Si-R220C V35.01 変更内容一覧

□機能追加・改善

No.	項目	内容
1	無線LAN管理機能改善	1)管理無線LANアクセスポイント(SR-M20AP1)の以下のV2版ファームウェア機能に対応しました。 ・show nodemanager logging wlanコマンドのIEEE802.11n規格表示対応 ・無線LANチャネル自動設定のIEEE802.11n規格対応 2)システムログメッセージ追加 以下のイベントについて監視ログだけでなくシステムログメッセージの出力を追加しました。 ・管理機器の消失検知 ・不明無線LANアクセスポイントの初回検知 ・不明無線LANアクセスポイントの消失検知
2	縮退機能追加	運用中に下記以外のハードウェア異常を検出したとき、装置をシステムダウンさせて縮退モードに遷移させるかどうかを選択可能にしました。 ・冷却ファン異常 ・温度異常 ・電源異常
3	RADIUS機能改善	IEEE802.1X認証時のAccessRequestパケットにNAS-IP-Addressアトリビュートを追加しました。

□修正内容

No.	影響範囲	内容
1	V34.00 ～ V35.00	動的VPNのINVITE自動ignore機能において、抑止されるべき動的VPN接続要求(INVITE)が発行される場合がある。
2	V35.00 ～ V35.00	IPsec/IKE(v1)のAggressive Modeにおいて、User-FQDNを受信するとID不一致によりIKEネゴシエーションが失敗する場合がある。
3	V32.03 ～ V35.00	弊社Si-Rシリーズ以外の装置との間でIPsec/IKEを使用して接続する運用環境において、IKEネゴシエーション実行中に装置がシステムダウンする場合がある。
4	V35.00 ～ V35.00	IPsec/IKEの動的VPN接続において、IKEネゴシエーション中にDead Peer Detection(DPD)生存確認の再送が発生するとメモリリークが発生し、5万回以上再送が発生すると装置がシステムダウンする場合がある。
5	V35.00 ～ V35.00	IPsec/IKE接続において、相手とのセッション開設に失敗するとメモリリークが発生し、累計5万回以上失敗すると装置がシステムダウンする場合がある。
6	V35.00 ～ V35.00	IPsec/IKEのテンプレート(AAA/RADIUS)接続において、Radius認証時に相手からIKEネゴシエーションパケットの再送が発生すると装置がシステムダウンする場合がある。
7	V35.00 ～ V35.00	IPsec/IKEのテンプレート(AAA/RADIUS)接続において、回線切断時またはtemplate定義変更時に装置がハングアップする場合がある。
8	V35.00 ～ V35.00	IPsec/IKEのテンプレート(AAA/RADIUS)接続において、IPsec/IKEの接続/切断時を累計3千回以上繰返すと装置がシステムダウンする場合がある。
9	V32.03 ～ V35.00	IPsec/IKEのAggressive Modeのレスポンダとして動作するとき、PPPoE回線切断時にIPsec SAが解放されないことがある。この事象は、通信等の運用動作への実質影響はなく、表示コマンドで不当な内容が表示される。
10	V35.00 ～ V35.00	IPsec/IKE 1対n構成でAggressive Modeを使用した通信において、2番目以降のIPsec SAが正常に確立できないことがある。
11	V32.03 ～ V35.00	IPsec/IKE 1対n構成での通信において、IKEセッション監視ダウンで全てのIKE/IPsecSAが解放されない場合がある。発生拠点においては、IKE/IPsec SA更新時間満了後、VPNセッションの開設やVPN通信が復旧する。本事象は、他の拠点へのVPNセッションの開設やVPN通信に影響を与えることはない。
12	V33.00 ～ V35.00	IPsec/IKEのAggressive Modeにおいて、Responder設定でIPsec/IKE接続後、IPsec SA更新時間満了となりIKE SAのみとなった状態の時に閉塞してもIKE SAが解放されない。発生拠点においては、IKE SA更新時間満了後、VPNセッションの開設やVPN通信が復旧する。本事象は、他の拠点へのVPNセッションの開設やVPN通信に影響を与えることはない。
13	V35.00 ～ V35.00	IPsec/IKEの定義において、remote ap ipsec ike encrypt aes-cbc(鍵長指定なし)を設定すると、IKE Phase2でネゴシエーションに失敗する。
14	V35.00 ～ V35.00	IPsec/IKEのNATトラバーサルを使用した構成において、VPN Clientとの接続がIKEネゴシエーション失敗となることがある。
15	V33.00 ～ V35.00	IPsec/IKEのNATトラバーサルが有効とならない構成において、NATトラバーサル定義の変更を行うとIPsec/IKE SAが解放される。ただし、何らかの通信が発生した時点で IPsec SAが再作成されるため、通信は問題なく継続される。
16	V33.00 ～ V35.00	IPsec/IKEの定義において、接続先情報の動的VPNとテンプレート情報の動的VPN定義が同一動的VPN Client定義を参照して運用しているとき、接続先情報の動的VPN定義を変更(datalink typeなど)すると定義重複エラーのsyslogが出力される。
17	V32.03 ～ V35.00	IPsec/IKEの定義において、接続先情報に動的VPNやAHプロトコルを設定し、かつ、NATトラバーサルを有効にすると、不要なNATトラバーサル用ポート(4500番)がオープンされる。
18	V33.00 ～ V35.00	IPsec/IKEの定義において、セッション監視を追加して動的構成定義変更したとき、セッション監視の宛先が到達不可の場合にIPsec SAがダウンタイマで解放されないことがある。発生拠点においては、IPsec SA更新時間満了後、VPNセッションの開設やVPN通信が復旧する。本事象は、他の拠点へのVPNセッションの開設やVPN通信に影響を与えることはない。
19	V35.00 ～ V35.00	IPsec/IKEのRSAデジタル署名認証において、相手証明書がなくIKEネゴシエーションが失敗するときに装置がシステムダウンする場合がある。
20	V32.03 ～ V35.00	IPsec/IKEのテンプレート(AAAまたはDVPN)接続で通信中に、同一経路のテンプレート定義を追加すると、それ以降その経路を使ったIPsec/IKE通信ができなくなる場合がある。
21	V32.03 ～ V35.00	IPsec/IKEのエンドポイントアドレスにIPv6を設定した通信環境において、IKEネゴシエーション時にメモリリークが発生し、5万回以上接続/切断を繰り返すと装置がシステムダウンする場合がある。
22	V32.03 ～ V35.00	IPsec/IKEのテンプレート接続(AAA/RADIUS)において、template ike mode autoを設定したにも関わらずMain Modeで接続できてしまう場合がある。装置動作としてAgressive Mode接続されるべきである。
23	V35.00 ～ V35.00	show nodemanager logging wlan staコマンドにMACアドレス長を超える文字列を指定すると装置がシステムダウンする場合がある。
24	V35.00 ～ V35.00	無線LAN管理機能の稼動監視において、監視装置(本装置)から被監視機器へpingコマンドを実行すると"command already running, please wait."と表示されエラーとなる場合がある。