clearswift

Clearswift SECURE Exchange Gateway

インストールおよび入門ガイド

バージョン4.7.0

ドキュメント リビジョン 1.0

clearswift

著作権

修正番号 1.0 2017 年11 月

Clearswift Ltd. 発行

© 1995–2017 年 Clearswift Ltd.

All Rights Reserved.

ここに含まれる資料は、特に定めのない限り、Clearswift Ltd の独占的な財産とします。Clearswift の財産は、いかなる部分においても、Clearswift Ltd の明白な許可なく、電子的、機械的、フォトコピー、録音によるいかなる方法を問わず、いかなる形態にても複製、配布、伝送、および読み込み可能なシステムに保存することはできません。また、その他いかなる方法にても使用することはできません。

この文書に含まれる情報には、説明の目的で架空の人物、企業、製品および出来事が含まれることがあります。実在の人物、企業、製品および出来事に類似する場合があっても、これらはすべて偶然であり、このような類似性に起因するいかなる損失に対しても Clearswift は一切の責任を負わないものとします。

Clearswift のロゴおよび Clearswift の製品名は、Clearswift Ltd. の商標です。その他すべての商標は、各社の商標です。Clearswift Ltd. (登録番号 3367495) は英国で登記しています。登録事務所の所在地は、1310 Waterside, Arlington Business Park, Theale, Reading, Berkshire RG7 4SA, England です。ユーザーは、輸出、輸入、および暗号の使用に関して、当該国のすべての法規を必ず遵守しなければなりません。

Clearswift は、この文書のいかなる部分においてもいつでも変更できる権利を留保します。

著作権と同意書の完全なバージョンは、 ここ をクリックしてご確認ください。

目次

著作権 ...... **ii**

目次 ...... **iii**

1. このガイドについて **6**

1.1 このガイドの対象になる方 6

2. インストールの前に **7**

2.1 インストールのタイプ 7

2.2 ソフトウェアの入手 8

2.3 動作環境 8

ハードウェア要件 8

インストール メディア 9

サポートされるブラウザー 9

Clearswift SXG Interceptor の動作環境 10

3. Clearswift SECURE Exchange Gateway のインストール手順 **11**

3.1 Clearswift SECURE Exchange Gateway のインストール手順 11

3.2 ISO イメージからのインストール 11

3.3 Clearswift のFirst Boot Console の実行 13

Clearswift SECURE Exchange Gateway インストール ウィザードの使用に関する注記 16

3.3.1 Gateway リリース 4.7.0 上で TLS v1.0 のを再有効化し暗号化(サイファー) をアップデートする方法: 16

3.3.2 Gateway バージョン 3 のピアのキーストアの更新方法 17

3.4 Clearswift オンライン リポジトリーへのアクセスの有効化または無効化 17

4. Clearswift SXG Interceptorのインストール **19**

4.1 Exchange Gateway 19

4.2 Exchange Server 19

4.3 Clearswift SXG Interceptorのインストール 20

4.4 SXG Interceptor のインストールの完了 21

4.5 SXG Interceptor のインストールの検証 24

4.6 SXG Interceptor のテスト: 24

5. Clearswift SECURE Exchange Gateway バージョン 3.8 からのアップグレード 25

5.1 オリジナル システムのバックアップ 25

5.2 Gateway のインストール 4.7.0 26

5.3 システム バックアップの復元 26

6. Clearswift SECURE Exchange Gateway バージョン 3.8 からのアップグレード 28

6.1 アップグレード プロセスの概要 28

6.2 オリジナル システムのバックアップ 29

6.3 SXG Interceptor のアップグレード 30

6.3.1 アンインストールと再インストール 30

6.4 Gateway のインストール 4.7.0 31

6.5 Exchange 環境の準備 31

6.5.1 Exchange Gateway を SXG Interceptor 環境に追加する方法: 32

6.6 SECURE Exchange Gateway 環境の準備 32

6.6.1 システム バックアップの復元 32

6.6.2 システム バックアップの復元 33

6.6.3 設定の復元 33

6.6.4 設定の完了 33

6.6.5 ピアリング 34

6.7 4.7.0 のGateway の有効化 34

6.7.1 4.7.0 のExchange Gateway を有効化する方法 35

6.7.2 3.8 のExchange Gateway を無効化する方法 35

6.8 3.8 の Gateway の削除 35

6.8.1 3.8 の SXG Gateway を削除する方法 35

6.8.2 SXG Interceptor の SSL3 を無効化します 35

7. リリース 4.x からリリース 4.7.0 へのアップグレード 36

8. SXG Interceptor のトラブルシューティング: 38

8.1 Interceptor に関する情報の表示 38

8.2 SXG Interceptor がトランスポート エージェントとしてインストールされているかどうかの確認 38
8.3 ログ レベルの設定 39
付録: ソフトウェアインストールプロセス(ディスクから) 40
インストール後の注意事項 41
ソフトウェアのインストールプロセスが完了したら... 41
付録: ソフトウェアのインストールプロセス(Clearswift オンラインリポジトリから) 41
インストール後の注意事項 43
ソフトウェアのインストールプロセスが完了したら... 43
付録: USB インストール メディアの準備 43

1. このガイドについて

このガイドにはClearswift SECURE Exchange Gateway を仮想マシンまたは物理サーバーにインストールする管理者向けの情報が記載されています。具体的には、完全インストールに必要な手順および要件について説明します。

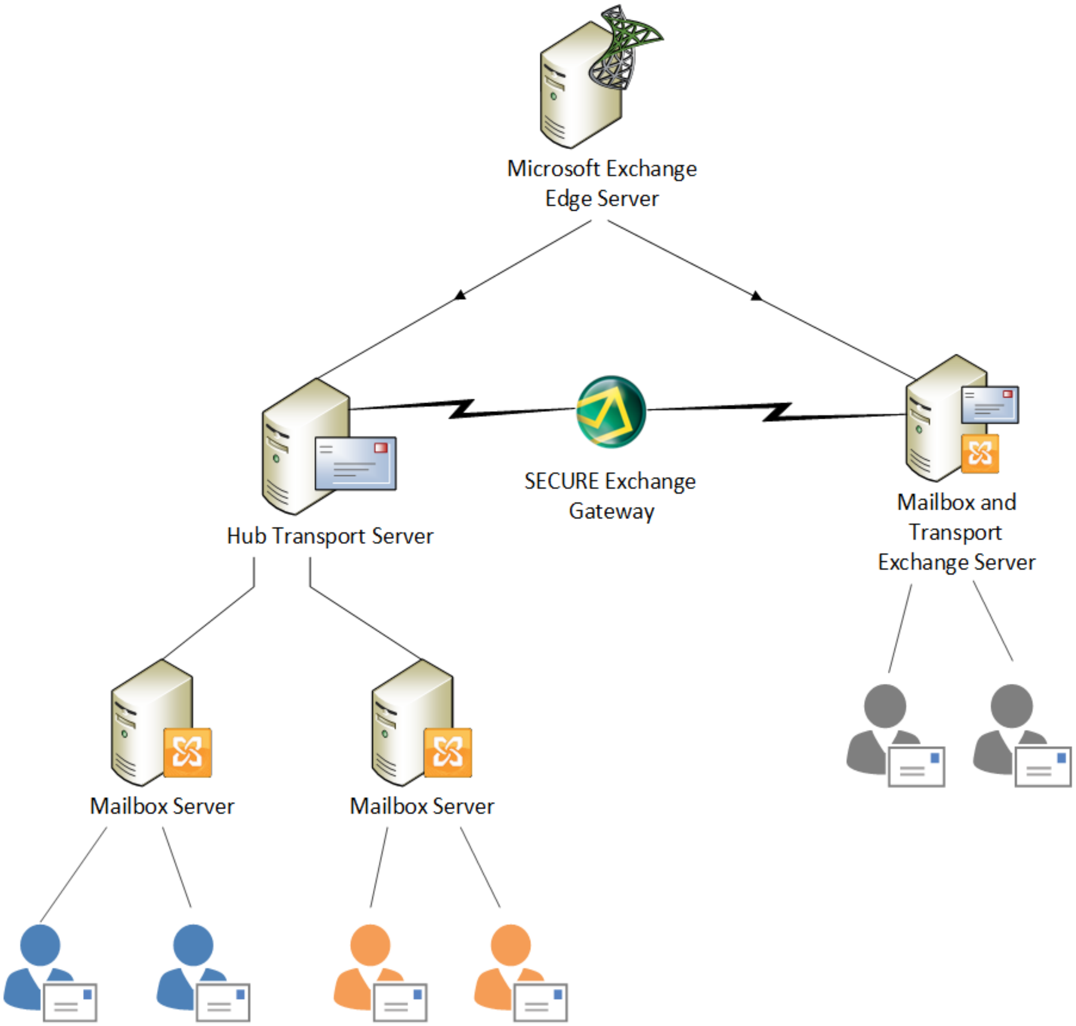
1.1 このガイドの対象になる方

このガイドの対象読者

- 初めてClearswift SECURE Exchange Gateway をインストールする新規ユーザー
- Clearswift SECURE Exchange Gatewayの最新バージョンの リリース 3.8 からリリース 4.7.0 にアップグレードするユーザー。
- Clearswift SECURE Exchange Gateway リリース 4.x から 4.7.0 リリース へのアップグレード

2. インストールの前に

このセクションでは、動作環境と Clearswift SECURE Exchange Gateway のインストール前に必要な考慮事項を説明しています。Gateway は、64 ビット Red Hat Enterprise Linux (RHEL 6.9) 上で動作します。物理サーバーまたは仮想マシンに製品をインストールすることができます。サポートされるプラットフォームの詳細については、「 動作環境」 を参照してください。



2.1 インストールのタイプ

次のいずれかのプロセスを使用して Clearswift SECURE Exchange Gateway をインストールできます。

インストール プロセス	説明	参照
標準インストール プロセス	RHEL 6.9 と Clearswift ソフトウェアの両方を含む ISO イメージを使用して本製品をインストー	ISO イメージからのインストー

インストール プロセス	説明	参照
	ルするユーザーに適用されます。	ル
ハードウェア インストール プロセス	Clearswift から提供されているプレインストール済みハードウェアを使用して本製品を導入するユーザーに適用されます。	デフォルトの資格情報を使用して、cs-admin としてログインします。
ソフトウェアインストール プロセス(ISOから)	既存の RHEL 6.9 プラットフォームに本製品をインストールするユーザーに適用されます。	付録 A: ソフトウェア インストール プロセス
ソフトウェアのインストールプロセス(オンライン Clearswift リポジトリから)	既存の RHEL 6.9 プラットフォームに本製品をインストールするユーザーに適用されます。	付録 B: ソフトウェア インストール プロセス

2.2 ソフトウェアの入手

Clearswift SECURE Exchange Gateway ソフトウェアは、以下から入手できます。

- Clearswift download area から Clearswift SECURE Exchange Gateway ISO イメージをダウンロードできます。
- Clearswift サポート ポータル から、インターセプターのソフトウエアをダウンロードできます。
- Clearswift (ハードウェアを購入の場合はすでにソフトウェアがプレインストールされています。)

2.3 動作環境

インストールの前に、以下の動作要件を確認してください。

ハードウェア要件

コンピューターまたは仮想マシンには、テストおよびデモ環境では、最低限 4 GB 以上の RAM と 60 GB 以上のハードドライブが必要です。Clearswift では、実稼働環境で使用する場合はストレージおよび処理要件に応じて200GB 以上のハードドライブをお勧めしています。ハードウェアのサイジングについての詳細は、 ハードウェアのサイジングについての詳細は、

メッセージ ボリューム	プロセッサー	プロセッサー数	メモリー	ディスク	RAID
低 (1時間あたり20,000以下)	デュアル コア	1	4GB	320GB+ SATA/SCSI	オプション
普通 (1時間あたり50,000以下)	デュアル/クアッド コア Xeon	1	4GB	320GB+ SATA/SCSI	オプション
高 (1時間あたり60,000以下)	デュアル/クアッド コア Xeon	1	6GB	2 x SAS 15,000 RPM	はい(RAID 1)
非常に高 (1時間あたり60,000以上)	クアッド コア Xeon	2	6GB	複数 SAS 15,000 RPM	はい (1, 10)

インストール メディア

必ず正しいバージョンのISOイメージを使用してください。**インストールに使用するISOバージョン：**EMAIL_470_170.iso

ISOイメージのコピーをClearswiftリポジトリーからダウンロードしたら、以下の方法を使用して、ソフトウェアをインストールします。

- 光学式DVDにISOイメージをコピーする: Clearswiftでは、Clearswift SECURE Exchange Gatewayソフトウェアをインストールする場合、この方法をお勧めしています。
- USBメディアにISOイメージをコピーする: 手順はこのガイドの付録Bを参照してください。
- 仮想DVDドライブとしてISOイメージをアタッチする: この方法は仮想マシンにのみ適用できます。

サポートされるブラウザー

TLS1.2 (サイファー) の暗号化を使用したClearswift SECURE Exchange Gatewayへの接続をサポートし、次のブラウザーでテストされています。

- Internet Explorer IE10 (Windows 7)
- Internet Explorer IE11 (Windows 7、Windows 8)

- Mozilla Firefox 17、24、30、36 以上
- Google Chrome 40 以上
- Microsoft Edge (Windows 10)

Clearswift SXG Interceptor の動作環境

Clearswift SXG Interceptor をインストールした後で、次を完了する必要があります。

- Windows 2008 SP2 およびそれ以降
- Exchange 2007 SP3 およびそれ以降
- Active Directory ライトウェイト ディレクトリー サービス (AD LDS)

> SXG 構成ストアコンポーネントがインストール時に選択された場合にのみ、AD LDSが必要です。SXG 構成ストアのコンポーネントは、Clearswift SXG Interceptor のインストール時にデフォルトで選択されます。しかし組織内の最初の サーバーに Clearswift SXG Interceptor をインストールした場合に、SXG 構成ストアコンポーネントが必要となります。

- Microsoft Office 3.5
- PowerShell 2.0

3. Clearswift SECURE Exchange Gateway のインストール手順

オンライン Cearswift リポジトリーでダウンロードできる ISO イメージから Clearswift SECURE Exchange Gateway ソフトウェアをインストールできます。

インストール プロセスでは次の作業を行います。

1. Red Hat Enterprise Linux 6.8 オペレーティング システムと Clearswift SECURE Exchange Gateway をインストール メディアからインストールします。
2. コンソール ベースの*Configure System*ウィザードを実行し、ネットワーク設定を含むデフォルトのシステム値を調整します。
3. ソフトウェアの最新の更新ファイルがある Clearswift のオンライン リポジトリーへのアクセスを有効化します。

Gateway がインストールされたら、*Clearswift Install Wizard*を [完了] をクリックして終了します。

3.1 Clearswift SECURE Exchange Gateway のインストール手順

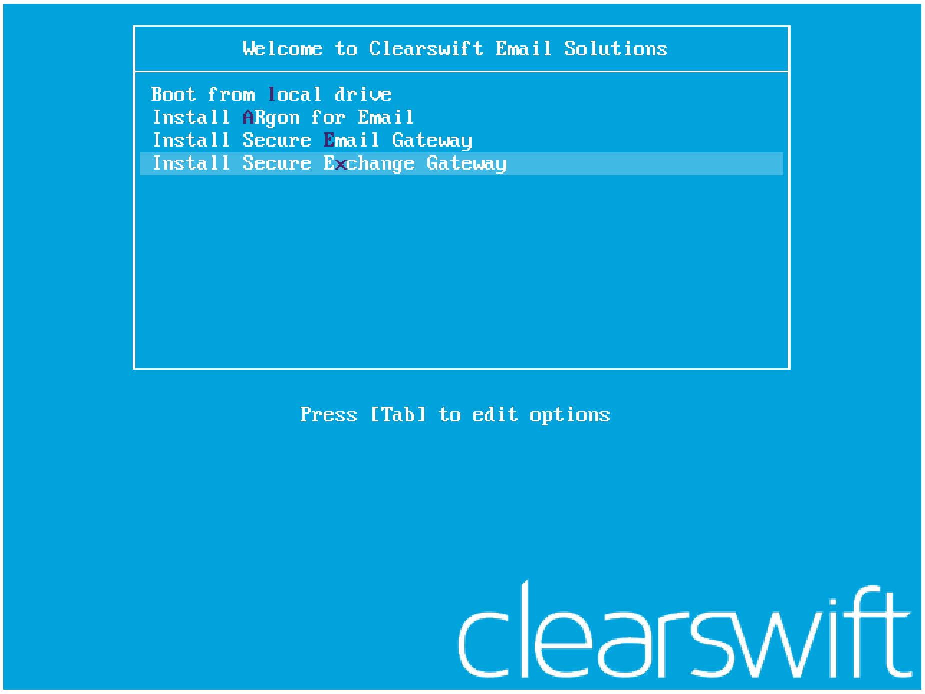
次の手順では、Red Hat Enterprise Linux 6.9 オペレーティングシステムのインストールが完了してから行う、Clearswift SECURE Exchange Gateway のインストール方法について説明しています。

> 「 セクション 3.2 ISO イメージからのインストール」は、RHEL 6.9 と Clearswift ソフトウェアの両方を含む ISO イメージを使用して標準インストールを実行する場合にのみ適用します。
>
> ハードウェア インストールを実行する場合には、「 セクション 3.3 Clearswift システム設定ウィザードの実行」を参照してください。
>
> 既存の RHEL 6.9 サーバーにインストールする場合は、このガイドの付録 A または付録 B の手順を使用してインストールを実行してください。その後、第 3.3 節の「 [First Boot Console] の実行」を参照して、Clearswift SECURE Exchange Gateway のインストールを完了します。

3.2 ISO イメージからのインストール

1. ISO イメージが格納されているメディアをドライブに挿入し、サーバーの電源を入れます。

   [Welcome to Clearswift Email *Solutions]* 起動画面が表示されます。起動デバイスが見つからない場合は、BIOSでシステムの起動シーケンスを調整する必要があります。



2. 矢印キーまたはキーボードのショートカットを使用して、メニューから **[Install Secure Exchange Gateway]** を選択します。**Enter** キーを押して、インストールを選択します。

   インストールプロセスが開始され、自動的に実行されます。

> インストール後のスクリプトなど、インストールプロセス全体を完了するために10～15分かかります。パッケージのインストールが完了したら、インストール プロセスでは 5 分ほど "Running post-installation scripts" のメッセージが表示されます。このメッセージが画面に表示されている間は、インストールプロセスがバックグラウンドで実行されているため、プロセスを中断しないようにしてください。インストール プロセスが完了すると、システムは自動的に再起動されます。*Welcome to Clearswift Solutions* と表示された起動画面が再び表示され、60秒のタイムアウト後に **Boot from local drive** が自動的に実行されます。

3.3 Clearswift のFirst Boot Console の実行

次の *[First Boot Console]* の手順を完了します。

1. Clearswift の[First Boot Console]の実行

   - ログイン: **cs-admin**
   - パスワード**password**

   [First Boot Console] が表示され、設定プロセスを開始することができます。

2. 画面の指示に従って以下を選択します。

   - **Locale Configuration**
   - **Keyboard Configuration**
   - **Timezone Configuration**

   > Gateway のシステム時間およびロケールの設定には、ここで選択した内容が反映されます。ロケールは後から変更できないため、インストール時に正しく設定することが重要です。

3. **[Network Configuration]** ページで次の設定を更新します:

   - System Hostname: 新しいホスト名を入力して、**[Save]** を押します。
   - Network Adapters: ネットワーク アダプターを選択して、**[Edit]** を押します。**[IPv4 Addresses]** を押して、選択した IP address を**Edit**します。編集したら、**[Save]** を押します。
   - DNS サーバーDNS サーバー: DNS エントリーを選択して、**[Edit]** を押します。必要な場合、**[Search Domains]** を追加するか、または空白のままにします。

     編集したら、**[Save]** を押します。

4. **Repository Configuration** ページでリポジトリー設定を構成します。

Clearswift オンラインリポジトリは、通常、インストール後にデフォルトで無効になっています。つまり、ローカルメディアからアップデートを取得しなければなりません。ただし、インターネットにアクセスできない場合は、**[Online Mode]** を選択して、Clearswiftオンラインリポジトリから更新情報を受け取ることができます。

5. **cs-admin password** ページにて、cs-admin アカウントの新しいパスワードを入力してください。パスワードの複雑さは、実施しているパスワードポリシーに依存します。Clearswift password policy は、デフォルトでISOイメージからの標準インストールに適用されます。このポリシーは、長さ8文字以上、辞書単語に似ていない(例：Pa55word) 、シーケンス(例：1234) が含まれていない、および下記の文字タイプら３つ、各文字タイプに少なくとも１つ以上の文字が含まれるパスワードを設定する必要があります。

   - 英大文字
   - 英小文字
   - 数字
   - 記号

   詳細および例については、オンラインヘプの「 Clearswift パスワードポリシーの必要条件」 を参照ください。オンラインヘルプで、パスワードポリシーを無効にする方法に関する情報を提供しています。

6. 設定を適用し、サーバーの再起動を確認します。

7. 再起動後、ブラウザーを開き、次の Gateway のIP アドレスに移動します。

   https://<*ip-address*>/Appliance

   IP アドレスを確認するには、デフォルトの資格情報を使用してコンソールにログインします。

   [View System Status] を選択して、**[OK]** をクリックします。

   [The *Clearswift SECURE Exchange Gateway* installation wizard] 画面が表示されます。

設定を適用してから、 Clearswift SECURE Exchange Gatewayを使えるようになるまで 5 ～ 10 分ほどかかります。Gateway のインターフェースにアクセスできる場合、オンラインヘルプの「 最初の手順」 を参照してください。

> 再起動後に Clearswift インストール メディアがイジェクトされたら、Clearswift インストール ウィザードを設定する*前に* DVD を再度挿入する**必要があります**。このウィザードでは、Gateway のセットアップを完了するためにインストール メディアにアクセスする必要があります。

Clearswift SECURE Exchange Gateway インストール ウィザードの使用に関する注記

ウィザードで表示されたネットワーク設定には、Red Hat Enterprise Linux を設定したときに作成した設定が反映されます。これらの設定は読み取り専用で表示されます。

ウィザードの設定は、インストールの直後、追加のネットワーク アダプターを設定する前に行うことをお勧めします。ただし、インストールウィザードの設定前にマシンの 再起動が必要な場合は、再起動後にファイアウォールを無効にしてください。ファイアウォールを無効にするには、*service iptables stop* コマンドを実行します。ウィザードを完了すると、ファイアウォールは自動的に再起動されます。

Clearswift Gateway バージョン 3 とバージョン 4 のピアリング

Clearswift Gatewayバージョン v4 にてセキュリティーを強化したことにより、ピアリングのためにTLS v1.0 プロトコルはサポートされません。TLS v1.2 のみサポートしています。

たとえば、PMM または Web Gateway Reporter を使用している Gatewayバージョン 3 を Gateway バージョン 4 とピアする場合、4.7.0 Gateway にて**TLS v1.0 を再度有効化**し、Gateway バージョン 4 およびバージョン 3 の**暗号化(サイファー) を更新**する必要があります。

すでに Gateway バージョン 4 上でPMMを実行している場合は、この手順を実行する必要はありません。

4.7.0 Gatewayのインストール後に、 *[Clearswift Installation Wizard]* を使用して Gateway の設定が完了してから、この手順を適用してください。

3.3.1 Gateway リリース 4.7.0 上で TLS v1.0 のを再有効化し暗号化 (サイファー) をアップデートする方法：

1. 次のファイルから **sslEnabledProtocols** 属性を検索します：

   ```
   /opt/tomcat/conf/
   server-bind.xml
   ```

```
server-bind2.xml
```

2. TLSv1.2 から TLSv1、TLSv1.2 に各プロトコルの値を変更します。

   server-bind2.xml 中に2つのインスタンスがあります。

3. 同じファイル内の **ciphers** 属性を検索します:

   ```
   /opt/tomcat/conf/
   ```

   ```
   server-bind.xml
   ```

   ```
   server-bind2.xml
   ```

4. 各ファイルのカンマ分割されたリストの最後に TLS_RSA_WITH_AES_256_CBC_SHA を追加します。

   server-bind2.xml 中に2つのインスタンスがあります。

5. 次のコマンドを使用して、UI を再起動します。

   ```
   cs-servicecontrol restart tomcat
   ```

3.3.2 Gateway バージョン 3 のピアのキーストアの更新方法

証明書の生成方法と Tomcat が使用するための KeySore への配置方法:

1. コマンド ラインで root の権限を使用します。
2. `cd /opt/msw/data/`
3. `mv keystore keystore.orig`
4. ```
   keytool -genkey -alias tomcat -keyalg RSA -sigalg SHA1withRSA
   -keystore keystore -storepass changeit --dname
   "CN=Clearswift,OU=Clearswift,O=Clearswift,L=Reading,S=Berkshi
   re,C=Uk" -validity 3650
   ```

   > 利用者自身の詳細によって証明書属性(CN、OU、Oなど) を更新します。

   このコマンドを入力した後、システムがTomcatのためのキーパスワードの入力を求めます。キーストアのパスワードと同じ場合は、RETURNを押します。

5. `uiservicecontrol restart tomcat`

3.4 Clearswift オンライン リポジトリーへのアクセスの有効化または無効化
   ```

Clearswift First Boot Console で、オンライン Clearswift リポジトリまたは(オフライン) ローカルメディアから適用する更新を選択しました。

Clearswift オンラインリポジトリは、通常、インストール後にデフォルトで無効になっています。つまり、ローカルメディアからアップデートを取得しなければなりません。ただし、インターネットにアクセスできない場合は、**[Online Mode]** を選択して、Clearswiftオンラインリポジトリから更新情報を受け取ることができます。

必要に応じて、後でオンラインリポジトリのソースを変更することができます。

[Configure System] > **[View and Apply Software Updates]** > **[Enable/Disable use of Online Repositories]** の順にクリックします。

オフラインリポジトリからオンラインリポジトリに切り替えると、通常、公開から24時間以内に Red Hat セキュリティ修正プログラムにアクセスできます。ほとんどのオフラインインストールでは、これを推奨しています。ただし、今後の Clearswift 製品のアップグレードにオンラインリポジトリも使用する予定がある場合にのみ、これを行う必要があります。

> オンラインからオフラインへの切り替えはサポートされておらず、将来的に更新の問題につながる可能性があります。

システムが最新の状態であることを確認するには、Server Console を使用してシステムまたは製品のアップグレードを適用する必要があります。コマンドラインを使ってアップグレードした場合、 'no updates available'と表示されます。

4. Clearswift SXG Interceptorのインストール

組織ごとの要件やインフラストラクチャーに応じて、次のオプションから選択できます。

- 単一の Microsoft Exchange Server、単一のSXG Interceptor、単一の Gateway
- 単一の Microsoft Exchange Server、単一のSXG Interceptor、複数の Gateway
- 複数の Microsoft Exchange Server、複数のSXG Interceptor、複数の Gateway

本ガイドでは、単一の Microsoft Exchange Server、単一のSXG Interceptor、単一の Gateway を使った構成について説明します。

Clearswift SXG Interceptorをインストールする前に、Exchange Gateway および Exchange Server で以下を完了しておく必要があります。

4.1 Exchange Gateway

1. 本インストール ガイドのセクション 3 に従って、SECURE Exchange Gateway をインストールおよび設定します。
2. Exchange Gateway 用の DNS エントリーを作成します。
3. SECURE Exchange Gateway の **[Exchange Server]** ページに Exchange Server を追加します。

   この手順の詳細については、Exchange Gateway オンライン ヘルプの *[Gateway と Exchange Server 間の通信の設定]* を参照してください。
4. Exchange Server の**クライアント ID** を書き留めておいてください。

4.2 Exchange Server

ユニバーサル セキュリティ グループと、設定ストアへのアクセスに使用するユーザーを作成する必要があります。

1. ユニバーサル セキュリティ グループを作成します。

   a. **[Active Directory ユーザーとコンピュータ]** で、フォレストのルート ドメインに ***Clearswift SXG Administrators*** と呼ばれるグループを作成します。**[グループの範囲]** が **[ユニバーサル]** に設定されていることを確認してください。

2. 設定ストアへのアクセスに使用するユーザーを作成します。

   a. **[Active Directory ユーザーとコンピュータ]** で、フォレストのルート ドメインにユーザーを作成します。**[パスワードを無期限にする]** チェックボックスを選択します。

3. ***[Clearswift SXG Administrators]*** グループにユーザーを追加します。

4. Interceptor のインストールを行うユーザーを ***[Clearswift SXG Administrators]*** グループに追加します。

5. さらに、SXG Interceptor Powershell コマンドレットを使用するすべてのユーザーを ***[Clearswift SXG Administrators]*** グループに追加します。

6. ログアウト後、再度ログインし、許可が有効になっていることを確認します。

4.3 Clearswift SXG Interceptorのインストール

1. https://www.clearswift.co.jp/support/portals にアクセスします。

2. Microsoft Exchange Server 上にSXG Interceptor インストーラーをダウンロードします。

3. Clearswift SXG 管理者グループのメンバーであるアカウントを使って、Microsoft Exchange Server にログオンします。

4. Windows Explorer を使ってダウンロードしたSXG Interceptor インストーラーを検索し、これを実行します。

5. セットアップ ウィザートの指示に従います。

   後続の表に、ウィザードのページに関する追加情報が記載されています。

ウィザードページ	追加情報
機能の選択	新たな配置で最初の Interceptor をインストールする際は、次のオプションを選択します。 ▪ Clearswift SXG Interceptor ▪ Clearswift SXG Interceptor Configuration Store ▪ Clearswift SXG Management Shell

ウィザード ページ	追加情報
	注記: インストールの対象から除外した機能は、インストーラーの実行時に再度提示されます。 設定ストアを Microsoft Exchange Server に保存したくない場合は、**[New instance]** チェックボックスのチェックを外します。 **注記:** 設定ストアなしで Interceptor をインストールするには、事前に別のサーバーに設定ストアがインストールされている必要があります。
前提条件の確認	Exchange、PowerShell、Microsoft.Net、Active Directory ライトウェイト ディレクトリー サービス (AD LDS) のすべてのバージョンがサポートされていることを確認してください。
インストール設定	SXG Interceptorをインストールする場合は、Exchange サーバーのクライアント ID を提示する必要があります。 ヒント: Exchange Gateway の [Exchange Server] ページからクライアント ID をコピーして貼り付けます。 この段階でクライアント ID がない場合は、SXG Interceptorのインストール後に設定できます。 *Client ID*についての詳細は、 Exchange Gateway のオンラインヘルプの「 Gateway と Exchange Server 間の通信の設定 」を参照してください。
Microsoft AD LDS 資格情報	設定ストアへのアクセス用に作成した、*DOMAIN\username* 形式のユーザー名を入力します。このアカウントは、SXG Interceptor 設定ストアの新たなインスタンスのインストール、およびアクセス権限を備えているはずです。

4.4 SXG Interceptor のインストールの完了

インストールを完了するには、最低条件として以下のタスクを実行する必要があります。

1. SXG Gateway を追加します
2. SXG Gateway を有効化します
3. SXG Interceptor を有効化します

この手順に続き、以下を実行することもできます(オプション)。

- Interception のルールの設定
- モニタ モードの使用。

- パフォーマンスカウンターを設定します
- インストールが有効であることを確認します

このセクションでは必須タスクについて説明します。

SXG Gateway を追加するには、**[Add-SXGGateway]** コマンドレットを使用します。この場合、次の操作を実行します。

1. **[スタート]** > **[すべてのプログラム]** > [**Clearswift SXG Interceptor**] > [**Clearswift SXG Interceptor Management Shell**] の順にクリックします。

   > Windows Server 2012 を使用している場合は、スタート画面で **Clearswift SXG Interceptor Management Shell**] アイコンをクリックします。

2. Gateway を追加します。コマンド ラインで次のコマンドを入力します。

```
Add-SXGGateway [[-Identity] <GatewayIdentity>]
[<CommonParameters>]]
```

   ここで、各スイッチの内容は以下のとおりです。

   - *<GatewayIdentity>* は追加する SXG の FQDN です。

     > FQDN を知るには、SXG UI から **[システム]** > **[イーサネットの設定]** をクリックします。

   - *<CommonParameters>* は verbose、debug などの一般的なパラメーターです。

> コマンドレットの詳細なヘルプは、**Clearswift SXG Interceptor Management Shell**を参照してください。それぞれのコマンドレットには拡張ヘルプオプションがあります。たとえば、*Add-SXGGateway* の例を確認するには、プロンプトに以下を入力します:
>
> ```
> get-help Add-SXGGateway -examples
> ```
>
> 技術的な情報については、プロンプトで次のコマンドを入力します。
>
> ```
> get-help Add-SXGGateway -detailed
> ```
>
> ```
> get-help Add-SXGGateway -full
> ```
>
> コマンドレットの一覧を表示するには、プロンプトで次のように入力します。
>
> ```
> get-command -module SXGInterceptor
> ```

3. Gateway を有効化します。コマンド ラインで次のコマンドを入力します。

```
Set-SXGGateway [[-Identity] <GatewayIdentity>] -Enabled
$true
```

   - *<GatewayIdentity>* は有効化する SXG の FQDN です。

4. Interceptor を有効化します。コマンド ラインで次のコマンドを入力します。

```
Set-SXGInterceptor [[-Identity] <InterceptorIdentity>] -
Enabled $true
```

   - *<InterceptorIdentity>* はSXG Interceptor がインストールされたサーバーの FQDN です。

> インターセプターは、同じADサイト同じピアグループに、内の Exchange Gateway のみ使用することができます。

インターセプトする規則の作成、およびパフォーマンスの監視などの Exchange Gateway を実行する上で必要な設定作業に関する情報は、Exchange Gateway のオンラインヘルプ を参照してください。

4.5 SXG Interceptor のインストールの検証

SXG Interceptor のインスールを検証するには、**Clearswift SXG Interceptor Management Shell**の次のコマンドを使用します。

```
Get-SXGSettings
```

予期される結果:: AD LDS ユーザー名、ログレベル、セキュリティプロトコルタイプが表示されるはずです。

```
Get-SXGInterceptor
```

予期される結果:: Interceptor の詳細が表示されるはずです。最初のインストールがExchange 以外のサーバーの設定ストアで行われた場合、詳細は表示されません。

```
Get-SXGInterceptionRules
```

予期される結果:: デフォルトの規則が表示されるはずです。

```
Get-SXGGateway
```

予期される結果:: レポートされたサイトに、Exchange が存在するサイトが含まれているはずです。

4.6 SXG Interceptor のテスト:

1. Exchange Server コンピュータで、Outlook または Outlook Web App のいずれかを使って電子メール メッセージをテスト送信します。
2. Exchange Gateway の **[ホーム]** ページで、**[最近のメッセージ]** エリアを確認します。
3. SXG Interceptor ログ (C:\ProgramData\Clearswift\SXGInterceptor\logs) を確認します。
4. **[イベント ビューア]** を使って、**[アプリケーション]** のイベント ログを表示します。

5. Clearswift SECURE Exchange Gateway バージョン 3.8 からのアップグレード

> Clearswift SECURE Exchange Gateway を初めてインストールする場合は、このセクションを省略してください。

Clearswift SECURE Exchange Gateway バージョン 3 からバージョン 4.7.0 にインストールする場合には、 まずGatewayバージョン 3 の最新バージョン である バージョン 3.8 に完全にアップグレードしてから、次の指示に従ってください。

このセクションでは、ポリシー設定とシステム設定を、Clearswift SECURE Exchange Gateway バージョン 3.8 から4.7.0にインポートする方法を説明します。Clearswift SECURE Exchange Gateway 4.7.0 をインストールする前に、既存のバージョンでバックアップを実行してください。

> Gateway バージョン 3 からの移行は、static hosts、static route、および DNS のなどのネットワーク設定は保存されません。Gatewayのアップグレード時に、Server Consoleを使用してネットワーク設定を再設定してください。クライアント統合認証を使用している場合、移行後に、再度ドメインに参加してください。

5.1 オリジナル システムのバックアップ

> FTP サーバーのシステム バックアップは、最新の適用された設定のみ対象となります。それよりも前のポリシー設定、および検疫されたメッセージ、監査とトラッキング データ、ログが必要な場合には、まずシステム バックアップからの復元を行い、次に新しい Gatewayのインストール後に .bk ファイルを復元する必要があります。

1. 設定を適用します。これにより、最新バージョンに移行します。
2. 既存のGateway システムを使用して、**[システム センター]** > **[バックアップとリストア]** ページに移動します。
3. タスク パネルの **[今すぐシステムをバックアップ]** オプションを使用して、システム バックアップを実行します。

使用可能なシステム領域をすべてバックアップすることをお勧めします。

システム バックアップは、障害復旧の手段として、またシステム アップグレード計画の際に使用することをお勧めします。他の目的で (たとえば、ピア グループを作成するときのGateway のクローンを作成する手段として) 使用しないでください。障害復旧およびシステム アップグレード以外の目的がある場合は、設定のバックアップとリストアを使用してください。

5.2 Gateway のインストール 4.7.0

このインストール ガイドの手順に従って Clearswift SECURE Exchange Gateway をインストールします。

Clearswift SECURE Exchange Gateway をインストールしたら、ソフトウェアの最新の更新ファイルがある Clearswift のオンライン リポジトリーへのアクセスを有効化する必要があります。一へのアクセスを設定する必要があります。詳細については、「 Clearswift オンラインリポジトリーへのアクセスの有効化 」を参照してください。

Interceptor を完全にインストールしてアップグレードするまでは、Gateway 4.7.0 を設定に追加しないでください。

Exchange Server を含む各 Active Directory サイトに、最低 2 つの Exchange Gateways (SXG) をインストールすることをお勧めします。SXG Interceptor は Gateway の IP アドレスを使って、Gateway が存在する各 AD サイトを定義します。

4.7.0 SXG と Exchange Server 間の情報フローを最大化し、SXG Interceptor が使用するクライアント ID を共有するためには、Exchange Gateway をピア接続する必要があります。

5.3 システム バックアップの復元

1. 新規のインストール済みGatewayを使用して、**[システム センター]** > **[バックアップとリストア]** ページに移動します。
2. タスク パネルのオプションを使用して、**[システムの復元]** を選択します。FTP 設定を入力し、**[接続]** をクリックします。

システムの復元には、バックアップの作成時に設定したすべての領域が含まれます。また、設定 および監査ログが含まれる場合もあります。システムの復元が完了すると、Gateway は再起動します。

6. Clearswift SECURE Exchange Gateway バージョン 3.8 からのアップグレード

> Clearswift SECURE Exchange Gateway を初めてインストールする場合は、このセクションを省略してください。

Clearswift SECURE Exchange Gateway バージョン 3 からバージョン 4.7.0 にインストールする場合には、 まずGatewayバージョン 3 の最新バージョン である バージョン 3.8 に完全にアップグレードしてから、次の指示に従ってください。

このセクションでは、ポリシー設定とシステム設定を、Clearswift SECURE Exchange Gateway バージョン 3.8 から4.7.0にインポートする方法を説明します。Clearswift SECURE Exchange Gateway 4.7.0 をインストールする*前*に、既存のバージョンでバックアップを実行してください。

> Gateway バージョン 3 からの移行は、static hosts、static route、および DNS のなどのネットワーク設定は保存されません。Gatewayのアップグレード時に、Server Consoleを使用してネットワーク設定を再設定してください。クライアント統合認証を使用している場合、移行後に、再度ドメインに参加してください。

6.1 アップグレード プロセスの概要

SECURE Exchange Gateway バージョン 3.8 から 4.7.0 への移行のアップグレードの方法として、次の手順をお勧めします。インプレース アップグレードは現時点では利用できないため、次の手順で段階的なアプローチを行うことをお勧めします。

1. 既存のすべての Exchange Gateway 3.8 の設定をバックアップします。
2. ドメイン フォレスト内のすべての Exchange Server の Interceptor をアップグレードします。
3. このインストール ガイドの手順に従って、Clearswift SECURE Exchange Gateway (SXG) 4.7.0をインストールします。複数の SXG をピア接続することをお勧めします。
4. Gateway 3.8 から新しくインストールした Gateway 4.7.0 に設定を復元します。必要な場合、既存の Gateway ピアを 4.7.0 の設定に追加します。

5. Exchange Server の SXG Management Shellで Add-SXGGateway コマンドレットを使って、Gateway 4.7.0 の設定を追加します。SXGGateway コマンドレットを使って新しい Gateway を有効化し、Set-SCGGateway コマンドレットを使って古い Gateway を無効化します。

6. Gateway 3.8 のすべての保留メッセージが解放、削除、転送、または Gateway 4.7.0に復元されていることを確認します。Gateway 3.8 が削除されると、それらのメッセージは配信できません。

7. Remove-SXGGateway コマンドレットを使用して Gateway 3.8 を削除します。

> 実稼働環境にできるだけ近い、実稼働以外の環境で、まずこのアップグレード プロセスを実行することを強くお勧めします。

6.2 オリジナル システムのバックアップ

> FTP サーバーのシステム バックアップは、最新の適用された設定のみ対象となります。それよりも前のポリシー設定、および検疫されたメッセージ、監査とトラッキング データ、ログが必要な場合には、まずシステム バックアップからの復元を行い、次に新しい Gatewayのインストール後に .bk ファイルを復元する必要があります。

1. 設定を適用します。これにより、最新バージョンに移行します。

2. 既存のGateway システムを使用して、**[システム センター]** > **[バックアップとリストア]** ページに移動します。

3. タスク パネルの **[今すぐシステムをバックアップ]** オプションを使用して、システム バックアップを実行します。

   > 使用可能なシステム領域をすべてバックアップすることをお勧めします。

   > システム バックアップは、障害復旧の手段として、またシステム アップグレード計画の際に使用することをお勧めします。他の目的で (たとえば、ピア グループを作成するときのGateway のクローンを作成する手段として) 使用しないでください。障害復旧およびシス

テム アップグレード以外の目的がある場合は、設定のバックアップとリストアを使用してください。

6.3 SXG Interceptor のアップグレード

トランスポート役割 (Exchange 2007 または 2010) または メールボックス役割 (Exchange 2013 または 2016) を持つ、組織内のすべての Exchange Server には、既存の SXG Interceptor がインストールされている必要があります。すべてのサーバーに Interceptor がインストールされていない場合、Exchange Gateway は組織内のすべての内部メールを処理できない場合があります。

SXG Gateway 4.7.0 がメールを処理する様に設定する前に、既存の Interceptor を 4.7.0 にアップグレードしておく必要があります。

1. Interceptor のインストーラーを検索し、セットアップ ウィザードを使ってインストールを実行します。
2. 入力を求められたら、SXG サービス アカウントにアカウントの詳細を入力します。

SXG Interceptor をインストールする前に、Microsoft Exchange トランスポート サービス (MSExchangeTransport) を停止する必要はありません。しかしながら、このサービスはアップグレード処理中に停止します。アップグレードが完了してサービスが再起動されたときに、すべてのキュー メッセージは配信されます。

アップグレードはピーク時間を避けて行うことをお勧めします。MSExchangeTransport の再起動には通常、数分間かかりますが、キュー メッセージがある場合には、より時間がかかる場合があります。

6.3.1 アンインストールと再インストール

SXG Interceptor をアンインストールして再インストールする場合、または追加の Exchange Server を追加して Interceptor を初めてインストールする場合、デフォルトでは SSL3 は設定されません。

SXG Interceptor を設定する際にはSSL3プロトコルを含めるようにしてください。これによって Interceptor は既存の 3.8 Exchange Gateway と通信できます。

1. SXG Management Shellで、次のコマンドレットを実行します。

   Set-SXGSettings –SecurityProtocolTypes “tls12 tls11 tls ssl3”

2. 3.8 SXG Gateway と新しい Interceptor をモニターし、設定が正しく動作していることを確認します。

> Get-SXGInterceptor コマンドレットを実行して、SXG Interceptor のバージョンを表示し、バージョン プロパティーを確認します。例:
>
> Get-SXGInterceptor | Select-Object identity,version
>
> Get-SXGInterceptor | fl identity,version
>
> Get-SXGInterceptor | ft identity,version

6.4 Gateway のインストール 4.7.0

このインストール ガイドの手順に従って Clearswift SECURE Exchange Gateway をインストールします。

Clearswift SECURE Exchange Gateway をインストールしたら、ソフトウェアの最新の更新ファイルがある Clearswift のオンライン リポジトリーへのアクセスを有効化する必要があります。一へのアクセスを設定する必要があります。詳細については、「Clearswift オンラインリポジトリーへのアクセスの有効化」を参照してください。

> **Interceptor を完全にインストールしてアップグレードするまでは、Gateway 4.7.0 を設定に追加しないでください。**
>
> Exchange Server を含む各 Active Directory サイトに、最低 2 つの Exchange Gateways (SXG) をインストールすることをお勧めします。SXG Interceptor は Gateway の IP アドレスを使って、Gateway が存在する各 AD サイトを定義します。
>
> 4.7.0 SXG と Exchange Server 間の情報フローを最大化し、SXG Interceptor が使用するクライアント ID を共有するためには、Exchange Gateway をピア接続する必要があります。

6.5 Exchange 環境の準備

Exchange Server のInterceptor 設定に、Clearswift SECURE Exchange Gateways (SXG) を、いつでも追加することができます。しかしながら、Gateway を設定してメッセージ を処理できるようにするまでは、Gateway を*有効化*しないでください。

6.5.1 Exchange Gateway を SXG Interceptor 環境に追加する方法:

1. Clearswift SXG 管理シェルで、Add-SXGGateway コマンドレットを使って、Gateway 4.7.0 を SXG 設定に追加します。

   Add-SXGGateway sxg1.example.com

   Add-SXGGateway 192.168.2.10

2. 新しい Gateway のホスト 'A' レコードが DNS に追加されていることを確認します。

必要な場合には、SXG を手動でサイトに割り当てる必要があります (自動サイト割り当てがデフォルトの設定で使用できない場合)。SXG Interceptor は SXG の IP アドレスを使用して一致するサイトを検索しますが、これは次のコマンドレットを使って上書きできます。

Set-SXGGateway sxg1.example.com -AssignedSites Site2

Gateway 'sxg1' は 'Site2' に割り当てられます。

6.6 SECURE Exchange Gateway 環境の準備

Exchange Gateway 4.7.0 をインストールしてピア接続したら、Gateway 3.8 の設定を復元します。保存した設定ファイルを復元するか、または FTP システム バックアップから復元することができます。

> 保存した設定を復元する場合は、ポリシー ルート、テキスト検索式、Exchange Server クライアント ID などの設定アイテムのみを復元します。システム バックアップを使って、保留メッセージ、レポート データ、システム ログを復元します。

6.6.1 システム バックアップの復元

1. 新規のインストール済みGatewayを使用して、**[システム センター]** > **[バックアップとリストア]** ページに移動します。

2. タスク パネルのオプションを使用して、**[システムの復元]** を選択します。FTP 設定を入力し、**[接続]** をクリックします。

> システムの復元には、バックアップの作成時に設定したすべての領域が含まれます。また、設定 および監査ログが含まれる場合もあります。システムの復元が完了すると、Gateway は再起動します。

6.6.2 システム バックアップの復元

システム バックアップの復元には、システム領域とポリシー設定が含まれます。システム バックアップを使って Gateway を復元する場合には、サーバーごとに移行を行い、新しい Exchange Gateway がメッセージの処理を始める前に古い Gateway を無効化する必要があります。

> ネットワーク構成は古い Gateway から復元されません。ネットワーク設定を設定するには、Gateway コンソールを使用します。詳細については、オンライン ヘルプの「ネットワーク設定」を参照してください。

6.6.3 設定の復元

新しい Exchange Gateway と平行して古い Gateway がメールを処理するようにする場合には、設定の復元が適切です。詳細についたは、オンラインヘルプの「設定のバックアップとリストアについて」を参照してください。

6.6.4 設定の完了

設定を適用する前に、設定アイテムが正しく復元されていることを確認します。

- ポリシー定義(ルート、コンテンツルール)
- ポリシーの参照(電子メールアドレス、ディスポーザルアクション、テキスト検索式)
- ファイル リスト
- Exchange Serverのクライアント のID

  > Exchange Gateway 3.8のの設定に、FQDN を使用して定義されたExchange Server が含まれている場合、これらは Gateway 4.7.0 の設定の IP アドレスに変換されます。Exchange Gateway バージョン 4.7.0 では、FQDNを使用してExchange Serverを入力することはできないためです。4.7.0 に IP アドレスを設定すると Gateway 3.8 の設定に Exchange Server を追加すると DNS ルックアップを解決できます。

- 通知
- PMM ユーザー情報 (該当する場合)

PMM をバックアップから復元する場合には、PMM ポータルを設定するための追加の設定が必要です。

設定を適用します。

6.6.5 ピアリング

移行中は、Exchange Gateway 4.7.0 と、環境内の既存の Exchange Gateway 3.8 の設定の復元と適用が完了した後ピアリングすることをお勧めします。次のことができます。

- すべての Gateway のメッセージ キューの表示
- Exchange Gateway とピア接続された既存の Clearswift SECURE Email Gateway (SEG) との間のメッセージのトラッキング
- 保留メッセージの表示、解放、転送、削除
- 両方のバージョンのレポートへのアクセス
- ブラックリスト イメージ、ホワイトリスト イメージなどのイメージ データの共有
- PMM データのアクセス (該当する場合)

最新のRHELの更新に後、Gateway バージョン 4 と Gateway バージョン 3 をピアすることはできません。 この問題の詳細については、Clearswift SECURE Exchange Gateway ヘルプ の「既知の問題」の「 **RHELを更新した後、Gateway バージョン 4 と Gateway バージョン 3 とのピアができない**」を参照してください。

残りの Exchange Gateway ゲートウェイは、バージョン3.8.8以降で動作している必要があります。

異なるバージョンで動作する Gateway との間で設定を適用することはできません。

Gateway をピアリングしている場合、設定を適用すると、互換性に関する警告が発生する場合があります。

6.7 4.7.0 のGateway の有効化

SXG Interceptor を SECURE Exchange Gateway 4.7.0 にアップグレードして設定を復元すると、4.7.0 の Gateway を有効化してメッセージを処理できます。これにより Gateway は、AD サイト内の新しい SXG の IP アドレス設定に一致するすべての Interceptor から、メールを受信できます。

6.7.1 4.7.0 のExchange Gateway を有効化する方法

SXG 管理シェルで、Set-SXGGateway コマンドレットを実行します。例:

- Set-SXGGateway sxg1.example.com –Enabled $true

> 最初の SXG 4.7.0 を有効化し、構成全体に段階的に配置する前に、テスト期間とします。

6.7.2 3.8 のExchange Gateway を無効化する方法

SXG 4.7.0 を段階的に配置する場合、各 4.7.0 の SXG を有効化した後に、次のコマンドレットを使って、対応する各 3.8 の SXG を無効化できます。

- Set-SXGGateway sxg38.example.com –Enabled $false

> Gateway が無効化されている間も、4.7.0 の Gateway とピア接続されている場合には、メッセージを処理できます。削除されると、それはできません。
>
> 3.8 の SXG を*削除*する前に、すべての保留メッセージを解放、配信または転送します。

6.8 3.8 の Gateway の削除

Gateway のテスト、安定化、モニタを行った後で、設定から 3.8 の SXGを削除します。

> 削除する Gateway に保留メッセージがないことを確認します。

6.8.1 3.8 の SXG Gateway を削除する方法

次のコマンドレットを実行します。

- Remove-SXGGateway sxg38.example.com

6.8.2 SXG Interceptor の SSL3 を無効化します

すべての 3.8 の Exchange Gateway を削除したら、それぞれの Interceptor に次のコマンドレットをローカルで実行します。

- Set-SXGSettings -SecurityProtocolTypes "Tls12 tls11 tls"

7. リリース 4.x からリリース 4.7.0 へのアップグレード

Clearswift SECURE Exchange Gateway を初めてインストールする場合は、このセクションを省略してください。

Clearswift SECURE Exchange Gateway 4.7.0 へのアップグレード時には、以下の手順に従いソフトウェア更新をダウンロードして適用してください。

SSH セッションを開き、Clearswift Server Console にアクセスします。cs-admin アクセス資格情報を使用してログインします。

オンラインモードとオフラインモード

*オフラインモードは、インストールがインターネットから切断された閉じた環境で動作するように設計されています。*特殊なシステムの要件がある場合を除き、**オンラインモード**で Clearswift SECURE Exchange Gatewayをインストールしてください。

オフライン アップグレードを実行するには、適切なメディア (DVD/USB) にマウントされた最新リリースの ISO コピーが必要です。この手順を完了するために、さらにガイダンスが必要な場合には、Clearswift テクニカル サポートにお問い合わせください。

オンラインリポジトリが有効になっている場合、更新は夜間に(自動的に) ダウンロードされます。すぐに適用することができます。最新のセキュリティ修正が発行されたと思われる場合は、**[Check for New Updates]** ボタンを使用することもできます。

ソフトウェア更新プログラムを適用するには:

1. Clearswift Server Console のメイン メニューで **[Configure System]** > **[View and Apply Software Updates]** > **[Apply Updates]** > **[OK]** の順に選択します。

2. **[Yes]** をクリックして、更新ファイルの適用を確認します。
   ダウンロードされたすべての更新がインストールされます。この処理には数分かかることがあります。進行状況ログが表示されます。

3. *操作完了*のメッセージが表示されたら、**[Done]** をクリックしてインストール処理を完了します。

アップグレードのプロセスの最後に、システムを再起動するか、ログアウトするように求めるメッセージが表示されます。画面の指示に従ってください。

どちらの場合も、Gateway サービスは自動的に再起動します。

アップグレードが完了したら、次のことを行う必要があります。

- 意図したとおりに動作するよう TLS の設定を変更します。アップグレードする以前のバージョンで TLS を設定していない場合は、この手順を無視してください。

> アップグレードするとメールフローが停止する**SMTP Inbound Transport**, **SMTP Outbound Transport**, and **SMTP Alert Transport** サービスを再起動してメールフローを有効にする前に、コネクションプロファイルで強制的 TLS の送信設定を変更する必要があります。

- 送信 TLS の場合、電子メールルーティングテーブルエントリーをコネクションプロファイルに関連付けます。
  ユーザーインターフェースに、関連付けを必要とするコネクションプロファイルの一覧に警告が表示されます。

- メールフローを再起動します。この手順は、以前のバージョンでアウトバンドの強制的 TLS を使用していた場合にのみ適用します。

- コネクションプロファイルのクライアントホストおよび送信者ドメインリストのメンテナンスを行います。送信者ドメインを別に設定します。
  アップグレード時にIPアドレス以、外両方のリストに配置されるため、クライアントホストリストからドメインを削除し、送信者ドメインリストからホストを削除する必要があります。詳細については、「 SMTP コネクションの管理」を参照してください。

8. SXG Interceptor のトラブルシューティング:

以下の情報は、Exchange Interceptor のインストールに関する問題への対処に役立ちます。

8.1 Interceptor に関する情報の表示

1. **Clearswift SXG Interceptor Management Shell**を開きます。
2. 以下を入力します。

```
Get-SXGInterceptor | Format-List
```

Interceptor に適用される値とともに、次の情報が表示されます。

```
Identity : HUB1.example.com InterceptorIdentity :
HUB1.example.com State : Inactive Enabled : True ClientID :
94bbc203-81a2-45be-a5ff-54c6a3dadad3 MonitorModeEnabled :
False QueueLength : 0 Version : 4.3.0.nHUB1.example.com
InterceptorIdentity : HUB1.example.com
State               : Inactive
Enabled             : True
ClientID            : 94bbc203-81a2-45be-a5ff-54c6a3dadad3
MonitorModeEnabled  : False
QueueLength         : 0
Version             : 4.5.0.n
```

8.2 SXG Interceptor がトランスポート エージェントとしてインストールされているかどうかの確認

1. **Clearswift SXG Interceptor Management Shell**を開きます。
2. 以下を入力します。

```
Get-TransportAgent
```

以下の情報が表示されます。

```
Identity                                                  Enabled
      Priority
--------                                                  -------
      --------
Transport Rule Agent                                      True
      1
Text Messaging Routing Agent                              True
```

```
      2
Text Messaging Delivery Agent                          True
      3
ClearswiftSXGInterceptor                               True
      4
```

8.3 ログ レベルの設定

ログ レベルを設定するには、**Clearswift SXG Interceptor Management Shell** の次のコマンドを使用します。

```
Set-SXGSettings -LogLevel [Off|Error|Warn|Info|Debug]
```

付録：ソフトウェアインストールプロセス(ディスクから)

ISO イメージを使用して既存の Red Hat Enterprise Linux (RHEL) 6.9 サーバー (適切に設定された AWS または Azure のインスタンスを含む) 上に、Clearswift SECURE Exchange Gateway をインストールする手順は次の通りです。

> RHEL 6.9 を**最小限**のサーバーとしてインストールし、/(root) パーティションと /var パーティションを個別に作成する必要があります。ルートパーティションに、最小限 20 GB、テスト環境のために/ varは最小限 60GB と本番環境のために 200GB が必要です。

Clearswift SECURE Exchange Gateway をインストールするには:

1. コマンド ラインで root の権限を使用します。
2. ISO イメージが格納されているメディアを挿入し、/media/os にマウントします。

```
mkdir -p /media/os
```

```
mount /dev/cdrom /media/os
```

3. cs-emailweb-repo-confemail-repo-conf パッケージを手動でインストールします。cs-emailweb-repo-confemail-repo-conf パッケージは、 Clearswift SECURE Exchange Gatewayをインストールするための準備をシステムに設定します。

```
rpm -ivh /media/os/cs-repo/Packages/cs-email-repo-conf-
3.4.1-2526.x86_64.rpm
```

4. postfix、rsyslog、samba V3 を強制的に削除します。

```
yum -y remove postfix rsyslog samba-common
```

5. 次のコマンドを使用して、必要な製品をインストールします。

```
yum install -y cs-sxg --enablerepo=cs-*
```

このコマンドは、外部リポジトリへのアクセスを可能にし、その後 Clearswift リポジトリのみが Gateway のインストールに使用されることを保証します。

> 新たな不一致事項のために手順 5 が失敗する場合は、手順 4 の間に別のパッケージの削除が必要な場合があります。

6. 完全にログアウトし、cs-admin として再度ログインします。「 First Boot Console の実行」を参照して 作業を続行します。

インストール後の注意事項

ソフトウェアのインストール プロセス完了後には、インストール プロセスにより、次のシステムの一部が変更されている場合があります。

1. ファイアウォールの設定は、Gateway の制御下になりました。SSH アクセスが必要な場合には、Clearswift SECURE Exchange Gateway ユーザー インターフェースから再度有効化する必要があります。詳細については、オンラインヘルプからClearswift SECURE Exchange Gateway の「 SSH アクセスの設定」を参照してください。

2. すべてのネットワーク構成は Server Console の制御下となりました。コマンドラインでネットワーク構成を変更すると、Gateway にネットワーク構成の変更が通知されないため、避けなくてはなりません。コマンドラインからネットワーク構成を変更する必要がある場合には、Clearswift サポートにお問い合わせください。

3. crontab の構成が変更されます。既存の root の cronjobs が失われる可能性がありますが、それらを再度追加することができます。

ソフトウェアのインストールプロセスが完了したら...

ソフトウェアのインストールプロセスでは、既存のリポジトリ構成は自動的に無効になりません。コマンドラインから追加のサードパーティ製ソフトウェアを通常の方法でインストールすることができます。これには追加の RedHat ソフトウェアが含まれます。

> 4.6 以降のバージョン では、Clearswift Server Consoleを使用して Clearswift が提供するアップグレードのみを適用することができます。Server Console では、アップグレードプロセス中に信頼できる Clearswift リポジトリのみが使用され、プロセス中にサードパーティのリポジトリからの意図しない更新が明示的にブロックされます。

付録：ソフトウェアのインストールプロセス(Clearswift オンラインリポジトリから)

次の手順では、Clearswift がオンラインでホストしているリポジトリを使用して、既存の Red Hat Enterprise Linux(RHEL) 6.9 サーバー(適切に構成された AWS または Azureのインスタンスを含む) に Clearswift SECURE Exchange Gateway をインストールする方法を説明します。このインストールを完了するには、インターネットにアクセスする必要があります。

> RHEL 6.9 を**最小限**のサーバーとしてインストールし、/(root) パーティションと /var パーティションを個別に作成する必要があります。ルートパーティションに、最小限 20 GB、テスト環境のために/ varは最小限 60GB と本番環境のために 200GB が必要です。

Clearswift SECURE Exchange Gateway をインストールするには:

1. コマンド ラインで root の権限を使用します。
2. cs-emailweb-repo-confemail-repo-conf パッケージを手動でインストールします。cs-emailweb-repo-confemail-repo-conf パッケージは、 Clearswift SECURE Exchange Gatewayをインストールするための準備をシステムに設定します。

```
rpm -ivh http://repo.clearswift.net/rhel6/gw/os/x86_64/Packages/cs-email-repo-conf-3.4.1-2526.x86_64.rpm
```

3. postfix、rsyslog、samba V3 を強制的に削除します。

```
yum -y remove postfix rsyslog samba-common
```

4. 次のコマンドを使用して、必要な製品をインストールします。

```
yum install -y cs-sxg --enablerepo=cs-*
```

このコマンドは、外部リポジトリへのアクセスを可能にし、その後 Clearswift リポジトリのみが Gateway のインストールに使用されることを保証します。

> 新たな不一致事項のために手順 5 が失敗する場合は、手順 4 の間に別のパッケージの削除が必要な場合があります。

5. 完全にログアウトし、cs-admin として再度ログインします。「 First Boot Console の実行」を参照してください。

インストール後の注意事項

ソフトウェアのインストール プロセス完了後には、インストール プロセスにより、次のシステムの一部が変更されている場合があります。

1. ファイアウォールの設定は、Gateway の制御下になりました。SSH アクセスが必要な場合には、Clearswift SECURE Exchange Gateway ユーザー インターフェースから再度有効化する必要があります。詳細については、オンライン ヘルプからClearswift SECURE Exchange Gateway の「SSH アクセスの設定」を参照してください。

2. すべてのネットワーク構成は Server Console の制御下となりました。コマンドラインでネットワーク構成を変更すると、Gateway にネットワーク構成の変更が通知されないため、避けなくてはなりません。コマンドラインからネットワーク構成を変更する必要がある場合には、Clearswift サポートにお問い合わせください。

3. crontab の構成が変更されます。既存の root の cronjobs が失われる可能性がありますが、それらを再度追加することができます。

ソフトウェアのインストールプロセスが完了したら...

ソフトウェアのインストールプロセスでは、既存のリポジトリ構成は自動的に無効になりません。コマンドラインから追加のサードパーティ製ソフトウェアを通常の方法でインストールすることができます。これには追加の RedHat ソフトウェアが含まれます。

> 4.6 以降のバージョン では、Clearswift Server Consoleを使用して Clearswift が提供するアップグレードのみを適用することができます。Server Console では、アップグレードプロセス中に信頼できる Clearswift リポジトリのみが使用され、プロセス中にサードパーティのリポジトリからの意図しない更新が明示的にブロックされます。

付録: USB インストール メディアの準備

次の手順では、Clearswift SECURE Exchange Gateway ソフトウェアの ISO イメージを USB メディアにコピーする方法を説明します。

1. Clearswift SECURE Exchange Gateway ソフトウェアの ISO イメージを、オンライン Clearswift リポジトリーからダウンロードします。

   > 必ず正しいバージョンの ISO イメージを使用してください。EMAIL_470_170.iso

2. ドライブのボリューム名を保持する USB ツールをダウンロードします。Rufus Portable の使用をお勧めします。

   > このプロセスにRufusの標準バージョンを使用しないでください。ポータブル版であることを確認してください。

   > Rufusの代わりにUSBツールを使う場合、以下のUSBツールはClearswift SECURE Exchange GatewayのソフトウェアISOイメージでは使用できません:
   >
   > - YUMI
   > - Universal USB Installer
   > - Fedora liveusb-creator

   次の手順では Rufus 2.11 Portable の使用を想定しています。

3. **rufus-2.11p.exe**を実行します。
4. USB メディアを挿入し、それを**[デバイス]** ドロップダウン メニューから選択します。
5. **[フォーマット オプション]** から **[ブート可能なディスクの作成]** を選択し、ディスク アイコン を選択して、書き込みを行うClearswift SECURE Exchange Gateway ISO を選択します。Rufus は ISO をスキャンし、他のオプションは自動的に記入されます。
6. **[Start]** をクリックします。**[ISOHybrid image detected]** のダイアログ ボックスが表示されます。**[Write in ISO Image mode (Recommended)]** を選択し、**[OK]** をクリックします。ドライブの既存のすべてのデータが削除されることを警告するダイアログ ボックスが表示されます。続行する場合は **[OK]** をクリックします。

7. インストールが完了したら、「 Clearswift SECURE Exchange Gatewayのインストール手順 」に戻ります。