Technical Information	
文書番号	SYMC-SMS-070719-2
タイトル	Symantec Mail Security Version 5.0.0-40 リリースノート
対象機器	Symantec Mail Security 8200/8300 Series
ソフトウェアバージョン	5.0.0-40
プラットフォーム	-
日付	2007/7/19
参照	-
問合せ先	日商エレクトロニクス株式会社 エンタープライズ事業本部 技術統括部 セキュリティサポートグループ E-mail: symc-support@nissho-ele.co.jp

■ 本書について

Symantec Mail Security 8200/8300 Series（以下 SMS） Version 5.0.0-40 に関する情報が含まれています。

■ 本リリースについて

SMS Version 5.0.0-40 は、Version 5.0.0-36 のパッチアップデートです。

■ リソース

詳細な情報は以下より入手可能です。

<メーカ マニュアル（日本語）>
http://www.symantec.com/region/jp/techsupp/enterprise/sms/8300/manuals.html

<メーカ リリースノート（日本語）>
ftp://ftp.symantec.com/public/japanese/products/symantec_mail_security/8300/manuals/sms_release_notes.pdf

<メーカ SMS 8200 Series ナレッジベース（英語）>
http://www.symantec.com/enterprise/support/knowledge_base.jsp?pid=51975

<メーカ SMS 8300 Series ナレッジベース（英語）>
http://www.symantec.com/enterprise/support/knowledge_base.jsp?pid=53991

■ 新機能

Version 5 の主な新機能 (Version 4.x と比較) は以下となります。

・ コンテンツコンプライアンス機能の強化
  - 添付ドキュメント内のキーワードスキャン
  - 偽装された添付ファイルの検知 (True File Type)
  - ユーザベースでコントロール可能なコンプライアンスフォルダの追加

・ レピュテーション分析機能の強化
  - ローカルでのレピュテーション学習による SMTP 接続制御の精度向上

・ 管理機能の強化
  - メールステータス (時間、送受信、等) を収集するメールトラッキング機能
  - UPS の監視及び停電時のシャットダウン等

・ アンチウイルス機能の強化
  - Symantec Security Response が提供する疑わしいメール添付ファイルの定義に基づき該当するメールを隔離 (Day Zero ウイルスプロテクション)

・ PCC(Premium Content Control)モジュールの提供 (※オプションベースのアドオン機能)
  - 予め設定されたポリシーテンプレートセットを提供

・ 管理者画面の完全日本語化

■ 追加/修正内容

● Version 5.0.0-40 の追加及び修正内容は以下となります。

・ フィルタハブの安定性の問題を解決しました。

・ 検疫に格納されたメールの From ヘッダが不正な場合に通知ダイジェストが送信されない問題が修正されました。

・ mallog --restore コマンドにてメッセージ追跡ログがリストア出来ない問題が修正されました。

・ 最大メッセージサイズを 69,905,067 以上の奇数に設定した場合に MTA キューの warning が出力される問題が修正されました。

・ 設定している最大メッセージサイズに達したメールは Maillog の warning に記録されるようになりました。

● Version 5.0.0-36 の追加及び修正内容は以下となります。

・ フィルタハブの安定性の問題を向上しました。

・ 検疫宛メールのルーティング問題を修正しました。

<詳細>
Version 5.0.0-XX でインバウンドとアウトバウンドのメールフィルタを使用している場合、検疫宛メールの送信元 IP アドレスがアウトバウンド MTA となる問題を修正しました。
（送信元 IP アドレスはインバウンド MTA となります。）

・ 特定の宛先を指定したインバウンドメールのルーティング問題を修正しました。

<詳細>
Version 5.0.0-XX でインバウンドとアウトバウンドのメールフィルタを使用、且つ、ローカルドメインで特定の宛先を指定している場合、特定の宛先を指定したインバウンドメールの送信元 IP アドレスがアウトバウンド MTA となる問題を修正しました。
（送信元 IP アドレスはインバウンド MTA となります。）

※ 更新の適用のみでは反映されません。反映するには、以下の何れかを実行します。

- ローカルドメインの何れかのドメインを再保存します。ローカルドメインを編集する必要はありません。また、何れかのドメインを再保存すれば、すべてのローカルドメインに適用されます。
- ［設定］-[ホスト]のスキャナを一度無効にして、再度有効にします。

・ レピュテーション判断処理に起因する不正確なレポートを修正しました。

・ 幾つかのメールエージェントで発生する、注釈を付加したメールに起因した表示の問題を修正しました。

・ Version 5.0.0-XX から Version 5.0.0-33 へ更新後に送信者グループが動作しない問題を修正しました。

・ 最大メッセージサイズに大きな値を設定した時に MTA キューの warning が出力される問題を修正しました。

※ 最大メッセージサイズに 69,905,067 以上の奇数は設定しないでください。偶数であれば問題はありません。

・ 無効なハードウェアの warning が出力される問題を修正しました。

・ コマンドラインインターフェースの clear コマンドに、壊れたレピュテーションデータベースの削除と再生を許容するオプションを追加しました。

● Version 5.0.0-33 の追加及び修正内容は以下となります。

・ フィルタハブの安定性の問題を解決しました。

・ ルールセットのロードと実行のパフォーマンスを改良しました。

・ 幾つかの LDAP エントリにおけるスペースの形式に関連する問題を緩和する新しいコマンドラインユーティリティを追加しました。

● Version 5.0.0-30 の追加及び修正内容は以下となります。

・ 夏時間に変更するための JRE を更新しました。

・ 証明書要求の生成に関する問題が解決されました。

・ 検疫データベース情報の削除に関する問題が解決されました。

● Version 5.0.0-24 の追加及び修正内容 (Version 5.0.0-16 と比較) は以下となります。

・ プロキシ経由でソフトウェアの更新ができない問題を修正しました。

・ filter-hub の安定性を改良しました。

・ プレーンテキストメッセージ処理を改良しました。

・ diagnostics にスキャナログ (及び core) が含まれない問題を修正しました。

・ /tmp 及び/var/tmp ファイル削除用のコマンドラインユーティリティを追加しました。

● Version 5.0.0-16 の追加及び修正内容（Version 4.x と比較）は以下となります。

・ ウイルスフィルタのアップデートが Conduit(※1)から Liveupdate(※2)へ変更しました。(スパムフィルタのアップデートは Conduit(※1)で変更ありません。)
(※1) https を利用します。
(※2) http/ftp を利用します。

・ [Policies] – [Group Policies]/[Policies] – [Virus]
- ウイルスフィルタポリシーの区分が細分化しました。

・ [Policies] – [Attacks]
- Spam Attack が無くなり、スパムスロットルへ変更しました。

・ [Policies] – [Archive]
- [設定] – [アーカイブ]へ移動しました。

・ [Settings] – [Alert Settings]
- Alert Conditions が増えました。

・ [Settings] – [Replication]
- [設定] – [コントロールセンター]と統合しました。

・ [Settings] – [Log Settings]
- Log Level にコンポーネント(JLU コントローラ)が増えました。

・ [Settings] – [Report Settings]
- Delete report data older than: の week/months が無くなり、分/時間へ変更しました。
- Week/months で利用の場合、アップデート後は『分』となります。

・ [Settings] – [Quarantine Settings]
- Quarantine Thresholds が Quarantine Expunger の設定に基づいて動作するように変更しました。

- [Settings] – [Virus Settings]
  - 一部の設定が[設定] – [スキャン] へ移動しました。
  - アップデート後は Maximum file size to scan の設定を引き継ぎません。

- [Settings] – [Local Domains]
  - Inbound and Outbound mail filtering を利用、且つ Local Domains で Optional Destination Host を設定の場合、該当ドメイン宛のメールは Outbound IP アドレスを使用するように変更されました。

- [Administration] – [Utilities]
  - [状態] – [ネットワーク]へ移動しました。

■ **アップグレード**

ソフトウェアの更新にて適用可能です。

<アップグレードの注意事項>

- 更新前にバックアップを作成してください。
- 更新前に検疫内のメールをすべて削除することを推奨します。バックアップの作成時間、アップグレード後の DB マイグレーション時間を短縮できます。
- 更新前にインバウンド及びアウトバウンドの MTA を停止、各キューを解除することを推奨します。
- 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。

<参考：Version 4.X から Version 5.X へのアップグレードに関する注意事項>
http://entkb.symantec.com/security/output/n2006110911420963.html
http://www.nissho-ele.co.jp/product/symantec/news/manual_SMS8200ver5up.pdf

■ **ダウングレード**

CD リストアにて可能です。

<参考：メーカ ナレッジベース>
http://service1.symantec.com/support/inter/brightmail-jp.nsf/jp_docid/20051201092024987?OpenDocument&dtype=corp

■ 既知の問題/注意事項

主な問題及び注意事項は以下となります。以下に記載の内容以外に関しましては、メーカのリリースノート及びナレッジベースを確認してください。

・ Version 5.0.0-XX から Version 5.0.0-33 へアップデート後、送信者グループが動作しません。有効にするには、以下の何れかを実行します。

- 何れかの送信者グループの何れかのメンバーを再保存します。メンバーを編集する必要はありません。また、何れかのメンバーを再保存すれば、すべての送信者グループが動作します。
- [設定]-[ホスト]のスキャナを一度無効にして、再度有効にします。

※ Version 4.1.3-7 から Version 5.0.0-33 へのアップデート時は発生しません。
※ 本問題は Version 5.0.0-36 で改修されております。

・ コンフィグの復元はコマンドラインから実行して下さい。
管理画面から復元を実行すると、『HTTP Status 503 - Servlet jsp is currently unavailable』と表示されます。内部では復元が動作しますが、復元完了を確認することが出来ません。

※ 管理画面から実行した場合には、ブラウザを更新してはいけません。更新したタイミングより復元処理が再開されます。

・ 警告通知で以下の警告条件が誤検知します。以下の警告条件を無効にすることを推奨します。

- 『新しいウイルスフィルタが利用可能』
- 『不適切な終了後のサービス開始』

<参考:メーカ ナレッジベース>
http://entsupport.symantec.com/docs/n2006110708135663
http://entsupport.symantec.com/docs/n2007012120331363

・ 証明書群及び中間証明書のインストールをサポートしません。

・ 添付ドキュメント内のキーワードスキャンでフィルタハブが crash する可能性があります。[設定]-[スキャン]のコンテンツ制御設定を無効にすることを推奨します。

<参考:メーカ ナレッジベース>
http://entsupport.symantec.com/docs/n2006111014125463

・ フィルタエンジン（フィルタハブ）とコンジットを同時に起動した場合に以下のエラーが出力されます。問題はありませんので、無視してください。

- 『The engine was unable to be kicked.』
- 『kicker: can not open filter-hub pid file /data/scanner/jobs/filter-hub/filter-hub.pid: No such file or directory.』

・ アンチウイルスライセンスが無い場合に以下のエラーが出力されます。問題はありませんので、無視してください。

- 『Cannot perform JLU update: license check failed.』
- 『License check for service (antivirus_content) failed.』

<参考:メーカ ナレッジベース>
http://entsupport.symantec.com/docs/n2006111407551763

・ 132 日以上の連続稼動にて下記のアラートメールが送信されます。
  - この問題発生時には下記のアラートメールが送信されますが無視してください。
    - 件名: Cron <root@hostname> /opt/Symantec/Brightmail/cli/sbin/watchdog
    - 本文: Please give a smaller interval value
  - この問題発生時は CPU 使用率を誤検知します。
  - 対処方法はハードウェアのリブートになります。

・ ポリシー ＞ 送信者グループの「オープンプロキシの送信者」、「スパマーの疑い」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⇒SMS の経路で SMS へメールを送信した場合
    - MTA2 の IP アドレスが「オープンプロキシの送信者」、「スパマーの疑い」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「オープンプロキシの送信者」、「スパマーの疑い」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.

■ 改訂履歴

2007/7/19 初版
2007/10/22 第二版
2010/01/28 第三版

以上