NEC

InterSecVM/SG V4.2

移行手順書

2019年 10月　1.2版

目　次

1. はじめに 2
1.1 本書について 2
1.2 InterSecVM/SG V4.2 の主な変更点 3
2. 事前準備 3
3. 移行手順 5
3.1 バックアップデータの取得 5
3.2 バックアップデータのリストア 7
4. 注意事項 9
5. (参考)V4.2 における IPsecVPN の暗号/認証アルゴリズムの変更 11
6. (参考)V4.2 における機能削減一覧 12

1. はじめに

1.1 本書について

本ガイドでは、「InterSecVM/SG V1.*またはV3.*、V4.0、4.2（以降「移行元」と記載）上に設定されているシステム基本情報、およびセキュリティポリシーをInterSecVM/SG V4.2（以降、「移行先」と記載）へ移行するための手順を記載しています。

バックアップデータにはManagement Console の下記画面上の設定が含まれます。

・基本設定
・ファイアウォール配下の全画面
・サービス配下の全画面
・システム > バックアップ／リストア一覧
・システム > ログ管理
・リモートメンテナンス

本ガイドの対象バージョンは下記となります。

移行元	移行先
InterSecVM/SG V4.2 InterSecVM/SG V4.0 InterSecVM/SG V3.* InterSecVM/SG V1.*	InterSecVM/SG V4.2

過去機種や、同機種からの移行はサポートいたしますが、過去機種への移行は対象外となります。

VMware版、Hyper-V版、KVM版の同一種類の移行はサポートしますが、異なる種類の移行はサポート対象外です。

例） InterSecVM/SG V4.0 for Hyper-VからInterSecVM/SG V4.2 for Hyper-Vへの移行はサポート対象
InterSecVM/SG V4.0 for Hyper-VからInterSecVM/SG V4.2 for VMwareへの移行はサポート対象外

また、過去機種からの移行時は、初期設定直後の機種にのみリストア可能です。初期設定後に、各種設定を行っている場合は、再インストールを実施し初期設定後にリストアください。

1.2 InterSecVM/SG V4.2 の主な変更点

InterSecVM/SG V4.2 の主な変更点を記載します。また本変更の為に、移行時に自動的な設定の変更などが発生します。その為移行前に、「3.2 注意事項」を必ず参照ください。

(1) InterSecVM/SG で使用しているオープンソースソフトウェアのバージョンアップを行いました。

(2) IPsecVPN が IKEv2 に対応しました。
その他暗号アルゴリズムおよび認証アルゴリズムの変更を行っております。
詳細は「5 (参考)V4.2 における IPsecVPN の暗号/認証アルゴリズムの変更」を参照ください。

(3) サポートする機能を見直しました。
詳細は「6 (参考)V4.2 における機能削減一覧」を参照ください。

2. 事前準備

移行前の必要な準備を記載します。

(1) 管理用 PC の準備

・Windows マシンの用意
移行元/移行先の内部 IP アドレス/内部サブネットに接続できるものをご用意ください。

・上記マシンの IE の設定
Management Console へ接続する際、ご使用になる Web ブラウザは、Internet Explorer (日本語版・Windows 版)のバージョン 11 以上が必要です。

Internet Explorer で下記の設定を行ってください。
①[ツール]→[インターネットオプション]で以下のように設定してください。
・[セキュリティ]→[インターネット]を選択し[レベルのカスタマイズ]を押します。
-[スクリプト]→[アクティブ スクリプト]→「有効にする」を選択します。
-[その他]→[ページの自動読み込み]→「有効にする」を選択します。
・[詳細設定]→[セキュリティ]→「暗号化されたページをディスクに保存しない」のチェックを外します。
・[プライバシー]→ポップアップブロックの[設定]を「中」以下にします。

② [ツール]→[互換表示設定]にて、InterSecVM/SG が互換性表示の対象とならないように以下のように設定してください。
・“互換表示に追加した web サイト”に InterSecVM/SG の IP アドレスを含めないようにします。
・“イントラネット サイトを互換性表示で表示する“をチェックしており、InterSecVM/SG がイントラネット サイトに含まれる場合は、InterSecVM/SG に接続時は本チェックを無効にします。

(2) ライセンスキーの入手

修正パッチの適用の際に必要となりますので、ライセンスキーをご用意ください。

InterSecVM/SG では、ファイアウォールを起動させるためのライセンスキーと、修正パッチを適用可能とするためのサポートキーの２種類があります。通常はライセンスキーの中にサポートキーも含まれております。
バックアップデータには、ファイアウォールを起動させるためのライセンスキーは含まれておりますが、サポートキーは含まれておりません。移行後に改めてライセンスキー（サポートキー）の登録が必要となります。

(3) パッチの入手

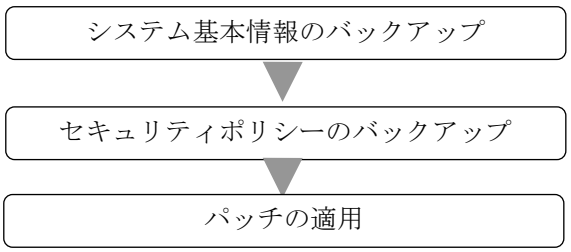
下記の HP を参照しパッチをダウンロードしておきます。パッチがなければ本作業は不要です。
パッチのインストール手順書を事前にご確認ください。

https://www.support.nec.co.jp/View.aspx?NoClear=on&id=3140106559
【InterSecVM/SG】リリースパッチ一覧 V4.2

3. 移行手順

3.1 バックアップデータの取得

Management Console より移行元へログインし、下記流れでバックアップデータを取得します。



所要時間： 約 5 分

所要時間： 約 5 分

所要時間： 約 5 分

〈注意〉
バックアップ前に必ず、「4 注意事項」をご確認お願いいたします。

(1) システム基本情報のバックアップ

① Management Console の[システム > バックアップ/リストア一覧]画面を開きます。
InterSecVM/SG V1.0 の場合は、[システム > バックアップ/リストア]画面を開き④に進みます。

② システム基本情報の[バックアップ]をクリックし、[システム > バックアップ/リストア一覧 > バックアップ]画面を開きます。

③ [PC へのバックアップ(ダウンロード)]をクリックし、[システム > バックアップ/リストア一覧 > バックアップ > PC へのバックアップ]画面を開きます。

④ [バックアップ]をクリックし、ファイルのダウンロード画面を開きます。

⑤ [保存]をクリックし、名前を付けて保存画面を開きます。

⑥ 任意のフォルダーを指定し［保存］をクリックします。

(2) セキュリティポリシーのバックアップ

① Management Console の[ファイアウォール > バックアップ・リストア]画面を開きます。

② バックアップ対象は「データと設定」を選択します。

③ [ダウンロード]をクリックし、ファイルのダウンロード画面を開きます。

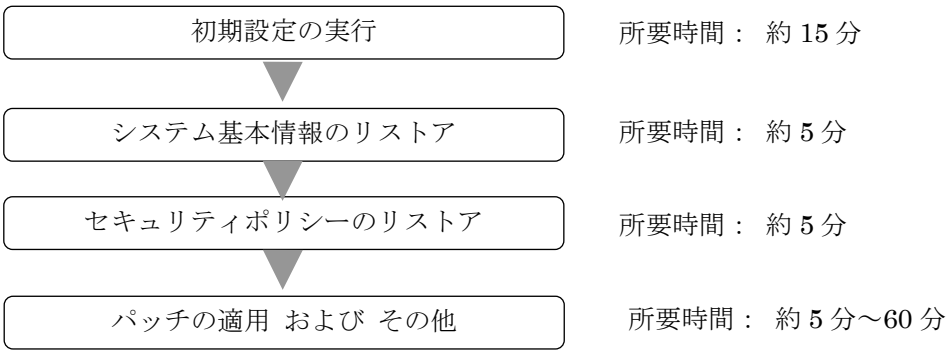
④ [保存]をクリックし、名前を付けて保存画面を開きます。

⑤ 任意のフォルダーを指定し［保存］をクリックします。

[重要]
③では、必ず「データと設定」を選択してください。
「ファイアウォール機能全体」を選択し取得したバックアップデータを移行先へ移行した場合、移行元のモジュールが移行されるため、障害の原因となります。InterSecVM/SG V4.2 では「ファイアウォール機能全体」メニューは存在しません。

3.2 バックアップデータのリストア

Management Console より移行先へログインし、下記流れでリストアを実施します。



(1) 初期設定の実行

以下の手順に従って、初期設定を実施します。

A) 初期設定の実施

① 移行先の InterSecVM/SG の「セットアップ手順書」に従い初期設定を実行します。

B) ライセンスの登録

① Management Console にアクセスする管理用 PC にライセンスキーを保存します。
② Management Console の [ファイアウォール]→[ライセンス]を選択します。
③ [ライセンスの登録]の[参照...]ボタンを押し、保存したライセンスキーを指定して[開く]ボタンを押します。
④ [登録]ボタンを押してライセンスを登録します。
⑤ [ファイアウォール]→[状態表示]を選択し、[再起動する]ボタンを押します。

(2) システム基本情報のリストア

① Management Console の[システム > バックアップ/リストア一覧]画面を開きます。

② システム基本情報の[リストア]をクリックし、[システム > バックアップ/リストア一覧 > リストア]画面を開きます。

③ [ファイルを指定してリストア]をクリックし、[システム > バックアップ/リストア一覧 > リストア > ファイルを指定してリストア]画面を開きます。

④ [参照]をクリックし、アップロードするファイルの選択画面を開きます。

⑤ システム基本情報のバックアップデータを選択し[開く]をクリックします。

⑥ [リストア] をクリックします。

⑦ 操作結果画面で「操作は成功しました。」が表示されることを確認します。

⑧ 操作結果画面の指示に従い、[基本設定]画面でリストア内容を確認し[設定]をクリックします。

⑨ 設定変更が必要な場合は、設定変更後［設定］をクリックします。
外部インタフェースの IP アドレスを変更しますと、ライセンスキーの新規発行が必要となります。外部インタフェースはかんたん設定で指定した外部ネットワークアドレスに属したインタフェースとなります。

⑩ リストアによりホスト名、または IP アドレスが変更となった場合は、システムを再起動します。

⑪ Management Console の[ファイアウォール > かんたん設定]を実施します。かんたん設定の内容に変更がない場合は、「次へ」ボタンを選択して、進めてください。

(3) セキュリティポリシーのリストア

① Management Console の[ファイアウォール > バックアップ・リストア]画面を開きます。

② 「アップロード」を選択し、[参照]ボタンを押下します。

③ アップロードするファイルの選択画面でセキュリティポリシーのバックアップデータを選択し、[開く]をクリックします。

④ [実行]をクリックします。

(4) パッチの適用 および その他

① 事前準備でダウンロードしておいたパッチのインストール手順書に従いパッチを適用します。
SSL-VPN サービスをご使用されるお客様は SSL-VPN サービスの再起動を実施します。

③ IPv6 RA 設定機能を使用していた場合は、「サービス > IPv6 RA 設定機能」の[設定]をクリックして、「サービス」にて IPv6 RA 設定機能の再起動をお願いいします。

④ RIP/RIPng 設定機能を使用していた場合は、「サービス > RIP/RIPng 設定機能」の[設定]をクリックして、「サービス」にて RIP/RIPng 設定機能の再起動をお願いいします。

4. 注意事項

(1) （重要）過去機種と比較し通信性能が低下する場合があります。
OS 供給元である RedHat 社の CPU 脆弱性対応(CVE-2017-5715、CVE-2017-5753、CVE-2017-5754、CVE-2018-3639、CVE-2018-3620)により、最大約 20%性能低下があることが報告されております。この性能低下に対して、回避することはできません。
参考)https://www.support.nec.co.jp/View.aspx?NoClear=on&id=3140104164

(2) （重要）本機種では SG 自身へ対する MSS が 500 以下の TCP パケットが破棄されます。OS 供給元である RedHat 社より掲示された、kernel 脆弱性(CVE-2019-11477、CVE-2019-11478、CVE-2019-11479)の回避策によるもので、一律適用されます。なお、RFC1191 の規約で、MSS の下限は 536 となっているため、特殊な環境でのご利用でなければ影響ございません。

(3) バックアップデータ移行時はすべての機能が停止するため、業務時間外に実施することをお勧めします。

(4) syslog 転送設定手順書に従い rsyslog.conf を設定している場合、本ファイルはバックアップ対象外となります。移行後、再設定ください。

(5) 権限委譲は、バックアップ対象外となります。移行後、再設定ください。

(6) リモートメンテナンス画面の SSH のプロトコルバージョンは移行先では「SSHv2」のみのサポートとなります。よって、移行元で「1 と 2 に対応」を指定していた場合、移行時に自動的に「SSHv2」に変更されます。

(7) InterSecVM/SG V4.2 より、下記入力値制限を追加しています。
過去機種から移行した場合、各機能の再設定時にエラーが発生する可能性があります。
本入力値制限は設定時に有効となりますので、移行元の設定のままでも運用することは可能です。

① 「ファイアウォール > 詳細設定 > ルール設定(サイト共通)」画面の"通信種別"と「ファイアウォール > 詳細設定 > ルール設定（サービス)」画面の"メンバ"で、IPv4 用プロトコルと IPv6 用プロトコルが混在して設定できないように制限を設けています。

② 「ファイアウォール > 詳細設定 > ルール設定(サイト共通)」画面の"発信元"および"宛先"に、インタフェース名指定時は複数指定できないように制限を設けています。

③ 「サービス > SSL-VPN 機能 > SSL-VPN 設定追加」画面の"設定名"に以下の制限を設けています。
指定可能な文字列：英数文字列、ハイフン(-)、アンダースコア(_)、ピリオド(.)、全角文字（日本語)。
最大文字数　　：最大 128 バイト。

④ 「サービス > SSL-VPN 機能 > SSL-VPN 設定追加」画面の"公開セグメント"に、「ネットワークアドレス / ネットマスク」の組み合わせのみ許可するように制限を設けています。

⑤ 「サービス > SSL-VPN 機能 > ユーザ情報一覧 > ユーザ情報追加」画面の"ユーザ名"に以下の制限を設けています。
指定可能な文字列：二重引用符(")とコンマ(,)以外の文字列すべて。
最大文字数　　：最大 128 バイト。

⑥ 基本設定画面の"ホスト名(FQDN)"にアンダースコア (_) を指定できないように制限を設けています。

⑦ レポート設定のメールアドレスに以下の制限を設けています。
・ メールアドレス
最大 254 文字。
「<メールアドレスローカル部>@<ドメイン>」形式。
・ メールアドレスローカル部
指定可能な文字列：英数字、特殊文字(.、!、#、$、%、&、'、*、+、¥、/、=、?、^、_、`、{、|、}、~、-)。
最大文字数　　：最大 64 文字。
・ドメイン
指定可能な文字列：英数字、ハイフン(-)、アンダースコア(_)。
各ラベルは 1 文字以上 63 文字以下、先頭および末尾にハイフン(-)は使用不可。
最大文字数　　：最大 253 文字。

(8) IPsecVPN 機能を過去機種から移行した場合に、下記の制限があります。

① 暗号アルゴリズムに「DES」を指定していた場合、移行時に自動的に「3DES」に変更されます。
② 以下の設定は移行されません。
- 共有鍵交換方式を利用した IPsecVPN パスの設定。
- 自動鍵交換方式のトランスポートモードを利用した IPsecVPN パスの設定。
- Phase2 の認証/暗号化として AH を利用した認証を行う IPsecVPN パスの設定。
- 「ルール設定(グループ)」画面で設定したトランスポート IPsecVPN パスの情報。

③ InterSecVM/SG V4.2 より、RSA 鍵情報の管理方法が変更となっています。よって、自ファイアウォールの RSA 公開鍵は過去機種からは移行されません。
以下の手順に従って、移行後に接続先 IPsecVPN 機器を更新ください。

1. 「ファイアウォール > 詳細設定 > IPsecVPN 設定 > IPsecVPN パス」画面の"鍵の出力"より、自ファイアウォールの RSA 公開鍵を取得。

2. 取得した RSA 公開鍵を接続先 IPsecVPN 機器に渡して、RSA 認証鍵として設定。

(9) 下記バージョンので SSL-VPN をご利用の場合、SSL-VPN の証明書のセキュリティ強化の為(SHA2 対応)、リストアはご利用できません。
- InterSecVM/SG v3.1
- InterSecVM/SG v4.0 で mp65128xx.pkg をご適用されていない場合

バックアップ前に、[サービス > SSL-VPN 機能]にてすべての SSL-VPN 設定を削除後、バックアップリストアを実施、リストア後に新規に SSL-VPN 設定をご登録ください。なお、必要でしたら、設定内容についてはお客様にてメモをご用意いただけますようお願いいたします。

5. (参考)V4.2におけるIPsecVPNの暗号/認証アルゴリズムの変更

・ Phase1 の暗号/認証アルゴリズム

暗号/認証アルゴリズム 組み合わせ	状況
AES256 & MD5	サポートする
AES256 & SHA1	サポートする
AES256 & SHA256	サポートする（新規）
AES256 & SHA384	サポートする
AES256 & SHA512	サポートする
AES128 & MD5	サポートする
AES128 & SHA1	サポートする
AES128 & SHA256	サポートする（新規）
AES128 & SHA384	サポートする
AES128 & SHA512	サポートする
3DES & MD5	サポートする
3DES & SHA1	サポートする
3DES & SHA256	サポートする（新規）
3DES & SHA384	サポートする
3DES & SHA512	サポートする
DES & MD5	サポートしない（変更）
DES & SHA1	サポートしない（変更）
DES & SHA384	サポートしない（変更）
DES & SHA512	サポートしない（変更）

・ Phase2 の暗号アルゴリズム

暗号アルゴリズム	状況
AES256	サポートする
AES128	サポートする
3DES	サポートする
DES	サポートしない（変更）

・ Phase2 の認証アルゴリズム

認証アルゴリズム	状況
MD5	サポートする
SHA1	サポートする
SHA256	サポートする（新規）
SHA384	サポートする（ESP を利用した認証を行う場合のみ）
SHA512	サポートする

・Phase2 の認証/暗号化のサポートは下記に変更となりました。

-過去機種

・ ESP のみ （認証、暗号化ともに ESP を使用する）

・ AH + ESP （認証として AH を使用し、暗号化として ESP を使用する）

※認証として AH を使用した際はアルゴリズム：MD5 固定。

- InterSecVM/SG V4.2

・ ESP のみ （認証、暗号化ともに ESP を使用する）

・ AH のみ （認証として AH を使用し、暗号化しない。）

※認証として AH を使用した際はアルゴリズムが
MD5,SHA1,SHA256,SHA512 から選択可能

6. (参考)V4.2における機能削減一覧

InterSecVM/SG V4.2 では下記の機能を削除致しました。

●サービス

削減機能
SMTP サーバー
POP サーバー
IPsecVPN の共有鍵交換、トランスポートモードの自動鍵交換（トンネルモードの自動鍵交換のみサポートします。）
L2TP/IPsec-VPN
Web キャッシュサーバー
冗長化機能
NTP サーバー
ネームサーバー
GRE 機能
稼動監視機能
One Point Wall
SMTP サーバー

●システム

削減機能
インタフェース一覧
ドメイン情報
設定確認

●その他

削減機能
仮想ファイアウォール
リンクアグリケーション
ポートミラーリング
ファイアウォール > ログ・アラート表示　の「外部統計用 CSV 出力」
ファイアウォール > バックアップ・リストアの「ファイアウォール機能全体」
システム > バックアップ/リストア一覧 の「ファイアウォール機能全体」
ファイアウォール > 詳細設定 > VPN 設定ウィザード
ファイアウォール > 詳細設定 > VPN パラメータ設定
ファイアウォール > 詳細設定 > インポートエクスポート
不正アクセス対策設定
LDAP 連携
コマンドによるブリッジ機能
システム情報の「サービスパックバージョン」「NEC ファイアウォール SG ソフトウェアバージョン」
SSH1（SSH2 のみサポートとなります。）

以上