

## SX-3550リリースノート

バージョン	リリース	<input checked="" type="checkbox"/> :機能追加 <input type="checkbox"/> :仕様変更 <input checked="" type="checkbox"/> :不具合修正他	内容
6.9.60	2016年10月06日	●	脆弱性対応 CVE-2016-2108、CVE-2016-2109、CVE-2016-4953、CVE-2016-4954、CVE-2016-4955 CVE-2016-4956、CVE-2016-4957、CVE-2011-4862、Apache Etag情報開示の脆弱性
		●	80Mバイトを超えるファイルをアップロードできない不具合を修正
6.9.50	2015年12月07日	□	SSLアクセラレーション処理で使用する暗号スイートからデフォルトでRC4を使用しないよう仕様変更  下記オペレーションによりRC4を有効にすることが出来ます。 adm(config)# compatibility enable-rc4
		●	Layer7負荷分散設定時、クライアントからの遅延ACKと受信ウィンドウがゼロである状態が同時に発生した場合、TCP遅延ACKが発生して通信遅延が発生する不具合を修正
		●	本装置のリアルタイム情報を複数のブラウザで長時間表示させていると、プロセスが正常に終了しない状況となり管理IPアドレスにアクセス出来なくなる不具合を修正  本現象が発生してもサービス通信に影響を与えることはありません
		●	no vrrp vridコマンドに対して数値パラメータを付与してもvridの削除が正しく行われない不具合を修正
6.9.40	2015年06月19日	●	下記条件を全て満たしている場合に通信できなくなる不具合を修正 ・仮想サーバにクッキー挿入の設定が行われている ・クライアントに対してクッキーが発行済みである ・同仮想サーバにHTTPリダイレクションの設定が行われている ・上記リダイレクト先のドメイン名をワイルドカード(*)で指定している ・クライアントがCookieヘッダより後ろにHostヘッダを付けてリクエストを送信
6.9.30	2015年06月12日	●	VRRPタイマ動作が誤動作し、予期せずMasterに遷移してしまう不具合を修正  発生条件 ・dateコマンドを使用し、システム時計を手動で3.6秒を超える修正をした場合 ・ntpサーバとの同期によりシステム時計が、step調整で3.6秒を超える修正が行われた場合
6.9.20	2015年04月23日	●	FREAK (CVE-2015-0204) 脆弱性対応 本機器のWeb管理画面にHTTPSアクセスした際に、EXP系の暗号スイートを 使用できないように修正  ※サービス通信でSSLアクセラレーション機能を使用している場合は、 「弱い暗号化の拒否」(CLIコマンド:keyfail)設定を行うことで 対応することができます。 デフォルトの設定は「弱い暗号化の拒否」を行いません。
		●	cookie又はcookie挿入によるセッション維持設定があり、 バインドされている複数の実サーバのポート番号が異なっている場合に HTTP負荷分散の通信が停止してしまう不具合を修正 (Ver6.8.70以降該当)  ※Ver6.9.20へバージョンアップを行わなくてもソースNAT設定を行うことで 現象を回避させることができます。 ソースNAT設定を行ってもSX-3550の内部動作が変わるのみで クライアントやサーバ側の通信に影響を及ぼすことはありません。
6.9.10	2015年02月17日	●	冗長構成でリンク切断時、リンク接続の復旧手順でMasterになる機器が 予測できなくなる不具合を修正 プリエンプト無効(no preempt)設定を行っていても切り替えが発生してしまう場合がある
		●	冗長構成時にMaster状態への遷移後のBackup状態への遷移がVRRP送信インターバルの 1.5倍以内の時間に発生した場合にL2フォワード停止(no backup-l2forward)設定が 機能しなくなり、フォワーディングループが発生してしまう不具合を修正 (Ver6.9.0のみ該当)
		●	ロケーションヘッダ書き換え後のリクエストが同一コネクション内で行われた場合に 後続のHTTPリクエストを破棄してしまう不具合を修正 (Ver6.8.60以降該当)
		●	短時間に大量のログが出力されるとログ文字列が壊れてしまう不具合を修正
6.9.0	2014年10月30日	●	冗長でループ構成あり、かつ「no vrrp backup-l2forward」設定がある条件で、 フェイルオーバーした時、またはMaster機を再起動した時に一時的に ループが発生する不具合を修正
6.8.90	2014年10月20日	□	脆弱性への対応のためデフォルトでSSL3.0を使用しないよう仕様変更  下記オペレーションによりSSL3.0を有効にすることが出来ます。 adm(config)# compatibility enable-ssl3
6.8.80	2014年07月16日	●	クライアント証明書挿入不具合修正
		●	コネクションカウンタ不具合修正
		■	SSL基板不具合時のフェイルオーバーに対応
		●	OpenSSL脆弱性対応 (CVE-2014-0224)
6.8.70	2014年5月15日	●	リバースNAT設定時の不具合
6.8.60	2014年04月11日	●	SSL設定+ロケーションヘッダ書き換え時の不具合
		●	NTP脆弱性対応 (JVNVU#96176042)
		□	シーケンス番号異常時の動作を選択可能に仕様変更

6.8.50	2014年01月28日	●	メール転送設定の不具合修正
6.8.40	2014年01月22日	●	クライアント認証時の不具合修正
		●	クライアント証明書インポート時の不具合修正
		●	CLIにてconfigモードに入れなくなる不具合修正
6.8.30	2013年10月18日	□	SHA-2ハッシュアルゴリズムで署名されたSSLサーバ証明書に対応
		●	L7設定時にパケットがIPフラグメント化される不具合修正
		●	TCPセグメントに分割されず、IPフラグメントに分割されていた
		●	Web設定画面からcookie挿入を設定した場合の動作不具合修正
		●	Webパスワードで「/」「.」「-」の3文字が使用できない不具合の修正
		●	SSL設定とDSR設定が同時に設定できてしまう不具合修正
		●	その他、細かな不具合の修正及び仕様の変更
●	SiteGuardのログがWebUIから取得出来ない不具合修正		
6.8.20	2013年08月28日	●	プロセス死活監視機能の不具合修正 プロセスの停止を誤検知した場合、同じプロセスを二重起動させてしまう
		●	SNMP不具合修正 一回のGETコマンドで複数のOID値を取得すると、SNMPプロセスが停止してしまう
6.8.10	2013年07月12日	□	シグネチャーファイル名変更
		□	メモリパフォーマンスの調整
		□	ダウンロードファイル拡張子の変更
6.8.0	2013年05月13日	-	新規リリース

※リリース日は出荷日と異なりますので、製品のversion確認をお願い致します。