユーザのホスト公開鍵データベースにホスト公開鍵が登録されていませんので，登録の確認メッセージがでます。Fingerprint(鍵の指紋) を確認し，接続しようとしている SSHv2 サーバの正しいホスト公開鍵であることを確認してください。確認ができましたら，yes と入力することで，データベースに登録し接続を続けます。(一旦，ユーザのホスト公開鍵データベースにホスト公開鍵を登録すれば，次回の接続時には Fingerprint の確認は不要です。)

③ staff のパスワードを入力してログインします。

[ご参考]

Fingerprint の確認方法

本装置の SSHv2 クライアントでは HEX 形式の Fingerprint をサポートしています。Fingerprint の利用方法は，まず，あらかじめサーバ側でホスト公開鍵の Fingerprint を表示し確認しておきます。そして，クライアント側で，サーバに接続する時にそれと照合することで，より安全で確実なサーバへの接続が可能となります。

以下，サーバ側での，ホスト公開鍵の Fingerprint の表示方法を紹介します。

(a) SSHv2 サーバが本装置の場合

サーバ側でホスト公開鍵の表示の運用コマンドを実行し，Fingerprint を表示します。

```
> show ssh hostkey
…
******* SSHv2 Hostkey *******
…
Fingerprint for key:
xogek-gacad-nutic-cisyr-lures-detes-vefig-solim-hatir-nozek-tixex
Fingerprint(HEX) for key:
75:c0:fa:9e:ec:4f:1d:98:1f:d5:59:1c:fc:35:07:b2
…
```

(b) SSHv2 サーバが SSH 社，F-SecureSSH 社製品の場合

サーバ側の ssh-keygen2 コマンドは bubblebabble 形式でのみの Fingerprint 表示のため，HEX 形式では確認できません。

(c) の手順にて OpenSSH 付属の ssh-keygen を利用し，確認してください。

(c) SSHv2 サーバが OpenSSH の場合

サーバ側の ssh-keygen コマンドでホスト公開鍵の Fingerprint を表示します。

```
> ssh-keygen -l -f ホスト公開鍵のファイル名指定
1024 75:c0:fa:9e:ec:4f:1d:98:1f:d5:59:1c:fc:35:07:b2 *****
```

6.2　セキュアコピーで SSH サーバにファイルを転送する

（1） 概要

本装置はセキュアコピー (scp) 機能をサポートしています。scp は SSHv1/SSHv2 を利用し，ファイルを転送できます。ftp と違い，通信路は SSHv1/SSHv2 を利用していますので，ユーザ名やパスワード，ファイルは暗号化されて送付され，外部に漏洩したり改ざんされたりすることはありません。

（2） 構成図と条件

本装置の scp クライアント (例では SSHv2 を使います) からネットワークを介して SSHv2 サーバへ接続し，本装置上に保存したコンフィグレーションファイルを転送する構成とします (図 6-2　本装置の scp クライアントから SSHv2 サーバへ接続 構成図)。

図 6-2　本装置の scp クライアントから SSHv2 サーバへ接続 構成図

[設定条件]

SSHv2 サーバ

※サーバ・クライアント間の通信の基本設定は完了しているものとします。

- SSHv2 サーバの設定を行い，SSHv2 クライアントから IPv4 もしくは IPv6 で接続しパスワード認証でログインできるようにします。(6.1 章（3）参照)

scp(SSHv2) クライアント

- SSHv2 クライアントの ssh コマンドで IPv4 もしくは IPv6 で接続しパスワード認証でログインできることを確認しておきます。(6.1 章（4）参照)
- 転送するファイル：コンフィグレーションファイル (あらかじめホームディレクトリに保存しておきます :config.txt)
- 転送先：/home/staff/config/ (サーバ側でディレクトリはあらかじめ作成しておきます)

（3） 接続方法

- IPv4 で接続の場合，本装置で scp(SSHv2) クライアントコマンドを入力します。

```
> scp config.txt staff@192.168.1.1:/home/staff/config/  ①
staff@192.168.1.1's password: ******  ②
config.txt                                    100% 4062     4.0KB/s   00:00 ③
>
```

［解説］

①運用コマンド scp を使用して，あらかじめホームディレクトリに保存したコンフィグレーションファイル config.txt を SSH サーバ 192.168.1.1 へユーザ staff として接続し，/home/staff/config/ 以下へ転送します。

② SSH サーバに 2 回目以降接続する際には，クライアントユーザのホスト公開鍵データベースにホスト公開鍵が登録されていますので，ホスト鍵の確認メッセージはでません。staff のパスワードを入力します。

③ファイルが転送されます。

- IPv6 で接続の場合，本装置で scp(SSHv2) クライアントコマンドを入力します。その際，IPv6 アドレスは [ ] で囲んで入力します。

```
> scp config.txt staff@[1111::1]:/home/staff/config/  ①
The authenticity of host '1111::1 (1111::1)' can't be established.
DSA key fingerprint is 75:c0:fa:9e:ec:4f:1d:98:1f:d5:59:1c:fc:35:07:b2
Are you sure you want to continue connecting (yes/no)? yes  ②
Warning: Permanently added '1111::1' (DSA) to the list of known hosts.
staff@1111::1's password: ******  ③
config.txt                                    100% 4062     4.0KB/s   00:00 ④
>
```

［解説］

①運用コマンド scp を使用して，あらかじめホームディレクトリに保存したコンフィグレーションファイル config.txt を SSH サーバ 1111::1 へユーザ staff として接続し，/home/staff/config/ 以下へ転送します。

② SSHv2 サーバに最初に接続する際には，クライアントユーザのホスト公開鍵データベースにホスト公開鍵が登録されていませんので，登録の確認メッセージがでます。Fingerprint(鍵の指紋) を確認し，接続しようとしている SSHv2 サーバの正しいホスト公開鍵であることを確認してください。確認ができましたら，yes と入力することで，データベースに登録し接続を続けます。(一旦，ユーザのホスト公開鍵データベースにホスト公開鍵を登録すれば，次回の接続時には Fingerprint の確認は不要です。)

③ staff のパスワードを入力します。

④ファイルが転送されます。

6.3　セキュア FTP で SSHv2 サーバにファイルを転送する

（1） 概要

本装置はセキュア FTP(sftp) 機能をサポートしています。sftp は SSHv2 を利用し，ftp と同様のインタフェースでファイルを転送できます。また，ftp と違い，通信路は SSHv2 を利用していますので，ユーザ名やパスワード，ファイルは暗号化されて送付され，外部に漏洩することはありません。sftp 機能は SSHv2 でのみ利用できる機能です。

（2） 構成図と条件

本装置の sftp クライアントからネットワークを介して SSHv2 サーバへ接続し，コンフィグレーションファイルを転送する構成とします (図 6-3　本装置の sftp クライアントから SSHv2 サーバへ接続 構成図)。

図 6-3　本装置の sftp クライアントから SSHv2 サーバへ接続 構成図

［設定条件］

SSHv2 サーバ

※サーバ・クライアント間の通信の基本設定は完了しているものとします。

- SSHv2 サーバの設定を行い，SSHv2 クライアントから接続しパスワード認証でログインできるようにします。(6.1 章（3）参照)

sftp クライアント

- あらかじめ，ssh(SSHv2 クライアントコマンド) で接続しパスワード認証でログインできることを確認しておきます。(6.1　章（4）参照)
- 転送するファイル：コンフィグレーションファイル (あらかじめホームディレクトリに保存しておきます :config.txt)
- 転送先：/home/staff/config/ (ディレクトリ” config” は sftp で新規作成します)

（3） 接続方法

本装置で sftp クライアントコマンドを入力します。

```
> sftp staff@1111::1  ①
Connecting to 1111::1...
staff@1111::1's password:******  ②
sftp> cd /home/staff/  ③
sftp> mkdir config  ④
```

```
sftp> cd config  ⑤
sftp> put config.txt  ⑥
Uploading config.txt to /home/staff/config/config.txt
config.txt                                    100% 4062     4.0KB/s   00:00
sftp> quit  ⑦
>
```

［解説］

①運用コマンド sftp を使用して，SSH サーバ 1111::1 へユーザ staff として接続します。

② SSH サーバに 2 回目以降接続する際には，クライアントユーザのホスト公開鍵データベースにホスト公開鍵が登録されていますので，ホスト公開鍵の確認メッセージはでません。

staff のパスワードを入力します。

③ /home/staff へディレクトリを移動します。

④ config ディレクトリを作成します。

⑤ /home/staff/config へディレクトリを移動します。

⑥ config.txt をサーバへ転送します。

⑦サーバから切断します。

6.4　SSH クライアントから本装置で運用コマンドを実行する

（1）概要

SSH クライアントから本装置に対して，ログインせずに運用コマンドを実行することができます。SSH を利用し，本装置の SSH サーバに接続し，ユーザ権限の運用コマンドを実行できます。

（2）構成図と条件

本装置の SSH クライアントからネットワークを介して本装置の SSHv2 サーバへ接続する構成とします（図 6-4　SSH クライアントから本装置の SSHv2 サーバでコマンド実行 構成図）。

図 6-4　SSH クライアントから本装置の SSHv2 サーバでコマンド実行 構成図

［設定条件］

※サーバ・クライアント間の通信の基本設定は完了しているものとします。

SSHv2 サーバ

- SSHv2 サーバの設定を行い，SSH クライアントから接続しログインできるようにします。（6.1　章（3）参照）

SSH クライアント

- SSH クライアントの ssh コマンドで接続しログインできることを確認しておきます。（6.1 章（4）参照）
- 実行するコマンド例 1 ：show system
- 実行するコマンド例 2 ：ping 10.10.10.1

(3) 接続方法

本装置の SSH クライアントコマンドで，本装置上での実行コマンドを入力します。

その際，強制的に仮想端末を割り当てるようにクライアント側でパラメータを指定する必要があります。一般的な SSH の実装では，SSH コマンドの -t パラメータを指定します。

- コマンド例 1 の場合

```
> ssh -t staff@192.168.1.1 show system
staff@192.168.1.1's password: ******
Date 2010/12/01 15:30:00 UTC
System: PF5240R-48T4XW, OS-F3PA Ver. S2.0.0.0
Node : Name=
    Contact=
    Locate=
…省略…
Connection to 192.168.1.1 closed.
>
```

- コマンド例 2 の場合

```
> ssh -t staff@192.168.1.1 ping 10.10.10.1
staff@192.168.1.1's password: ******
PING 10.10.10.1 (10.10.10.1): 56 data bytes
64 bytes from 10.10.10.1: icmp_seq=0 ttl=255 time=0.108 ms
64 bytes from 10.10.10.1: icmp_seq=1 ttl=255 time=0.113 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=255 time=0.116 ms
^C
--- 10.10.10.1 PING statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max = 0.108/0.114/0.118 ms
Connection to 192.168.1.1 closed.
>
```

(4) 注意事項

- SSH クライアントから，本装置にログインせずに本装置の運用コマンドを実行するには，クライアントの”-t”パラメータを指定して，強制的に仮想端末を割り当てる必要があります。
- 本装置に対して reload 運用コマンドなど (y/n) の確認メッセージの入力を促すコマンドは，SSH でリモートコマンド実行できません。このようなコマンドに確認なしで強制実行するオプションがある場合は，そのオプションを指定して実行するか，SSH で本装置にログインしてから実行してください。
- 本装置に対して SSH でリモートコマンド実行できるコマンドは一般ユーザ権限のコマンドのみです。装置管理者モードのコマンドは SSH で本装置にログインして，装置管理者モードになってから実行してください。

7 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。

7.1　SSH サーバのログを確認・消去する

7.2　SSH サーバのホスト公開鍵の確認をする

7.3　SSH サーバのホスト鍵ペアの変更をする

7.4　SSH サーバのホスト鍵ペアを保存・復元する

7.1　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 2010/12/01 15:30:00 UTC
```

（ア）

```
2010/12/01 15:02:07 sshd[7036] Disconnecting: Too many authentication failures for staff1
2010/12/01 15:02:07 sshd[7036] Failed password for staff1 from 172.16.1.2 port 1303
2010/12/01 15:02:07 sshd[7036] Failed password for staff1 from 172.16.1.2 port 1303
2010/12/01 15:02:06 sshd[7036] Failed password for staff1 from 172.16.1.2 port 1303
2010/12/01 15:02:04 sshd[7036] Encryption type: 3des
2010/12/01 15:02:04 sshd[7036] Sent 768 bit server key and 1024 bit host key.
2010/12/01 15:02:04 sshd[7036] Client protocol version 1.5; client software version TTSSH/
2.23 Win32
2010/12/01 15:02:04 sshd[7036] Connection from 172.16.1.2 port 1303
2010/12/01 15:02:04 sshd[7036] RSA key generation complete.
2010/12/01 15:02:03 sshd[7036] Generating 768 bit RSA key.
```

（イ）

```
2010/12/01 11:29:18 sshd[3182] Entering interactive session for SSH2.
2010/12/01 11:29:18 sshd[3182] Accepted publickey for staff2 from 172.16.1.1 port 1401 ssh2
2010/12/01 11:29:18 sshd[3182] Found matching DSA key:
51:1f:41:40:51:cf:81:eb:9e:23:09:72:f7:28:c2:b3
2010/12/01 11:29:14 sshd[3182] kex: server->client aes128-cbc hmac-sha1 none
2010/12/01 11:29:14 sshd[3182] kex: client->server aes128-cbc hmac-sha1 none
2010/12/01 11:29:13 sshd[3182] Client protocol version 2.0; client software version TTSSH/
2.23 Win32
2010/12/01 11:29:13 sshd[3182] Connection from 172.16.1.1 port 1401
2010/12/01 11:29:13 sshd[3182] RSA key generation complete.
2010/12/01 11:29:13 sshd[3182] Generating 768 bit RSA key.
```

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 172.16.1.2 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 staff2 が 172.16.1.1 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。

7.2　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 SSH サーバは異なるホスト鍵ペアを持っています。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 2010/12/01 15:30:00 UTC

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

1024 35  109147548322424184536098490151498564119088351027112111026195058856178
145836958704688259837857086245260390721046147337105951057428553478746408884234 9
086512917821804910936884081762724591230413436150708914248020237892188247957038 5
245078235464045729583338607954746200134983292716651022739065173822492188128840 0
783 1024-bit rsa1 hostkey

Fingerprint for key:

xelic-kovup-vedek-kusom-kumah-fusoz-hokog-kadiv-fydib-kubag-goxux
Fingerprint(HEX) for key:
dc:9b:cb:8b:3e:a0:b1:02:87:f7:06:cd:da:63:52:c2

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

ssh-dss AAAAB3NzaC1kc3MAAACBAPedNeJHIUN/
3hOFkO7llyATWpIKXByAqjDRP5prTejwPSlSI86V0dAuxOejnIHg/lAOjMFiZh/761oPqhG/Re6rtNy
R9ogpuu6RAkCfC6W0DapBGatwT3tCo32a+iALDSGDZqym/lqkggUEYUiVuE1xrhZQ7OlVC1PI8HyfPJ
Y5AAAAFQDN0fx8oAUR7Z2eXSM7/2XFG0YqowAAAIBfWdJZMWULalryEbHRiMWDLj81oU/RxsJb4pDqL
A2guJhUYXxfTol63+YUO33g+GgiTr7J+wjqJAr6mP1lOAOo0ZmtK24uR3h3JaHvLEna1x5+Hw1iQaug
p81UdJ13MhtgS6GE16A7tbnPn9rshh1PNT1VfreFuU8sbLWOExdLfQAAAIAXjVxmO1Vkwxd8vxoaJav
GcvH5QdblhNTvZGwohKvb4h9lq+Wy2UChlIPZGnrOXPo7gWYKJCtFE4RUMkqoiTcJHhrbOyoEJc/du8
+cIU7cf0XKQGHWBnS8hh0MnZqlYWd5/ZsJCcMSTt3NWM1obfdv+sH7xZrpZ6tZWwCxNY99pg== 1024
-bit dsa hostkey

Fingerprint for key:
xuzaz-zyhek-pavuz-kunaz-kutub-belon-cezyd-pikol-bydas-buryc-dexux
Fingerprint(HEX) for key:
1c:4a:67:21:93:a6:67:72:bb:86:af:41:3a:ae:f0:cd
>
```

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。

7.3　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を持っています。このホスト鍵ペアは初回の装置起動時に自動生成されていますので，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 のホスト鍵ペアを持っています (図 7-1　SSH サーバのホスト鍵ペア変更 構成図)。

図 7-1　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

- SHv1 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 pair.
Your identification has been saved.
Your public key has been saved.
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.
Your identification has been saved.
Your public key has been saved.
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 changed Completely.
#
```

変更の確認です。
y を入力します。

（4） 動作確認

SSH サーバのホスト公開鍵確認コマンド (show ssh hostkey) を実行 (7.2　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。）

7.4　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を持っています。このホスト鍵ペアは初回の装置起動時に自動生成されています。

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 のホスト鍵ペアを持っていますが，これらをバックアップファイルとして保存・復元できます（図 7-2　SSH サーバのホスト鍵ペア保存・復元 概念図）。

なお，SSH に関連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　運用情報のバックアップ・リストア」をご参照ください。

図 7-2　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 Vol.1」をご参照ください。

（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 (7.2　章を参照) 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 もしくは 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。

8 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。

8.1　他装置から本装置に対して SSH で接続できない

8.2　本装置から他装置に対して SSH で接続できない

8.3　他装置から本装置に対して SSH リモートコマンド実行できない

8.4　他装置から本装置に対して SCP 実行できない

8.5　ローカルパスワード認証時のパスワードを忘れてしまった

8.6　公開鍵認証時のパスフレーズを忘れてしまった

8.7　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

8.1　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，scp，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。

8.1.1　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。

8.1.2　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 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」をご参照ください。

図 8-1　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 2          ←――――――――― line vty が設定されているか？
  transport input ssh ←――――――――― 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？
```

8.1.3　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未設定の場合は，本装置に対して SSH で接続できません。また，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は接続できません。

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「9. 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 8-1　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 8-2　本装置で SSH コンフィグレーションを確認する

```
(config)# show ip ssh
ip ssh                                  ← ip ssh が設定されているか？
ip ssh version 2                        ← SSHプロトコルバージョンは正しいか？
ip ssh authentication password          ← 認証方式は正しいか？
ip ssh ciphers aes128-cbc               ← 暗号化方式は正しいか？
ip ssh macs hmac-sha1                   ← MAC方式は正しいか？
ip ssh authkey staff1 key1 "xxxxxx"     ← 公開鍵認証時は，ユーザ公開鍵が
ip ssh authkey staff1 key2 "xxxxxx"       正しく登録されているか？
!

(config)#
```

8.1.4　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 8-3　本装置でユーザ公開鍵を確認する

```
(config)# show ip ssh
ip ssh
ip ssh authkey staff1 key1 “xxxxxx”     ← 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？
(config)#
```

8.1.5　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 /usr/home/ と /home/ 配下にホームディレクトリが存在するユーザ（ただし remote_user は除く）のみです。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 8-4　本装置でのユーザアカウント確認例

```
# ls /usr/home/
operator   remote_user    staff1    staff2     staff3
# ls /home/
staff4
#
```

8.1.6 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ログがでていないかを show logging コマンドにて確認してください。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」をご参照ください。

図 8-5 本装置で最大ログイン数を超えている場合の例

```
> show logging
EVT 04/13 18:03:54 E3 ACCESS 00000003 0207:000000000000 Login refused for too
many users logged in.
```

8.1.7 本装置に対して不正なアクセスが無いか確認する

本装置の SSH サーバ機能では不正アクセスを防止するために，ログインユーザ数の制限のほかに，ログインするまでの認証途中の段階でのアクセス数制限，ログイン完了までの時間制限（2 分間）を行っています。

よって本装置上の show sessions コマンドで表示するログインユーザ数が少ないにも関わらず SSH で接続できない場合は，接続されているもののログインされていないセッションが残っていることが考えられます。以下を確認してください。

(1) 本装置で show ssh logging を実行して SSH サーバログを確認します。

下記の例では，接続されているもののログインされていないセッションがあるなど，接続中のセッション数が不正に多いため Login refused for too many sessions. として切断しています。

図 8-6 接続されているセッション数が不正に多いため切断している場合の例

```
> show ssh logging
Date 2010/12/01 15:30:00 UTC
2010/12/01 15:20:04 sshd[662] fatal: Login refused for too many sessions.
2010/12/01 15:19:50 sshd[638] fatal: Login refused for too many sessions.
2010/12/01 15:19:00 sshd[670] fatal: Login refused for too many sessions.
```

(2) 接続されているもののログインされていない不正なセッションの接続元の調査を行い，リモートアクセス制限を実施するなどの対応をとってください。なお，接続されているもののログインされていない不正な SSH セッションは 2 分後には解放され，再度 SSH でログインできるようになります。なお，急ぎの場合は，運用コマンド clear tcp にて強制的に TCP セッションを切断して開放させることもできます。

8.2　本装置から他装置に対して SSH で接続できない

本装置から他装置に対して ssh，scp，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。

8.2.1　リモート接続経路の確立を確認する

本装置と他装置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。

8.2.2　他装置のリモートアクセス制御を確認する

他装置のリモートアクセス制御やファイヤーウォールが本装置からのアクセスやログインを拒否している可能性がありますので確認してください。また他装置で SSH サーバが起動していることを確認してください。

8.2.3　SSH サーバとクライアントの認証方式などが一致するか確認する

他装置の SSH サーバの設定と，本装置の SSH クライアントで指定する認証方式が一致しない場合は接続できません。

本装置では SSH クライアント機能に関する項目を運用コマンドパラメータにて設定できます。SSH 運用コマンドの詳細については「6　SSH クライアント機能の利用ガイド」と「10　運用・保守機能」を参照してください。他装置の SSH サーバの詳細設定については，御使用の SSH サーバマニュアルを参照してください。

表 8-2　本装置の SSH クライアント機能で指定する情報

項番	SSH クライアントオプション	内容
1	SSH プロトコルバージョン	SSH プロトコルバージョン本装置の SSH クライアントはプロトコルバージョン 1 と 2 を接続先の SSH サーバのバージョンに合せて自動的に切り替えます。 またパラメータにて明示的にプロトコルバージョン指定を行うことができます。 sftp クライアントは SSHv2 のみの機能です。
2	SSH ポート番号指定	他装置の SSH サーバにて指定しているポート番号を，本装置の SSH クライアント運用コマンドのパラメータで指定します。
3	認証方式（指定不可。パスワード認証のみ）	本装置の SSH クライアント機能はパスワード認証のみをサポートします。よって他装置の SSH サーバでパスワード認証を有効にする必要があります。
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	送信元 IP アドレス	送信元 IP アドレスを指定します。

8.2.4　他装置にアカウントが存在するか確認する

他装置に存在しないアカウントではログインできません。他装置にアカウントが存在するか確認してください。他装置のサーバ設定によっては，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ログインできない場合があります。

8.3 他装置から本装置に対して SSH リモートコマンド実行できない

8.3.1 SSH クライアントの指定オプションの確認

他装置 SSH クライアントから本装置に対して SSH でログインせずに cli 運用コマンドを実行（リモートコマンド実行）した場合にコマンド実行結果が表示されずに以下のエラーが表示されることがあります。

図 8-7 本装置に対するコマンド実行が失敗する場合

```
client-host> ssh operator@myhost show ip arp
operator@myhost's password: ******
Not tty allocation error.
client-host>
```

本装置に対して SSH でリモートコマンド実行する場合には -t オプションで端末を割り当てる必要があります。

図 8-8 本装置に対するコマンド実行が成功する場合

```
client-host> ssh -t operator@myhost show ip arp
operator@myhost's password: ******
Date 2010/12/01 15:30:00 UTC
Total: 2 entries
 IP Address       Linklayer Address  Netif             Expire     Type
 192.168.0.1      0000.0000.0001     VLAN0001          3h55m56s   arpa
 192.168.0.2      0000.0000.0002     VLAN0001          3h58m56s   arpa
Connection to myhost closed.
client-host>
```

8.3.2 実行するコマンドの入力モードの確認

本装置に対して SSH でリモートコマンド実行できるコマンドは一般ユーザモードのコマンドのみです。装置管理者モードのコマンドを実行した場合には以下のようなエラーとなります。

装置管理者モードのコマンドは SSH で本装置にログインして，装置管理者モードになってから実行してください。

図 8-9 本装置に対して装置管理者モードのコマンドをリモート実行した場合

```
client-host> ssh -t operator@myhost set ssh hostkey
operator@myhost's password: ******
set ssh hostkey
    ^
% Permission denied
client-host>
```

8.3.3 y/n 確認メッセージが必要なコマンドを実行していないか確認

本装置に対して reload 運用コマンドなど (y/n) の確認メッセージの入力を促すコマンドは，SSH でリモートコマンド実行できません。このようなコマンドに確認なしで強制実行するオプションがある場合は，そのオプションを指定して実行するか，SSH で本装置にログインしてから実行してください。

8.4 他装置から本装置に対して SCP 実行できない

8.4.1 SCP クライアントの確認

一部の scp クライアントでは，仮想端末を割り当てずに対話型のセッション (CLI) へログインし，ログイン後に scp コマンドを実行してファイル転送を実現するものがあります。本装置では仮想端末を割り当てない対話型のセッション (CLI) へのログインはサポートしていません。クライアント側のトレース・ログを確認し本装置より下のようなメッセージが届いていないか確認してください。このような scp クライアントからは本装置に対して scp 実行できません。

図 8-10 本装置に対する scp が失敗するクライアントのログ例

```
Not tty allocation error.
```

なお，このような scp クライアントでも，sftp プロトコルをサポートしている場合はそちらを使用することによりファイル転送できます。

8.5 ローカルパスワード認証時のパスワードを忘れてしまった

本装置での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。

8.5.1 パスワードの変更，または削除

装置管理者モードで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 8-11 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 8-12 ユーザのパスワードを削除

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

8.6 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 8-13 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 ip ssh
ip ssh
ip ssh version 2
ip ssh authentication publickey
ip ssh authkey staff1 key1 "xxxxxxxxxx"
ip ssh authkey staff1 key2 "xxxxxxxxxx"
!

(config)# no ip ssh authkey staff1 key1

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

（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「9. コンフィグレーション」をご参照ください。

8.7 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

他装置から本装置に対して SSH で接続したときに「@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @」のメッセージが表示されるのは，前回接続した時と本装置側のホスト公開鍵が変わっていることを示しています。

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。

8.7.1 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。

図 8-14 理由無くホスト公開鍵が変更されていた場合の SSH 接続の中断

```
client-host> ssh operator@myhost
@@@
```

8.7.2 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 8-15 ホスト公開鍵の Fingerprint の事前確認

```
> show ssh hostkey
Date 2010/12/01 15:30:00 UTC
******* SSHv1 Hostkey *******
    :
   (中略)
    :
******* SSHv2 Hostkey *******
    :
   (中略)
    :
    :

                                                 本装置の SSHv2 ホスト鍵の
Fingerprint for key:                             Fingerprint(bubblebabble 形式)
xovib-gahis-ninin-zurit-bokap-zerom-kodoc-pireh-begop-pilon-pexox
Fingerprint(HEX) for key:
1c:9b:58:b8:d5:1d:cf:e5:4a:38:b7:db:1e:da:14:c2
                                                 本装置の SSHv2 ホスト鍵の
                                                 Fingerprint (HEX 形式)
>
```

(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。

図 8-16　Fingerprint を確認して接続

```
client-host> ssh operator@myhost
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
  :
（中略）
                                          このFingerprintが(2)と等しいか確認
  :
The fingerprint for the DSA key sent by the remote host is
1c:9b:58:b8:d5:1d:cf:e5:4a:38:b7:db:1e:da:14:c2
Please contact your system administrator.
  :                                       ここで「yes」を入力すると接続します
（中略）
  :
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'myhost' (DSA) to the list of known hosts.
```

ユーザのホスト鍵データベースにホスト鍵を登録し，
次回，同一サーバに SSH 接続した時に自動的にホストの確認が行えます。

8.7.3　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。

9 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。

9.1　コンフィグレーションコマンド一覧

9.2　コンフィグレーションコマンド

9.3　コンフィグレーションコマンドのエラーメッセージ

9.1 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 9-1 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。

9.2 コンフィグレーションコマンド

9.2.1 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の 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 モードにて ip access-group，ipv6 access-class や，transport input 設定を行ってください。

[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]

- 本設定のみでは 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の 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 モードにて ip access-group，ipv6 access-class や，transport input 設定を行ってください。
- 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

transport input

ip access-group

ipv6 access-class

ip ssh version

ip ssh authentication

ip ssh ciphers

ip ssh macs

ip ssh authkey

9.2.2 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

省略不可

値の設定範囲

1：プロトコルバージョン 1 のみ接続を許可します。

2：プロトコルバージョン 2 のみ接続を許可します。

[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]

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は ip ssh 設定と line vty 設定もおこなってください。
- セキュリティ確保のためにプロトコルバージョン 2 のみを使用することをお勧めします。

[関連コマンド]

line vty

transport input

ip access-group

ipv6 access-class

ip ssh

ip ssh authentication

ip ssh ciphers

ip ssh macs

ip ssh authkey

9.2.3 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 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

省略不可

値の設定範囲

publickey：公開鍵認証のみ許可します。

password：パスワード認証のみ許可します。

[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]

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は ip ssh 設定と line vty 設定もおこなってください。

[関連コマンド]

line vty

transport input

ip access-group

ipv6 access-class

ip ssh

ip ssh version

ip ssh ciphers

ip ssh macs

ip ssh authkey

9.2.4 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通鍵暗号方式を，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

省略不可

値の設定範囲

以下の暗号方式名を指定します。

表 9-2 共通鍵暗号方式

項番	暗号方式名
1	aes128-ctr
2	aes192-ctr
3	aes256-ctr
4	arcfour256
5	arcfour128
6	arcfour
7	aes128-cbc
8	aes192-cbc
9	aes256-cbc
10	3des
11	blowfish

［コマンド省略時の動作］

SSHv2 サーバで許可する共通鍵暗号方式は，aes128-ctr，aes192-ctr，aes256-ctr，arcfour256，arcfour128，arcfour，aes128-cbc，aes192-cbc，aes256-cbc，3des，blowfish 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］

- SSH サーバを動作させるためには ip ssh 設定と line vty 設定もおこなってください。
- 本設定の有無に関係なく，SSHv1 では 3des と blowfish 両方のサポートとなります（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

transport input

ip access-group

ipv6 access-class

ip ssh

ip ssh version

ip ssh authentication

ip ssh macs

ip ssh authkey

9.2.5 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

省略不可

値の設定範囲

以下の MAC 方式名を指定します。

図 9-1 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]

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は ip ssh 設定と line vty 設定もおこなってください。
- 本設定は，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

transport input

ip access-group

ipv6 access-class

ip ssh

ip ssh version

ip ssh authentication

ip ssh ciphers

ip ssh authkey

9.2.6 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。

ユーザ公開鍵を登録して公開鍵認証でログインできるように設定する場合，本設定でユーザの公開鍵を登録する前に，該当ユーザのアカウントを運用コマンド adduser で登録してください。

公開鍵を登録できるユーザは装置全体で 20 人までです。

[入力形式]

情報の設定

ip ssh authkey <user name> <authentication key name>
{ “<public key>” | 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指定します。

本パラメータ省略時の初期値

省略不可

値の設定範囲

ユーザ名 (16 文字以下)

<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指定します。

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指定してください。

本パラメータ省略時の初期値

省略不可

値の設定範囲

鍵名称 (英数字と _ と－で 14 文字以下)

{ ” <public key>” | 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

省略不可

値の設定範囲

“”で囲んだユーザ公開鍵の内容を直接入力します。

もしくは，load-key-file に続けてローカルディレクトリ上のユーザ公開鍵ファイル名を指定します。ファイル名にはパスを指定できます。

- 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ガイド Vol.1 文字コード一覧」をご参照ください。

  ただし，次の文字は使用できないのでご注意ください。ダブルクォート（”），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指定されている場合は，”.”に変換して読み込まれます。

- 公開鍵内容を直接””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 9-2　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のみ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 9-3　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，scp，ftp 等でホームディレクトリへ転送してそのファイル名を指定してください。カレントディレクトリは，config モード移行時のディレクトリです。

[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は ip ssh 設定と line vty 設定もおこなってください。
- 本設定にてユーザ公開鍵を設定したユーザ名が，本装置のアカウントに登録されていない場合には，運用コマンドの adduser コマンドにて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。
- 各ユーザホームディレクトリ配下に，”.ssh”ディレクトリを作成しないでください。さらに，この”.ssh”ディレクトリ配下にファイルを転送したり，ファイルをコピー・生成したりしないでください。このディレクトリは，本装置の SSH サーバ機能が自動的に生成し，使用します。ユーザがファイルを置いた場合，削除されたり上書きされたりします。

[関連コマンド]

line vty

transport input

ip access-group

ipv6 access-class

ip ssh

ip ssh version

ip ssh authentication

ip ssh ciphers

ip ssh macs

9.2.7 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のみアクセスを許可し，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 : 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。

[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，グローバルモードの ftp-server で設定してください。

[関連コマンド]

line vty

ftp-server

ip access-group

ipv6 access-class

ip ssh

9.3　コンフィグレーションコマンドのエラーメッセージ

表 9-3　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: '<file path>' file open error.(<reason>)	指定ファイルがオープンできません。
	<file path>：指定ファイル
	<reason>：エラー種別
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 number of bits of a public key is out of range.	公開鍵のビット数は範囲外です。
ssh: The public key is bad format.	公開鍵が不正な形式です。
ssh: The public key is nothing.	公開鍵がありません。
ssh: Usernames are a maximum of 20 entries.	ユーザ名称は最大 20 エントリです。
ssh: Public keys are a maximum of 10 entries per one user.	公開鍵は 1 ユーザ最大 10 エントリです。

10 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。

10.1　運用コマンド一覧

10.2　運用コマンド詳細

10.1　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 10-1　に示します。

表 10-1　運用コマンドサポート機能一覧

項番	分類	コマンド	機能
10.2.1	クライアント機能	ssh	SSH クライアントコマンド
10.2.2		sftp	sftp クライアントコマンド
10.2.3		scp	scp クライアントコマンド
10.2.4	ホスト鍵管理	show ssh hostkey	ホスト公開鍵 表示コマンド
10.2.5		set ssh hostkey	ホスト鍵ペア 変更コマンド
10.2.6	サーバ保守	show ssh logging	SSH サーバトレース情報 表示コマンド
10.2.7		clear ssh logging	SSH サーバトレース情報 消去コマンド

10.2　運用コマンド詳細

10.2.1　ssh コマンド

［機能］

SSHv1/v2 クライアント機能を提供します。

［入力形式］

ssh [-4 | -6] [-v <version>] [-l <user>] [-c <cipher>] [-m <mac>] [-b <source address>]

[-p <port>] [-t] [<user>@]<host> [<command>]

［パラメータ］

-4

IPv4 限定で接続します。

-6

IPv6 限定で接続します。

-v <version>

接続するプロトコルバージョンを固定します。以下の <version> が指定できます。

1 … SSHv1 限定で接続します。

2 … SSHv2 限定で接続します。

-l <user>

認証時のユーザ名を指定します。

指定しない場合は現在のログインユーザ名となります。

-c <cipher>

接続に利用する共通鍵暗号方式名を指定します。

以下の暗号方式名のいずれかを指定できます。

表 10-2　共通鍵暗号方式

項番	暗号方式名	未指定時	
		SSHv1	SSHv2
1	aes128-ctr	—	1
2	aes192-ctr	—	2
3	aes256-ctr	—	3
4	arcfour256	—	4
5	arcfour128	—	5
6	arcfour	—	6
7	aes128-cbc	—	7
8	aes192-cbc	—	8
9	aes256-cbc	—	9
10	3des	○	10
11	blowfish	△	11

数字：優先順位　○：使用　△：未使用（指定可）　－：未サポート

-m <mac>

接続に利用する MAC(メッセージ認証コード)名を指定します。

以下の MAC 方式名のいずれかを指定できます。

なお，SSHv1 接続の場合は，本指定は無効となります。

表 10-3　MAC 方式

項番	MAC 方式名	未指定時の優先順位
		SSHv2
1	hmac-md5	1
2	hmac-md5-96	2
3	hmac-sha1	3
4	hmac-sha1-96	4

-b <source address>

SSH 接続の送信元アドレスを指定します。

IPv4 アドレス，IPv6 アドレスを指定できます。

-p <port>

接続先 SSH サーバのポート番号を指定します。(指定しない場合は 22 です)。

(値の範囲 1-65535 までです。)

-t

<command> 指定のコマンド実行時に仮想端末を強制的に割り当てます。

本装置に対して運用コマンドを実行する際に指定が必要です。

<user>@

認証時のユーザ名を指定します。

指定しない場合は現在のログインユーザ名となります。

-l <user> と両方指定した場合は <user>@ が優先されます。

<host>

接続先の SSH サーバを指定します。

ホスト名，IPv4 アドレス，IPv6 アドレスを指定します。

<command>

認証後にサーバ側で実行するコマンドを指定します。

［入力モード］

一般ユーザモード

［実行例］

SSH クライアントを使用してホスト hostA.example.jp にリモートログインします。

```
> ssh hostA.example.jp
operator@hostA.example.jp’s password: ******
***ログイン***
```

SSH クライアントを使用してホスト hostA.example.jp にユーザ名 staff を指定してリモートログインします。

```
> ssh staff@hostA.example.jp
staff@hostA.example.jp’s password: ******
***ログイン***
```

SSH クライアントを使用してホスト hostA.example.jp で運用コマンド show ip arp（リモートログインせずに）実行します。

```
> ssh -t staff@hostA.example.jp show ip arp
staff@hostA.example.jp’s password: ******
Date 2010/12/01 15:30:00 UTC
Total: 2 entries
 IP Address       Linklayer Address  Netif             Expire     Type
 192.168.0.1      0000.0000.0001     VLAN0001          3h55m56s   arpa
 192.168.0.2      0000.0000.0002     VLAN0001          3h58m56s   arpa
Connection to hostA.example.jp closed.
>
```

[応答メッセージ]

メッセージ	内容
Connection closed by remote host.	リモートホストにより接続が閉じられました。
Permission denied, please try again.	権限がありません。もう一度実行してください。
Remote machine has too old SSH software version.	リモート運用端末の SSH ソフトウェアが古すぎます。
Protocol major versions differ: <number1> vs. <number2>	SSH プロトコルの指定バージョンが違います。 <number1>：クライアント側のバージョン <number2>：サーバ側のバージョン
<host>: No address associated with hostname	指定された <host> に対応するアドレスがありません。 <host>：ホスト名称
Host key verification failed.	ホストキーの照合に失敗しました。
Selected cipher type <type> not supported by server.	指定された <type> はサーバで未サポートです。 <type>：暗号方式
no matching cipher found: client <type1> server <type2>	適合する暗号方式がありませんでした。 <type1>：クライアント側の暗号方式リスト <type2>：サーバ側の暗号方式リスト
No valid SSH1 cipher, using <type> instead.	有効な SSHv1 の暗号方式ではありません。<type> を使用しました。 <type>：暗号方式
Permission denied.	権限がありません。
Received disconnect from <host>: <code>: Too many authentication failures for <user>	認証失敗数が一定回数を超えたので，切断されました。 <host>：サーバ名・アドレス <code>：SSH プロトコルの理由コード <user>：ユーザ名
no matching mac found: client client <type1> server <type2>	適合する MAC 方式がありませんでした。 <type1>：クライアント側の MAC 方式リスト <type2>：サーバ側の MAC 方式リスト
Warning: remote port forwarding failed for listen port <port>	リモートポート転送に失敗しました。 <port>：指定ポート
bind: <address>: Can't assign requested address	送信元アドレスを割り当てできませんでした。 <address>：送信元アドレス
ssh: connect to host <host> port <port>: Connection refused	サーバに接続を拒否されました。 <host>：サーバ名・アドレス <port>：ポート番号
ssh: connect to host <host> port <port>: Can't assign requested address	送信元アドレスを割り当てできなかったため，接続できませんでした。 <host>：サーバ名・アドレス <port>：ポート番号
ssh: connect to host <host> port <port>: Permission denied	指定 <host> へは，接続できませんでした。 <host>：サーバ名・アドレス <port>：ポート番号
ssh_exchange_identification: Connection closed by remote host	サーバに接続を切断されました。
Connection closed by <host>	サーバに接続を切断されました。 <host>：サーバ名・アドレス
Read from socket failed: Connection reset by peer	サーバに接続を切断されました。

メッセージ	内容
The authenticity of host '<host>' can't be established.	接続先サーバの信憑性が確認できていません。 <host>：サーバ名・アドレス
WARNING: <key type> key found for host <host> in [/usr]/home/<user>/.ssh/known_hosts: <number>	接続先サーバのホスト鍵が見つかりました（しかし，今回は違う種類のホスト鍵で接続しようとしています）。 <key type>：ホスト鍵の種類 <host>：サーバ名・アドレス <user>：ユーザ名 <number>：データベースファイルに書かれている行番号
<key type> key fingerprint is <fingerprint>. Are you sure you want to continue connecting (yes/no)?	ホスト鍵のフィンガープリントを確認して，接続確認を行ってください。 <key type>：ホスト鍵の種類 <fingerprint>：ホスト鍵のフィンガープリント
Warning: Permanently added '<host>' (<key type>) to the list of known hosts.	接続先サーバのホスト鍵をクライアントのデータベースに追加しました。 <host>：サーバ名・アドレス <key type>：ホスト鍵の種類
'@@@

［注意事項］

- 本コマンドの <command> パラメータを使用して本装置に対して運用コマンドを実行する場合は -t パラメータも同時に指定してください。指定しない場合はエラーとなります。また，reload 運用コマンドなど (y/n) の確認メッセージの入力を促すコマンドは実行できません。このようなコマンドは強制実行オプションを付けて実行するか，ssh で本装置にログインしてから実行してください。

10.2.2　sftp コマンド

［機能］

sftp クライアント機能 (SSHv2 を用いた対話型のファイル転送) を提供します。

本クライアントは SSHv2 でのみ接続が可能です。

［入力形式］

sftp [-4 | -6] [-l <user>] [-c <cipher>] [-m <mac>] [-P <port>] [<user>@]<host>

［パラメータ］

-4

IPv4 限定で接続します。

-6

IPv6 限定で接続します。

-l <user>

認証時のユーザ名を指定します。

指定しない場合は現在のログインユーザ名となります。

-c <cipher>

接続に利用する共通鍵暗号方式名を指定します。

以下の暗号方式名のいずれかを指定できます。

表 10-4　共通鍵暗号方式

項番	暗号方式名	未指定時の優先順位
		SSHv2
1	aes128-ctr	1
2	aes192-ctr	2
3	aes256-ctr	3
4	arcfour256	4
5	arcfour128	5
6	arcfour	6
7	aes128-cbc	7
8	aes192-cbc	8
9	aes256-cbc	9
10	3des	10
11	blowfish	11

-m <mac>

接続に利用する MAC(メッセージ認証コード) 名を指定します。

以下の MAC 方式名のいずれかを指定できます。

表 10-5 MAC 方式

項番	MAC 方式名	未指定時の優先順位
		SSHv2
1	hmac-md5	1
2	hmac-md5-96	2
3	hmac-sha1	3
4	hmac-sha1-96	4

-P <port>

接続先 ssh サーバのポート番号を指定します。(指定しない場合は 22 です)。

(値の範囲 1-65535 までです)

<user>@

認証時のユーザ名を指定します。

指定しない場合は現在のログインユーザ名となります。

-l <user> と両方指定した場合は <user>@ が優先されます。

<host>

接続先の SSH サーバを指定します。

[sftp プロンプト時のコマンド]

sftp コマンド実行後，プロンプト”sftp>”が表示されている時，以下のコマンドを使用できます。

quit

exit

bye

アプリケーションを終了して sftp プロンプトを終了します。

cd <path>

リモートホストのディレクトリを移動します。

lcd <path>

ローカルホストのディレクトリを移動します。

pwd

リモートホストのカレントディレクトリを表示します。

lpwd

ローカルホストのカレントディレクトリを表示します。

ls [ls-options [<path>]]

リモートホストの <path> のファイル一覧を表示します。

<path> を指定しない場合は，カレントディレクトリのファイル一覧を表示します。

-l オプションを指定するとファイルの権限 , 所有者 , サイズ，更新時刻を表示します。

lls [ls-options [<path>]]

ローカルホストの <path> のファイル一覧を表示します。

詳細は上記 ls と同じです。

get <remote path> [<local path>]

mget <remote path> [<local path>]

リモートホストからローカルホストにファイルを転送します。

また get *.txt と指定すると複数のファイルを転送できます。

put <local path> [<remote path>]

mput <local path> [<remote path>]

ローカルホストからリモートホストにファイルを転送します。

また put *.txt と指定すると複数のファイルを転送できます。

rm　<path>

リモートホストの <path> を削除します。

mkdir <path>

リモートホストにディレクトリを作成します。

lmkdir <path>

ローカルホストにディレクトリを作成します。

rmdir <path>

リモートホストのディレクトリを削除します。

rename <old path> <new path>

リモートホストの <old path> 名称を <new path> 名称に変更します。但し <new path> が存在する場合は名称変更を行いません。

progress

転送時の経過表示の表示・非表示を切り替えます。

?

help

コマンドの help を表示します。

［入力モード］

一般ユーザモード

[実行例]

sftp 接続で staff.conf を get する例です。

```
> sftp staff@hostA.example.jp
*** SSHv2認証 ***
sftp> ls
staff.conf                              test.conf
sftp> get staff.conf
Fetching /usr/home/staff/staff.conf to staff.conf
/usr/home/staff/staff.conf            100% 4115     4.0KB/s   00:01
sftp> quit
>
```

sftp は，従来の ftp プログラムと同様な操作インタフェースで使用できます。

[応答メッセージ]

ssh コマンドと同一の SSH 接続に関するメッセージ・内容に加え，以下のメッセージが出力されます。

メッセージ	内容
Connection closed	回線が切断されました。
Invalid command.	指定されたコマンドは不正です。
Couldn't stat remote file: <reason>	指定されたリモートファイルは存在しません。 <reason>：エラー詳細
You must specify a path after a <command> command.	<command> の後ろにパスを指定する必要があります。
Cannot download non-regular file: <path>	指定された <path> は不正なファイルです。ダウンロードできません。 <path>：指定ファイル名
Connecting to <host>...	接続しています。 <host>：ホスト名・アドレス
Request for subsystem 'sftp' failed on channel 0	指定したサーバには sftp 接続できませんでした。

[注意事項]

- sftp コマンドを使用して本装置にファイルを転送する前に，本装置の空き容量が転送しようとしているファイルサイズより大きいことを確認してから転送してください。
- sftp コマンドを使用してローカルホスト上のファイルを転送して上書きしないでください。
- sftp コマンドにてファイル転送先のディレクトリの権限を確認してから転送してください。
- 本クライアントは SSHv2 でのみ接続が可能です。SSHv1 では接続できません。

10.2.3　scp コマンド

［機能］

scp クライアント機能 (SSHv1/SSHv2 を用いたファイル転送) を提供します。

［入力形式］

scp [-4 | -6] [-v <version>] [-l <user>] [-c <cipher>] [-m <mac>] [-p] [-r] [-P <port>]

[<user>@][<host>:]<directory/file> [<user>@][<target host>:]<directory/file>

［パラメータ］

-4

IPv4 限定で接続します。

-6

IPv6 限定で接続します。

-v <version>

接続するプロトコルバージョンを固定します。以下の <version> が指定できます。

1 … SSHv1 限定で接続します。

2 … SSHv2 限定で接続します。

-l <user>

認証時のユーザ名を指定します。

指定しない場合は現在のログインユーザ名となります。

-c <cipher>

接続に利用する共通鍵暗号方式名を指定します。

以下の暗号方式名のいずれかを指定できます。

表 10-6　共通鍵暗号方式

項番	暗号方式名	未指定時	
		SSHv1	SSHv2
1	aes128-ctr	—	1
2	aes192-ctr	—	2
3	aes256-ctr	—	3
4	arcfour256	—	4
5	arcfour128	—	5
6	arcfour	—	6
7	aes128-cbc	—	7
8	aes192-cbc	—	8
9	aes256-cbc	—	9
10	3des	○	10
11	blowfish	△	11

数字：優先順位　○：使用　△：未使用（指定可）　－：未サポート

-m <mac>

接続に利用する MAC(メッセージ認証コード)名を指定します。

以下の MAC 方式名のいずれかを指定できます。

なお，SSHv1 接続の場合は，本指定は無効となります。

表 10-7　MAC 方式

項番	MAC 方式名	未指定時の優先順位
		SSHv2
1	hmac-md5	1
2	hmac-md5-96	2
3	hmac-sha1	3
4	hmac-sha1-96	4

-p

ファイル属性とタイムスタンプを保持します。

-r

サブディレクトリを再帰的にコピーします。

-P <port>

接続先 ssh サーバのポート番号を指定します。(指定しない場合は 22 です)。

(値の範囲 1-65535 までです)

<user>@

認証時のユーザ名を指定します。

指定しない場合は現在のログインユーザ名となります。

-l <user> と両方指定した場合は <user>@ が優先されます。

<host>

<target host>

接続先の SSH サーバを指定します。

ホスト名，IPv4 アドレス，IPv6 アドレスを指定します。

IPv6 アドレスは大カッコ“[ ]”で囲み指定します。

(IPv6 アドレス指定の例） scp aaa.txt [1234::1]:aaa.txt

<directory/file>

ディレトリとファイル名を指定します。

［入力モード］

一般ユーザモード

［実行例］

ローカルの staff.cnf をリモートサーバに転送します。

```
> scp staff.conf staff@backup.example.jp:/usr/home/staff/staff.conf
staff@backup.example.jp's password: ******
staff.conf                          100%   89     0.1KB/s   00:00
>
```

転送先に対して相対パスも使用できます。この場合ユーザのログインディレクトリ

(ホームディレクトリ ） に対する相対パスになります。

［応答メッセージ］

ssh コマンドと同一の SSH 接続に関するメッセージ・内容に加え，

以下のメッセージが出力されます。

メッセージ	内容
<path>: Permission denied	権限がありませんでした。 <path> : ファイル名
<path>: No such file or directory	指定 <path> は存在しませんでした。 <path> : ファイル名
<path>: not a regular file	指定 <path> は通常のファイルではありません。 <path> : ファイル名
lost connection	切断しました。
No match.	コピーに失敗しました。（リモートからリモートへのコピーを行った場合など）

［注意事項］

- scp コマンドを使用して本装置にファイルを転送する前に，本装置の空き容量が転送しようとしているファイルサイズより大きいことを確認してから転送してください。
- SSH コマンドにてコピー先ファイルのディレクトリおよびファイルの権限を確認してからコピーしてください。
- リモートサーバからリモートサーバへの転送は未サポートのため使用できません。エラーとなります。

10.2.4　show ssh hostkey コマンド

［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 2010/12/01 15:30:00 UTC

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

1024 35 109147548322424184536098490151498564119088351027112111026195058856178 14
583695870468825983785708624526039072104614733710595105742855347874640888423490 8
651291782180491093688408176272459123041343615070891424802023789218824795703852 4
507823546404572958333860795474620013498329271665102273906517382249218812884007 8
3 1024-bit rsa1 hostkey

Fingerprint for key:
xelic-kovup-vedek-kusom-kumah-fusoz-hokog-kadiv-fydib-kubag-goxux
Fingerprint(HEX) for key:
dc:9b:cb:8b:3e:a0:b1:02:87:f7:06:cd:da:63:52:c2


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

ssh-dss AAAAB3NzaC1kc3MAAACBAPedNeJHIUN/3hOFkO7llyATWpIKXByAqjDRP5prTejwPSlSI86
V0dAuxOejnIHg/lAOjMFiZh/761oPqhG/Re6rtNyR9ogpuu6RAkCfC6W0DapBGatwT3tCo32a+iALDS
GDZqym/lqkggUEYUiVuE1xrhZQ7OlVC1PI8HyfPJY5AAAAFQDN0fx8oAUR7Z2eXSM7/2XFG0YqowAAA
IBfWdJZMWULalryEbHRiMWDLj81oU/RxsJb4pDqLA2guJhUYXxfTol63+YUO33g+GgiTr7J+wjqJAr6
mP1lOAOo0ZmtK24uR3h3JaHvLEna1x5+Hw1iQaugp81UdJ13MhtgS6GE16A7tbnPn9rshh1PNT1Vfre
FuU8sbLWOExdLfQAAAIAXjVxmO1Vkwxd8vxoaJavGcvH5QdblhNTvZGwohKvb4h9lq+Wy2UChlIPZGn
rOXPo7gWYKJCtFE4RUMkqoiTcJHhrbOyoEJc/du8+cIU7cf0XKQGHWBnS8hh0MnZqlYWd5/ZsJCcMST
t3NWM1obfdv+sH7xZrpZ6tZWwCxNY99pg== 1024-bit dsa hostkey

Fingerprint for key:
xuzaz-zyhek-pavuz-kunaz-kutub-belon-cezyd-pikol-bydas-buryc-dexux
Fingerprint(HEX) for key:
1c:4a:67:21:93:a6:67:72:bb:86:af:41:3a:ae:f0:cd

>
```

[応答メッセージ]

メッセージ	内容
Can't execute (<reason>). (<reason>=Don't care)	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。

10.2.5　set ssh hostkey コマンド

［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。

ホスト鍵ペアは初回の装置起動時に自動生成されますので，通常は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.
Your identification has been saved.
Your public key has been saved.
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.
Your identification has been saved.
Your public key has been saved.
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.
#
```

[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。
Canceled, The Hostkeys were not changed.	ホスト鍵変更がユーザによってキャンセルされました。
SSHv1 Hostkey-generation was interrupted. Please, Re-try.	シグナル ([Ctrl+C] など) を受けたか，もしくは内部エラーで SSHv1 ホスト鍵生成がキャンセルされました。 [対応] コマンドを再実行してください。
SSHv2 Hostkey-generation was interrupted. Please, Re-try.	シグナル ([Ctrl+C] など) を受けたか，もしくは内部エラーで SSHv2 ホスト鍵生成がキャンセルされました。 [対応] コマンドを再実行してください。
Can't execute (<reason>). (<reason>=Don't care)	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]

- ホスト鍵ペアは初回の装置起動時に自動生成されますので，通常は変更の必要はありません。

10.2.6　show ssh logging コマンド

［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 2010/12/01 15:30:00 UTC
2010/12/01 15:07:50 [4409] Closing connection to 192.168.0.2
2010/12/01 15:07:30 [4409] Accepted password for staff from 192.168.0.2 port 4226
2010/12/01 15:07:26 [4409] Failed none for staff from 192.168.0.2 port 4226
2010/12/01 15:07:22 [4409] Connection from 192.168.0.2 port 4226
2010/12/01 15:07:22 [4409] Generating 768 bit RSA key.
2010/12/01 15:07:22 [4409] RSA key generation complete.
2010/12/01 15:07:22 [4409] Generating 768 bit RSA key.
2010/12/01 15:07:15 [11970] Closing connection to 192.168.0.1
2010/12/01 15:07:15 [11970] Connection closed by 192.168.0.1
2010/12/01 15:06:59 [11970] Accepted publickey for staff from 192.168.0.1 port
4225 ssh2
2010/12/01 15:06:59 [11970] Found matching RSA key: 14:a5:b4:9e:73:24:13:1d:b6
:18:b2:a3:93:93:ce:33
2010/12/01 15:06:56 [11970] Found matching RSA key: 14:a5:b4:9e:73:24:13:1d:b6:
18:b2:a3:93:93:ce:33
2010/12/01 15:06:56 [11970] Failed none for staff from 192.168.0.1 port 4225 ssh2
2010/12/01 15:06:55 [11970] Connection from 192.168.0.1 port 4225
2010/12/01 15:06:55 [11970] RSA key generation complete.
2010/12/01 15:06:55 [11970] Generating 768 bit RSA key.
```

［応答メッセージ］

メッセージ	内容
Can't execute　(<reason>). (<reason>=Don't care)	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。

［ログフォーマット］

```
yyyy/mm/dd hh:mm:ss [プロセス番号] messsage
        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 [invalid user] <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（無効なユーザ名の場合は invalid user が付与されます） <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
Postponed <authentication method> for [invalid user] <user> from <host> port <port> [ssh2]	ユーザ認証を延期しました。 <authentication method>：認証種類 <user>:ユーザ名（無効なユーザ名の場合は invalid user が付与されます） <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
trying public RSA key file [/usr]/home/<user>/.ssh/authorized_keys	SSHv1 の公開鍵認証を試行しています。 <user>：ユーザ名
[/usr]/home/<user>/.ssh/authorized_keys, line <number>: non ssh1 key syntax	登録されたユーザ公開鍵にSSHv1の公開鍵でないものがありました。SSHv1 の公開鍵認証では使用されません。 <user>：ユーザ名 <number>：公開鍵ファイル内の行を指します
Could not write ident string to <host>	<host> へバージョン識別子を送れませんでした。 <host>：リモートホスト
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
Bad protocol version identification '<string>' from <host>	<host> から不正なバージョン識別子を受信しました。 <string>：受信したバージョン識別子 <host>：リモートホストまたは UNKNOWN
probed from <host> with <id>. Don't panic.	<host> から <id> で探索されましたが問題ありません。 <host>：リモートホスト <id>：バージョン識別子
scanned from <host> with <id>. Don't panic.	<host> から <id> で検索されましたが問題ありません。 <host>：リモートホスト <id>：バージョン識別子

メッセージ	内容
Protocol major versions differ for <host>: <server id> vs. <client id>	<host> との SSH プロトコルバージョンが <server id> と <client id> で異なります。 <host>：リモートホスト <server id>：サーババージョン識別子 <client id>：クライアントバージョン識別子
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
Disabling protocol version 1. Could not load host key	SSHv1 ホスト鍵が読み込めませんでした。運用コマンド set ssh hostkey にてホスト鍵を再作成してください。
Disabling protocol version 2. Could not load host key	SSHv2 ホスト鍵が読み込めませんでした。運用コマンド set ssh hostkey にてホスト鍵を再作成してください。
sshd: no hostkeys available -- exiting.	ホスト鍵が読み込めませんでした。運用コマンド set ssh hostkey にてホスト鍵を再作成してください。
error: Could not load host key: /config/ssh/ssh_host_dsa_key	本装置のホスト鍵が読み込みできませんでした。運用コマンド set ssh hostkey にてホスト鍵を再作成してください。
error: Could not load host key: /config/ssh/ssh_host_key	本装置のホスト鍵が読み込みできませんでした。運用コマンド set ssh hostkey にてホスト鍵を再作成してください。
Unknown packet type received after authentication: <type>	認証後に不正なパケットタイプ <type> を受信しました。 <type>：SSH クライアントメッセージタイプ
User <user> not allowed because /etc/nologin exists	指定ユーザはログインできません。 <user>：ユーザ名
User uucp not allowed because shell /usr/libexec/uucp/uucico does not exist	指定ユーザ (uucp) はログインできません。
subsystem request for sftp	sftp 接続を要求されました。
subsystem request for <subsystem> failed, subsystem not found	<subsystem> を要求されましたが失敗しました。(当該 <subsystem> は存在しません) <subsystem>：要求サブシステム名
Wrong response to RSA authentication challenge.	RSA 認証の応答が間違っていました。
Warning: keysize mismatch for client_host_key: actual <size1>, announced <size2>	クラアントホスト鍵の長さが合っていません。 <size1>：実際の鍵長 <size2>：広告された鍵長
error: auth_rsa_verify_response: RSA modulus too small: <size> < minimum 512 bits	公開鍵認証で使用する RSA 鍵長が小さすぎます。 <size>：鍵長
error: auth_rsa_verify_response: <reason>	公開鍵認証で使用する RSA 鍵に異常があります。 <reason>：異常理由
error: RSA_public_decrypt failed: error: <reason>	公開鍵認証で使用する RSA 鍵が長い (5120bit を超える) など，異常があります。 <reason>：内部詳細情報 (Don’t care)
error: key_read: uudecode <key> failed	公開鍵認証で使用する鍵に異常があります。 <key>：鍵内容
error: key_read: key_from_blob <key> failed	公開鍵認証で使用する鍵に異常があります。 <key>：鍵内容
error: key_read: <reason>	公開鍵認証で使用する鍵に異常があります。 <reason>：異常理由 (鍵内容など)

メッセージ	内容
error: key_from_blob: <reason>	公開鍵に異常があります。 <reason>：異常理由
error: buffer_get_bignum2_ret: <reason>	公開鍵に異常があります。 <reason>：異常理由
error: buffer_get_string_ret: <reason>	公開鍵に異常があります。 <reason>：異常理由
error: buffer_get_ret: <reason>	公開鍵に異常があります。 <reason>：異常理由
<authentication method> authentication disabled.	<authentication method> は使用できません。 <authentication method>：認証方式
Invalid user <user> from <host>	<user> は無効です。ログインできません。 <user>：ユーザ名 <host>：リモートホスト
kex: client->server <cipher> <mac> <compression>	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 <compression>：圧縮方式名
kex: server->client <cipher> <mac> <compression>	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 <compression>：圧縮方式名
Encryption type: <cipher>	共通鍵暗号方式は <cipher> を使用します。 <cipher>：共通鍵暗号方式名
Exec command '<command>'	コマンドが実行されました。 <command>：コマンド
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>: <code>: No further authentication methods available.	これ以上の認証方式がありませんので，切断されました。 <host>：リモートホスト <code>：SSH プロトコルの理由コード
Received disconnect from <host>: <code>: Authentication cancelled by user.	認証がキャンセルされましたので，切断されました。 <host>：リモートホスト <code>：SSH プロトコルの理由コード
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
Received disconnect from <host>: <code>: disconnected by server request	リモートホスト要求によって切断されました。 <host>：リモートホスト <code>：SSH プロトコルの理由コード

メッセージ	内容
Received disconnect from <host>: <reason>	リモートホストによって切断されました。 <host>：リモートホスト <reason>：リモートホストからの切断理由
Read error from remote host <host>: Network is down	リモートホストとのネットワークがダウンしました。 <host>：リモートホスト
Read error from remote host <host>: <message>	リモートホストからの受信エラーです。 <host>：リモートホスト <message>：エラー内容
fatal: Write failed: Broken pipe	リモートホストに強制的に切断されました。
fatal: Write failed: <reason>	リモートホストに強制的に切断されました。 <reason>：切断理由
fatal: Timeout before authentication for <host>	ログイン認証がタイムアウトしました。 <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
Disconnecting: crc32 compensation attack: network attack detected	CRC32 攻撃を検知したため，切断しました。
Disconnecting: deattack denial of service detected	DoS 攻撃を検知したため，切断しました。
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
User <user> from <host> not allowed because none of user's groups are listed in AllowGroups	<host> から接続された <user> は無効なユーザです (認証でエラーとなります)。 <user>：ユーザ名 <host>：リモートホスト
User <user> from <host> not allowed because not in any group	<host> から接続された <user> は無効なユーザです (認証でエラーとなります)。 <user>：ユーザ名 <host>：リモートホスト
fatal: Login refused for too many sessions.	SSH サーバへ接続中のセッションが多いため接続を拒否しました。 接続元の端末を確認してください。不要なセッションは本装置の clear tcp コマンドにて切断するか，接続タイムアウトで切断するのを待ってください。

［注意事項］

- ログは最大 64Kbyte 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。

10.2.7 clear ssh logging コマンド

[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。
Canceled. SSH server's log was NOT cleared.	ログの消去がキャンセルされました。 (ログは消去されませんでした。)
Interrupted. Please, Re-try.	シグナル ([Ctrl+C] など) を受けて キャンセルされました。 [対応] コマンドを再実行してください。
Can't execute (<reason>). (<reason>=Don't care)	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

11 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。

11.1　ログメッセージ一覧

11.1　ログメッセージ一覧

表 11-1　ログメッセージ一覧 (イベント発生部位＝ ACCESS)

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	付加情報上位 4 桁	メッセージテキスト
	内容				
1	E3	ACCESS	00000001	0207	**Unknown host address <ip address>.**
	SSH で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> は IP アドレス，または IPv6 アドレスです。 ［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 アドレスまたは IPv6 アドレスが <ip address> のリモートホストをチェックしてください。 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をチェックしてください。 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指定を行ってください。				
2	E3	ACCESS	00000002	0207	**Login incorrect <user name>.**
	<user name> のアカウントでパスワード認証ログインしようとしましたが，ログインを許可しませんでした。 ［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。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。 2. 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。したがって，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 adduser コマンド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：ls /usr/home と ls /home でホームディレクトリがあるか確認)				
3	E3	ACCESS	00000003	0207	**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。				
4	E3	ACCESS	00030001	0207	**Local authentication succeeded.**
	ユーザからのログイン要求に対し，ローカル認証を行い認証に成功しました。 ［対応］ なし				
5	E3	ACCESS	00030002	0207	**Local authentication failed.**
	ユーザからのログイン要求に対し，ローカル認証を行い認証に失敗しました。 ［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。したがって，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。				
6	E3	ACCESS	00030003	0207	**RADIUS authentication accepted from <host>.**
	ユーザからのログイン要求に対し，RADIUS 認証を行い認証に成功しました。(<host>: サーバのアドレスもしくはホスト名) ［対応］ なし				

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	付加情報上位 4 桁	メッセージテキスト
	内容				
7	E3	ACCESS	00030004	0207	**RADIUS authentication rejected from <host>. "<message>"**
	ユーザからのログイン要求に対し RADIUS 認証を行いましたが，RADIUS サーバにより否認されました。(<host>: サーバのアドレスもしくはホスト名，<message>: サーバからの応答メッセージ) ［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。したがって，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。				
8	E3	ACCESS	00030005	0207	**RADIUS server (<host>) didn’t response.**
	ユーザからのログイン要求に対し RADIUS 認証を行おうとしましたが，RADIUS サーバが応答を返しませんでした。(<host>: サーバのアドレスもしくはホスト名) ［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。				
9	E3	ACCESS	00030006	0207	**RADIUS server configuration is not defined.**
	ユーザからのログイン要求に対し RADIUS 認証を行おうとしましたが，RADIUS サーバに関するコンフィグレーションがありませんでした。 ［対応］ 1. radius-server と aaa 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。 2. radius-server コンフィグレーションにて acct-only が指定され認証が抑止されていないか確認してください。				
10	E3	ACCESS	00030007	0207	**Invalid response is received from <host>.**
	ユーザからのログイン要求に対し RADIUS 認証を行いましたが，RADIUS サーバからの応答が不正でした。 (<host>: サーバのアドレスもしくはホスト名) ［対応］ 1. RADIUS 鍵が本装置と RADIUS サーバ間で一致していることを確認してください。				
11	E3	ACCESS	00030008	0207	**RADIUS authentication failed.**
	ユーザからのログイン要求に対し，RADIUS 認証を行い認証に失敗しました。 ［対応］ 1. 本メッセージの他に RADIUS 認証に関する運用ログが出力されている場合は，そのメッセージを参照してください。				
12	E3	ACCESS	0003000a	0207	**Can't communicate with RADIUS server (<host>).**
	RADIUS サーバと通信できません（<host>: RADIUS サーバの IP アドレスまたはホスト名）。 ［対応］ 1. RADIUS サーバまでの経路があることを確認してください。 2. RADIUS サーバをホスト名で指定している場合は，名前解決ができることを確認してください。				
13	E3	ACCESS	0003000b	0207	**RADIUS authorization response with no contents.**
	RADIUS コマンド承認を行いましたが，RADIUS サーバから正常に取得できたコマンドリストが 1 つもありませんでした。 ［対応］ 1. RADIUS サーバ側の設定（ベンダー固有設定）に Class， Alaxala-Allow-Commands, Alaxala-Deny-Commands が正しく設定されていることを確認してください。				
14	E3	ACCESS	00030013	0207	**TACACS+ authentication accepted from <host>.**
	ユーザからのログイン要求に対し，TACACS+ 認証を行い認証に成功しました（<host>: TACACS+ サーバの IP アドレスまたはホスト名）。 ［対応］ なし。				

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	付加情報上位4桁	メッセージテキスト
	内容				
15	E3	ACCESS	00030014	0207	**TACACS+ authentication rejected from <host>.**
	ユーザからのログイン要求に対し，TACACS+ 認証を行いましたが，TACACS+ サーバにより否認されました（<host>: TACACS+ サーバの IP アドレスまたはホスト名）。 ［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. 本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。したがって，本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. TACACS+ サーバの設定を確認してください。				
16	E3	ACCESS	00030015	0207	**TACACS+ server (<host>) didn't response.**
	ユーザからのログイン要求に対し TACACS+ 認証，コマンド承認（aaa コンフィグレーションで TACACS+ コマンド承認指定有りの場合）を行おうとしましたが，TACACS+ サーバが応答を返しませんでした（<host>: TACACS+ サーバの IP アドレスまたはホスト名）。 ［対応］ 1. TACACS+ 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。				
17	E3	ACCESS	00030016	0207	**TACACS+ server configuration is not defined.**
	ユーザからのログイン要求に対し TACACS+ 認証を行おうとしましたが，TACACS+ サーバに関するコンフィグレーションがありませんでした。 ［対応］ 1. tacacs-server と aaa 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。 2. tacacs-server コンフィグレーションにて acct-only が指定され認証が抑止されていないか確認してください。				
18	E3	ACCESS	00030018	0207	**TACACS+ authentication failed.**
	ユーザからのログイン要求に対し，TACACS+ 認証を行い認証に失敗しました。 ［対応］ 1. 本メッセージの他に TACACS+ 認証に関する運用ログが出力されている場合は，そのメッセージを参照してください。				
19	E3	ACCESS	0003001a	0207	**Can't communicate with TACACS+ server (<host>).**
	TACACS+ サーバと通信できません（<host>: TACACS+ サーバの IP アドレスまたはホスト名）。 ［対応］ 1. TACACS+ サーバまでの経路があることを確認してください。 2. TACACS+ サーバをホスト名で指定している場合は，名前解決ができることを確認してください。 3. TACACS+ コンフィグレーションで設定したポート番号を使用し，TACACS+ サーバが起動していることを確認してください。 4. TACACS+ サーバ側のクライアント IP アドレスに本装置の IP アドレスが登録されていることを確認してください。				
20	E3	ACCESS	0003001b	0207	**TACACS+ authorization response with no contents.**
	TACACS+ コマンド承認を行いましたが，TACACS+ サーバから正常に取得できたコマンドリストが 1 つもありませんでした。 ［対応］ 1. TACACS+ サーバ側の設定（ベンダー固有設定）に class，allow-commands，deny-commands が正しく設定してあることを確認してください。				
21	E3	ACCESS	0003001c	0207	**TACACS+ authorization rejected from <host>.**
	TACACS+ コマンド承認を行いましたが，TACACS+ サーバにより否認されました（<host>: TACACS+ サーバの IP アドレスまたはホスト名）。 ［対応］ 1. TACACS+ サーバ側の設定（本装置のベンダー固有設定）の service 名が正しいことを確認してください。 2. TACACS+ サーバ側でエラーが発生していないことを確認してください。				

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	付加情報上位 4 桁	メッセージテキスト
	内容				
22	E3	ACCESS	0003001d	0207	**Local authorization response with no contents.**
	ローカルコマンド承認を行いましたが，ユーザ名とそれに対応したコマンドクラスまたはコマンドリストの設定がありませんでした。 ［対応］ ローカルログインで認証されたユーザに，コマンドクラス (username view-class) またはコマンドリスト (usrname view・parser view・commands exec) の設定が正しく設定されていることを確認してください。				

付録

付録 A　用語解説

付録 B　準拠規格

付録 C　謝辞 (Acknowledgments)

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-Hellmann 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のみ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，ユーザはユーザ名をパスワードをサーバに送る必要があります。

付録 B　準拠規格

表 B-1　SSH 規格

項番	規格	名称
1	draft-ietf-secsh-architecture-12.txt January 31，2002	SSH Protocol Architecture
2	draft-ietf-secsh-connect-15.txt January 31，2002	SSH Connection Protocol
3	draft-ietf-secsh-dh-group-exchange-02.txt January 2002	Diffie-Hellman Group Exchange for the SSH Transport Layer Protocol
4	draft-ietf-secsh-transport-14.txt March 20，2002	SSH Transport Layer Protocol
5	draft-ietf-secsh-publickeyfile-03.txt October 16，2002	SSH Public Key File Format
6	draft-ietf-secsh-userauth-15.txt February 28，2002	SSH Authentication Protocol

付録 C　謝辞 (Acknowledgments)

This file is part of the OpenSSH software.

The licences which components of this software fall under are as
follows. First, we will summarize and say that all components
are under a BSD licence, or a licence more free than that.

OpenSSH contains no GPL code.

1)
```
 * Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland
 *                    All rights reserved
 *
 * As far as I am concerned, the code I have written for this software
 * can be used freely for any purpose.  Any derived versions of this
 * software must be clearly marked as such, and if the derived work is
 * incompatible with the protocol description in the RFC file, it must be
 * called by a name other than "ssh" or "Secure Shell".

[Tatu continues]
 *  However, I am not implying to give any licenses to any patents or
 * copyrights held by third parties, and the software includes parts that
 * are not under my direct control.  As far as I know, all included
 * source code is used in accordance with the relevant license agreements
 * and can be used freely for any purpose (the GNU license being the most
 * restrictive); see below for details.

[However, none of that term is relevant at this point in time.  All of
these restrictively licenced software components which he talks about
have been removed from OpenSSH, i.e.,

 - RSA is no longer included, found in the OpenSSL library
 - IDEA is no longer included, its use is deprecated
 - DES is now external, in the OpenSSL library
 - GMP is no longer used, and instead we call BN code from OpenSSL
 - Zlib is now external, in a library
 - The make-ssh-known-hosts script is no longer included
 - TSS has been removed
 - MD5 is now external, in the OpenSSL library
 - RC4 support has been replaced with ARC4 support from OpenSSL
 - Blowfish is now external, in the OpenSSL library

[The licence continues]

Note that any information and cryptographic algorithms used in this
software are publicly available on the Internet and at any major
bookstore, scientific library, and patent office worldwide.  More
information can be found e.g. at "http://www.cs.hut.fi/crypto".

The legal status of this program is some combination of all these
permissions and restrictions.  Use only at your own responsibility.
You will be responsible for any legal consequences yourself; I am not
making any claims whether possessing or using this is legal or not in
```

your country, and I am not taking any responsibility on your behalf.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2)

The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a BSD-style license.

```
 * Cryptographic attack detector for ssh - source code
 *
 * Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.
 *
 * All rights reserved. Redistribution and use in source and binary
 * forms, with or without modification, are permitted provided that
 * this copyright notice is retained.
 *
 * THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED
 * WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE
 * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR
 * CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS
 * SOFTWARE.
 *
 * Ariel Futoransky <futo@core-sdi.com>
 * <http://www.core-sdi.com>
```

3)

ssh-keyscan was contributed by David Mazieres under a BSD-style license.

```
 * Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>.
 *
 * Modification and redistribution in source and binary forms is
 * permitted provided that due credit is given to the author and the
 * OpenBSD project by leaving this copyright notice intact.
```

4)

The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers
and Paulo Barreto is in the public domain and distributed
with the following license:

```
* @version 3.0 (December 2000)
*
* Optimised ANSI C code for the Rijndael cipher (now AES)
*
* @author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>
* @author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>
* @author Paulo Barreto <paulo.barreto@terra.com.br>
*
* This code is hereby placed in the public domain.
*
* THIS SOFTWARE IS PROVIDED BY THE AUTHORS "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 AUTHORS 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.
```

5)

One component of the ssh source code is under a 3-clause BSD license,
held by the University of California, since we pulled these parts from
original Berkeley code.

```
* Copyright (c) 1983, 1990, 1992, 1993, 1995
*     The Regents of the University of California.  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. Neither the name of the University nor the names of its contributors
*    may be used to endorse or promote products derived from this software
*    without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``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 REGENTS 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.

6)

Remaining components of the software are provided under a standard
2-term BSD licence with the following names as copyright holders:

Markus Friedl
Theo de Raadt
Niels Provos
Dug Song
Aaron Campbell
Damien Miller
Kevin Steves
Daniel Kouril
Wesley Griffin
Per Allansson
Nils Nordman
Simon Wilkinson

Portable OpenSSH additionally includes code from the following copyright
holders, also under the 2-term BSD license:

Ben Lindstrom
Tim Rice
Andre Lucas
Chris Adams
Corinna Vinschen
Cray Inc.
Denis Parker
Gert Doering
Jakob Schlyter
Jason Downs
Juha Yrj
Michael Stone
Networks Associates Technology, Inc.
Solar Designer
Todd C. Miller
Wayne Schroeder
William Jones
Darren Tucker
Sun Microsystems
The SCO Group

* 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.

*
* THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``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 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.

8) Portable OpenSSH contains the following additional licenses:

a) md5crypt.c, md5crypt.h

* "THE BEER-WARE LICENSE" (Revision 42):
* <phk@login.dknet.dk> wrote this file. As long as you retain this
* notice you can do whatever you want with this stuff. If we meet
* some day, and you think this stuff is worth it, you can buy me a
* beer in return. Poul-Henning Kamp

b) snprintf replacement

* Copyright Patrick Powell 1995
* This code is based on code written by Patrick Powell
* (papowell@astart.com) It may be used for any purpose as long as this
* notice remains intact on all source code distributions

c) Compatibility code (openbsd-compat)

Apart from the previously mentioned licenses, various pieces of code
in the openbsd-compat/ subdirectory are licensed as follows:

Some code is licensed under a 3-term BSD license, to the following
copyright holders:

Todd C. Miller
Theo de Raadt
Damien Miller
Eric P. Allman
The Regents of the University of California
Constantin S. Svintsoff

* 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. Neither the name of the University nor the names of its contributors

*　may be used to endorse or promote products derived from this software
*　without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``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 REGENTS 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.

Some code is licensed under an ISC-style license, to the following
copyright holders:

Internet Software Consortium.
Todd C. Miller

* Permission to use, copy, modify, and distribute this software for any
* purpose with or without fee is hereby granted, provided that the above
* copyright notice and this permission notice appear in all copies.
*
* THE SOFTWARE IS PROVIDED "AS IS" AND TODD C. MILLER DISCLAIMS ALL
* WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES
* OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL TODD C. MILLER BE LIABLE
* FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
* WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION
* OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN
* CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Some code is licensed under a MIT-style license to the following
copyright holders:

Free Software Foundation, Inc.

* Permission is hereby granted, free of charge, to any person obtaining a *
* copy of this software and associated documentation files (the *

```
* "Software"), to deal in the Software without restriction, including      *
* without limitation the rights to use, copy, modify, merge, publish,      *
* distribute, distribute with modifications, sublicense, and/or sell       *
* copies of the Software, and to permit persons to whom the Software is    *
* furnished to do so, subject to the following conditions:                 *
*                                                                           *
* The above copyright notice and this permission notice shall be included  *
* in all copies or substantial portions of the Software.                    *
*                                                                           *
* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS  *
* OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF                *
* MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT.   *
* IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY
CLAIM,   *
* DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR
*
* OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE
OR    *
* THE USE OR OTHER DEALINGS IN THE SOFTWARE.                               *
*                                                                           *
* Except as contained in this notice, the name(s) of the above copyright   *
* holders shall not be used in advertising or otherwise to promote the     *
* sale, use or other dealings in this Software without prior written       *
* authorization.                                                            *
*****************************************************************************/
```

$OpenBSD: LICENCE,v 1.19 2004/08/30 09:18:08 markus Exp $

```
 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) 1998-2005 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.]
*/
```