Cisco E メール セキュリティ アプライアンス向け AsyncOS 12.1 リリース ノート

発行日 : April 12, 2019
改訂日 : 2019 年 5 月 27 日

目次

- 今回のリリースでの変更点 (2 ページ)
- 動作における変更 (3 ページ)
- アップグレードの方法 (4 ページ)
- インストールおよびアップグレードに関する注意事項 (5 ページ)
- 既知および修正済みの問題 (10 ページ)
- 関連資料 (11 ページ)
- サービスとサポート (12 ページ)

Cisco Systems, Inc.
www.cisco.com

今回のリリースでの変更点

機能	説明
インテリジェント マルチスキャンの強化	インテリジェント マルチスキャン（IMS）は、パフォーマンスの高いマルチレイヤ スパム対策ソリューションです。Cisco E メール セキュリティ アプライアンスの本リリースは、最新の IMS エンジンを提供します。このエンジンは、スパム対策エンジンの様々に組み合わせることによってスパム検出率を向上します。 最新の IMS エンジンを使用するには、IMS 機能キーを追加し、アプライアンスでライセンスを承認する必要があります。既存の IMS ユーザの場合は、IMS のすべてのメール ポリシーが移行され、最新の IMS エンジンでシームレスに機能します。
カスタム DLP ポリシーに向けたエンティティ ベースのカスタム分類子ルールの最小スコア	カスタム DLP ポリシーに向けてカスタム分類子を作成する際に、推奨される最小スコアを使用するか、エンティティ ベースのルールの最小スコアを上書きすることを選択できるようになりました。 設定されたルールの重みに代わって、エンティティ ベースのルールの最小スコアを使用できます。最小スコアは部分的一致と完全一致を区別し、それに従ってスコアを計算します。これにより、誤検出と検出漏れの数を削減できます。 以下の方法で最小スコアを設定します。 1. [Mail Policies] > [DLP Policy Customizations] > [Custom Classifiers Settings] セクションで、[Use recommended minimum scores for entity-based rules] チェックボックスを選択します。 2. [Mail Policies] > [DLP Policy Customizations] > [Add Custom Classifier] に移動し（または既存のカスタム分類子を確認し）、最小スコアを入力します。 詳細については、ユーザ ガイドの「Data Loss Prevention」の章を参照してください。

動作における変更

SSL 設定の変更	このリリースにアップグレードすると、TLS v1.0 方式と v1.2 方式を同時に有効にはできません。ただし、SSL 設定を行うことで、これらの方式は TLS v1.1 方式と共に有効にできます。
Attachment File Info コンテンツ フィルタまたはメッセージ フィルタの変更	次のいずれかの条件に基づいて、アプライアンスで 'Attachment File Info' コンテンツ フィルタまたはメッセージ フィルタを設定します。 • [Filename] オプションを選択して、[Does Not Equal]、[Does Not Contain]、[Does Not End With]、または [Does Not Begin] オプションを選択し、ファイル名を入力する。 • [File type] オプションを選択して、[Is not] オプションを選択し、ドロップダウン リストからファイル タイプを選択する。 • [MIME type] オプションを選択して、[Is Not] オプションを選択し、MIME タイプを入力する。 アプライアンスは、上記のいずれかの条件に基づいて、添付ファイルがあるかどうかにかかわらず、メッセージに対して設定されたアクションを実行するようになりました。
データ損失防止（DLP）でサポートされる文字エンコーディングの変更	データ損失防止では、中国語、日本語、韓国語のマルチバイト プレーン テキストファイルに対して、次の文字エンコーディングがサポートされるようになりました。 • 中国語（繁体字）（Big5） • 中国語（簡体字）（GB2312） • 韓国語（KS-C-5601/EUC-KR） • 日本語（Shift-JIS（X0123）） • 日本語（EUC） ただし、データ損失防止（DLP）は、次の文字エンコーディングをサポートしません。 • 日本語（ISO-2022-JP） • 韓国語（ISO2022-KR） • 中国語（簡体字）（HZGB2312）
メール ポリシー設定の変更	このリリースへのアップグレード後、アプライアンスが着信メッセージと発信メッセージのメッセージ ヘッダーをチェックする際の優先順位を設定できます。最初に、アプライアンスはすべてのメール ポリシーで優先順位の最も高いメッセージ ヘッダーをチェックします。いずれのメール ポリシーとも一致するヘッダーがない場合、アプライアンスはすべてのメール ポリシーの優先順位リスト内の次のメッセージ ヘッダーを検索します。いずれのメール ポリシーとも一致するメッセージ ヘッダーがない場合は、デフォルトのメール ポリシー設定が使用されます。

アップグレードの方法

- リリース 12.1.0-087 へのアップグレード - GD（一般導入）更新（4 ページ）
- リリース 12.1.0-071 へのアップグレード - GD（一般導入）（4 ページ）

リリース 12.1.0-087 へのアップグレード - GD（一般導入）更新

次のバージョンから、リリース 12.1.0-087 にアップグレードすることができます。

- 9.7.2-145
- 11.0.0-274
- 11.0.1-027
- 11.0.2-037
- 11.0.2-044
- 11.0.3-238
- 11.0.3-242
- 11.1.0-128
- 11.1.0-131
- 11.1.0-135
- 11.1.0-603
- 11.1.1-042
- 11.1.2-023
- 11.1.2-509
- 11.1.2-701
- 11.1.2-802
- 11.1.3-006
- 12.0.0-281
- 12.0.0-419
- 12.1.0-071
- 12.1.0-085

リリース 12.1.0-071 へのアップグレード - GD（一般導入）

次のバージョンから、リリース 12.1.0-071 にアップグレードすることができます。

- 11.0.0-274
- 11.0.1-027
- 11.0.2-037
- 11.0.2-044
- 11.0.3-238

- 11.1.0-128
- 11.1.0-131
- 11.1.0-135
- 11.1.0-603
- 11.1.1-042
- 11.1.2-023
- 11.1.2-509
- 11.1.2-701
- 11.1.2-802
- 12.0.0-281
- 12.0.0-419
- 12.1.0-043
- 12.1.0-070

インストールおよびアップグレードに関する注意事項

このセクションに記載されているインストールとアップグレードの影響を把握および検討してください。

Web インターフェイスまたは CLI（コマンド ライン インターフェイス）から AsyncOS をアップグレードすると、設定は /configuration/upgrade ディレクトリ内のファイルに保存されます。FTP クライアントを使用して、アップグレード ディレクトリにアクセスできます。各設定ファイル名にはバージョン番号が付加され、設定ファイル内のパスワードは人間が判読できないようにマスクされます。

管理者権限を持つユーザとしてログインして、アップグレードする必要があります。また、アップグレード後にアプライアンスを再起動する必要があります。

このリリースでサポートされているハードウェア

- すべての仮想アプライアンス モデル
- 次のハードウェア モデル - C380、C680、C190、C390、または C690

  アプライアンスがサポートされているかどうかを確認し、現在互換性がない場合にその状況を解決するには、http://www.cisco.com/c/en/us/support/docs/field-notices/638/fn63931.html を参照してください。

このリリースでは、次のハードウェアはサポートされていません。

- C160、C360、C660、および X1060
- C170、C370、C370D、C670、および X1070 アプライアンス

仮想アプライアンスの展開またはアップグレード

仮想アプライアンスを展開またはアップグレードする場合は、『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください。このドキュメントは http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html から入手できます。

仮想アプライアンスのアップグレード

現在の仮想アプライアンスのリリースが 2 TB 以上のディスク領域をサポートしておらず、このリリースで 2 TB 以上のディスク領域を使用する場合は、仮想アプライアンスを単にアップグレードすることはできません。

代わりに、このリリース用に新しい仮想マシン インスタンスを導入する必要があります。

仮想アプライアンスをアップグレードすると、既存のライセンスは変更されません。

ハードウェア アプライアンスから仮想アプライアンスへの移行

ステップ 1 仮想アプライアンスの展開またはアップグレード (6 ページ) で説明されているマニュアルを使用して、この AsyncOS リリースで仮想アプライアンスをセットアップします。

ステップ 2 ハードウェア アプライアンスをこの AsyncOS リリースにアップグレードします。

ステップ 3 アップグレードされたハードウェア アプライアンスから設定ファイルを保存します。

ステップ 4 ハードウェア アプライアンスから仮想アプライアンスに設定ファイルをロードします。

ネットワーク設定に関連する適切なオプションを選択してください。

仮想アプライアンスのテクニカル サポートの取得

仮想アプライアンスのテクニカル サポートを受けるための要件は、http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html にある『*Cisco Content Security Virtual Appliance Installation Guide*』に記載されています。

以下のサービスとサポート (12 ページ) も参照してください。

仮想アプライアンスからの Cisco Registered Envelope Service 管理者のプロビジョニングとアクティブ化

仮想アプライアンスのプロビジョニングに必要な情報については、Cisco TAC にお問い合わせください。

アップグレード前の注意事項

アップグレードする前に、次の事項を確認してください。

- FIPS の準拠性 (7 ページ)
- 集中管理 (クラスタ化されたアプライアンス) を使用した展開のアップグレード (7 ページ)

- 直前のリリース以外のリリースからのアップグレード (7 ページ)
- コンフィギュレーション ファイル(7 ページ)
- アップグレード中の IPMI メッセージ(7 ページ)

FIPS の準拠性

AsyncOS 12.1 リリースは、FIPS 準拠のリリースではありません。アプライアンスで FIPS モードを有効にしている場合は AsyncOS 12.1 にアップグレードする前に FIPS モードを無効にする必要があります。

集中管理(クラスタ化されたアプライアンス)を使用した展開のアップグレード

クラスタに C160、C360、C660、X1060、C170、C370、C670、または X1070 ハードウェア アプライアンスが含まれている場合は、アップグレードの前に、これらのアプライアンスをクラスタから削除してください。

クラスタ内のすべてのマシンが同じバージョンの AsyncOS を実行している必要があり、x60 および x70 ハードウェアをこのリリースにアップグレードすることはできません。必要に応じて、x60 および x70 アプライアンス用に別のクラスタを作成してください。

直前のリリース以外のリリースからのアップグレード

このリリースの直前のリリース以外のメジャー(AsyncOS X.0)またはマイナー(AsyncOS X.x)リリースからアップグレードする場合は、現在のリリースとこのリリースの間にあるメジャー リリースとマイナー リリースのリリース ノートを確認する必要があります。

メンテナンス リリース(AsyncOS X.x.x)には、バグ修正のみが含まれています。

コンフィギュレーション ファイル

通常、シスコは、以前のメジャー リリースに関して、設定ファイルの下位互換性をサポートしていません。マイナー リリースのサポートが提供されています。以前のバージョンの設定ファイルは以降のリリースで動作する可能性がありますが、ロードするために変更が必要になる場合があります。設定ファイルのサポートについて不明な点がある場合は、シスコ カスタマー サポートでご確認ください。

アップグレード中の IPMI メッセージ

CLI を使用してアプライアンスをアップグレードする場合、IPMI に関連するメッセージが表示されることがあります。これらのメッセージは無視しても差し支えありません。これは既知の問題です。

障害 ID:CSCuz28415

このリリースへのアップグレード

はじめる前に

- ワーク キュー内のすべてのメッセージをクリアします。ワーク キューをクリアせずにアップグレードを実行することはできません。
- 既知および修正済みの問題（10 ページ）とインストールおよびアップグレードに関する注意事項（5 ページ）を確認してください。
- 仮想アプライアンスをアップグレードする場合は、仮想アプライアンスのアップグレード（6 ページ）を参照してください。

手順

E メール セキュリティ アプライアンスをアップグレードするには、次の手順を実行します。

ステップ 1 アプライアンスから、XML コンフィギュレーション ファイルを保存します。

ステップ 2 セーフリスト/ブロックリスト機能を使用している場合は、アプライアンスからセーフリスト/ブロックリスト データベースをエクスポートします。

ステップ 3 すべてのリスナーを一時停止します。

ステップ 4 ワーク キューが空になるまで待ちます。

ステップ 5 [System Administration] タブで、[System Upgrade] ページを選択します。

ステップ 6 [Available Upgrades] ボタンをクリックします。ページが更新され、使用可能な AsyncOS アップグレード バージョンのリストが表示されます。

ステップ 7 [Begin Upgrade] ボタンをクリックすると、アップグレードが開始されます。表示される質問に答えます。

ステップ 8 アップグレードが完了したら、[Reboot Now] ボタンをクリックしてアプライアンスを再起動します。

ステップ 9 すべてのリスナーを再開します。

次の作業

- アップグレード後、SSL の設定を確認し、使用する正しい GUI HTTPS、インバウンド SMTP、およびアウトバウンド SMTP 方式が選択されていることを確認します。[System Administration] > [SSL Configuration] ページを使用するか、CLI で `sslconfig` コマンドを使用します。手順については、ユーザ ガイドまたはオンライン ヘルプの「System Administration」の章を参照してください。
- パフォーマンス アドバイザリ（9 ページ）を確認してください。

アップグレード後の注意事項

- インテリジェント マルチスキャンおよびグレイメール グローバル設定の変更（9 ページ）
- AsyncOS 12.x へのアップグレード後のクラスタ レベルでの DLP 設定の不整合（9 ページ）

インテリジェント マルチスキャンおよびグレイメール グローバル設定の変更

AsyncOS 12.1 にアップグレードした後のインテリジェント マルチスキャン（IMS）およびグレイメールのグローバル設定の変更点は次のとおりです。

- IMS およびグレイメールのグローバル設定が異なるクラスタ レベルで設定されている場合、アプライアンスはグローバル設定を最も低い設定レベルにコピーします。たとえば、クラスタ レベルで IMS を設定し、マシン レベルでグレイメールを設定すると、アプライアンスは IMS グローバル設定をマシン レベルにコピーします。
- スキャン メッセージの最大メッセージ サイズとタイムアウト値が異なる場合、アプライアンスは [maximum timeout] および [maximum message size] の値を使用して、IMS およびグレイメールのグローバル設定を行います。たとえば、IMS およびグレイメールの最大メッセージサイズの値がそれぞれ 1M と 2M である場合、アプライアンスは IMS とグレイメールの両方の最大メッセージ サイズ値として 2M を使用します。

AsyncOS 12.x へのアップグレード後のクラスタ レベルでの DLP 設定の不整合

AsyncOS 12.x にアップグレードした後、アプライアンスがクラスタ モードになっていて、DLP が設定されている場合、CLI を使用して `clustercheck` コマンドを実行すると、DLP 設定の不整合が表示されます。

この不整合を解決するには、クラスタ全体でクラスタ内の他のいずれかのマシンの DLP 設定を使用するように強制します。次の例に示すように、`clustercheck` コマンドで「`How do you want to resolve this inconsistency?`」というプロンプトを使用します。

```
(Cluster)> clustercheck
Checking DLP settings...
Inconsistency found!
DLP settings at Cluster test:
mail1.example.com was updated Wed Jan 04 05:52:57 2017 GMT by 'admin' on mail2.example.com
mail2.example.com was updated Wed Jan 04 05:52:57 2017 GMT by 'admin' on mail2.example.com
How do you want to resolve this inconsistency?
1. Force the entire cluster to use the mail1.example.com version.
2. Force the entire cluster to use the mail2.example.com version.
3. Ignore.
[3]>
```

パフォーマンス アドバイザリ

DLP

- 着信メッセージに対してスパム対策およびウイルス対策スキャンがすでに実行されているアプライアンスで発信メッセージの DLP を有効にすると、10 % 未満のパフォーマンス低下が発生する可能性があります。
- 発信メッセージだけを実行し、スパム対策およびウイルス対策が実行されていないアプライアンスで DLP を有効にすると、前のシナリオと比べてパフォーマンスがさらに低下する可能性があります。

SBNP

SenderBase Network Participation では、コンテキスト適応スキャン エンジン（CASE）を使用してデータを収集し、IronPort 情報サービスを駆動するようになりました。一部の設定では、中程度のパフォーマンス低下が発生する可能性があります。

アウトブレイク フィルタ（Outbreak Filters）

アウトブレイク フィルタは、コンテキスト適応スキャン エンジンを使用してメッセージの脅威レベルを判定し、アダプティブ ルールとアウトブレイク ルールの組み合わせに基づいてメッセージにスコアを付けます。一部の設定では、中程度のパフォーマンス低下が発生する可能性があります。

IronPort スパム隔離

C シリーズまたは X シリーズのアプライアンスに対して IronPort スパム隔離オンボックスを有効にすると、公称水準の負荷がかかっているアプライアンスでは、システム スループットにわずかな低下が生じます。ピーク スループット付近またはピーク スループットで実行されているアプライアンスの場合、アクティブな隔離からの追加の負荷によって、スループットが 10 ～ 20 % 低下する可能性があります。システムがキャパシティの上限に達しているか上限に近いときに IronPort スパム隔離を使用する場合は、規模が大きい C シリーズ アプライアンスまたは M シリーズ アプライアンスへの移行を検討してください。

スパム対策ポリシーをスパムのドロップから隔離に変更する場合（オンボックスまたはオフボックス）、ウイルスおよびコンテンツ セキュリティのために追加のスパム メッセージをスキャンする必要があるため、システムの負荷が増大します。インストールのサイジングを適切に行う際にサポートが必要な場合は、認定サポート プロバイダーにお問い合わせください。

既知および修正済みの問題

シスコのバグ検索ツールを使用して、このリリースの既知および修正済みの不具合に関する情報を検索します。

- バグ検索ツールの要件（10 ページ）
- 既知および修正済みの問題のリスト（10 ページ）
- 既知および解決済みの問題に関する情報の検索（11 ページ）

バグ検索ツールの要件

シスコ アカウントを持っていない場合は、登録します。
https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui に移動します。

既知および修正済みの問題のリスト

既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=12.1&sb=afr&sts=open&svr=3nH&bt=custV
修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=12.1.0-087&sb=fr&sts=fd&svr=3nH&bt=custV

既知および解決済みの問題に関する情報の検索

シスコのバグ検索ツールを使用して、既知および解決済みの不具合に関する最新情報を検索します。

はじめる前に

シスコ アカウントを持っていない場合は、登録します。
https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui に移動します。

手順

ステップ 1 https://tools.cisco.com/bugsearch/ に移動します。

ステップ 2 シスコ アカウントのクレデンシャルでログインします。

ステップ 3 [Select from list] > [Security] > [Email Security] > [Cisco Email Security Appliance] の順にクリックし、[OK] をクリックします。

ステップ 4 [Releases] フィールドに、リリースのバージョン（たとえば、11.1）を入力します。

ステップ 5 要件に応じて、次のいずれかを実行します。

- 解決済みの問題のリストを表示するには、[Show Bugs] ドロップダウンから、[Fixed in these Releases] を選択します。
- 既知の問題のリストを表示するには、[Show Bugs] ドロップダウンから [Affecting these Releases] を選択し、[Status] ドロップダウンから [Open] を選択します。

（注） ご不明な点がある場合は、ツールの右上にある [Help] または [Feedback] リンクをクリックしてください。また、インタラクティブなツアーもあります。これを表示するには、[search] フィールドの上のオレンジ色のバーにあるリンクをクリックします。

関連資料

マニュアルの内容（Cisco Content Security 製品）	参照先
ハードウェアおよび仮想アプライアンス	この表で該当する製品を参照してください。
Cisco コンテンツ セキュリティ管理	http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Cisco Web セキュリティ	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
Cisco E メール セキュリティ	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html
Cisco コンテンツ セキュリティ アプライアンスの CLI リファレンス ガイド	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html

マニュアルの内容 （Cisco Content Security 製品）	参照先
Cisco IronPort 暗号化	http://www.cisco.com/c/en/us/support/security/email-encryption/tsd-products-support-series-home.html

サービスとサポート

（注） 仮想アプライアンスのサポートを受けるには、仮想ライセンス番号（VLN）をご用意の上 Cisco TAC に連絡してください。

Cisco TAC：http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

従来の IronPort のサポート サイト：http://www.cisco.com/web/services/acquisitions/ironport.html

重大ではない問題の場合は、アプライアンスからカスタマー サポートにアクセスすることもできます。手順については、ユーザ ガイドまたはオンライン ヘルプを参照してください。

このマニュアルは、「関連資料」の項に記載されているマニュアルと併せてご利用ください。