日本語 HP TCP/IP Services for OpenVMS リリース・ノート

2005 年 7 月

本書はソフトウェアに対する新機能と変更，インストール，アップグレード，互換性情報，新規および既存のソフトウェアの問題点や制限事項，およびソフトウェアとドキュメントの修正事項について解説したものです。

改訂情報: 本書は改訂版です。
オペレーティング・システム: 日本語 OpenVMS Alpha V8.2
ソフトウェア・バージョン: 日本語 HP TCP/IP Services for OpenVMS V5.5

日本ヒューレット・パッカード株式会社

2005 年 7 月

本書は，日本語 VAX DOCUMENT V 2.1を用いて作成しています。

目次

表

まえがき

日本語 HP TCP/IP Services for OpenVMS は， TCP/IP ネットワーキング・プロトコル体系とインターネット・サービスを日本語 OpenVMS システム用に実装した製品です。本書では，日本語 HP TCP/IP Services for OpenVMS バージョン 5.5 の製品について説明します。

日本語 TCP/IP Services は，異機種間ネットワーク通信およびリソース共有のための業界標準プロトコルをサポートする関数およびアプリケーションの包括的なスイートを提供します。

インストレーション手順については，『日本語 HP TCP/IP Services for OpenVMS インストレーション/コンフィギュレーション・ガイド』を参照してください。

リリース・ノートで提供するバージョン固有の情報は，ドキュメント・セットに記載されている情報に代わるものです。ソフトウェアの本バージョンの機能，制限事項，および訂正事項は，リリース・ノートで説明しています。ソフトウェアをインストールする前には，必ずリリース・ノートをお読みください。

対象読者

本リリース・ノートは，経験のある OpenVMS および UNIX のシステム管理者を対象にしており， OpenVMS のシステム管理， TCP/IP ネットワーク，および日本語 TCP/IP Services 製品に関する知識があるものと想定しています。

関連資料

表 1 に，日本語 TCP/IP Services の本バージョンで利用できるドキュメントを示します。

表 1　日本語 TCP/IP Services のドキュメント

マニュアル	内容
Compaq TCP/IP Services for OpenVMS Concepts and Planning	このマニュアルでは，日本語 TCP/IP Services ソフトウェアを使用するためにシステムのコンフィギュレーションを行う前に考慮すべき一般的な設計上の問題を含め， OpenVMS システム上での TCP/IP ネットワーキングに関する概念的な情報を提供します。 また，このマニュアルでは， TCP/IP Services のドキュメント・セットのマニュアルについて記述し，日本語 TCP/IP Services ソフトウェア製品で使用されている用語および頭文字の用語集を提供しています。
日本語 HP TCP/IP Services for OpenVMS リリース・ノート	リリース・ノートでは，ドキュメント・セットの情報に置き代わるバージョン固有の情報を提供しています。ソフトウェアの本バージョンの機能，制限事項，および訂正事項については，リリース・ノートに記載されています。ソフトウェアをインストールする前には必ずリリース・ノートをお読みください。
日本語 HP TCP/IP Services for OpenVMS インストレーション/コンフィギュレーション・ガイド	このマニュアルは，日本語 TCP/IP Services 製品のインストレーションとコンフィギュレーションの方法について説明しています。
日本語 HP TCP/IP Services for OpenVMS 日本語機能の手引き	このマニュアルは，日本 HP TCP/IP Services for OpenVMS の日本語機能の概要と，漢字フィルタの使用方法，および漢字フィルタのプログラミングについて説明しています。
HP TCP/IP Services for OpenVMS User's Guide	このマニュアルは，リモート・ファイル操作，電子メール，TELNET， TN3270，ネットワーク印刷など，日本語 TCP/IP Services で利用できるアプリケーションの使用方法について説明しています。また，これらのサービスを使って，プライベート・インターネットや世界規模のインターネット上のシステムと通信を行う方法についても説明しています。
HP TCP/IP Services for OpenVMS Management	このマニュアルは，日本語 TCP/IP Services 製品のコンフィギュレーションと管理の方法について説明しています。 このマニュアルは，『*HP TCP/IP Services for OpenVMS Management Command Reference*』と併用してください。
HP TCP/IP Services for OpenVMS Management Command Reference	このマニュアルは，日本語 TCP/IP Services の管理コマンドについて説明しています。 このマニュアルは『*HP TCP/IP Services for OpenVMS Management*』と併用してください。
HP TCP/IP Services for OpenVMS Management Command Quick Reference Card	このリファレンス・カードでは，構成要素ごとに TCP/IP 管理コマンドをリストし，各コマンドの目的を説明しています。
HP TCP/IP Services for OpenVMS UNIX Command Equivalents Reference Card	このリファレンス・カードには，よく実行されるネットワーク管理タスクおよび対応する TCP/IP 管理と UNIX コマンド書式に関する情報が記載されています。
HP TCP/IP Services for OpenVMS ONC RPC Programming	このマニュアルは，オープン・ネットワーク・コンピューティングのリモート・プロシージャ・コール (ONC RPC) を使った高水準プログラミングについて概説しています。また， RPC プログラミング・インタフェースや， RPCGEN プロトコル・コンパイラを使ったアプリケーションの作成方法についても説明しています。
HP TCP/IP Services for OpenVMS Guide to SSH	このマニュアルは， OpenVMS ソフトウェア用の SSH のコンフィギュレーション，セット・アップ，使い方，および管理に津いて説明してます。

(次ページに続く)

表 1 (続き) 日本語 TCP/IP Services のドキュメント

マニュアル	内容
HP TCP/IP Services for OpenVMS Sockets API and System Services Programming	このマニュアルは，ソケット API と OpenVMS システム・サービスを使って，ネットワーク・アプリケーションを開発する方法について説明しています。
HP TCP/IP Services for OpenVMS SNMP Programming and Reference	このマニュアルは，簡易ネットワーク管理プロトコル (SNMP) および SNMP アプリケーション・プログラミング・インタフェース (API) について説明しています。また， TCP/IP Services で提供されるサブエージェント，サブエージェントの管理のために提供されているユーティリティ，およびユーザ独自のサブエージェントの構築方法についても説明しています。
HP TCP/IP Services for OpenVMS Tuning and Troubleshooting	このマニュアルでは，ネットワーク問題の原因を切り分ける方法，および最高の性能を引き出すために日本語 TCP/IP Services ソフトウェアをチューニングする方法について説明しています。
HP TCP/IP Services for OpenVMS Guide to IPv6	このマニュアルでは， IPv6 環境，この環境におけるシステムの役割り，異なる IPv6 アドレスのタイプと機能，および 6bone ネットワークにアクセスするために日本語 TCP/IP Services をコンフィギュレーションする方法について説明しています。

HP OpenVMS の製品およびサービスについての詳細は，次の HP の Web サイトにアクセスしてください。

```
http://www.hp.com/go/openvms
```

TCP/IP プロトコル体系の包括的な概要については， Douglas Comer 著『Internetworking with TCP/IP: Principles, Protocols, and Architecture』が役に立ちます。

表記法

「TCP/IP Services」は日本語 HP TCP/IP Services for OpenVMS を指します。

「UNIX」は Tru64 UNIX オペレーティング・システムを指します。

本書で使用している IP アドレスは架空のものです。

本書では次の表記法に従っています。

Ctrl/*x*	Ctrl/*x*のような表記は， Ctrl というラベルの付いたキーを押しながら，別のキーまたはポインティング・デバイスのボタンを押すことを示します。
PF1 *x*	PF1 *x*のような表記は，まず， PF1 というラベルの付いたキーを押して放し，その後，別のキーまたはポインティング・デバイスのボタンを押すことを示します。

Return	例中では，四角で囲まれたキー名は，ユーザがキーボードのキーを押すことを示します (本文中では，キー名は四角で囲まれません)。 本書の HTML 版では，この表記は四角ではなく，カッコになります。
. . .	例中の水平方向の省略記号は，次のいずれかを示します。 • 文で追加のオプション引数が省略されている。 • 前述の項目 (1 つまたは複数) が 1 回以上繰り返される。 • 追加のパラメータ，値，または他の情報が入力できる。
. . .	垂直方向の省略記号は，コーディング例またはコマンド形式で項目が省略されていることを示します。つまり，説明しているトピックに関して重要でない事項であるため，省略されています。
( )	コマンド形式の説明で，カッコは，複数選択する場合には，選択したものをカッコで囲む必要があることを示します。
[ ]	コマンド形式の説明で，大カッコはオプション選択を示します。ユーザは 1 つまたは複数の項目を選択することも，あるいは選択しないこともできます。コマンド行に大カッコを入力してはなりません。ただし， OpenVMS のディレクトリ指定，または割り当て文の部分列指定の構文では大カッコを含める必要があります。
|	コマンド形式の説明では，縦線は大カッコまたは中カッコ内で選択項目を区切ります。大カッコ内では，選択はオプションですが，中カッコ内では，必ず 1 つ以上を選択する必要があります。コマンド行に縦線を入力してはなりません。
{ }	コマンド形式の説明で，中カッコは必須の選択を示し，リストされている項目から 1 つ以上の項目を選択する必要があります。コマンド行に中カッコを入力してはなりません。
bold text	この書体は，新しい用語であることを示します。また，引数の名前，属性，あるいは理由を示します。
italic text	斜体のテキストは，変数を示します。変数には，システム出力 (Internal error *number*)，コマンド行 (/PRODUCER=*name*)，および本文中のコマンド・パラメータ (このとき，*dd*はデバイス・タイプの事前に定義されたコードを表します) において異なる情報も含まれます。
UPPERCASE TEXT	大文字は，コマンド，ルーチン名，ファイル名，またはシステム特権の短縮形を示します。
`Monospace text`	この書体は，コーディング例および対話型の画面表示を示します。 C プログラミング言語では，テキスト中のこの書体は次の項目を示します。つまり，キーワード，単独でコンパイルされた外部関数とファイル，構文のまとめ，例中の変数または識別子の参照を示します。
-	コマンド形式の説明，コマンド行，コード行の終わりのハイフンは，コマンドまたは文が次の行に継続することを示します。
数	本文中のすべての数は，特に明記していなければ， 10 進数です。基数が 10 進法以外の場合，つまり， 2 進， 8 進， 16 進の場合には，明記されています。

1

新機能と拡張された動作

この章では， TCP/IP ServicesVersion 5.5 の新機能および拡張された動作について説明します。

注意

日本語 TCP/IP Services **バージョン** 5.5 **は，** OpenVMS Alpha **システムでのみサポートされます。** Industry Standard 64 (I64) **システムでは標準版** TCP/IP Services **バージョン** 5.5 **を使用してください。また，** VAX **システムでは，日本語** TCP/IP Services **バージョン** 5.3 **を使用してください。**

TCP/IP Services **バージョン** 5.5 **を使用するには，** OpenVMS **バージョン** 8.2 **以上にアップグレードする必要があります。**

TCP/IP Services のインストールとコンフィギュレーションについては，『日本語 HP TCP/IP Services for OpenVMS インストレーション/コンフィギュレーション・ガイド』を参照してください。

表 1–1 は， TCP/IP Services Version 5.5 の新機能と，各機能を説明している箇所を示しています。

表 1–1 TCP/IP Services for OpenVMS の新機能

機能	参照先	説明
HP Industry Standard 64 サーバ・プラットフォームのサポート	1.1	TCP/IP Services は Alpha プラットフォームだけでなく， I64 プラットフォームでも動作します。
failSAFE IP での IPv6 のサポート	1.2	failSAFE IP は IPv6 をサポートします。本バージョンの TCP/IP Services では， failSAFE IP を管理するために，新たに`ifconfig`コマンドが提供されるようになりました。
Secure IMAP	1.3	Secure IMAP は SSL (Secure Sockets Layer) を使用します。
IPv6 のアップデートと拡張機能	1.4	近隣探索と IPv6 API が拡張されました。
libpcap API のサポート	1.5	本リリースの TCP/IP Services では，`libpcap`アプリケーション・プログラミング・インタフェース (API) がサポートされるようになりました。

(次ページに続く)

表 1–1 (続き) TCP/IP Services for OpenVMS の新機能

機能	参照先	説明
NTP (Network Time Protocol) V4.2 のサポート	1.6	NTP はバージョン 4.2 にアップグレードされ, IPv6 をサポートするようになりました。
SSH の新機能	1.7	SSH はバージョン 3.2 にアップグレードされ, IPv6 をサポートするようになりました。
TCPDUMP バージョン 3.8.3	1.8	TCPDUMP はバージョン 3.8.3 にアップグレードされました。
TCPIP$EXAMPLES でアップデートされたヘッダ・ファイル	1.9	TCPIP$EXAMPLES にあるヘッダ・ファイルがアップデートされました。

1.1 HP Industry Standard 64 サーバ・プラットフォームのサポート

TCP/IP Services は HP Itanium®ベース (I64) プラットフォームでも動作するようになり， Alpha プラットフォームと基本的に同じ機能を提供するようになりました。I64 のサポートについての詳細は，次の節を参照してください。

- 第 2.5 節, OpenVMS Cluster へのシステムの追加
- 第 3.1 節, OpenVMS I64 プラットフォームの制限事項

1.2 failSAFE IP での IPv6 のサポート

本リリースで failSAFE IP サービスがアップグレードされ， IPv6 環境もサポートされるようになりました。

ifconfigユーティリティもアップデートされました。このユーティリティについての詳細は，次のコマンドを入力してください。

```
$ TCIPIP HELP IFCONFIG
```

ifconfigユーティリティを使用してインタフェース・フェールオーバを監視する方法についての詳細は，『*HP TCP/IP Services for OpenVMS Management*』を参照してください。

1.3 Secure IMAP

本リリースの TCP/IP Services には Secure IMAP が付属しており， SSL (Secure Sockets Layer) をサポートします。 Secure IMAP は，メッセージの安全な検索および管理機能を提供します。 Secure IMAP はポート 993 で接続を受け付け，パスワード，データ，および IMAP コマンドを暗号化します。 Outlook Express, Netscape， Mozilla など， SSL を使用するクライアントと互換性があります。この

機能を使用するには，以下の HP OpenVMS Security Web サイトから OpenVMS Alpha 用の HP SSL キットをダウンロードする必要があります。

```
http://h71000.www7.hp.com/openvms/security.html
```

HP SSL ソフトウェアがインストールされていない場合は， IMAP サーバは非 SSL モードで通信します。

SSL 論理名は SSL スタートアップ・プロシージャで定義されます。したがって，SSL 論理名を使用して証明書およびキー・ファイルを検索するように IMAP をコンフィギュレーションしている場合は， TCP/IP Services スタートアップ・プロシージャより前に， SSL スタートアップ・プロシージャが確実に実行されるようにする必要があります。

Secure IMAP コンフィギュレーションは，コンフィギュレーション・ファイル SYS$SYSDEVICE:[TCPIP$IMAP]TCPIP$IMAP.CONF によって制御されます。

Secure IMAP を管理するには，次の新しいコンフィギュレーション・オプションおよび論理名を使用します。

- SSL-Server-Port

  このオプションは， SSL 接続のために IMAP サーバが使用できるポートを定義します。デフォルトのポートは 993 です。たとえば，次の設定ではポート 1004 を指定しています。

  ```
  SSL-Server-Port:1004
  ```

- Disable-Clear-Text

  このオプションを有効にすると， IMAP サーバはクリアテキスト接続をサービスしなくなります。したがって，ポート 143 でクライアント接続要求を行うと，次のエラー・メッセージが出力されます。

  ```
  The IMAP server serves ONLY SSL client requests. Please reconfigure your
  client for SSL.
  ```

  たとえば，次の設定はこのオプションを有効にします。

  ```
  Disable-Clear-Text:YES
  ```

- Disable-SSL

  このオプションを有効にすると， IMAP は SSL クライアント接続をサービスしなくなります。たとえば，次の設定はこのオプションを有効にします。

  ```
  Disable-SSL:YES
  ```

- TCPIP$IMAP_CERT_FILE

  この論理名は， IMAP が SSL のために使用する証明書ファイルの名前を指定します。この名前を定義しないと，デフォルトはSSL$CERTS:SERVER.CRTになります。

この論理名に割り当てる値として，完全なファイル指定またはその一部を指定できます。つまり，ディレクトリとファイル名のいずれか一方，または両方を指定できます。ファイル指定で省略した部分には，デフォルトが適用されます。

たとえば，次のコマンドはファイル名を TCPIP$IMAP.CRT に変更します。

```
$ DEFINE/SYSTEM/EXECUTIVE_MODE TCPIP$IMAP_CERT_FILE SSL$CERTS:TCPIP$IMAP.CRT
```

- TCPIP$IMAP_KEY_FILE

  この論理名は， IMAP が SSL のために使用するキー・ファイルの名前を指定します。この名前を定義しないと，デフォルトはSSL$CERTS:SERVER.KEYになります。

  値として，完全なファイル指定またはその一部を指定できます。つまり，ディレクトリとファイル名のいずれか一方，または両方を指定できます。ファイル指定で省略した部分には，デフォルトが適用されます。

  たとえば，次のコマンドはファイル名を TCPIP$IMAP.KEY に変更します。

```
$ DEFINE/SYSTEM/EXECUTIVE_MODE TCPIP$IMAP_KEY_FILE SSL$KEY:TCPIP$IMAP.KEY
```

論理名とコンフィギュレーション・オプションが確実に有効になるようにするには，これらの設定を変更する前に， IMAP サーバを停止する必要があります。

1.4 IPv6 のアップデートと拡張機能

ここでは， IPv6 (Internet Protocol Version 6) のアップデートされた機能および拡張機能について説明します。

IPv6 の変更点についての詳細は，第 4.7 節を参照してください。

1.4.1 IPv6 のコンフィギュレーションの拡張

IPv6 のサポートが拡張され，ip6.arpaゾーンの動的アップデート機能が提供されるようになり， IPv6 API もアップデートされました。

1.4.2 近隣探索は ip6.arpa DNS リバース・ゾーンの動的アップデート要求をサポートする

近隣探索 (TCPIP$ND6HOST プロセス) は RFC 3152 をサポートするようになり，ip6.arpa DNS リバース・ゾーンに対してのみ，動的アップデート要求を送信するようにコンフィギュレーションできるようになりました。

これまで，近隣探索デーモンは，ip6.int DNS リバース・ゾーンに対してのみ，動的アップデート要求を送信していました (ip6.int DNS リバース・ゾーンは廃止される予定です)。

ip6.intゾーンをもとにした委任をサポートする必要がある場合は，ip6.intゾーンが正しく存在していることを確認してください。詳細については，『*HP TCP/IP Services for OpenVMS Guide to IPv6*』の 3.1.3 項「Using DNAME To Rename ip6.int」を参照してください。

ゾーンをアップデートするには， TCPIP$ND6HOST は動的アップデートをプライマリ・マスタ・ネーム・サーバに送信します。プライマリ・マスタ・ネーム・サーバの名前は，ゾーンの SOA レコードの MNAME フィールドに格納されます。マスタ・ネーム・サーバを特定するには， TCPIP$ND6HOST はゾーンの SOA レコードを要求するクエリを， DNS リゾルバ・コンフィギュレーションに指定されているネーム・サーバに送信します。 DNS リゾルバ・コンフィギュレーション情報を表示するには， TCP/IP 管理コマンドSHOW NAME_SERVICEを使用します。

この機能を使用するには，動的アップデートを有効に設定する必要があります。デフォルトでは，動的アップデートは DNS サーバで拒否されます。動的アップデートを有効に設定する方法については，『*HP TCP/IP Services for OpenVMS Management*』の BIND に関する章を参照してください。

1.4.3 IPv6 API のアップデート

IPv6 プログラミング API はアップデートされました。本リリースでは，新しいプログラミング・サンプルが提供されます。 IPv6 API で変更された点は次のとおりです。

- IPv6 の変更点:
  - これまでgetaddrinfo関数呼び出しのai_flagsパラメータに指定していたフラグ値 AI_DEFAULT は無効になりました。今後のリリースでは， NETDB.H ファイルから削除される予定です。このフラグで定義されていた動作を実行するには，フラグ値 AI_V4MAPPED と AI_ADDRCONFIG の論理和 (OR) を指定します。
  - BIND リゾルバは，次の RFC ドラフトの記述に従ってアップデートされました。

    draft-ietf-ipngwg-scoping-arch-04.txt

    この変更により，目的のスコープ・ゾーンも指定することで， IPv6 非グローバル・アドレスを正確に指定できるようになりました。形式は次のとおりです。

    address%zone_id

    非グローバル・アドレスの形式には，次の情報が含まれます。
    - addressは，リテラルの IPv6 アドレスです。
    - zone_idは，アドレスのゾーンを指定する文字列です。
    - %は，アドレスとゾーン識別子を区切る区切り文字です。

次の例では，インタフェース WE0 上の非グローバル・アドレスを指定しています。

```
fe80::1234%WE0
```

- SYS$COMMON:[SYSHLP.EXAMPLES.TCPIP]に格納されている， IPv4 TCP および UDP クライアント/サーバ C ソケット・プログラミングのサンプル・プログラムは， IPv6 に移植されました。これらのサンプル・プログラムの IPv6 バージョンは， SYS$COMMON:[SYSHLP.EXAMPLES.TCPIP.IPV6]に格納されています。
- SYS$COMMON:[SYSHLP.EXAMPLES.TCPIP.IPV6.BIND]に格納されている IPv6 のサンプル・データベースおよびサンプル・コンフィギュレーション・ファイルは，最新の状況を反映するようにアップデートされています。

『*HP TCP/IP Services for OpenVMS Sockets API and System Services Programming*』に記載されているように，初期の Early Adoper Kits (EAK) で提供されていたいくつかのプログラミング関数は廃止されました。これらの関数は TCP/IP Services バージョン 5.5 以降ではサポートされません。新規アプリケーションを作成する場合は，これらの関数を使用しないでください。

以下の表に関数と代替関数を記載します。既存のアプリケーションがこれらの関数を使用している場合，コードの修正方法に関して『*HP TCP/IP Services for OpenVMS Sockets API and System Services Programming*』を参照してください。

廃止関数	代替関数
getipnodebyname	getaddrinfo
getipnodebyaddr	getnameinfo
freehostent	freeaddrinfo

1.5 libpcap API のサポート

本リリースでは，libpcap API (バージョン 0.8.3) がサポートされるようになりました。論理名TCPIP$LIBPCAP_EXAMPLESに関連付けられているディレクトリにサンプル・プログラムが用意されています。また，包括的なドキュメンテーション・ファイル$$TCPIP$LIBPCAP_DOCUMENTATION.HTML もそのディレクトリに格納されています。libpcap関数TCPIP$LIBCAP_SHR.EXEをインプリメントするlibpcap共有イメージは，論理名 SYS$SHARE に関連付けられているディレクトリにあります。

1.6 NTP (Network Time Protocol) V4.2 のサポート

本バージョンの TCP/IP Services では， NTP V4.2.0 がサポートされるようになりました。本リリースでは， NTP バージョン 3 および NTP バージョン 2 との下位互換性もサポートされますが， NTP バージョン 1 はサポートされません。 NTP バージョン 1 がサポートされなくなったのは，セキュリティの脆弱性のためです。

本リリースでは， IPv4 アドレス・ファミリのサポートに加えて， IPv6 アドレス・ファミリもサポートされます。同じシステムで同時にいずれか一方または両方のアドレス・ファミリを使用できます。

これまで IPv4 アドレス・ファミリの使用をサポートしていたコンフィギュレーション・オプションは， IPv6 アドレス・ファミリも受け付けるようになりました。この機能を使用するには，『日本語 HP TCP/IP Services for OpenVMS インストレーション/コンフィギュレーション・ガイド』の説明に従って， TCP/IP Services で IPv6 を有効にしておく必要があります。

1.6.1 暗号化のサポート

本リリースでは，対称鍵暗号方式を使用した認証がサポートされるようになりました。 Autokey 公開鍵暗号方式は本リリースでは使用できません。対称鍵暗号方式についての詳細は，第 1.6.7 項および『*HP TCP/IP Services for OpenVMS Management*』の NTP に関する章を参照してください。

1.6.2 BIND (Berkeley Internet Name Domain) での NTP V4.2.0 の使用

IPv6 対応システムで NTP を使用するときに， IPv4 アドレスと IPv6 アドレスの両方が DNS の同じドメイン名に関連付けられている場合， BIND リゾルバは TCPIP$NTP.CONF に指定されているホストに対して， IPv6 アドレスを使用します。

1.6.3 NTPDC ユーティリティの使用

本リリースの TCP/IP Services より前に提供されていた NTPDC の各バージョンは IPv6 対応ではありません。このため，次のコマンドを使用すると， IPv4 の関連付けだけが表示されます。

- `peers`
- `dmpeers`
- `listpeers`
- `monlist`
- `pstats`

- reslist
- showpeer

1.6.4 NTPQ ユーティリティの使用

本リリースの TCP/IP Services より前に提供されていた NTPQ の各バージョンは IPv6 対応ではありません。このため，次のコマンドを使用すると， IPv6 の関連付けに対しては 0.0.0.0 が表示されます。

- peers
- lopeers
- lpassociations
- lpeers
- opeers
- passociations
- pstatus

1.6.5 NTPTRACE ユーティリティの使用

NTPTRACE ユーティリティは NTP V4.2.0 にアップデートされておらず， IPv4 アドレス・ファミリだけを取り扱います。

1.6.6 IPv6 の場合の NTP パケット・ヘッダ

IPv6 関連付けで動作する場合， NTP パケット・ヘッダのreference IDフィールドは変化します。 IPv4 関連付けの場合，このフィールドにはサーバの 32 ビット IPv4 アドレスが格納されます。 IPv6 関連付けの場合は，このフィールドにはアドレスから作成された MD5 ハッシュの最初の 32 ビットが格納されます。このため，関連付けが IPv6 ホストの場合，peersコマンドや，本リリースの NTPQ で提供される他の同様のコマンドを使用すると，refidには， IPv4 アドレスの形式でランダムな数値が表示されます。

1.6.7 NTP_GENKEYS ユーティリティは NTP_KEYGEN に変更

本バージョンの TCP/IP Services では， NTP_GENKEYS ユーティリティが新しい NTP_KEYGEN ユーティリティに変更されました。 NTP バージョン 3 および NTP バージョン 4 の対称鍵認証で使用されるランダムなキーを生成するには，NTP_KEYGEN ユーティリティを使用してください。

16 のランダムな対称鍵を格納した TCPIP$NTPKEY_MD5KEY_hostname.timestampファイルをプログラムで生成するには，-Mコマンド・ライン・オプションを使用します。大文字を残すには，次の例に示すように，-Mを二重引用符で囲んでコマンド・ラインに指定する必要があります。

```
$ @SYS$MANAGER:TCPIP$DEFINE_COMMANDS.COM
$ ntp_keygen -"M"
```

ホスト名 (gethostname( )関数から返されるhostname) とタイムスタンプは，ファイル名の一部として使用されます。タイムスタンプを生成するアルゴリズムは，システム・クロックをもとにしているため，プログラムを実行するたびに，異なるファイル名が生成されます。

TCPIP$NTPKEY_MD5KEY_hostname.timestampファイルには， 16 の MD5 キーが格納されます。各キーは， ASCII の 95 文字印刷サブセットからランダムに選択された 15 文字で構成されます。このファイルは， TCPIP$NTP.CONF コンフィギュレーション・ファイルのkeysコマンドで指定される場所にある NTP サーバが読み取ります。 NTPQ プログラムと NTPDC プログラムで使用するために，覚えやすいパスワードで構成される追加キーを手動で追加してください。このファイルは，同じセキュリティ区画を共有する他のサーバおよびクライアントに安全な方法で配布する必要があります。 MD5 プログラムのキー識別子は，識別子 1 ～ 16 だけを使用します。各関連付けのキー識別子は，serverまたはpeerコンフィギュレーション・ファイル・コマンドに指定します。

1.6.8 NTP クロック同期化の拡張

クロックを徐々に調整するための NTP スルー・メカニズム (slew mechanism) は，1 秒以上のオフセットの同期化を容易に行うことができるように拡張されました。最大スルー値 (NTP が 1 回の試行でクロックを調整する最大値) が変更され，このようなオフセットに対してより迅速にクロックの同期をとることができるようになりました。 1 秒のオフセットを修正するのに，以前のバージョンの NTP では約 30 分かかっていましたが，本バージョンでは， NTP はわずか 20 秒で修正できるようになりました。

1 秒未満のクロック・オフセットについては，スルー・メカニズムは変更されていません。

1.7 SSH の新機能

ここでは， SSH サービスで新たに開発された機能について説明します。

1.7.1 SSH バージョン 3.2 へのアップグレード

SSH サービスはバージョン 3.2 にアップグレードされました。このアップグレードで，SSH ユーティリティが変更されました。SSH ユーティリティについての詳細は，次の例に示すように，ユーティリティのコマンド・ラインで-hフラグを使用してください。

```
$ SSH -h
```

1.7.2 SSH は IPv6 をサポート

本リリースの TCP/IP Services の SSH では，IPv6 環境がサポートされるようになりました。

SSH が IPv6 環境で動作するには，サービスを IPv6 に設定する必要があります。SSH の設定を表示するには，次のコマンドを入力します。

```
$ TCPIP
TCPIP> SHOW SERVICE SSH /FULL
```

IPv6 フラグが指定されていない場合は，次のコマンドを入力します。

```
TCPIP> SET SERVICE SSH /FLAG=IPV6
```

1.7.3 SSH ポート・フォワーディング

SSH for OpenVMS では，UNIX と同様のポート・フォワーディング・コマンドがサポートされます。たとえば，-xフラグや+xフラグをはじめ，ForwardX11コンフィギュレーション・キーワードもサポートされます。SSH ポート・フォーワーディングについての詳細は，以下を参照してください。

- 第 4.14.4 項
- 表 5–2

1.7.4 SSH ファイル転送

SSH ファイル・コピー操作の最大ファイル・サイズは，4 メガバイトから 4 ギガバイトに拡張されました。さらに，使用できるリソース，CPU，ネットワークの状態などに応じて，ファイル転送の速度も大幅に向上しています。制限事項については，第 3.11.13 項を参照してください。

1.7.5 SSH バッチ・ジョブ

本バージョンの TCP/IP Services では，バッチ・ジョブで SSH コマンドを使用できるようになりました。 SSH セッションに対してバッチ・ジョブを使用する場合の制限事項については，第 3.11.10 項を参照してください。

1.8 TCPDUMP バージョン 3.8.3

本リリースの TCP/IP Services では， TCPDUMP ユーティリティがアップグレードされています。バージョン 2.2 からバージョン 3.8.3 にアップグレードされた TCPDUMP では，libpcapバージョン 0.8.3 API が使用されます。新しいバージョンの TCPDUMP についての詳細は， Web サイトwww.tcpdump.orgを参照するか，または「TCPIP HELP TCPDUMP」と入力して，新バージョンに関する情報を表示してください。

この機能をいち早く利用するユーザのために，libpcap API が用意されています。詳細については，第 1.5 節を参照してください。

1.9 TCPIP$EXAMPLES でアップデートされたヘッダ・ファイル

本リリースの TCP/IP Services では， TCPIP$EXAMPLES に格納されている複数のヘッダ・ファイルがアップデートされています。このようにアップデートされたのは，次の理由によります。

- IETF (Internet Engineering Task Force) RFC (Request for Comments) の最近の変更
- パフォーマンスに関する配慮 (構造のベース・アライメントの向上)
- TCP/IP Services の内部的な変更

下位互換性は保証されません。

アップデートされたヘッダ・ファイルは次のとおりです。

- IF.H
- IF_TYPES.H
- IN.H
- IN6.H
- SOCKET.H
- STROPTS.H
- TCP.H
- PCAP.H

- PCAP-PDF.H
- __DECC_INCLUDE_PROLOGUE.H

2

インストール，コンフィギュレーション，スタートアップ，およびシャットダウン

この章では， TCP/IP Services のインストールとコンフィギュレーションをはじめ，スタートアップ・プロシージャやシャットダウン・プロシージャに関する注意事項と変更点について説明します。この章の内容は，『日本語 HP TCP/IP Services for OpenVMS インストレーション/コンフィギュレーション・ガイド』も手元に置いて参照してください。

注意

TCP/IP Services バージョン 5.5 を使用するには，OpenVMS バージョン 8.2 にアップグレードする必要があります。

2.1 V5.3 EAK (アーリー・アダプターズ・キット) がインストールされている場合の注意

次の V5.3 EAK を 1 つ以上インストールしている場合は， TCP/IP Services V5.5 をインストールする前に， PCSI REMOVE コマンドを使用して， EAK を削除する必要があります。

- SSH for OpenVMS EAK
- failSAFE IP EAK

注意

failSAFE IP EAK を削除した後，現在のバージョンの TCP/IP Services をインストールする場合は，TCPIP$CONFIG.COM を実行して，ターゲット・インタフェースとホーム・インタフェースを再確立する必要があります。

2.2 TCP/IP Services バージョン 4.x からのアップグレード

ここでは，以前のバージョンの TCP/IP Services (UCX) から現在のバージョンへアップグレードするときに，ソフトウェアの動作を以前と同じになるように保持する方法について説明します。

2.2.1 LPD のアップグレード

- 編集結果をシステム・スタートアップ・コマンド・プロシージャにマージする場合，キュー UCX$LPD_QUEUE を起動および停止するコマンドを入れないようにしてください。このキューは， TCPIP$LPD_QUEUE に置き換えられています。 TCPIP$LPD_QUEUE を起動および停止するコマンドは， LPD スタートアップ・コマンド・プロシージャ・ファイルおよび LPD シャットダウン・コマンド・プロシージャ・ファイルにあります。
- 編集結果をマージした後，追加した LPD クライアント・キュー・スタートアップ・コマンドの/PROCESSOR 修飾子の値を， UCX$LPD_SMB から TCPIP$LPD_SMB に変更します。たとえば，次のコマンドを入力します。

```
LSE Command> SUBSTITUTE/ALL "ucx$lpd_smb" "tcpip$lpd_smb"
```

2.2.2 SNMP スタートアップおよびシャットダウン時の動作の保持

現在のバージョンの TCP/IP Services にアップグレードした後，次のいずれかの操作を行って， SNMP のスタートアップが正しく行われるようにする必要があります。

- SNMP が以前の TCP/IP Services のインストレーション (UCX) の下でコンフィギュレーションされていて，以前のコンフィギュレーションをそのまま保持する場合は， SYS$MANAGER:TCPIP$CONFIG.COM コマンド・プロシージャを実行し， UCX コンフィギュレーション・ファイルを自動的に変換するオプションを選択します。
- 現在のバージョンの TCP/IP Services にアップグレードした後，SYS$MANAGER:TCPIP$CONFIG.COM コマンド・プロシージャを実行します。 SNMP がまだ有効な場合は， SNMP をいったん無効にした後，再び有効にします。このコンポーネントが正常に動作するには，この操作が必要です。

UCX$SNMP_STARTUP.COM および UCX$SNMP_SHUTDOWN.COM コマンド・プロシージャをカスタマイズしたバージョン (拡張サブエージェントの起動と停止に使用) を使用している場合は，新バージョンの TCP/IP Services へアップグレードする前に，カスタマイズしたファイルを別のディレクトリに保存してください。この操作を行わないと，カスタマイズした情報が失われます。

次に示す場所で，これらのファイルのバージョンを確認してください。

- SYS$MANAGER
- SYS$STARTUP
- SYS$SYSDEVICE:[UCX$SNMP]

TCP/IP Services をインストールした後，『*HP TCP/IP Services for OpenVMS Management*』の説明に従って，TCPIP$SNMP_SYSTARTUP.COM および TCPIP$SNMP_SYSHUTDOWN.COM コマンド・プロシージャにコマンドを手動で入力します。

2.2.3 SNMP のスタートアップとシャットダウンのカスタマイズ

TCPIP$CONFIG.COM コマンド・プロシージャを使用して SNMP を有効にした場合，次のファイルは作成されなくなりました。

- TCPIP$SNMP_SYSTARTUP.COM
- TCPIP$SNMP_SYSHUTDOWN.COM

これらのコマンド・プロシージャ・ファイルは，カスタム SNMP サブエージェントの起動と停止に使用されます。将来のバージョンの TCP/IP Services をインストールしても，これらのファイルに影響ありません。

2.2.4 TCP/IP Services のインストール時の SNMP メッセージ

同じバージョンの TCP/IP Services を 2 回以上インストールするサイトでは，次のような情報メッセージがインストレーション・ダイアログに表示されることがあります。

```
Do you want to review the options? [NO]

Execution phase starting ...

The following product will be installed to destination:
    DEC AXPVMS TCPIP T5.3-9I              DISK$AXPVMSSYS:[VMS$COMMON.]
The following product will be removed from destination:
    DEC AXPVMS TCPIP T5.3-9H              DISK$AXPVMSSYS:[VMS$COMMON.]
%PCSI-I-RETAIN, file [SYSEXE]TCPIP$ESNMP_SERVER.EXE was not replaced because
file from kit does not have higher generation number
%PCSI-I-RETAIN, file [SYSEXE]TCPIP$HR_MIB.EXE was not replaced because file
from kit does not have higher generation number
%PCSI-I-RETAIN, file [SYSEXE]TCPIP$OS_MIBS.EXE was not replaced because file
from kit does not have higher generation number
%PCSI-I-RETAIN, file [SYSLIB]TCPIP$ESNMP_SHR.EXE was not replaced because file
from kit does not have higher generation number
%PCSI-I-RETAIN, file [SYSLIB]UCX$ESNMP_SHR.EXE was not replaced because file
from kit does not have higher generation number
```

これらのメッセージは無視してかまいません。

2.2.5 SNMP サブエージェントのスタートアップ・メッセージ

SNMP スタートアップ・プロシージャは，次のエラー・メッセージをサブエージェント・ログ・ファイルに出力することがあります。

```
25-JUL-2001 14:13:32.47 **ERROR ESNMP_INIT.C line 3777: Could not
connect to master: connection refused
25-JUL-2001 14:13:32.94 WARNING OS_MIBS.C line 942: Master agent
cannot be reached.  Waiting to attempt reconnect.
```

これらのメッセージが記録されるのは，タイミングに関する問題が発生したためですが，無視してかまいません。

2.3 インストールの変更点

インストールに関する変更点は次のとおりです。

- 対称型マルチプロセシング (SMP) システムで TCP/IP のパフォーマンスを最適化するスケーラブル・カーネルは， TCP/IP Services の以前のリリースではオプションでした。本リリースでは，標準カーネルの代わりにスケーラブル・カーネルが使用されるようになりました。
- 次の各コンポーネントに関して， TCP/IP Services バージョン 5.4 では 2 つのイメージが提供されていました。 1 つは従来のイメージで，もう 1 つは，"_PERF"サフィックスが指定されている (たとえば， TCPIP$INTERNET_SERVICES_PERF.EXE など) 代替 SMP (Symmetric MultiProcessing) イメージです。
  - SYS$LOADABLE_IMAGES:TCPIP$BGDRIVER_PERF.EXE
  - SYS$LOADABLE_IMAGES:TCPIP$INTERNET_SERVICES_PERF.EXE
  - SYS$LOADABLE_IMAGES:TCPIP$TNDRIVER_PERF.EXE
  - SYS$SYSTEM:TCPIP$INETACP_PERF.EXE

  代替 SMP (Symmetric MultiProcessing) イメージを選択するのに，これまでは論理名 TCPIP$STARTUP_CPU_IMAGES が使用されていました。

  TCP/IP Services バージョン 5.5 では，代替 (_PERF) イメージが必要ありません。このため，論理名 TCPIP$STARTUP_CPU_IMAGES は無視されます。SYS$MANAGER:SYLOGICALS.COM コマンド・プロシージャやその他のコマンド・プロシージャからこの論理名の定義を削除することをお勧めします。

2.4 イメージ識別とリンク日付

TCP/IP Services で提供される実行イメージには通常， V5.5-xxaaという形式のイメージ識別が含まれています。ここで，xxは正の整数であり，aaはリビジョン・レベルを示す 0 文字以上の英字です。さらに，キットに含まれているイメージのリンク日付は通常，相互に数時間以内の範囲です。

しかし，最新の TCP/IP Services キットに含まれる複数のイメージは，このルールに従っていません。製品が正しくインストールされているかどうか確認するのに役立つように，ここではその例外について説明します。

次のイメージは， V5.5-xxaa PF という形式の識別を使用します。 "PF"は，イメージが改善されたリビジョンであることを示します。

- TCPIP$BGDRIVER.EXE
- TCPIP$INTERNET_SERVICES.EXE
- TCPIP$INETACP.EXE

これらのイメージのリンク日付は，相互に 1 時間前後の範囲内になっているはずです。

OpenVMS Alpha システムにインストールした場合，次のファイルは，識別およびリンク日付に関する上記のルールに従いません。

```
TCPIP$CFS_SHR         V5.5-6A        27-MAR-2004  SYS$COMMON:[SYSLIB]
TCPIP$NTPTRACE.EXE    V5.5           30-MAR-2004  SYS$COMMON:[SYSEXE]
TCPIP$TELNET_SERVER   V5.4/KRB V2.0   9-JUL-2003  SYS$COMMON:[SYSEXE]
```

OpenVMS I64 システムにインストールした場合，次のファイルは，識別およびリンク日付に関する上記のルールに従いません。

```
SYS$COMMON:[SYSLIB]TCPIP$CFS_SHR.EXE
"V1.0"
10-MAY-2003 13:12:22.14

SYS$COMMON:[SYSEXE]TCPIP$NTPTRACE.EXE
"V5.5"
30-MAR-2004 23:22:14.46

SYS$COMMON:[SYSEXE]TCPIP$TELNET_SERVER.EXE
"V5.4/KRB V2.0"
 5-DEC-2003 00:21:54.16
```

2.5 OpenVMS Cluster へのシステムの追加

TCP/IP Services バージョン 5.5 の TCPIP$CONFIG.COM コンフィギュレーション・プロシージャは，以前のバージョンより大きいシステム・パラメータ値を使用して， OpenVMS アカウントを作成します。新しいアカウントに対してだけ，これらの大きい値が割り当てられます。これらの値は OpenVMS Alpha システムでは便利ですが， OpenVMS I64 システムでは必須です。

OpenVMS I64 システムを TCP/IP ホストとして OpenVMS Cluster に追加するには， TCP/IP Services をコンフィギュレーションする前に，システムをクラスタに追加することをお勧めします。第 2.5.1 項に示したガイドラインでは，この順序でクラスタを追加することを前提にしています。

システムをクラスタに追加する前に， TCP/IP Services をコンフィギュレーションする場合は，第 2.5.2 項を参照してください。

2.5.1 新たにコンフィギュレーションされたホストをクラスタで実行する場合

次に示すガイドラインでは，システムを OpenVMS Cluster に追加した後，システムで TCP/IP Services をコンフィギュレーションすることを前提にしています。

TCP/IP Services がすでにクラスタにインストールされていて，システムで TCP/IP コンポーネントを実行するときに問題が発生した場合は，クラスタのシステム登録ファイル (SYSUAF) を変更して，影響を受けるコンポーネントが使用するアカウントのパラメータ値を大きくします。推奨される最小値は表 2–1 に示すとおりです。

表 2–1 SYSUAF パラメータの最小値

パラメータ	最小値
ASTLM	100
BIOLM	400
BYTLM	108000
DIOLM	50
ENQLM	100
FILLM	100
PGFLQUOTA[1]	50000
TQELM	50
WSEXTENT	4000
WSQUOTA	1024

[1] このパラメータ値の設定は特に重要です。

PGFLQUOTA や，上記の他のパラメータに割り当てた値が小さすぎる場合は， IMAP， DHCP，および XDM コンポーネントでアカウント・パラメータに関する問題が発生する可能性があります。 SYSUAF パラメータを変更するには， OpenVMS

AUTHORIZE ユーティリティを使用します。詳細については，『*HP OpenVMS System Management Utilities Reference Manual: A-L*』を参照してください。

2.5.2 システムをクラスタに追加する前に TCP/IP Services をコンフィギュレーションする場合

システムをクラスタに追加する前に TCP/IP Services をコンフィギュレーションする場合は，システムをクラスタに追加するときに，各 TCP/IP サービス SYS$LOGIN ディレクトリ (TCPIP$service-name，ただし，service-nameはサービスの名前) の UIC が不正になることがあります。これらの UIC を修正するには， OpenVMS AUTHORIZE ユーティリティを使用します。

2.6 TCPIP$CONFIG.COM の変更点

ここでは，本リリースでの TCPIP$CONFIG.COM コンフィギュレーション・プロシージャの変更点について説明します。

2.6.1 TCPIP$CONFIG.COM の警告メッセージ

IPv6 を有効にするために TCPIP$IP6_SETUP.COM コンフィギュレーション・プロシージャを実行した後， TCPIP$CONFIG.COM コンフィギュレーション・プロシージャを実行すると，Core environmentオプションを選択した際に ika の警告メッセージが表示されます。

```
                        WARNING

This node has been configured for IPv6.  If you make any additional
changes to the configuration of the interfaces, you must run
TCPIP$IP6_SETUP again and update your host name information in
BIND/DNS for the changes to take effect.
```

2.6.2 SSH サーバの無効化または有効化

TCPIP$CONFIG.COM コンフィギュレーション・プロシージャを使用して SSH サーバを無効化または有効化すると，次のプロンプトが表示されます。

```
* Create a new default Server host key? [YES]:
```

新しいデフォルト・サーバ・ホスト・キーを作成する特別な理由がない限り，このプロンプトに対しては「N」と入力してください。デフォルトを使用する場合，古いキーのクライアントは新しいキーを取得しなければならなくなります。詳細については，第 3.11.6 項を参照してください。

2.7 SSH コンフィギュレーション・ファイルはアップデートが必要

本バージョンの TCP/IP Services の SSH クライアントとサーバは，前のバージョンの SSH のコンフィギュレーション・ファイルを使用できません。

SSH クライアントとサーバが古いバージョンの SSH からシステム単位のコンフィギュレーション・ファイルを検出すると，クライアントおよびサーバは起動できません。クライアントは次の警告メッセージを表示し，サーバは次の警告メッセージを SSH_RUN.LOG ファイルに書き込みます。

```
You may have an old style configuration file. Please follow the
instructions in the release notes to use the new configuration
files.
```

SSH クライアントが古いバージョンの SSH からユーザ固有のコンフィギュレーション・ファイルを検出した場合は， SSH クライアントは警告を表示しますが，ユーザは操作を続行することができます。

SSH サーバのコンフィギュレーション・ファイルと SSH クライアントのコンフィギュレーション・ファイルに対して行った変更を保存するには，次に示すように，新バージョンの SSH で提供されるテンプレートを編集する必要があります。

1. 次のコマンドを使用して，テンプレート・ファイルを抽出します。

   ```
   $ LIBRARY/EXTRACT=SSH2_CONFIG SYS$LIBRARY:TCPIP$TEMPLATES.TLB -
   _$ /OUT=TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]SSH2_CONFIG.

   $ LIBRARY/EXTRACT=SSHD2_CONFIG SYS$LIBRARY:TCPIP$TEMPLATES.TLB -
   _$ /OUT=TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]SSHD2_CONFIG.
   ```

   これらのコマンドは，新しいテンプレート・ファイルを新しいバージョン番号で SSH2 コンフィギュレーション・ディレクトリにコピーします。

2. 古いバージョンのコンフィギュレーション・ファイルに対して行った変更を新しいバージョンにコピーします。

3. 次のコマンドを使用して， SSH を起動します。

   ```
   $ @SYS$STARTUP:SSH_STARTUP.COM
   $ @SYS$STARTUP:SSH_CLIENT_STARTUP.COM
   ```

2.8 SMTP と LPD のシャットダウンの問題のトラブルシューティング

SMTP または LPD のシャットダウンで，キュー・マネージャが実行されていないことを示すエラーが発生した場合には，サイト固有のシャットダウン・コマンド・プロシージャ (SYS$MANAGER:SYSHUTDWN.COM) をチェックしてください。このプロシージャがキュー・マネージャを停止するコマンド (STOP/QUEUE/MANAGER) を含んでいる場合には，このコマンドが TCPIP$SHUTDOWN.COM プロシージャの呼び出しの後に置かれていることを確認してください。

注意

キュー・マネージャを明示的に停止する必要はありません。キュー・マネージャは自動的に停止され，システムの再起動の際に自動的に起動されます。

3

制限事項と問題点

この章では，本バージョンの TCP/IP Services の問題点と制限事項について説明し，コマンド構文やメッセージの変更など，特定のコマンドやサービスに関する情報も示します。

3.1 OpenVMS I64 プラットフォームの制限事項

次の制限事項は， OpenVMS I64 プラットフォームにだけ適用されます。

- TCP/IP 管理コマンド SHOW VERSION/ALL の出力は， OpenVMS Alpha および VAX システムに表示される出力と異なります (情報は 1 列に表示され，イメージの名前と場所は一緒に表示されます)。
- 本リリースでは，次のコンポーネントは OpenVMS I64 プラットフォームで動作しません。
  - NFS サーバ
  - PPP

3.2 NFS サーバは I64 プラットフォームで動作しない

本リリースでは， NFS サーバは Alpha プラットフォームでは完全に機能しますが，I64 プラットフォームでは動作しません。この問題は， TCP/IP Services の今後のアップデートで修正される予定です。

I64 システムでは，将来のリリースで NFS サーバを提供できるようにするために，NFS 関連のコンポーネントがインストールされます。しかし，これらのコンポーネントは動作しません。これらのコンポーネントを起動しようとしても，起動できず，エラーになります。

NFS サーバを I64 システムでコンフィギュレーションすることはできますが，サーバを起動することはできません。サーバはただちに終了してしまいます。関連する TCP/IP 管理コマンドはエラーを返します。次の例を参照してください。

```
TCPIP> SHOW MAP
%LIB-E-KEYNOTFOU, key not found in tree
%TCPIP-E-CFSERROR, error processing TCPIP file system request
-TCPIP-E-NOCFS, error resolving TCPIP$CFS_SHR entry point
-LIB-F-KEYNOTFOU, key not found in tree
```

```
TCPIP> MAP "/x" DKA100:
%LIB-E-KEYNOTFOU, key not found in tree
%TCPIP-E-MAPERROR, error processing MAP or UNMAP request
-TCPIP-E-NOCFS, error resolving TCPIP$CFS_SHR entry point
-LIB-F-KEYNOTFOU, key not found in tree
```

NFS サーバに関連する他のエラーも発生することがあります。

Alpha プラットフォームでの NFS に関連する制限事項については，第 3.8 節を参照してください。

3.3 PPP の制限事項

本リリースの TCP/IP Services では， Alpha プラットフォームでも I64 プラットフォームでも， PPP (point-to-point protocol) は動作しません。この問題は， TCP/IP Services の今後のアップデートで修正される予定です。

PPP を使用しようとすると，次のエラーが発生することがあります。

```
$ PPPD CONN TTA08
%PPPD-I-CONNECTTERM, converting connection on device _TTA0: to a Point-to-Point connection

%LIB-E-ACTIMAGE, error activating image
DKA0:[SYS0.SYSCOMMON.][SYSLIB]TCPIP$PPPD_CALLOUT.EXE;1
-SYSTEM-F-PRIVINSTALL, shareable images must be installed to run privileged image

%PPPD-E-PROTOERR, error initiating network protocol callback routine

%SYSTEM-F-PRIVINSTALL, shareable images must be installed to run privileged image
%PPPD-F-ABORT, fatal error encountered; operation terminated.
```

イメージ TCPIP$PPPD_CALLOUT.EXE を手動でインストールした場合，この例に示したコマンドを実行すると，システムはエラーになります。イメージを手動でインストールするには特権が必要なため，これはセキュリティ上の問題ではありません。

3.4 SLIP の制限事項

本リリースの TCP/IP Services では， Alpha プラットフォームでも I64 プラットフォームでも， SLIP (serial line IP protocol) は動作しません。この問題は， Alpha プラットフォームでは TCP/IP Services の今後のアップデートで修正される予定です。

3.5 アドバンスト・プログラミング環境の制限事項とガイドライン

TCPIP$EXAMPLES 内に提供されているヘッダ・ファイルはアドバンスト TCP/IP プログラミング環境の一部として提供されています。以下に，これらを使用する場合の制限事項とガイドラインを示します。

- TCPIP$EXAMPLES:RESOLV.H に記載されている関数とデータ構造体の使用は 32-bit ポインタに限定されます。内部実装は 32-bit ポインタのみ処理します。以前は， 64-bit ポインタを不正に受け付けましたが，内部実装は不定な動きとなります。
- IP.H と IP6.H ヘッダ・ファイルは OpenVMS 環境では不完全です。これらは，本バージョンの TCP/IP Services が提供しないヘッダ・ファイルに対するinclude指示子を含みます。詳細は『*HP TCP/IP Services for OpenVMS Sockets API and System Services Programming*』を参照してください。

3.6 BIND/DNS の制限事項

DNSSEC を使用する場合， BIND バージョン 9 には次の制限事項があります。

- BIND サーバの特定のインプリメンテーションでは， AAAA (IPv6 アドレス) レコードがサポートされません。 BIND リゾルバで AAAA (IPv6) レコード・タイプを問い合わせると，これらのネーム・サーバは，同じドメイン名に対して A (IPv4) レコードが存在する場合でも， NXDOMAIN という状態を返します。これらのネーム・サーバは，このようなクエリに対して，本来なら状態として NOERROR を返さなければなりません。この問題により，ホスト名の解決で遅延が発生することがあります。

  本バージョンの TCP/IP Services でサポートされる BIND バージョン 9.2.1 では，この問題は発生しません。

- セキュア・ゾーンのサービス

  信頼されるネーム・サーバとして動作しているときに，クエリに DO フラグが設定されている場合， BIND バージョン 9 では， RFC 2535 の指定に従って，応答に KEY， SIG，および NXT レコードが含まれます。

  セキュア・ゾーン内でのワイルドカード・レコードに対する応答の生成は，完全にはサポートされていません。名前が存在しないことを示す応答には，名前自体が存在しないことを示す NXT レコードが含まれますが，対応するワイルドカード・レコードが存在しないことを示す NXT レコードは含まれません。ワイルドカードの展開から得られる肯定応答には，非ワイルドカード一致や，より特定のワイルドカード一致が存在しないことを示す NXT レコードは含まれません。

- セキュア・リゾリューション

  応答の DNSSEC 署名の検証に対する基本サポートは，インプリメントされていますが，まだ実験的な段階であると考えてください。

  キャッシング・ネーム・サーバとして動作する場合， BIND バージョン 9 は，不在応答だけでなく，肯定応答の基本的な DNSSEC 検証を実行することができます。この機能は， DNSSEC 階層構造の最上位レベルのゾーン・キーを含むtrusted-keysをコンフィギュレーション・ファイルに指定することで有効になります。

現在，ワイルドカード応答の検証はサポートされていません。特に，一致するワイルドカードが存在しないことを示すNXTレコードがサーバに含まれていない場合でも，“name does not exist”応答は正しいと検証されます。

セキュア・ゾーンから委任された非セキュア・ゾーンの非セキュア状態の検証は，ゾーンが完全に非セキュアである場合は機能します。セキュア・ゾーンから委任されたプライベート・セキュア・ゾーンは，どの場合も機能しません。たとえば，プライベート・セキュア・ゾーンが祖先(親を除く)ゾーンと同じサーバのサービスを受けている場合などは，正常に機能しません。

クエリのCDビットの取り扱いは完全にインプリメントされました。CDが設定されている場合，再帰的クエリに対して検証は行われません。

- セキュアな動的アップデート

  セキュア・ゾーンの動的アップデートは部分的にインプリメントされています。アップデートが行われるときに，影響を受けるNXTおよびSIGレコードは，サーバによってアップデートされます。高度なアクセス制御を行うには，ゾーン定義にupdate-policy文を指定します。

- セキュアなゾーン転送

  BINDバージョン9では，RFC 2535のゾーン転送セキュリティ機能がインプリメントされていません。これは，ゾーン転送の整合性を維持するのに，これらの機能を使用するより，TSIGやSIG(0)を使用する方が有利であると考えられているからです。

3.7 IPv6の制限事項

ここでは，IPv6を使用する際の制限事項について説明します。

3.7.1 モバイルIPv6の制限事項

本バージョンのTCP/IP Servicesでインプリメントされているモバイル IPv6では，draft-ietf-mobileip-ipv6-15.TXTのセクション4.4に指定されているバインディング・アップデート認証はサポートされません(セクション5.6に定義されている認証データ・サブオプションもサポートされません)。未認証のバインディングを受け付けると，システムの整合性が損なわれる可能性があるため，本バージョンは，攻撃される可能性のないテスト環境でのみ使用するように制限してください。

3.7.2 6to4のコンフィギュレーションはサポートされない

TCP/IP Servicesには，ノードでIPv6のコンフィギュレーションを行うために，TCPIP$IP6_SETUP.COMコマンド・プロシージャが付属しています。本リリースでは，このプロシージャを使用して6to4トンネルをコンフィギュレーションする機能

はサポートされません。このプロシージャを使用して 6to4 トンネルをコンフィギュレーションしようとしても，その操作は失敗します。

3.7.3 IPv6 では BIND リゾルバが必要

IPv6 を使用している場合には， BIND リゾルバを有効にする必要があります。BIND リゾルバを有効にするには， TCPIP$CONFIG.COM コマンド・プロシージャを使用します。「Core」メニューから「BIND Resolver」を選択してください。

BIND リゾルバを有効にするには， BIND サーバを指定する必要があります。 BIND サーバにアクセスできない場合は， BIND サーバとしてノード・アドレス 127.0.0.0 を指定します。

3.8 Alpha プラットフォームでの NFS の問題点と制限事項

ここでは， NFS の問題点と制限事項について説明します。

3.8.1 NFS サーバの問題点と制限事項

- Solaris バージョン 9 クライアントからlsコマンドを使用すると， OpenVMS サーバはハングすることがあり，そのとき，クライアントでもサーバでもエラー・メッセージは出力されません。この問題を回避するには， nfs サブシステム属性ovms_xqp_plus_enabledを 7 に設定します。この属性についての詳細は，『*HP TCP/IP Services for OpenVMS Management*』を参照してください。
- コンテナ・ファイル・システム内のディレクトリは， TCP/IP 管理コマンド REMOVE DIRECTORY を使用して削除することができず，クライアントが削除することもできません。このような操作を実行すると，次のエラー・メッセージが表示されます。

  ```
  no such file
  ```

- TCP/IP Services バージョン 5.3 で， ODS-5 ボリュームに対して， TYPELESS_DIRECTORIES エクスポート・オプションを指定して NFS クライアント・コマンド“mkdir dirname.dir”を使用すると， OpenVMS のディレクトリ名“dirname.DIR;1”を持つディレクトリが作成されます。この名前が NFS クライアントに表示されるときは，単に“dirname”として表示されます。

  この問題は TCP/IP Services バージョン 5.4 で修正されています。作成されるディレクトリの名前は， OpenVMS ファイル指定“dirname.dir.DIR;1”になります。この名前がクライアントに表示されるときは，“dirname.dir”として表示されます。

したがって，ODS-5 ボリュームを使用している OpenVMS 以外のクライアントは常に，TYPELESS_DIRECTORIES オプションが使用されているかどうかに応じて，ディレクトリを参照する必要があります。

- TYPELESS_DIRECTORIES オプションを使用している場合は，ファイル“dirname.DIR;1”は“dirname”として参照しなければなりません。
- TYPELESS_DIRECTORIES オプションを使用していない場合は，ファイル“dirname.DIR;1”は“dirname.dir”として参照しなければなりません。

一部のエクスポート・レコードは，各ディレクトリ・レベルに“.dir”を含むように変更するか，または TYPELESS_DIRECTORIES オプションを追加する必要があります。

クライアントの MOUNT コマンドもこの規則に従う必要があります。

- OPCOM を有効にして，マウント操作を実行したり，NFS サーバを起動したりする場合は，TCP/IP Services MOUNT サーバは誤って次のメッセージを表示することがあります。

```
%TCPIP-E-NFS_BFSCAL, operation MOUNT_POINT failed on file /dev/dir
```

このメッセージは，MOUNT や NFS の起動が正常に行われた場合でも表示されます。マウント操作の場合，操作が実際に正常終了しているときは，次のメッセージも表示されます。

```
%TCPIP-S-NFS_MNTSUC, mounted file system /dev/dir
```

- NFS サーバと NFS クライアントが異なるドメインに存在し，要求で修飾されないホスト名が使用されている場合は，ロック・サーバ (LOCKD) は要求を処理することができず，ファイルはロックされません。

  サーバが，完全修飾ホスト名 (たとえば，johnws.abc com) ではなく，修飾されないホスト名 (たとえば，johnws) を使用してホストを検索しようとしたときに，ホストがサーバと同じドメインに存在しない場合には，要求は失敗します。

  この種の問題を解決するには，次のいずれかの操作を実行します。

  - NFS クライアントのコンフィギュレーションを行うときに，ドメイン名も含む完全修飾ホスト名を指定します。このようにすると，変換は正しく行われます。
  - NFS サーバのホスト・データベースに，クライアントの修飾されていないホスト名のエントリを追加します。このホスト名を変換できるのは，その NFS サーバだけです。クライアントが DHCP から動的にアドレスを取得する場合は，この対処法は機能しません。

3.8.2 NFS クライアントの問題点と制限事項

- DST (Daylight Savings Time) のためにシステム時間が変更されたとき，正しいタイムスタンプにするには，すべての DNFS デバイスをディスマウントします (TCP/IP管理コマンド SHOW MOUNT でマウント済みのデバイスがゼロと表示されるはずです)。その後，デバイスを再マウントします。
- NFS クライアントは， ODS-5 ディスク・ボリューム上のセミコロンの付いたファイル名を適切に処理すべきです (たとえば，a^;b.dat;5は有効なファイル名です)。

  しかし，現在のバージョンでは，これらのタイプのファイル名は適切に処理されず，セミコロンで切り捨てられます。
- TCP/IP Services に含まれている NFS クライアントは， NFS Version 2 プロトコルだけを使用します。
- NFS Version 2 プロトコルでは，ファイル・サイズの値は 32 ビットに制限されています。
- ISO Latin-1 文字セットがサポートされています。 UCS-2 文字はサポートされていません。
- ファイル名は，ファイル拡張子を含めて， 236 文字以下でなければなりません。
- OpenVMS のアクティブなバージョン上の ODS-5 によって受け付けられない文字を含むファイル，またはファイル名と拡張子が 236 文字を超えているファイルは，長さが 0 に切り捨てられます。これにより，これらのファイルは OpenVMS から見えなくなり，以前の OpenVMS NFS クライアントの動作と一致します。

3.9 NTP の問題と制限事項

NTP サーバの階層の上限は 15 です。サーバは， 15 以上の階層を報告するタイム・サーバとは同期をとりません。このため，(local-masterコマンドで)「自由実行」として指定されている UCX NTP サーバを実行しているサーバとの同期を試みると，問題が生じることがあります。正常に実行させるためには，local-master指定を 14 以下の階層で指定する必要があります。

3.10 SNMP の問題点

本節では，本リリースの SNMP 構成要素の制限事項を説明します。 SNMP の使用についての詳細は，『*HP TCP/IP Services for OpenVMS SNMP Programming and Reference*』を参照してください。

3.10.1 不完全な再起動

SNMP マスタおよびサブエージェントに障害が発生したか停止した場合，日本語 TCP/IP Services は一般にすべてのプロセスを自動的に再起動することができます。しかし，特定の条件下では，サブエージェント・プロセスが再起動しないことがあります。つまり， DCL コマンド SHOW SYSTEM 表示に， TCPIP$OS_MIBS および TCPIP$HR_MIB が含まれなくなります。これが起こった場合は，以下のコマンドを発行して SNMP を再起動します。

```
$ @SYS$STARTUP:TCPIP$SNMP_SHUTDOWN.COM
$ @SYS$STARTUP:TCPIP$SNMP_STARTUP.COM
```

3.10.2 SNMP IVP エラー

低速システムでは， SNMP のインストレーション検証プロシージャ (IVP) は，サブエージェントがテスト問い合わせに応答しなかったために失敗することがあります。次のようなエラー・メッセージが表示されます。

```
   .
   .
   .
Shutting down the SNMP service... done.

Creating temporary read/write community SNMPIVP_153.
Enabling SET operations.
Starting the SNMP service... done.
SNMPIVP: unexpected text in response to SNMP request:
"- no such name - returned for variable 1"
See file SYS$SYSDEVICE:[TCPIP$SNMP]TCPIP$SNMP_REQUEST.DAT for more
details.
sysContact could not be retrieved.  Status = 0
The SNMP IVP has NOT completed successfully.
SNMP IVP request completed.
Press Return to continue ...
```

IVP のこれらのタイプのメッセージは無視してもかまいません。

3.10.3 既存の MIB サブエージェント・モジュールの使用

既存のサブエージェントが正しく実行されなかった場合には，現在のバージョンの TCP/IP Services に再リンクして，正常に動作するイメージを作成しなければならないことがあります。また，一部のサブエージェント (Compaq Insight Manager の OpenVMS サポートなど) も最低限のバージョンの OpenVMS と最低限のバージョンの TCP/IP Services を必要とします。

次に示す一般的な制限事項が適用されます。

- 一般に，以下のバージョンの eSNMP 共用可能イメージにリンクされた実行可能イメージのみが現在のバージョンの TCP/IP Services との上位互換性を維持しています。
  - TCP/IP Services バージョン 4.2 ECO 4 の UCX$ESNMP_SHR.EXE
  - TCP/IP Services バージョン 5.0A ECO 1 の TCPIP$ESNMP_SHR.EXE

  これ以外のバージョンで構築されたイメージは，いずれかの共用イメージ，または現在のバージョンの日本語 TCP/IP Services の TCPIP$ESNMP_SHR.EXE と再リンクすることができます。
- 下位の eSNMP API は， V5.0 の DPI から現在のバージョンの TCP/IP Services の AgentX に変更されています。このため， API の古いオブジェクト・ライブラリ・バージョン (*$ESNMP.OLB) にリンクされた実行可能イメージは，新しいオブジェクト・ライブラリまたは新しい共用可能イメージのどちらかに再リンクする必要があります。共用可能イメージにリンクすると，将来の上位互換性が保証され，イメージ・サイズも小さくなります。

注意

イメージを再リンクしなくても動作することがありますが，下位互換性は保証されていません。このようなイメージでは，不正確なデータが生成されたり，実行時に問題が生じたりする可能性があります。

- 本バージョンの TCP/IP Services では， TCP/IP Services バージョン 4.2 ECO 4 でリンクされたサブエージェントとの互換性を維持するために， UCX$ESNMP_SHR.EXE 共用可能イメージのアップデート・バージョンが提供されます。このファイルは削除しないでください。
- SNMP サーバは，クラスタ・エイリアスに送られた SNMP 要求に正しく応答します。しかし，クラスタ・グループのメンバであるが，現在のインパーソネータではない TCP/IP Services バージョン 4.xシステムからの問い合わせは，目的のホスト以外に届けられることがあります。
- DNS クエリで使用したときに，論理名 TCPIP$INET_HOST の値がホストの機能インタフェースの IP アドレスを生成しない場合は， SNMP マスタ・エージェントおよびサブエージェントは起動しません。サーバ・ホストが常時ネットワーク接続 (たとえば，イーサネットや FDDI) で正しくコンフィギュレーションされている場合は，この問題は発生しません。ホストが PPP を介して接続されていて，PPP 接続で使用される IP アドレスが論理名 TCPIP$INET_HOST の IP アドレスと一致しない場合には，この問題が発生することがあります。
- 主に OpenVMS VAX システムで監視されている特定の状況では，内部の`select()`ソケット呼び出しからのエラーで，マスタ・エージェントまたはサブエージェントが終了します。ほとんどの場合，ループは発生しません。ループが発生する場合は，論理名TCPIP$SNMP_SELECT_ERROR_LIMITを定義することで，繰り返しの回数を制御できます。

- TCP/IP Services (TCPIP$SNMP_REQUEST.EXE) で提供される MIB ブラウザでは，コンポーネントとして 32 ビットの OpenVMS プロセス ID を含む OID をgetnextで処理する機能がサポートされています。しかし，他の MIB ブラウザでは，この機能はサポートされません。

  たとえば，次の OID および値は OpenVMS でサポートされます。

```
1.3.6.1.2.1.25.4.2.1.1.1321206828 = 1321206828
1.3.6.1.2.1.25.4.2.1.1.1321206829 = 1321206829
1.3.6.1.2.1.25.4.2.1.1.1321206830 = 1321206830
```

  これらの例はhrSWRunTableからの抜粋です。hrSWRunPerfTableも影響を受けることがあります。

- Get，GetNext，GetBulk要求のいずれかに対する応答として，ヌルの OID 値 (0.0) が取得された場合，ログ・ファイルに次の警告メッセージが記録されていても，無視してかまいません。

```
o_oid; Null oid or oid->elements, or oid->nelem == 0
```

3.10.4 SNMP のアップグレード

現在のバージョンの TCP/IP Services にアップグレードした後には，TCPIP$CONFIG コンフィギュレーション・コマンド・プロシージャを使って SNMP を無効にし，再び有効にする必要があります。“this node”と“all nodes”のどちらかを指定するように求められた場合には，以前のコンフィギュレーションを反映するオプションを選択します。

3.10.5 通信コントローラ・データが完全に更新されない

日本語 TCP/IP Services をアップグレードした後に，既存の通信コントローラを変更すると，通信コントローラを使用するプログラムは更新された情報にアクセスできない場合があります。

MIB ブラウザ (SNMP_REQUEST) などのプログラムが通信コントローラに関する新しいデータにアクセスできるようにするには，以下の操作を行います。

1. TCP/IP 管理コマンド DELETE COMMUNICATION_CONTROLLER を使って通信コントローラを削除します。
2. TCPIP$CONFIG.COM コマンド・プロシージャを実行し，終了することによって，通信コントローラを再設定します。
3. 次のコマンドを入力して，プログラム (SNMP など) を再起動します。

```
$ @SYS$STARTUP:SNMP_SHUTDOWN.COM
$ @SYS$STARTUP:SNMP_STARTUP.COM
```

4. TCP/IP 管理コマンド LIST COMMUNICATION_CONTROLLER を使って，情報を表示します。

3.10.6 SNMP MIB ブラウザの使用方法

-l (ループ・モード) または-t (ツリー・モード) フラグを使用した場合には，-m (最大繰り返し回数) フラグや-n (非反復) フラグを同時に指定することはできません。後者のフラグは，ループ・モードとツリー・モードのどちらとも互換性を持っていません。

-nおよび-mフラグの使い方を間違えると，次のようなメッセージが表示されます。

```
$ snmp_request mynode.co.com public getbulk -v2c -n 20 -m 10 -t 1.3.6.1.2.1
Warning: -n reset to 0 since -l or -t flag is specified.
Warning: -m reset to 1 since -l or -t flag is specified.
1.3.6.1.2.1.1.1.0 = mynode.company.com
```

3.10.7 重複するサブエージェント識別子

本バージョンの日本語 TCP/IP Services では， 2 つのサブエージェントが同じ識別子パラメータを持つことができます。ただし，同じ名前のサブエージェントが 2 つあると，ログ・ファイルに報告される問題の原因を判断するのが難しくなることに注意してください。

3.10.8 コミュニティ名の制限事項

TCPIP$CONFIG.COM では，以下に示すコミュニティ名に関する制約事項があります。

- スペース文字を含むコミュニティ名を指定しないでください。
- コミュニティ名の一部として指定された引用符 (") は正しく処理されません。SHOW CONFIGURATION SNMP コマンドを使って名前の正当性を確認してください。

3.10.9 eSNMP プログラミングとサブエージェントの開発

以下に， eSNMP プログラミングとサブエージェントの開発に関する注意事項を示します。

- マニュアルで使われている**拡張サブエージェント**，**カスタム・サブエージェント**，および**ユーザ作成サブエージェント**という言葉は， TCP/IP Services 製品に付属している MIB-II および Host Resources MIB 用の標準サブエージェント以外のすべてのサブエージェントを指します。

- TCPIP$EXAMPLES の[.SNMP]サブディレクトリにある.C，.H，.COM，.MY，および.AWK 拡張子を持つファイルにもコメントとドキュメントが含まれています。
- TCPIP$SNMP_REQUEST.EXE， TCPIP$SNMP_TRAPSND.EXE，および TCPIP$SNMP_TRAPSND.EXE プログラムは，拡張サブエージェントの開発の際のテストに役立ちます。
- eSNMP API のルーチンのプロトタイプと定義については， TCPIP$SNMP: ESNMP.H ファイルを参照してください。

3.11 SSH の問題点と制限事項

ここでは，次の情報について説明します。

- SSH 関連のセキュリティに関する勧告 (第 3.11.1 項)
- SSH に関する全般的な注意事項と制限事項 (第 3.11.2 項)
- SSH でサポートされない UNIX の機能 (第 3.11.3 項)
- SSH コマンド構文に関する注意事項と制限事項 (第 3.11.4 項)
- SSH 認証に関する注意事項と制限事項 (第 3.11.5 項)
- SSH キーに関する注意事項と制限事項 (第 3.11.6 項)
- SSH セッションの制限事項 (第 3.11.7 項)
- SSH メッセージに関する注意事項と制限事項 (第 3.11.8 項)
- SSH リモート・コマンドに関する注意事項と制限事項 (第 3.11.9 項)
- SSH バッチ・モードの制限事項 (第 3.11.10 項)
- X11 ポート転送の制限事項 (第 3.11.11 項)
- ファイル転送の制限事項 (すべてのファイル・サイズ) (第 3.11.12 項)
- ファイル転送の制限事項 (大きいファイル) (第 3.11.13 項)

注意

SSH， SCP， SFTP コマンドに関する情報は， SSH2， SCP2， SFTP2 コマンドにもそれぞれ適用されます。

3.11.1 SSH 関連のセキュリティに関する勧告

CERT® (Computer Emergency Readiness Team) 勧告は，カーネギー・メロン大学が連邦政府の予算で運営している研究開発センター Software Engineering Institute においてインターネット・セキュリティを専門に研究している CERT/CC (CERT Coordination Center) が発行している勧告です。 CERT 勧告は， US-CERT (United

States Computer Emergency Readiness Team) が発行する「Technical Cyber Security Alerts」というドキュメントの中心的なコンポーネントであり，セキュリティ関連の問題点，脆弱性，弱点などに関する最新情報をタイムリーに提供します。

CERT および HP SSRT (Software Security Response Team) の SSH に関するアクティビティによってセキュリティに関する勧告が出される場合があります。 CERT 勧告は次の CERT/CC Web サイトに掲載されています。

`http://www.cert.org/advisories.`

表 3–1 は SSH 関連の複数の勧告の要約を示しています。

表 3–1 CERT/SSRT ネットワーク・セキュリティ勧告

勧告	OpenVMS に与える影響
CERT CA-2003-24	OpenSSH のみ。 OpenVMS は脆弱ではありません。
CERT CA-2002-36	この脆弱性による最悪の結果は，次のいずれかの単一接続に対して，サービスが拒否されること (DoS) です。 • 悪意のあるクライアントからの接続を取り扱うサーバ・プロセス • 悪意のあるサーバに接続するクライアント・プロセス いずれの場合も，悪意のあるリモート・ホストは OpenVMS ホストにアクセスすることができず (たとえば，任意のコードを実行するために)，その一方で OpenVMS サーバは新しい接続を受け付けることができます。
CERT-2001-35	OpenVMS は脆弱ではありません。 SSH バージョン 1 にだけ影響しますが，このバージョンはサポートされません。
CERT CA-1999-15	RSAREF2 ライブラリは使用されません。このため，OpenVMS は脆弱ではありません。
SSRT3629A/B	OpenVMS は脆弱ではありません。

3.11.2 SSH に関する全般的な注意事項と制限事項

ここでは，特定の SSH アプリケーションに限定されない，全般的な注意事項と制限事項について説明します。

- UNIX パス/etcは， OpenVMS SSH サーバで TCPIP$SSH_DEVICE:[TCPIP$SSH]として解釈されます。
- 次のイメージは本リリースでは提供されません。
  - TCPIP$SSH_SSH-CERTENROLL2.EXE

    このイメージは，証明書登録 (certificate enrollment) 機能を提供します。
  - TCPIP$SSH_SSH-DUMMY-SHELL.EXE

    このイメージは，ファイル転送機能だけが許可されているシステムへのアクセスを可能にします。

– TCPIP$SSH_SSH-PROBE2.EXE

このイメージは，ssh-probe2コマンドを提供します。このコマンドは，クエリ・パケットを UDP データグラムとしてサーバに送信し，クエリに応答したサーバのアドレスと SSH バージョン番号を表示します。

3.11.3 SSH でサポートされない UNIX の機能

ここでは， UNIX 環境で提供されている機能のうち， SSH for OpenVMS でサポートされない機能について説明します。

- サーバ・コンフィギュレーション・パラメータPermitRootLoginはサポートされません。
- クライアント・コンフィギュレーション・パラメータEnforceSecureRutilsはサポートされません。
- UNIX ROOT アカウントから OpenVMS SYSTEM アカウントへの自動マッピングは行われません。
- SSH1 プロトコル・スイートは，端末セッション，リモート・コマンド実行，およびファイル転送操作に対してサポートされません。サーバ・コンフィギュレーション・ファイルとクライアント・コンフィギュレーション・ファイルで，SSH1 に関連するパラメータは無視されます。

3.11.4 SSH コマンド構文

ここでは，コマンド構文に関連する注意事項と制限事項について説明します。

- OpenVMS クライアント以外から，名前 (たとえばデバイス名) に対して OpenVMS の構文を使用する場合は，名前を単一引用符で囲むことで，特定の文字が UNIX システムのルールに従って解釈されないようにする必要があります。

  たとえば，次のコマンドでは， UNIX はデバイス名 SYS$SYSDEVICE:[user]のドル記号 ($) を区切り文字として解釈するので，デバイス名は SYS:[user]になります。

  ```
  # ssh user@vmssystem directory SYS$SYSDEVICE:[user]
  ```

  この問題を回避するには，次の形式でコマンドを入力します。

  ```
  # ssh user@vmssystem directory 'SYS$SYSDEVICE:[user]'
  ```

3.11.5 SSH 認証

ここでは，SSH 認証に関する注意事項と制限事項について説明します。

- 本バージョンの SSH は Kerberos ベースの認証をサポートしません。
- SHOSTS.EQUIV ファイルの置き場所がTCPIP$SSH_DEVICE:[TCPIP$SSH]からTCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]へ変更されました。
- ホストベースの認証が機能しない場合には，SSH サーバが，クライアントから送信されたホスト名と，DNS から検出したホスト名の対応付けに失敗した可能性があります。この問題が発生したかどうかは，次のコマンドの出力を比較することで確認できます (出力される文字列で，大文字と小文字の違いは無視してください)。
  - サーバ・ホスト:

    ```
    $ TCPIP
    TCPIP> SHOW HOST client-ip-address
    ```

  - クライアント・ホスト:

    ```
    $ write sys$output -
    $_ "''f$trnlnm("TCPIP$INET_HOST")'.''f$trnlnm("TCPIP$INET_DOMAIN")'"
    ```

    2 つの文字列が一致しない場合は，クライアント・ホストでホスト名およびドメインのコンフィギュレーションをチェックしてください。クライアント・ホストで，TCP/IP Services を再コンフィギュレーションし，再起動しなければならない可能性があります。
- SYSUAF ユーザ・レコードのユーザ・デフォルト・ディレクトリが大かっこ (例: [user-name]) ではなく，不等号 (例: <user-name>) と共に指定された場合，ホスト鍵認証が失敗します。これを回避するためには，ユーザ・レコードで大かっこ ([]) を使うように変更してください。
- AUTHORIZE ユーティリティの SHOW /IDENTIFIER コマンドにより表示される OpenVMS rights database のユーザ名と UIC の組は，SYSUAF レコード内の当該ユーザ名の組と一致する必要があります。一致しない場合，ユーザが SSH セッションを確立する際に以下のエラー・メッセージが表示されます。

  ```
  Received signal 10, SIGBUS: invalid access to memory objects.
  ```

  これを回避するためには，AUTHORIZE ユーティリティを使って OpenVMS rights database 内のユーザ名と UIC の組を訂正してください。

3.11.6 SSH 鍵

ここでは，SSH 鍵に関する注意事項と制限事項について説明します。

- SSH クライアントは，独自にカスタマイズした SSH2_CONFIG. ファイルをコピーし，変数StrictHostKeyCheckingの値を変更することができます。この変数の値を“no,”に設定すると，ユーザはクライアントに SSH サーバに最初に交信した時にそのサーバから自動的に (確認せずに) 公開鍵をコピーさせることができます。

  システム管理者は，システム・ワイドな SSH2_CONFIG. ファイルの変数StrictHostKeyCheckingを“yes”に設定し，ユーザにこのシステム・ワイドのファイルのみを参照させることによりセキュリティを強化することができます。この場合，ユーザ (およびシステム・マネージャ) は，サーバから公開鍵をコピーするために別の機構 (例えば特権を持ったユーザは公開鍵を手動でコピーすることができます) を使う必要があります。このセキュリティの強化を行うために，システム管理者は以下のことを行ってください。

  1. TCPIP$SSH_DEVICE:[TCPIP$SSH]SSH2_CONFIG. を編集して，次の行を追加します。

     ```
     StrictHostKeyChecking  yes
     ```

  2. TCPIP$SSH_DEVICE:[TCPIP$SSH]SSH2_CONFIG. へのユーザのアクセスを制限します。次の例を参照してください。

```
$ SET SECURITY/PROTECTION=(G,W) TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]SSH2_CONFIG.;
```

  3. SYS$STARTUP:TCPIP$SSH_CLIENT_STARTUP.COM コマンド・プロシージャを編集して，スタートアップ時に READALL 特権を使用して， SSH サーバ・イメージをインストールするようにします。次の例に示すように，既存の行 (existing line) を置き換えの行 (replacement) に変更します。

     ```
      . . .
     $     image = f$edit("sys$system:tcpip$ssh_ssh2.exe","upcase")
     $!    call install_image 'image' ""          <== existing line
     $     call install_image 'image' "readall"   <== replacement
      . . .
     ```

  4. 『*HP TCP/IP Services for OpenVMS Guide to SSH*』の説明に従って，SSH クライアントを有効にします。

注意

ステップ 2 と 3 はシステム・ファイルの修正が必要になります。このため，将来の TCP/IP Services のバージョンアップ時には同じ修正を繰り返すことになる場合があります。

- SSH_ADD コマンドにキー・ファイルを指定しておらず， SSH_ADD が INDENTIFICATION. ファイルを見つけることができなかった場合，検索された最初のプライベート・キーだけが[username.SSH2]ディレクトリに追加されます。

- SSH_KEYGEN -eオプションは使用しないでください(鍵のコメントあるいはパスフレーズを編集するために使用)。このオプションは機能しません。
- 本リリースでは，SSH_KEYGEN ユーティリティにより生成される鍵の省略時のサイズは 2048 ビットです(初期のリリースでは，省略時のサイズは 1024 ビットでした)。このため，鍵の生成には時間がかかります。場合によっては 5 から 10 分かかります。低速なシステム，あるいは SSH コンフィギュレーション時には，鍵の生成が実際にはハングしていないにもかかわらず，ハングしているように見える場合があります。進捗度が表示されません。SSH コンフィギュレーション時には，以下のメッセージが鍵の生成中であることを示します。

```
Creating private key file: TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]HOSTKEY
Creating public key file: TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]HOSTKEY.PUB
```

3.11.7 SSH セッション

ここでは，SSH セッションに関連する制限事項について説明します。

- OpenVMS サーバの SSH セッションでは，発信側のクライアント・ホスト名と，ユーザ名またはポート識別子が表示されません。たとえば，TELNET セッションでは，OpenVMS DCL コマンド SHOW TERMINAL は UNIX クライアントに関して次の情報を表示します。

```
Remote Port Info: Host: unixsys.myco.com Port:2728
```

同様に，OpenVMS クライアントに関する情報は次のように表示されます。

```
Remote Port Info: Host: mysys.com Locn:_RTA4:/USER
```

同様の SSH セッションでは，上記のような情報は表示されません。

- SSH セッションを再帰的に起動すると (たとえば，既存の SSH セッションの内部から別の SSH セッションを起動するなど)，セッションのレイヤが作成されます。最も内側のレイヤからログアウトすると，そのセッションを起動したレイヤ以外のレイヤに戻る可能性があります。
- OpenVMS サーバで SSH 端末セッションからカット&ペーストを行うと，データが途中で切り捨てられることがあります。この場合は，次のエラー・メッセージが表示されます。

```
-SYSTEM-W-DATAOVERUN, data overrun
```

- たとえば，次のコマンドを実行することで，SSH セッションから OpenVMS システムをシャットダウンすることはできません。

```
$ @SYS$SYSTEM:SHUTDOWN.COM
```

シャットダウンの中のユーザ・プロセスを停止するフェーズで，SSH セッションが切断されます。

- SSH エスケープ・シーケンスは完全にはサポートされません。たとえば，Escape . (エスケープ文字の後にスペースとピリオド) 終了シーケンスは， 2 回入力しないと動作しないことがあります。終了時に，端末は NOECHO および PASTHRU モードのままになります。
- OpenVMS 以外の特定のクライアントで， SFTP セッションを終了しようとした後，オペレーティング・システム・プロンプトに戻るには， Enter キーを 2 回押す必要があります。

3.11.8 SSH メッセージ

ここでは， SSH セッション・メッセージに関する制限事項について説明します。

- システム論理名 SYS$ANNOUNCE の変換は，認証完了後に表示されます。本バージョンの SSH には，このテキストをプリログイン・バナーとして表示するための自動機能はありません。

  テキスト・ファイルからプリログイン・バナーを提供するには，ログイン前に表示されるテキストを格納したファイル SSH_BANNER_MESSAGE. を作成します。

  複数行のバナー・テキストを入力するには，最後の行以外の各行の末尾にキャッリジ・リターン文字を入力します。

  バナー・メッセージ・ファイルはTCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]ディレクトリに保存し，ユーザ・アカウント[TCPIP$SSH]からの読み込みを許可する特権を与えます。

  バナー・メッセージ・ファイルに対して，省略時のファイル名および保存場所を使用しない場合は， TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]SSHD2_CONFIG. ファイルでBannerMessageFileオプションを使用して定義します。バナー・メッセージ・ファイルの場所とファイル名は，次のいずれかの形式を使用して，オプションの引数として指定します。

  ```
  BannerMessageFile   TCPIP$SSH_DEVICE:[TCPIP$SSH]BANNER1.TXT
  BannerMessageFile   /TCPIP$SSH_DEVICE/TCPIP$SSH/BANNER2.TXT
  BannerMessageFile   /etc/banner3.txt
  ```

  引数は， OpenVMS 形式でも UNIX 形式でもかまいません。引数では，大文字と小文字は区別されません。コンフィギュレーション・ファイルに同じオプションの定義が 2 つ以上登録されている場合は，最後に登録されている定義が有効になります。

- 一部の SSH 情報メッセージ・コード， SSH 警告メッセージ・コード， SSH エラー・メッセージ・コードの表示は，途中で切り捨てられます。次の例を参照してください。

  ```
  %TCPIP-E-SSH_FC_ERR_NO_S, file doesn't exist
  ```

- 一部の SSH ログおよびトレース出力メッセージ，情報メッセージ，警告メッセージ，およびエラー・メッセージでは，ファイル指定が UNIX パス名として表示されます。
- 特定のエラー条件のもと，あるいは SSH セッションを終了する際， SSH は (UNIX システムで表示されるような) シグナル情報を表示します。例えば，Ctrl/C を押すと，以下のメッセージが表示されます。

```
Received signal 2, SIGINT: Interactive attention signal.
```

このメッセージは無視してください。

- 次の例に示すように，ログアウト時に，ホストtst1で確立された SSH セッションから， "Connection to hostname closed."というメッセージがログアウト・メッセージの最後の行に上書きされることがあります。

```
$ LOGOUT
Connection to tst1 closed.at  7-AUG-2003 14:37:15.01
```

3.11.9 SSH リモート・コマンド

ここでは， SSH リモート・コマンドに関する制限事項について説明します。

- SSH 経由のリモート・コマンド実行用のコマンド・ラインは最大 153 文字です。
- SSH リモート・コマンドを実行した後， DCL プロンプトに戻るために，Return キーを押さなければならないことがあります。
- OpenVMS SSH サーバでリモート・コマンドを実行すると，ユーザ・アカウントの論理名 SYS$LOGIN によって定義されるディレクトリに，ログ・ファイル TCPIP$SSH_RCMD.LOG が作成されます。このログ・ファイルは，手動でパージする必要があります。
- OpenVMS SSH サーバ以外のサーバに接続されている OpenVMS SSH クライアントでリモート・コマンドを実行すると，次の問題が発生することがあります。
- 出力が正しく表示されないことがあります。たとえば，次の例に示すように，改行がないと，一連の行がずれて表示されることがあります。

```
$ ssh user@unixhost ls -a
  user's password:
  Authentication successful.
  .
   ..
     .TTauthority
                 .Xauthority
                            .cshrc
                                  .dt
                                     .dtprofile
```

出力を正しく表示するには，次のコマンドの例のようにコマンドに-tオプションを使用します。

```
$ ssh -t user@unixhost ls -a
```

- 表示を更新するOpenVMSコマンドをリモートSSHコマンドとして実行すると，予測できない結果が発生することがあります。たとえば，次のコマンドを実行すると，予測できない動作が発生します。

  ```
  $ MONITOR PROCESS/TOPCPU
  ```

  このコマンドをローカルに実行すると，継続的に更新される棒グラフが表示されます。リモート・コマンドとして実行すると，更新された各画面が順に表示されます。さらに，Ctrl/Cを使用してコマンドを終了することもできません。

3.11.10 SSH バッチ・モード

ここでは，バッチ・モードの制限事項について説明します。

- SSHコマンド，SFTPコマンド，およびSCPコマンドは，UNIXソースから移植されたコードでインプリメントされているため，コマンド・プロシージャでSYS$INPUT，SYS$OUTPUT，およびSYS$ERRORに対する標準的なOpenVMSの動作のすべてがサポートされるわけではありません。次の例を参照してください。
  - SYS$INPUTはデフォルトのバッチ・コマンド・プロシージャではありません。
  - バッチ・ログ・ファイルやその他のSYS$OUTPUTファイルに書き込まれる出力には，余分な<CR> (ASCII decimal 13) やその他の明示的な書式設定文字が含まれることがあります。
  - 次の例に示すように，SYS$OUTPUTをファイルに出力することができます。

    ```
    $ ASSIGN OUT.DAT SYS$OUTPUT
    ```

- これらのコマンドを対話型コマンド・プロシージャから実行する場合は，次の表に示すように，明示的なUNIXバッチ・モード・フラグを使用する必要があります。

目的	フラグ
SSH (リモート・コマンド実行またはポート転送)	-o batchmode yes
SCP	"-B"
SFTP	"-B" {batchfile}

- 対話型セッション (つまり，リモート・コマンド実行やポート転送の設定のためではない) で， SSH コマンドをバッチ・モードで使用すると，バッチ・ジョブはハングします。

  "-S"オプションを対話型 SSH セッションで使用したり， DCL コマンド・プロシージャで対話方式で実行される SSH コマンドに対して使用したりすると，端末セッションはハングします。 Ctrl/Y と Ctrl/C を使用しても， DCL プロンプトに戻ることができません。端末セッションのハング状態を解除するには， SSH クライアントとサーバを再起動する必要があります。

- SFTP コマンドの場合は，次のことに注意してください。

  – -b {batchfile}または"-B" {batchfile}オプションを指定せずに，このコマンドを使用すると， SFTP はデフォルトでファイル SYS$LOGIN:TCPIP$SFTP_BATCHFILE.TXT を使用します。

  – 最後の行を除き，batchfileの各行の末尾にはライン・フィード (<LF>， ASCII decimal 10) を指定する必要があります。

- バッチ・モードで実行する場合，次のことに注意してください。

  – SFTP コマンドは最終的な進行状態インディケータを表示しますが， SCP コマンドは表示しません。

  – SSH コマンドは，パスワード，パスワードのアップデート，パスフレーズを求めるプロンプトを表示しません。いずれかが要求されると，バッチ・ジョブはエラーになります。

  – StrictHostkeyCheckingの値が“no”の場合， SSH コマンドは新しいホスト・キーを保存しません。値が“ask”の場合は， SSH は新しいホスト・キーを求めるプロンプトを表示しません。

    キーに関連するその他の注意事項や制限事項については，第 3.11.6 項を参照してください。

  – lsコマンドが SFTP バッチ入力に含まれていて，対話型出力でキーボードからの入力の続行が要求される場合は，出力行の一部がバッチ・ログ・ファイルから省略されることがあります。

3.11.11 SSH X11 ポート転送

ここでは， X11 ポート転送の制限事項と問題点について説明します。

- ネイティブ・モードで X11 転送を使用するには，システムで DECwindows MOTIF バージョン 1.3 以上を実行している必要があります。さらに， X Authority ユーティリティ (xauth) がシステムに必要です。 X11 サーバは，ホスト/ユーザ接続を認証するのにこのユーティリティを使用します。このユーティリティの使い方についての詳細は， HP DECwindows Motif for OpenVMS のドキュメントを参照してください。

- リモート X11 クライアント・アプリケーションを X11 サーバで表示するには，X11 クライアントの display 変数を，クライアントの接続先の X11 サーバのアドレスに設定する必要があります。次の DCL コマンドを使用すると，変数が正しく設定されているかどうか確認できます。

  ```
  $ SHOW LOGICAL DECW$DISPLAY
  ```

  WSA デスプレイ・デバイスの場合は， SHOW DISPLAY コマンドを使用して display 変数の値を表示します。

  OpenVMS クライアントで display 変数をサーバに設定するには，次の例に示すように， SET DISPLAY コマンドを使用します。ただし， 16.20.176.33 はサーバ・ノード・アドレスです。

  ```
  $ SET DISPLAY/CREATE/NODE=16.20.176.33/TRANSPORT=TCPIP
  ```

  OpenVMS 上の SSH は，ローカル・トランスポートと TCP/IP トランスポートだけをサポートします。ローカル・トランスポートを使用する場合は，ディスプレイが表示されるシステムをローカル・システムとして使用し，そのシステムで X11 サーバを実行している必要があります。ローカル・トランスポートの場合は，次のコマンドを使用してディスプレイを設定します。

  ```
  $ SET DISPLAY/CREATE/TRANSPORT=LOCAL
  ```

  UNIX システムでは，次のコマンドを使用して display 変数を設定することで，アドレスが 16.20.176.33 で TCP/IP トランスポートを使用するサーバ・ノードを指定します。

  ```
  >setenv display 16.20.176.33:0.0
  ```

  ローカル・トランスポートを使用するには，次の UNIX コマンドを使用します。

  ```
  >setenv display :0.0
  ```

- リモート OpenVMS システムで標準ポート転送セッションを設定する場合は， リモート・ポート転送を使用することをお勧めします。ローカル・ポート転送は動作しません。

3.11.12 SSH ファイル転送 (すべてのファイル・サイズ)

ここでは，ファイル転送操作に関連する SSH の制限事項について説明します。

- OpenVMS で， SSH2_CONFIG. ファイルのForcePTTYAllocationキーワードを“yes”に設定すると，ファイル・コピー操作を実行するときに障害が発生することがあります (SSH の他のインプリメントでは， SSH2_CONFIG. ファイルでForcePTTYAllocationキーワードを“yes”に設定すると， SSH コマンドに-tオプションを指定したのと同じ結果になります)。

- 次の例に示すように， OpenVMS SSH クライアントで SFTP コマンドと SCP コマンドを使用して， OpenSSH サーバにアクセスすると，パケット関連の警告が表示されることがあります。

```
sftp> ls
.
.bash_logout
.login
Warning: packet length mismatch: expected 27, got 8;  connection to
non-standard server?
```

一時停止した後，次のメッセージが表示されます。

```
sftp> Warning: packet length mismatch: expected 23, got 8;  connection to
non-standard server?
```

警告が表示されても， OpenVMS での操作は正しく実行されます。警告は無視してかまいません。警告が表示されないようにするには，次の例に示すように，論理名 TCPIP$SSH_TOLERANT_PROTOCOL_STATUS をシステム単位で割り当てます。

```
$ DEFINE/SYSTEM TCPIP$SSH_TOLERANT_PROTOCOL_STATUS 1
```

リブートのたびにこの割り当てを保持するには，このコマンドを適切なスタートアップ・コマンド・プロシージャに追加します。

- ファイル転送は，(DIRECTORY/FULL コマンドで表示される) 次のレコード形式の OpenVMS ファイルに制限されます。
  - STREAM_LF
  - 固定長の 512 バイト・レコード
- OpenVMS クライアントとサーバでファイルを参照する場合， UNIX パス名のすべての変形がサポートされるわけではありません。
- 次の Windows クライアントからの SCP コマンドと SFTP コマンドはテストされており， OpenVMS SSH サーバと正しく相互運用できます。
  - PuTTY
  - SSH 通信

  プロトコルのインプリメントや，クライアントが OpenVMS 形式のファイル指定を取り扱うことができるかどうかなどの要因に応じて，他のバージョンや他のクライアントも問題なく動作する可能性があります。
- SFTP コマンドを使用する場合， Ctrl/C を押しても "Cancel"は表示されません。また， Ctrl/T は DCL ではステータス・ラインを表示しますが，このシーケンスも機能せず， UNIX システムの場合のように， 2 つの隣接する文字を入れ替えます。第 4.14 節に示すように，文字の取り扱いに関するその他の問題点は本リリースで修正されています。
- SFTP lsコマンドは， 1 ページのデータを表示した後，次ページを表示するまでに，長時間にわたって停止します。

- SCP コマンドまたは SFTP コマンドを使用して，ファイルをそれ自体にコピーすると (ローカル・モード，またはクライアント・ホストに接続することで)，次のエラーが発生します。

  ```
  %TCPIP-E-SSH_FC_ERR_INVA, file record format invalid for copy
  ```

- SSH バージョン 1 を使用しているクライアントから実行された SCP コマンドは，OpenVMS SSH サーバで動作しません。 OpenVMS サーバは SSH バージョン 1 をサポートしません。

3.11.13 大きいファイルを転送する SSH

ここでは，大きいファイルの転送に関連する制限事項について説明します。

- システムで動作する DECC$SHR のバージョンは， OpenVMS バージョン 8.2 でリリースされたバージョン以上でなければなりません。
- ファイル・コピー・クライアントおよびサーバで必要とされるメモリ容量に対応するには，メモリ・パラメータ (WSDEF， WSQUO， WSEXTENT，および PGFLQUO) を調整する必要があります。正確な値は，システム・リソースおよび仮想メモリ・コンフィギュレーションに応じて異なります。詳細については，第 2.5 節を参照してください。
- SCP コマンドまたは SFTP コマンドを使用してファイル転送を開始した後，Ctrl/Y または Ctrl/C を使用して転送を中断することはできません。転送を停止するには，別のセッションからクライアント・プロセスまたはサーバ・プロセスを終了する必要があります。
  - OpenVMS クライアント・プロセスを停止するには

    クライアントでのファイル転送サーバ・サブプロセス名はusername_nという形式です。ただし，usernameは現在のユーザ名に対応し，nは整数です。プロセスが停止されると，次のメッセージがクライアントに表示されます。

    ```
    %TCPIP-E-SSH_FC_ERROR, undetermined error within sshfilecopy
    ```

    次のメッセージが OpenVMS SSH サーバに表示されます。

    ```
    log (TCPIP$SSH_GOME:TCPIP$SSH_RUN.LOG):
    Mon 28 13:09:15 INFORMATIONAL: Local disconnected:
       Connection closed.
    Mon 28 13:09:15 INFORMATIONAL: connection lost:
       'Connection closed.'
    ```

  - OpenVMS サーバ・プロセスを停止するには

    ファイル転送がアクティブなときに， OpenVMS DCL コマンド SHOW SYSTEM を使用すると，このコマンドはファイル転送に関連する 2 つのプロセスを表示します。 1 つのプロセスの名前は TCPIP$SSH_nという形式です。ただし，nは整数です。もう 1 つのプロセスの名前は TCPIP$prefix_BGnという形式です。ただし，nは BG デバイス番号，prefixは S， SS， SSH のいずれ

かです。 BG プロセスを停止する必要がありますが， TCPIP$SSH_nプロセスを停止すると，クライアントがハングします。

サーバが停止された後，次のメッセージがクライアントに表示されます。

```
Disconnected; connection lost (Connection closed.)
tcpip$ssh_scp2.exe: warning: child process
(/sys$system/tcpip$ssh_ssh2) exited.

%TCPIP-E-SSH_FC_ERROR, undetermined error within sshfilecopy
```

3.12 TCPDUMP の制限事項

TCPDUMP は， OpenVMS システムでも UNIX システムと同様に動作しますが，次の制限事項があります。

- UNIX システムでは，tcpdumpは NIC (network interface controller) を promiscuous モードに設定し，転送中のすべてのものをtcpdumpに送信します。

  OpenVMS システムでは， TCPDUMP はローカル・ホスト宛てのパケットおよびローカル・ホストから送信されるパケットだけを認識します。したがって，TCPDUMP は copy-all モードで動作します。 TCPDUMP は， TCP/IP カーネルで処理されるパケットのコピーだけを認識するので，イーサネット上で IP, IPv6，および ARP プロトコルだけをネイティブにトレースすることができます。

  TCPDUMP は， promiscuous モードで TCPDUMP を実行している別のプラットフォームからトレースされたパケットの書式設定またはフィルタ処理を行うことができます。この場合， DECnet などの他のプロトコルを処理します。

- サポートされる NIC のタイプはイーサネットだけです。 NIC の他のタイプ (ATM， FDDI，トークン・リング， SLIP， PPP など) はサポートされません。

- -iオプションはサポートされません。 UNIX システムでは，このオプションは，tcpdumpの接続先のインタフェースを指定します。

  OpenVMS システムでは， TCPDUMP は TCP/IP カーネルからパケットを取得します。

- -pオプションはサポートされません。 UNIX システムでは，このオプションは，tcpdumpが promiscuous モードでの動作を停止することを指定します。

  OpenVMS では， TCPDUMP は promiscuous モードで動作しません。したがって，デフォルトとしてこのオプションが設定されます。

- Ethereal ソフトウェアを使用して IPv6 ネットワーク・トラフィックをダンプする場合は，次のコマンド形式を使用して，データを正しい形式で書き込んでください。

  ```
  $ TCPDUMP -s 1500 -w filename
  ```

- 一度に 1 つのプロセスだけがトレースを実行できます。これは， TCPTRACE と TCPDUMP の両方に共通の制限事項です。

3.13 チャネル割り当てからの TCP/IP デバイス名の判断

OpenVMS では，チャネル割り当てに基づいてデバイス名を判断する方法をいくつか提供しています。 SYS$GETDVI/SYS$GETDVIW システム・サービスを使用すると， DVI$_DEVNAM， DVI$_FULLDEVNAM，および DVI$_UNIT アイテムはすべて，デバイスに関する情報を返します。最初の 2 つのアイテムは完全なデバイス名を返しますが， DVI$_UNIT アイテムはデバイスのユニット番号だけを返します。完全なデバイス名を作成するには，プログラムでユニット番号の前に文字列としてデバイス名およびコントローラ情報を付加する必要があります。 TCP/IP デバイス名の場合は，文字列BGまたはBGAを追加できます。たとえば，BG + 1234と指定すると，デバイス名はBG1234:になります。

TCP/IP のデバイス名は，将来のリリースで変更される可能性があります。プログラミングの際は， DVI$_DEVNAM または DVI$_FULLDEVNAM アイテムを使用して，完全なデバイス名の文字列を取得するようにしてください。このようなプログラムは， TCP/IP デバイス名が BGnnnnや BGAnnnnであるということを前提にしていないため， TCP/IP デバイス名の方針が今後変更されても，その影響を受けません。

3.14 TCP/IP 管理コマンドの制限事項

次の制限事項は， TCP/IP 管理コマンドに適用されます。

- TCP/IP Services バージョン 5.4 で failSAFE IP が導入されました。その結果，IP クラスタ・エイリアス・アドレスは使用されなくなります。したがって，次の TCP/IP 管理コマンドは今後サポートされません。
  - SET INTERFACE /NOCLUSTER
  - SHOW INTERFACE /CLUSTER

  IP クラスタ・エイリアス・アドレスも含めて，インタフェースのアドレスを表示するには，次の TCP/IP 管理コマンドを使用します。

  ```
  TCPIP> ifconfig -a
  ```

  クラスタ・エイリアス・アドレスをアクティブ・システムから削除するには，次のコマンドを使用します。

  ```
  TCPIP> ifconfig ie0 -alias 10.10.10.1
  ```

  次の TCP/IP 管理コマンドは今後もサポートされます。
  - SET INTERFACE/CLUSTER
  - SET CONFIGURATION INTERFACE /CLUSTER

- SET CONFIGURATION INTERFACE /NOCLUSTER
- SHOW CONFIGURATION INTERFACE /CLUSTER

- SET NAME_SERVICE /PATH

  このコマンドにはSYSNAM特権が必要です。プロセス・レベルで必要な特権がないのに，このコマンドを入力すると，コマンドは動作せず，しかもそのことは通知されません。コマンドをSYSTEMレベルで入力すると，コマンドは動作しませんが，エラー・メッセージが表示されます。

- SET SERVICEコマンド

  サービスに対するパラメータを変更した後，その変更を有効にするには，サービスをいったん無効にした後，再び有効にする必要があります。

TCP/IP Services管理コマンドについての詳細は，『*HP TCP/IP Services for OpenVMS Management Command Reference*』を参照してください。

3.15 日本語機能についての制限事項および注意事項

この節では，TCP/IP Servicesを日本語環境で使用する場合の制限事項および注意事項について説明します。

3.15.1 日本語ファイル名のサポートについて (Alpha のみ)

本バージョンではFTPでのファイル転送でODS-5ディスクに対するExtended File Specifications（長いファイル名，深いディレクトリ階層，拡張文字セット）がサポートされています。しかし，日本語OpenVMS V7.2で提供される日本語ファイル名の使用はサポートされません。

3.15.2 漢字フィルタの互換性について

本バージョンでは既存の漢字フィルタに関して下位互換性を保ちます。以前のバージョン用に作成された漢字フィルタは，ファイル名や，指定する際の論理名を変更することなくそのまま使用することができます。

3.15.3 POP クライアントを日本語環境で使用する場合の注意事項

POPクライアントを日本語環境で使用する場合，以下の点に注意する必要があります。

- SMTPサーバに漢字フィルタが設定されている場合，漢字コードが変換されたメールがOpenVMS NEWMAILフォルダに格納されます。POPサーバは，OpenVMS NEWMAILフォルダからメールを取り出し，メール中の漢字コードの変換を行うことなくPOPクライアントに送信します。したがってPOPクライア

ントが受信するメールには，第 3.15.4 項「SMTP における漢字フィルタに関する注意事項」に記述する内容がそのまま適用されます。

- POP サーバが動作する環境で， OpenVMS Mail ユーティリティを使用してメールの交換が行われている場合， DEC 漢字を含んだメールも POP クライアントに送信されます。この場合，日本語 EUC をサポートする POP クライアントを使用する必要があります (日本語 EUC は， DEC 拡張漢字文字を除き， DEC 漢字と互換性があります)。

3.15.4 SMTP における漢字フィルタに関する注意事項

- 漢字フィルタが漢字コードの変換対象として扱うのは，メール本文だけです。メール・ヘッダ部は漢字コードの変換対象外です。
- 漢字フィルタは，メール本文全体を漢字コードの変換対象として扱います。たとえば， MIME (Multipurpose Internet Mail Extensions) 標準 (RFC1521) のメールであっても， MIME は解釈されずに漢字コードの変換が行なわれます。

3.15.5 SMTP における日本語に関する制限及び注意事項

- SMTP では，メール・ヘッダ部での日本語の使用をサポートしていません。そのため， OpenVMS Mail ユーティリティにおけるパーソナル・ネームの設定は，特に注意が必要です。 OpenVMS Mail ユーティリティを使用して， SMTP によるメールの送信を行う場合，パーソナル・ネームに日本語文字列を設定しないようにしてください。パーソナル・ネームに日本語文字列が設定されていると，問題が発生する可能性があります。
- OpenVMS Mail ユーティリティ（V7.0 より古いバージョン）には，アドレス内のネストした二重引用符を処理できないという制限があるため， SMTP は，二重引用符をセント記号に変換しています。ただし，セント記号は， DEC 漢字の一部の漢字コードと重複するため，日本語環境では，セント記号を表示することができません。
- 8 ビットの漢字コードを含んだメールを送信する場合， SMTP サーバに対して，8 ビット文字の転送を指定する必要があります。 SMTP システム・パラメータの詳細については，『Compaq TCP/IP Services for OpenVMS Management』を参照してください。
- SMTP サーバが受信したメールを OpenVMS NEWMAIL フォルダに格納する際，メール本文の 1 行の大きさを 255 バイトに分割します。このため，日本語文字列を含むメール本文の 1 行の大きさが， 255 バイトを越えている場合，文字化けを起こすことがあります。また，漢字フィルタにより文字列のバイト数が増減することがあります。漢字フィルタによる変換後の 1 行の大きさが 255 バイトを越えると， SMTP サーバは， OpenVMS NEWMAIL フォルダにメールを格納することができず，エラーのメールが返されます。

3.15.6 IMAP クライアントを日本語環境で使用する場合の注意事項

IMAP クライアントを日本語環境で使用する場合，以下の点に注意する必要があります。

- SMTP サーバに漢字フィルタが設定されている場合，漢字コードが変換されたメールが OpenVMS NEWMAIL フォルダに格納されます。 IMAP サーバは，OpenVMS NEWMAIL フォルダからメールを取り出し，メール中の漢字コードの変換を行うことなく IMAP クライアントに送信します。したがって IMAP クライアントが受信するメールには，第 3.15.4 項「SMTP における漢字フィルタに関する注意事項」に記述する内容がそのまま適用されます。また， MIME ヘッダを使用して漢字コードを指定している場合には， MIME ヘッダの漢字コードの指定と実際にエンコードされている漢字コードとの不整合から，正常に文字が表示されない場合があります。
- IMAP サーバが動作する環境で， OpenVMS Mail ユーティリティを使用してメールの交換が行われている場合， DEC 漢字を含んだメールも IMAP クライアントに送信されます。この場合，日本語 EUC をサポートする IMAP クライアントを使用する必要があります (日本語 EUC は， DEC 拡張漢字文字を除き， DEC 漢字と互換性があります)。
- サーバ上のフォルダ名では，漢字や仮名などの 2 バイト文字はサポートされません。 2 バイト文字を使用すると，フォルダ名がまったく違った文字列に変換されてしまい， IMAP クライアントからの操作ができなくなることがあります。

3.15.7 VIEW コマンドでの日本語機能の未サポート

FTP クライアントの VIEW コマンドでは漢字フィルタを指定することはできません。

3.15.8 SSH での日本語機能の未サポート

SSH クライアントおよびサーバのセキュア・ログインおよびファイル転送では漢字フィルタを指定することはできません。

4

修正された問題点

この章では，本バージョンの TCP/IP Services で修正された問題点について説明します。

4.1 アドバンスト・プログラミング環境に関して本リリースで修正された問題点

ここでは，本リリースで修正されたプログラミング関連の問題点について説明します。

4.1.1 TCPIP$LIB.OLB ライブラリにリンクすると，リンクの競合が発生する

問題点:

strdupまたはputenv関数への参照を含むプログラムを TCPIP$LIB.OLB ライブラリにリンクすると，リンクの競合が発生します。リンカは%LINK-W-MULDEF という警告メッセージを生成し， C RTL ライブラリ内の同じ名前の関数と競合することを示します。

修正結果:

以前のバージョンの TCP/IP Services では， TCPIP$LIB.OLB ライブラリは，より新しいバージョンの OpenVMS C RTL ライブラリに定義されている関数をインクルードしていました。これらの TCPIP$LIB.OLB ルーチンには DECC$というプリフィックスが付加されており，新しいバージョンの C RTL ライブラリの同じ名前のルーチンと競合します。本リリースの TCP/IP Services では，このような競合が発生しないように， TCPIP$LIB.OLB ライブラリが変更されました。

4.2 本リリースで修正された BIND サーバの問題点

ここでは，本リリースで修正された BIND サーバの問題点について説明します。

4.2.1 BIND スレーブは通知要求を拒否する

問題点:

スレーブとしてコンフィギュレーションされている BIND サーバは，マスタ・サーバからの通知要求を拒否することがあります。スレーブの TCPIP$BIND_RUN.LOG に書き込まれるエラー・メッセージには， "refused notify from non-master"という文字列が含まれます。この問題は， TCPIP$BIND.CONF コンフィギュレーション・ファイルの options ステートメントにlisten-on-v6ディレクティブを指定することで，IPv6 通信に対してマスタ・サーバを有効に設定したときに発生します。

修正結果:

この問題は本リリースで修正されました。

4.2.2 BIND バージョン 9 サーバ・プロセスは "Assertion Failure"エラーで終了する

問題点:

BIND サーバ・プロセスはエラーで終了し， TCPIP$BIND_RUN.LOG ファイルに次のいずれかのメッセージが記録されます。

```
REQUIRE((((task) != 0L) && (((const isc__magic_t*)(task))->magic
== ((('T')<< 24 | ('A') << 16 | ('S') << 8 | ('K')))))) failed
Sun 19 03:00:13 CRITICAL: exiting (due to assertion failure)
%SYSTEM-F-OPCCUS, opcode reserved to customer fault at
PC=FFFFFFFF80A6C924, PS=0000001B

REQUIRE(res->item_out == isc_boolean_true) failed
Fri 19 13:12:04 CRITICAL: exiting (due to assertion failure)
%SYSTEM-F-OPCCUS, opcode reserved to customer fault at
PC=FFFFFFFF80E6C924, PS=0000001B
```

修正結果:

この問題は本リリースで修正されました。

4.3 本リリースで修正された failSAFE IP の問題点

ここでは，本リリースで修正された failSAFE IP の問題点について説明します。

4.3.1 failSAFE IP ファントム障害

問題点:

failSAFE IP が複数のインタフェース上で単一のインタフェース・アドレスによってコンフィギュレーションされているシステムでは，ファントム障害が発生することがあります。 LAN トラフィックの頻度が低い場合は， failSAFE IP は誤ったエラーを通知することがあります。

修正結果:

この問題は本リリースで修正されました。 failSAFE IP はデフォルトで MAC レベルのブロードキャスト・パケットを生成するようになりました。新しいコンフィギュレーション・パラメータGENERATE_TRAFFICを設定して， failSAFE IP が強制的に gratuitous ARP パケットを生成するようにすることができます。次の新しいコンフィギュレーション・パラメータを TCPIP$FAILSAFE.CONF ファイルに指定できます。

GENERATE_TRAFFIC

failSAFE IP が定期的に MAC レベルのブロードキャストまたは無意味な ARP パケットを生成することを指定します。 failSAFE IP がトラフィック生成を行わないようにコンフィギュレーションすることもできます。

デフォルト: mac (MAC レベルのブロードキャスト)
その他のオプション: arp (無意味な ARP パケット) またはoff

次のコンフィギュレーション・ファイルの例は，無意味な ARP パケットを生成するようにパラメータを設定している行を示しています。

```
GENERATE_TRAFFIC: ARP
```

MAC_PTY

MAC レベルのブロードキャスト・トラフィックが生成されている場合，このパラメータには MAC プロトコル・タイプ (6005 などの 2 バイトの 16 進数) を指定できます。

MAC_PTY を指定しないと， MAC ブロードキャストは，使用可能なプロトコル・タイプが見つかるまで，各プロトコル・タイプを試します。

次のコンフィギュレーション・ファイルの例は， MAC プロトコル・タイプを 6005 として設定する行を示しています。

```
MAC_PTY: 6005
```

failSAFE IP のコンフィギュレーションについての詳細は，『*HP TCP/IP Services for OpenVMS Management*』を参照してください。

4.3.2 ユーザは failSAFE IP ログ・ファイルの場所を変更できない

問題点:

failSAFE IP ログ・ファイルの名前は常に次のように設定されます。

SYS$SYSDEVICE:[TCPIP$FSAFE]TCPIP$FAILSAFE_node-name.LOG

ユーザがシステム上の別の場所を指定することはできません。

修正結果:

この問題は本リリースで修正されました。新しいコンフィギュレーション・パラメータ LOGFILE を使用することで，ユーザはログ・ファイルの場所としてデフォルト以外の場所を指定できるようになりました。

LOGFILE	failSAFE IP が作成するログ・ファイルのファイル指定を指定します。デフォルトは SYS$SYSDEVICE:[TCPIP$FSAFE]TCPIP$FAILSAFE_node-name.log です。パラメータとファイルの場所は，次の例に示すように指定してください。 LOGFILE: DEV1:[STATS]FAILSAFE.LOG

failSAFE IP のコンフィギュレーションについての詳細は，『*HP TCP/IP Services for OpenVMS Management*』を参照してください。

4.3.3 SHOW INTERFACE コマンドは擬似インタフェース・アドレスを表示しない

問題点:

インタフェースで障害が発生した後や，エイリアス・アドレスを回復した後， TCP/IP 管理コマンド SHOW INTERFACE は擬似インタフェース・アドレスを表示しません。

修正結果:

この問題は本リリースで修正されました。

4.4 本リリースで修正された FTP サーバの問題点

ここでは，本リリースで修正された FTP サーバの問題点について説明します。

4.4.1 FTP では IP アドレス指定ができない

問題点:

FTP サーバでは，接続先のクライアント以外の IP アドレス，つまり特権付きポートの指定を， PORT コマンド， LPRT コマンド， EPRT コマンドに指定できません。このようなコマンドは拒否され，次のエラーが発生します。

```
500 Illegal {PORT|LPRT|EPRT} command.
```

FTP サーバとクライアントは，サード・パーティによるデータ接続の「盗用」を防止します。 FTP サーバの場合は，クライアント以外の IP アドレス，つまり特権付きポートからのパッシブ・モード接続に適用されます。 FTP クライアントの場合は，サーバ以外の IP アドレス，つまりポート 20 以外のポートからのアクティブ・モード接続を拒否します。

修正結果:

このようなソフトウェアの変更が不都合な場合は，次の論理名を定義することで，元の動作に戻すことができます。

サーバ	クライアント
TCPIP$FTPD_ALLOW_ADDR_REDIRECT	TCPIP$FTP_ALLOW_ADDR_REDIRECT
TCPIP$FTPD_ALLOW_PORT_REDIRECT	TCPIP$FTP_ALLOW_PORT_REDIRECT

これらの論理名を定義すると， FTP サーバと FTP クライアントで行われる IP アドレスとポートのチェックを緩和することができます。

4.4.2 DCL DIRECTORY または UNIX ls コマンドは "Illegal Port Command"エラーを返す

問題点:

FTP クライアントで，スペースを含むパスワードを使用して OpenVMS FTP サーバにログインすると， DCL コマンド DIRECTORY または UNIX コマンドlsに対する応答として，次のエラー・メッセージが返されます。

```
500 Illegal PORT command.
```

修正結果:

この問題は本リリースで修正されました。

4.5 本リリースで修正された FTP クライアントの問題点

ここでは，本リリースで修正された FTP クライアントの問題点について説明します。

4.5.1 GET/MGET コマンドの後，FTP クライアントは中間ファイルを削除しない

問題点:

ワイルドカード文字を含めて入力した FTP GET または MGET コマンドが終了すると， FTP が作成した一時的な TCPIP$FTP_TEMPnnnnnnnn.TMD ファイルは SYS$SCRATCH 領域から削除されるはずです。しかし，ワイルドカードに一致するものがファイルから検索されないと， FTP は一時ファイルを削除しません。少なくとも 1 つのファイルがワイルドカードの条件に一致する場合は， FTP は SYS$SCRATCH に作成された TCPIP$FTP_TEMPnnnnnnnn.TMD ファイルを正しく削除します。

修正結果:

この問題は本リリースで修正されました。

4.6 本リリースで修正された IMAP の問題点

ここでは，本リリースで修正された IMAP の問題点について説明します。

4.6.1 IMAP での移動とパージの後，メール・メッセージが消失する

問題点:

手動でメッセージをフォルダから移動した後， IMAP を使用してソース・フォルダをパージすると，メールが消失します。

この問題は，次の場合に発生します。

1. IMAP クライアントを使用して，メール・ファイルを選択した場合
2. OpenVMS Mail を使用してメッセージを読み取り，別のフォルダに移動した場合
3. IMAP クライアントを使用して，選択したフォルダで Expunge コマンドを入力した場合

メッセージは移動先フォルダから消去されます。メッセージを新しいフォルダにコピーした場合には，フォルダ自体がなくなります。

修正結果:

この問題は本リリースで修正されました。

4.6.2 IMAP CLOSE コマンドは正常に機能しない

問題点:

クライアントが IMAP CLOSE コマンドを実行してログアウトするときに， IMAP サーバは削除の対象としてマークされているすべてのメッセージを削除しません。

修正結果:

この問題は本リリースで修正されました。 CLOSE コマンドを入力すると， IMAP サーバは削除の対象としてマークされているすべてのメッセージを削除します。

4.7 本リリースで修正された IPv6 の問題点

ここでは，本リリースで修正された IPv6 の問題点について説明します。

4.7.1 TCPIP$IP6_SETUP.COM の問題点

ここでは，本リリースで修正された TCPIP$IP6_SETUP.COM の問題点について説明します。

- **問題点**:

  IPv6 のコンフィギュレーションを行うための TCPIP$IP6_SETUP.COM コマンド・プロシージャには，次の問題点があります。

  – 6to4 トンネルをコンフィギュレーションしようとすると，エラーになります。

  – 6to4 リレー・ルータで必要とされるすべてのルートがコンフィギュレーションされるわけではありません。

  – 自動トンネルの終端は正しくコンフィギュレーションされません。

  – IPv6 over IPv6 手動トンネルはコンフィギュレーションできません。

  – IPv6 ホストまたはルータのコンフィギュレーションで， IPv6 コンフィギュレーション・ファイルと初期化ファイルにエラーが生成されます。

  – 手動経路選択はコンフィギュレーションできません。

  修正結果:

  コンフィギュレーション・コマンド・プロシージャは， 6to4 トンネル， 6to4 リレー・ルータで必要とされるすべてのルート，自動トンネル， IPv6 over IPv6 手動トンネル，および手動ルートを正しくコンフィギュレーションできるようになりました。詳細は，『日本語 HP TCP/IP Services for OpenVMS インストレーション/コンフィギュレーション・ガイド』を参照してください。

- **問題点**:

  TCPIP$IP6_SETUP.COM コマンド・プロシージャでは，指定されたアドレスを検証するために， TCP/IP Services を起動することが必要です。

  修正結果:

  この問題は本リリースで修正されました。 TCPIP$IP6_SETUP.COM を実行するために， TCP/IP Services を起動する必要はありません。

4.7.2 iptunnel create コマンドを実行すると，BIND は IPv4 アドレスを検索する

問題点:

トンネルのソース・ポイントまたはエンド・ポイントとして IPv4 アドレスを指定したiptunnel createコマンドを起動すると，名前の解決が必要ないにもかかわらず，膨大な DNS 名前解決クエリがネーム・サーバに送信されます。これらのクエリによって送信遅延が発生することがあります。

修正結果:

この問題は本リリースで修正されました。

4.8 本リリースで修正された NFS サーバの問題点

ここでは，本リリースで修正された NFS サーバの問題点について説明します。

4.8.1 NFS サーバは大文字と小文字を区別する検索でファイルに上書きする

OpenVMS バージョン 7.3-1 以上で， SET PROCESS コマンドに/CASE_LOOKUP=BLIND 修飾子を指定すると，検索でファイル名の大文字と小文字の区別は無視されますが，/CASE_LOOKUP=SENSITIVE を指定すると，ファイル名の大文字と小文字が区別されます。しかし， NFS サーバで大文字と小文字を区別しないように設定しているときに， NFS クライアントが大文字と小文字の区別を除いて同じ名前のファイルを作成しようとすると，予測しない結果が発生することがあります。たとえば， 2 番目に作成したファイルが最初のファイルに上書きされる可能性があります。

本リリースの TCP/IP Services では， TCP/IP 管理コマンド ADD EXPORT に CASE_BLIND と CASE_SENSITIVE という 2 つの新しいオプションが追加されました。これらのオプションは， NFS サーバのファイル検索で， UNIX と同様に大文字と小文字の区別を制御します。たとえば，大文字と小文字を区別するように設定すると， NFS はファイル名 AaBBc.TXT と AABBC.TXT で大文字と小文字の区別を保持するので，これらのファイルは 2 つの異なるファイルとして取り扱われます。

一般に，検索で大文字と小文字を区別するかどうかは， TCP/IP Services クライアント (サーバではない) が判断します。これは，クライアントがファイルの検索をサーバで行うのではなく，ローカル・ディレクトリ・キャッシュで行うからです。しかし，ファイルの作成時には，サーバが，大文字と小文字の区別が有効かどうかを制御します。サーバとクライアントで大文字と小文字の区別に関するオプションの設定が一致しているかどうか確認してください。一致していないと，予測しない結果が発生することがあります。

CASE_BLIND オプションと CASE_SENSITIVE オプションについての詳細は，次のコマンドを入力して確認してください。

```
$ TCPIP HELP ADD EXPORT
```

4.8.2 VMS クライアント以外で作成されるディレクトリはバージョン・リミットを継承しない

問題点:

新たに作成されるディレクトリは，バージョン・リミット属性を親ディレクトリから継承します。 OpenVMS NFS クライアントの要求でディレクトリが作成される場合は，この属性は正しく継承されます。しかし， OpenVMS NFS クライアント以外の要求で作成されるディレクトリは，この属性を継承しません。 UNIX ファイルにはバージョンが 1 つしかありませんが，新しいディレクトリのバージョン・リミットは 0 (リミットなし) に設定されるので， UNIX クライアントの場合は特に問題です。

修正結果:

この問題は本リリースで修正されました。 OpenVMS NFS クライアント以外の要求で作成されるディレクトリも，親ディレクトリのバージョン・リミット属性を継承するようになりました。

4.8.3 NFS サーバと netstat は，EV56 以上のテクノロジを実行していない Alpha システムで正常に動作しない

問題点:

EV56 プロセッサ搭載のシステムより古い Alpha システムでは， NFS サーバとnetstatユーティリティは，インストラクション実行時間が非常に長くなるか，またはまったく動作しません。

修正結果:

この問題は本リリースで修正されました。

4.8.4 本リリースで修正された MOUNT サーバの問題点

ここでは，本リリースで修正された MOUNT サーバの問題点について説明します。

4.8.4.1 マウント・ポイントのチェックは正しくない

問題点:

MOUNT サービスは，エクスポートされたファイル・システムのマウント・ポイントに関して，誤ったチェック結果を示します。

修正結果:

この問題は本リリースで修正されました。

4.8.4.2 ODS-5 ファイル・システムをマウントできない

問題点:

ADD EXPORT コマンドに TYPELESS_DIRECTORIES オプションを指定すると，末尾が.dir でないディレクトリ指定がエクスポート・エントリに指定されている場合でも， ODS-5 ファイル・システムをマウントできません。

修正結果:

この問題は本リリースで修正されました。

4.8.4.3 ホスト名のチェックがマウント操作中に実行され，エラーになる

問題点:

クライアントがファイル・システムをマウントしようとすると，mountd_option_* nfsサブシステム属性が設定されていない場合でも，ホスト名のチェックが実行されます。クライアントに出力されるエラー・メッセージまたはイベント・メッセージには，拒否されたアクセス権が示されることがあります。 MOUNT サーバは，クライアントのホスト名と IP アドレスがホスト・データベース (TCPIP$HOST) または DNS/BIND 情報と矛盾することを示す OPCOM メッセージを生成することがあります。

修正結果:

この問題は本リリースで修正されました。

4.8.4.4 誤解を招く MOUNT サーバ・エラー

問題点:

マウント・ポイントがすでに使用中の場合， MOUNT サーバは誤解を招く可能性のあるエラー・メッセージを報告します。

マウント・ポート (ポート 10) がすでに使用されている場合， MOUNT サーバは次のエラーを報告します。

```
ERROR: bind: address already in use
```

このメッセージは， BIND/DNS の問題であると誤解される可能性がありますが，実際に問題を起こしているのは， C RTL 呼び出しbind()です。

修正結果:

この問題は本リリースで修正されました。メッセージは次のように変更されました。

```
ERROR: bind: mount server port(10) already in use
```

4.9 本リリースで修正された NTP の問題点

ここでは，本リリースで修正された NTP の問題点について説明します。

4.9.1 ハイ・パフォーマンス Alpha システムでは NTP がシステム・クロックを調整できない

問題点:

特定のハイ・パフォーマンス Alpha システムでは， NTP がシステム・クロックを調整できないことがあります。したがって， NTP は正確に時刻を管理できません。この場合，次のエラー・メッセージが NTP ログ・ファイルに記録されます。

```
%SYSTEM-F-BADLOGIC, internal logic error detected
VMS timekeeping is not working as expected - can't proceed
```

修正結果:

この問題は本リリースで修正されました。

4.9.2 NTP は ODS-5 ディスクに小文字のファイル名を作成する

問題点:

以前のリリースの TCP/IP Services では， NTP サーバが ODS-5 ディスクにファイルを作成する場合，小文字のファイル名を付けていました。その結果，大文字のファイル名を使用する ODS-5 以外のディスクとの間に，ファイル名の付け方に関する矛盾が発生していました。

修正結果:

この問題は本リリースで修正されました。ファイルはすべて，大文字のファイル名を使用して作成されます。

4.10 本リリースで修正された RCP の問題点

ここでは，本リリースで修正された RCP の問題点について説明します。

4.10.1 複数のファイルまたはディレクトリに関係する RCP ファイル・コピー操作はエラーになる

問題点:

- 再帰的なファイル・コピー操作を行うと，明らかな理由がないのに途中で操作が中断するか，または読み取りエラーか書き込みエラーになります。
- ファイルをコピーしようとすると，操作はエラーになり，次のエラー・メッセージが出力されます。

```
%CONV-F-OPENOUT, error opening !AS as output
```

/RECURSIVE 修飾子またはワイルドカードを使用して，8 レベルより深い階層のディレクトリにあるファイルをコピーしようとすると，この問題が発生します。

修正結果:

これらの問題は本リリースで修正されました。 RCP は， 8 レベルより深い階層のディレクトリ構造に対するコピー操作をサポートするようになりました。最大 255 レベルまでのディレクトリ指定がサポートされるようになりました。

4.10.2 OpenVMS 相互間のコピー操作でファイル属性が保持されない

問題点:

OpenVMS システム間の RCP コピー操作では，ファイル属性 (ファイル編成と構造) が保持されません。ファイルは自動的に STREAM_LF 形式に変換されます。

修正結果:

本リリースでは， RCP で/VMS 修飾子を指定することで，ファイル属性を保持できるようになりました。 UNIX 形式の場合は，-vオプションを使用します。

注意

この修飾子は，2 台の OpenVMS システム間のファイル・コピー操作に対してだけ指定してください。それ以外の場合に使用すると，操作はエラーになります。

4.10.3 2GB より大きいファイルのコピーはエラーになる

問題点:

2 ギガバイトより大きいサイズのファイルをコピーしようとすると，エラーになります。

修正結果:

本リリースでは，RCP で 2GB より大きいファイルをコピーできるようになりました。最大 4GB のサイズまでコピーできます。

4.11 本リリースで修正された SMTP の問題点

ここでは，本リリースで修正された SMTP の問題点について説明します。

4.11.1 SMTP レシーバは受信者が配布可能なアドレスかどうかチェックしない

問題点:

SMTP レシーバは，RCPT TO SMTP プロトコル・コマンドに指定された受信者の電子メール・アドレスが配布可能なアドレスかどうかのチェックを行いません (たとえば，ユーザ・アカウントがシステムに存在するかどうかのチェックなど)。このチェックは，SMTP シンビオント・プロセスが SMTP キュー内のメール・メッセージを処理するまで行われません。その時点まで，メッセージに関する責任はホストが負い，メッセージの配布に問題がある場合は，メッセージを宛先不明で返す必要があります。

SPAM の受信時には，この動作がさらに問題になります。SPAM がホストに到着したときに，宛先のユーザが存在しないと，ホストのシンビオント・プロセスは SPAM の Return-Path: ヘッダに指定された電子メール・アドレスに SPAM を宛先不明で返します。しかし，SPAM の Return-Path: ヘッダに指定されている電子メール・アドレスは無効であるため，宛先不明で返した SPAM はホストの POSTMASTER アカウントに返されます。POSTMASTER アカウントのメールは SYSTEM アカウントに転送されるので，SYSTEM ユーザはこれらの二重に返送された SPAM と，有効な電子メールとをより分けるる処理を絶えず行わなければなりません。

修正結果:

SMTP レシーバが変更され，RCPT TO SMTP プロトコル・コマンドに指定されている受信者の電子メール・アドレスが配布可能なアドレスかどうかをチェックするようになりました。この問題は，不明ユーザに宛てた SPAM をホストに返さないようにすることで解決されました。

Symbiont-Checks-Deliverabilityコンフィギュレーション・オプションを使用すると，この機能をオンまたはオフに設定することができます。このコンフィギュレーション・オプションは，SMTP コンフィギュレーション・ファイル(SMTP.CONFIG)に指定します。

このオプションを TRUE に設定すると，シンビオントは RCPT TO 受信者が配布可能な宛先かどうかを確認します。Symbiont-Checks-Deliverabilityを FALSE (デフォルト)に設定すると，配布可能かどうかのチェックを受信者が行うことになります。

4.11.2 SMTP はブロックすべき送信者からのメールを受け付ける

問題点:

SMTP は，ブロックすべき送信者からのメールを受け付けることがあります。ブロックすべき送信者とは，SMTP.CONFIG ファイルの anti-SPAM Reject-Mail-Fromフィールドに指定されている送信者です。Reject-Mail-Fromフィールドのエントリが，SMTP.CONFIG ファイルのフィールドの制限である 500 文字を超える場合，SMTP はこのようなメールをブロックできません。

修正結果:

この問題は本リリースで修正されました。SMTP.CONFIG ファイルのフィールドの長さの制限が 500 文字から 10,000 文字に拡大されました。

4.11.3 2 つのメッセージの Message-ID ヘッダの値が同一になる

問題点:

100 分の 1 秒単位まで同じ時刻に 2 つのメッセージが作成されると，メッセージの Message-ID ヘッダの値が同一になります。その結果，メール・システムによっては，2 つのメッセージのうち，2 番目のメッセージが重複するメッセージとして削除されることがあります。Message-ID は一意の値でなければなりません。

修正結果:

この問題は本リリースで修正されました。100 分の 1 秒単位まで同じ時刻に 2 つのメッセージが作成されても，Message-ID ヘッダの値は一意になるようになりました。

4.11.4 SMTP To: または Cc: ヘッダに指定された複数のアドレスによって発生する可能性のある問題点

問題点:

OpenVMS mail で作成される To: SMTP メール・ヘッダに複数のアドレスがある場合，アドレスは複数行のテキストに分離されず，1 行に表示されます。 OpenVMS でこのようなメッセージを受信するときに，この To: 行の長さが OpenVMS のメールの 1 行の長さの制限である 255 文字を超えると， SMTP シンビオントはメッセージを配布するときに複数行に分割しますが， 2 行目以降はインデント (タブとばし) されません。このため，メッセージの各行は，不正な形式のヘッダのように見えます。その結果，電子メールを自動的に読み取る一部のプログラムの動作が正しく実行されないことがあります。 Cc: 行が OpenVMS メールの文字数の制限を超える場合も，同じ問題が発生します。

修正結果:

この問題は本リリースで修正されました。ユーザがメール・メッセージを作成するときに， SMTP To: ヘッダと Cc: ヘッダを作成する SMTP ソフトウェアは， To: ヘッダ行と Cc: ヘッダ行が 75 文字を超えないようにします。ヘッダ行に次の受信者のアドレスを追加した結果，行の長さが 75 文字を超える場合は， SMTP ソフトウェアは，その受信者のアドレスを追加する前に，ヘッダにライン・フィードとタブを挿入します。

4.12 本リリースで修正された SNMP の問題点

ここでは，本リリースで修正された SNMP の問題点について説明します。

4.12.1 TCPIP$CONFIG.COM は特殊文字を含む SNMP コミュニケーション名を拒否する

問題点:

TCP/IP Services バージョン 5.1 およびバージョン 5.3 では， TCPIP$CONFIG.COM は特殊文字をチェックし，特殊文字を含むコミュニティ名を拒否します。

修正結果:

これらの制限事項は本リリースで緩和されました。しかし， TCPIP$CONFIG.COM はスペースを含む SNMP コミュニティ名を受け付けません。さらに，コミュニティ名の一部として指定した引用符 (") は， TCPIP$CONFIG.COM で正しく処理されないことがあります。 SHOW CONFIGURATION SNMP コマンドを使用して，名前が正しいかどうかチェックするようにユーザに警告するメッセージが表示され，必要に応じて， SET CONFIGURATION SNMP コマンドを使用して名前を修正するように要求されることもあります。

4.13 本リリースで修正されたソケット API の問題点

ここでは，本リリースで修正されたソケット API の問題点について説明します。

4.13.1 ソケット関数 getaddrinfo( )はハングする

問題点:

同じプログラムでgetaddrinfo( )を 2 回連続して呼び出すと， 2 回目の呼び出しはハングします。この問題は，afパラメータが AF_INET6 に設定されていて，ai_flagsパラメータが AI_ALL または AI_ADDRCONFIG に設定されていない場合にだけ発生します。

修正結果:

この問題は本リリースで修正されました。

4.14 本リリースで修正された SSH の問題点

ここでは，本リリースで修正された SSH の問題点について説明します。

4.14.1 SSH サーバはパスワードの変更を認めない

問題点:

アカウント・パスワードの有効期限が切れたときに， SSH サーバは， VMS クライアント以外のクライアントに対するパスワード変更要求をサポートしません。

修正結果:

SSH コンフィギュレーション・オプションAllowNonvmsLoginWithExpiredPwdが"yes"に設定されているときに，パスワードの有効期限が切れると，サーバは，新しいパスワードの入力をユーザに求める要求をクライアントに送信します。この場合，ユーザはパスワードを変更する必要があります。変更しないと，アカウントはロックされ，次回ログインしようとしても失敗します。

しかし， OpenVMS アカウントで SYSUAF にDisForce_Pwd_Changeフラグが設定されている場合は，サーバはユーザのログインを許可し，次のメッセージを表示します。

```
WARNING - Your password has expired; update immediately with SET
PASSWORD!
```

DisForce_Pwd_Changeフラグは，各 OpenVMS アカウントに個別に適用する必要があります。

AllowNonvmsLoginWithExpiredPwdオプションのデフォルト設定は，"yes"に変更されました。AllowNonvmsLoginWithExpiredPwdオプションが"no"に設定されている場合は，パスワードの有効期限が切れたときに，OpenVMS クライアント以外のユーザはパスワード認証を受けることができません。ユーザにはパスワードを変更するオプションがありません。詳細は，第 5.2 節を参照してください。

4.14.2 言語タグのサポート

問題点:

SSH クライアントに送信されるパスワード変更要求には，言語タグが含まれることがあります。しかし，一部のクライアントは言語タグをサポートしません。

修正結果:

この機能は，SSH サーバ・コンフィギュレーション・ファイル (SSHD2.CONFIG) のDisableLanguageTagコンフィギュレーション・オプションを使用して制御できます。デフォルトでは，OpenVMS パスワード変更要求には，言語タグが含まれます。言語タグをサポートしないクライアントがこのような変更要求を受け取ると，エラー・メッセージを出力します。言語タグの送信は，SSH サーバ・コンフィギュレーション・ファイルでDisableLanguageTagオプションを"yes"に設定することで，無効にすることができます。このように設定すると，パスワード変更要求に言語タグが一切含まれなくなります。

4.14.3 2 つのパスワードの受け付け

問題点:

OpenVMS SSH サーバは，パスワード認証で第 2 パスワードをサポートしません。

修正結果:

SSH サーバは，ユーザが第 2 パスワードを保有していることを検出します。この場合，OpenVMS は第 2 パスワードの入力を求めます。1 つのパスワードの有効期限が切れていると，ユーザにパスワードの変更が求められます。2 つのパスワードの有効期限がどちらも切れている場合は，第 1 パスワードの変更が要求された後，第 2 パスワードの変更が要求されます。

SSH クライアントが第 2 パスワードの入力を求める OpenVMS プロンプトを受け付けるには，次のいずれか一方または両方のコンフィギュレーション・オプションを 2 に設定する必要があります。

- クライアント・コンフィギュレーション・ファイル (SSH2_CONFIG): NumberOfPasswordPrompts

- サーバ・コンフィギュレーション・ファイル(SSHD2_CONFIG): PasswordGuesses

どちらのコンフィギュレーション・ファイルも TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]に保存できます。さらに，ユーザはユーザ固有の SSH ディレクトリ ([username.SSH2]) にクライアント・コンフィギュレーション・ファイルを格納することができます。

注意

複数のパスワードのサポートについては，SSH 関連のどの RFC にも指定されていません。

第 2 パスワードを求めるプロンプトは， OpenVMS で第 1 パスワードに対してエラー状況を強制的に設定することで有効になります。これは OpenVMS ソフトウェアで内部的に処理されます。しかし，第 1 パスワードを入力した後に表示されるメッセージは，クライアント・ソフトウェアに応じて異なります。認証が有効に設定されている場合は，不正侵入レコードは作成されません。しかし，いずれかのパスワードの入力が誤っていると，不正侵入レコードが作成されます。

一部のクライアントは，両方のパスワードの有効期限が切れている場合でも，第 2 パスワードの要求を受け付けます。しかし。第 2 パスワードの要求を受け付けないクライアントもあり，これらのクライアントは，いずれか一方のパスワードの有効期限が切れている場合にだけ，正常に機能します。

4.14.4 ネイティブ・モードの X11 ポート転送は動作しない

問題点:

SSH for OpenVMS では， (-xまたは+x SSH コマンド・オプションを使用するか，またはクライアント・コンフィギュレーション・ファイルでForwardX11キーワード，サーバ・コンフィギュレーション・ファイルでAllowX11Forwardingキーワードを使用して) X11 ポート転送をインプリメントするためのネイティブ・モード SSH メカニズムがサポートされません。 SSH では標準ポート転送だけをサポートするので， X11 機能を有効にするには，特別なセットアップ操作が必要です。

修正結果:

この問題は本リリースで修正されました。詳細は，表 5–2 を参照してください。

4.14.5 SFTP の二重エコーとキーの取り扱いに関する問題点

問題点:

SFTP を使用してリモート・システムに接続する前に，SFTP プロンプト (SFTP>) で入力した文字は二重にエコー表示されます。さらに，リモート・システムに接続すると，左向き矢印キーと右向き矢印キーが期待どおりに動作せず，Ctrl/X (行の消去)，Ctrl/W (行の再表示)，および Ctrl/C (終了) シーケンスもそれぞれ期待どおりに動作しません。

修正結果:

これらの問題点は本リリースで修正されました。しかし，Ctrl/C を押しても，"Cancel"は表示されません

4.14.6 SSH，SFTP，および SCP コマンドはバッチ・モードでエラーになるか，または正常に動作しない

問題点:

SSH，SCP，および SFTP コマンドはバッチ・モードでエラーになるか，または正常に動作しません。

修正結果:

この問題は本リリースで修正されました。

バッチ・モードに関連する制限事項については，第 3.11.10 項を参照してください。

4.14.7 RSA キー・タイプは受け付けられない

問題点:

以前のバージョンの SSH for OpenVMS では，サーバに対するクライアントの認証で RSA キーが受け付けられていましたが，クライアントに対するサーバの認証では受け付けられていませんでした。

修正結果:

本リリース以降，TCP/IP Services では，クライアントに対するサーバの認証でも，サーバに対するクライアントの認証でも，RSA キー・タイプと DSA キー・タイプの両方が受け付けられるようになりました。

4.15 本リリースで修正されたSSLの問題点

ここでは，本リリースで修正されたSSLの問題点について説明します。

4.15.1 SSLのインストール後，POP SSLは機能しなくなる

問題点:

TCP/IP ServicesにSSL V1.2キットをインストールした後，POP SSLのサポートは機能しなくなります。POPサーバはSSLポートを認識しなくなるため，SSLを介して接続するクライアントをサービスできません。TCPIP$POP_RUN.LOG POPサーバ・ログ・ファイルに次の行が記録されます。

```
POP server will not listen for SSL connections.
SSL$LIBCRYPTO_SHR32_INIT status: %LIB-E-KEYNOTFOU, key not found in tree
```

修正結果:

この問題は本リリースで修正されました。

4.16 本リリースで修正されたTELNETの問題点

ここでは，本リリースで修正されたTELNETの問題点について説明します。

4.16.1 TELNETの不正侵入検出機能の柔軟性の問題点

問題点:

特定の状況で，あるユーザが不正侵入(不正なログインなど)を行うと，システムがロックされ，端末サーバなどのマルチポート・サーバでは，すべてのポートがロックされることがあります。この問題を回避するために，論理名TCPIP$TELNET_NO_REM_IDが設定されました。しかし，この論理名の設定によって，不正侵入しているユーザは，システムからロックされずに，別のポートにログインすることができます。

修正結果:

この問題は本リリースで修正されました。論理名TCPIP$TELNET_TRUST_LOCATIONで，TELNET不正侵入レコードをどのように取り扱うかを指定することができます。この論理名を定義すると，リモート・クライアントが指定した位置文字列が不正侵入レコードに含まれるようになります。たとえば，多くの端末サーバは物理ポート番号を提供しますが，OpenVMSクライアントは送信元のユーザ名と端末ラインを提供します。この情報を不正侵入レコー

ドに含むことで，リモート・ホスト全体(およびすべてのユーザ・ポート)がロックされるのではなく，特定のユーザまたはポートだけがロックされるようになります。

5
マニュアルのアップデート

この章では， TCP/IP Services 製品のマニュアルで提供される情報のアップデートについて説明します。

5.1 本リリースでアップデートされたマニュアル

TCP/IP Services V5.5 で次のマニュアルがアップデートされています。

表 5–1 最新のマニュアルの変更

タイトル	変更点

HP TCP/IP Services for OpenVMS SNMP Programming and Reference	• TCPIP$CONFIG.COM コマンド・プロシージャ，TCP/IP 管理コマンド SET CONFIG SNMP, SYS$SYSDEVICE:[TCPIP$SNMP]TCPIP$VMS_SNMP_CONF.DAT ファイルで，通常の SNMP に対してコンフィギュレーションされているトラップ・コミュニティは，トラップ・レシーバ・ホストやコミュニティの名前の判断に使用されません。
	SNMP_TRAPSND ユーティリティに対する-cフラグと-hフラグの値は，次のように処理されます。
	– -c (community) フラグが使用されていないときは，省略時の名前である "public"がトラップで使用されます。
	– -h (host) フラグが使用されていないときは，トラップは LOCALHOST に送信されます。
	• SNMPv1 トラップ PDU の "agent address"フィールドの値は，マスタ・エージェント (TCPIP$ESNMP_SERVER) が稼動しているホストのプライマリ・インタフェースのアドレスです。このアドレスの値は，次の手順で確認できます。
	1. 論理名 TCPIP$INET_HOSTADDR を変換します。
	2. 次の TCP/IP コマンドを使用して， LOCALHOST の値を取得します。
	`$ TCPIP SHOW CONFIGURATION COMMUNICATION`
	この値が IP アドレスの形式でない場合は，次のコマンドを使用して IP アドレスを判断します。
	`$ TCPIP SHOW HOST/LOCAL local-host-name`

(次ページに続く)

表 5–1 (続き) 最新のマニュアルの変更

タイトル	変更点
HP TCP/IP Services for OpenVMS Sockets API and System Services Programming	• TCPIP_KEEPIDLEオプションの省略時の設定が修正されました。 • 新しいソケット・オプション TCP_TSOPTENA, TCP_PAWS, and TCP_SACKENA が記載されました。 • acceptルーチンが Xopen エラー戻り値を明確に記載しました。 • ポート番号の変換手順に関する情報が記載されました。 • Information about using 64-bit addresses with the send()およびreceive()ファンクションでの 64 ビット・アドレスの使い方に関する情報が記載されました。 • ポート番号のネットワーク・バイト・オーダへの変換に関する情報がgetservbyport()ファンクションに記載されました。 • IOCTL に関する情報が追加されました。 • ソケット API に関する情報が*HP C Run-Time Library Reference Manual for OpenVMS Systems*から*HP TCP/IP Services for OpenVMS Sockets API and System Services Programming*へ移動されました。 • プログラミングに関する情報が*HP TCP/IP Services for OpenVMS Guide to IPv6*から*HP TCP/IP Services for OpenVMS Sockets API and System Services Programming*へ移動されました。 • IPv6 での QIO の使い方に関する情報が追加されました。
HP TCP/IP Services for OpenVMS ONC RPC Programming	第 3.5.1 項の例が修正されました。
日本語 HP TCP/IP Services for OpenVMS インストレーション/コンフィギュレーション・ガイド	• I64 プラットフォームへのインストレーションに関する情報が追加されました。 • VAX プラットフォームへのインストレーションに関する情報が削除されました。 • IPv6 をコンフィギュレーションするために拡張された IP6_SETUP.COM コマンド・プロシージャの使い方に関する情報が追加されました。 • インストレーションとコンフィギュレーションのスクリプトがアップデートされました。

さらに，以下に示すいくつかのヘルプ・ファイルがアップデートされ，拡張されました。

- HELP TCPIP_SERVICES PROGRAMMING_INTERFACES
- HELP TCPIP_SERVICES REMOTE_COMMANDS RCP
- HELP TCPDUMP
- TCPIP HELP IFCONFIG
- TCPIP HELP SYSCONFIG

5.2 本リリースでアップデートされなかったマニュアル

TCP/IP Services V5.5 では次のマニュアルはアップデートされていません。これらのマニュアルに対する変更予定内容が記載されています。

表 5–2 将来のマニュアルの変更

タイトル	変更点
Compaq TCP/IP Services for OpenVMS Concepts and Planning	• I64 プラットフォームに関する情報が追加されます。 • OpenVMS ファイル仕様に関する情報がアップデートされます。
HP TCP/IP Services for OpenVMS Management	本マニュアルは以下の内容が拡張されます。 • リリース・ノートの第 1.6 節, NTP (Network Time Protocol) V4.2 のサポートに記載されている情報が追加されます。 • リリース・ノートの第 1.2 節, failSAFE IP での IPv6 のサポートに記載されている情報が追加されます。 また， TCPIP$FAILSAFE 論理名の説明に対する修正が加えられます。 • リリース・ノートの第 1.3 節, Secure IMAP に記載されている情報が追加されます。 • リリース・ノートの第 4.8.1 項, NFS サーバは大文字と小文字を区別する検索でファイルに上書きする に記載されている情報が追加されます。 • FTP に関する情報に新しい論理名 TCPIP$FTP_COMPAT_REV と TCPIP$FTPD_COMPAT_REV が含まれます。 • リリース・ノートの第 4.11.1 項, SMTP レシーバは受信者が配布可能なアドレスかどうかチェックしないに記載されている情報が追加されます。 • *HP TCP/IP Services for OpenVMS Guide to IPv6*に記載されている情報が追加されます。 • コンフィギュレーション・ファイルを指定する論理名の使用方法に関する説明において， DEFINE コマンドの/SYSTEM および/EXECUTIVE_MODE修飾子の使用方法ならびにこれらの論理名を変更する前にサービスを停止することを推奨すること等の詳細が含まれるように拡張されます。

(次ページに続く)

表 5–2 (続き) 将来のマニュアルの変更

タイトル	変更点
HP TCP/IP Services for OpenVMS Guide to SSH	• リリース・ノートの第 1.7 節, SSH の新機能に記載されている変更点に関する情報が含まれます。 • 第 3 章に以下の情報が追加されます。 Xauthentication 実行ファイルは SSH クライアント・コンフィギュレーション・ファイルで指定することができます。省略時の置き場所 (SYS$SYSTEM:DECW$XAUTH.EXE) 以外のデバイスとディレクトリを指定するために，Xauthpatキーワードを使用してください。 • リリース・ノートの第 4.14.4 項, ネイティブ・モードの X11 ポート転送は動作しないを反映するために第 5 章がアップデートされます。 X11 ポート・フォワーディングが SSH クライアントとサーバの両方で有効になっている場合， SSH を使って SSH サーバに接続し， X11 クライアント・プログラムをサーバで実行し，ローカルの画面上に表示させることができます。また，複数のシステムに対してポート・フォワーディングを鎖状に接続することもできます。その場合，中間のシステムで X11 サーバを実行していなくても構いません。例えば， SYSTEM1 から SYSTEM2 に接続し，さらに SYSTEM2 から SYSTEM3 に接続するために SSH を使います。 SYSTEM3 で実行している X11 クライアント・アプリケーションは SYSTEM1 上で安全に表示されます。 • 以下のオプションが第 4 章の "Managing Auditing"節に追加されます。 AllowVmsLoginWithExpiredPw Allowed values: yes, no Default: yes Description: Controls the behavior when an OpenVMS client attempts to establish an SSH connection to an OpenVMS server account with an expired password. The value yes allows the client to interact with the server to update an expired password. The value no rejects the login. Note that when the disforce_pwd_change flag is set in the user's SYSUAF record, the client user is allowed to log in; a warning message is displayed instructing the user to change the password. If the user does not change the password, the account will be locked out and the user will not be allowed to log in again.

(次ページに続く)

表 5–2 (続き) 将来のマニュアルの変更

タイトル	変更点
	• 以下のオプションの説明が変更されます。省略時の設定値が "no"から "yes"に変わりました。 AllowNonvmsLoginWithExpiredPw Allowed values: yes, no Default: yes 詳細な情報はリリース・ノートの第 4.14.1 項, SSH サーバはパスワードの変更を認めないを参照してください。 • "Port Forwarding for FTP"節の例が修正されます。 • 6.9.1, Changing the Default Configuration が修正されます。複数のホストを指定した場合，最大で 3 つの BIND サーバが使われます。
HP TCP/IP Services for OpenVMS User's Guide	• リリース・ノートの第 4.10 節, 本リリースで修正された RCP の問題点に記載された RCP ファイル・フォーマットおよびサイズ情報がアップデートされます。 • リリース・ノートの第 4.10.2 項, OpenVMS 相互間のコピー操作でファイル属性が保持されないに記載されている RCP の新しい/VMS 修飾子が追加されます。
HP TCP/IP Services for OpenVMS Tuning and Troubleshooting	• *HP TCP/IP Services for OpenVMS Guide to IPv6*に記載されている情報が追加されます。
HP TCP/IP Services for OpenVMS Management Command Reference	• リリース・ノートの第 3.14 節, TCP/IP 管理コマンドの制限事項に記載されている情報を反映するためにアップデートされます。 • リリース・ノートの第 4.8.1 項, NFS サーバは大文字と小文字を区別する検索でファイルに上書きする に記載されている ADD EXPORT の新しいオプション CASE_BLIND とCASE_SENSITIVEが追加されます。 • IPv6 近隣探索論理名が追加されます。 IPv6 近隣探索の問題を解析するために，SYS$MANAGER:TCPIP$ND6HOST.LOG ログ・ファイル中のデバッグ・メッセージを取得するために論理名を定義することができます。 論理名を設定するために以下のコマンドを入力してください。 $ DEFINE /SYSTEM TCPIP$ND6HOST_DEBUG 1 TCP/IP Services を起動する前にこの論理名を定義してください。

(次ページに続く)

表 5–2 (続き) 将来のマニュアルの変更

タイトル	変更点
HP TCP/IP Services for OpenVMS Guide to IPv6	第 2.6 節 (Configuring an IPv6 Router) のsysconfigコマンドは誤りです。このコマンド・ラインのサブシステム・パラメータはipv6です。 IP6_SETUP.COM プロシージャを実行する前にこのコマンドを入力する必要はありません。 IP6_SETUP.COM は適切な属性を設定します。 このマニュアルは将来廃止されます。新しいバージョンの『日本語 HP TCP/IP Services for OpenVMS インストレーション/コンフィギュレーション・ガイド』および『*HP TCP/IP Services for OpenVMS Sockets API and System Services Programming*』はアップデートされ，訂正されました。 *HP TCP/IP Services for OpenVMS Guide to IPv6*の残りの情報は将来のバージョンの*HP TCP/IP Services for OpenVMS Management*と*HP TCP/IP Services for OpenVMS Tuning and Troubleshooting*に含まれます。

上記マニュアルは TCP/IP Services の将来のリリースでアップデートされます。

日本語 HP TCP/IP Services for OpenVMS
リリース・ノート

2005 年 7 月　発行

日本ヒューレット・パッカード株式会社

〒 140-8641 東京都品川区東品川 2-2-24 天王洲セントラルタワー

電話　(03)5463-6600 (大代表)
