CHAPTER 1

Cisco Business Class Email for iOS の設定と使用

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、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。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

概要

Cisco Business Class Email（BCE）モバイル アプリケーションは、暗号化された電子メール メッセージの送受信を Apple iOS スマートフォン デバイス上で直接行う機能を提供します。Cisco BCE モバイル アプリケーションのコンフィギュレーション モードに応じて、次のタスクを実行できます。

- Cisco BCE を使用して、暗号化された電子メールをスマートフォン上で開く。
- Cisco BCE を使用して、暗号化した電子メールをスマートフォンから送信する。
- Cisco BCE を使用して、スマートフォンから送信した安全な電子メールを管理する。
- Cisco BCE を使用して、暗号化してスマートフォンから送信した電子メールをロックまたはロック解除する。
- Cisco BCE を使用して、暗号化してスマートフォンから送信した電子メールの有効期限を設定または変更する。
- Cisco BCE を使用して、暗号化してスマートフォンから送信した電子メールに対する開封確認を受信する。
- 暗号化した電子メールのオプションをスマートフォンで確認または変更する。

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 3 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。Cisco BCE アプリケーションでデフォルトのコンフィギュレーション モードは Decrypt Only であり、このモードの Cisco BCE は Apple App Store からダウンロードできます。

他のバージョンおよびコンフィギュレーション モードで使用できるようにするには、更新済みの添付ファイルを管理者から受け取り、それを使用してスマートフォン デバイスを設定します。

3 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が可能です。
- **Decrypt and Flag**：安全な電子メール メッセージの復号化とフラグ設定が可能です。フラグのオプションを使用すると、暗号化する電子メールにフラグを設定できます。このフラグを設定した電子メールは、Cisco IronPort 暗号化アプライアンスまたは電子メール セキュリティ アプライアンスで暗号化されたうえで、ネットワークから送信されます。フラグが設定されたメッセージを検出してサーバで復号化できるようサーバの設定を行う必要があります。
- **Decrypt and Encrypt**：安全な電子メール メッセージの暗号化と復号化が可能です。

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

Cisco Business Class Email アプリケーションのダウンロードおよびインストール

Cisco BCE アプリケーションをインストールするには、Apple iOS デバイスで **Apple App Store** にアクセスし、**Cisco BCE** アプリケーションを検索します。アプリケーションをダウンロードし、目的のデバイス上でインストールを開始します。「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」（P.1-4）を参照してください。

Cisco Business Class Email for iOS の起動

iOS に Cisco BCE アプリケーションを正常にインストールすると、新しく *Cisco BCE* アプリケーションのアイコンが表示されます。このアプリケーションを起動するには、iOS ホーム画面にある **Cisco BCE** のアイコンをタップします。このアプリケーションを起動すると、暗号化された電子メールの送受信に必要なメニューがデバイスに追加されます。

アプリケーションのランディング画面

Cisco BCE のアイコンをタップするとアプリケーションのランディング画面が開きます。この画面のアイコンの中には、コンフィギュレーション モードによってはグレー表示となり、利用できなくなるものがあります。「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」（P.1-4）を参照してください。

次の表は、アプリケーションのランディング画面にあるオプションをまとめたものです。

オプション	説明
Inbox	暗号化された電子メールをこのデバイス上で開いた電子メール アカウントのリストが表示されます。個々の電子メール アカウントまたは [All Email Accounts] をタップすると、選択したアカウントで復号化して開いた電子メールのリストが表示されます。 暗号化されたメッセージを開いた電子メール アドレスが 1 つのみの場合は、電子メール アカウントのリストは表示されません。
Sent Items	暗号化した電子メールをデバイスから送信した電子メール アカウントをリスト表示します。個々の電子メール アカウントまたは [All Email Accounts] をタップすると、選択したアカウントで暗号化して送信した電子メールのリストが表示されます。 暗号化したメッセージを送信した電子メール アドレスが 1 つのみの場合は、電子メール アカウントのリストは表示されません。
Secure Compose	安全なメッセージを作成するための画面を開きます。「暗号化した電子メールの送信」（P.1-14）を参照してください。
Settings	アプリケーションの一般的な設定を行う設定画面を開きます。「Cisco Business Class Email の設定」（P.1-6）を参照してください。
About	Cisco BCE アプリケーションのバージョン情報を表示します。

Cisco Business Class Email の設定ファイルの起動

電子メール アカウントで添付ファイルの *securedoc.html* を開く前に、Cisco BCE アプリケーションを開いて実行状態にしておく必要があります。

BCE アプリケーションを有効にして設定するには、次の作業を実行します。

ステップ 1　Cisco BCE アプリケーションを開きます。

ステップ 2　iPhone デバイス上で電子メールの *securedoc.html* 添付ファイルを開きます。これにより、iPhone デバイスにインストールされている Cisco BCE アプリケーションが自動的に設定されます。

（注）　暗号化された電子メールが受信トレイにない場合は、スパム メールまたは迷惑メールのフォルダを調べます。

- Cisco CRES 登録アカウントがない場合は、アカウントの登録を求めるプロンプトが表示されます。
  - [New User Registration] フォームの所要事項を入力して [Register] をクリックします。受信トレイにアカウントのアクティベーション電子メールが届いていないか確認します。
  - アカウントのアクティベーション電子メールで [Click here to activate this account] リンクをクリックします。アカウントのアクティベーションが確認され、登録した電子メール アドレスに暗号化されて送信された電子メールを表示できるようになったことを通知するメッセージが表示されます。
  - HTML ファイルが添付された元の電子メールに戻ります。添付ファイルをタップしたままにします。画面の表示に応じて、[Open in Cisco BCE] をタップするか、[Open In...]、[Open in Cisco BCE] の順にタップします。

ステップ 3　プロンプトが表示されたら設定を確定し、この手順を完了します。

Cisco Business Class Email の設定

[Settings] 画面で、電子メールの一般的なセキュリティ オプションを設定できます。これらの設定にアクセスするには、[Cisco BCE]、[Settings] の順にタップします。使用しているコンフィギュレーション モードによっては、設定で使用できないオプションがあります。「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」（P.1-4）を参照してください。

[Settings] 画面で使用できる電子メールのセキュリティ オプションは次のとおりです。

オプション	説明
Name	Cisco BCE 登録アカウントで使用するために送信された名前。
Email	Cisco BCE 登録アカウントで使用するために送信された電子メール アドレス。
Cache Password	デフォルトでは、このオプションは有効になっていて、暗号化パスワードがキャッシュされます。キャッシュをクリアした場合は、次回のログイン時にパスワードをもう一度入力する必要があります。
Cache Duration (mins)	キャッシュが保持される期間を分の単位で入力します。デフォルトでは 1,440 分です。

オプション	説明
Clear Cache	タップするとキャッシュがただちにクリアされます。デバイスをシャットダウンまたは再起動すると、キャッシュは自動的にクリアされます。
Default Expiration (mins)	デフォルトの有効期限を分の単位で入力します。このオプションは、暗号化された電子メール メッセージを有効な状態で維持できる期間を指定します。有効期限の分数が経過すると、そのメッセージは期限切れとなり、以降は受信者がそのメッセージを開くことはできなくなります。「電子メールの有効期限の設定」（P.1-16）を参照してください。
Request Read Receipt	デフォルトでは、このオプションは有効になっていて、受信者が暗号化されたメッセージを開くと、デフォルトの開封確認通知を送信者に送信するように要求されます。「開封確認の受信」（P.1-17）を参照してください。
Allow Reply	デフォルトでは、このオプションは有効になっていて、返信の対象となる暗号化されていたメッセージは自動的に暗号化されます。「電子メールへの返信、全員への返信、および転送」（P.1-14）を参照してください。
Allow Reply All	デフォルトでは、このオプションは有効になっていて、暗号化されていたメッセージのすべての受信者に返信するときに、この暗号化されていたメッセージが自動的に暗号化されます。
Allow Forward	デフォルトでは、このオプションは有効になっていて、転送の対象となる暗号化されていたメッセージは自動的に暗号化されます。
Message Sensitivity	デフォルトではメッセージの秘密度は [High] に設定されています。このドロップダウン リストでは、ほかに [Medium] と [Low] を選択できます。「メッセージの秘密度」（P.1-19）を参照してください。
Diagnostic Log Level	ログ レベルを定義することにより、アプリケーションで維持するログのタイプを設定します。「ログ レベルの設定」（P.1-21）を参照してください。
Cache Envelope Size (MB)	ダウンロードした安全なエンベロープは、初めて開いた後、デバイス上でキャッシュされます。デフォルトでは、この値は 6 MB です。
Save Draft	デフォルトでは、このオプションは無効になっています。[Save Draft] を有効にすると、[Secure Compose] を指定して入力したデータは、メッセージを送信するまで保持されます。このデータはキャッシュに保存され、デバイスが紛失や盗難にあった場合は、このキャッシュからデータを回復できます。

コンフィギュレーション モードごとの使用可能な電子メール暗号化オプション

Cisco BCE 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 3 種類あり、そのバージョンにより、使用できる電子メール暗号化オプションと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。それぞれのコンフィギュレーション モードの導入の詳細については、「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」（P.1-4）を参照してください。暗号化され

た電子メールを開くオプションは、3 種類のコンフィギュレーション モードのすべてで使用できます。

3 種類のコンフィギュレーション モードそれぞれの電子メール暗号化オプションについて、次の各項で説明します。

（注）　iPhone では、Google Gmail を初めとして数多くのメール アプリケーションを使用できますが、現時点の Cisco BCE は、電話に付属しているネイティブのメール アプリケーションとのみ統合されています。

Decrypt Only モードで使用できるオプション

Cisco BCE アプリケーションでデフォルトのコンフィギュレーション モードは Decrypt Only であり、このバージョンの Cisco BCE は Apple App Store からダウンロードできます。Decrypt Only モードでは、暗号化されたメッセージを受信して開くことはできますが、暗号化したメッセージを送信することはできません。

暗号化された電子メールを開く - 新しいメッセージ

Cisco BCE アプリケーションでは、暗号化された電子メール メッセージを iOS 電子メール クライアントで直接開くことができます。

- Cisco BCE は、メッセージが暗号化されていることを検出し、そのメッセージを復号化するために、Cisco BCE 登録アカウントのクレデンシャルの入力を要求します。
- 正しいユーザ名とパスワードを入力すると、Cisco BCE によってエンベロープがダウンロードされ、復号化されたメッセージがスマートフォン デバイス上に表示されます。

暗号化された新しいメッセージを開くには、次の作業を実行します。

ステップ 1　iOS デバイス上で電子メール クライアントを起動します。

ステップ 2　暗号化された電子メールを電子メール リストのビューでタップして開きます。

（注）　暗号化された電子メールが受信トレイにない場合は、スパム メールまたは迷惑メールのフォルダを調べます。

ステップ 3　電子メールで HTML 添付ファイルを参照します。メニュー オプションが表示されるまで、HTML 添付ファイルをタップしたままにします。

ステップ 4　画面の表示に応じて、[Open in Cisco BCE] をタップするか、[Open In...]、[Open in Cisco BCE] の順にタップします。ログイン画面が表示されます。

- Cisco CRES 登録アカウントがない場合は、アカウントの登録を求めるプロンプトが表示されます。
  - [New User Registration] フォームの所要事項を入力して [Register] をクリックします。受信トレイにアカウントのアクティベーション電子メールが届いていないか確認します。
  - アカウントのアクティベーション電子メールで [Click here to activate this account] リンクをクリックします。アカウントのアクティベーションが確認され、登録した電子メール アドレスに暗号化されて送信された電子メールを表示できるようになったことを通知するメッセージが表示されます。
  - HTML ファイルが添付された元の電子メールに戻ります。添付ファイルをタップしたままにします。画面の表示に応じて、[Open in Cisco BCE] をタップするか、[Open In...]、[Open in Cisco BCE] の順にタップします。
- 複数の電子メール アドレスが存在する場合は、次の作業を実行します。
  - ドロップダウン リストで該当の電子メール アドレスを選択し、Cisco BCE 登録アカウントのパスワードを入力します。
- これより前の段階で、暗号化された電子メールを開くために電子メール アドレスとパスワードを入力していた場合は、その情報がキャッシュされているのでログイン画面は表示されません。

ステップ 5　[Login] をタップします。安全な電子メールが復号化され、そのメッセージが表示されます。

（注）　iPhone デバイスにダウンロードできる添付ファイルのデフォルトの最大サイズは、使用するメール サーバとデバイスのハードウェアに応じて異なります。

暗号化された電子メールを開く - すでに開いたことがあるメッセージ

メッセージを開くと、その電子メールは Cisco BCE アプリケーションの受信トレイに追加されるので、Cisco BCE の受信トレイから再び開くことができます。

暗号化されたメッセージを再び開くには、次の作業を実行します。

ステップ 1　[Cisco BCE]、[Inbox] の順にタップして、受信トレイの電子メール アカウント画面を開きます。

ステップ 2　[All Email Accounts] または特定の電子メール アドレスをタップします。選択したアカウントの復号化された電子メールのリストが表示されます。

ステップ 3　電子メールのリストで、暗号化された電子メールをタップして開きます。

- 所要の電子メール アドレスとパスワードがキャッシュされていない場合は、ログイン画面が表示されます。電子メール アドレスを選択し、Cisco BCE 登録アカウントのパスワードを入力して [Login] をタップします。
- 所要の電子メール アドレスとパスワードがキャッシュされている場合、ログイン画面は表示されません。

復号化したメッセージが表示されます。

Decrypt and Flag モードで使用できるオプション

Decrypt and Flag モードでは、安全な電子メール メッセージの復号化とフラグ設定が可能です。フラグのオプションを使用すると、暗号化する電子メールにフラグを設定できます。このフラグを設定した電子メールは、Cisco IronPort 暗号化アプライアンスまたは電子メール セキュリティ アプライアンスで暗号化されたうえで、ネットワークから送信されます。サーバでは、フラグが設定されたメッセージを検出して、サーバで復号化できる設定が必要です。

Decrypt and Flag モードを使用できるようにするには、更新済みの添付ファイルを管理者から受け取り、それを使用してスマートフォン デバイスを設定します。更新された添付ファイルを受け取り、使用しているスマートフォンの電子メール アカウントでそのファイルを起動すると、ここで説明しているオプションを使用できるようになります。

暗号化された電子メールを開く - 新しいメッセージ

Cisco BCE アプリケーションでは、暗号化された電子メール メッセージを iOS 電子メール クライアントで直接開くことができます。

- Cisco BCE は、メッセージが暗号化されていることを検出し、そのメッセージを復号化するために、Cisco BCE 登録アカウントのクレデンシャルの入力を要求します。
- 正しいユーザ名とパスワードを入力すると、Cisco BCE によってエンベロープがダウンロードされ、復号化されたメッセージがスマートフォン デバイス上に表示されます。

暗号化された新しいメッセージを開くには、次の作業を実行します。

ステップ 1　iOS デバイス上で電子メール クライアントを起動します。

ステップ 2　暗号化された電子メールを電子メール リストのビューでタップして開きます。

（注）　暗号化された電子メールが受信トレイにない場合は、スパム メールまたは迷惑メールのフォルダを調べます。

ステップ 3　電子メールで HTML 添付ファイルを参照します。メニュー オプションが表示されるまで、HTML 添付ファイルをタップしたままにします。

ステップ 4　画面の表示に応じて、[Open in Cisco BCE] をタップするか、[Open In...]、[Open in Cisco BCE] の順にタップします。ログイン画面が表示されます。

- Cisco CRES 登録アカウントがない場合は、アカウントの登録を求めるプロンプトが表示されます。
  - [New User Registration] フォームの所要事項を入力して [Register] をクリックします。受信トレイにアカウントのアクティベーション電子メールが届いていないか確認します。

  - アカウントのアクティベーション電子メールで [Click here to activate this account] リンクをクリックします。アカウントのアクティベーションが確認され、登録した電子メール アドレスに暗号化されて送信された電子メールを表示できるようになったことを通知するメッセージが表示されます。
  - HTML ファイルが添付された元の電子メールに戻ります。添付ファイルをタップしたままにします。画面の表示に応じて、[Open in Cisco BCE] をタップするか、[Open In...]、[Open in Cisco BCE] の順にタップします。
- 複数の電子メール アドレスが存在する場合は、次の作業を実行します。
  - ドロップダウン リストで該当の電子メール アドレスを選択し、Cisco BCE 登録アカウントのパスワードを入力します。
- これより前の段階で、暗号化された電子メールを開くために電子メール アドレスとパスワードを入力していた場合は、その情報がキャッシュされているのでログイン画面は表示されません。

ステップ 5　[Login] をタップします。安全な電子メールが復号化され、そのメッセージが表示されます。

（注）　iPhone デバイスにダウンロードできる添付ファイルのデフォルトの最大サイズは、使用するメール サーバとデバイスのハードウェアに応じて異なります。

暗号化された電子メールを開く - すでに開いたことがあるメッセージ

メッセージを開くと、その電子メールは Cisco BCE アプリケーションの受信トレイに追加されるので、Cisco BCE の受信トレイから再び開くことができます。

暗号化されたメッセージを再び開くには、次の作業を実行します。

ステップ 1　[Cisco BCE]、[Inbox] の順にタップして、受信トレイの電子メール アカウント画面を開きます。

ステップ 2　[All Email Accounts] または特定の電子メール アドレスをタップします。選択したアカウントの復号化された電子メールのリストが表示されます。

ステップ 3　電子メールのリストで、暗号化された電子メールをタップして開きます。

- 所要の電子メール アドレスとパスワードがキャッシュされていない場合は、ログイン画面が表示されます。電子メール アドレスを選択し、Cisco BCE 登録アカウントのパスワードを入力して [Login] をタップします。
- 所要の電子メール アドレスとパスワードがキャッシュされている場合、ログイン画面は表示されません。

復号化したメッセージが表示されます。

暗号化する電子メールのフラグ設定

フラグの暗号化オプションを使用すると、暗号化する電子メールにフラグを設定できます。このフラグを設定した電子メールは、Cisco IronPort 暗号化アプライアンス（IEA）または電子メール セキュリティ アプライアンス（ESA）で暗号化されたうえで、ネットワークから送信されます。

暗号化する電子メールにフラグを設定するには、次の作業を実行します。

ステップ 1　[Cisco BCE]、[Secure Compose] の順にタップして [Secure Compose] 画面を開きます。

ステップ 2　デフォルトでは、登録した電子メール アカウントの電子メール アドレスが [From] フィールドに追加されます。

次の各フィールドに適切に入力します。

- Address（To、CC、および BCC）
- Subject

ステップ 3　メッセージのテキストを入力します。

ステップ 4　安全なメッセージを作成するとき、必要に応じ、送信するメッセージのメッセージ設定を [Envelope Settings] 画面で変更できます。[Envelope Settings] にアクセスするには、画面右上の [Options] アイコンをタップし、[Envelope Settings] をタップします。

（注）　iPhone でメッセージを作成する場合、添付ファイルを追加することはできません。

ステップ 5　メッセージが完成したところで、画面右上の [Options] アイコンをタップし、[Send Secure] をタップします。

Decrypt and Encrypt モードで使用できるオプション

Decrypt and Encrypt モードでは、安全な電子メール メッセージの暗号化と復号化が可能です。Decrypt and Encrypt モードを使用できるようにするには、更新済みの添付ファイルを管理者から受け取り、それを使用してスマートフォン デバイスを設定します。更新された添付ファイルを受け取り、使用しているスマートフォンの電子メール アカウントでそのファイルを起動すると、ここで説明しているオプションを使用できるようになります。

暗号化された電子メールを開く - 新しいメッセージ

Cisco BCE アプリケーションでは、暗号化された電子メール メッセージを iOS 電子メール クライアントで直接開くことができます。

- Cisco BCE は、メッセージが暗号化されていることを検出し、そのメッセージを復号化するために、Cisco BCE 登録アカウントのクレデンシャルの入力を要求します。
- 正しいユーザ名とパスワードを入力すると、Cisco BCE によってエンベロープがダウンロードされ、復号化されたメッセージがスマートフォン デバイス上に表示されます。

暗号化された新しいメッセージを開くには、次の作業を実行します。

ステップ 1　iOS デバイス上で電子メール クライアントを起動します。

ステップ 2　暗号化された電子メールを電子メール リストのビューでタップして開きます。

（注）　暗号化された電子メールが受信トレイにない場合は、スパム メールまたは迷惑メールのフォルダを調べます。

ステップ 3　電子メールで HTML 添付ファイルを参照します。メニュー オプションが表示されるまで、HTML 添付ファイルをタップしたままにします。

ステップ 4　画面の表示に応じて、[Open in Cisco BCE] をタップするか、[Open In...]、[Open in Cisco BCE] の順にタップします。ログイン画面が表示されます。

- Cisco CRES 登録アカウントがない場合は、アカウントの登録を求めるプロンプトが表示されます。
  - [New User Registration] フォームの所要事項を入力して [Register] をクリックします。受信トレイにアカウントのアクティベーション電子メールが届いていないか確認します。
  - アカウントのアクティベーション電子メールで [Click here to activate this account] リンクをクリックします。アカウントのアクティベーションが確認され、登録した電子メール アドレスに暗号化されて送信された電子メールを表示できるようになったことを通知するメッセージが表示されます。
  - HTML ファイルが添付された元の電子メールに戻ります。添付ファイルをタップしたままにします。画面の表示に応じて、[Open in Cisco BCE] をタップするか、[Open In...]、[Open in Cisco BCE] の順にタップします。
- 複数の電子メール アドレスが存在する場合は、次の作業を実行します。
  - ドロップダウン リストで該当の電子メール アドレスを選択し、Cisco BCE 登録アカウントのパスワードを入力します。
- これより前の段階で、暗号化された電子メールを開くために電子メール アドレスとパスワードを入力していた場合は、その情報がキャッシュされているのでログイン画面は表示されません。

ステップ 5　[Login] をタップします。安全な電子メールが復号化され、そのメッセージが表示されます。

（注）　iPhone デバイスにダウンロードできる添付ファイルのデフォルトの最大サイズは、使用するメール サーバとデバイスのハードウェアに応じて異なります。

暗号化された電子メールを開く - すでに開いたことがあるメッセージ

メッセージを開くと、その電子メールは Cisco BCE アプリケーションの受信トレイに追加されるので、Cisco BCE の受信トレイから再び開くことができます。

暗号化されたメッセージを再び開くには、次の作業を実行します。

ステップ 1　[Cisco BCE]、[Inbox] の順にタップして、受信トレイの電子メール アカウント画面を開きます。

ステップ 2　[All Email Accounts] または特定の電子メール アドレスをタップします。選択したアカウントの復号化された電子メールのリストが表示されます。

ステップ 3　電子メールのリストで、暗号化された電子メールをタップして開きます。

- 所要の電子メール アドレスとパスワードがキャッシュされていない場合は、ログイン画面が表示されます。電子メール アドレスを選択し、Cisco BCE 登録アカウントのパスワードを入力して [Login] をタップします。
- 所要の電子メール アドレスとパスワードがキャッシュされている場合、ログイン画面は表示されません。

復号化したメッセージが表示されます。

暗号化した電子メールの送信

暗号化したメッセージを送信すると、そのメッセージはすべての受信者に対して暗号化されます。

暗号化した電子メールを送信するには、次の作業を実行します。

ステップ 1　[Cisco BCE]、[Secure Compose] の順にタップして [Secure Compose] 画面を開きます。

ステップ 2　デフォルトでは、登録した電子メール アカウントの電子メール アドレスが [From] フィールドに追加されます。

次の各フィールドに適切に入力します。

- Address（To、CC、および BCC）
- Subject

ステップ 3　メッセージのテキストを入力します。

ステップ 4　安全なメッセージを作成するとき、必要に応じ、送信するメッセージのメッセージ設定を [Envelope Settings] 画面で変更できます。[Envelope Settings] にアクセスするには、画面右上の [Options] アイコンをタップし、[Envelope Settings] をタップします。

（注）　iPhone でメッセージを作成する場合、添付ファイルを追加することはできません。

ステップ 5　メッセージが完成したところで、画面右上の [Options] アイコンをタップし、[Send Secure] をタップします。電子メールが暗号化され、送信する電子メールに HTML として添付されて送信されます。

電子メールへの返信、全員への返信、および転送

返信または転送の対象となる暗号化された電子メールは、デフォルトで自動的に暗号化されます。安全なメッセージでは、次の各操作を任意の組み合わせで許可できます（どれも許可しないことも可能です）。

- 安全な返信
- 全員への安全な返信
- 安全な転送

暗号化された電子メールに対して [Settings] 画面で定義された権限に基づき、該当のメニュー オプションがスマートフォン デバイスに追加されます。たとえば、暗号化された電子メールに転送のみを許可する権限が設定されている場合は、[Forward] メニュー オプションのみが使用できるようになります。「Cisco Business Class Email の設定」（P.1-6）を参照してください。

（注）　安全な返信、全員への安全な返信、または安全な転送で応答するには、それに使用するスマートフォン デバイスで、暗号化したメッセージを送信できる必要があります。Decrypt Only モードでは、これらのオプションは使用できません。

暗号化された電子メールへの返信またはその転送をするには、次の作業を実行します。

ステップ 1　「暗号化された電子メールを開く - すでに開いたことがあるメッセージ」（P.1-13）または「暗号化した電子メールの送信」（P.1-14）の手順を実行します。

ステップ 2　画面右上の [Options] アイコンをタップします。[Secure Reply]、[Secure Reply All]、または [Secure Forward] をタップします。

新しいメッセージを作成する画面に、元のメッセージが追加されます。応答を追加し、元のメッセージの内容を編集します。

ステップ 3　[Send] をタップします。

暗号化した電子メールのロックまたはロック解除

暗号化した電子メールを送信した後、その電子メールをロックして受信者が電子メールを開くことができないようにすることが可能です。誤った受信者に電子メールを送信した場合や電子メールの送信後に情報の更新が発生した場合などに、このオプションを使用できます。

（注）　これらの機能をサポートしていないキー サーバでは、[Lock/Unlock Email Messages] メニュー オプションと [Edit Lock Reason] メニュー オプションは使用できません。

暗号化した電子メールをロックするには、次の作業を実行します。

ステップ 1　[Cisco BCE]、[Sent Items] の順にタップします。暗号化した電子メールを現在のデバイスから送信した電子メール アカウントのリストが [Cisco BCE Mailbox] 画面に表示されます。暗号化した電子メールを送信した電子メール アカウントが 1 つのみの場合、この画面は表示されません。

ステップ 2　[All Email Accounts] または特定の電子メール アドレスをタップします。選択したアカウントから送信された復号化した電子メールのリストが表示されます。

ステップ 3　暗号化した電子メールのうち、ロックするものをこの電子メールのリストから選択します。選択した電子メールをタップしてメニュー オプションを表示します。

ステップ 4　[Lock] をタップします。キャッシュが期限切れになっている場合は、ログイン画面が表示されます。

ステップ 5　必要に応じて、メッセージをロックする理由を入力します。受信者がエンベロープを表示すると、このロックした理由が示されます。Cisco BCE 登録アカウントの電子メール アドレスとパスワードの入力を求められることがあります。

ステップ 6　[Lock] をタップします。指定の電子メール メッセージを正常にロックしたことが確認されます。ロックした電子メールには、錠が付いたエンベロープのアイコンが表示されます。

（注）　電子メールをロックした後、ロックした電子メールを選択することでロックの理由を編集できます。選択した電子メールをタップしてメニュー オプションを表示し、[Edit Lock Reason] をタップします。

暗号化した電子メールのロックを解除するには、次の作業を実行します。

ステップ 1　[Cisco BCE]、[Sent Items] の順にタップします。暗号化した電子メールを現在のデバイスから送信した電子メール アカウントのリストが [Cisco BCE Mailbox] 画面に表示されます。暗号化した電子メールを送信した電子メール アカウントが 1 つのみの場合、この画面は表示されません。

ステップ 2　[All Email Accounts] または特定の電子メール アドレスをタップします。選択したアカウントから送信された復号化した電子メールのリストが表示されます。

ステップ 3　暗号化した電子メールのうち、ロックを解除するものをこの電子メールのリストから選択します。選択した電子メールをタップしてメニュー オプションを表示します。

ステップ 4　[Unlock] をタップします。

電子メールの有効期限の設定

暗号化した電子メールに有効期限を設定できます。暗号化した電子メールが有効性を維持できる期間の指定が可能です。この期限が経過するとメッセージは期限切れとなり、受信者がそのメッセージを開くことはできなくなります。有効期限を設定する際に、次の各オプションを使用できます。

- すべての安全な電子メールにデフォルトの有効期限を設定できます。
- 特定の電子メールに、デフォルトの有効期限とは異なる有効期限を設定できます。
- 電子メールの送信後に有効期限を変更できます。

デフォルト設定

デフォルトの有効期限を設定するには、次の作業を実行します。

ステップ 1　[Cisco BCE]、[Settings] の順にタップして [Settings] 画面を開きます。

ステップ 2　[Default expiration (mins)] で、電子メールが期限切れになるまでの期間を分数で指定します。

ステップ 3　終了して変更を保存するには [Done] をタップします。

メッセージごとの設定

特定の電子メールに有効期限を設定するには、次の作業を実行します。

ステップ 1　[Cisco BCE]、[Secure Compose] の順にタップして [Secure Compose] 画面を開きます。

ステップ 2　暗号化したメッセージを送信する登録電子メール アカウントの名前と電子メール アドレスを入力します。[Apply] をタップします。

ステップ 3　メッセージの作成を完了したところで画面右上の [Options] アイコンをタップし、続いて [Envelope Settings] をタップします。

ステップ 4　[Set Expiry] をタップします。[New Expiry Date] 画面が表示されます。

ステップ 5　電子メールが期限切れになる日時を選択します。

ステップ 6　[Set Expiry] をタップして変更を保存します。

ステップ 7　[Done] をタップして [Envelope Settings] 画面を終了し、元の安全な電子メールに戻ります。

ステップ 8　画面右上の [Send] をタップしてメニュー オプションを表示し、[Send Secure] をタップします。

ステップ 9　電子メールが暗号化され、HTML 添付ファイルで表示されます。[Send] をタップします。

メッセージ送信後の操作

電子メールを送信した後で、それに有効期限を設定するには、次の作業を実行します。

ステップ 1　[Cisco BCE]、[Sent Items] の順にタップします。暗号化した電子メールを現在のデバイスから送信した電子メール アカウントのリストが [Cisco BCE Mailbox] 画面に表示されます。暗号化した電子メールを送信した電子メール アカウントが 1 つのみの場合、この画面は表示されません。

ステップ 2　[All Email Accounts] または特定の電子メール アドレスをタップします。選択したアカウントから送信された復号化した電子メールのリストが表示されます。

ステップ 3　有効期限を設定する暗号化した電子メールを、この電子メールのリストから選択します。選択した電子メールをタップしてメニュー オプションを表示します。すでにメッセージに有効期限が設定されている場合は、現在の有効期限が表示されます。

ステップ 4　[Set Expiry] をタップします。[New Expiry Date] 画面が表示されます。

ステップ 5　電子メールが期限切れになる日時を選択します。

ステップ 6　[Set Expiry] をタップして変更を保存します。メッセージが有効期限切れになる日時を確定したことを示す通知が表示されます。

有効期限のクリア

電子メールを送信した後で、その有効期限をクリアするには、次の作業を実行します。

ステップ 1　[Cisco BCE]、[Sent Items] の順にタップします。暗号化した電子メールを現在のデバイスから送信した電子メール アカウントのリストが [Cisco BCE Mailbox] 画面に表示されます。暗号化した電子メールを送信した電子メール アカウントが 1 つのみの場合、この画面は表示されません。

ステップ 2　[All Email Accounts] または特定の電子メール アドレスをタップします。選択したアカウントから送信された復号化した電子メールのリストが表示されます。

ステップ 3　有効期限をクリアする暗号化した電子メールを、この電子メールのリストから選択します。選択した電子メールをタップしてメニュー オプションを表示します。

ステップ 4　[Set Expiry] をタップします。[New Expiry Date] 画面が開き、現在の有効期限が表示されます。

ステップ 5　[Clear Expiry] をタップします。

開封確認の受信

送信した電子メールを受信者が開いたときに、スマートフォン上でその受信者に対して開封確認の送信を直接要求できます。

デフォルト設定

開封確認を要求（デフォルト設定）するには、次の作業を実行します。

ステップ 1　[Cisco BCE]、[Settings] の順にタップして [Settings] 画面を開きます。

ステップ 2　[Request Read Receipt] をタップします。これはデフォルトで有効になっています。

ステップ 3　終了して変更を保存するには [Done] をタップします。

メッセージごとの設定

このオプションが該当するのは、デフォルト設定を有効にせず、個別の電子メール単位で開封確認を要求する場合です。

特定の電子メールの開封確認を要求するには、次の作業を実行します。

ステップ 1　[Cisco BCE]、[Secure Compose] の順にタップして [Secure Compose] 画面を開きます。

ステップ 2　暗号化したメッセージを送信する登録電子メール アカウントの名前と電子メール アドレスを入力します。[Apply] をタップします。

ステップ 3　メッセージの作成を完了したところで画面右上の [Options] アイコンをタップし、続いて [Envelope Settings] をタップします。

ステップ 4　[Request Read Receipt] をタップして、このオプションを有効にします。

ステップ 5　[Done] をタップします。

送信した安全なメッセージの管理

スマートフォンから送信済みの暗号化した電子メールのリストは [Sent Items] 画面に表示されます。

この画面にアクセスするには、[Cisco BCE]、[Sent Items] の順にタップします。この送信済みの暗号化した電子メールのリストから、電子メール アドレスと変更または表示する電子メールを選択します。選択した電子メールをタップしてメニュー オプションを表示します。

送信済みの暗号化した電子メールに対して、[Cisco BCE Mailbox] で次の操作を実行できます。

- [Lock]： 暗号化した電子メールを送信した後、その電子メールをロックして受信者が電子メールを開くことができないようにすることが可能です。電子メールをロックすると、この画面から [Edit Lock Reason] オプションと [Unlock] オプションを使用できます。「暗号化した電子メールのロックまたはロック解除」（P.1-15）を参照してください。
- [Set Expiry]： 暗号化した電子メールに有効期限を設定できます。「電子メールの有効期限の設定」（P.1-16）を参照してください。
- [View Details]： 現在のデバイスから送信済みの暗号化した電子メールの詳細を表示します。

送信済み電子メール メッセージの詳細

[Cisco BCE Mailbox] では、現在のデバイスから送信済みの暗号化した電子メールの詳細を表示できます。[Cisco BCE Mailbox] にアクセスするには [Cisco BCE]、[Sent Items] の順にタップします。この送信済みの暗号化した電子メールのリストから、電子メール アドレスと表示する電子メールを選択します。選択した電子メールをタップしてメニュー オプションを表示します。[View Details] をタップします。

次の情報が表示されます。

- [Subject]： メッセージの件名。
- [To]： 受信者の電子メール アドレス。
- [Open Date]： 暗号化されたメッセージを該当の受信者が開いた日付。
- [Locked Status]： 暗号化した電子メールがロックされている場合は、錠のアイコンが表示されます。ロックされていない場合は、ロック解除のアイコンが表示されます。
- [Locked Reason]： 暗号化した電子メールをロックしたときに入力したコメントが表示されます。
- [Expiration Date]： 暗号化した電子メールの有効期限。

エンベロープの設定

安全な電子メールの作成では、作成中の電子メールのメッセージ設定を変更できます。

エンベロープの設定を変更するには、次の作業を実行します。

ステップ 1　[Cisco BCE]、[Secure Compose] の順にタップして [Secure Compose] 画面を開きます。

ステップ 2　デフォルトでは、登録した電子メール アカウントの電子メール アドレスが [From] フィールドに追加されます。

次の各フィールドに適切に入力します。

- Address（To、CC、および BCC）
- Subject

ステップ 3　メッセージのテキストを入力します。

ステップ 4　[Envelope Settings] にアクセスするには、画面右上の [Options] アイコンをタップし、[Envelope Settings] をタップします。

ステップ 5　次をタップして、該当のメッセージ オプションを有効または無効にします。

- Expiration
- Request Read Receipt
- Allow Reply
- Allow Reply All
- Allow Forward
- Message Sensitivity

ステップ 6　[Done] をタップして変更を保存します。

メッセージの秘密度

送信者は、[Cisco BCE] から開く [Settings] 画面で、暗号化した電子メールの秘密度を指定できます。メッセージに設定できる秘密度のオプションは次のとおりです。

- [High]： メッセージに高い秘密度を指定すると、それを暗号化したメッセージを復号化するたびに認証のためのパスワードが要求されます。
- [Medium]： メッセージに中程度の秘密度を指定すると、受信者のパスワードがキャッシュされていれば、そのメッセージを暗号化したメッセージを復号化するときにパスワードは要求されません。
- [Low]： メッセージに低い秘密度を指定すると、安全な送信は可能ですが、それを暗号化したメッセージを復号化するときにパスワードが要求されません。

すべてのメッセージにはデフォルトで [High] の秘密度が設定されます。特定のメッセージについて [Envelope Settings] で秘密度の値を変更することで、このデフォルトの設定を変更できます。

（注）　管理者は、設定ファイルで秘密度のオプションから High、Medium、または Low を指定することで、メッセージの最低限の秘密度を定義できます。この最低限のメッセージ秘密度が定義されていると、ユーザ側ではそれより低い秘密度をメッセージに設定できなくなります。

キャッシュ管理

パスワードのキャッシュ

Cisco BCE 登録アカウントのパスワードは一定の期間キャッシュされますが、[Cisco BCE] からアクセスする [Settings] 画面でこの期間を設定できます。パスワードのキャッシュはデフォルトで有効になっていて、デフォルトのキャッシュ期間は 1,440 分（24 時間）です。[Settings] 画面でパスワードのキャッシュを無効にすることができます。[Cache Password] をタップして有効または無効に設定し、[Done] をタップして変更を保存します。

[Cisco BCE] からアクセスする [Settings] 画面で [Clear Cache] をタップすると、パスワードのキャッシュをクリアできます。デバイスをシャットダウンまたは再起動すると、パスワードのキャッシュは自動的にクリアされます。

安全なエンベロープのキャッシュ

ダウンロードした安全なエンベロープは、初めて開いた後、デバイス上でキャッシュされます。これにより、同じ安全なエンベロープを次回開くときに、そのエンベロープが再度ダウンロードされることがありません。

キャッシュ処理は時間とサイズの組み合わせに基づいて実行されます。キャッシュするエンベロープの最大サイズは管理者が設定します。デフォルトは 6 MB です。デバイス上で 24 時間ごとに実行されるタスクにより、キャッシュされている期間が 2 週間を超えているエンベロープはすべて削除されます。

診断ツールを使用したトラブルシューティング

Cisco BCE アプリケーションには、問題のトラブルシューティングに効果的な診断ツールが付属しています。エラーを受け取った場合や Cisco BCE アプリケーションに問題が発生した場合は、この診断ツールを使用できます。

この診断ツールでは、収集したデータを電子メールに添付します。診断のための電子メールには、暗号化アプリケーションとの対話操作の際にデバイスについて生成されたデータが記述されます。

（注） デバイス上で 24 時間ごとに実行されるタスクにより、作成から 1 週間を経過しているログはすべて削除されます。

診断ツールの実行

（注） 診断のための電子メールには、受け取ったあらゆるエラーまたは Cisco BCE アプリケーションで発生したあらゆる問題の説明を記述することが重要です。トラブルシューティングおよび問題解決で、これらの情報が役に立ちます。

診断ツールを実行して診断のための電子メールを送信するには、次の作業を実行します。

ステップ 1　[Cisco BCE]、[About] の順にタップして、Cisco BCE の [About] 画面を開きます。

ステップ 2　画面右上の [Options] アイコンをタップし、続いて [Diagnostic] をタップします。

診断出力が添付された [Email Compose] 画面が表示されます。この診断出力は、*device.txt*、*BCE.txt*、および *config.txt* の 3 つのファイルで構成されています。

ステップ 3　送信先アドレスを [To] に入力して、メッセージの内容を作成します。管理者による [Subject] フィールドと [To] フィールドの設定に応じて、これらのフィールドには事前に情報を入力済みとすることができます。これらを編集できるようにすることも可能です。

ステップ 4　[Send] をタップします。

ログ レベルの設定

[Advanced Settings] 画面でログ レベルを定義することで、アプリケーションに保持するログの種類を設定できます。[Cisco BCE]、[Settings] の順にタップします。[Settings] 画面で [Diagnostic Log Level] をタップして、ログ レベルを表示または設定します。使用しているコンフィギュレーション モードによっては、このオプションを設定に使用できないことがあります。

設定できるログ レベルは次のとおりです。

- [Error]： Cisco BCE で生成されたエラー メッセージがログに記録されます。これはデフォルトのオプションです。
- [Warning]： アプリケーションで生成された警告とエラー メッセージがログに記録されます。
- [Info]： アプリケーションで生成されたエラー、警告、および情報のメッセージがログに記録されます。ログに記録された内容を使用して、アプリケーションの処理フローを確認できます。このオプションを使用すると、スマートフォン デバイスの動作速度が低下します。
- [Debug]： アプリケーションで生成されたエラー、警告、情報、およびデバッグ情報がログに記録されます。このオプションを使用すると、スマートフォン デバイスの動作速度が低下します。

Cisco Business Class Email アプリケーションのアップグレード

Cisco BCE アプリケーションのアップグレードは Apple App Store から入手できます。Apple App Store を使用して元のアプリケーションをインストールしている場合は、更新されたバージョンが入手可能になると、自動的にそれが通知されます。

アップグレード後も、これまでの設定が保持されます。

Cisco Business Class Email アプリケーションのアンインストール

iOS 上の Cisco BCE をアンインストールするには、次の作業を実行します。

ステップ 1　iOS ホーム画面に移動します。

ステップ 2　[Cisco BCE] アイコンをタップし、削除アイコン（**X**）が表示されるまでそのまま保持します。

ステップ 3　削除アイコン（**X**）をタップします。アプリケーションが削除されます。

カスタマー サポート

Cisco Business Class Email に関する助言を得るには、担当のシステム管理者に問い合わせてください。