2007年9月28日

お客様各位

エスアイアイ・ネットワーク・システムズ株式会社

NS－2484－10 システムソフトウェア リリースノート

Version3.7

Version3.7 では、下記の機能追加を行っています。

(1)装置全体で着信可能なチャネル数制限機能

ISDN 回線から着信処理において、現在通信中および接続処理中の呼の合計が、あらかじめ設定されている
チャネル数を超えた場合、着信呼を拒否（理由表示#17：着ユーザビジー）する機能を追加しました。

本機能を制御するために、新たに isdn.conf ファイルが追加されました。
以下に isdn.conf ファイルに設定するキーワードの使用方法を示します。
設定を変更した場合、reload コマンドを実行すると、変更内容が本装置に反映されます。

channel_limit

書式　channel_limit　*number*（1～69）
デフォルト　なし（本機能は無効となります）
使用例　channel_limit　10
解説　number には、制限する（許可する）チャネル数を指定します。
指定されたチャネル数を超えると、着信を拒否します。
注意　チャネル数制限は、回線ごとではなく、装置全体のチャネル数として設定します。
発信時には本機能は動作しません。ただし着信時においては、発信により
通信中あるいは接続処理中の呼は、チャネル数制限のチェック時に使用中
のチャネル数のカウントの対象になります。

また本機能により着信を拒否した場合に出力されるワーニングメッセージを以下に示します。

ワーニングメッセージ	意味	対処
CC:WAN#:InFail over channel limit	装置全体で着信可能なチャネル数制限機能により着信を拒否したことを示します。	特に対処する必要はありません。

Version3.6

Version3.6 では、下記の不具合修正を行っています。

(1)DNS クライアントの不具合対処

本装置へのコマンド入力時、IP アドレスでなく、ホスト名を入力した場合、ホスト名を IP アドレスに変換できず入力したコマンドが実行できない不具合を修正しました。
本装置の「hosts」ファイルに登録されていないホスト名で、かつ「resolv.conf」ファイルに DNS サーバが設定されている場合、該当 DNS サーバへ IP アドレス変換要求を送信しますが、キーワードであるドメイン(domain)、ネームサーバの IP アドレス(nameserver)の設定位置によって不具合が発生する場合がありました。
「resolv.conf」ファイルに設定するキーワードの先頭に、「スペース」、または「TAB」が設定されている場合、該当キーワードが無効となる不具合を修正しました。

Version3.5

Version3.5 では、下記の不具合修正を行っています。

(1)TCP 脆弱性に関する対策

TCP プロトコルに関して、SYN または RST フラグがセットされた成りすまし、TCP セグメントによるコネクション切断、および成りすまし TCP セグメントによるデータの不正注入に関する TCP 脆弱性について対策を実施しました。

TCP 脆弱性の内容に関しましては、下記をご参照ください。

JPCERT/CC Alert 2004-04-21(1)

また、対策につきましては、下記のインターネットドラフトを参考としております。

draft-ietf-tcpm-tcpsecure-01.txt

(2) radius 関連のメンテナンス機能(非公開部分) の不具合を修正

radius 関連のメンテナンス機能 (非公開部分) を使用した際に、radiusd が異常終了する不具合を対処しました。

Version3.4

Version3.4 では、下記の機能追加と不具合修正を行っています。

(1)SNTP クライアント機能のサポート

ネットワーク上の時間同期プロトコルとして、SNTP (Simple NetworkTime Protocol) をサポートしました。
SNTP クライントから NTP サーバに時刻を問い合わせ、応答した時刻に同期させます。
SNTP クライアント機能を使用する場合、まず servers ファイルに

/share/sntpd

の行を追加し、write コマンドを実行した後、本装置を再起動 (reboot コマンド) を実行してください。
SNTP 機能を制御するために、sntp.conf ファイルが追加されました。
以下に各キーワードの使用方法を示します。設定を変更した場合、reload コマンドを実行すると、
変更内容が本装置に反映されます。

mode

書式	mode { on | off }
デフォルト	off
使用例	mode on
解説	on に設定した場合、本装置の SNTP 機能が有効になります。 off に設定した場合、SNTP 機能は停止します。
注意	あらかじめ servers ファイルに「/share/sntpd」の設定を行い、本装置を再起動してください。 server キーワードが正しく設定されていない場合、on の設定を行っても、SNTP 機能は開始されません。

server

書式	server <IP アドレス>
デフォルト	なし
使用例	server 172.16.1.3
解説	時刻を問い合わせる NTP サーバーの IP アドレスを設定します。

polltime

書式	polltime <ポーリング時間>
デフォルト	60
使用例	polltime 120
解説	NTP サーバーに時刻を問い合わせる間隔を秒単位で設定します。

設定値の範囲は、60～1800 (秒) です。

srcaddr

書式　　srcaddr　{auto | hostname | specify <IP アドレス>}

デフォルト　auto

使用例　　srcaddr specify 172.31.1.1

解説　　本装置が送出する sntp パケットの送信元 IP アドレスの指定を行います。

auto　　：送出インターフェースの IP アドレスを使用します。

hostname　：自局ホスト名に対応する IP アドレスを使用します。

specify　　：<IP アドレス>で設定された IP アドレスを使用します。

注意　　specify で設定する IP アドレスは、interface ファイルなどで、本装置の IP アドレスとして、あらかじめ設定されている必要があります。

また SNTP 使用時に出力される可能性のあるワーニングメッセージを以下に示します。

ワーニングメッセージ	意味	対処
sntp:NTP server no response	NTP サーバからの応答がありません。	NTP サーバが起動されているかどか、及び sntp.conf の server キーワードに NTP サーバーの IP アドレスが正しく設定されているかどうか、確認してください。
sntp:NTP server not ready	NTP サーバの準備ができていません。	NTP サーバが上位の NTP サーバと同期するまで、待ってください。
sntp:adjust time(sec) is too large	NTP サーバとの時間差が大きすぎるため、補正ができません。	date コマンドで本装置の時刻を NTP サーバと 30 分以内の時刻に設定してください。
sntp.conf(line X):invalid parameter	sntp.conf ファイルのキーワードに対するパラメータの設定が正しくありません。	X 行目のパラメータの設定を確認してください。
sntp.conf(line X):no parameter	sntp.conf ファイルのキーワードに対するパラメータが設定されていません。	X 行目のキーワードに対するパラメータを設定してください。
sntp.conf(line X):invalid IP address	IP アドレスの設定が正しくありません。	X 行目の IP アドレスの設定を確認してください。
sntp.conf(line X):invalid value	パラメータの設定値が正しくないか、設定範囲を超えています。	X 行目の設定値を確認してください。

(2) ping コマンドの不具合対処

ping コマンド実行時に、本装置から送信する ICMP パケットの識別子が、まれに直前に実行した ping コマンドの ICMP 識別子と同じ値になる可能性がある不具合を修正しました。

(3) RIP 機能に関する不具合対処

RIP 機能に関して、以下の問題点に対処しました。

・interface ファイルに設定されたブロードキャストアドレスを、ルーティングテーブルから削除してしまう場合がある不具合に対処しました。

・RIP でバックアップしている場合に、バックアップ経路から切り戻らない場合がある不具合に対処しました。

・rip.conf に設定されていないインタフェースの先のアドレスを、公告するルートの nexthop に設定してもエラーにならない不具合に対処しました。

・rip.conf に公告するルートを設定するとルーティングテーブルに登録できるエントリ数が少なくなる不具合に対処しました。

・RIP でインタフェースがダウンしたときにダウンしたインタフェースのルート情報が消去されない場合がある不具合に対処しました。

(4) ipfilters ファイルの文法エラー時のワーニングメッセージの表示

ipfilters ファイルに%filter 分類キーワード内に文法エラーが発生した場合に、適切なワーニングメッセージが表示されるように修正しました。表示されるされるワーニングメッセージを以下に示します。

ワーニングメッセージ	意味	対処
ipfilters(line X):Name unknown	X 行目のフィールドエントリで未定義の名前が検出されまた。	%CONST による定義、hosts ファイルの設定などを確認してください。
ipfilters(line X):Filter unknown	X 行目のフィールドエントリで予約語以外の名前が検出されました。	設定されている名前を確認してくだい。
ipfilters(line X):Mask out of range	IP アドレスのマスク設定が範囲を超えています。	IP アドレスのマスクの設定を確認してください。
ipfilters(line X):Primitive syntax error	X 行目のフィールドエントリの演算子の次に設定れている値に誤りがあります。	設定されている値を確認してください。
ipfilters(line X):Syntax error	X 行目に文法エラーがあります	設定内容を確認してください。
ipfilters(line X):Filter name required	X 行目の%filter でフィルタ名が定義されていません。	フィルタ名を設定してください。
ipfilters(line X):Literal syntax error	X 行目で使用できない文字や数の表記法が検出されました。	設定内容を確認してください。
ipfilters(line X):Out of sync. skip some words	構文解析でエラーが発生したため、X 行目から次の%filter 行までスキップされました。	エラー要因となっているワーニングメッセージをもとに、エラー要因を修正してください。

また起動時あるいは reload コマンド実行時に、ipfilters ファイルをシステムが解析した結果を表示する filstat コマンドをサポートしました。以下に filstat コマンドの仕様を説明します。

＜filstat コマンド＞

機能　　：ipfilters ファイルをシステムが解析した結果、有効なフィルターエントリを表示します。

フォーマット：filstat

パラメータ　：なし

使用例　　：

```
Filter   <testFIL> is defined, 4 cells are allocated
        PROTO = ICMP
      OR PROOT = TCP AND SPORT = 23
```

解説：

使用例の 1 行目の<>で囲まれた部分は、%filter で指定したフィルタ名が表示されます。
また「XX cells are allocated」の XX には、そのフィルタで使用されるセル数（システム内部で使用する内部フィルタ要素数）が表示されます。
その次の行からは、そのフィルタにおいて有効なフィールドエントリが表示されます。
文法エラーが発生している場合には、エラーが発生しているフィールドエントリ以降は、表示されません。

注意：

本装置では、1つのフィルタで使用できるセル数は、約 300 です。

(5) servers ファイルへの telnetd の登録に関する機能追加

servers ファイルに telnetd を登録する際に設定可能な

-r ： 相手ホスト名の指定

-l ： 自局ホスト名の指定

において、従来は hosts ファイルに設定されているホスト名のみが設定可能でしたが、直接 IP アドレスを指定できるように機能追加しました。

(6) SNMP の sysUpTime オブジェクトの仕様変更

SNMP の MIB2 の sysytem グループで定義されている sysUpTime オブジェクト（装置が起動してからの 1/100 秒単位の時間：32 ビットのカウンター）がオーバーフローした場合に、従来のバージョンでは、オーバーフロー前の最後にマネージャからアクセスされた時点の sysUpTime 値を返す仕様になっていました。
本バージョンから、sysUpTime オブジェクトのカウンターがオーバーフローした場合には、0 に戻るように仕様を変更しました。

Version3.3.2

Version3.3.2 では、下記の機能追加と不具合修正を行っています。

(1)auth ｺﾏﾝﾄﾞの機能追加

auth ｺﾏﾝﾄﾞにおいて、本装置にﾛｸﾞｲﾝできるﾕｰｻﾞの追加と、ﾊﾟｽﾜｰﾄﾞの設定を同時にできるように機能追加しました。以下に auth ｺﾏﾝﾄﾞに追加したﾊﾟﾗﾒｰﾀの使用方法を示します。

[フォーマット]　auth　addp　ﾕｰｻﾞ名　ﾕｰｻﾞ ID

[パラメータ]　addp　ﾕｰｻﾞの追加とﾊﾟｽﾜｰﾄﾞを設定する

[使用例]　ﾕｰｻﾞ (siins)/ﾕｰｻﾞ ID(10) の追加とﾊﾟｽﾜｰﾄﾞを設定する場合

```
#auth addp siins 10 ↓
Enter New Password? _____↓      ･･･ パスワードを入力します
Re-Enter New Password? _____↓   ･･･ 確認のため再度パスワードを入力します
#
```

(注意)入力したパスワードは表示されません。

(2)IP の不具合対処

不正な IP ヘッダを持ったパケットを受信した場合、本装置が reboot してしまう不具合に対処しました。

(3)バージョンアップサーバの不具合対策

バージョンアップサーバ(FTP サーバ)がポートスキャンを受けると、バージョンアップサーバの状態が不正な状態のままロックしてしまう場合があり、以後バージョンアップが行えなくなる不具合に対処しました。

Version3.3

Version3.3 では、下記の機能追加と不具合修正を行っています。

(1) LCP の不具合対処

PPP の LCP のネゴシエーションにおいて、本装置が送信した CREQ(Configure Request)パケットに対して、不正なオプションタイプを含んだ CREJ(Configure Reject) パケットを受信した場合、本来のメモリ領域を越えて内部バッファに書き込みを行なってしまう場合があり、

- PPP 認証ができなくなる。
- メモリの allocation に失敗し、コマンドを実行できなくなる。
- 本装置が reboot してしまう。

などの現象が発生する不具合に対処しました。

(2) ネットマスク変更時の不具合対処

interface ファイルの en0、en1 インターフェースのネットマスクの bit 長を以前より短く変更し、reload コマンドを実行しても、ブロードキャストアドレスが変更されない不具合に対処しました。

(3) RIP2 の不具合対処

本装置が RIP2 で広告したルートに対して、NextHop フィールドを本装置のアドレス、metric を 16 にして、RIP2 で送り返してくるルータが存在した場合、広告したルートが無効になってしまう不具合に対処しました。

(4) RIP の不具合対処

RIP で得たルートと、gateways ファイルで設定したスタティックルートが競合する環境で、gateways ファイルの設定を無効に(設定をコメントにして reload コマンドを実行)したり、有効に(コメントアウトされている設定のコメントを外して reload コマンドを実行) したりする動作を繰り返した場合に発生する以下の不具合に対処しました。

- スタティックルートの設定が無効な場合に、RIP からのルートがルーティングテーブルに反映されない。
- スタティックルートの設定が有効な場合に、スタティックルートが RIP のエージングでルーティングテーブルから削除されてしまう。

(5) TCP の不具合対処

不正な TCP オプションを持ったパケットを受信した場合に、本装置がまれに reboot してしまう場合がある不具合を対処しました。

(6) support コマンドのサポート

本装置のメンテナンス情報を収集し、表示するための support コマンドを追加しました。
このコマンドの出力内容については、弊社サポート時に使用しますので、内容に関する説明書はございません。

(7) CLID による RADIUS 認証時のアトリビュートの追加

CLID(発信者電話番号) により RADIUS 認証を行う場合、本装置が送信する Access Request パケットに、Calling-Station-ID アトリビュートを追加しました。

Version3.2.1

Version3.2.1 では、下記の機能追加と不具合修正を行っています。

(1) syslog の機能拡張

本装置が送出する syslog パケットの、送信元 IP アドレスを指定できるようにしました。
従来は送信元 IP アドレスに、パケットを送信するインタフェースの IP アドレスを割り付けており、送信インタフェースの変化に伴い、送信元 IP アドレスも変化していました。
今回の機能拡張により、送信インタフェースに依存することなく、送信元 IP アドレスを指定した IP アドレスに、固定することができます。
以下にキーワードの使用方法を示します。

srcaddr

キーワード　　syslog.conf ファイル

書式　srcaddr { auto | hostname | specify <IP アドレス> }

デフォルト　auto

例1　srcaddr　auto

例2　srcaddr　hostname

例3　srcaddr　specify　172.32.2.241

解説　本装置が送出する syslog パケットの送信元 IP アドレスの指定を行います。

auto　: 送出インタフェースの IP アドレスを使います。
hostname : 自局ホスト名に対応する IP アドレスを使います。
specify　: <IP アドレス>で指定された IP アドレスを使います。
<IP アドレス>部分は、ホスト名での指定も可能です。

注意　送信元 IP アドレスは、interface ファイルなどで、本装置の IP アドレスとして、あらかじめ設定されている必要があります。

(2) SNMP 脆弱性に関する不具合対処

SNMP 脆弱性に関する CERT の報告(*)にある PROTOS テストスイートを実行すると、SNMP エージェントがダウンするか、またはシステムソフトウェアがダウンする不具合に対処しました。

(*) CERT 報告に関する URL は、
http://www.cert.org/advisories/CA-2002-03.html
をご参照ください。

(3) RADIUS 認証機能の不具合対処

RADIUS 認証で menu アトリビュートを利用すると、NS-2484-10 が RADIUS 認証できなくなる不具合に対処しました。

(4) PRI フレーマの起動手順の改善

本装置の起動時に、PRI 回線の送信信号が一時的に不定な状態(*)になっていることが判明したため、PRI フレーマチップの起動手順を変更し、不定な状態をなくして無信号になるよう改善しました。

(*)不定な状態とは、B8ZS でエンコードされていない信号が送信ラインにのっている状態を示します。

(5) load コマンドの問題点の対処

load コマンドを FireWall 越しで実行した場合に、一部の FireWall では、load コマンドを実行できない問題に対処しました。

(6) users ファイルの不正設定時の不具合対処

users ファイルの%user の設定では、1つの interface キーワードしか設定できませんが、間違って複数の interface キーワードを設定し、「connect_on_demand on」の設定を行った場合、interface キーワードの設定内容によっては、reload コマンド実行後正常動作ができなくなったり、この設定のまま本装置を再起動すると正常に起動しなくなる問題点に対処しました。

(7) ローカル認証における CBCP の不具合への対処

本装置の users ファイルに
- CBCP の callback を行う。
- 着信時には PPP 認証の要求を行う。
- 発信時(callback 時) には PPP 認証の要求を行わない。

という接続条件で設定されている接続相手への callback が失敗してしまう問題に対処しました。
なおこの現象は、V3.0～V3.2 のみで発生します。

(8) L2TP の通信に関する問題点への対処

アクセスリストを設定しているインターフェースから、フラグメントされた自局宛て IP フレームを受信すると、廃棄されてしまう問題点に対処しました。この問題は L2TP を使用している場合に発生する可能性があります。

(9) モデムの接続性の向上

回線品質が悪い場合の、一部のソフトウェアモデムとの接続性を改善しました。

Version3.2

Version3.2 では、下記の機能追加と不具合修正を行っています。

(1)「NS-281 8BRI 拡張ボード」と「NS-344 NS-2484 用 DSP 拡張ボード」のサポート

NS-2484 で BRI ポートをサポートしました。
この機能強化により、BRI(128Kbps)の ISDN を複数回線で運用を開始し、ユーザの増加に合わせて
PRI(1.5Mbps)の ISDN 回線に切り替えたり、増設することが可能です。
拡張ボードのボードタイプの設定や組み合わせ可能な構成などの詳細は、取り扱い説明書の PDF ファイルを
ダウンロードし参照してください。

http://www.sii.co.jp/js/nshp/product/index.html

尚、従来のバージョンを使用しているお客様が、Version 3.2 にバージョンアップして上記のボードを使用する場合には、以下の操作が必要になります。

● wans ファイルの追加設定

wans ファイルに wan1～wan8 を「isdn」で登録する。

(例) wans ファイル

```
wan1        isdn
wan2        isdn
wan3        isdn
          :  (省略)
wan8        isdn
wan10       isdn
wan20       isdn
wan30       isdn
```

● 拡張 POC のバージョンアップ

新たなハードウェアを追加した場合は、OS のバージョンアップ行い、再起動した後に拡張 POC(自己診断テストプログラム)をバージョンアップする必要があります。
reboot コマンドに下記のオプションを指定することで自動的に拡張 POC のバージョンアップができます。
拡張 POC のバージョンアップは、readme.txt を必ず参照してください。

```
# reboot    /pocvup
```

(2) RIP を使用した ISDN 回線よるバックアップにおける不具合点の修正

RIP を使用して、本装置以外のルータ経由のルート(以下メインルートと呼びます)を、本放置に設定されている ISDN 回線経由のルート(以下バックアップルートと呼びます) でバックアップするシステム構成において、メインルートが RIP で通知されなくなり、本装置のバックアップルートにデータが流れる際、本装置が ISDN 回線経由のバックアップルートに対して自動発呼できない不具合点を修正しました。

Version3.1

Version3.1 では、下記の不具合修正を行っています。

(1)LAN 間接続で発呼が失敗する不具合の対処

LAN 間接続において発呼に失敗することがある不具合を対処しました。
本不具合は、Version3.0 で LAN 間接続の環境でのみ発生する可能性があります。

Version3.0

Version3.0 では、下記の機能追加と不具合修正を行っています。

(1) L2TP の対応

トンネリングプロトコルとして L2TP(Layer2 Tunneling Protocol:RFC2661) をサポートしました。

L2TP は、ダイヤルアップで利用されている PPP のパケットをそのままトンネリングすることができ、仮想リモートアクセスを提供することができます。
L2TP は、インタネットサービスプロバイダのアクセスポイントに設置される LAC(L2TP Access Concentrator)と、企業内に設置される仮想アクセスポイントである LNS(L2TP Network Server) との間でトンネルを作成します。

本装置は、LAC の着信接続の動作をサポートしています。

L2TP のサポートに伴い、下記の設定ファイルやコマンドが拡張されています。
設定ファイルやコマンドについての詳細な情報は、取扱説明書の PDF ファイルをダウンロードし参照してください。
http://www.sii.co.jp/js/nshp/product/index.html

●l2tp ファイル

新規に追加された L2TP の設定ファイルです。
バージョンアップ後、「clear -up」を実行することで l2tp ファイルが追加されます。
l2tp ファイルでは、L2TP の基本的な設定やトンネルを作成するための条件、詳細なトンネル情報を設定します。
また、l2tp ファイルで設定した内容は、reload コマンドで有効にすることができます。

●l2tpstat コマンド

L2TP で作成したトンネル／セッションの詳細な状態を表示するコマンドを追加しました。
現在接続されているトンネル／セッションの合計やトンネル／セッションごとの接続相手の情報、状態等を見ることができます。

(2) 二重ログインのチェック方法の変更

従来のバージョンでは、ユーザ名が同一でもプロトコルが異なる場合は、別のユーザとみなして着信を許可していました。
本バージョンから、プロトコルが異なっていてもユーザ名が同一の場合は、二重ログインとして着信を拒否するように変更しました。

(3) PIAFS の接続性の改善

一部の PHS 端末との PIAFS を使用した CBCP による callback において、接続できない場合がある点を改善しました。

(4) NS-341(PRI/DSP 拡張ボード)の初期化手順の訂正

NS-341(PRI/DSP 拡張ボード)BootROM の未使用ピンに対する初期化手順の誤りを訂正しました。

Version2.3

Version2.3 では、下記の機能追加と不具合修正を行っています。

(1) 自動発呼機能の不具合の対処

下記の4項目の条件を満たす環境で自動発呼ができない不具合を対処しました。
CLID 認証を利用した LAN 間接続の構成において本不具合が発生する可能性があります。

- NS-2484-10 の users ファイルにユーザ情報を登録する
- 自動発呼機能を使用する
- PPP 認証を行わず CLID 認証のみを使用する
- %user エントリに remote_name の設定を行わない

尚、Version2.2 をご利用の場合は、remote_name を設定することにより回避することができます。

```
[users ファイル]
  %user
        remote_name       sii
        remote_tel          03-1234-5678
            :
```

(2) 発着呼の衝突における不具合の対処

非常に希な現象ですが、発呼と着呼が衝突した場合に、自動発呼ができなくなる不具合を対処しました。
本不具合は、LAN 間接続の環境で発生する可能性があります。

Version2.2

Version2.2 では、下記の機能追加と不具合修正を行っています。

(1) RADIUS サーバによる CLID(発信者電話番号) 認証のサポート

RADIUS サーバを使用した CLID 認証を行う機能をサポートしました。
本機能を使用する場合、従来のローカルファイルで CLID 認証を行うための設定を users ファイルに行い、
さらに radius ファイルの%radius_auth 分類キーワードに以下の設定を行います。

```
[radius ファイル]
    %radius_auth
            clid_auth       on
```

上記設定を行うと、まずローカルファイルを使用して CLID 認証を行い、認証できなかった場合、RADIUS サーバに認証を行います。
このキーワードを記述しない場合、およびこのキーワードを off に設定した場合には、RADIUS サーバによる認証は行いません。

CLID 認証を RADIUS サーバに対して行う場合、NS-2484-10 は、ユーザ名に CLID を、またパスワードに"siipassword"を設定して RADIUS サーバに認証要求を発行します。このパスワードを変更したい場合には、radius ファイルの%radius_auth 分類キーワードに以下の設定を行います。
(以下の例では、CLID 認証におけるパスワードを"clidpassword"に設定しています)

```
[radius ファイル]
    %radius_auth
            ext_passwd      clidpassword
```

(2) RADIUS 認証用のデフォルトフィルタ設定機能のサポート

RADIUS サーバを使用して認証を行う場合に、RADIUS サーバから filter 情報が送られてこなかった場合に、NS-2484-10 にあらかじめ設定されているフィルタを設定する機能をサポートしました。

本機能を使用する場合、ipfilters ファイルに登録されているフィルタ名を radius ファイルの%radius_auth 分類キーワードに設定します。この例では、使用される interface に設定するデフォルトの filter を"filterDEF"、アクセスリストの include を"includeDEF"、アクセスリストの exclude を"excludeDEF"、出力フィルタを"outputDEF"に設定しています。

```
[radius ファイル]
    %radius_auth
            default_filter      filterDEF
            default_include     includeDEF
            default_exclude      excludeDEF
            defalut_outputfil   outputDEF
```

(3) 認証失敗時における RADIUS AccountStop の送信抑止機能の追加

PPP 認証が失敗した場合は、不正アクセス防止に役立つように AccountStop のみを RADIUS サーバへ通知します。本機能を抑止したい(認証が成功した時にだけ AccountStart/AccountStop を RADIUS サーバへ送信する)場合は、radius ファイルの%radius_acct 分類キーワードに以下の設定を行います。

```
[radius ファイル]
    %radius_acct
            stop_ignore         on
```

(4) SNMP のセッション管理用プライベート MIB のサポート

NS-2484-10 の現在のセッション情報およびセッションの統計情報などを SNMP を使用して取得するためのプライベート MIB として、ダイアルアップグループをサポートしました。

またこのダイアルアップグループでは、RADIUS アカウントサーバ用に生成された Acct-Session-Id を index として、SNMP からセッションを切断する機能をサポートしました。
本機能を使用することにより、NS-2484-10 内で確立しているセッションを、SNMP を使用して切断することが可能になります。

NS-2484-10 のプライベート MIB の詳細については、弊社ホームページの NS-2484-10 の FAQ をご参照ください。

(5) SecurID の Next Tokencode モード／New PIN モードへの対応

Security Dynamics 社のワンタイムパスワード製品である「SecurID」の Next Tokencode モード／New PIN モードに対応しました。
ただしこれらのモードを実行する場合、クライアントのパソコン上にネットマークス社のソフトウェア「ISDN Dialer」をインストールする必要があります。「ISDN Dialer」に関しては弊社にお問い合わせください。

(6) CLID が通知されない接続相手の切断機能のサポート

CLID(発信者電話番号) が通知されない接続相手からの着信を拒否する機能をサポートしました。
本機能を使用する場合、使用する WAN ポートに対応する isdn.wanXX ファイルに、設定します。

たとえば、WAN10 ポートに CLID が通知されない接続相手から着信した時にこれを拒否する場合、isdn.wan10 ファイルに以下の設定を行います。

```
[isdn.wan10 ファイル]
    clid_require                    on
```

(7) モデムの接続性の向上

回線品質が悪い環境における接続性を、若干改善しました。

(8) PIAFS のパフォーマンスの改善

比較的短かいフレームを回線速度(32Kbps あるいは 64Kbps) に近い速度で送受信した場合に、送信遅延がやや大きくなる現象を改善しました。

(9) オートリブート現象の改善

装置全体の負荷が高い状態で、TA／ルータとの接続／切断において、極まれに NS-2484-10 がオートリブートしてしまう現象について、Version 2.1 からさらに改善を行いました。

(10) HDLC 通信におけるショートフレーム受信の改善

TA／ルータとの HDLC 通信中に、NS-2484-10 が短いフレームを連続して受信した場合の、パフォーマンスの改善を行いました。
（たとえば、ネットワーク対戦型ゲーム「Unreal」において、ゲーム操作の応答性が悪い場合があり、この現象を改善できる可能性があります）

(11) SNMP の MIB2 の ipAdEntNetMask 値の取得に失敗する現象の修正

特定の条件で SNMP の MIB2 における ip アドレスグループの ip アドレステーブルの ipAdEntNetMask (1.3.6.1.2.1.ip(4).ipAddrTable(20).ipAddrEntry(1).ipAdEntNetMask(3)) 値の取得に失敗する現象を修正しました。

Version2.1

Version2.1 では、下記の機能追加と不具合修正を行っています。

(1) syslog の対応

NS-2484-10 内で発生したイベント(エラーメッセージ、トレースメッセージなど) を、syslog を使用してネットワーク上の他のホストに通知する機能を追加しました。
syslog への対応に伴い、syslog の動作を設定する syslog.conf ファイルが追加されました。
syslog.conf ファイルの設定方法、および syslog に出力されるメッセージについては、取扱説明書を参照してください。

ここでは、簡単な設定例を示します。
syslog を使用して、ホスト(172.16.1.3) にファシリティ local0 でエラーメッセージを通知する場合には、syslog.conf を以下のように設定します。

```
[syslog.conf ファイル]
    mode        on
    host        172.31.1.3
    facility    local0
```

(2) ProxyARP の機能強化

従来、ダイアルアップ接続において、PPP のアドレスネゴシエーションの結果相手端末に割り当てた IP アドレス(たとえば ippool ファイルに設定されている IP アドレスを相手端末に割り当てる場合など) が、使用する LAN インターフェースと同じネットワークに属するアドレスの場合のみ、ProxyARP で応答することが可能でした。

この ProxyARP の機能強化によって、相手端末に割り当てた IP アドレスが、使用する LAN インターフェースと異なるネットワークに属するアドレスの場合にも、ProxyARP で応答することが可能になりました。

本機能を使用する場合には、interface ファイルにおいて、ProxyARP 動作を実行させる LAN インターフェース(en0 あるいは en1) の設定に、以下の proxyarp キーワードの設定を追加してください。

```
[interface ファイル]
    interface   en0     */*     numbered
            proxyarp        on_demand       all
```

なお、proxyarp キーワードのパラメータには、auto、all、off の3種類あります。
このキーワードの設定を行わない場合、従来と同様の動作である auto がデフォルトとして設定されます。

auto ： 割り当てた相手 IP アドレスが、この論理インターフェース(この例では en0) と同じネットワークに属するアドレスの場合、ProxyARP で応答します。

all ： 割り当てた相手 IP アドレス全てに対して、ProxyARP で応答します。

off ： 割り当てた相手 IP アドレスに対して ProxyARP で応答しません。

(3) RADIUS 関連の機能追加1

RADIUS 認証サーバに送信する認証要求パケット(AccessRequest) に、Acct-Session-Id アトリビュートを格納する機能を追加しました。
デフォルトでは、Acct-Session-Id アトリビュートは認証要求パケットには格納されませんが、radius ファイルの radius_auth 分類キーワード(%radius_auth の部分) に、以下の set_session_id キーワードの設定を追加することによって、Acct-Session-Id アトリビュートを認証要求パケットに格納することができます。

```
[radius ファイル]
    %radius_auth
        set_session_id      on
```

(4) RADIUS 関連の機能追加2

RADIUS アカウントサーバおよび RADIUS 認証サーバに送信する Acct-Session-ID アトリビュートの表示方式を変更できるようにしました。
デフォルトでは、Acct-Session-Id は 16 進数表示ですが、radius ファイルの radius_acct 分類キーワード(%radius_acct の部分) に以下の base_session_id キーワードの設定を追加することによって、Acct-Session-Id を 10 進数表示にすることができます。

```
[radius ファイル]
    %radius_acct
        base_session_id      dec
```

(5) 着サブアドレスのチェック方法の変更

従来、ISDN からの着信時に、着サブアドレスが通知された場合、isdn.wanXX ファイル(XX=10,20,30) にサブアドレスが設定されていない場合には、着信を拒否していました。
本バージョンから、isdn.wanXX ファイルにサブアドレスが設定されていない場合には、着信を許可するように変更しました。
なお、isdn.wanXX ファイルにサブアドレスが設定されている場合には、従来と同様、設定値と比較し、一致しない場合には、着信を拒否します。

(6) ethernet の受信処理の改善

コリジョン発生後の ethernet からの受信フレームを、まれにエラーフレームとして処理する場合がある点を改善しました。

(7) PPP 認証時の CLID 認証の動作の改善

ローカル認証における PPP 認証時に、CLID 認証を行う設定(users ファイルの%user に「clid_auth must」を設定) を行った場合に、直前に CLID が通知されて CLID 認証が OK になったユーザが、CLID を通知しないで接続すると、接続できてしまう場合がある点を改善しました。

(8) 無課金コールバックの不具合点の改善

無課金コールバックが正常に動作しない不具合点を改善しました。

Version2.0

Version2.0 では、下記の機能追加と不具合修正を行っています。

(1) RIP／RIP2 の対応

ダイナミックルーティング機能として、RIP(Routing Information protocol) のバージョン 1、バージョン 2 をサポートしました。

それに伴い、下記の設定ファイルやコマンドが拡張されています。
設定ファイルやコマンドについての詳細な情報は、取り扱い説明書の PDF ファイルをダウンロードし参照してください。
http://www.sii.co.jp/js/nshp/product/index.html

● servers ファイル

初期設定では、RIP/RIP2 は動作していません。NS-2484 でRIP/RIP2 を動作させるには、routed を有効にする必要があります(/share/routed を追加する)。

```
        :
        :
/share/routed
```

尚、servers ファイルに設定を追加した場合は、必ず、再起動する必要があります。

● rip.conf ファイル

新規に追加された RIP/RIP2 の設定ファイルです。
バージョンアップ後、clear -up コマンドを実行することで rip.conf ファイルがセットアップカードに追加されます。

○ rip.conf ファイル設定例1

LAN1(en0)の RIP パケットは、RIP1,RIP2 パケットの両方を受信する。
送信は、RIP1 のブロードキャストで送信する。
NS-2484 の ISDN 側(ダイヤルアップユーザに割り当てするアドレス)のネットワークアドレス 172.31.0.0/16 を NS-2484 が RIP1(メトリック 2)で広告する。

```
interface              en0
  in                   both
  out                  rip1
destination  172.31.0.0/16   2
```

○ rip.conf ファイル設定例2

LAN1(en0)の RIP パケットは、RIP2 パケットのみを受信する。
送信は、RIP2 のブロードキャストで送信する。
NS-2484 の ISDN 側(ダイヤルアップユーザに割り当てするアドレス)のネットワークアドレス 172.31.1.0/24 を NS-2484 が RIP2(メトリック 2)で広告する。

```
interface              en0
  in                   rip2
  out                  rip2
destination  172.31.1.0/24   2
```

● netstat コマンド

ルーティングテーブルを表示する netstat -r コマンドを拡張しました。
RIP で取得した情報の属性には「RIP」と表示されます。

● ripstat コマンド

RIP の統計情報を表示する ripstat コマンドを追加しました。
ルートが変化した回数や RIP リクエスト、RIP レスポンスの回数等の統計情報を見る事ができます。

● riptrace コマンド

送受信した RIP パケットの内容をコンソールへ出力するコマンドです。
riptrace を実行することで送受信している RIP のバージョン、送信先/送信元の IP アドレスなどのトレースを取得することができます。

● reload コマンド

reload コマンドの対象ファイルを拡張しました。reload コマンドにより rip.conf ファイルの変更内容を再起動せずに有効にすることができます。

Version1.2

Version1.2 では、下記の機能追加と不具合修正を行っています。

(1) RADIUS サーバへの認証リクエストのアトリビュート追加

認証リクエスト(AccessRequest)に NAS-Port と NAS-Port-Type の Attribute を格納するように変更しました。

(2) アカウント情報(Connect-Info)の不具合の修正

RADIUS サーバへ送るアカウント情報の Connect-Info において、V.32bis の場合に送信スピードの表示がおかしい点(75 と表示される)を修正しました。

(3) ISDN 呼制御の改善

V.110 機能で TA から接続された場合に、確実に ISDN 呼制御レベルで拒否するように改善しました。

(4) モデムの接続性の向上

- LAPM(エラー制御)無効時の接続性の向上

  PC 側で LAPM(エラー制御)を無効にしている時に接続性が悪いことがあります。
  LAPM 無効時の接続性を改善しました。

- CONEXANT の HSF モデム(ソフトウェアモデム)の接続性の向上

  CONEXANT の HSF モデムで利用している回線の品質が悪い場合の接続性を向上しました。

- 古い ROCKWELL チップを使用したモデム(V.34)の接続性の向上

  古い ROCKWELL チップを使用した初期の 33.6Kbps 対応の V.34 モデムとの接続が時々失敗する点を改善しました。

- CirrusLogic 社チップを搭載したモデムの接続性の向上

  CirrusLogic 社チップを搭載したモデムの接続性を向上しました。

Version1.1

Version1.1 では、下記の不具合修正を行っています。

(1) DSP フロー制御の修正

DSP のフロー制御に問題があり、まれに Modem/PIAFS が接続できなくなる不具合を修正しました。

(2) phy パラメータの修正

interface ファイルで指定する phy パラメータが有効にならない不具合を修正しました。

以上