SR-S352TR1 V20.11 変更内容一覧

□機能追加・改善

No.	項目	内容
1	TLS/暗号スイート最新化	IPAガイドラインで推奨されているTLS/暗号スイートに対応した。 1) HTTPSサーバ機能でTLSv1.2、TLSv1.3をサポートした。 2) SSHサーバ機能で下記暗号スイートをサポートした。 - ホスト認証アルゴリズム：ecdsa-sha2-nistp256, ssh-ed25519, rsa-sha2-512, rsa-sha2-256 - メッセージ認証コード ：hmac-sha2-256, hmac-sha2-512, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com - 鍵交換アルゴリズム ：diffie-hellman-group-exchange-sha256, curve25519-sha256@libssh.org, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group16-sha512, diffie-hellman-group14-sha256 3) 下記コマンドを新規サポートした。 - https server secure (HTTPS サーバ機能のセキュアモード設定) - ssh server generate cipher type (SSHホスト鍵の暗号方式の設定) - ssh server secure (SSH サーバ機能のセキュアモード設定) - clear certificate https (HTTPS サーバ証明書キーとHTTPS サーバ証明書の消去) - clear hostkey ssh (ホスト鍵の消去)
2	コアファイル(corefile)管理機能改善	障害調査用のコアファイル管理機能について、以下の改善対応を行う。 - ftp/sftpクライアント経由の取得機能をサポート - コアファイル削除コマンドの追加 - clear corefile (コアファイルの削除)

□修正内容

No.	影響範囲	内容
1	V20.00～V20.08 NXconcierge運用時	プロキシサーバを経由して管理ポータルにアクセスする構成、かつ、proxy認証ID・パスワードに @ を含む場合、NXconciergeエージェントが管理ポータルと通信できない場合がある。
2	V14.06～V20.08 コンソール使用時	コンソール接続して長時間使用すると、本装置宛の通信全般(ping や SNMP 等)が応答しなくなる場合がある。
3	V14.06～V20.08 resetコマンド実行時	定期ログ機能を有効(defaultは有効)に設定、または、snmp機能を有効(defaultは無効)に設定して、装置起動直後、または、定期ログ採取周期(default 3h)と同じタイミングでresetコマンドを実行すると、極稀に装置がハングアップ状態になり、約15分後に、エラーコード[d4000063]が記録されて再起動する場合がある。
4	V14.06～V20.08 SSH機能利用時	マルチログイン接続環境で外部装置から本装置へのSSH接続/切断を連続して繰り返すと資源不足によりシステムダウン(error code [02000000:08000000]、または、[00000021:fffffffec])することがある。
5	V14.06～V20.08 MACテーブルフラッシュ機能利用時	MACテーブルフラッシュ機能利用時、監視するMACアドレスを装置のポート番号が一番大きいポートで学習した場合に、mac flush address設定が効かず、対象のMACアドレスがMAC学習テーブルから消えない。
6	V14.06～V20.08 HTTP/HTTPSサーバ機能利用時	HTTPサーバ機能(IPv4)とHTTPサーバ機能(IPv6)とHTTPSサーバ機能(IPv4)とHTTPSサーバ機能(IPv6)の全てが動作中の状態から全てを停止すると、httpsポートがクローズされないことがある。
7	V14.06～V20.08 FLASHメモリ異常発生後の装置再起動時	起動バンクのソフトウェアがFLASHメモリの故障で正常に起動できなかった場合に、指定したバンクと反対のバンクで装置が起動するが、ハード故障を示すCHECKランプ表示、エラーログ出力、trap送信等が行われないため、FLASHメモリの故障に直ぐに気づけない場合がある。(指定したバンクと反対のバンクで装置が起動した場合はスイッチとしての通信動作には影響はない)