NVC

Cisco Ironport ESA AsyncOS 7.0.1
リリースノート要約

株式会社ネットワークバリューコンポネンツ
エンジニアリング部　第二グループ

目次

1. はじめに

当リリースノートの要約は弊社において Ciscoo 社発行のリリースノート(ESA_7.0.1_GA_Release_Notes)を
独自に要約した書となります

2. AsyncOS 7.0 新機能の紹介

・RSA Email Data Loss Prevention

AsyncOS7.0 では、RSA Security 社から提供される DLP スキャンエンジンおよび DLP ポリシーのテンプレートが実装されました。RSA Email DLP を有効にすることで、機密情報の保護、法令遵守の強化、ユーザの過失による機密情報の送信を防ぐための内部ポリシーの策定が可能となります。管理者は利用者に対して、どのようなデータの送信を許可するか設定することが可能です。

RSA Email DLP は定義済みの DLP ポリシーテンプレートと RSA Security 社によって設計されたコンテンツマッチングルールが含まれています。また、DLP インシデント用の新しいレポートが含まれています。

RSA Email DLP は以下のモデルを除く全ての C シリーズと X シリーズでご利用可能です。
対象外モデル：C10, C30, C60, C100, C300D, C350D, C360D

・Unwanted Marketing Message Detection

AsyncOS7.0 では、スパムメールと合法的な送信元からのマーケティングメールを区別することが可能です。マーケティングメールがスパムメールであると見なされないとしても、これらを必要としないユーザのためにスパムメールと同様のアクションを提供することが可能です。

・Prioritized SMTP Routes

AsyncOS7.0 では、SMTP ルートによる送信先の優先付けが可能です。設定した優先順位に従ってメールの送信先を選択して送信を試みます。複数の送信先の優先順位が同じ場合は、ラウンドロビンでの配送となります。

・Encryption Enhancements

AsyncOS7.0 のメール暗号化機能では、以下のような新機能が提供されます。

- Guaranteed Secure Delivery

  コンテツフィルタおよび DLP ポリシーによって、送信先コントロールでの TLS 接続設定に従って、メールを暗号化する前に TLS 接続でのメール配送を試みることが可能です。

- Encrypt on Delivery
  コンテンツフィルタの条件にメール配送時に暗号化するオプションが追加されました。これにより、該当するメールを暗号化する前にスキャンすることが可能です。

- Encrypt on Quarantine Exit
  スパム隔離管理画面上に、メールをリリースした際にそれが暗号化されるか否かが表示されます。

- Encryption Multi-Envelope Branding
  複数の暗号化プロファイルを設定することが可能です。複数のブランドで運用している場合に、それぞれに応じたロゴを PXE エンベロープ上に表示させることが可能です。

- PXE Engine Updates
  GUI のセキュリティサービス > サービスのアップデート から PXE エンジンの自動アップデートを設定することが可能です。

・RADIUS Groups and Protocols for External Authentication
AsyncOS7.0 では、RADIUS ディレクトリ上のグループにユーザロールを割り当てることが可能です。また、PAP または CHAP での RADIUS 認証が可能です。

・Quarantined Message Attachments Enhancements
AsyncOS7.0 のスパム隔離では、以下のような新機能が提供されます。

- スパム隔離中のメールの管理画面の添付ファイル名のリンクから、添付ファイルをダウンロードすることが可能です。なお、添付されているウィルスをダウンロードしようとした場合は、警告されます。

- スパム隔離中のメールの管理画面の[message body]リンクから、メッセージボディ部分をダウンロードすることが可能です。

- スパム隔離中のメールの管理画面上に、不適切な添付画像に対する画像解析機能による解析結果のスコアが表示されます。

3. 修正された不具合

・Reporting Engine Stops Allocating Memory, Stops Processing Data, and Causes an Application Fault When the Housekeeper Thread Stops (*)
Housekeeper スレッドが停止した時に、レポーティングエンジンのメモリ領域の割り当ておよびデータの処理が停止し、アプリケーションフォルトが発生する場合があった問題が改修されました。

・Italian Translation Errors
イタリア語の誤訳が修正されました。

・TLS/SSL Man-in-the-Middle Vulnerability
TLS プロトコルの実装に、セッションの再ネゴシエーション時の処理にマン・イン・ザ・ミドル攻撃を受ける恐れがある脆弱性が見つかり、この問題に対する改修が行われました。

・DKIM Does Not Use Sender: Header to Check Against Domain Profile
DKIM 認証を用いる事で、メール送信時に From:ヘッダが DKIM 署名用のドメインプロファイルが存在するか確認を行いますが、これまで DKIM 署名ではなく、DomainKeys プロファイルのみが用いられていた問題が改修されました。

・$filenames and $filetypes Variables Return Confusing Information
$filenames と $filetypes の変数について、.tar.gz, .zoo, .ear などの圧縮ファイル形式について、矛盾した紛らわしい値を返していた問題が改修されました。
現在、これらの値には MIME 準拠の圧縮形式の情報が格納されます。

・Exported IP Address Search Results for Incoming Mail Shows “Last Sender Group” Twice
Incoming Mail のレポートページから IP アドレスの検索結果を CSV 出力した際に、“Last Sender Group”の項目が二重に出力される問題が改修されました。

・IronPort Spam Quarantine Authentication Fails for Queries Configured to Use LDAP Referrals in Active Directory
Active Directory サーバに対して LDAP 参照を行う場合に、スパム隔離ユーザ認証のクエリが失敗する問題が改修されました。

・The IronPort Spam Quarantine GUI Does Not Highlight Matched Content Containing Spaces
スパム隔離の GUI 上で、SSN(Social Security Number)のフィルタにマッチした 9 桁の文字列にスペースが含まれているメッセージがハイライトされない問題が改修されました。

・Message Filters Cannot Reference Interface Groups for Clustered Appliances
クラスタ構成時に、メッセージフィルタで IP インターフェイスグループを正しく参照できず、誤ったグループを自動的に参照していた問題が改修されました。

・Service Updates Page Displays Local Server URL After Changing to IronPort Update Servers
アップデート設定の参照先サーバをローカルサーバから IronPort アップデートサーバに変更した際に、ローカルサーバの設定が表示され続ける問題が改修されました。

・Revert Does Not Reset Configuration Settings to the Default Values
以前のバージョンの AsyncOS に戻した際に、ユーザ定義済みの設定が初期化されない問題が改修されました。

・TLS Connections Graph Does Not Include Unencrypted Connections to “TLS Preferred” Domains
TLS 接続を推奨と設定している際に、受信者ドメイン宛の復号された接続が「送信 TLS 接続数」および「送信 TLS 接続数サマリ」のレポートに集計されていなかった問題が改修されました。

4. アップグレード時の注意点及びアップグレードパス

〈アップグレード時の注意点〉

Security Management Appliances Discard Reporting Data for DLP and Marketing Mail

AsyncOS6.7.3 または、それよりも古いバージョンで使用されているセキュリティは AsyncOS7.0 または､それよりも新しいバージョンでは DLP やマーケティングメール機能のレポートデータはサポートできません。DLP やマーケティングメール機能を中心に使用するなら、AsyncOS6.7.6 または、それよりも新しいバージョンにアップグレードして下さい。

Maximum Scanning Size Increases

AsyncOS7.0 は最大で 25 MB の添付ファイルメッセージのためにスキャンサイズを増加させることができます。

Space Available for System Quarantines Increases

AsyncOS7.0 はシステム検疫のために利用できるストレージ量を増加させることができます。

(下のデータは検疫に利用できる容量を表示したものです)

IronPort Appliance	AsyncOS6.5 Storage Space	AsyncOS7.0 Storage Space
X1000/1050/1060	5GB	10GB
C600/650/660	5GB	10GB
C300/350/360	2GB	4GB
C150/160	1GB	2.5GB

New Scanned File Types for Attachments

AsyncOS7.0 には次のファイルタイプが加えられました。

Attachment Group Name	Scanned File Types
Text	txt/html/xml
Media	wma/amv

Re-enable SNMP

アンプライアンスを AsyncOS7.0 にアップグレードした後に、boot を行うと SNMP は起動しません。

Email Authentication

SPF/SIDF の証明のために、spf-pass ルールをフィルター内では利用できません。そのために、下位互換性を維持するには、フィルター内の spf-pass ルールは XML コンフィギュレーション・ファイルからは許可すると共に、似ている定義は spf-status ルールに変換することができます。

Configuration Files

以前にリリースされた、コンフィギュレーション・ファイルの下位互換性は行えません。

Received Headers

[Defect IDs: 16254, 25816]

Feature Keys

[Defect ID: 29160]

<アップグレードパス>

このリリースへの適当なアップグレードパスは以下のとおりです。

Version6.5.1-005 から Version7.0.1-010

Version6.5.2-101 から Version7.0.1-010

Version6.5.3-007 から Version7.0.1-010

Version6.5.3-009 から Version7.0.1-010

Version6.5.3-013 から Version7.0.1-010

Version6.5.3-014 から Version7.0.1-010

Version6.6.0-202 から Version7.0.1-010

Version6.6.1-016 から Version7.0.1-010

Version7.0.0-702 から Version7.0.1-010

Version7.0.1-009 から Version7.0.1-010

5. パフォーマンス観点での注意事項

RSA Email DLP

RSA を可能にして受信トラフィック上でスパム対策とアンチウイルスを実行すると、アンチウイルススキャンが 10%以下となりパフォーマンスが低下します。スパムやアンチウィルスを受信時に作動させていないアンプライアンスは重要な性能の低下があるかもしれません。

DomainKeys

電子メールに署名の DomainKeys のサインを行うと、メッセージのスループットの低下を引き起こす可能性があります。 これには小さい署名用のキーを(512 バイトまたは 768 バイト)使用することで緩和することができます。

SBNP

SenderBase ネットワークへ参加するには、IronPort の情報サービスのデータを集めるのに適応性があるスキャンエンジン(CASE)を使用します。そのため、顧客の環境により性能の低下が発生するかもしれません。

Virus Outbreak Filters

ウイルスの発生フィルターは、メッセージ脅威のレベルを決めるのに、文脈の適応性があるスキャンエンジンを使用し、規則に適合する、また発生の規則の組合せに基づいてメッセージを記録します。 そのため、ある環境下では、性能の低下が発生するかもしれません。

IronPort Spam Quarantine

検疫機能が作動し、さらに負荷がかかるとスループットがピークになるため、10-20%のスループットの減少を引き起こすかもしれません。

6. その他

7. 改定履歴

2010 年 5 月 31 日　第 1 版作成