2026年1月30日

お客様各位

セイコーソリューションズ株式会社

NS-2250 システムソフトウェア Version 3.2 リリースノート

目次

Version 3.2　(リリース日：2026/1/30)

Version 3.2 では以下の機能拡張、不具合修正を行いました。

1　ポートサーバの両モード動作

direct モード/select モードを同時に動作させる機能を追加しました。
本機能の追加に伴い、コマンドのオプションパラメータ追加、一部コマンドの出力内容の変更があります。

2　command ログの syslog 転送

システムログ、ポートログに加え、NS-2250 で実行された command ログを syslog 転送できるようになりました。
また、本機能の追加に伴いコマンドのオプションパラメータ追加、一部コマンドの出力内容の変更があります。

3　拡張ユーザの権限追加

拡張ユーザ(extusr)に全ての show コマンドが実行可能な権限及び
既存の root 権限に加えて、portusr、verup グループの権限が追加可能になりました。
本機能の追加に伴い、コマンドのオプションパラメータ追加、一部コマンドの出力内容の変更があります。

4　RADIUS 認証の機能拡張

デフォルトユーザーグループの指定に normal を追加しました。
これによりグループを指定できないユーザは、normal(一般ユーザ)グループでアクセスが可能になりました。
また、RADIUS 認証サーバに送信するアトリビュートに Message-Authenticator を追加しました。
本機能の追加に伴い、コマンドのオプションパラメータ追加、一部コマンドの出力内容の変更があります。

5　Openssh V9.0 以降の scp コマンドへの対応

scp クライアントからファイルを put する場合、サイズ調整以外の要求を受け取った時には、何も処理を実施しないよう変更しました。

6　シリアルポートごとの最大セッション数の拡張

rw:2/ro:3 から rw:10/ro:5 に最大セッション数を拡張しました。
なお、装置全体の最大セッション数の変更はありません。

7　未使用ポートのクローズ

本体設定で disable telnetd かつ set portd session で telnet が全ての tty で指定されていない場合、ポート 23 番を CLOSE とするように変更しました。
また、ssh も同様に disable sshd かつ set portd session で ssh が全ての tty で指定されていない場合、ポート 22 番を CLOSE とするように変更しました。

8　ssh 暗号化方式の変更

version3.0 で追加した SSH サーバの暗号強度の設定を変更しました。
set sshd strong_encryption on 設定時に 3des-ctr の暗号化方式を無効化しました。

9　show sntp の状態を表示するコマンドを追加

show sntp の状態を分かりやすくするため show sntp detail コマンドを追加しました。

10　cmdchar を tty 先に送付する不具合の修正

tty 先へ接続した後、メニューに戻る際に利用する cmdchar コマンドが tty 先にも送信していた不具合を修正しました。

11　port_sshd が syslog に出力するメッセージの不具合修正

port_sshd が syslog に出力するメッセージが文字化けしている不具合を修正しました。

12　sshxpt でセッションが切断される不具合の修正

sshxpt で 8192 文字以上の文字列を入力すると、セッションが切断されてしまう不具合を修正しました。

13　show ipsec spd コマンドの表示結果が一部欠ける不具合の修正

show ipsec spd コマンドを実行した際に出力結果が一部欠けてしまう不具合を修正しました。

14　strongswan 脆弱性対応

以下の脆弱性に対応しました。

・CVE-2021-41991 キャッシュの署名のリプレースによる整数オーバーフローについての脆弱性

15 RESTAPI の脆弱性対応

以下の脆弱性に対応しました。

・CVE-2018-25103 細工した HTTP リクエストを受信する事により、http のデーモンがクラッシュ、メモリ内容を漏洩する可能性のある脆弱性。

Version 3.1.1　(リリース日：2023/10/6)

Version 3.1.1 では以下の不具合修正を行いました。

1　一部コマンドが実行できなくなる不具合の対処

本装置から SNMP Trap が大量に送信される環境で長期間使用した場合、write などの一部コマンドが実行できなくなる不具合を対処しました。
本不具合が発生した場合は装置を再起動することで復旧いたしますが、Trap が大量に発生することで不具合事象が再発いたします。
本不具合はシステムソフトウェアが v2.2、v3.0、v3.1 の場合に発生いたします。

Version 3.1　(リリース日：2022/11/18)

Version 3.1 では以下の機能拡張、不具合修正を行いました。

1　LLDP 機能の追加

LLDP を使用して本装置の情報を定期的に隣接装置に通知したり、隣接装置からの情報を収集できるようになりました。
本装置の LLDP 機能に関する仕様は下記の通りです。

項目		説明
機能有効化		enable lldp コマンドで機能を有効化します。 有効化すると eth1、eth2 で LLDP パケットを送受信します。 送信間隔は 30 秒です。 本機能は装置全体として有効/無効を設定します。
送信パケット(TLV)	Chassis ID	eth1 の MAC アドレスが使用されます。
	Port ID	eth1 から送信する場合は「eth1」、eth2 から送信する場合は「eth2」となります。
	Time To Live	120 秒です。
	Port Description	eth1 から送信する場合は「eth1」、eth2 から送信する場合は「eth2」となります。
	System Name	set hostname コマンドで設定したホスト名となります。
	System Description	SNMP の「sysDescr」と同じ値となります。 詳細は SNMP-MIB 説明書の「2.1.1 system(1)グループ」を参照して下さい。
	Management Address	インタフェイスに設定されている IPv4、IPv6 アドレスが 1 つずつ使用されます。インタフェイスの優先度は bond1、eth1、eth2 の順となります。 また、アドレス未設定の場合は未指定となります。
情報表示		以下 2 つの情報表示をサポートしています。 ・送信パケット情報 ・受信パケット情報(summary/detail)

また、本機能の追加に伴いコマンドの新規追加、一部コマンドの出力内容の変更がございます。
コマンドの詳細については「コマンドリファレンス」を参照してください。

2　SNMP プライベート MIB の追加

SNMP MIB で本装置のシリアル番号を取得することが可能になりました。
本機能追加に伴い、プライベート MIB NS-ENTITY-CS-MIB を追加しています。
NS-ENTITY-CS-MIB の詳細については「SNMP-MIB 説明書」を参照してください。

3　起動時に TCP ポート番号がデフォルト値となる不具合への対処

telnet/SSH/シリアルポートアクセスの TCP ポート番号の変更が設定ファイル(startup config)に保存されている状態で本装置を再起動した場合、ポート番号がデフォルト値で起動する不具合を対処しました。
本不具合の修正に伴い、ポート番号を変更した際の処理を見直しました。
本不具合は再起動後のシステムソフトウェアが v3.0 の場合にのみ発生いたします。

Version 3.0　(リリース日：2022/6/20)

Version 3.0 では以下の機能拡張を行いました。

1　REST API 機能の追加

REST API を使用して、本装置および本装置のシリアルポートに接続されている監視対象機器を操作することが可能になりました。
本機能の追加に伴い、http サーバ機能、https サーバ機能を追加しました。
また、拡張ユーザに root 権限を付与することが可能になりました。

REST API 機能を使用することで、以下の 2 つの機能が利用可能となります。

・CLI コマンド機能
設定変更や情報取得、コンソールログの取得と検索などを REST API で実行する際に使用します。

・コンソールアクセス機能
本装置のシリアルポートに接続されている監視対象機器に対して REST API でコマンドを実行する機能です。本機能は、tty マネージ機能を使用することで動作します。

また、本機能の追加に伴いコマンドの新規追加、オプションパラメータの追加、一部コマンドの出力内容の変更がございます。

2　tty マネージ機能の拡張

以下のコマンドのオプションパラメータを追加しました。

・ttysend コマンドの拡張
制御文字（0x00～1F、7F）と可視化文字（0x20～7E）を複数連続して送信できるオプション”hex”を ttysend コマンドに追加しました。

・ttylog コマンドの拡張
ポートログに指定した文字列が含まれるかどうかを検索するオプション”search”を ttylog コマンドに追加しました。

3　SSH サーバの機能拡張

SSH サーバの設定で、暗号強度がより強い方式を選択できるようになりました。
本機能の追加に伴い、set sshd strong_encryption コマンドを追加しています。また、一部コマンドの出力内容に変更がございます。

4　root 権限でログイン（外部認証）した場合に実行できないコマンドがある不具合の対処

外部認証を利用して root 権限でログインをした際、一部のコマンドが実行できない不具合に対処しました。

5　NETDEV WATCHDOG の対応

装置が高負荷な状態で稀に発生する NETDEV WATCHDOG によって、ネットワークインタフェースの通信ができなくなる問題に対処しました。

6　TCP タイムスタンプオプションの脆弱性の対応

以下の脆弱性に対応しました。

・CVE-2005-0356
TCP タイムスタンプオプションの不正なパケットによって TCP 接続をリセット可能な脆弱性

Version 2.2　(リリース日：2020/10/30)

Version 2.2 では以下の機能拡張、不具合修正を行いました。

1　SNMPv3 機能の追加

SNMP サーバからの Get 要求、およびトラップ送信について Version3 に対応しました。
MIB および TRAP の内容は、Version1/Versionv2(2c)と同一となります。

SNMP Version3 に関する本装置の仕様は下記の通りです。

項目	説明
認証アルゴリズム	HMAC-MD5-96/HMAC-SHA-96
暗号アルゴリズム	DES-CBC/AES128-CFB

また、本機能の追加に伴い下記のコマンドを追加/拡張しております。

コマンド	内容
set snmp engineid	SNMP Version3 の通信で通知される snmpEngineID を設定します。
set snmpuser name	SNMP Version3 で使用するユーザ、認証アルゴリズム、暗号アルゴリズムを設定します。
set trap manager	トラップの送信先やバージョンを設定します。バージョンに Version3 を指定可能となります。

2　IPv6 通信機能の拡張

IPv6 通信で利用可能な機能を拡張しました。
各システムソフトウェアのバージョンで、IPv6 をサポートしている機能は以下の表の通りです。

カテゴリ	機能	V1.3 以降	V2.2 以降
ポートアクセス機能	ポートサーバ機能	○	○
	ポートログ送信機能(SYSLOG/NFS/FTP/メール)	－	○
運用管理機能	DNS クライアント機能	○	○
	スタティックルーティング機能	○	○
	Telnet/SSH サーバ機能	○	○
	Telnet クライアント機能	○	○
	FTP/SFTP サーバ機能	FTP － SFTP ○	FTP ○ SFTP ○
	ボンディング機能	○	○
	SNTP クライアント機能	－	○
	SNMP エージェント機能	－	○
	SYSLOG クライアント機能	－	○
	FTP/TFTP クライアント機能	－	○
セキュリティ機能	各種サーバのアクセス制限(allowhost)	○ (ftpd 除く)	○
	RADIUS 認証/アカウント機能	－	○
	TACACS+機能	－	○
	Firewall(ip6filter)機能	－	○
	IPsec 機能	－	－

3　SNMP IF-MIB ifLastChange 不正な値を返す不具合への対処

ifLastChange の get 要求に対し、不正な値を返す不具合を修正しました。
本装置は ifLastChange をサポートしておりません。インタフェイスの種類にかかわらず、常に 0 を返す仕様です。

Version 2.1　(リリース日：2019/10/18)

Version 2.1 では以下の機能拡張、不具合修正、脆弱性対応を行いました。

1　SSH トランスペアレント接続機能(sshxpt)の追加

ポートサーバ機能に SSH トランスペアレント接続機能(sshxpt)を追加しました。
本機能は各シリアルポートに割り当てられた TCP ポート番号を SSH クライアントで指定することで監視対象機器と透過的な通信をする機能です。
運用自動化の管理ツール「Ansible」と連携する場合に、他社の Ansible モジュールを本装置経由で動作させることが可能です。

SSH トランスペアレント接続機能に関連する仕様は、以下の表の通りです。

項目	説明
機能有効化	set portd tty session コマンドで sshxpt オプションを指定することで、指定されたシリアルポートで sshxpt 用の TCP ポートが有効となります。
接続ユーザ	portusr グループのユーザを作成し、接続可能なシリアルポートを設定することで利用可能となります。
接続ポート	set portd sshxpt コマンドでサービスポート開始番号を変更することが可能です。 デフォルトのサービスポート開始番号は 9301 で、シリアルポートの数だけ連続して割り当てられます。
接続プロトコル	SSH でのみ接続可能です。telnet/console からの接続はできません。
接続時のアクション設定	set portd tty connted send_nl オプションを指定することで接続時に改行コードを送信します。

2　ポートサーバ機能、tty マネージ機能との排他機能の拡張

ポートサーバ機能のノーマルモード(rw)セッションと tty マネージ機能は、これまで排他制御が有効となる動作のみでしたが、設定により無効とすることを可能にしました。
set portd service exclusive コマンドで排他機能を設定します。
排他機能が有効(デフォルト)の場合、いずれかのセッションがすでに存在するシリアルポートへはアクセスできません。
排他機能が無効の場合、各機能のセッション同士に排他がかかりません。
検証や環境構築時には本機能のご利用によって、スムーズな操作を行うことができます。

3　tty マネージ機能の拡張

・show log ttymanage send コマンドの追加
tty マネージ機能にて、シリアルポートに送信した内容を確認するコマンドを追加しました。

・制御文字送信機能の追加
tty マネージ機能にて、制御文字を送信する機能を追加しました。
対応の制御文字は、[Ctrl-@](0x00)～[Ctrl-_](0x1f) および DELETE(0x7f)の全 33 種です。

4　SSH のプロトコルバージョン識別文字列の変更

SSH のプロトコルバージョン識別文字列を「SSH-2.0-port_sshd」に変更しました。

5　TCP ポートが意図せず開く不具合の対処

セレクトモードにて「set portd tty session」を実行後、特定の設定コマンドを実行した際に
ダイレクトモードの TCP ポートが開く不具合を対処しました。

6　tty マネージ機能で文字列が送信されない不具合の対処

tty マネージ機能で input オプション利用時に制御文字を入力すると、それ以降の文字列が送信されない場合のある不具合を対処しました。

7　Linux カーネル(TCP SACK PANIC)脆弱性の対応

以下の脆弱性に対応しました。

・CVE-2019-11477
改変された SACK シーケンスにより整数オーバーフローを引き起こし、Kernel Panic を引き起こす可能性がある脆弱性

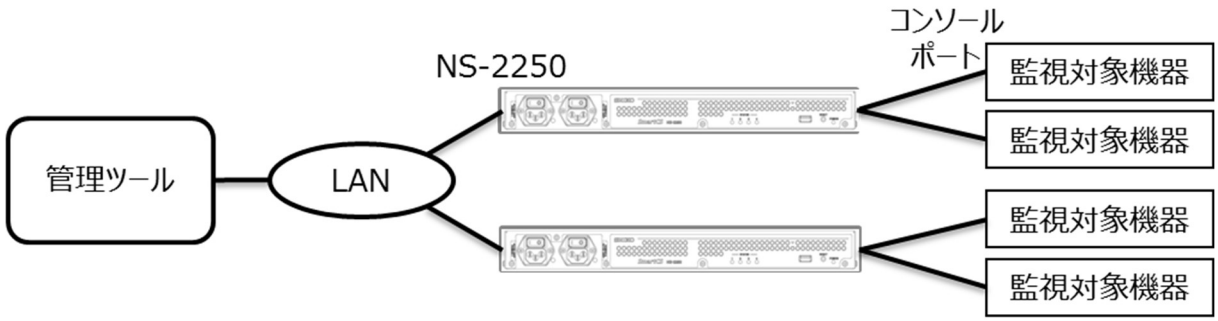
・CVE-2019-11478
改変された SACK シーケンスを送ることにより TCP retransmission(再送)キューにフラグメントを引き起こす可能性がある脆弱性

Version 2.0　(リリース日：2019/4/12)

Version 2.0 では以下の機能拡張、不具合修正、脆弱性対応を行いました。

1　tty マネージ機能の追加

本装置のシリアルポートに接続されている監視対象機器の設定変更や情報取得を行うことができる tty マネージ機能を追加しました。本機能を使用することで、外部 API や管理ツールと連携して監視対象機器を操作することが可能になります。
本機能を使用する場合、新たに追加された extusr グループに所属する拡張ユーザを作成し、tty マネージ機能を有効化してください。



tty マネージ機能に関連する仕様は、以下の表の通りです。

項目	説明
ユーザ	extusr グループのユーザを作成し、tty マネージ権限を付与することで利用可能となります。tty マネージ権限が付与されていない場合は、normal グループのユーザと同様の権限で動作します。 ttysend 等のコマンドを実行する場合は、ユーザがアクセス可能なシリアルポートを設定する必要があります。 ユーザの最大登録数は 10 です。(ユーザ ID:401～410)
機能有効化	enable ttymanage コマンドで、tty マネージ機能を有効化することで利用可能となります。
接続プロトコル	SSH でのみ接続可能です。telnet/console からの接続はできません。
コマンド	extusr グループのユーザでログイン後、ttysend 等のコマンドを実行することで監視対象機器に文字列を送受信することができます。 また ttylog コマンドを使うことで、ポートログの表示/削除を

	行うことができます。
監視対象機器への接続	1 つのシリアルポートに対して ttysend 等のコマンドは 1 つのみ実行することができます。
ポートサーバ機能のセッションとの排他	既にポートサーバ機能のノーマルモード(rw)セッションが存在する場合、tty マネージ機能では接続できません。tty マネージ機能によって該当のシリアルポートと通信中の場合は、ノーマルモード(rw)セッションが接続できません。 ただし、ポートサーバ機能のモニターモード(ro)セッションは排他の対象外となります。

2　コマンドの新規追加/オプションパラメータ追加

・disconnect コマンドのオプションパラメータ追加
disconnect コマンドで TCP セッションを切断する際に、端末デバイス番号を指定してセッションを切断できるよう、device オプションを追加しました。
show user login コマンドで端末デバイス番号を確認し、接続中の一般ユーザ、拡張ユーザ、装置管理ユーザのセッションを切断することが可能です。
・show ipinterface コマンドのオプションパラメータ追加
本装置のインタフェイス情報を個別に確認できるよう、インタフェイスを指定するオプションを追加しました。
・上述のコマンドの他にも、tty マネージ機能の追加等に伴いコマンドの新規追加、オプションパラメータの追加、一部コマンドの出力内容の変更がございます。

3　RTC 異常検出時のエラーメッセージを追加

本装置の RTC 異常を検出した際に、コンソールログにエラー情報を出力するよう変更しました。

4　Mail サーバのポート番号が削除されない不具合の対処

ポートログの送信先として登録した Mail サーバ設定を削除した際に、Mail サーバのポート番号が削除されない不具合を対処しました。

5　リソース枯渇の脆弱性の対応

以下の脆弱性に対応しました。

・CVE-2018-5391
細工されたパケットを受信することにより、CPU が高負荷状態に可能性がある脆弱性

Version 1.3 (リリース日：2017/4/14)

Version 1.3 では以下の機能拡張や脆弱性対応を行いました。

1 IPv6 通信機能の追加

IPv6 環境で運用できるよう、IPv6 通信機能を追加しました。
IPv4/IPv6 デュアルスタックに対応しており、IPv6 でサポートしている機能は以下の表の通りです。

カテゴリ	機能	サポート状況
ポートアクセス機能	ポートサーバ機能	○
	ポートログ送信機能(SYSLOG/NFS/FTP/メール)	－
運用管理機能	DNS クライアント機能	○
	スタティックルーティング機能	○
	Telnet/SSH サーバ機能	○
	Telnet クライアント機能	○
	FTP/SFTP サーバ機能	FTP －/ SFTP ○
	ボンディング機能	○
	SNTP クライアント機能	－
	SNMP エージェント機能	－
	SYSLOG クライアント機能	－
	FTP/TFTP クライアント機能	－
セキュリティ機能	各種サーバのアクセス制限(allowhost)	○
	RADIUS 認証/アカウント機能	－
	TACACS+機能	－
	Firewall(ipfilter)機能	－
	IPsec 機能	－

工場出荷時の設定では IPv6 通信機能は無効となっており、アドレスも設定されていません。
create ip6 コマンドで IPv6 通信機能を有効にした後に、set ip6addr コマンドで IPv6 アドレスを設定します。

2　telnet でポートアクセスした際の一部動作の仕様変更

セレクトモードでの利用環境において、create allowhost コマンドで telnetd/portd telrw/portd telro を指定せず、telnet 接続を拒否するよう設定した場合でもポートセレクトメニューを表示していましたが、
ポートセレクトメニューを表示しないように仕様を変更しました。

3　メール送信機能の仕様変更

ポートログをメール送信する際に、SMTP のヘッダに DATE/FROM データを挿入するよう仕様を変更しました。

4　traceroute コマンドの仕様変更

DNS サーバ設定時に、traceroute コマンドの出力結果内の IP アドレスをホスト名に逆変換して出力していましたが、IP アドレスで出力するように仕様を変更しました。
DNS サーバからの応答が無い場合に、タイムアウト時間が経過するまで traceroute の実行が待たされることが無くなります。

5　リモートからの DoS の脆弱性の対応

以下の脆弱性に対応しました。

・CVE-2017-5970
IP オプションを改変したパケットを受信することにより、カーネルがクラッシュする可能性がある脆弱性

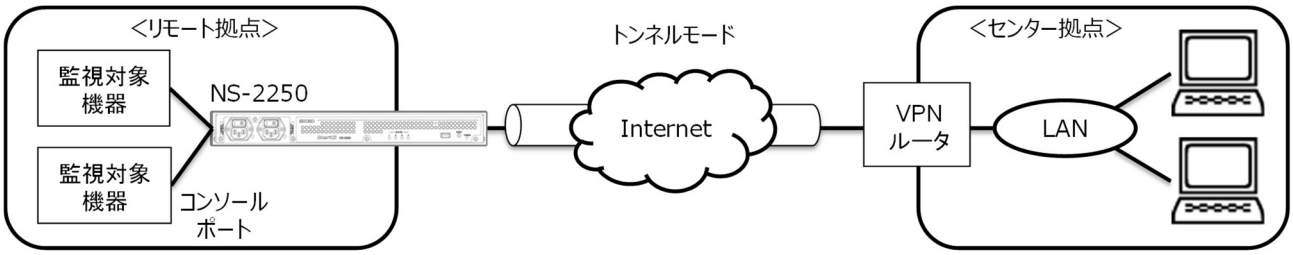
・CVE-2017-6214
リモートから URG フラグが立てられた TCP パケットを受信すると、無限ループに陥る可能性がある脆弱性

Version 1.2　(リリース日：2016/10/28)

Version 1.2 では以下の機能拡張や不具合修正を行いました。

1　IPsec 機能の追加

VPN ルータとの間で暗号化通信を行う IPsec 機能を追加しました。
IPsec 接続を要求するイニシエータと IPsec 接続を受けるレスポンダの両方に対応しています。
事前共有鍵(PSK)による暗号鍵認証をサポートしており、最大 8 コネクションの暗号化通信をトンネルモードで構築できます。



IPsec の接続形態や動作モード、設定可能なコネクション数は下表のとおりです。

項目	説明
接続形態	事前共有鍵(PSK)による暗号鍵認証
動作モード	トンネルモード
コネクション数	最大 8 コネクション 対向ネットワーク(サブネット)毎に IPsec コネクションを確立するための設定が必要
監視機能	DPD(Dead Peer Detection)によるトンネル通信断の検出
その他	NAT トラバーサル機能(ESP の UDP カプセリング)

本装置は以下の IKE ISAKMP-SA(Phase1)機能をサポートしています。

項目	説明
IKE プロトコル	IKEv1/IKEv2
暗号アルゴリズム	3DES/AES128/AES128CTR/AES256
認証アルゴリズム	MD5/SHA1
DH グループ	2(1024bit)/5(1536bit)/14(2048bit)
ISAKMP-SA の生存時間	3600～86400 秒(デフォルト 10800 秒)

本装置は以下の IPsec-SA(Phase2)機能をサポートしています。

項目	説明
暗号アルゴリズム	3DES/AES128/AES128CTR/AES256
認証アルゴリズム	HMAC-MD5/HMAC-SHA1
DH グループ(PFS 実施時)	2(1024bit)/5(1536bit)/14(2048bit)
IPsec-SA の生存時間	3600～86400 秒(デフォルト 3600 秒)

IPsec 機能とボンディング機能との併用はできません。

2 Firewall(ipfilter)機能の追加

強固なアクセス制限を行うために Firewall(ipfilter)機能を拡張しました。
本装置はインタフェイス受信部で動作するビルトインフィルタとカスタムフィルタの 2 種類をサポートしています。

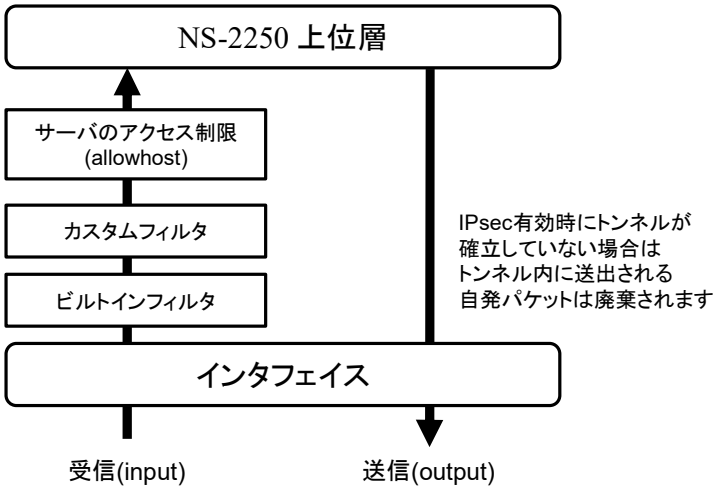
あらかじめシステムに登録されているビルトインフィルタは、Firewall 機能を有効にした時に
TCP-ESTABLISHED パケット/Related パケット/ループバックデバイスのパケットを透過します。
ビルトインフィルタの条件はユーザによる削除/変更はできません。

カスタムフィルタはインタフェイスの受信部で処理される、ユーザが設定可能なフィルタです。
カスタムフィルタは装置全体で最大 64 エントリの登録が可能です。

項目		説明
フィルタ種別	ビルトイン フィルタ(受信)	ビルトインフィルタは予めシステムに登録されているフィルタです。下記の受信パケットを透過します。 ・TCP-ESTABLISHED パケット Related パケット(TCP 以外で戻りが期待されるパケット (tftp/sntp/nfs(udp)/radius/icmp echo/IKE 等) ・ループバックデバイスのパケット Firewall 機能を有効にすると自動的に動作します(デフォルト無効) 。フィルタの削除や変更はできません。
	カスタム フィルタ(受信)	カスタムフィルタはインタフェイスの受信部で処理されるユーザが設定可能なフィルタです。 ビルトインフィルタの後で処理されます 装置全体で最大 64 エントリ登録できます。

フィルタ条件	インタフェイス	eth1: LAN1 ポート eth2: LAN2 ポート bond1: ボンディングポート
	IP アドレス	SA: 送信元 IP アドレス DA: 宛先 IP アドレス
	プロトコル	ICMP: ICMP タイプ(0-255) TCP: TCP ポート番号(1-65535) UDP: UDP ポート番号(1-65535) ESP: ESP プロトコル
	処理	accept: 透過 drop: 廃棄

Firewall(ipfilter)機能を有効にした場合、各フィルタは下図の順序で評価されます。



3 Telnet クライアント機能の拡張

本装置に搭載している Telnet クライアントのエスケープ文字を Ctrl+]固定から変更/無効化できるように機能拡張しました。
本機能拡張により、踏み台サーバ等を介した環境下で Telnet によるログインを何度も繰り返して利用する場合において、Telnet セッションの切断等の操作ができるようになります。
本機能拡張に伴い、set telnet cmdchar コマンドを追加しております。

4 MTU を設定する機能の追加

本装置のインタフェイスの MTU 値を変更する機能を追加しました。
本機能追加に伴い、set ipinterface mtu コマンドを追加しております。

5 Off-Path TCP Exploits 脆弱性(CVE-2016-5696)の対応

TCP プロトコルは RFC 5961 により DOS 攻撃に備えて Challenge ACK の送信量を制限するよう実装されています。
その制限を利用したコネクション切断やデータ注入の攻撃を受ける可能性がある脆弱性に対応しました。

Version 1.1.1　(リリース日：2016/7/8)

Version 1.1.1 では以下の機能拡張を行いました。

1　シリアルポートの DSR 信号遷移検出機能の拡張

シリアルポートの DSR 信号遷移検出方式にポーリング方式を追加しました。
従来の検出方式(edge)は、DSR 信号の遷移を厳密に検出しており、実際の対向装置の DSR 信号遷移以外にノイズなどのごくわずかな時間の信号遷移にも反応する場合があります。
新たに拡張した方式(polling)は、検出を緩やかに行い、DSR 信号の状態が OFF→ON 及び ON→OFF へ約 10 ミリ秒以上続いた場合に信号遷移を検出します。

本機能強化により、set tty detect_dsr コマンドに edge と polling オプションを追加しております。
本コマンドのデフォルトは off(無効)です。
on オプションを選択した場合のデフォルトは edge です。

```
set tty <ttylist> detect_dsr { on [{edge | polling}] | off }
```

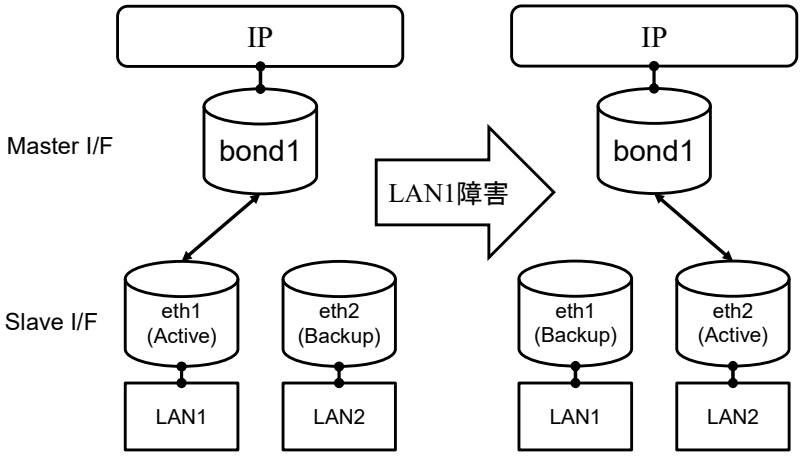
Version 1.1　(リリース日：2016/5/13)

Version 1.1 では以下の機能拡張や不具合修正を行いました。

1　ボンディング機能の追加

2 つの LAN ポートを仮想的に 1 つのポート(bond1)として動作できるよう機能拡張を行いました。
動作モードはアクティブ/バックアップ方式です。通信に使用するポートはアクティブポートのみで、バックアップポートから受信したパケットは内部で破棄されます。

ボンディング機能有効時、使用する IP アドレスは 1 つで bond1 のみに設定します。
アクティブポートとバックアップポートの切り替わりは、アクティブポートのリンクダウン検出による自動切り替えと、switch bonding コマンドによる手動切り替えの 2 方式をサポートしています。
リンクアップによる自動切り戻りはありません。
アクティブポート切り替え発生時には GARP を送出します。



2　シリアルポートのラベル名設定の仕様変更

set portd tty label コマンドで設定するシリアルポートのラベル名にスペースを使用できるよう仕様を変更しました。スペースを含む文字列の場合、ダブルコーテーションで囲んだ文字列で指定します。

3　trace icmp 機能の追加

radius/tacacs に加え icmp のデータをトレースできるように、trace コマンドのオプションに icmp を追加しました。

4 GNU C ライブラリ(glibc)脆弱性(CVE-2015-7547)の対応

GNU C ライブラリ(glibc)脆弱性(CVE-2015-7547)を対処しました。
旧システムソフトウェアで DNS サーバ設定をしている場合、以下のコマンドや処理において脆弱性の影響を受ける可能性があります。
脆弱性の影響を受けたパケットを受信した場合、スタックオーバーフローを起こし、コマンドや FTP 転送が異常終了する場合があります。

- ping/telnet/traceroute コマンド
- ポートログの FTP 送信

Version 1.0.3　(リリース日：2016/3/14)

Version 1.0.3 では以下の不具合を対処しました。

1　システムが再起動する不具合の対処

電源 ON や再起動により本装置を起動した後、約 100 日後に Watchdog Reset が発生し、システムが再起動する不具合を対処しました。

Version 1.0.2 (リリース日：2016/1/20)

Version 1.0.2 では以下の不具合を対処しました。

1 装置の時刻がずれてしまう不具合の対処

年に関係なく 10 月に下記のいずれかのコマンドを実行すると、装置の RTC(Real Time Clock)に不正な値が書き込まれ、12 月以降の装置起動で時刻がずれる不具合を対処しました。

- date もしくは date ntp コマンドによる時刻設定
- reboot コマンド
- shutdown コマンド

本不具合で RTC に不正な値が書き込まれても、12 月以降に装置を起動するまでの間は正しい時刻がシステムに適用されておりシステムの動作に影響はありません。
12 月以降に本装置を起動して時刻がずれると、コンソールアクセスなどの機能は正常に動作しますが、NS-2250 の内部ログや Syslog が不正な時刻になります。
NTP サーバから時刻を取得する設定をされていても、10 月に上記のコマンドを実行された場合は、次の再起動から NTP サーバから時刻を取得するまでの間は不正な時刻になります。

2 時刻変更の影響により、設定やログファイルが初期化される不具合の対処

装置起動時の日時よりも装置内部に保存されている下記ファイルへのアクセス(保存・参照)日時が新しい場合、対象ファイルが初期化されます。

- 本体内部の設定ファイル
- 本体のシステムログ
- シリアルポートのポートログ
- logsave コマンドによって保存されたポートログ

例えば装置起動後 write コマンドなどによって設定を保存したのち、date コマンドや NTP サーバのアクセスなどで本体のシステム時刻が大きく過去に戻された場合、設定ファイルのアクセス日時は修正された日時情報よりも未来のものになっています。本不具合は次回起動時に装置時刻よりもファイルアクセス日時が 1 日以上新しい場合ファイルを初期化してしまう不具合です。
なお USB メモリに保存されている設定ファイルは初期化されません。

3 時刻変更の影響により、システムが初期化される不具合の対処

装置再起動後に date コマンドや NTP サーバのアクセスなどでシステム時刻が大きく過去に戻されたのち、restore コマンドによるシステム復元を行うとコマンドがエラーとなり、restore コマンドにて指定した復元先(main/backup)のシステムが削除される場合があります。

Version 1.0.1　(リリース日：2015/10/23)

Version 1.0.1 では以下の機能改善や不具合修正を行いました。

1　起動時処理の改善

設定ファイルから読み込む際のコマンドチェック処理を変更し、起動時処理の時間を短縮しました。

2　echo コマンドの仕様改善

echo コマンドを起動時のみ実施されるものとし、通常の CLI(Command Line Interface)では何も表示しないよう仕様を変更しました。
設定情報を CLI から流し込む際に、設定に含まれる echo コマンドの出力が設定の妨げになることを防ぐ事ができます。

3　経路の異なる受信パケットを廃棄する不具合の対処

受信パケットのソース IP アドレスが受信 LAN ポートの経路情報に含まれていない場合、そのパケットを廃棄してしまう不具合を対処しました。

4　delete ip route の不具合を対処

同じ宛先で異なるゲートウェイのルートが複数設定されている場合、delete ip route コマンドでルートを削除すると、指定したルートと異なるルートを削除してしまう不具合を対処しました。

5　Telnet/SSH セッション上のコンソールログ出力が停止する不具合を対処

Telnet/SSH クライアントから本装置にログインし console on コマンドを実行してそのセッション上でコンソールログを出力している場合に、新規の SSH 接続で認証に失敗すると、Telnet/SSH セッション上のコンソールログ出力が停止してしまう場合がある不具合を対処しました。

以上