Cisco Cloud/Hybrid Secure Email 用 AsyncOS 14.2 リリースノート

発行日:2022 年 6 月 8 日

改訂日:2024 年 2 月 13 日

目次

Cisco Cloud Secure Email

Cisco Cloud Secure Email には、**Cisco Secure Email Gateway 用の AsyncOS 14.2** と **Cisco Secure Email and Web Manager 用の AsyncOS 14.2** が含まれています。この項では、このリリースの新機能、既知の問題、および修正済みの問題について説明します。

最新情報

Cisco Systems, Inc.
www.cisco.com

Cisco Secure Email Gateway 用の AsyncOS 14.2 の新機能

機能	説明
URL レトロスペクティブ判定と URL 修復	レピュテーションが不明な URL は常に、ユーザのメールボックスに達した後であっても、悪意のあるファイルに変化する可能性があります。Talos から受信した URL レトロスペクティブ判定に基づいてアラートを送信するように、E メールクラウドゲートウェイで URL フィルタリングを設定できます。URL 判定が不明から悪意ありに変更されたときにユーザのメールボックス内のメッセージに対して自動修復アクションを実行するように電子メールゲートウェイを設定することもできます。 詳細については、ユーザーガイドの「Protecting Against Malicious or Undesirable URLs」の章を参照してください。
URL フィルタリング結果のモニタ	[URL レトロスペクションレポート（URL Retrospection Report）] ページには、URL レトロスペクティブサービスによって処理された URL が表示されます。また、悪意のある URL、URL レトロスペクティブサービスから判定を受け取った日時、影響を受けたメッセージの修復ステータスが一覧表示されます。 詳細については、ユーザー ガイドの「Using Email Security Monitor」の章を参照してください。

送信者の成熟度	このリリースでは、従来の送信者ドメインのレピュテーション（SDR）ドメインのエージ機能が、送信者の成熟度に置き換えられます。送信者の成熟度は、送信者のレピュテーションを確立するための重要な機能です。送信者の成熟度は、スパムを分類するために、複数の情報源に基づいて自動的に生成され、「Whois-based domain age」とは異なる場合があります。 [送信者の成熟度（Sender Maturity）] は、電子メール送信者としてのドメインの成熟度に関する Cisco Talos の見解を表します。成熟度の値は、電子メールに関する脅威の検出を有効にするように調整されており、通常は「Whois-based domain age」で表されるドメインの経過時間は反映されません。 [送信者の成熟度（Sender Maturity）] は 30 日の制限に設定されており、この制限を超えるとドメインは電子メール送信者として成熟していると見なされてそれ以上の詳細は提供されません。 **（注）** このリリース以降、[SDR ドメインのエージ（SDR Domain Age）] 設定済みフィルタは、[SDR 送信者の成熟度（SDR Sender Maturity）] フィルタに自動的に更新されます。[送信者の成熟度（Sender Maturity）] の値が無効なフィルタは、アップグレード後に「非アクティブ」としてマークされます。メッセージまたはコンテンツフィルタを確認し、適宜変更してください。 送信者の成熟度は送信者のレピュテーションの計算に使用されます。未熟なドメインには低いレピュテーションが割り当てられます。Cisco Talos では、ポリシーアクションの決定にのみ送信者のレピュテーションを使用することを推奨しています。送信者の成熟度は、特定の標準外シナリオに合わせてフィルタを微調整するために使用されます。 **（注）** Cisco Talos ではドメインの成熟度を手動で調整しませんが、最適な値を決定するために自動システムとセンサーに依存します。 詳細については、ユーザーガイドの「Sender Domain Reputation Filtering」の章を参照してください。
送信者ドメインのレピュテーション フィルタリングの改善	このリリースでは、ユーザーエクスペリエンスおよび送信者ドメインのレピュテーション（SDR）サービスの全体的な品質が、パフォーマンスの改善、可用性の向上、および SDR の展開によって強化されています。

新しい送信者ドメインのレピュテーション判定	このリリース以降、送信者ドメインのレピュテーション（SDR）の判定は、意図する意味と推奨される使用法を正確に反映するように更新されています。 アップグレード中に、システムは送信者ドメイン レピュテーション メッセージまたはコンテンツフィルタ設定を自動的に更新して、新しい判定を反映します。メッセージまたはコンテンツフィルタを確認し、適宜設定してください。 新しい SDR 判定ごとに実行できる推奨されるアクションの詳細については、ユーザーガイドの「Sender Domain Reputation Filtering」の章の「SDR Verdicts」セクションを参照してください。 AsyncOS 14.2.x リリースにアップグレードすると、コンテンツまたはメッセージフィルタ、レポート、およびメッセージトラッキングの従来の SDR 判定は、次のように新しい SDR 判定に置き換えられます。 • 信頼できない • 要検討 • ニュートラル • 好ましい • 信頼できる • 不明 **（注）** SDR レポーティングおよびトラッキング AsyncOS API は、新しい SDR 脅威レベルとカテゴリ構造を反映するように更新されています。 **（注）** SDR メールおよびトラッキングログが更新され、新しい SDR 脅威レベルと送信者の成熟度の詳細が反映されます。 **（注）** このリリース以降、メッセージの送信者ヘッダーを受信した後に、追加の送信者ドメイン レピュテーション チェックが実行されます。（電子メールゲートウェイで）構成された SDR 拒否レベルに一致する脅威レベルのメッセージは拒否されます。 詳細については、次の資料を参照してください。 • ユーザーガイドの「Sender Domain Reputation Filtering」の章。 • CLI リファレンスガイドの「The Commands: Reference Examples」の章の「Sender Domain Reputation Filtering」セクション。

接続先コントロールのための TLS 証明書の拡張	特定のドメインの「デフォルト」接続先コントロールエントリで設定された証明書以外の別の証明書を選択できるようになりました。 別の証明書は、次のいずれかの方法で選択できます。 • 対応する接続先コントロールエントリを編集し、Web インターフェイスの [TLS 証明書(TLS certificate)] オプションを使用して別の証明書を選択する。 • 接続先コントロールエントリを作成または編集するときに、CLI で `destconfig > new` または `edit` サブコマンドを使用して証明書を選択する。 詳細については、ユーザーガイドの「Configuring Routing and Delivery Features」の章にある「Controlling TLS」セクションを参照してください。
クラシックライセンスの変更:Web インターフェイスおよび CLI の期限日	このリリース以降、クラシックライセンスの Web インターフェイスおよび CLI の既存の [期限日(Expiration Date)] 列ヘッダーが [期限日(猶予期間を含む)(Expiration Date (including grace period))] に変更されます。これは、期限日に猶予期間が含まれることを示しています。 **(注)** すべてのアラートメッセージとメールログは、機能キーの猶予期間を含む期限日を表示するように変更されます。
プレフィックス付きまたはプレフィックスなしのスマート識別子の検出	電子メールゲートウェイは、メッセージコンテンツのプレフィックスとして追加されたキーワード (「credit」、「ssn」、「cusip」、または「aba」) の有無にかかわらず、スマート識別子を検出します。 プレフィックスとして追加されたキーワードの有無にかかわらず、スマート識別子を検出するように、コンテンツフィルタ条件またはメッセージフィルタルールを次の方法で設定できます。 • メッセージ本文、メッセージ本文または添付ファイル、および添付ファイルのコンテンツについて、コンテンツフィルタ条件で、[スマート識別子のプレフィックスを含む(Contains smart identifier prefix)] オプションを使用する。詳細については、ユーザーガイドの「Content Filter」の章の「Content Filter Condition」セクションを参照してください。 • メッセージフィルタルールで、*プレフィックス*構文を使用する。詳細については、ユーザーガイドの「Using Message Filters to Enforce Email Policies」の章の「Smart Identifier Syntax」セクションを参照してください。

Syslog プッシュ ログ サブスクリプションのキャッシング	Syslog プッシュ ログ サブスクリプションのローカルディスクバッファを設定できるようになりました。これにより、リモート Syslog サーバーが使用できないときに、電子メールゲートウェイがログイベントをキャッシュできます。Syslog サーバーが使用可能になると、電子メールゲートウェイは、そのログサブスクリプションのバッファ内のすべてのデータを Syslog サーバーに送信します。 ディスクバッファパラメータは、次の方法で設定できます。 • Web インターフェイスの [システム管理（System Administration）] > [ログサブスクリプション（Log Subscriptions）] ページ詳細については、ユーザーガイドの「Logging」の章の「Log Retrieval Methods」セクションを参照してください。 • CLI での `logconfig` コマンド。詳細については、CLI リファレンスガイドの「The Commands：Reference Example」の章の「Logging and Alerts」セクションを参照してください。 **（注）** ディスクバッファパラメータの構成は、TCP プロトコルにのみ適用されます。
電子メールゲートウェイのコンテンツディクショナリの最大数の設定	電子メールゲートウェイで最大 150 のコンテンツディクショナリを設定できるようになりました。 **（注）** デフォルトでは、電子メールゲートウェイに最大 100 のコンテンツディクショナリを設定できます。 デフォルトの制限を変更するには、CLI で `dictionaryconfig > dictionarylimits` サブコマンドを使用します。 **（注）** [メッセージ本文または添付ファイル（Message Body or Attachments）] コンテンツフィルタ条件または [本文のスキャン（Body Scanning）] または [添付ファイルのスキャン（Attachment Scanning）] メッセージフィルタルールでコンテンツディクショナリを広範囲に使用すると、システムパフォーマンスが低下する場合があります。 詳細については、このリリースに関連する CLI リファレンスガイドの「The Commands: Reference Examples」の章の「Policy Enforcement」セクションを参照してください。

Cisco Secure Email Gateway 用の AsyncOS 14.2 で変更された動作

sdrstatus および sdrupdate CLI コマンドのサポートなし	このリリース以降、sdrstatus および sdrupdate CLI コマンドはサポートされなくなりました。 次の CLI コマンドを使用して、sdrstatus および sdrupdate CLI コマンドの機能を設定できるようになりました。 • talosstatus：SDR コンポーネントの現在のバージョンを表示します。 • talosupdate：SDR コンポーネントを手動で更新します。
FQDN 検証の変更	このリリース以降、ピア証明書を検証するか、証明書をインポートするときに、インポートする証明書またはサーバー証明書で件名（共通名）フィールドが使用できない場合、FQDN 検証は SAN 拡張が重要かどうかを確認します。 （注） この動作の変更は、証明書のインポートまたはピア証明書の検証中に FQDN 検証を有効にしている場合にのみ適用されます。
アップデータサーバーの CA 証明書の変更	このリリースで加えられたアップデータサーバーの CA 証明書の動作の変更は次のとおりです。 • 電子メールゲートウェイにアップデータサーバーの CA 証明書を追加するときに、FQDN 検証が実行されます。新しいステートメント「共通名または SAN:dNSName または両方が完全修飾ドメイン名（FQDN）フォーマットであるかどうかを確認しますか？（Do you want to check if Common Name or SAN:dNSName or both are in Fully Qualified Domain Name(FQDN) format?）」が、FQDN 検証を実行するための CLI の updateconfig > trusted_certificates > add サブコマンドに追加されます。 • CA 証明書の検証は、電子メールゲートウェイにアップデータ CA 証明書を追加するときに実行されます。 （注） 電子メールゲートウェイでは、ルート CA 証明書とチェーン内の他の証明書が信頼されている場合、アップデータ CA 証明書を追加できます。
Web UI 非アクティブ時のタイムアウトの変更	このリリースで加えられた「Web UI 非アクティブ時のタイムアウト」値の動作の変更は次のとおりです。 • （新しい AsyncOS インストールのみに適用）：[Web UI 非アクティブ時のタイムアウト（Web UI Inactivity Timeout）] オプションのデフォルト値が 30 分から 5 分に変更されました。必要に応じて値を変更できます。 • （AsyncOS アップグレードのみに適用）：アップグレード時に、「Web UI 非アクティブ時のタイムアウト（Web UI Inactivity Timeout）」オプションは、アップグレード前に設定された値と同じ値を保持します。

ピア証明書の FQDN 検証の変更	このリリース以降、ピア証明書の共通名（CN）または SAN: DNS 名フィールドに解決可能なドメインがある場合、ピア証明書の FQDN 検証は成功します。
AWS S3 プッシュ構成の変更	このリリースより前は、「AWS S3 プッシュ」ログ取得方法を設定すると、統合イベントログを転送するための [システム管理（System Administration）] > [ログサブスクリプション（Log Subscription）] > [ログサブスクリプションの追加（Add Log Subscription）] ページの [S3 バケット名（S3 Bucket Name）] フィールドに AWS（S3）バケット名しか入力できませんでした。 このリリース以降、「AWS S3 プッシュ」ログ取得方法を設定した場合、統合イベントログを転送するための [システム管理（System Administration）] > [ログサブスクリプション（Log Subscription）] > [ログサブスクリプションの追加（Add Log Subscription）] ページの [S3 バケット（S3 Bucket）] フィールドに AWS（S3）バケット内のディレクトリパスと一緒に AWS（S3）バケット名を入力できるようになりました。 たとえば、[S3 バケット（S3 Bucket）] フィールドに「test1esa/dir1」と入力した場合、「test1esa」は AWS S3 バケット名で、「dir1」は「test1esa」バケット内のディレクトリパスです。
メールポリシーエントリの変更	このリリース以降、電子メールゲートウェイでは次のことができなくなります。 • CLI を介して、または電子メールゲートウェイに XML 構成ファイルを読み込むときに、メールポリシーに重複ユーザーを追加する。 • メールポリシーを編集して、重複ユーザーをメールポリシーに追加する。 **（注）** メールポリシーのユーザーは一意である必要があります。
Web UI セッションのタイムアウトの変更	このリリースより前は、[Web UI 非アクティブ時のタイムアウト（Web UI Inactivity Timeout）] オプションのデフォルト値を 12 時間を超える値に設定すると、12 時間後に電子メールゲートウェイの新しい Web インターフェイスからログアウトされませんでした。12 時間後も引き続き新しい Web インターフェイスにアクセスできました。 このリリースにアップグレードした後は、[Web UI 非アクティブ時のタイムアウト（Web UI Inactivity Timeout）] オプションのデフォルト値を 12 時間を超える値に設定すると、12 時間後に電子メールゲートウェイの新しい Web インターフェイスから自動的にログアウトされます。

Syslog ディスクバッファサイズ構成の変更	このリリースより前は、syslog プッシュ ログ サブスクリプションに許可された最大ディスクバッファサイズは 10 GB でした。 このリリースにアップグレードした後、syslog プッシュ ログ サブスクリプションに許可される最大ディスクバッファサイズは 1 GB です。 (AsyncOS アップグレードのみに適用):アップグレード前に既存の設定値が 1 GB を超えている場合、システムはアップグレード中に最大ディスクバッファサイズ値を自動的に 1 GB に減らします。 **(注)** アップグレード中に、割り当てられたその他のディスククォータが設定された制限を超えた場合は、最大ディスクバッファサイズ値(既存の設定値が 1 GB を超える場合)を減らして、割り当てられたその他のディスククォータスペースを解放して、アップグレードプロセスを続行する必要があります。
システムアップグレード中の CA 証明書の検証	このリリース以降、E メールゲートウェイをアップグレードすると、CA 証明書がアクティブ(期限切れではない)で、証明書の CA フラグが true に設定されている場合にのみ、既存の CA 証明書がアップグレードされます。E メールゲートウェイは、システムのアップグレード中に期限切れの証明書と CA フラグが false に設定された CA 証明書を拒否します。また、E メールゲートウェイに構成ファイルをロードすると、CA フラグが false に設定された CA 証明書と期限切れの証明書が削除されます。
メールログとトラッキングログの変更	このリリース以前は、メールログとトラッキングログの件名の情報は引用符で囲まれていませんでした。 このリリースへのアップグレード後、メールログとトラッキングログの件名の情報は二重引用符で囲まれるようになりました。
非 FIPS モードでの証明書検証の変更	このリリース以降、E メールゲートウェイが非 FIPS モードで、自己署名証明書または署名証明書を追加またはアップロードすると、E メールゲートウェイが必要な証明書を検証するようになりました。
スパム対策のメールポリシー構成の変更	このリリース以降、スパム対策構成が特定のレベルで定義されてから別のレベル (たとえば、クラスタからマシンレベル)に移動された場合、移動されたレベル(たとえば、マシンレベル)でのみスパム対策のメールポリシーを設定できます。

テキストリソース名の変更	このリリースより前は、空白を含むテキストリソースに名前を追加できました。 このリリースにアップグレードした後は、空白を含むテキストリソース名を入力できません。テキストリソース名は、文字または下線で始める必要があります。それに任意の数の文字、数字、下線またはハイフンが続きます。 **（注）** 空白は使用できません。 このリリースにアップグレードすると、以前のリリースバージョンのテキストリソースが同じフォーマットで新しいリリースバージョンにアップグレードされます。 **（注）** アップグレード後、空白を含むテキストリソースの名前を変更することを推奨します。
システム正常性 API の変更	このリリースより前のリリースでは（AsyncOS 13.5.x および 13.7 リリースバージョンのみに適用）、システム正常性 API のサンプル応答に、配信ステータス API とシステムステータス API の詳細が含まれていました。 このリリース以降、配信ステータス API とシステムステータス API の詳細は、システム正常性 API の応答から削除されます。これらの詳細は、配信ステータス API とシステムステータス API の対応する応答で表示できるようになりました。
ファイル分析のための HTML および Octet-stream ファイルのアップロードにおける変更	[このリリースの前]: ファイル分析用のファイル拡張子が選択されている場合、電子メールゲートウェイは、HTML および Octet-stream ファイル（MIME タイプ：application/octet-stream および text/html）のみをファイル分析サーバーにアップロードできました。 [このリリース以降]: 電子メールゲートウェイは、ファイル分析用のファイル拡張子が選択されていない場合でも、ファイル分析のために HTML および Octet-stream ファイルをファイル分析サーバーにアップロードできるようになりました。 **（注）** ファイル分析サーバーにアップロードされるファイルの数が増えると、電子メールゲートウェイがすぐにファイル分析サーバーのファイルアップロード制限に達する可能性があります。

ファイル分析のためのアーカイブファイルのアップロードにおける変更	[このリリースの前]:AMP エンジンがメッセージからアーカイブファイル(パスワードで保護されアーカイブされた添付ファイルを含む)の抽出に失敗すると、添付ファイルはファイル分析サーバーにアップロードされませんでした。 [このリリース以降]:AMP エンジンがメッセージからアーカイブファイル(パスワードで保護されアーカイブされた添付ファイルを含む)の抽出に失敗した場合に、添付ファイルはファイル分析のためにファイル分析サーバーにアップロードされるようになりました。 (注) ファイル分析サーバーにアップロードされるファイルの数が増えると、電子メールゲートウェイがすぐにファイル分析サーバーのファイルアップロード制限に達する可能性があります。

Cisco Secure Email and Web Manager 用の AsyncOS 14.2 の新機能

機能	説明
PVO 検疫しきい値アラート	Cisco Secure Email and Web Manager では、PVO 検疫メッセージの数が、特定の期間と PVO 検疫に対して設定されたユーザー定義のしきい値を超えると、受信者にアラートが送信されます。 Cisco Secure Email and Web Manager を使用すると、電子メールとして設定したアラートを受信できます。 次の方法を使用して、PVO 検疫しきい値アラートを設定できます。 • レガシー Web インターフェイスの [電子メール(Email)] > [メッセージ検疫(Message Quarantine)] > [ポリシー、ウイルス、およびアウトブレイク検疫(Policy, Virus, and Outbreak Quarantines)] ページ • CLI の `quarantineconfig` コマンド 詳細については、ユーザーガイドの「Centralized Policy, Virus, and Outbreak Quarantines」の章の「PVO Quarantine Threshold Alert」セクションを参照してください。

共有メールボックス用のエンドユーザー検疫の設定	管理者がシングルサインオンによる EUQ へのアクセスを有効にしていて、共有メールボックスへの委任アクセス権を持っている場合、その共有メールボックスのエンドユーザー検疫（EUQ）にアクセスして、スパム検疫済みメッセージに対して任意のアクションを実行できるようになりました。そのため、管理者のワークロードが軽減され、検疫済みメッセージのタイムリーな配信が可能になります。 SAML 2.0 認証を使用して EUQ にログインできる場合、EUQ にアクセスして共有メールボックスのスパム検疫メッセージを検索できます。プライマリメールボックスのスパム検疫済みメッセージを表示したり、アクセスできる共有メールボックスを追加して、その共有メールボックスのスパム検疫済みメッセージを表示したりできます。 EUQ を使用すると、複数の共有メールボックスを追加でき、スパム検疫済みメッセージを表示、検索、リリース、リリースしてセーフリストに追加、および削除するオプションが使用可能になります。 共有メールボックスには、次の方法でアクセスできます。 • スパム検疫通知メールに含まれている [電子メール検疫（email quarantine）] または [すべての検疫済みメッセージを表示（View All Quarantined Messages）] リンクをクリックします。 • スパム検疫ポータルを使用して、Cisco Secure Email and Web Manager EUQ にログインします。 詳細については、ユーザーガイドの「Spam Quarantine」の章の「Configuring End-User Quarantine for Shared Mailbox」セクションを参照してください。 **（注）** Office 365 ユーザーは、この機能を使用できます。この機能では、Microsoft Azure Active Directory API を使用して、共有メールボックスに関連付けられたエンドユーザー検疫へのアクセスが提供されます。

中央集中型電子メールトラッキングサービスのデータストレージ時間の管理	日数に基づいて中央集中型電子メール トラッキング データベースにメッセージ(データ)を保存するように Cisco Secure Email and Web Manager を設定できるようになりました。 この機能は、次のいずれかの方法で設定できます。 • レガシー Web インターフェイスの [システム管理(System Administration)] > [ディスク管理(Disk Management)] > [データ ディスク管理の編集(Edit Data Disk Management)] ページで、[データストレージ時間の適用(Apply Data Storage Time)] オプションを使用する。 • CLI の `diskquotaconfig > edit > Centralized Email Tracking` サブコマンドで `Manage data based on the storage time` ステートメントを使用する。 **重要**:Cisco Secure Email and Web Manager 13.6.2 バージョン以降、Splunk データベースは電子メールトラッキングデータに使用されなくなりました。新しい電子メールトラッキングデータはすべて Lucene データベースに保存されます。この機能を使用すると、電子メールトラッキングデータを含む Splunk データベースが自動的に削除されます。 **アクション**:電子メールトラッキングデータのバックアップを作成します(必要な場合)。CLI の `backupconfig` コマンドを使用して、バックアップアクションを実行できます。詳細については、ユーザーガイドの「Common Administrative Tasks」の章の「Scheduling Single or Recurring Backups」セクションを参照してください。 **(注)** 組織のネットワークにある Cisco Secure Email and Web Manager が 1 つだけの場合は、ネットワークに新しい仮想マシン(VM)を展開する必要があります。仮想 Cisco Secure Email and Web Manager の展開方法の詳細については、『Cisco Secure Email and Web 仮想アプライアンス設置ガイド』を参照してください。 詳細については、ユーザーガイドの「Common Administrative Tasks」の章の「Managing Data Storage Time」セクションを参照してください。
新しい送信者ドメインのレピュテーション判定	このリリースでは、送信者ドメインのレピュテーションの判定は、意図する意味と推奨される使用法を正確に反映するように更新されています。 AsyncOS 14.2.x リリースにアップグレードすると、レポートおよびメッセージトラッキングの従来の SDR 判定は、次のように新しい SDR 判定に置き換えられます。 • 信頼できない • 要検討 • ニュートラル • 好ましい • 信頼できる • 不明

	SDR レポートとメッセージトラッキングの結果は、アップグレード時に新しい判定で更新されます。電子メールゲートウェイも、新しい SDR 判定を含む最新の 14.2 バージョンにアップグレードしてください。 **（注）** SDR レポーティングおよびトラッキング AsyncOS API は、新しい SDR 脅威レベルとカテゴリ構造を反映するように更新されています。 **（注）** SDR トラッキングログが更新され、新しい SDR 脅威レベルと送信者の成熟度の詳細が反映されます。
Cisco Secure Email Cloud Gateway 用 AsyncOS 14.2 の新機能のサポート	[URL レトロスペクションレポート（URL Retrospection Report）] ページ：このレポートページには、URL レトロスペクティブサービスによって処理された URL が表示されます。また、悪意のある URL、URL レトロスペクティブサービスから判定を受け取った日時、影響を受けたメッセージの修復ステータスが一覧表示されます。 **（注）** URL レトロスペクション レポート データは、クラウド管理者ユーザーのみが利用できます。 詳細については、ユーザーガイドの「Using Centralized Email Security Reporting」の章の「URL Retrospection Report Page」セクションを参照してください。
クラシックライセンスの変更：Web インターフェイスおよび CLI の期限日	このリリース以降、クラシックライセンスの Web インターフェイスおよび CLI の既存の [期限日（Expiration Date）] 列ヘッダーが [期限日（猶予期間を含む）（Expiration Date (including grace period)）] に変更されます。これは、期限日に猶予期間が含まれることを示しています。 **（注）** すべてのアラートメッセージとメールログは、機能キーの猶予期間を含む期限日を表示するように変更されます。
Syslog プッシュ用の新しいパラメータ：Syslog ディスクバッファ	（TCP プロトコルのみに適用可能）：Syslog ディスクバッファのパラメータを使用すると、Syslog プッシュ ログ サブスクリプションのローカルディスクバッファを設定でき、リモート Syslog サーバーを使用できない場合、Cisco Secure Email and Web Manager がログイベントをキャッシュできます。Syslog サーバーが使用可能になると、Cisco Secure Email and Web Manager は、そのログサブスクリプションのバッファにあるすべてのデータを Syslog サーバーに送信し始めます。 詳細については、ユーザーガイドの「Logging」の章の「Log Retrieval」セクションを参照してください。

Cisco Secure Email and Web Manager 用の AsyncOS 14.2 で変更された動作

絶対タイムアウトの変更	このリリース以前は、デフォルトの Web UI の [非アクティブタイムアウト（Inactivity Timeout）] フィールドを 12 時間以上に設定した場合、12 時間経過しても Cisco Secure Email and Web Manager の新しい Web インターフェイスからログアウトされず、インターフェイスで使用可能なオプションにアクセスできました。 このリリースにアップグレード後は、デフォルトの Web UI の [非アクティブタイムアウト（Inactivity Timeout）] フィールドを 12 時間以上に設定しても、12 時間経過すると Cisco Secure Email and Web Manager の新しい Web インターフェイスからログアウトされます。
レポートカレンダーの変更	このリリース以前の新しい Web インターフェイスでは、月ごとに集計されているレポートデータの日付を選択できましたが、データが月ごとに集計されている場合にのみ月次データを表示できるため、日付に対して間違った結果が表示されました。 このリリースにアップグレード後は、毎月初日のみを選択できるため、その月の完全なレポートデータが表示されます。
メールログの変更	このリリース以前は、メールログの件名の情報は引用符で囲まれていませんでした。 このリリースにアップグレード後は、メールログの件名の情報は二重引用符で囲まれるようになりました。
FQDN 検証の変更	このリリース以降、ピア証明書を検証するか、証明書をインポートするときに、インポートする証明書またはサーバー証明書で件名（共通名）フィールドが使用できない場合、FQDN 検証は SAN 拡張が重要かどうかを確認します。 **（注）** この動作の変更は、証明書のインポートまたはピア証明書の検証中に FQDN 検証を有効にしている場合にのみ適用されます。

アップデータサーバーの CA 証明書の変更	このリリースで加えられたアップデータサーバーの CA 証明書の動作の変更は次のとおりです。 • FQDN 検証は、Cisco Secure Email and Web Manager にアップデータサーバーの CA 証明書を追加するときに実行されます。新しいステートメント「*共通名または SAN:dNSName あるいは両方が完全修飾ドメイン名（FQDN）形式であるか確認しますか？（Do you want to check if Common Name or SAN:dNSName or both are in Fully Qualified Domain Name(FQDN) format?）*」が、FQDN 検証を実行するための CLI の `updateconfig > trusted_certificates > add` サブコマンドに追加されます。 • CA 証明書の検証は、Cisco Secure Email and Web Manager にアップデータ CA 証明書を追加するときに実行されます。 **（注）** Cisco Secure Email and Web Manager では、ルート CA 証明書とチェーン内の他の証明書が信頼されている場合、アップデータ CA 証明書を追加できます。
システムアップグレード中の CA 証明書の検証	このリリース以降、Cisco Secure Email and Web Manager をアップグレードすると、CA 証明書がアクティブ（期限切れではない）で、証明書の CA フラグが true に設定されている場合にのみ、既存の CA 証明書がアップグレードされます。Cisco Secure Email and Web Manager では、システムのアップグレード中に期限切れの証明書と CA フラグが false に設定された CA 証明書が拒否されます。また、Cisco Secure Email and Web Manager に構成ファイルをロードすると、CA フラグが false に設定された CA 証明書と期限切れの証明書が削除されます。

既知および修正済みの問題

Cisco Secure Email Gateway 用の AsyncOS 14.2 での既知の問題と修正済みの問題

既知の問題	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=afr&svr=3nH&rls=14.2.0&prdNam=Cisco%20Secure%20Email%20Gateway
修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=fr&svr=3nH&rls=14.2.0-620&prdNam=Cisco%20Secure%20Email%20Gateway

Cisco Secure Email and Web Manager 用の AsyncOS 14.2 での既知の問題と修正済みの問題

既知の問題	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&rls=14.2.0&sb=afr&sts=open&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager
修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&rls=14.2.0&sb=fr&sts=fd&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager

Cisco Hybrid Secure Email

Cisco Hybrid Secure Email は Cisco Secure Email Gateway 用の AsyncOS 14.2 をベースにしています。この項では、Cisco Secure Email Gateway 用の AsyncOS 14.2 にアップグレードする方法について説明します。

（注） このリリースの新機能、拡張機能、および既知の問題の詳細については、最新情報（1 ページ）および Cisco Hybrid Secure Email（17 ページ）を参照してください。

アップグレード パス

リリース 14.2.0-620 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 14.2.0-620 にアップグレードできます。

- 13.5.1-277
- 13.5.2-036
- 13.7.0-093
- 14.0.0-480
- 14.0.0-657
- 14.0.0-692
- 14.0.0-698
- 14.0.1-033
- 14.0.1-103
- 14.0.2-020

- 14.0.2-228
- 14.0.2-606
- 14.2.0-102
- 14.2.0-468
- 14.2.0-524
- 14.2.0-616

Cisco Secure Email and Web Manager 用の AsyncOS 14.2 へのアップグレード

次のバージョンから、リリース 14.2.0-206 にアップグレードすることができます。

- 14.2.0-203
- 14.1.0-239
- 14.1.0-250
- 14.1.0-227
- 14.1.0-199
- 14.0.0 - 404
- 14.0.0 - 418
- 13.8.1-068

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。

アップグレードするには、管理者としてログインする必要があります。また、アップグレード後に電子メールゲートウェイ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
- C190、C195、C390、C395、C690、C695、および C695F のハードウェアモデル。

  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
- C380 および C680 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 コンテンツセキュリティ仮想アプライアンス インストール ガイド』を参照してください。このドキュメントは https://www.cisco.com/c/ja_jp/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しても、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（19 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/ja_jp/support/security/email-security-appliance/products-installation-guides-list.html にある『Cisco コンテンツセキュリティ仮想アプライアンス インストール ガイド』に記載されています。

以下のサービスとサポート（27 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。

- 非 FIPS モードの電子メールゲートウェイでの TLS v1.0 の有効化（20 ページ）
- 電子メールゲートウェイで IDN ドメインを使用して設定可能な機能（20 ページ）
- 既存の URL レピュテーション判定の新しいカテゴリと新しい名前（22 ページ）
- Cisco Talos サービスにアクセスするためのファイアウォール設定（22 ページ）

- Cisco Advanced Phishing Protection クラウドサービスにアクセスするためのファイアウォールの設定（23 ページ）
- 電子メールゲートウェイでのサービスログの有効化（23 ページ）
- FIPS の準拠性（23 ページ）
- 中央管理（アプライアンス）を使用した展開のアップグレード（23 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（24 ページ）
- 設定ファイル（24 ページ）.

非 FIPS モードの電子メールゲートウェイでの TLS v1.0 の有効化

非 FIPS モードで TLS v1.0 が有効になっている下位の AsyncOS バージョン（例：12.x または 13.0）から AsyncOS 14.x 以降にアップグレードすると、TLS v1.0 がデフォルトで無効になります。アップグレード後に、電子メールゲートウェイで TLS v1.0 方式を有効にする必要があります。

電子メールゲートウェイで IDN ドメインを使用して設定可能な機能

前提条件：

国際化ドメイン名（IDN）機能を使用する前に、次の前提条件を満たしていることを確認します。

- すべての着信メッセージには UTF-8 でエンコードされた IDN が必要です。
  たとえば、電子メールゲートウェイにメッセージを送信する MTA は IDN をサポートし、メッセージ内のドメインが UTF-8 形式であることを確認する必要があります。
- すべての発信メッセージには UTF-8 でエンコードされた IDN が必要であり、宛先サーバーはそれに応じて IDN を受け入れ、サポートする必要があります。
  たとえば、電子メールゲートウェイからのメッセージを受け入れる MTA は UTF-8 形式でエンコードされた IDN とドメインをサポートする必要があります。
- 該当するすべての DNS レコードで、Punycode 形式を使用して IDN を設定する必要があります。
  たとえば、IDN に MX レコードを設定する場合、DNS レコードのドメインは Punycode 形式である必要があります。

このリリースでは、電子メールゲートウェイ内で IDN ドメインを使用して設定できるのは次の機能**のみ**です。

- **SMTP ルートの設定：**
  - IDN ドメインを追加または編集します。
  - IDN ドメインを使用して SMTP ルートをエクスポートまたはインポートします。
- **DNS の設定：**IDN ドメインを使用して DNS サーバーを追加または編集します。
- **リスナーの設定：**
  - インバウンドリスナーまたはアウトバウンドリスナーのデフォルトドメインの IDN ドメインを追加または編集します。
  - HAT テーブルまたは RAT テーブルで IDN ドメインを追加または編集します。
  - IDN ドメインを使用して HAT テーブルまたは RAT テーブルをエクスポートまたはインポートします。

- **メールポリシーの設定:**
  - [着信メールポリシー(Incoming Mail Policies)] の送信者([送信者を追跡する(Following Senders)] オプションまたは [送信者を追跡しない(Following Senders are not)] オプション)と受信者([受信者を追跡する(Following Recipients)] または [受信者を受信しない(Recipients are not)] オプション)の IDN ドメインを使用してドメインを追加または編集します。
  - [発信メールポリシー(Outgoing Mail Policies)] の送信者([送信者を追跡する(Following Senders)] オプションまたは [送信者を追跡しない(Following Senders are not)] オプション)と受信者([受信者を追跡する(Following Recipients)] または [受信者を受信しない(Recipients are not)] オプション)の IDN ドメインを使用してドメインを追加または編集します。
  - [着信メールポリシー(Incoming Mail Policies)] または [送信メールポリシー(Outgoing Mail Policies)] で IDN ドメインを使用した送信者または受信者の検索
  - IDN ドメインを使用して送信者判定の例外を定義します。
  - IDN ドメインを使用してアドレスリストを作成します。
  - 宛先の制御に IDN ドメインを使用して宛先ドメインを追加または編集します。
- **バウンスプロファイルの設定:**IDN ドメインを使用して代替電子メールアドレスを追加または編集します。
- **送信者ドメインレピュテーションの設定:**IDN ドメインの送信者ドメイン レピュテーション スコアを定義します。
- **IP レピュテーションの設定:**IDN ドメインの IP レピュテーションスコアを定義します。
- **LDAP の設定:**IDN ドメインを使用して、LDAP グループクエリを作成し、クエリを受け入れ、クエリをルーティングし、クエリをマスカレードします。
- **レポートの設定:**IDN データ(ユーザー名、電子メールアドレス、ドメイン)をレポートに表示します。
- **メッセージトラッキングの設定:**メッセージトラッキングに IDN データ(ユーザー名、電子メールアドレス、およびドメイン)を表示します。
- **ポリシー、ウイルス、およびアウトブレイク隔離の設定:**
  - ウイルス対策エンジンによる判定に従って、マルウェアを送信する可能性のある IDN ドメインを含むメッセージを表示します。
  - スパムまたはマルウェアの可能性があるとアウトブレイクフィルタによって検出された IDN ドメインを含むメッセージを表示します。
  - メッセージフィルタ、コンテンツフィルタ、および DLP メッセージアクションによって検出された IDN ドメインを含むメッセージを表示します。
- **スパムの隔離の設定:**
  - スパム、または疑いのあるスパムとして検出された IDN ドメインを含むメッセージを表示します。
  - IDN ドメインを含む電子メールアドレスをセーフリストとブロックリストのカテゴリに追加します。

(注) 現在、IDN ドメインを持つ受信者は、[スパムの隔離(Spam Quarantine)] 設定ページの [エンドユーザーの隔離アクセス(End-User Quarantine Access] セクションでエンドユーザー認証方式が [なし(None)] に設定されている場合にのみ、エンドユーザーの隔離にアクセスできます。

- [SPF 構成設定(SPF Configuration Settings)]:IDN ドメインを使用してメッセージの SPF 検証を実行します。
- [DKIM 構成設定(DKIM Configuration Settings)]:IDN ドメインを使用して DKIM 署名とメッセージの検証を実行します。
- [DMARC 構成設定(DMARC Configuration Settings)]:IDNドメインを使用してメッセージの DMARC 検証を実行します。

既存の URL レピュテーション判定の新しいカテゴリと新しい名前

次の表に、電子メールゲートウェイの既存の URL レピュテーション判定の新しいカテゴリと新しい名前を示します。

現在の URL レピュテーション判定名	新しい Cisco Talos URL レピュテーション判定名	スコア範囲	説明
クリーン	信頼できる	+6.0 ～ +10.0	優れた安全性を示す動作を表示します。
ニュートラル	好ましい	+0.1 ～ +5.9	一定のレベルの安全性を示す動作を表示します。
	ニュートラル	-3.0 ～ 0.0	好ましい動作や望ましくない動作は表示されません。ただし、この判定は評価の結果です。
	要検討	-5.9 ～ -3.1	リスクを示す可能性のある動作、または望ましくない動作を表示します。
悪意のある	信頼できない	-10.0 ～ -6.0	非常に悪い、悪意のある、または望ましくない動作を表示します。
スコアなし	不明	スコアなし	この判定は、これまで評価されなかった場合や、脅威レベルの判定をアサートできない場合に表示されます。

Cisco Talos サービスにアクセスするためのファイアウォール設定

電子メールゲートウェイを Cisco Talos サービスに接続するには、次のホスト名または IP アドレス用にファイアウォール上で HTTPS(Out)443 ポートを開く必要があります(以下の表を参照)。

(注) HTTPS アップデータプロキシ設定は、Cisco Talos サービスへの接続に使用されます。

ホスト名	IPv4	IPv6
grpc.talos.cisco.com	146.112.62.0/24	2a04:e4c7:ffff::/48
email-sender-ip-rep-grpc.talos.cisco.com	146.112.63.0/24	2a04:e4c7:fffe::/48
serviceconfig.talos.cisco.com	146.112.255.0/24	-
	146.112.59.0/24	-

詳細については、ユーザーガイドの「Firewall」の章を参照してください。

Cisco Advanced Phishing Protection クラウドサービスにアクセスするためのファイアウォールの設定

電子メールゲートウェイを Cisco Advanced Phishing Protection クラウドサービスに接続するには、次のホスト名用にファイアウォール上で HTTPS（Out）443 ポートを開く必要があります。

- kinesis.us-west-2.amazonaws.com
- sensor-provisioner.ep.prod.agari.com
- houston.sensor.prod.agari.com

詳細については、ユーザーガイドの「Firewall」の章を参照してください。

電子メールゲートウェイでのサービスログの有効化

サービスログは、Cisco E メール セキュリティ アプライアンス データ シートに基づいて個人データを収集するために使用されます。

サービスログは、フィッシング検出を改善するために Cisco Talos クラウドサービスに送信されます。

Cisco E メール セキュリティ ゲートウェイは、顧客の電子メールから限定された個人データを収集し、幅広く有用な脅威検出機能を提供します。この機能は、検出された脅威アクティビティを収集し、傾向を提示し、関連付けるための専用分析システムと組み合わせることができます。シスコでは、個人データを使用して、脅威の状況を分析し、悪意のある電子メールに脅威の分類ソリューションを提供し、スパム、ウイルス、ディレクトリ獲得攻撃などの新しい脅威から電子メールゲートウェイを保護するために、電子メールゲートウェイの機能を向上させています。

アップグレードプロセス中に、次のいずれかから電子メールゲートウェイでサービスログを有効にする方法を選択できます。

- Web インターフェイスの [システム管理（System Administration）] > [システムアップグレード（System Upgrade）] ページで、[サービスログ（Service Logs）] に [同意する（I Agree）] オプションを選択します。
- `upgrade` CLI コマンドの「*サービスログをデフォルトで有効にして続行しますか？[Y]（Do you agree to proceed with Service Logs being enabled by default? [y]）*」ステートメントに「**Yes**」と入力します。

詳細については、ユーザーガイドの「Improving Phishing Detection Efficacy using Service Logs」の章を参照してください。

FIPS の準拠性

AsyncOS 14.2 リリースは、FIPS 準拠のリリースではありません。電子メールゲートウェイで FIPS モードを有効にしている場合は AsyncOS 14.2 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。

中央管理（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、C380、C680、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、これらの電子メールゲートウェイをクラスタから削除します。

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、x70、および x80 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、x70、および x80 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。

設定ファイル

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。

このリリースへのアップグレード

はじめる前に

- Cisco Hybrid Secure Email（17 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（18 ページ）を確認してください。
- 仮想電子メールゲートウェイ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（19 ページ）を参照してください。

手順

次の手順を実行して電子メールゲートウェイをアップグレードします。

ステップ 1 電子メールゲートウェイから、XML 構成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、電子メールゲートウェイからセーフリスト/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 キューが空になるまで待ちます。

ステップ 5 [システム管理（System Administration）] タブで、[システムアップグレード（System Upgrade）] ページを選択します。

ステップ 6 [利用可能なアップグレード（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 [アップグレードの開始（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、[今すぐリブート（Reboot Now）] ボタンをクリックして電子メールゲートウェイを再起動します。

ステップ 9 すべてのリスナーを再開します。

次の作業

パフォーマンスアドバイザリ（26 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

IP レピュテーションサービスのステータスのモニタリング

アップグレード後、IP レピュテーションのデバッグログに IP アドレス 172.0.0.2 が表示される場合があります。

IP アドレス 172.0.0.2 は、主に IP レピュテーション クラウド サービスの可用性を確認するために使用されます。この IP アドレスは、IP レピュテーション クラウド サービスと電子メールゲートウェイの接続を確認するために内部的に使用されます。IP アドレスは、送受信されるメッセージやユーザーネットワークとは関係ありません。

DLP サービスステータスチェック

このリリースにアップグレードした後、DLP サービスで問題が発生する可能性があります。

ソリューション：CLI で `diagnostic` > `services` > `DLP` > `status` サブコマンドを使用して、電子メールゲートウェイの DLP サービスのステータスを確認します。DLP サービスが実行されていない場合は、既知の問題リストにある CSCvy08110 の不具合の「回避策」セクションを参照してください。既知の問題を表示する方法については、リリースノートの既知および修正済みの問題（16 ページ）セクションを参照してください。

電子メールゲートウェイでのパスワードで保護された添付ファイルのスキャン

パスワード保護された添付ファイルをスキャンするように電子メールゲートウェイのコンテンツスキャナを設定する場合、電子メールトラフィックにパスワード保護された添付ファイルが高い割合で含まれていると、パフォーマンスに影響を与える可能性があります。

AsyncOS 13.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 13.x にアップグレードした後、電子メールゲートウェイ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は、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「この不整合をどのように解決しますか？（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]>
```

インテリジェント マルチスキャンおよびグレイメールのグローバル設定の変更

AsyncOS 14.0 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、電子メールゲートウェイ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、電子メールゲートウェイは 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、電子メールゲートウェイは [最大タイムアウト（maximum timeout）] および [最大メッセージサイズ（maximum message size）] の値を使用して、IMS と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、電子メールゲートウェイは 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。

パフォーマンスアドバイザリ

アウトブレイクフィルタ

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。システムのキャパシティがいっぱいか、いっぱいに近いときに 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。

サービスとサポート

（注） Cisco クラウド E メール セキュリティ（CES）に関するサポートが必要な場合、Cisco TAC にご連絡いただく際には契約番号をお手元にご用意ください。

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、電子メールゲートウェイ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、ユーザーガイド またはオンラインヘルプを参照してください。