

SG3600 V8.0

移行手順書

目 次

1.	はじめに	1
1.1	本書について	1
1.2	SG3600 Ver8.0 の主な変更点.....	1
2.	事前準備	2
3.	移行手順	3
3.1	バックアップデータの取得	3
3.2	バックアップデータのリストア	5
4.	注意事項	9

1. はじめに

1.1 本書について

本ガイドでは、「SG3000LJ/LG/LM（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SG3600LJ/LG/LM Ver8.0（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
UNIVERGE SG3000LJ/LG Ver1.2.*、Ver3.0.* SG3600LJ/LG V6.* SG3600LJ/LG V7.* SG3600LJ/LG/LM V8.*	SG3600LJ/LG/LM Ver8.0.* (2015年モデル)

サポートサービスを利用してのバージョンアップは、同一機種のみが可能です。

（例）SG3600LJ v6.2→SG3600 LJ v8.0)

但し、別機種でも、ご購入いただければ、LJよりLG/LM、LGよりLMへの設定移行は可能です。
詳細は、サポートポータルよりお問い合わせください

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。

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下さい。

1.2 SG3600 Ver8.0 の主な変更点

SG3600 Ver8.0 より搭載された主な機能を記載します。

(1) 仮想ファイアウォール機能

1台で複数の仮想ファイアウォールを最大12まで実行できます。

※SG3600LMのみの機能で、SG3600LJ/LGでは別途オプションライセンスが必要になります。

(2) LDAP 連携機能

Active Directory と連携し、利用者のログオン情報をもとに、アクセス制御を行います。

(3) IDS 機能

パケットヘッダの異常などを検知するアノマリ検知や、大量パケットによる DoS 攻撃を検知・防御します。

2. 事前準備

バックアップデータを移行する前に準備する必要のある事柄を記載します。

(1) 管理用 PC の準備

- ・ Windows マシンの用意

移行元/移行先の内側 IP アドレス/内側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）が必要です。

Internet Explorer は、[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]→[設定]を「中」以下にします。

また、Internet Explorer 8～10 の場合は、[ツール]→[互換表示設定]にて、SG が互換性表示の対象となるよう、“互換表示に追加した web サイト”に SG の IP アドレスを追加してください。

Internet Explorer 11 の場合は、[ツール]→[互換表示設定]にて、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 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、SG がイントラネット サイトに含まれる場合は、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

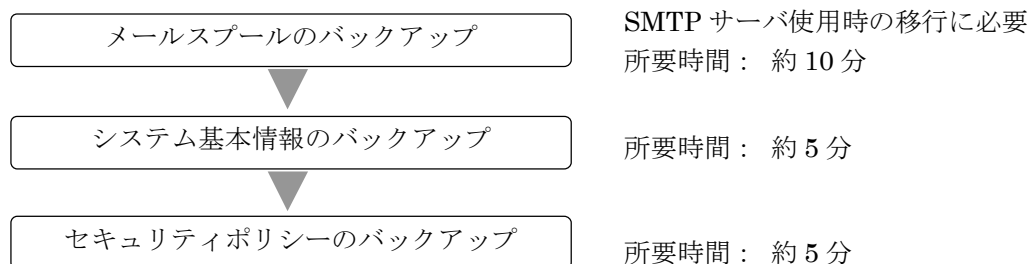
(3) バックアップデータを格納する USB メモリ (以降、USB メモリと記載)

SG3000 にて SMTP 機能、POP 機能を利用している際のメールスプールの移行方法として、USB メモリによる移行を選択される場合に必要となります。” 3-1 バックアップデータの取得 (1) メールスプールのバックアップ”を参照いただき、ファイルサイズに余裕のある USB メモリをご用意ください。

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。



(1) メールスプールのバックアップ

SMTP サーバをご使用されている場合はメールスプールの移行を行う為に必要となります。
メールスプールのバックアップ方法は、下記 3 種類となります。

- USB へのバックアップ
- Samba を使用して Windows 共有フォルダへのバックアップ
- FTP を使用した転送先 IP アドレスへのバックアップ

(2)

バックアップ対象は下記ファイルとなります。

```
/var/spool/mqueue/*  
/var/spool/mail/*
```

必要に応じて移行元の SG3000 にてバックアップ対象のファイルサイズを確認し、バックアップ方法を検討ください。バックアップデータは gzip で圧縮を行います。ファイル内容により増減がありますが、一般的にテキストファイルを圧縮する場合は、圧縮前の 10%~40% の大きさになります。

ファイルサイズ確認例)

```
du -sk /var/spool/mqueue  
du -sk /var/spool/mail
```

- ① USB へのバックアップを行う場合は、SG3000 に USB メモリを接続します。
- ② 管理用 PC から、SG3000 の Management Console へログインします。
- ③ [サービス] 画面を開きます。
- ④ SMTP サーバ、および POP サーバの[停止] をクリックしサービスを停止します。
- ⑤ 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。
- ⑥ メールスプールの[設定]をクリックし、[システム > バックアップ/リストア一覧 > 設定(メールスプール)] 画面を開きます。

- ⑦ Samba、または USB デバイス、FTP を選択後、必要な情報を入力し、[設定]をクリックします。
- ⑧ メールスプールの[バックアップ]をクリックします。
- ⑨ [サービス] 画面を開きます。
- ⑩ SMTP サーバ、および POP サーバの[起動] をクリックしサービスを起動します。

(3) システム基本情報のバックアップ

- ① 管理用 PC から、移行元の Management Console へログインします。
- ② 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。
SG3000LJ 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。
- ③ 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。
- ④ [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。
- ⑤ [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。
- ⑥ [保存]をクリックし、名前を付けて保存画面を開きます。
- ⑦ 任意のフォルダを指定し [保存] をクリックします。

(4) セキュリティポリシーのバックアップ

- ① 管理用 PC から、移行元の Management Console へログインします。
- ② 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。
- ③ バックアップ対象は「データと設定」を選択します。
- ④ [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。
- 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。

3.2 バックアップデータのリストア

バックアップデータをリストアする手順は、下記流れとなります。



(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 移行先に添付されている「セットアップ手順説明書」に従い初期設定を実行します。

B) ライセンスの登録

- ① 管理用 PC にライセンスキーを保存します。
- ② 管理用 PC から Web ブラウザで SG3600 シリーズの Management Console にログインします。
- ③ 「設定」画面左メニューの[Administrator]にある[ファイアウォール]→[ライセンス]を選択します。
- ④ [ライセンス登録]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。
- ⑤ [登録]ボタンを押してライセンスを登録します。
- ⑥ [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。

管理用 PC から、移行先の Management Console へログインし、システム基本情報、セキュリティポリシー、およびメールスプールのバックアップデータをリストアします。

(2) システム基本情報のリストア

- ① 管理用 PC から、移行先の Management Console へログインします。
- ② 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。
- ③ 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。
- ④ [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。

- ⑤ [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。
- ⑥ 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。
- ⑦ [リストア] をクリックします。
- ⑧ 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。
- ⑨ 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。

下記すべての条件に該当する場合は、SMTP サーバの起動に数十秒～数分以上(冗長化機能、またはサーバ公開ルールで使用する仮想 IP アドレス*数十秒)かかります。

- ・移行先が SG3600LG、または SG3600LM である
- ・移行元で二重化機能、冗長化機能、またはサーバ公開ルールを使用している
- ・移行作業中も含め、移行先で「基本設定」画面に設定しているネームサーバにアクセスできない

SMTP サーバの起動に時間がかかる事象を回避するには、「基本設定」画面のネームサーバの設定をアクセス可能なネームサーバに変更するか、またはネームサーバの設定を削除します。削除を行う場合は、アクセス可能となる時点で再設定します。

- ⑩ 移行元の SG3000 上で冗長化機能を使用されている場合は、[サービス > 冗長化機能 > 設定]画面にて下記を確認します。
 - ・「仮想 IP アドレス」が内側、および外側に設定されていること
→設定されていない場合は、バックアップ元とリストア先の IP アドレスを一致させる必要があります。
- ⑪ 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。
- ⑫ 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。
- ⑬ 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、進めて下さい。

※メールのアドレス変換を使用していた場合は、「サービス > SMTP サーバ > アドレス変換 > アドレス変換情報編集」の[設定]をクリックして、「サービス」にて SMTP サーバの再起動をお願いいたします。

※バックアップ後に「基本設定」画面の IPv4 アドレスを変更し、且つ、Web キャッシュサーバを使用されていた場合は、「サービス > Web キャッシュサーバ > 詳細設定」の[設定]をクリックし「サービス」Web キャッシュサーバの再起動をお願いいたします。

(3) ネームサーバの設定編集

SG3600 Ver6.2 より、DNS サーバの仕様変更を行っております。SG3000LG で DNS 機能を使用されている場合、下記について動作が異なります。

- ・オープンリゾルバ対策として、再起問い合わせを許可する範囲のデフォルトをローカルネットワークのみに限定したため、ローカルネットワーク以外からの再起問い合わせができない場合があります。

SG3000LG と同じ動作とするためには、下記手順に従い設定変更を行ってください。

- ① 管理用 PC から、移行先の Management Console へログインします。
- ② [サービス > ネームサーバ]画面を開きます。
- ③ [Option 設定] ボタンを押下し、[サービス > ネームサーバ > Option 設定] 画面を開きます。
- ④ 「allow-recursion」に値が設定されていない、かつ「その他の Option」に allow-query が設定されていないことを確認します。
いずれも設定されていない場合は、「allow-recursion」に「any;」を追加し、[設定]ボタンを押下します。
いずれかが設定されている場合は、ここでの作業は不要です。
- ⑤ [サービス > ネームサーバ]画面を開きます。
- ⑥ [編集結果を反映]ボタンを押下します。

[重要]

④では、「any;」を設定する手順となっておりますが、これは従来版と同じ動作とするための設定となります。DNS サーバを外部公開されるような場合は、オープンリゾルバ対策として再起問い合わせを許可する範囲を必要最小限に変更されることを推奨します。

参考サイト：<https://www.jpccert.or.jp/at/2013/at130022.html>

SG3000 から SG3600 に移行時、ネームサーバが起動しない場合は下記の設定変更をおこなってください。

- ① 管理用 PC から、移行先の Management Console へログインします。
- ② [サービス > ネームサーバ> Zone ファイル編集]画面及び、
[サービス > ネームサーバ > Zone ファイル編集 > SOA 編集]画面を開きます。
- ③ 所有者、管理者、設定値を FQDN で記載しており、且つ、値の最後に.(ピリオド)が付いていない場合は.(ピリオド)の追記をお願いします。

(4) セキュリティポリシーのリストア

- ① 管理用 PC から、移行先の Management Console へログインします。
- ② 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。
- ③ 「アップロード」を選択し、[参照]ボタンを押下します。
- ④ 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。
- ⑤ [実行]をクリックします。

(5) メールスプールのリストア

SG3600 へメールスプールの移行を行う場合に必要となります。

- ① USB メモリへのバックアップを行われた場合は、移行先に USB メモリを接続します。
- ② 管理用 PC から、移行先の Management Console へログインします。
- ③ [サービス] 画面を開きます。
- ④ SMTP サーバ、および POP サーバの[停止] をクリックしサービスを停止します。
- ⑤ 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。
- ⑥ メールスプールの[設定]をクリックし、[システム > バックアップ/リストア一覧 > 設定(メールスプール)] 画面を開きます。
- ⑦ [バックアップ方式] で Samba, または USB デバイスを選択後、必要な情報を入力し、[設定] をクリックします。
- ⑧ メールスプールの[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 (メールスプール)]画面を開きます。
- ⑨ バックアップのリストア先、リストアするバックアップファイルを選択し[実行]をクリックします。
- ⑩ [サービス] 画面を開きます。
- ⑪ SMTP サーバ、および POP サーバの[起動] をクリックしサービスを起動します。

(6) その他

- ① 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。
- ② 冗長化サービスをご使用されている場合、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、進めて下さい。
- ③ 下記の HP を参照しパッチを適用します。同機種からのリストアを行った場合は、パッチのリストアも行われますので、「パッケージ > SG パッケージ(パッチ)の適用履歴」でご確認頂き、未適用のパッチがございましたら適用下さい。過去機種からのリストアを行った場合、パッチの適用に失敗した旨表示されますが問題ございませんので、下記のパッチを適用ください。

<https://www.support.nec.co.jp/View.aspx?NoClear=on&id=3140103081>

【SG3600】リリースパッチ一覧 v8.0

4. 注意事項

- (5) バックアップデータ移行時は全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。
移行に要する時間は、お客様環境によって前後しますが、単体構成でおよそ 1 時間、冗長化構成でおよそ 2 時間が目安となります。
- (6) ログ・アラート機能を使われている場合、ログ・アラートファイル設定の[パーティション残量確保]のパラメータのデフォルト値が、SG3000 では 65536 KB、SG3600 では 1048576 KB と異なります。必要に応じてご変更ください。
- (7) [システム]->[シリアルポート設定]の設定項目は、バックアップ対象外になります。
- (8) syslog 転送の rsyslog.conf はバックアップ対象外となります。
- (9) 権限委譲は、バックアップ対象外となります。

以上