

## Si-R70brin V01.01 変更内容一覧

### □機能追加・改善

No.	項目	内容
1	IPsec/IKE常時接続	IPsec/IKEトンネルあて先の経路情報が存在している状態であれば、IPsec/IKE接続を行います。起動時にIPsec/IKEが接続可能状態であればすぐにIKEネゴシエーションを開始し、またなんらかの原因でIPsec/IKE SAが解放された場合にも、未接続状態の検出により迅速に再接続が行えます。
2	DHCPサーバ機能拡張(WINS/SIPサーバ広報)	WINS(NetBIOS)サーバアドレス、SIPサーバアドレス広報をサポートしました。
3	FENICSサービス連携機能	FENICS(ネットワークサービス)との連携によるSi-Rのコンフィグ管理機能に対応しました。詳細は下記URLからご覧ください。 <a href="http://fenics.fujitsu.com/networkservice/vpn-service/feature_config.html">http://fenics.fujitsu.com/networkservice/vpn-service/feature_config.html</a>
4	トンネル接続の拡張	IPv6 over IPv4、Ethernet over IP接続に加えて、以下のトンネル接続をサポートします。 ・IPv6 over IPv6 ・IPv4 over IPv6 ・IPv4 over IPv4

### □修正内容

No.	影響範囲	内容
1	V01.00	相手装置から未サポートのケーパビリティ値を通知された場合、NOTIFICATIONのメッセージを送信するため、BGPのセッションが確立できない。
2	V01.00	相手装置から未サポートのケーパビリティ値を通知された場合、未サポートを示すために送信するNOTIFICATIONメッセージ内のデータ部(相手装置から通知されたケーパビリティ値)が不正な値となる場合がある。
3	V01.00	IPv6アドレスのlocalnetを複数指定して動的VPN接続できない。
4	V01.00	接続先監視アドレスとlocalnetの先頭アドレスに異なるアドレスファミリ(af)、2定義目と同じafのアドレスを設定してcommitすると以下のメッセージを出力して定義反映エラーとなる。 protocol: template 0 is not available: lack or invalid configuration.
5	V01.00	拡張IPsec対象範囲(extension-range)設定がある接続先情報を削除し動的定義変更を実施するとsysdownする場合がある。
6	V01.00	動的VPNの送出インターフェースがPPPoE+NATを使用している場合にPPPoEが切断された後に送出されるIPsecトンネルアドレスが不正な値になる場合がある。
7	V01.00	IPsecの回線閉塞でISAKMP SAが削除されず再接続できない場合がある。
8	V01.00	IKE-SA/IPsec-SAの組み合わせによってはIPsec通信できない場合がある。
9	V01.00	装置内でIKEを設定しているremote定義と手動鍵を設定しているremote定義が混在し、各々でremote定義で接続先監視を行い、接続先がダウンした場合にIKE側の接続先監視が復旧しない場合がある。
10	V01.00	動的VPNで接続中の相手トンネルエンドポイントアドレスと同じアドレスのIPsec/IKE定義を行い、反映後に接続するとシステムダウンが発生する。
11	V01.00	テンプレートのRADIUS/AAA着信において16進数で奇数桁の共有鍵を使用すると、IKEネゴシエーションで失敗する。
12	V01.00	テンプレート定義の動的VPN接続を行い、Phase1ネゴシエーション確立に15秒以上かかり、かつ、相手側動的VPNクライアントからの切断要求が受信できない場合に動的VPNセッションを解放できなくなり、再接続不能となる。
13	V01.00	VU#2672891に対する対応を実施する。
14	V01.00	UDPチェックサム0の packets を NAT の宛先変換でアドレスを変換すると、UDPチェックサムを不正な値に補正してしまい、到達したホストで不正なUDPパケットとして破棄されてしまう。
15	V01.00	IPアドレスを範囲指定した静的NATを定義したとき、FTPによるデータ転送ができない。
16	V01.00	グローバルポート番号に65535を含む範囲指定されたNATテーブルを解放すると、装置が無応答となる。
17	V01.00	lenフィールドが0のBattle.netパケットをNAT処理すると、装置が無応答となる。
18	V01.00	マルチNATを使用した時にプライベートポート番号2880番のUDPパケットが通過すると、システムダウンもしくは異常動作をする場合がある。
19	V01.00	ダイナミックVPNのSIPを使用するインターフェースでNATを併用した場合、ダイナミックVPNを使用した通信を行えない。
20	V01.00	NATを使ったICMP通信が不可となる場合がある。
21	V01.00	特定のネットワーク構成において、Si-RがASBRとして動作しているOSPFエリアの種別を一般エリアからNSSAに動的定義変更すると、ABRが変換できないtype7 LSAをSi-Rが生成する場合がある。
22	V01.00	一般エリアでASBRとして動作するSi-Rについて、経路変動発生直後に一般エリアからNSSAエリアに動的定義変更すると、ABRが変換できないtype7 LSAをSi-Rが生成する場合がある。
23	V01.00	Si-RがNSSAのASBRとして動作しているとき、再配布経路がなくなってもメモリが開放されない。
24	V01.00	OSPF(Internal Area)経路のABRのインターフェース経路の経路がOSPF(External Area)経路情報と表示される場合がある。
25	V01.00	ospf ip definfoの動的定義反映で、default経路のLSAが正しく生成、または削除されない場合がある。

No.	影響範囲	内容
26	V01.00	show ip ospf routeにおいて、バックボーン以外でAS外部type1経路を表示すると、Area IDが常に、0.0.0.0と表示される。
27	V01.00	show ip ospf protocolで表示される再配布情報に次のように誤って表示されることがある。 ・show ip ospf protocolにおいて、再配布情報がStaticと表示される。 ・show ip ospf protocolにおいて、再配布情報がConnectedと表示される。
28	V01.00	OSPFネットワークが複数エリアで構成された構成において、ASBRを含むエリアをNSSAに変更すると、ABRがtype7 LSAをtype5 LSAに変換しない、またはASBRのNSSA外部経路を誤計算する場合がある。
29	V01.00	OSPFv2のデフォルトルート広報の設定を追加して動的定義反映を実施した場合、システムダウンする場合がある。
30	V01.00	sftpを使用してファームウェアの更新ができない。ダウンコードは[00000080:00000300]となる。
31	V01.00	Windowsのフリーソフトウェア UTF-8 TeraTerm Pro with TTSSH2 を使用してsshログインを繰り返すとシステムダウンする。
32	V01.00	show vrrp で表示されるVirtual Router IP Address: に設定削除済みの仮想IPアドレスが表示される場合がある。
33	V01.00	Web設定のUPnP情報において、ポートマッピング有効期限として”無期限”を選択して設定しても、UPnP情報を再表示すると、ポートマッピング有効期限として「設定する」を選択してしまう。
34	V01.00	OSPFエリア情報/バーチャルリンク情報のWeb設定画面において保存操作を行ったとき、システムダウンする場合がある。
35	V01.00	ポートスキャン・RCPスキャン時にシステムダウンする場合がある。
36	V01.00	WEB/サーバ情報より、httpサーバ機能を停止しても停止されない場合がある。
37	V01.00	ARPパケットが優先されない。
38	V01.00	IPv4 OSPFで、areaのdefcostの値が初期値以外でも、構成定義をallパラメタ付きで表示すると、初期値が表示される。
39	V01.00	RIP, BGP, OSPFの統計情報クリア操作コマンドを実行しても、統計情報がクリアされない場合がある。
40	V01.00	装置起動時に、構成定義矛盾のシスログを多数出力する場合、装置が起動中のままとなる場合がある。
41	V01.00	FTP接続後の回線断で、再接続できなくなる場合がある。
42	V01.00	ftplによる接続の後、telnetで接続できなくなる場合がある。
43	V01.00	大量の宛先への自発パケットが短時間に発生した場合に、資源枯渇によりシステムハングまたはシステムダウンが発生する場合がある。
44	V01.00	IPv4パケット転送時に、IPヘッダチェックサム値が不正値(0xffff)になる場合がある。
45	V01.00	SSH/SFTPセッションの切断開始から0.5ミリ秒以内に接続要求を受信するとシステムダウンが発生する場合がある。
46	V01.00	remote定義を利用した通信において、相手装置からフラグメントパケットを受信し、それを転送する場合に、パケット内容が不正になる場合がある。
47	V01.00	OpenSSLライブラリのバージョン0.9.7jに脆弱性問題が見つかったため、OpenSSLの最新バージョン0.9.7kにバージョンアップする。