CHAPTER 1

Cisco Business Class Email 2.1 アドミニストレータ ガイド

この文書は、次の項で構成されています。

- 概要（1-1 ページ）
- Cisco Business Class Email アプリケーションに必要な TCP サービス（1-2 ページ）
- Cisco Business Class Email アプリケーションのダウンロード（1-2 ページ）
- サポートされるオペレーティング システム（1-2 ページ）
- ライセンシング バージョンおよびコンフィギュレーション モード（1-3 ページ）
- 管理者による BCE アプリケーションの構成時の設定（1-4 ページ）
- 関連資料（1-5 ページ）
- 詳細情報の入手先（1-6 ページ）
- Cisco Welcomes Your Comments（1-7 ページ）

概要

Cisco Business Class Email（BCE）プラグイン モバイル アプリケーションは、Apple iOS®、Google Android™、スマートフォン、タブレットで直接メッセージを暗号化および復号化する機能を提供します。

モバイル デバイスの急増によって、エンド ユーザは常にビジネス ネットワークおよび個人ネットワークに接続されています。企業のモバイル ワーカーは絶えず動き回りながら、接続された状態を保ち、仕事を処理する必要があります。さらに、モバイル ワーカーは、自由時間にも電子メールにアクセスし、返信します。

コンプライアンスおよび企業ポリシーのため、暗号化される重要な電子メール メッセージは増加しています。受信者は、ラップトップを使うときまで、電子メール メッセージへのアクセスを待っていられません。エンド ユーザは、ラップトップとモバイル デバイスの間にシームレスなエクスペリエンスを求めます。そのため多くの組織では、エンド ユーザが暗号化メッセージに使用するすべてのデバイス、コンピュータ、スマートフォンで一貫したエクスペリエンスを必要としています。この要求に応えるために、シスコは Business Class Email を市場投入します。これは、スマートフォンから暗号化された電子メールを送信するソリューションです。

Cisco Business Class Email により、従来の電子メール ツールのセキュリティが強化され、信頼性の高い制御が可能になります。これは、最も一般的な電子メール技術と、エンド ユーザの日々の電子メール作業に完全に統合されています。Business Class Email の 3 つのコンポーネントは、機密性、シームレスなエンド ユーザ認証、および高度なメッセージ制御です。

- **機密性**：Cisco Business Class Email ソリューションは、利用可能な最も信頼性の高い暗号化アルゴリズムを使用する強力な電子メール暗号化テクノロジーに基づいています。データを暗号化することで、ネットワーク上で転送されている間の機密性を確保できるだけでなく、最新の認証メカニズムを採用しているため、暗号キーに簡単かつ安全にアクセスすることができます。
- **高度なメッセージ制御**：メッセージの安全性が確保されるため、エンド ユーザは高度なメッセージ制御機能を利用できます。電子メールが暗号化されることにより、送信される情報の機密性が確保されるだけでなく、送信者は電子メールを失効させる、または回収することができ、また正確なメールの開封日時を確認できます。以下に具体的な機能について説明します。
  - **開封確認通知**：受信者がメッセージを開封すると（認証され、暗号キーを受け取ると）、開封されたことが確認され、開封確認通知が数秒以内に送信者に送信されます。
  - **メッセージの失効**：送信者は、メッセージに失効日を設定できます。失効日を過ぎると暗号キーが破棄され、そのメッセージの内容を表示できなくなります。
  - **転送/返信制御**：受信されたメッセージに対して許可する操作を細かく制御できます。転送、返信、全員に返信、の各オプションを有効または無効にすることができます（送信者の所属企業または管理者が許可している場合のみ）。

さらに、Business Class Email ソリューションでは、暗号化およびキー管理の複雑さを排除しているので、エンド ユーザは非暗号化電子メールと同じように簡単に安全なメッセージの送受信が可能です。

Cisco Business Class Email アプリケーションに必要な TCP サービス

Cisco BCE アプリケーションでは、HTTPS または HTTP に使用する空きポートが必要です。Cisco BCE アプリケーションでは通常、ポート 443 で HTTPS を使用するように設定され、これ以外に設定されることはほとんどありません。ただし、HTTPS、HTTP のいずれかを任意の空きポートで使用するようにアプリケーションを設定することは可能です。他の TCP プロトコルはすべて、Cisco BCE アプリケーションの動作に影響を与えることなく無効にできます。

Cisco Business Class Email アプリケーションのダウンロード

Cisco Business Class Email アプリケーション（*Cisco BCE*）は、Apple App Store および Google Play からスマートフォンまたはタブレットに直接ダウンロードできます。ユーザは、Apple App Store および Google Play から Cisco BCE アプリケーションをダウンロードしたら、「ライセンシング バージョンおよびコンフィギュレーション モード」セクション（1-3 ページ）に示すようにアカウントを作成する必要があります。

サポートされるオペレーティング システム

*Cisco 暗号化互換性マトリクス*には、Cisco BCE でサポートされているオペレーティング システムが掲載されており、以下の URL からアクセスできます。

http://www.cisco.com/en/US/docs/security/iea/Compatibility_Matrix/IEA_Compatibility_Matrix.pdf

ライセンシング バージョンおよびコンフィギュレーション モード

Cisco Business Class Email アプリケーションでは、導入できるライセンシング バージョンが 2 種類あり、そのバージョンによってアプリケーションのコンフィギュレーション モードが決まります。2 種類のライセンシング バージョンとコンフィギュレーション モードは次のとおりです。

- **Decrypt Only**：受信した安全な電子メール メッセージの復号化を行うことができ、転送および返信が可能です。
- **Decrypt and Encrypt**：安全な電子メール メッセージの暗号化と復号化を行うことができます。

注　**Flag** モードはサポートされていません。

Cisco BCE アプリケーションのデフォルトのコンフィギュレーション モードは Decrypt Only です。

ユーザは、Apple App Store および Google Play から Cisco BCE アプリケーションをダウンロードしたら、次のようにアカウントを作成する必要があります。

- 復号化のアカウントは、ネイティブの電子メール システムを使用して、安全な電子メールを開くだけで作成されます。
- 暗号化のアカウントを作成するには、ユーザは管理者から受信したコンフィギュレーション ファイルを、次のように適用する必要があります。

管理者は、エンド ユーザの電子メール アカウントに *BCE_Config_signed.xml* 添付ファイルを送信します。エンド ユーザはこのファイルを *securedoc.html* ファイルとして受信します。エンド ユーザが *securedoc.html* 添付ファイルを長押しすると、先ほどインストールしたアプリケーションがメッセージに添付された設定情報を検出し、更新された設定を適用します。

次の表は、各コンフィギュレーション モードでサポートされる機能を示しています。

機能	Decrypt Only	Decrypt and Encrypt
暗号化したメッセージを送信		X
暗号化された電子メールを開封	X	X
返信/すべてに返信/転送	X（注を参照）	X
電子メールのロックおよびロック解除	X	X
電子メールの有効期限	X	X
電子メールの診断（エラー/ログ レポート）	X	X
開封確認		X
エンベロープ設定		X
設定	X	X
送信済みアイテム	X	X
受信者の言語選択		X

注　返信オプションが使用できるかどうかは、受信メッセージの設定によって異なります。

管理者による BCE アプリケーションの構成時の設定

Cisco BCE プラグイン モバイル アプリケーションを展開するには、提供される設定テンプレートを使用して、各エンド ユーザのコンフィギュレーション ファイルを作成する必要があります。そして、署名済みコンフィギュレーション ファイルをエンド ユーザに送信します。

デフォルトのコンフィギュレーション モードである Decrypt Only では、署名済みコンフィギュレーション ファイルは必要ではありません。しかし、Decrypt and Encrypt コンフィギュレーション モードを有効にするには、エンド ユーザは署名済みコンフィギュレーション ファイルを受信して起動し、BCE アプリケーションを再設定する必要があります。

Cisco Registered Envelope Service（CRES）は、Cisco 暗号化テクノロジーをサポートするホスト サービスです。暗号化メッセージの受信者は、復号化キーを受信するサービスを使って自分自身を認証します。次の手順を実行するには、CRES のアカウント管理者である必要があります。

各エンド ユーザのコンフィギュレーション ファイルの作成

注　Cisco IronPort Encryption Appliance（IEA）をキー サーバとして使用する場合、開始する前に、CRES の管理者アカウントを作成してもらう必要があります。http://www.cisco.com/web/ironport/index.html にある Cisco カスタマー サポートにお問い合わせください。

各エンド ユーザの署名済みコンフィギュレーション ファイルを作成するには、次の手順を行います。

ステップ 1　CRES のアカウントで、https://res.cisco.com/admin にログインします。管理コンソールが表示されます。

ステップ 2　BCE コンフィギュレーション ファイルに署名し、それを展開するには、[Accounts] タブに移動し、BCE モバイル アプリケーションを有効化するのに使用するアカウントを選択します。次に、[BCE Config] タブに移動します。

ステップ 3　設定テンプレートで使用するトークンを選択します。トークンには次の 2 種類があります。

- [CRES]：キー サーバが CRES の場合に選択します。
  - [SecureCompose]：CRES トークンとしてこのオプションを選択しないでください。
  - [Token <Account number>]：CRES トークンとしてこのオプションを選択します。
- [IEA]：キー サーバが Cisco IronPort Encryption Appliance（IEA）の場合に選択します。
  - [Browse]：クリックして IEA トークン ファイルを探し、アップロードします。

ステップ 4　[Download Template] をクリックして、編集するテンプレート ファイルをダウンロードします。ファイル名は *BCE_Config.xml* です。

ステップ 5　コンフィギュレーション ファイルを編集します。

BCE_Config.xml ファイルには、特定の環境に合わせて編集する必要があるフィールドの詳細が含まれています。テキスト エディタでファイルを開き、コメントに記載されている手順に従って必要な変更を行います。

ステップ 6　[Browse] をクリックして、編集した *BCE_Config.xml* ファイルを探し、ファイルが見つかったら [Upload and Sign] をクリックします。

コンフィギュレーション ファイルに署名すると、その署名したバージョンが *BCE_Config_signed.xml* としてダウンロードされます。このファイルをローカル マシンに保存します。

エンド ユーザへのコンフィギュレーション ファイルの送信

ステップ 1　CRES の管理者として CRES にログインし、[Secure Compose] ページを使って暗号化電子メールを構成します。

ステップ 2　ローカル マシンを参照し、前の手順で作成した *BCE_Config_signed.xml* ファイルを見つけます。

ステップ 3　*BCE_Config_signed.xml* ファイルを暗号化された電子メールに添付します。エンド ユーザはこのファイルを *securedoc.html* ファイルとして受信します。

ステップ 4　BCE を有効にするエンド ユーザの電子メール アカウントに、暗号化された電子メールを送信します。

エンド ユーザが彼らのデバイスの電子メールで添付ファイルを開くと、自動的に Cisco BCE アプリケーションが設定されます。

注　送信者の電子メールは、*BCE_Config.xml* ファイルに署名したアカウント管理者と同じである必要があります。

注　メーリング リスト宛てに *BCE_Config_signed.xml* ファイルを送らないでください。CRES はメーリング リストに対応していません。

関連資料

BCE ユーザ ガイド、互換性マトリクス、およびリリース ノートは、http://www.cisco.com/c/en/us/support/security/email-encryption/products-user-guide-list.html にあります。

BCE を使用するには、キー サーバが必要です。これには、Cisco Registered Envelope Service（CRES）または Cisco IronPort Encryption Appliance（IEA）が使用できます。IEA をキー サーバとして使用する場合、開始する前に、CRES の管理者アカウントを作成してもらう必要があります。管理者による BCE アプリケーションの構成時の設定（1-4 ページ）を参照してください。

Cisco IEA の設定方法については、次のマニュアルを参照してください。

- *Cisco Registered Envelope Service 4.4 Account Administrator Guide*。このマニュアルでは、Cisco 暗号化テクノロジーをサポートする Cisco Registered Envelope Service（CRES）について説明しています。また、署名済みコンフィギュレーション ファイルの送信による、Cisco Business Class Email プラグインまたはモバイル アプリケーションの展開に関する情報が含まれています。このマニュアルは、CRES ソフトウェア内のリンクからアクセスできます。

- *IronPort Encryption Appliance Installation Guide*。このマニュアルでは、電子メール暗号化のインストールおよび設定手順について説明しています。プラグインの設定と連動するように暗号化アプライアンスを設定する方法を理解する上で役立ちます。

詳細情報の入手先

シスコでは、Cisco Business Class Email およびシスコのセキュリティ製品の詳細に関して、次のリソースを提供しています。

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 エンド ユーザと情報を共有したりできます。

シスコ サポート コミュニティには次の URL からアクセスできます。

https://supportforums.cisco.com

Cisco カスタマー サポート

You can request our support by phone, email, or online 24 hours a day, 7 days a week.

注　利用可能なサポートのレベルは、お客様のサービス レベル契約によって異なります。Cisco カスタマー サポートのサービス レベル契約の詳細については、サポート ポータルをご覧ください。サポート レベルの詳細については、この Web サイトを確認してください。

カスタマー サポートの営業時間外に緊急のサポートが必要な重大な問題をレポートするには、次のいずれかの方法を使用してシスコにお問い合わせください。

米国フリー ダイヤル：1 (877) 646-4766

サポート サイト：http://www.cisco.com/web/ironport/index.html

If you purchased support through a reseller or another supplier, please contact that supplier directly with your product support issues.

サード パーティ コントリビュータ

Cisco BCE に含まれるソフトウェアには、Apple iOS および Google Android のソフトウェア ライセンス契約の条項、通知、条件の下で配布されるものがあります。これらのライセンス契約の詳細については、次の URL を参照してください。

- http://www.cisco.com/web/mobile/terms.html
- http://www.cisco.com/c/dam/en/us/td/docs/security/iea/bce2-1/release_notes/Cisco_BCE_2-1_Android_Open_Source_Documentation.pdf
- http://www.cisco.com/c/dam/en/us/td/docs/security/iea/bce2-1/release_notes/Cisco_BCE_2-1_iOS_Open_Source_Documentation.pdf

Cisco Welcomes Your Comments

Cisco Content Security 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。Your comments and suggestions are always welcome. You can send comments to the following email address:

contentsecuritydocs@cisco.com