

Technical Information	
文書番号	SYMC-SBG-091111-1
タイトル	Symantec Brightmail Gateway Version 8.0.3-11 リリースノート
対象機器	Symantec Brightmail Gateway 8200/8300 Series
ソフトウェアバージョン	8.0.3-11
プラットフォーム	-
参照	-
問合せ先	日商エレクトロニクス株式会社 ソリューションパートナー事業本部 技術統括部 サポート第一グループ E-mail: symc-support@nissho-ele.co.jp

### 本書について

Symantec Brightmail Gateway 8200/8300 Series(以下 SBG) Version 8.0.3-11 に関する情報が含まれています。

## 本リリースについて

SBG Version 8.0.3-11 は、Version 8.0.2-12 のパッチアップデートとなります。

## リソース

詳細な情報は以下より入手可能です。

<メーカーマニュアル/メーカーリリースノート(日本語)>

<http://www.symantec.com/region/jp/techsupp/enterprise/sbm/8.0/manuals.html>

<メーカー ナレッジベース(英語)>

[http://www.symantec.com/business/support/knowledge\\_base\\_sli.jsp](http://www.symantec.com/business/support/knowledge_base_sli.jsp)

## 新機能または強化点

Version 8.0 の主な新機能 (Version 7.7 と比較) は以下となります。

- ・ 接続クラス
  - 自己学習機能が強化されました。
  - インバウンド IP アドレスの接続を動的に分類し、管理可能になりました。
- ・ ファストパス
  - 正当なメッセージを動的にスパムスキャンから免除することが可能になりました。
- ・ Brightmail レピュテーション統合管理
  - レピュテーションデータに基づいてフィルタ処理を実行する複数の機能が、[レピュテーション] タブに統合されました。
- ・ バウンス攻撃防止
  - バウンス攻撃から保護する機能が追加されました。
- ・ Vontu Network Prevent との統合
  - Vontu Network Prevent と連携し機密データの漏洩を防止可能になりました。
  - 弊社では本機能はサポート対象外とさせて頂いておりますので、本機能をご使用頂いた場合のお問い合わせには対応致しかねます。予めご了承の程お願い申し上げます。
- ・ ログの強化点
  - ローカルとリモート(Syslog)のログレベルを変更可能になりました。
- ・ 複数のダウンストリーム MTA のサポート
  - 最大 3 つの静的経路をメール配信用のリレーとして定義できるようになりました。
- ・ 配信バインド戦略
  - ローカルおよび非ローカルの電子メール用と、スパム検疫への電子メール用の送信元の IP アドレスを指定可能になりました。
- ・ 改善されたキュー管理
  - キュー内のメッセージ数に制限を設けることが可能になりました。

- ・ レポート
  - 接続クラスの概略レポートで、接続クラスごとの接続データの概略が追加されました。
  - レピュテーションの概略レポートと接続の概略レポートが強化されました。
- ・ メッセージ監査ログの強化
  - ファストパスと接続クラスを判定可能になりました。
- ・ ドメインがない送信者アドレスのデフォルトドメイン
  - アウトバウンドメッセージの送信元メールアドレスにドメインが含まれていない場合に、デフォルトのドメインを設定可能になりました。
- ・ ポリシー単位のアーカイブ
  - 電子メールアドレスのアーカイブをポリシー単位で設定可能になりました。
- ・ インシデント管理のメッセージをそのまま転送するためのオプション
  - もとのメッセージをそのまま転送するためのフィールドが追加されました。
- ・ 不達メッセージをメッセージ監査ログで特別に追跡
  - 配信できなかった電子メールメッセージを、メッセージ監査ログで配信エラーとして追跡可能になりました。
- ・ ユーザーログインのバイパス機能
  - ユーザー名とパスワードを 1 回入力して、指定した期間においてコントロールセンターのログオンページをバイパス可能になりました。

### 変更された内容

Version 8.0 で変更された内容 (Version 7.7 と比較) は以下となります。

- ・ デフォルトで参照するレピュテーション情報が変更されました。
- ・ .cab ファイルがスキャン可能になりました。
- ・ スпам検疫ログイン URL を変更可能になりました。

- ・ ローカルに保存したバックアップを削除もしくはエクスポートが可能になりました。
- ・ SMTP グリーティングと postmaster アドレスのカスタマイズが可能になりました。
- ・ 送信者認証の SPF、SenderID で利用するドメインリストを更新しました。
- ・ MTA ログの出力形式が変更されました。
- ・ 8 ビット MIME の通知が選択可能になりました。

Version 8.0.2-12 で変更された内容は以下となります。

- ・ agent\_log のログレベルが変更可能になりました。
- ・ Symantec Brightmail Gateway DNS UDP パケットサイズを 512 バイトに制限されました。
- ・ Symantec Brightmail Gateway によってバウンスされる大容量のメッセージが切り捨てられるようになりました。
- ・ Symantec Brightmail Gateway の内部ホスト名を開示しないように変更されました。
- ・ LDAP 受信者検証の %u マクロと %d マクロが正しく代入されるようになりました。
- ・ OpenLDAP を使用して正しく処理できるようになりました。
- ・ MX レコードの優先度が 3 番目以降の場合に正しく試行されるようになりました。

## 追加/修正内容

- Version 8.0.3-11 の追加及び修正内容は以下となります。
  - ・ LDAP ルーティングにおいてクエリーフィルタが (uid=%u) の場合に、システムはメールアドレスのユーザー ID 部分に基づいたクエリーベースの検索が出来ない問題が修正されました。
  
- Version 8.0.2-12 の追加及び修正内容は以下となります。
  - ・ 同じサブネット上に 2 つのイーサネットインターフェースを設定した場合に、一方のイーサネットインターフェースの MAC アドレスが返される問題が修正されました。
  
- Version 8.0.1-7 の追加及び修正内容は以下となります。
  - ・ 「お気に入り」レポートを削除出来ない問題が修正されました。
  - ・ メッセージ監査ログにおいてリアルタイム検索できない問題が修正されました。
  - ・ メッセージ監査ログにて送信元が表示されない問題が修正されました。
  - ・ レポートの種類によってレポートの最後までスクロールできない問題が修正されました。
  - ・ 検疫のポート番号を他の通信のソースポートに使用され、検疫に隔離出来ない問題が修正されました。

## 日商ナレッジ

- ・ メッセージ監査ログの検索結果が最大設定値の 1000 件を超えた件数が表示される場合があります。  
1 通のメールで複数の宛先が含まれている場合、To 毎に件数が表示されるために、検索結果で表示される件数は最大設定値の 1000 件を超えた件数が表示されます。
- ・ メッセージ監査ログの処理に「メッセージを中止する」と表示される場合があります。  
「メッセージを中止する」とは送信元から SBG へメール送信する通信中にセッションが終了した場合に記録されます。  
調査方法は、SBG が接続されている SWITCH 側にてパケットを取得後に、送信元と SBG のどちらがパケットを切断しているかご確認下さい。  
SBG が切断している場合には弊社にて調査させていただきます。

## 既知の問題/注意事項

現在、Version 8.0.3-11 で確認されている問題は以下となります。

ここに記載の内容以外の問題に関しましてはメーカーリリースノートをご覧ください。

---

- ・ ウイルスのアクションがクリーニングで RAR 形式の圧縮ファイルからウイルスを検出した場合、圧縮内のウイルスのみ削除せず、RAR ファイル自体が削除されます。  
この動作により RAR ファイル内のウイルスに感染してない正常なファイルも削除されます。
- 

- ・ SBG の Interface1、Interface2 の両方に同一のサブネットを設定する場合、support アカウントで以下のコマンドを設定することにより、Interface2 の MAC アドレスが正しく返されるようになります。

```
$ set-eth-arp-ignore 1
```

---

- ・ private key とサーバ証明書のエクスポート、インポートは出来ません。
- 

- ・ インスタントメッセージ機能はサポート対象外とさせて頂いております。
- 

- ・ Vontu Network Prevent 機能はサポート対象外とさせて頂いております。
- 

- ・ 複数台構成において ScannerOnly の機能を使用して 1 台の ControlCenter で集中管理する構成を弊社が構築していない場合、保守サポートのご提供は致しかねますのでご了承の程お願い申し上げます。
    - 2007 年 10 月 10 日現在、既に上記構成で弊社と保守契約をご締結のお客様は引き続きサポートさせていただきます。
-



- 
- ・ レピュテーション > 悪い送信者の「シマンテックグローバルの悪い送信者」を有効。  
「SMTP 接続を拒否する」、「SMTP 接続を遅延する」を選択した場合、拒否や遅延以外の動作になる場合があります。
    - 動作説明経路: MTA1 MTA2 SBG の経路で SBG へメールを送信した場合
      - MTA2 の IP アドレスが「シマンテックグローバルの悪い送信者」と判定された場合は拒否、遅延の動作を行います。
      - MTA1 の IP アドレスが「シマンテックグローバルの悪い送信者」と判定された場合はメールを一度受信している為に拒否、遅延の動作が出来ずに次の動作になります。
        - 拒否を選択している場合: メールが削除され受信者にメールが届きません。
        - 遅延を選択している場合: メールが削除され受信者にメールが届きません。
  - また、送信者に対して以下のバウンスメールを送信します。  
件名: Returned Mail  
本文: Your message could not be delivered for the following reasons.  
This message has been blocked.
- 
- ・ コマンドラインを使用してサービスを停止した場合に、管理画面からサービスを開始することが出来ません。
- 
- ・ 過去バージョンにて検疫にメールが隔離することが出来ず、検疫ポートをデフォルト値 (41025) から変更している場合、v8.0 にアップデート後にデフォルト値(41025)に戻していただけますようお願いいたします。
    - アップグレード後、下記方法により変更します。  
管理 > コントロールセンター > リスナーポート を「41025」に変更し保存。  
本体再起動
-

- ・ グローバルレピュテーションの参照 DB が V8.0 から変更され、130 万から 2～4 億の登録数に増加しました。
    - グローバルレピュテーションでブロックされた場合、「IP レピュテーションルックアップ」から該当 IP を検索し、同ページのハイライト「削除の要求」より、Symantec(ipremoval)に削除要求をして下さい。
-

## アップグレードについて

Software Update(ソフトウェアの更新)にて入手/適用可能です。

アップグレード後に自動で OS の再起動が行なわれます。

### <アップグレードの注意事項>

- ・ アップデート前にバックアップを作成してください。
- ・ アップデート前にメールの受信をしないようにして各キューを解除 (Flush) することを推奨します。
  - [管理] -> [設定] -> スキャナのホストをクリックする。
  - 「着信メッセージを受け入れない」を選択して保存をする。
  - アップグレード後は「通常どおりにメッセージを受け入れて配信する」を選択して、保存をしてください。
- ・ 更新開始から完了まで、再ブートやシャットダウンを実行しないでください。
- ・ V4 より V8.0 へアップデートする場合は V5 を経由する必要があります。V5 及び V7 からは直接 V8 にアップデートできます。

#### ➤ V5 及び V7 からのアップデート方法

##### 1-1. MTA サービスの停止

GUI にて SBG へログイン後に設定(v7 では管理) -> ホスト -> LocalHost を開きます。

「着信メッセージを受け入れない」を選択し、保存をクリックします。

##### 1-2. Mail Queue のフラッシュ

CLI にて下記コマンドを入力し Mail Queue のフラッシュを実施します。

```
>mta-control all flush
```

Mail Queue の確認は下記コマンドにて確認ができます。

```
>mta-stats
```

delivery\_queued\_msgs: inbound\_queued\_msgs: outbound\_queued\_msgs: の数字が Queue の数になります。

##### 1-3. Control Center サービスの停止

CLI にて下記コマンドを入力し Control Center サービスを停止させます。

本操作実施後は GUI にてログインができなくなります。

> service controlcenter stop

#### 1-4. アップグレードの実施

CLI の「install」コマンドにてアップグレードを行います。

> install 8.0.3-11

ネットワーク環境によりダウンロード完了までに数時間かかりますが途中で止めないようにご注意ください。

ダウンロード中に下記のエラーが表示された場合は再度 install コマンドにてアップグレードを実施してください。

```
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
```

```
Fetches 152MB in 59m50s (42.3kB/s)
```

```
Err No such file or directory
```

OS のダウンロード完了後に自動で機器の再起動が実施されます。

再起動後に全てのサービスが起動するまでに数時間かかる事がありますが、起動途中で電源を OFF にしないようにご注意ください。

#### 1-5. MTA サービスの起動

GUI にて SBG へログイン後に設定 (v7 では管理) -> ホスト -> LocalHost を開きます。

「通常どおりにメッセージを受け入れて配信する」を選択し、保存をクリックします。

➤ V4からのアップデート方法  
別紙、アップグレード手順及びメーカーのナレッジベースを参照ください。

[http://www.nissho-ele.co.jp/product/symantec/key/news/manual\\_SMS8200ver5up.pdf](http://www.nissho-ele.co.jp/product/symantec/key/news/manual_SMS8200ver5up.pdf)

### ダウングレードについて

CD リストア以外にございません。

<参考:メーカーナレッジベース>

<http://service1.symantec.com/SUPPORT/ent-gate.nsf/docid/2005040414130363>

### 改訂履歴

2009/11/11      初版

以上