Si−R570 V34.00 変更内容一覧

□機能追加・改善

No.	項目	1:追加内容
1	IPv6 Ready Logo Phase2認定取得	IPv6 Ready Logo Phase2認証取得申請中。
2	IPv6 DHCP機能の拡張	PDクライアント機能のlan対応、取得パラメタ追加を行いました。 リレー機能を追加しました。 サーバ機能のlan対応、IPv6アドレスの配布、配布パラメタ追加を行いました。
3	IPv6 VRRP機能	IPv6対応するため、VRRP v3機能を追加しました。
4	BGP IPv6機能	BGP4でIPv6機能をサポートしました。 ※ Si-R570において、BGP4でIPv6機能を使用する場合は、拡張用512Mメモリモジュールが必要です。
5	ログインアカウント改善	admin, user以外にログインアカウントを追加登録できるようにしました。ただし、複数アカウントでの同時ログインはできません。また、RADIUS機能を利用してアカウントを管理することが可能です。
6	LLDP機能	LLDP機能を追加しました。LLDP(Link Layer Discovery Protocol)とは、自装置情報を広報することにより隣接装置の把握や接続状態の確認などを目的とした隣接探索プロトコルです。
7	SNMP機能の拡張	SNMPv3の認証および暗号機能を追加しました。 SNMPv3のアクセス制御機能を追加しました。
8	IEEE802.1X認証機能	IEEE802.1X に準拠した認証機能(802.1X認証)を追加しました。本装置では、1 つの物理ポートで複数の端末を認証できます。この場合、本装置の物理ポートにスイッチングHUBなどを接続し、そこに複数の端末を接続して、それぞれの端末で認証を行う運用が可能です。
9	ARP認証機能の改善	・認証失敗端末の送信を妨害するためのARPパケットを定期的に送信する機能を追加しました。 ・認証成功時のシステムログを追加しました。 ・端末のIPアドレス変更時の再認証機能を追加しました。 ・IPアドレスを指定して認証を許可する機能を追加しました。 ・認証プロトコルはCHAP固定でしたが、PAPも指定できるようにしました。
10	MACアドレス認証／DHCP MACアドレスチェック機能の改善	・認証プロトコルはPAP固定でしたが、CHAPも指定できるようにしました。
11	PKI-VPN機能	PKI-VPN機能として、IKEフェーズ1の相手認証にRSAデジタル署名認証を使用したIPsec接続機能を追加しました。
12	動的VPN機能の改善	remoteを用いてHUB拠点(本社、センターなど)と接続する運用において、HUB拠点のネットワークを増設した場合に、不要なINVITEを送出しないために全拠点に対しignore条件のINVITEルールを設定する必要がありました。INVITEルールを指定されたremoteにおいては、動的VPN接続時に相手ネットワークの情報を自動的にignoreルールに加えるよう機能改善を行いました。
13	マルチキャスト機能の拡張	ランデブーポイント(RP)を静的に設定できる機能を追加しました。
14	BGP機能の拡張	・4 Octet AS AS番号枯渇問題に対応するため、ASフィールドを4オクテットに拡張しました。 ・フィルタ変更時のセッション維持 従来、経路フィルタ変更時にBGPセッションを開放していましたが、そのまま維持するよう改善しました。
15	NAT機能の拡張	設定によりNAT変換テーブル数を拡張できるようにしました。本装置のNAT変換テーブル数については取扱説明書「仕様一覧」のシステム最大値一覧を参照してください。 なお、OSPF、BGPを使用する場合、NAT変換テーブル数の拡張は行えません。

□修正内容

No.	影響範囲	内容
1	V31.01～	ハードウェアエラーログのFlashへの書き込みが正しく行われない場合がある。
2	V21.02～	LANFiberスロット(SFPオプションモジュール用スロット)のポートがリンクアップ状態にならないことがある。
3	V21.02～	Si-R570を使用したATMメガデータネッツ網での通信においてpingロスが発生することがある。
4	V21.02～	show ip bgp routeコマンド実行すると、BGP経路情報内表示で無効な経路が有効経路として表示されることがある。
5	V21.02～	本装置が同一ネットワーク内の複数のルータとBGP接続する環境において、誤って本装置が自アドレスをnexthopとする経路情報を広報する場合がある。このため、本装置を経由しなくてよい運用トラフィックを本装置が中継してしまう。
6	V32.00～	動的定義でBGPのTCP-MD5認証鍵を設定追加しても、この認証鍵が有効にならない場合がある。
7	V21.02～	1台の装置内で複数インタフェースに包含関係にあるIPアドレス(例えば、192.168.0.0/16と192.168.1.0/24)が設定された環境でE-BGPを使うと、次の事象が発生することがある。 ・BGP未使用インタフェースのリンクダウン契機で別インタフェースのBGPセッションがダウンする ・BGP使用中インタフェースのリンクダウン契機でそのインタフェースを使って確立中のBGPセッションがダウンしない。
8	V32.00～	BGP TCP-MD5認証の認証鍵を動的に変更すると、BGPセッションが再接続できなくなることがある。
9	V33.00～	BGPグレースフルリスタート機能を使用すると、相手装置でBGP内部状態矛盾となる場合がある。
10	V33.00～	BGPで10以上の経路情報を送信する構成でグレースフルリスタート機能を使用するとシスダウンする場合がある。
11	V21.02～	Router Advertisementメッセージ(RA)関連設定を動的定義変更しても、RAパケットを即時送信しない場合がある。このため、10分(デフォルト値)後にRAが送信されるまで、PC等のRA受信装置側の設定が変更されない。
12	V30.00～	マルチNATを使用した回線(PPPoE等)で、運用中の回線断および再接続後に一定期間動的VPN接続できなくなる場合がある。
13	V21.02～	IKEネゴシエーションにおいて、送信パケットのIKEネゴシエーションペイロード内のRESERVED fieldに0以外の値を設定し相手へ送信する場合があり、IKEネゴシエーションに失敗する場合がある。 ※Si-Rシリーズルータが、IKEネゴシエーションペイロード内のRESERVED fieldに0以外の値が設定されたパケットを受信した場合、invalid RESERVED field.のsyslogを表示する。
14	V31.00～	相手装置からLifebyteを含むRESPONDER-LIFETIME通知パケットを受信すると、内部資源解放漏れが発生する。このパケットはIPsec／IKEネゴシエーション時に受信することがあり、装置起動後に通算10万回(*1)以上受信すると、内部資源枯渇によって装置が再起動することがある。また、本事象はSi-Rルータ同士の接続では発生しない。 *1:回数は機種および運用構成により異なります。Si-R180B:3万回、Si-R220C/240B/260B:6万回、Si-R370:10万回、Si-R570:55万回以上を目安としてください。
15	V32.00～	接続先情報設定に、動的VPN設定とPPPoE回線設定がある状態で運用中、PPPoE回線断が発生すると、そのPPPoE回線を利用しない接続先情報の動的VPNが切断される。

16	V30.00～	NATを使用した複数のインタフェースが存在する動的VPN環境において、動的VPN接続によるIKE経路情報が追加される前にIKEネゴシエーションパケットを受信すると動的VPN接続が失敗する場合がある。
17	V33.00～	IPsec/IKE定義反映(主に動的VPNクライアント定義)エラーのsyslogメッセージが不適切な場合がある。
18	V33.00～	テンプレートを使用した動的VPN定義でアドレスファミリの異る動的VPNサーバ情報を複数設定して定義反映を行うと、システムダウンする場合がある。
19	V33.00～	標準MIB：ipSystemStatsInHdrErrorsが正しくカウントされないことがある。
20	V21.02～	sshでログインして最初にTABキーを入力すると、コマンド一覧ではなくコマンド説明あるいはコマンド形式が表示される場合がある。
21	V21.02～	sshでの自動ログアウトやコンソールログインによる排他ログアウト後に、再びsshでログインすると接続が拒否されたりログインできてもコマンド実行するとコマンドが終了しない場合がある。ssh接続が拒否された場合はsshにて再ログインすれば問題ない。sshログイン後のコマンド実行が終了しない場合は、装置再起動するまで継続し、この間telnetやftpでの接続、WEB設定操作はできない。
22	V21.02～	TCPパケットがTCPオプション部の途中でフラグメントされていた場合、正常なフラグメントに関わらずIPフィルタでoverlap fragmentと検出され破棄される。
23	V30.00～	IPv6フィルタ設定があり、かつフラグメントされたIPv6パケットがACLルールにより透過条件に合致した場合、統計情報のpass(static)の数値が正しくカウントされない。
24	V21.02～	lan vlan bind設定を有効にしたLAN/スイッチインタフェースにて、lan bind定義または、bind先lan定義を変更するとVRRPの不要な切り替わりやマスタ状態遷移の繰り返しが発生する場合がある。
25	V30.00～	VRRP定義をLAN定義番号が小さいLANへ移動させた場合に、VRRPグループがマスタ状態へ遷移しない場合がある。または、マスタ状態へ遷移しても仮想MACあて転送が行われない場合がある。
26	V33.02～	WEB画面から相手情報-接続先情報(IPsec/IKE)-接続制御情報において、接続先監視が設定できない場合がある。
27	V33.02～	Web画面の相手情報設定画面でIPsec情報(自動鍵)を設定／保存すると、必ずSA有効時間の設定誤りエラーとなる。なお、エラーメッセージは表示されるが、設定値が正しい設定可能範囲であれば、装置へ反映されている。
28	V21.02～	templateを使った通信環境において、構成定義の復元や設定再投入後のcommit操作を実行すると、以後templateを使って通信が正しく通信できない場合がある。
29	V21.02～	template着信を利用した不特定相手着信時に、相手装置に割り当てるIP addressのプールが枯渇し、通信できなくなる場合がある。
30	V21.02～	ISDNを利用したtemplate接続において、aaa情報に相手経路が存在し、かつ10万回(*1)以上のPPP認証が実施された場合、システムハングまたはシステムダウンが発生する場合がある。 *1：回数は機種および運用構成により異なります。Si-R180B：3万回、Si-R220C/240B/260B：6万回、Si-R370：10万回、Si-R570：55万回以上を目安としてください。
31	V21.02～	フラグメントパケットが、選択されるべきap以外から送出される場合がある。
32	V21.02～	show ip multicast pimsm rpコマンドの表示結果にRPの適用グループが正常に表示されない.
33	V21.02～	scheduleコマンドで装置再起動時にresetコマンドを実行するようスケジュール設定すると、装置が再起動リセットを繰り返し正常に起動しなくなる。本件は、誤った設定を投入した時に発生する。
34	V32.00～	MACアドレス認証用パスワードやWired Equivalent Privacy(WEP)暗号キーに不正な値を指定してもエラー表示されないことがある。この場合、エラー表示されないだけであり、設定値は無効扱いとなる。