

Si-R220C V35.00 変更内容一覧

□機能追加・改善

No.	項目	内容
1	無線LAN管理機能	弊社製の無線LANアクセスポイント機器(SR-M20AP1)を対象とした以下の無線LAN管理機能を追加しました。 1)アクセスポイントモニタリング機能 - アクセスポイントをグループごとに設定、操作、状態表示を可能とします。 2)周辺アクセスポイント検出機能 - 無線LANの電波を監視し、周辺に存在するアクセスポイントを検出します。 3)クライアントモニタリング機能 - 無線LANの端末および電波強度を監視します。 4)MACアドレスフィルタ配布機能 - 管理無線LANアクセスポイントでの無線LAN端末の接続可否を制御するMACアドレスフィルタリングを集中管理し配布します。 5)電波出力自動調整機能 - 管理無線LANアクセスポイントの無線送信出力を自動的に調整します。 6)装置リセット機能 - 管理無線LANアクセスポイントをリセットします。 7)チャネル自動調整機能 - 管理無線LANアクセスポイントの無線LANモジュールに対して、最適な空チャネルまたは無線受信強度が比較的弱いチャネルを自動的に割り当てます。
2	外部メディアスタート機能	装置起動時に外部メディア(USBメモリ)に格納されたファームウェアおよび構成定義を使った自動更新を可能としました。本操作は、操作用PCを使わずに実行できます。
3	コンフィグトライアル機能	commitコマンドによる、構成定義反映の有効時間を指定可能としました。
4	シスログ機能強化	以下の改善を行いました。 1)RFC3164にて推奨されている、ホスト名(またはIPアドレス)とタイムスタンプをシスログメッセージのヘッダ部に設定できるようにしました。 2)認証機能メッセージのイベント毎制御 IEEE802.1X認証/ARP認証について、認証成功/認証失敗/認証解除(解除はIEEE802.1X認証のみ)のシスログメッセージの出力有無をイベント毎に選択できるようにしました。
5	IKE機能の拡張	鍵交換としてのIKEv2機能を追加しました。
6	IPsec機能の拡張	1)IPsec v3に対応しました。 2)IPsec DPD(Dead Peer Detection)機能 - RFC3706に基づいたIPsecトンネルの通信断を検出できるように対応しました。 3)拡張IPsec機能の改善。 - 複数の接続先(ap)情報に拡張IPsec対象範囲設定した場合に、それぞれの接続先情報でIKEネゴシエーションが行えるよう機能改善します。
7	VPN機能の拡張	- 動的VPNインタフェースのバックアップ ルータ1台でのバックアップ構成を可能とするために動的VPNインタフェースの複数指定をサポートし、動的VPNインタフェースでのバックアップ構成を組めるように対応しました。
8	シェーピング機能の改善	lanインタフェースに実装されているシェーピング方式は、rmtインタフェースに実装されているシェーピング方式と比べると精度が劣るため、これをlanインタフェースにも実装することでlanインタフェースのシェーピング精度の改善を行いました。
9	Si-R Security Softwareバージョン変更	IKEv2、IPsecV3対応を行うためにSi-R Security Softwareの対象範囲であるソースコードに変更が生じたため、Si-R Security SoftwareバージョンをV02.03→V03.00へアップしました。

□修正内容

No.	影響範囲	内容
1	V32.03 ~ V34.02	Si-Rシリーズ装置がDHCPサーバとして動作中に配布済IPアドレスに対して、端末から“DHCP DECLINE”を受信するとDHCPサーバは以後装置再起動までそのIPアドレスでの配布をしなくなる。
2	V32.03 ~ V34.02	相手装置からSIPのINVITE要求を受信して動的VPN接続を行う場合にSIPセッション確立後、IKEネゴシエーションが行われず、SIPセッションが確立された状態のまま通信不能になる場合がある。
3	V32.03 ~ V34.02	情報交換セッションの開始メッセージ(INVITE要求)をリダイレクトしたことを示すシステムログの「情報交換の着側ユーザID」にリダイレクト先URIが表示される。
4	V34.00 ~ V34.02	本装置にftp接続し、一度ログインに失敗したあと、同じ接続で再びログインを試みた場合、ログイン成功あるいは失敗のシスログに接続元IPアドレスが表示されない。
5	V32.03 ~ V34.02	IPv6リンクローカルアドレスを宛先として本装置にftp接続すると、関連するシスログ表示内の接続元アドレスのインタフェース名に%が2つ表示される。
6	V32.03 ~ V34.02	IPv6リンクローカルアドレスしか持たないPCから、本装置のIPv6グローバルアドレスにftp接続すると、ログイン/ログアウト時のシスログ表示内の接続元アドレスに「%インタフェース名」が付加されない。
7	V34.00 ~ V34.02	terminal prompt login コマンドで任意のログイン入力プロンプト文字列を設定しても、電源投入直後やリセット直後に 未設定時の表示“Login: ”が表示される。
8	V34.00 ~ V34.02	ftp接続でログイン後、userコマンドで不正なユーザ名あるいはパスワード入力でユーザ認証に失敗しても、ログイン成功のシスログが出力される。
9	V32.03 ~ V34.02	コンソールで表示コマンドを連続入力すると、ネットワーク通信が遅延し、VRRP切替えが発生するなどの影響が出る場合がある。
10	V33.00 ~ V34.02	表示量が多いコマンドでページャ(terminal pager enable設定 あるいは moreコマンド)を利用すると、ネットワーク通信が遅延する場合がある。
11	V32.03 ~ V34.02	ページャ機能有効時、コンソールで1画面未満の出力をする表示コマンドを連続入力すると、ネットワーク通信が遅延し、VRRP切替えなどが発生する場合がある。
12	V32.03 ~ V34.02	本装置にtelnet接続してユーザ認証に失敗した後の3秒間で8フレーム以上受信すると3秒間経過までの間、通信が停止する場合がある。

13	V32.03 ~ V34.02	コマンド設定またはWeb設定操作にて設定したIPアドレスのブロードキャストアドレス指定が、LAN 情報 (物理LAN)] → [IP 関連] → [IP アドレス情報] にて設定画面表示に反映されない。
14	V34.01 ~ V34.02	clear ip nat statistics や clear statistics コマンドで表示される NAT 統計情報中の "same node" カウンタがクリアされない場合がある。
15	V32.03 ~ V34.02	NAT 使用時に、ICMP メッセージに対するエラーメッセージを装置が受信したとき、システムダウンする場合がある。
16	V33.00 ~ V34.02	AAA/Radius 接続の Main Model において、併用できない NAT トラバーサル 定義を有効にすると誤って 4500 番ポートがオープンする。
17	V32.03 ~ V34.02	remote 定義の動的 VPN にて show ike statistics interface コマンドで統計情報が表示されない。
18	V33.01 ~ V34.02	IPsec/IKE 接続で keep connect 設定時にシステムダウンする場合がある。
19	V32.03 ~ V34.02	動的 VPN サーバが存在しない環境で次の事象が発生することがある。 ・動的 VPN 接続に関する remote ap keep 設定にて keep connect 適用後、keep off へ変更すると停止すべき動的 VPN 接続要求 (DVPN_ACQUIRE) パケットが不在サーバへ再送され続ける。 ・動的 VPN 接続に関する remote ap keep 設定にて keep connect 適用後、接続 (online remote コマンド) を契機に起動された動的 VPN 接続要求の再送動作が、その状態で閉塞 (offline remote コマンド) を投入しても止まらない。
20	V32.03 ~ V34.02	remote ip dvpn autoignore および remote ip6 dvpn autoignore 設定した接続先からのパケットを大量に受信後、INVITE 対象のパケットを受信しても INVITE を送出しないことがある。
21	V33.02 ~ V34.02	ISDN 回線相当の低速帯域を使い、リモートよりブラウザ経由にて設定を行うと、設定反映ボタンを押すと「設定反映中です。>>>」の画面が続きエラーが表示される。
22	V32.03 ~ V34.02	本装置を DHCP サーバとして使う運用において、本装置から端末へ送信される DHCP 応答パケットに含まれる送信元 MAC アドレスがすべて先頭 LAN ポート (lan 0) の MAC アドレスになる。
23	V34.00 ~ V34.02	ARP 認証不要 IP アドレスが設定された端末に対して、誤って ARP 認証を行う場合がある。
24	V32.03 ~ V34.02	IEEE802.1X 認証状態表示コマンド (show dot1x port) の表示内容に次の不正な表示がある。 1) 認証端末の切断後、show dot1x port にて切断した端末のユーザ名情報が表示される 2) 複数のサブクライアント接続時に show dot1x port コマンドで表示される、認証成功/失敗回数が該当ポートの累積回数になっている。
25	V32.03 ~ V34.02	本装置が DHCP クライアントとして動作する環境において、DHCP サーバからの DHCP-ACK メッセージを受信すると Gratuitous ARP を 2 度送信する。
26	V32.03 ~ V34.02	本装置が DHCP クライアントとして動作する環境において、電源投入時の時刻情報自動設定が正常に動作しないことがある。
27	V33.00 ~ V34.02	ARP 認証で認証失敗した端末が VLAN を移動すると、通信妨害が行われないことがある。
28	V34.00 ~ V34.02	通信速度 10Mbps で link-up した LAN ポートに対して、送信データが滞留するようなデータ送信負荷がかかった場合、装置性能内の通信負荷であっても、すべての LAN ポートにおいて受信パケットをロストする場合がある。
29	V32.03 ~ V34.02	動的 VPN 機能を使った運用構成において、装置電源投入後にシステムダウンすることがある。
30	V32.03 ~ V34.02	IPsec/IKE 機能を使う運用環境にて show ike trace コマンドを実行するとシステムダウンまたは、トレース情報の表示がされない場合がある。