SR-S312PE1 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)

□修正内容

No.	影響範囲	内容
1	V20.10 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)を一旦無効化して再度有効化するとhttp/httpsポートがオープンできず通信できない場合がある。