CHAPTER 1

Cisco Business Class Email for iOS の設定と使用

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 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 iOS デバイス上で開く
- Cisco BCE を使用して、暗号化した電子メールを iOS デバイスから送信する
- Cisco BCE を使用して、iOS デバイス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 iOS デバイス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 iOS デバイス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 iOS デバイス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 iOS デバイスで確認または変更する

最新情報

このリリースには、次の新機能が含まれています。

- 登録済みエンベロープに受信者言語を選択できるようになりました。この新しいオプションでは、受信者に設定されたロケールに応じてどの言語をメッセージ本文に使用するかを指定することができます。詳細については、「アカウント設定」セクション（ 1-5 ページ）を参照してください。

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。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。

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 メッセージを復号化したり、受信メッセージに転送して応答することができます。復号化アカウントを作成するには、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きます。
- **Decrypt and Encrypt**: 安全な電子メール メッセージを暗号化および復号化できます。暗号化されたアカウントを作成するには、「Cisco Business Class Email の設定ファイルの起動」セクション（ 1-3 ページ）の説明に従って、管理者から受信したコンフィギュレーション ファイルを適用します。

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

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。暗号化されたアカウントを作成するには、「Cisco Business Class Email の設定ファイルの起動」セクション（ 1-3 ページ）の説明に従って、管理者から受信したコンフィギュレーション ファイルを適用する必要もあります。BCE アカウントのタイプの詳細については、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（ 1-2 ページ）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、新しい *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。

注　同じデバイスで BCE の電子メールを開く場合でも複数の CRES または IEA のアカウントを使用できます。複数のアカウントを作成するには、アカウントが異なるサーバに関連付けられるように設定します。これらのアカウントにはそれぞれ独自のアカウント設定があります。また、別個のアカウントはオフライン メッセージを開いたときに作成されます。

アプリケーションのホーム画面

Cisco BCE のアイコンをタップするとアプリケーションのホーム画面が開きます。

次の表は、アプリケーションのホーム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
[account name] > [Inbox]	選択したアカウントのために開いた復号化された電子メールのリストを表示できます。
[account name] > Manage Messages	自分のデバイスおよび他のデバイスから送信された電子メール メッセージを管理できます。アカウントを選択して、現在のデバイスから送信されていないメッセージをサーバからロードできます。個々の電子メール アカウントをタップすると、選択したアカウントから暗号化して送信された電子メールのリストが表示されます。
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（ 1-13 ページ）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（ 1-4 ページ）を参照してください。
チュートリアル	Cisco BCE アプリケーションを有効にする方法の簡単な説明

Cisco Business Class Email の設定ファイルの起動

暗号化されたアカウントを作成するには、次に示すように、Cisco BCE アプリケーションのインストール後に管理者から受信したコンフィギュレーション ファイルを適用する必要があります。

暗号化されたアカウントの BCE アプリケーションを有効化し、設定するには、次の作業を行います。

ステップ 1　iOS デバイスを提供するネイティブの電子メール 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。添付ファイルに押し続けます。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

次の表に、Cisco BCE に設定できる 2 種類の設定を表示します。

- General Settings
- [Account Settings]

General Settings

一般設定を設定するには、[Settings]、[General 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 (1-2 ページ) を参照してください。

[General 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
Default Account	デフォルトの Cisco BCE 登録アカウントとして使用する電子メール アカウントのアドレスを指定します。
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。
Send Usage Data	匿名の使用状況データを BCE アプリケーションを向上させるために Cisco に送信するかを決定します。
Reset Identifier	使用状況データを送信するのに使用する ID をリセットするかどうかを決定します。

オプション	説明
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（1-17 ページ）を参照してください。
Send Diagnostic Email	トラブルシューティングの目的で診断メールを送信します。
About	アプリケーションのバージョン番号、サードパーティのライセンスおよび通知、使用状況データの詳細、利用規約、およびユーザ ガイドなどの BCE アプリケーションに関する情報を表示します。

アカウント設定

アカウント設定を設定するには、[Settings]、[account name] 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（1-2 ページ）を参照してください。

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

オプション	説明
名前	Cisco BCE 登録アカウントで使用するために送信されたアカウント名。
ログイン	Cisco BCE 登録アカウントで使用するために送信されたログイン名。
[サーバ]	Cisco BCE 登録アカウントで使用するために送信されたサーバ名。
Password Cache Duration	キャッシュ期間を日、時、分で入力します。デフォルトは 1 日です。
Clear Password Cache	タップするとキャッシュがただちにクリアされます。キャッシュはパスワード キャッシュ時間の期間が過ぎると自動的にクリアされます。
Expiration	暗号化した電子メールに有効期限を指定するデフォルトの有効期限を設定します。特定の日付後、メッセージは期限切れとなり、受信者はこの後に開くことができません。電子メールの有効期限の設定（1-11 ページ）を参照してください。
Request Read Receipt	受信者が暗号化されたメッセージを開いたときにデフォルトの開封確認通知を送信者に要求するかどうかを決定します。デフォルトでは有効に設定されています。送信した安全なメッセージの管理（1-12 ページ）を参照してください。
Message Security	メッセージのセキュリティ レベルを Low、Medium、または High に設定するかどうかを決定します。デフォルトではメッセージのセキュリティ レベルは High に設定されています。Message Security（1-16 ページ）を参照してください。
Envelope Cache Size	ダウンロードされた安全なエンベロープを初めて開いた後のキャッシュ サイズ（MB 単位）を定義します。デフォルトでは、この値は 6 MB です。

オプション	説明
Envelope Cache Duration	キャッシュがクリアされるまでの時間を指定します。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。デフォルトは、30 日です。
Allow Reply	メッセージ設定も許可した場合、受信した暗号化されたメッセージに暗号化応答を送信できるかどうかを決定します。デフォルトでは有効に設定されています。電子メールへの返信、全員への返信、および転送（ 1-9 ページ）を参照してください。
Allow Reply All	メッセージ設定も許可した場合、受信した暗号化されたメッセージの受信者すべてに暗号化応答を送信できるかどうかを決定します。デフォルトで、このオプションは有効になっています。
Allow Forward	メッセージ設定も許可した場合、受信した暗号化されたメッセージを転送できるかどうかを決定します。デフォルトで、このオプションは有効になっています。
Recipient Language	受信者に設定されているロケールに応じて、どの言語をメッセージ本文に使用するかをアプリケーションで決定できるようにします。暗号化されたメッセージを同じロケールを持つ受信者に送信する場合は、このオプションを使用します。受信者がさまざまなロケールを持つ場合、メッセージ本文には、通常次のオプションから選択するデフォルトの言語を使用します。 • サーバのデフォルト • 英語 • フランス語 • ドイツ語 • スペイン語 • ポルトガル語 • 日本語 • イタリア語
Submit Diagnostic Information	トラブルシューティングの目的で送信される診断メールの受信者、件名、コンテンツを指定できます。アプリケーションで維持するログのタイプを、ログ レベルで定義されているように設定するには、ログ レベルの設定（ 1-17 ページ）を参照してください。

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 2 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（1-2 ページ）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、両方のコンフィギュレーション モードで使用できます。

2 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 と Encrypt モードの両方で使用できるオプション

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。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。

統合された 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。

いずれかのモードを有効にする方法の詳細については、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（1-2 ページ）を参照してください。

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 iOS 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 添付ファイルを押したままにします。

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。添付ファイルを押したままにします。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、パスワードが自動でパスワード フィールドに入力されます。

ステップ 5　[Submit] 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値は、7 MB に制限されています。

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　[account name]、[Inbox] の順にタップして、受信箱の電子メール アカウント画面を開きます。

ステップ 2　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 [Submit] をタップします。
- 電子メール アドレスとパスワードがキャッシュされて、パスワードはパスワード フィールドに自動的に入力されます。

復号化したメッセージが表示されます。

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 iOS 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（ 1-4 ページ）を参照してください。

注　応答のセキュリティを維持するために、受信者のリストは変更できません。

応答または暗号化された電子メールを転送するには、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（ 1-8 ページ）または暗号化した電子メールの送信（ 1-13 ページ）の手順を実行します。

ステップ 2　[Settings] 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　メッセージが完了すると、[Encrypt] をタップして、iOS 電子メール システムを開き、操作を完了します。

ステップ 4　[Send] をタップします。

メッセージが暗号化され、送信する電子メールに HTML ファイルとして添付されて送信されます。

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　[account name]、[Manage Messages] の順にタップします。

選択したアカウントから送信した、暗号化された電子メール メッセージのリストを表示するには、プルダウン ジェスチャーを実行します。

ステップ 2　電子メールのリストでロックする暗号化された電子メール メッセージにチェックを入れます。

これによりロックおよび期限切れアイコンが有効化されます。

ステップ 3　[Lock] をタップします。

ステップ 4　選択した電子メール メッセージがまだオンになっている間は、必要に応じてそのメッセージをロックする理由を入力し、[Update] をタップします。

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。

ステップ 5　[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　[account name]、[Manage Messages] の順にタップします。

選択したアカウントから送信した、暗号化された電子メール メッセージのリストを表示するには、プルダウン ジェスチャーを実行します。

ステップ 2　電子メールのリストでロック解除する暗号化された電子メール メッセージを確認します。

ステップ 3　[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　[Settings]、[account name] の順にタップして、電子メール アカウントの設定画面を開きます。

ステップ 2　[Expiration] をタップして、電子メールが期限切れになるまでの日数を指定します。

ステップ 3　[< account name] をタップし、終了して変更を保存します。

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　[Secure Compose] アイコンをタップして、[Secure Compose] 画面を開きます。

ステップ 2　[Encrypt] をタップして、暗号化されたメッセージを送信するのに使用する登録済み電子メール アカウントを選択します。

ステップ 3　メッセージの作成を完了したら、iPhone の画面左下とタブレットの画面右上にある [Settings] アイコンをタップします。

ステップ 4　[Expiration] 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　[< Message Settings] をタップして変更を保存します。

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

ステップ 8　メッセージが完了すると、[Encrypt] をタップして、iOS 電子メール システムを開き、操作を完了します。

ステップ 9　[Send] をタップします。メッセージが暗号化され、送信する電子メールに HTML ファイルとして添付されて送信されます。

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　[account name]、[Manage Messages] の順にタップします。

選択したアカウントから送信した、暗号化された電子メール メッセージのリストを表示するには、プルダウン ジェスチャーを実行します。

ステップ 2　電子メールのリスト内で、有効期限を設定する、暗号化電子メール メッセージにチェックを入れます。

これによりロックおよび期限切れアイコンが有効化されます。

ステップ 3　[Expiration] アイコンをタップします。

ステップ 4　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 5　[Set] 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認します。

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　[account name]、[Manage Messages] の順にタップします。

選択したアカウントから送信済みの暗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 2　電子メールのリスト内で、有効期限をクリアする、暗号化電子メール メッセージにチェックを入れます。

これによりロックおよび期限切れアイコンが有効化されます。

ステップ 3　[Expiration] アイコンをタップします。

ステップ 4　[Never] をタップします。

ステップ 5　[Update] をタップして、変更を保存します。

送信した安全なメッセージの管理

[Manage Massages] 画面を使用して、自分のデバイスおよび他のデバイスの両方から送信されたメッセージを確認し、管理できます。デバイスから送信されたメッセージは [Sent from this device] アイコンでマークされます。[Manage Massages] 画面では、メッセージを削除、ロック、または期限切れにしたり、詳細を表示したりすることもできます。

[Filter] ボタンをタップしたり、[sent from device] を選択することによって自分のデバイスから送信された、こうしたメッセージだけを表示することができます。フィルタを削除するには、[Filter] ボタンをタップして [show all] を選択します。すべてのフィルタ処理されたメッセージが送信された日付でソートされます。

デバイスから送信されたメッセージを削除すると、メッセージは「Sent from this device」としてマークされなくなります。ただし、送信したメッセージを削除しても、いくつかのメッセージ情報は表示されたままです（件名、受信者、および送信された日付など）。メッセージが削除されると、別のデバイスから送信されたかのように、つまり Web インターフェイスを使用して開かれます。削除済みメッセージのメッセージの詳細をロックしたり、期限切れにしたり、参照することができますが、メッセージ本文と添付ファイルは表示できません。

モバイル デバイスから送信済みの暗号化された電子メールのリストを表示するには、[account name]、[Manage Messages] の順にタップします。ロックの原因または有効期限を設定または表示するために送信済みの暗号化されたメッセージのリストから電子メール アドレスと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、送信済みの暗号化された電子メールに使用できる次のメニュー オプションを表示します。

- [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（ 1-10 ページ）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（ 1-11 ページ）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。
- [Remove]：削除を行います。

iPhone で、メッセージをロックする、期限切れにする、または開くかどうかを決定するための適切なアイコンを表示できます。

iPad で、管理メッセージ テーブルのメッセージに関する次の情報を表示できます。

- [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。
- [Expiration Date]：暗号化した電子メールの有効期限。
- [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。

デバイスから送信済みの暗号化された電子メールの詳細も表示できます。メッセージのセキュリティ設定によっては、メッセージをタップして詳細を表示するときにパスワードの入力が必要な場合があります。次の情報が表示されます。

- [Subject]：メッセージの件名。
- [Date]：メッセージが送信された日付。
- [To]：受信者の電子メール アドレス。
- [From]：送信者の電子メール アドレス。
- 本文
- 添付ファイル

Encrypt モードのみで使用できるオプション

統合された 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。

このモードを有効にする方法の詳細については、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（ 1-2 ページ）を参照してください。

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　[Secure Compose] アイコンをタップして、[Secure Compose] 画面を開きます。[Secure Compose] アイコンは、「暗号化」タイプのエディションが BCE コンフィギュレーション ファイルに適用された場合のみ使用可能です。

ステップ 2　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

設定された電子メール アカウントが 1 つだけの場合、そのアカウントは新しいメッセージの [Encrypt with] フィールドに追加されます。複数の設定された電子メール アカウントがある場合、フィールドの [Encrypt] の [Compose] 画面に表示されるデフォルトのアカウントとしてアカウントを選択できます。デフォルトのアカウントを設定するには、[General Settings]、[Default Account] の順に選択します。

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、iPad に右上の画面と iPhone の画面の下部にある [Settings] アイコンをタップします。

注　iPhone で安全なメッセージを作成すると、3 MB の大きい添付ファイルを追加できます。

注　[Save Draft] オプションを [Settings] 画面で有効化した場合、メッセージのドラフトを保存できます。メッセージの内容は、アプリケーションが再起動、またはバックグラウンドで返されたときに表示されます。

ステップ 5　メッセージが完了すると、[Encrypt] をタップして、iOS 電子メール システムを開き、操作を完了します。

ステップ 6　[Send] をタップします。メッセージが暗号化され、送信する電子メールに HTML ファイルとして添付されて送信されます。

開封確認の要求

送信した電子メールを受信者が開いたときに、iOS デバイス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　[Settings]、[account name] の順にタップして、電子メール アカウントの設定画面を開きます。

ステップ 2　[Request Read Receipt] スイッチを有効に設定します。デフォルトではイネーブルです。

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　[Secure Compose] アイコンをタップして、[Secure Compose] 画面を開きます。

ステップ 2　[Encrypt] をタップして、暗号化されたメッセージを送信するのに使用する登録済み電子メール アカウントを選択します。

ステップ 3　メッセージの作成を完了したら、iPhone の画面左下とタブレットの画面右上にある [Settings] アイコンをタップします。

ステップ 4　[Request Read Receipt] スイッチを有効に設定します。デフォルトではイネーブルです。

ステップ 5　[Set] をタップして、変更内容を保存します。

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　[account name]、[Secure Compose] の順にタップして [Secure Compose] 画面を開きます。

ステップ 2　[Encrypt] をタップして、暗号化されたメッセージを送信するのに使用する登録済み電子メール アカウントを選択します。

ステップ 3　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 4　メッセージのテキストを入力します。

ステップ 5　メッセージの作成を完了したら、iPhone の画面左下とタブレットの画面右上にある [Settings] アイコンをタップします。

ステップ 6　適切なメッセージ オプションを設定します。

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

ステップ 7　[Set] をタップして、変更内容を保存します。

Message Security

送信者は、[Settings]、[account name]、[Message Security] の順にタップすることによって、暗号化された電子メール用のセキュリティ レベルを指定できます。メッセージに設定できるセキュリティのオプションは次のとおりです。

- [High]: メッセージに高度のセキュリティを指定すると、暗号化されたメッセージを復号化するたびに認証用のパスワードが要求されます。
- [Medium]: メッセージに中程度のセキュリティを指定すると、受信者のパスワードがキャッシュされていれば、暗号化され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]: メッセージに低いセキュリティを指定した場合、送信は安全に行われますが、暗号化され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] のセキュリティが設定されます。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。

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、[Settings]、[account name]、[Password Cache]、[Duration] の順にタップして設定できる期間にキャッシュされます。デフォルトのキャッシュ期間は、1,440 分（24 時間）です。パスワードのキャッシュは、デフォルトではオフですが、[Medium Security messages] 画面または [Manage Messages] 画面にある [Remember Password] スイッチを使用してオンにできます。

ハスワード キャッシュは、[Settings]、[account name]、[Clear Password Cache] の順にタップして、[Account Settings] 画面からクリアすることができます。暗号化アカウントの場合は、パスワード キャッシュ期間を設定することもできます。

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。エンベロープは、エンベロープの有効なキャッシュ サイズ（MB）と期間（時間）を超えていると、受信箱と管理メッセージ フォルダを再び開いたときに、受信箱と管理メッセージ フォルダから削除されます。

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　最大 2,000 行はログに保存できます。ログが 2,000 行を超えると、最も古いログが削除されます。

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　[account name]、[Submit Diagnostic Information] の順にタップして、[Cisco BCE Diagnostics] 画面を開きます。

ステップ 2　[Subject] をタップして、診断メールの件名行として表示するテキストを入力します。

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 Diagnostic Email] 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。[Settings]、[General 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。

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。
- [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。
- [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。

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

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] アイコンを押し、削除（**X**）アイコン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。