Cisco Email Security スタートアップガイド

この章は、次の項で構成されています。

AsyncOS 13.0 の新機能

表 *1 : AsyncOS 13.0* の新機能

機能	説明
Microsoft Exchange online、Microsoft Exchange オンプレミス、ハイブリッド、およびマルチテナント展開でのメールボックス自動修復	ファイルは常に、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。AMP は、新しい情報が発生する際にこの変化を識別し、アプライアンスにレトロスペクティブ アラートを送信することができます。脅威判定が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アプライアンスを設定できます。 アプライアンスは、次のメールボックス展開のメッセージに対して自動修復アクションを実行できます。 • Microsoft Exchange Online：Microsoft Office 365 でホストされたメールボックス • Microsoft Exchange オンプレミス：ローカルの Microsoft Exchange サーバ • ハイブリッド/マルチテナント構成：Microsoft Exchange Online 展開および Microsoft Exchange オンプレミス展開で設定されたメールボックスの組み合わせ 詳細については、メールボックスのメッセージの自動修復を参照してください。
FIPS 認定	Cisco E メール セキュリティ アプライアンスは FIPS 認定され、次の FIPS 140-2 認定の暗号化モジュールを統合しました：Cisco Common Crypto Modul（FIPS 140-2 認定番号 2984）。 詳細については、FIPS 管理を参照してください。
SAML 2.0 を使用したシングル サインオン（SSO）	Cisco E メール セキュリティ アプライアンスは SAML 2.0 SSO をサポートするようになりました。これにより、管理ユーザは組織内で他の SAML 2.0 SSO 対応サービスへのアクセスに使用している同じクレデンシャルでアプライアンスの Web インターフェイス（レガシー Web インターフェイスおよび新しい Web インターフェイスの両方）にログインできます。 詳細については、システム管理を参照してください。

機能	説明
Common Event Format（CEF）ベースのロギングのサポート	Cisco E メール セキュリティ アプライアンスは、各メッセージ イベントを 1 つのログラインにまとめる新しいタイプのログ サブスクリプションである「統合イベント ログ」をサポートするようになりました。これにより、分析のためにセキュリティ情報イベント管理（SIEM）ベンダーに送信されるデータ（ログ情報）のバイト数が減ります。 統合イベント ログのログ メッセージ形式は、すべての SIEM ベンダーがサポートする Common Event Format（CEF）です。 詳細については、ログを参照してください。
メッセージの添付ファイルを Safe Print で出力する機能。	悪意のあるまたは疑わしいと検出されたメッセージの添付ファイルの安全なビュー（Safe Print で出力される PDF バージョン）を提供するように電子メール ゲートウェイを構成できます。メッセージの添付ファイルの安全なビューがエンド ユーザに配信され、元の添付ファイルはメッセージから削除されます。 「Safe Print」コンテンツ フィルタ アクションを使用すると、設定されたコンテンツ フィルタ条件に一致するすべてのメッセージの添付ファイルを Safe Print で出力できます。 電子メール ゲートウェイでメッセージの添付ファイルを Safe Print で出力する機能は、組織が次のことを行うのに役立ちます。 • 悪意のあるコンテンツや疑わしいコンテンツを含むメッセージの添付ファイルが組織のネットワークに侵入するのを防ぎます。 • 悪意のあるメッセージや疑わしいメッセージの添付ファイルをマルウェアの影響を受けずに表示します。 • エンドユーザの要求に応じて元のメッセージ添付ファイルを配信します。 詳細については、メッセージの添付ファイルを Safe Print で出力する場合の電子メール ゲートウェイの設定を参照してください。

機能	説明
アプライアンスと Cisco Threat Response との統合	アプライアンスを Cisco Threat Response と統合すると、Cisco Threat Response で次の操作を実行できます。 • 組織内の複数のアプライアンスからメッセージ トラッキングのデータを確認します。 • メッセージ トラッキングで検出された脅威を特定、調査、および修正します。 • 特定した脅威を迅速に解決し、特定した脅威に対して推奨されるアクションを実行します。 • 脅威をドキュメント化して調査内容を保存し、他のデバイスと情報を共有します。 詳細については、Cisco Threat Response との統合を参照してください。
ケースブックを使用した脅威分析の実行	Cisco E メール セキュリティ アプライアンスには、ケースブックとピボット メニューのウィジェットが含まれるようになりました。 （注） Microsoft Internet Explorer ブラウザを使用してアプライアンスにアクセスしている場合、[ケースブック（Casebook）] ウィジェットを使用することはできません。 [ケースブック（Casebook）] ウィジェットと [ピボット メニュー（Pivot Menu）] ウィジェットを使用して、アプライアンスで次のアクションを実行できます。 • 観測対象をケースブックに追加し、脅威分析の調査を実行します。 • 新しいケース、既存のケース、または Cisco Threat Response ポータルに登録されているその他のデバイス（エンドポイント向け AMP、Cisco Umbrella、Cisco Talos Intelligence など）の監視対象をピボットし、脅威分析のために調査します。 詳細については、Cisco Threat Response との統合を参照してください。

機能	説明
機能の使用状況の統計情報を収集することによるユーザエクスペリエンスの向上	シスコ E メール セキュリティ アプライアンスでは、アプライアンスの新しい Web インターフェイスで機能やインターフェイスの使用状況統計が収集されるようになり、全体的なユーザエクスペリエンスが向上します。収集されたすべてのデータは匿名化されます。この機能の選択を解除する場合は、Web インターフェイスで [システム管理（System Administration）] > [一般設定（General Settings）] > [使用状況分析（Usage Analytics）] ページに移動して無効にします。詳細については、新しいWebインターフェイスを使用したアプライアンスの使用状況統計の収集を参照してください。
スパム対策スキャン設定の強化	新しい「アグレッシブな」スキャンプロファイルがスパム対策のグローバル設定に追加されました。このプロファイルを使用して、スパムとして検出された着信または発信メッセージに、より高いプライオリティを割り当てたり、誤検出の可能性を高めたりすることができます。 このオプションは、次のいずれかの方法で有効化できます。 • Web インターフェイスの [セキュリティサービス（Security Services）] > [IronPortスパム対策（IronPort Anti-Spam）] > [グローバル設定の編集（Edit Global Settings）]。「IronPort Anti-Spam スキャンの設定」を参照してください。 • CLI の `antispamconfig` コマンド。『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。 （注） アグレッシブスキャンプロファイルのオプションが有効になっている場合、スパム対策しきい値に対するメールポリシーを調整すると、通常のプロファイルスキャンが使用される場合よりも与える影響が大きくなります。したがって、スパムの捕捉率と誤検出率との最適なバランス調整のため、既存のスパム対策メールポリシーしきい値設定を確認する必要があります。

機能	説明
レポート、隔離、およびトラッキングのための新しいWebインターフェイス	

機能	説明

	アプライアンスには、現在、次を検索および表示するための新しい Web インターフェイスがあります。
	• 電子メール脅威のレポート
	• ファイルおよびマルウェアのレポート
	• 接続およびフローのレポート
	• ユーザ レポート
	• フィルタのレポート
	• スケジュール設定されたレポート（Scheduled Reports）
	• アーカイブ レポート（Archived Reports）
	• 詳細については、新しい Web インターフェイスの電子メール セキュリティ モニタ ページを参照してください。
	• **スパム隔離**
	  • スパムやスパムの疑いがあるメッセージを、Web インターフェイス ページの **[隔離（Quarantine）] > [スパム隔離（Spam Quarantine）] > [検索（Search）]** で表示および検索できるようになりました。
	  • セーフリストやブロックリストに追加されたドメインを、Web インターフェイスの **[隔離（Quarantine）] > [スパム隔離（Spam Quarantine）] > [セーフリスト（Safelist）]** または **[ブロックリスト（Blocklist）]** ページで表示、追加、および検索できます。
	詳細については、スパム隔離を参照してください。
	• **ポリシー、ウイルスおよびアウトブレイク隔離**。ポリシー隔離、ウイルス隔離、およびアウトブレイク隔離は、Web インターフェイスの [隔離（Quarantine）] > [その他の隔離（Other Quarantine）] > [検索（Search）] ページで表示および検索できます。詳細については、ポリシー、ウイルス、およびアウトブレイク隔離を参照してください。
	• **メッセージ トラッキング**。メッセージまたはメッセージのグループは、検索条件に応じて Web インターフェイスの **[トラッキング（Tracking）] > [検索（Search）]** ページから検索できます。詳細については、メッセージ トラッキングを参照してください。

機能	説明

	重要
	• アプライアンスで AsyncOS API が有効になっていることを確認してください。
	• AsyncOS HTTPS API ポートが複数のネットワーク インターフェイスで有効になっていないことを確認します。
	• デフォルトで、`trailblazerconfig` はアプライアンスで有効になっています。
	  • 設定した HTTPS ポートがファイアウォールで開かれていることを確認します。デフォルトの HTTPS ポートは 4431 です。
	  • また、アプライアンスにアクセスするために指定したホスト名を DNS サーバが解決できることを確認します。

`trailblazerconfig` CLI コマンド	`trailblazerconfig` コマンドを使用すると、新しい Web インターフェイスで HTTP と HTTPS のポートを介して受信接続と送信接続をルーティングできます。 （注） デフォルトで、`trailblazerconfig` のCLI コマンドはアプライアンスで有効になっています。`help trailblazerconfig` コマンドを入力すると、インライン ヘルプを参照できます。 詳細については、『*Cisco Email Security Command Reference Guide*』を参照してください。
メッセージ トラッキング機能拡張	メッセージの「`Reply To`」ヘッダーに基づいてメッセージを検索できるようになりました。 詳細については、メッセージ トラッキングを参照してください。

機能	説明
[高度なマルウェア防御（Advanced Malware Protection）] レポートの拡張機能	[高度なマルウェア防御（Advanced Malware Protection）] レポート ページには、次の拡張機能が追加されています • 新しいセクション - [カテゴリ別受信マルウェア ファイル（Incoming Malware Files by Category）] セクションは、[カスタム検出（Custom Detection）] に分類される、AMP for Endpoints コンソールから受信したブラックリスト ファイル SHA の割合を表示します。 AMP for Endpoints コンソールから取得されるブラックリストに追加されたファイル SHA の脅威名は、レポートの [着信マルウェア脅威ファイル（Incoming Malware Threat Files）] セクションで [シンプル カスタム検出（Simple Custom Detection）] として表示されます。 • 新しいセクション - **[カテゴリ別受信マルウェア ファイル（Incoming Malware Files by Category）]** セクションは、**[カスタム検出（Custom Detection）]** に分類されるしきい値設定を基にしてブラックリスト ファイル SHA の割合を表示します。 • レポートの [詳細（More Details）] セクションでリンクをクリックすると、AMP for Endpoints コンソールでのブラックリスト追加ファイル SHA のファイル トラジェクトリ詳細を表示できます。 • 新しい判定 - ファイルの分析後に、ファイルに動的なコンテンツが存在しないときの新しい判定 [低リスク（Low Risk）] が導入されました。判定の詳細は、レポートの [AMPにより渡された受信ファイル（Incoming Files Handed by AMP）] セクションに表示されます。 [高度なマルウェア防御（Advanced Malware Protection）] ページ を参照してください。

機能	説明
メトリックバー ウィジェット	[メトリックバー（Metrics Bar）] ウィジェットを使用すると、[高度なマルウェア防御（Advanced Malware Protection）] レポート ページで Cisco Threat Grid アプライアンスによって実行されるファイル分析のリアルタイム データを確認できます。 詳細については、[高度なマルウェア防御（Advanced Malware Protection）] ページを参照してください。
IP アドレスを永続的なホワイトリストまたはブラックリストに分類する機能	SSH を使用してアプライアンスにアクセスするために使用する IP アドレスを永続的なホワイトリストまたはブラックリストに分類することができます。アプライアンスまたは `ipblockd` サービスが再起動されても、永続的なブラックリストまたはホワイトリスト内の IP アドレスは保持されます。 IP アドレスを永続的なホワイトリストまたはブラックリストに分類するには、CLI で `sshconfig > access` 管理サブコマンドを使用できます。 詳細については、『*CLI Reference Guide for AsyncOS 13.0 for Email Security Appliances*』の「`sshconfig`」の項を参照してください。
偽装電子メール検出の強化	**[メールポリシー（Mail Policies）] > [アドレスリスト（Address Lists）]** を選択して、完全な電子メールアドレスのみで構成された例外リストを作成し、偽装電子メール検出コンテンツフィルタをバイパスすることができます。 アプライアンスで、設定済みのコンテンツフィルタから電子メール アドレスをスキップする場合、偽装電子メール検出ルールでこの例外リストを使用できます。

機能	説明
How-To ウィジェットで使用可能な新しいウォークスルー	How-To は、アプライアンスで複雑なタスクを実行するためにウォークスルー形式でユーザにアプリ内アシスタンスを提供する、コンテキスト型ウィジェットです。このリリースでは、次のウォークスルーが追加されています。 • SAML 2.0 を使用するシングルサインオン • メールボックスの自動修復を使用したメールボックス内の悪意のあるメッセージの修復 • 悪意のあるメッセージまたは疑わしいメッセージの添付ファイルの安全なビューを提供 • Common Event Format（CEF）の統合ロギングの設定 ウォークスルーのリストは更新可能なクラウドです。ハウツーウィジェットの更新バージョンとポップアップウィンドウを表示するには、必ずブラウザのキャッシュをクリアしてください。 詳細は、ユーザーガイドまたはオンラインヘルプの「Accessing the Appliance」の章と『CLI Reference Guide for AsyncOS for Cisco Email Security Appliances』を参照してください。 各リリースでサポートされているハウツーのリストを表示するには、『Walkthroughs Supported in AsyncOS for Cisco Email Security Appliances』を参照してください。

Webインターフェイスの比較、新しいWebインターフェイスとレガシー Web インターフェイス

次の表は、新しい Web インターフェイスの以前のバージョンとの比較を示しています。

表 *2:* 新しい *Web* インターフェイスとレガシー *Web* インターフェイスとの比較

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
ランディングページ	アプライアンスにログインすると、[メールフロー概要（Mail Flow Summary）] ページが表示されます。	アプライアンスにログインすると、[マイダッシュボード（My Dashboard）] ページが表示されます。
レポートドロップダウン	[レポート（Reports）] ドロップダウンで、アプライアンスのレポートを表示できます。	[モニタ（Monitor）] メニューで、アプライアンスのレポートを表示できます。
[マイ レポート（My Reports）] ページ	[レポート（Reports）] ドロップダウンから [マイレポート（My Reports）] を選択します。	[マイレポート（My Reports）] ページは、[モニタ（Monitor）] > [マイダッシュボード（My Dashboard）] から表示できます。
[メール フロー概要（Mail Flow Summary）] ページ	[メールフロー概要（Mail Flow Summary）] ページには、着信および送信メッセージに関するトレンド グラフやサマリー テーブルが表示されます。	[受信メール（Incoming Mail）] には、着信および発信メッセージに関するグラフやサマリー テーブルが含まれます。
高度なマルウェア防御レポートページ	[レポート（Reports）] メニューの [高度なマルウェア防御（Advanced Malware Protection）] レポートページでは、次のセクションを使用できます。 • [概要（Overview）] • [AMP ファイル レピュテーション（AMP File Reputation）] • [ファイル分析（File Analysis）] • [ファイル レトロスペクション（File Retrospection）] • [メールボックスの自動修復（Mailbox Auto Remediation）]	アプライアンスの [モニタ（Monitor）] メニューには、次の [高度なマルウェア防御（Advanced Malware Protection）] レポートページがあります。 • [高度なマルウェア防御（Advanced Malware Protection）] • [AMP ファイル分析（AMP File Analysis）] • [AMP判定のアップデート（AMP Verdict Updates）] • [メールボックスの自動修復（Mailbox Auto Remediation）]

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
アウトブレイク フィルタ ページ	新しい Web インターフェイスの [アウトブレイクフィルタリング（Outbreak Filtering）] レポート ページでは、[過去1年間のウイルスアウトブレイク（Past Year Virus Outbreaks）] および [過去1年間のウイルスアウトブレイクの概要（Past Year Virus Outbreak Summary）] は使用できません。	[モニタ（Monitor）] > [アウトブレイクフィルタ（Outbreak Filters）] ページには、[過去1年間のウイルスアウトブレイク（Past Year Virus Outbreaks）] および [過去1年間のウイルスアウトブレイクの概要（Past Year Virus Outbreak Summary）] が表示されます。
スパム隔離（管理ユーザーおよびエンド ユーザー）	新しい Web インターフェイスで **[隔離（Quarantine）] > [スパム隔離（Spam Quarantine）] > [検索（Search）]** をクリックします。 エンドユーザは、次の URL を使用してスパム隔離にアクセスできます。 `https://example.com:<https-api-port>/euq-login` `example.com` はアプライアンス ホスト名で、`<https-api-port>` はファイアウォールで開いている AsyncOS API HTTPS ポートです。	スパム隔離は、[モニタ（Monitor）] > [スパム隔離（Spam Quarantine）] から表示できます。
ポリシー、ウイルスおよびアウトブレイク隔離	新しい Web インターフェイスで **[隔離（Quarantine）] > [その他の隔離（Other Quarantine）]** をクリックします。 新しい Web インターフェイスでは、[ポリシー、ウイルス、およびアウトブレイク隔離（Policy, Virus and Outbreak Quarantines）] のみを表示できます。	アプライアンスでは、[モニタ（Monitor）] > [ポリシー、ウイルス、およびアウトブレイク隔離（Policy, Virus and Outbreak Quarantines）] を使用して、ポリシー、ウイルス、およびアウトブレイク隔離を表示、設定、および変更できます。

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
隔離内のメッセージに対するすべてのアクションの選択	複数（またはすべて）のメッセージを選択し、削除、遅延、リリース、移動などのメッセージ アクションを実行できます。	複数のメッセージを選択して、メッセージ アクションを実行することはできません。
添付ファイルの最大ダウンロード制限	隔離されたメッセージの添付ファイルのダウンロードの上限は 25 MB に制限されています。	-
拒否された接続	拒否された接続を検索するには、で、[トラッキング（Tracking）] > [検索（Search）]> [拒否された接続（Rejected Connection）] タブをクリックします。	-
クエリ設定	では、メッセージトラッキング機能の [クエリ設定（Query Settings）] フィールドは使用できません。	メッセージ トラッキング機能の [クエリ設定（Query Settings）] フィールドで、クエリのタイムアウトを設定できます。
有効なメッセージ トラッキング データ	[有効なメッセージトラッキングデータ（Message Tracking Data Availability）] ページにアクセスするには、Web インターフェイスのページの右上にある歯車アイコンをクリックします。	アプライアンスの欠落データインターバルを表示することができます。
メッセージの追加詳細の表示	[判定チャート（Verdict Charts）]、[最後の状態（Last State）]、[送信者グループ（Sender Groups）]、[送信者IP（Sender IP）]、[SBRSスコア（IP Reputation Score）]、[ポリシー一致（Policy Match）] の詳細など、メッセージの追加詳細を表示できます。	-

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
判定チャートと最後の状態の判定	判定チャートに、アプライアンス内の各エンジンによってトリガーされる可能性のあるさまざまな判定の情報が表示されます。 メッセージの最後の状態によって、エンジンのすべての可能な判定の後に、トリガーされる最終判定が決まります。	メッセージの判定チャートと最後の状態の判定は、使用できません。
メッセージの詳細におけるメッセージ添付ファイルとホスト名	アプライアンスでは、メッセージの添付ファイルとホスト名は、メッセージの [メッセージの詳細（Message Details）] セクションには表示されません。	メッセージの添付ファイルとホスト名は、メッセージの [メッセージの詳細（Message Details）] セクションに表示されます。
メッセージの詳細における送信者グループ、送信者 IP、SBRSスコア、およびポリシー一致	メッセージの送信者グループ、送信者 IP、SBRSスコア、およびポリシー一致の詳細は、アプライアンスの [メッセージの詳細（Message Details）] セクションに表示されます。	メッセージの送信者グループ、送信者 IP、SBRSスコア、およびポリシー一致は、メッセージの [メッセージの詳細（Message Details）] セクションには表示されません。
メッセージの方向（受信または送信）	メッセージの方向（受信または送信）は、アプライアンスのメッセージトラッキング結果ページに表示されます。	メッセージの方向（受信または送信）は、メッセージ トラッキング結果ページには表示されません。

詳細情報の入手先

シスコでは、アプライアンスに関する理解を深めて頂くために次の資料を提供しています。

- サード パーティ コントリビュータ （18 ページ）
- マニュアルに関するフィードバック （18 ページ）
- シスコ アカウントの登録 （18 ページ）

資料

アプライアンスの GUI で右上の [ヘルプとサポート（Help and Support）] をクリックすることにより、ユーザ ガイドのオンライン ヘルプ バージョンに直接アクセスできます。

Cisco E メール セキュリティ アプライアンス のマニュアルセットには次のマニュアルが含まれます。

- リリース ノート
- ご使用の Cisco Email Security Appliances モデルのクイック スタート ガイド
- ご使用のモデルまたはシリーズのハードウェア インストール ガイドまたはハードウェア インストールおよびメンテナンス ガイド
- 『*Cisco Content Security Virtual Appliance Installation Guide*』
- 『*Cisco E* メール セキュリティ アプライアンス 向け *AsyncOS* ユーザーガイド』（本書）
- 『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances* 』
- 『AsyncOS API for Cisco Email Security Appliances - Getting Started Guide』

Cisco Content Security 製品のすべてに関する資料が以下で入手できます。

Cisco コンテンツ セキュリティ製品のマニュアル	**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 E メール セキュリティ	https://www.cisco.com/c/ja_jp/support/security/email-security-appliance/series.html
Cisco Web セキュリティ	https://www.cisco.com/c/ja_jp/support/security/web-security-appliance/series.html
Cisco コンテンツ セキュリティ管理	https://www.cisco.com/c/ja_jp/support/security/content-security-management-appliance/series.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	https://www.cisco.com/c/ja_jp/support/security/email-security-appliance/products-command-reference-list.html
Cisco IronPort 暗号化	https://www.cisco.com/c/ja_jp/support/security/email-security-appliance/products-command-reference-list.html

トレーニング

シスコでは、技術者、パートナー、学生など、それぞれのニーズに合わせた、さまざまなトレーニングプログラムおよびトレーニングコースを用意しています。

- http://www.cisco.com/c/en/us/training-events/training-certifications/supplemental-training/email-and-web-security.html

- http://www.cisco.com/c/en/us/training-events/training-certifications/overview.html

Cisco 通知サービス

セキュリティ アドバイザリ、フィールド ノーティス、販売終了とサポート終了の通知、およびソフトウェアアップデートと既知の問題に関する情報などのCiscoコンテンツセキュリティアプライアンスに関連する通知が配信されるように署名して参加します。

受信する情報通知の頻度やタイプなどのオプションを指定できます。使用する製品ごとの通知に個別に参加する必要があります。

参加するには、http://www.cisco.com/cisco/support/notifications.html に移動します。

Cisco.com アカウントが必要です。ない場合は、シスコ アカウントの登録 （18 ページ）を参照してください。

ナレッジ ベース

手順

ステップ 1 製品のメイン ページ（http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html）にアクセスします。

ステップ 2 名前に **TechNotes** が付くリンクを探します。

シスコサポートコミュニティ

シスコ サポート コミュニティは、シスコのお客様、パートナー、および従業員のオンラインフォーラムです。電子メールおよびWebセキュリティに関する一般的な問題や、特定のシスコ製品に関する技術情報について話し合う場を提供します。このフォーラムにトピックを投稿して質問したり、他のシスコ ユーザと情報を共有したりできます。

Customer Support Portal のシスコ サポート コミュニティには、次の URL からアクセスします。

- 電子メール セキュリティと関連管理:

  https://supportforums.cisco.com/community/5756/email-security

- Web セキュリティと関連管理：

  https://supportforums.cisco.com/community/5786/web-security

シスコカスタマーサポート

シスコ TAC：http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

従来の IronPort のサポート サイト：http://www.cisco.com/c/en/us/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、ユーザー ガイドまたはオンライン ヘルプを参照してください。

サード パーティ コントリビュータ

次のページにある、ご使用のリリースのオープン ソース ライセンス情報を参照してください。
http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-release-notes-list.html

Cisco AsyncOS 内に付属の一部のソフトウェアは、FreeBSD、Stichting Mathematisch Centrum、Corporation for National Research Initiatives などのサード パーティ コントリビュータのソフトウェア使用許諾契約の条項、通知、条件の下に配布されています。これらすべての契約条件は、Cisco ライセンス契約に含まれています。

これらの契約内容の全文は次の URL を参照してください。

https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html

Cisco AsyncOS 内の一部のソフトウェアは、Tobi Oetiker の書面による同意を得て、RRDtool を基にしています。

このマニュアルには、Dell Computer Corporation の許可を得て複製された内容が一部含まれています。このマニュアルには、McAfee の許可を得て複製された内容が一部含まれています。このマニュアルには、Sophos の許可を得て複製された内容が一部含まれています。

マニュアルに関するフィードバック

シスコのテクニカル マニュアル チームは、製品ドキュメントの向上に努めています。コメントおよびご提案をお待ちしています。ぜひ以下の電子メールまでお知らせください。

contentsecuritydocs@cisco.com

メッセージの件名には、製品名、リリース番号、このマニュアルの発行日をご記入ください。

シスコ アカウントの登録

Cisco.com の多数のリソースへアクセスするには、シスコのアカウントが必要です。

Cisco.com のユーザ ID をお持ちでない場合は次のリンク先で登録できます。
https://idreg.cloudapps.cisco.com/idreg/register.do

関連項目

- Cisco 通知サービス （17 ページ）
- ナレッジ ベース （17 ページ）

Cisco E メール セキュリティ アプライアンス の概要

AsyncOS™ オペレーティング システムには、次の機能が組み込まれています。

- SenderBase レピュテーション フィルタと Cisco Anti-Spam を統合した独自のマルチレイヤアプローチによるゲートウェイでの**スパム対策**。
- SophosおよびMcAfeeウイルス対策スキャンエンジンによるゲートウェイでの**ウイルス対策**。
- 新しいアップデートが適用されるまで危険なメッセージを隔離し、新しいメッセージ脅威に対する脆弱性を削減する、新しいウイルス、詐欺、およびフィッシングの拡散に対するシスコの独自保護機能である**アウトブレイク フィルタ™**。
- **ポリシー、ウイルス、およびアウトブレイク検疫**は、疑わしいメッセージを保存して管理者が評価するための安全な場所を提供します。
- 隔離されたスパムおよび陽性と疑わしいスパムへのエンドユーザアクセスを提供する、オンボックスまたはオフボックスの**スパム隔離**。
- **電子メール認証**。Cisco AsyncOS は、発信メールに対する DomainKeys および DomainKeys Identified Mail（DKIM）の署名の他に、着信メールに対する Sender Policy Framework（SPF）、Sender ID Framework（SIDF）、DKIM の検証など、さまざまな形式の電子メール認証をサポートします。
- Cisco **電子メール暗号化**。HIPAA、GLBA、および同様の規制要求に対応するために発信メールを暗号化できます。これを行うには、アプライアンスで暗号化ポリシーを設定し、ローカルキーサーバまたはホステッドキーサービスを使用してメッセージを暗号化します。
- アプライアンス上のすべての電子メールセキュリティサービスおよびアプリケーションを管理する、単一で包括的なダッシュボードである**電子メール セキュリティ マネージャ**。電子メール セキュリティ マネージャは、ユーザ グループに基づいて電子メール セキュリティを実施でき、インバウンドとアウトバウンドの独立したポリシーを使用して、Cisco レピュテーション フィルタ、アウトブレイク フィルタ、アンチスパム、アンチウイルス、および電子メール コンテンツ ポリシーを管理できます。
- **オンボックスのメッセージ トラッキング**。AsyncOS for Email には、アプライアンスが処理するメッセージのステータスの検索が容易にできる、オンボックスのメッセージトラッキング機能があります。
- 企業のすべての電子メール トラフィックを全体的に確認できる、すべてのインバウンドおよびアウトバウンドの電子メールに対する**メール フロー モニタ機能**。
- 送信者の IP アドレス、IP アドレス範囲、またはドメインに基づいた、インバウンドの送信者の**アクセス制御**。
- 広範な**メッセージおよびコンテンツ フィルタリング** テクノロジーを使用して、社内ポリシーを順守させ、企業のインフラストラクチャを出入りする特定のメッセージに作用させることができます。フィルタ ルールでは、メッセージまたは添付ファイルの内容、ネットワークに関する情報、メッセージ エンベロープ、メッセージ ヘッダー、またはメッセージ本文に基づいてメッセージを識別します。フィルタ アクションでは、メッセージをドロップ、バウンス、アーカイブ、ブラインド カーボン コピー、または変更したり、通知を生成したりできます。
- **セキュアな SMTP over Transport Layer Security 経由のメッセージの暗号化**により、企業のインフラストラクチャとその他の信頼できるホストとの間でやりとりされるメッセージが暗号化されるようなります。
- **Virtual Gateway™** テクノロジーにより、アプライアンスは、単一サーバ内で複数の電子メールゲートウェイとして機能できるため、さまざまな送信元またはキャンペーンの電子

メールを、それぞれ独立した IP アドレスを通して送信するように分配できます。これにより、1 つの IP アドレスに影響する配信可能量の問題が、他の IP アドレスに及ばないようにします。

- 複数のサービスによって提供される、電子メール メッセージ内の**悪意のある添付ファイルやリンクからの保護**。
- **データ損失防止**により、組織から出る情報の制御と監視を行います。

AsyncOS は、メッセージを受け入れて配信するために、RFC 2821 準拠の Simple Mail Transfer Protocol（SMTP）をサポートします。

レポート作成コマンド、モニタリング コマンド、およびコンフィギュレーション コマンドのほとんどは、HTTP 経由でも HTTPS 経由でも Web ベースの GUI から使用できます。さらに、セキュア シェル（SSH）または直接シリアル接続でアクセスするインタラクティブなコマンドライン インターフェイス（CLI）がシステムに用意されています。

また、複数のアプライアンスのレポート、トラッキング、および隔離管理を統合するようにセキュリティ管理アプライアンスを設定できます。

関連項目

- サポートされる言語 （20 ページ）

サポートされる言語

AsyncOS は次の言語のいずれかで GUI および CLI を表示できます。

- 英語
- フランス語
- スペイン語
- ドイツ語
- イタリア語
- 韓国語
- 日本語
- ポルトガル語（ブラジル）
- 中国語（繁体字および簡体字）
- ロシア語

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。