



Cisco Secure Email Encryption Service 6.2 受信者ガイド

初版：2020年12月1日

最終更新：2022年2月12日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

最初のセキュアメッセージを開く	1
セキュアメッセージの概要	2
セキュアメッセージを使用する理由	2
セキュアメッセージの通知	2
セキュアメッセージのコンポーネント	6
初めてセキュリティで保護されたメッセージを開封するための手順	8
暗号化されたメッセージの添付ファイルをハードドライブに保存する	9
ファイルを Web ブラウザで開く	10
[Register] ボタンをクリックして Cisco Registered Envelope Service に登録する	10
Encryption Service アカウントの有効化	12
セキュアメッセージの再表示とパスワードの入力	12
Encryption Service アカウントの有効化後にセキュアメッセージを開く	13
Google サインインによりセキュリティで保護されたメッセージを開く	13

第 2 章

電子メールの送信の概要	15
電子メールの作成と送信	16
[Automatically BCC me on this Email] オプションの使用	18
開封通知の要求	18
アドレス帳の使用	18
アドレス帳へのアドレスの追加	19
アドレス帳からのアドレスの削除	19
アドレスの編集	19
メッセージへのアドレス帳の電子メールアドレスの追加	19
メッセージの管理	20

すべての送信済みメッセージの取得	20
特定のメッセージの取得	21
基本検索	21
詳細検索	21
メッセージの詳細の表示	23
各メッセージの詳細を表示する	23
メッセージをロック/ロック解除する	24
メッセージのロック	24
メッセージのロック解除	25
メッセージの有効期限を設定する	25
メッセージの有効期限を削除する	26
プロフィールの編集	27
ローカルタイムゾーンの設定	27
個人の詳細と設定の編集	27
<hr/>	
第 3 章	セキュアメッセージに関する問題のトラブルシューティング 29
トラブルシューティングのヒント	29
問題：[開く (Open)] ボタンがメッセージに表示されない、または正常に機能しない	29
問題：メールアドレスが [To:] フィールドに表示されない	30
問題：セキュアメッセージが正常に表示されない	30
問題：メッセージの処理速度が遅い、または停止する	30
問題：パスワードを忘れた、またはパスワードが機能しない	31
問題：Microsoft OWA 2007 の互換性	32
問題：左側のナビゲーションメニューに [Compose Message] リンクが表示されない	32
問題：セキュアな電子メール（プレーンテキストまたはHTML）でアクセント付き文字が 正しくレンダリングされない	32
関連リソース	33
セキュアメッセージのヘルプ	33
FAQ	33
カスタマー サポート	33



第 1 章

最初のセキュアメッセージを開く

この章では、パスワードで保護されたセキュアメッセージを初めて受信した際の操作手順を紹介します。Cisco Secure Email Encryption Service に登録し、セキュアメッセージを開封する方法について説明します。

この章は、次の内容で構成されています。



- (注) このガイドの最新バージョンと、Cisco Secure Email Encryption Service に関するその他のドキュメントは、<https://www.cisco.com/c/en/us/support/security/email-encryption/products-user-guide-list.html> から入手できます。



重要 Web ブラウザで JavaScript が無効になっている場合、一部の Web ページは機能しません。



重要 Internet Explorer を使用して Web ページにアクセスする場合は、アライメントの問題が発生する可能性があります。次のサポートされているブラウザのいずれかに切り替えることをお勧めします。

- Google Chrome
- Mozilla Firefox
- Safari (MAC オペレーティングシステムの場合)

- [セキュアメッセージの概要 \(2 ページ\)](#)
- [初めてセキュリティで保護されたメッセージを開封するための手順 \(8 ページ\)](#)
- [Encryption Service アカウントの有効化後にセキュアメッセージを開く \(13 ページ\)](#)
- [Google サインインによりセキュリティで保護されたメッセージを開く \(13 ページ\)](#)

セキュアメッセージの概要

セキュアメッセージは、暗号化された電子メールメッセージの一種です。パスワードによって保護されているセキュアメッセージや、暗号化されていてもパスワードを必要としないセキュアメッセージもあります。

パスワードで保護されたセキュアメッセージを受信した場合は、Cisco Secure Message Service で無料のユーザーアカウントを設定して暗号化されたメッセージを開封する必要があります。

登録を済ませると、アカウントのパスワードを使用して受信したすべてのセキュアメッセージを開くことができます。また、このサービスを使用して、独自のセキュアメッセージを送信および管理することもできます。

セキュアメッセージを使用する理由

セキュアメッセージを使用すると、暗号化された電子メールを簡単に送受信できます。通常、メッセージの送信者は、重要な情報や機密情報を安全に相手へ伝えるためにメッセージを暗号化します。暗号化によって、予想外の機密保護違反や意図的な違法性のあるおよび悪意のある機密保護違反から大切な情報を守ります。個人または組織がセキュアメッセージを送信する場合、ほとんどはメッセージ受信者のために機密情報を保護することを目的として使用されます。また、政府の規制や法令によって、メッセージの送信者が情報の機密性を維持する必要があります。たとえば、セキュアメッセージを使用して、医療組織が患者の病歴に関する機密情報を送信したり、金融機関が顧客の銀行口座に関する機密情報を送信したりすることもできます。

セキュアメッセージの通知

セキュアメッセージが送信されると、次のファイルを受信します。

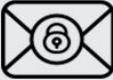
- **通知メールメッセージ。**暗号化された安全なメッセージをセキュアメッセージの形式で受信したことを知らせます。また、セキュアメッセージおよびEncryption Serviceに関する情報へのリンクも含まれています。
- **暗号化されたメッセージの添付ファイル。**通知メッセージには、暗号化されたメッセージの添付ファイルが含まれます。この添付ファイルは、`securedoc_dateTime.html` という命名規則を使用します。ここで、`date` と `time` はファイルに付加されたタイムスタンプです。たとえば、`securedoc_20100615T193043.html` というファイルを受信した場合、20100615 が年月日を表し、193043 が時刻を表します。このファイルには、セキュアメッセージと暗号化されたコンテンツの両方が含まれています。セキュアメッセージを表示するには、添付ファイルをハードドライブに保存します。次に、このファイルをダブルクリックして、セキュアメッセージを Web ブラウザに表示します。通常、コンピュータでセキュアメッセージを正しく表示してメッセージを復号するには、インターネット接続が必要です。



- 注 メール管理者が大容量ファイル添付のサポートを有効にしており、セキュアメッセージに 25 MB を超えるファイルが添付されている場合、`securedoc.html` 添付ファイルはセキュアメッセージ内に表示されません。

受信した通知メッセージは、次のいずれかの方法で表示されます。

- 次の図は、[メッセージを読む (Read Message)] ボタンがある通知メールメッセージを示しています。セキュリティで保護されたメッセージを確認するには、[Read Message] ボタンをクリックします。デフォルトでは、[Read Message] リンクは最大 14 日間有効です。リンクの有効期限が切れた後は、受信者は、Web ブラウザで添付ファイルを開くか、`mobile.res.cisco.com` にメッセージを転送することにより、メッセージを読むことができます。



This is a secure message

[Read Message](#)

The link to open this message is valid till **02/05/2020 01:09:35 PM UTC**.

How to open link after expiry

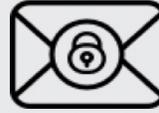
-  To read this message on desktop, open the `securedoc_20200122T050934.html` attachment in a web browser.
-  To read this message on a mobile device, forward this message to mobile@qa.res.cisco.com to receive a mobile login URL.

[Need Help?](#)

Contact the sender directly if you are not sure about the validity of this message.

Copyright © 2011-2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

- 次の図は、[メッセージを読む (Read Message)] ボタンがある通知メールメッセージを示しています。電子メールの有効期限の月はテキスト形式で、日付はタイムスタンプ付きです。この新しい日付形式は、カスタムテンプレートにのみ適用されます。



This is a secure message

Read Message

The link to open this message is valid till **June 09, 2020 01:17:44 PM UTC**.

How to open link after expiry



To read this message on desktop, open the **securedoc_20200604T131200.html** attachment in a web browser.

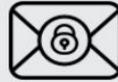


To read this message on a mobile device, forward this message to mobile@res.cisco.com to receive a mobile login URL.

Need Help?

Contact the sender directly if you are not sure about the validity of this message.

- 次の図は、[メッセージを読む (Read Message)] ボタンのない通知メールメッセージを示しています。セキュリティで保護されたメッセージを読むには、Web ブラウザで **securedoc_dateTime.html** 添付ファイルを開くか、mobile.res.cisco.com にメッセージを転送してください。詳細については、[初めてセキュリティで保護されたメッセージを開封するための手順 \(8 ページ\)](#) を参照してください。



This is a secure message

How to open



To read this message on desktop, open the **securedoc_20200124T015154.html** attachment in a web browser.



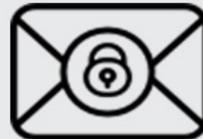
To read this message on a mobile device, forward this message to mobile@qa.res.cisco.com to receive a mobile login URL.

[Need Help?](#)

Contact the sender directly if you are not sure about the validity of this message.

Copyright © 2011-2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

- 次の図は、secureoc.html 添付ファイルと有効期限のない通知メールを示しています。この通知タイプは、セキュアメッセージに 25 MB を超えるファイルが添付されている場合に表示されます。このような場合は、[メッセージを読む (Read Message)] ボタンをクリックしてセキュアメッセージを開きます。



This is a secure message

[Read Message](#)

[Need Help?](#)

Contact the sender directly if you are not sure about the validity of this message.

Copyright © 2011-2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



- (注) 添付ファイルには、ユーザーアカウントのパスワードを入力したときに暗号化されたメッセージを復号するソフトウェアが含まれます。付属するソフトウェアがメッセージを復号化できない場合があります、その場合は、代わりに復号化メソッドを使用する必要があります。セキュアメッセージを開封する際の別の方法については、[セキュアメッセージに関する問題のトラブルシューティング \(29 ページ\)](#) を参照してください。

セキュアメッセージのコンポーネント

受信したセキュアメッセージの [メッセージを読む (Read message)] ボタンをクリックすると、Web ブラウザにリダイレクトされ、メッセージが表示されます。

[Secure Message] ログインページには、受信者のメールアドレスが検索可能なドロップダウンボックスに表示されます。検索可能なドロップダウンボックスを使用して、次のいずれかの方法でセキュリティで保護されたメッセージを開くことができます。

- 検索可能なドロップダウンボックスから、必要な受信者のメールアドレスを選択します。
- 検索可能なドロップダウンボックスに、受信者のメールアドレスと一致する文字を入力して、受信者のメールアドレスを検索します。



- (注) Web ブラウザで JavaScript が無効になっている場合、受信者のメールアドレスは検索できません。検索可能なドロップダウンボックスでは、受信者のメールアドレスのリストを表示して選択することしかできません。

セキュアメッセージを単一の受信者に送信すると、[お客様のアドレス (Your Address)] フィールドに受信者の電子メールアドレスが自動的に入力されます。セキュアメッセージの [宛先 (To)] および [コピー送信先 (CC)] アドレスフィールドに複数の受信者が存在する場合、受信者のメールアドレスと一致するいずれかの文字を検索可能なドロップダウンボックスに入力すると、[お客様のアドレス (Your Address)] フィールドに自動入力されます。



- (注) BCC 受信者としてセキュリティで保護されたメッセージを受信した場合は、検索可能なドロップダウンボックスから [Address Not listed] オプションを選択し、受信者のメールアドレスを手動で入力する必要があります。

すでにサービスに登録している場合は、[Open] ボタンが表示されます。[Open] ボタンをクリックし、コンテンツを復号してメッセージを表示します。

サービスに登録していない場合、パスワードを入力する前に、登録してユーザーアカウントを作成することを求められます。メールアドレスがユーザーアカウントに関連付けられていない場合は、メッセージに [登録 (Register)] ボタンが表示されます。その場合は、[Register] ボタンをクリックしてサービスに登録します。

受信したメールの **securedoc** 添付ファイルを開くと、Web ブラウザにセキュアメッセージが表示されます。

次の表で、上の図で示されているセキュアメッセージの重要な機能について説明します。

機能	説明
アドレスフィールドと件名	アドレスフィールドでは、送信者のアドレスが [From:] フィールドに、宛先アドレスが [To:] フィールドに表示されます。
Password フィールド	セキュアメッセージがパスワードによって保護されている場合は、Encryption Service パスワードを入力してメッセージを開封します。サービスに登録していない場合は、パスワードを入力する前に登録するように求められます。
[Open] ボタン	<p>パスワードで保護されたメッセージを受信すると、すでにサービスに登録している場合は、[Open] ボタンが表示されます。[Open] ボタンをクリックし、コンテンツを復号してメッセージを表示します。[Open] ボタンは、サービスに登録してユーザーアカウントを作成した後に初めて表示されます。メールアドレスがユーザーアカウントに関連付けられていない場合は、[開く (Open)] ボタンの代わりに [登録 (Register)] ボタンが表示されます。その場合は、[Register] ボタンをクリックしてサービスに登録します。</p> <p>低セキュリティのセキュアメッセージを受信した場合は、[開く (Open)] ボタンの代わりに [確認 (Acknowledge)] ボタンが表示されます。</p> <p>(注) 企業によっては、Cisco Secure Message Service でシングルサインオン (SAML) ログインが使用できるよう設定されている場合があります。その場合は、企業の資格情報を使用してログインするためのポップアップが表示されます。</p>
[Sign in with Google] ボタン	Google アカウントがある場合は、[Google Sig-up] ボタンをクリックして登録する必要があります。登録すると、Google でサインインしてセキュリティで保護されたメッセージを確認できるようになります。この場合、Encryption Service に登録したり、Encryption Service パスワードを入力したりする必要はありません。
[Help] リンク	[ヘルプ (Help)] リンクをクリックし、セキュアメッセージのオンラインヘルプにアクセスします。オンラインヘルプでは、セキュアメッセージを開封するための標準的な方法および代替方法について説明します。よく寄せられる質問 (FAQ) へのリンクもあります。
メッセージのセキュリティレベル	メッセージのセキュリティレベルは、低、中、または高に設定できます。デフォルトは medium です。低セキュリティで送信されたメッセージを開くには、パスワードを入力する必要はありません。中セキュリティでは、標準のパスワード機能を使用できます。高セキュリティで送信されたメッセージを開封するには、[Remember me on this computer] オプションをオンにしている場合にも、必ずパスワードを入力する必要があります。

機能	説明
[Remember Me] チェックボックス	[Remember me on this computer] チェックボックスをオンにすると、設定内容がコンピュータに記録されます。この設定は、暗号化プロファイルによって異なります。たとえば、中セキュリティのメッセージを受信した場合は、開封のためにパスワードを入力する必要がない場合もありますが、高セキュリティのメッセージを受信した場合は、開封のために必ずパスワードを入力する必要があります。
言語	受信するセキュアメッセージの翻訳に使用する言語を選択します。この選択により、BCE設定ファイルに設定されたシステムのデフォルトロケールによって決定される言語が上書きされます。
ロゴ	Encryption Service アプリケーションの [アカウント管理 (Account Management)] > [ブランディング (Branding)] > [イメージ (Images)] ページに、エンベローププロファイル用に選択したカスタムロゴが表示されます。

セキュアメッセージのその他の機能については、次のアドレスから「よく寄せられる質問 (FAQ)」をご覧ください。

<https://res.cisco.com/websafe/help?topic=FAQ>

セキュアメッセージのほとんどの構成要素はメッセージごとに異なります。エンベロープの構成要素に影響を与える要因には以下が挙げられます。

- 送信者のアカウント設定。
- 受信者のコンピュータにインストールされているソフトウェア。
- 電子メールゲートウェイによって、暗号化されたメッセージの添付ファイルに追加された変更。
- 受信者がすでにサービスに登録済みかどうか。

セキュアメッセージは動的であり、特定のメッセージの構成要素は時間の経過によって変化する可能性があります。

初めてセキュリティで保護されたメッセージを開封するための手順

このセクションでは、パスワード保護されたセキュアメッセージを初めて開封する方法について詳しく説明します。この手順は、初めて受信した場合の標準的なシナリオです。手順は状況によって異なる場合があります。Google アカウントがある場合は、Google 認証を使用してセキュリティで保護されたメッセージを開くことができます。詳細については、[Google サインインによりセキュリティで保護されたメッセージを開く \(13 ページ\)](#) を参照してください。



- (注) これらの手順は、パスワードで保護されたメッセージを初めて受信したユーザーのみに適用されます。Encryption Service に登録してアカウントを有効化すると、パスワードを使用して、どの送信者からのセキュアメッセージでも開けるようになります。パスワードによって保護されていないセキュアメッセージを受信した場合、メッセージの開封のために登録する必要はありません。詳細については、[Encryption Service アカウントの有効化後にセキュアメッセージを開く \(13 ページ\)](#) を参照してください。

最初のセキュアメッセージを開くには、次の手順を実行する必要があります。



- (注) セキュアメッセージに 25 MB を超えるファイルが添付されている場合、`securedoc.html` 添付ファイルはセキュアメッセージ内に表示されません。このような場合は、セキュアメッセージ上にある [メッセージを読む (Read Message)] ボタンをクリックして、下記の手順 3 から開始します。

手順

- ステップ 1 [暗号化されたメッセージの添付ファイルをハードドライブに保存する \(9 ページ\)](#)
- ステップ 2 [ファイルを Web ブラウザで開く \(10 ページ\)](#)
- ステップ 3 [\[Register\] ボタンをクリックして Cisco Registered Envelope Service に登録する \(10 ページ\)](#)
- ステップ 4 [Encryption Service アカウントの有効化 \(12 ページ\)](#)
- ステップ 5 [セキュアメッセージの再表示とパスワードの入力 \(12 ページ\)](#)

暗号化されたメッセージの添付ファイルをハードドライブに保存する

セキュアメッセージの通知を受け取った場合、添付ファイル (`securedoc_dateTime.html`。 `date` と `time` は、メールの送信時に付加されたタイムスタンプを表します) をダウンロードして、ファイルを開く前にハードドライブに保存する必要があります。



- (注) 添付ファイルを保存するためのダイアログボックスは、お使いの電子メールプログラムや Web メールサイト (Yahoo! メール、Gmail、Hotmail) によって異なる場合があります。

通知メッセージの詳細については、[セキュアメッセージの通知 \(2 ページ\)](#) を参照してください。

ファイルを Web ブラウザで開く

Web ブラウザで `securedoc_date Ttime .html` ファイル（ダウンロードしたファイルの保存先から）を開きます。



- (注) 電子メールの添付ファイルから直接ファイルを開かないでください。最初にファイルをシステムにダウンロードし、ダウンロードしたファイルの保存先から `html` ファイルを開く必要があります。

セキュアメッセージに登録ページが表示されます。

[Register] ボタンをクリックして Cisco Registered Envelope Service に登録する

セキュアメッセージを開くには、Cisco Secure Email Encryption Service にアカウントに登録する必要があります。



- (注) 企業によっては、Encryption Service でシングルサインオン (SAML) 認証が使用できるよう設定されている場合があります。その場合は新規ユーザー登録が簡略化され、ポータル言語と Encryption Service ユーザーアカウントに使用する名前のみ入力する必要があります。次の図は、SAML 認証による新規ユーザー登録を示しています。

[新規ユーザー登録 (New User Registration)] ページが表示されます。



- (注) [新規ユーザー登録 (New User Registration)] ページでは、アカウントを Cisco Secure Message Service に登録するまで、カスタマイズされたロゴとフッターリンクを表示できません。



- (注) 新しいアカウントの登録時に、セキュリティに関する質問と個人のセキュリティに関するフレーズは不要になりました。

次のフィールドに情報を入力します。

表 1: Encryption Service 登録ページのフィールド

フィールド	値
First Name	必須です。Encryption Service ユーザーアカウントの名前 (名) を入力します。

フィールド	値
Last Name	必須です。Encryption Service ユーザーアカウントの名前（姓）を入力します。
Password および Confirm Password	<p>必須です。アカウントのパスワードを入力し、再度確認入力します。パスワードは英数字を使用し、大文字と小文字を区別する必要があります。</p> <p>次のパスワード要件は、アカウント管理者が追加の設定を行うことができます。</p> <ul style="list-style-type: none"> • パスワードには、小文字、大文字、数字、特殊文字のうち、3つ以上の文字タイプが含まれる必要があります。 • パスワードには3回以上連続して繰り返される文字を含めることはできません。 • パスワードにはユーザー名または反転したユーザー名を含めることはできません。 • パスワードには「Cisco」、「ocsic」の文字列を使用することはできません。また、同様の文字列の大文字/小文字を変更したものや、「i」を「1」、「j」を「!」に置き換えたもの、「o」を「0」に置き換えたもの、「s」を「\$」に置き換えたものも使用できません。 <p>(注) パスワードを忘れた場合は、セキュアメッセージの [パスワードを忘れた場合 (Forgot Password?)] ボタンをクリックして、パスワードをリセットします。</p> <p>企業が Cisco Secure Message Service でシングルサインオン (SAML) ログインを使用できるよう設定している場合には、企業のサポートグループに問い合わせるパスワードを入手またはリセットしてください。</p>
Encryption Service の利用規約に同意します	Encryption Service でアカウントを登録するには、このチェックボックスをオンにする必要があります。



(注) ダイナミックなパスワード検証では、アカウント管理者が Encryption Service に対して設定した追加のパスワードルールについては検証が行われません。

登録時に、次のアカウント アクティベーション ページが表示されます。Encryption Service アカウントを有効化するには、アカウント アクティベーション メール の指示に従う必要があります。



- (注) 複数のメールアドレスでセキュアメッセージを受信する場合、複数のユーザーアカウントを設定する必要が生じることがあります。各メールアドレスには個別のユーザーアカウントが必要です。

Encryption Service アカウントの有効化

受信トレイにアカウント有効化のメッセージがサービスから届いているかを確認してください。受信トレイに電子メールが届いていない場合は、アカウント有効化のメッセージがフィルタされている可能性があるため、迷惑メールフォルダを確認してください。

アカウント有効化メールメッセージで、リンクをクリックしてユーザーアカウントを有効にします。

セキュアメッセージの再表示とパスワードの入力

手順

ステップ 1 セキュアメッセージに戻ります。[登録 (Register)] ボタンは、メッセージに表示されなくなります。代わりに、[開く (Open)] ボタンが表示されます。

ステップ 2 Cisco Secure Message Service のユーザーアカウントのパスワードを入力し、[開く (Open)] をクリックします。

- (注) 企業によっては、Cisco Secure Message Service でシングルサインオン (SAML) ログインが使用できるよう設定されている場合があります。その場合は、企業の資格情報 (ユーザー名とパスワード) を使用してログインし、暗号化された電子メールを認証し開くためのポップアップが表示されます。Google アカウントでサインインする場合は、セキュリティで保護されたメッセージを確認するために Encryption Service のユーザー名とパスワードを入力する必要はありません。

復号されたメッセージがブラウザウィンドウに表示されます。

ステップ 3 セキュアメッセージを開封すると、[返信 (Reply)] をクリックしてセキュリティで保護された返信メッセージを送信するか、[転送 (Forward)] をクリックしてセキュリティで保護された転送メッセージを送信できます。セキュリティで保護された返信メッセージまたは保護された転送メッセージを送信すると、受信者は暗号化されたメッセージを含むセキュアメッセージを受信します。

- (注) オリジナルメッセージの送信者の設定によって、特定の機能が使用できない場合があります。たとえば、セキュリティで保護されたメッセージを返信または転送できない場合があります。

Encryption Service アカウントの有効化後にセキュアメッセージを開く

Cisco Secure Message Service に登録してアカウントを有効化すると、Encryption Service パスワードを使用して、どの送信者からのセキュアメッセージでも開けるようになります。

セキュアメッセージを開封するときに Encryption Service パスワードを忘れた場合は、セキュアメッセージの [パスワードを忘れた場合 (Forgot Password?)] ボタンをクリックして、パスワードをリセットします。アカウントに関連付けられているメールアドレスに新しいパスワードのメッセージが送信されます。

新しいパスワードメッセージには [Create New Password] ページへのリンクが表示されます。このリンクをクリックすると、新しいパスワードを作成するためのブラウザにリダイレクトされます。アカウントにログインしてセキュアメッセージを開封する際、ここで設定したパスワードを使用します。パスワードをリセットするたびに、Encryption Service アカウントに関連付けられているメールアドレスに通知メールが送信されます。パスワードをリセットするためのセキュリティに関する質問は不要になりました。



(注) 企業が Cisco Secure Message Service でシングルサインオン (SAML) ログインを使用できるように設定している場合には、企業のサポートグループに問い合わせるパスワードを入手またはリセットしてください。

Google サインインによりセキュリティで保護されたメッセージを開く

Google アカウントがある場合は、Google 認証を使用してセキュリティで保護されたメッセージを開くことができます。この場合、セキュアメッセージを開封するために Encryption Service に登録したり、Encryption Service パスワードを入力したりする必要はありません。

最初に Google 認証によりセキュリティで保護されたメッセージを開く方法：

手順

ステップ 1 添付の **securedoc.html** ファイルをシステムにダウンロードします。

ステップ 2 ファイルが保存されている場所に移動し、Web ブラウザでファイルを開きます。

(注) セキュアメッセージに 25 MB を超えるファイルが添付されている場合、securedoc.html 添付ファイルはセキュアメッセージ内に表示されません。このような場合は、セキュアメッセージ上にある [メッセージを読む (Read Message)] ボタンをクリックします。

ステップ 3 [Google Sign-up] ボタンをクリックして登録します。

ステップ 4 Google アカウントを選択します。

ステップ 5 [New Google User Registration] ページで、姓と名を入力し、**[Register]** をクリックします。

確認メッセージが表示されます。電子メール宛てに確認が送信されます。

ステップ 6 セキュアメッセージに戻り、**[Googleでサインインする (Sign in with Google)]** ボタンをクリックしてセキュリティで保護されたメッセージを確認します。

(注) **[パスワード (Password)]** フィールドは、Encryption Service 認証でのみ必要となります。Google サインインによりセキュリティで保護されたメッセージを開く場合は、**[Password]** フィールドは使用しません。このフィールドはスキップして、**[Sign in with Google]** をクリックします。



第 2 章

電子メールの送信の概要

暗号化されたメールを Encryption Service アカウントから送信することができます。Encryption Service アカウントにサインアップすると、暗号化された電子メールを受信できるだけでなく、暗号化された電子メールを自分のアカウントから送信できます。暗号化された電子メールを Encryption Service から送信すると、暗号化サーバーが送信メッセージを暗号化し、目的の宛先へ転送します。暗号化されたメールを決まった宛先に頻繁に送信する場合は、そのメールアドレスを Encryption Service のアドレス帳に保存しておき、メールの作成時に、保存したアドレスを選択することができます。



- (注) アカウント管理者は、[Secure Compose] へのアクセスを無効にできます。アカウント管理者がこの機能を無効にしている場合は、左側のナビゲーションメニューに [メッセージの作成 (Compose Message)] リンクが表示されず、Encryption Service の Web サイトからセキュリティで保護されたメッセージを送信できません。



重要 Web ブラウザで JavaScript が無効になっている場合、一部の Web ページは機能しません。



重要 Internet Explorer を使用して Web ページにアクセスする場合は、アライメントの問題が発生する可能性があります。次のサポートされているブラウザのいずれかに切り替えることをお勧めします。

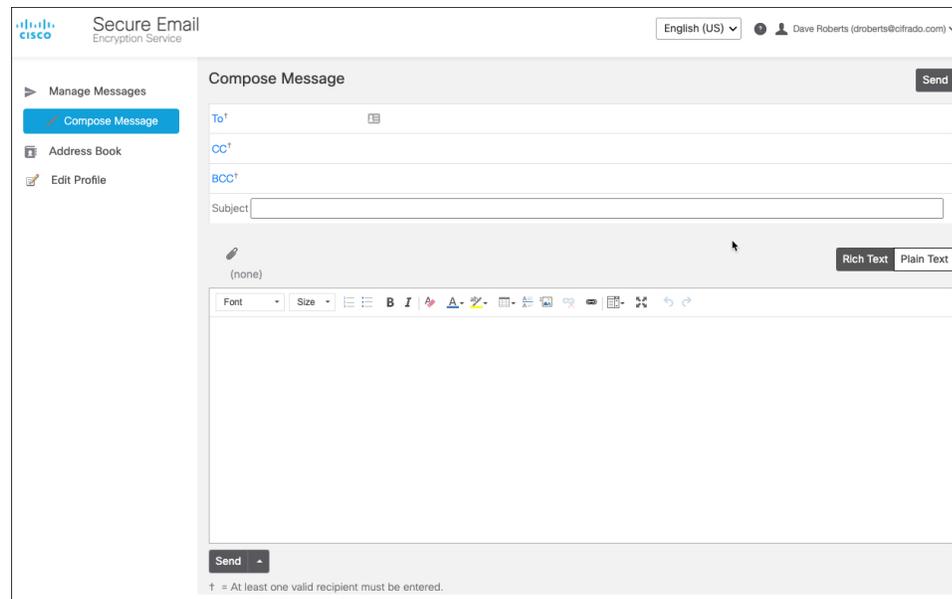
- Google Chrome
- Mozilla Firefox
- Safari (MAC オペレーティングシステムの場合)

- [電子メールの作成と送信 \(16 ページ\)](#)
- [アドレス帳の使用 \(18 ページ\)](#)
- [メッセージの管理 \(20 ページ\)](#)

- [プロフィールの編集 \(27 ページ\)](#)

電子メールの作成と送信

Encryption Service の Web サイトからセキュリティで保護されたメッセージを作成して送信するには、左側のナビゲーションメニューから **[メッセージの作成 (Compose Message)]** を選択します。



Encryption Service からセキュリティで保護されたメッセージを送信すると、暗号化された内容を含むセキュアメッセージが宛先へ送られます。Encryption Service ユーザーアカウントを所有していない受信者は、まずサービスに登録し、無料のユーザーアカウントを設定してメッセージを開封する必要があります。

手順

- ステップ 1** メッセージの作成は、[Compose Message] ページで行います。メールアドレスを入力するか、または [To:] フィールドをクリックするか、左側ペインの [Address Book] アイコンをクリックしてアドレス帳を開きます。
アドレス帳の使用の詳細については、次を参照してください。 [アドレス帳の使用 \(18 ページ\)](#)
- ステップ 2** [Compose Message] ページで、該当するアドレスフィールド ([To]、[CC]、および [BCC]) を入力します。
BCC オプションの詳細については、次を参照してください。 [\[Automatically BCC me on this Email\] オプションの使用 \(18 ページ\)](#)

ステップ 3 **[Subject]** フィールドに入力します（オプション）。

ステップ 4 **[Attachments]** ボタンをクリックして、ファイルを添付します（オプション）。

すべての添付ファイルの最大ファイルサイズは **25 MB** です。メール管理者が大容量ファイル添付のサポートを有効にしている場合は、最大 **100 MB** のファイルを添付できます。

ステップ 5 暗号化されるメッセージの本文を **[Message]** フィールドに入力します。メッセージの書式を設定するには、**[Rich Text]** リンクをクリックします。必要に応じて書式設定オプションを使用して書式を設定します。書式設定オプションの詳細については、「書式設定オプションの説明」の表を参照してください。

ステップ 6 メッセージのコピーを自分宛てに **BCC** 送信するには、チェックボックスをオンにします（オプション）。

ステップ 7 受信者がメッセージを初めて開封したときに開封通知を受け取るには、チェックボックスをオンにします（オプション）。

開封通知の詳細については、次を参照してください。 [開封通知の要求（18 ページ）](#)

ステップ 8 **[Send]** をクリックします。

[Compose Message] ページの上部に、メッセージが送信されたことを知らせる通知が表示されます。

(注) セキュリティで保護されたメッセージの作成中に **20 分以上** 入力を停止すると、Web ブラウザのセッションがタイムアウトする場合があります。タイムアウト状態のまま、**[Send]** をクリックするとエラーメッセージが表示されます。メッセージを送信するには、**Encryption Service** の Web サイトへもう一度ログインしてください。

表 2: 書式設定オプションの説明

アイコン	説明
	選択したテキストのすべての書式設定を解除します。
	長いメッセージのセクションを区切るために横線を挿入します。
	メッセージにファイルを添付します。
	メッセージにハイパーリンクを挿入します。
	メッセージからハイパーリンクを削除します。
	テキストを左揃え、右揃え、または中央揃えにするか、段落間のインデントを増やします。

	<p>テキストボックスを最大化します。テキストボックスを最小化するには、最大化の後にこのアイコンをもう一度クリックします。</p>
---	---

[Automatically BCC me on this Email] オプションの使用

セキュリティで保護されたメッセージを送信するときに、[Automatically BCC me on this email] チェックボックスをオンにすると、メッセージのコピーを自分のメールアカウントで受信できます。



(注) [Preferences] セクションの [Edit Profile] ページにある [Bcc me on messages that I send] チェックボックスをオンにすることで、このオプションのデフォルト値を設定できます。

開封通知の要求

セキュリティで保護されたメッセージを送信する際、チェックボックスをオンにして開封通知を要求できます。開封通知とは、送信した保護されたメッセージが受信者によって初めて開封されたときに、そのことを知らせる通知メールメッセージです。



(注) 受信者のメールシステムの設定によっては、開封通知が返信されない場合がありますので、開封通知の返送は保証されているわけではありません。受信者が初めてメッセージを開封した日時を確認するには、Encryption Service の Web サイトの [メッセージの管理 (Manage Messages)] 機能を使用してメッセージの詳細を表示します。

アドレス帳の使用

セキュリティで保護されたメッセージを送信する際、頻繁に使用するメールアドレスをアドレス帳に登録すれば、簡単にアクセスできるようになります。アドレス帳を使用して、次の操作を実行できます。

- [アドレス帳へのアドレスの追加 \(19 ページ\)](#)
- [アドレス帳からのアドレスの削除 \(19 ページ\)](#)
- [アドレスの編集 \(19 ページ\)](#)
- [メッセージへのアドレス帳の電子メールアドレスの追加 \(19 ページ\)](#)

アドレス帳へのアドレスの追加

手順

- ステップ1 左側のペインの **[Address Book]** アイコンをクリックして、アドレス帳を開きます。
- ステップ2 連絡先の名、姓、メールアドレスを入力します。
- ステップ3 **[保存 (Save)]** をクリックします。
- ステップ4 新しいアドレスがアドレス帳に追加されます。

アドレス帳からのアドレスの削除

手順

- ステップ1 左側のペインの **[Address Book]** アイコンをクリックして、アドレス帳を開きます。
- ステップ2 削除するアドレスの横にあるごみ箱アイコンをクリックします。
- ステップ3 または、削除するアドレスの横にあるチェックボックスをオンにして、**[Delete Contact]** をクリックします。

アドレスの編集

手順

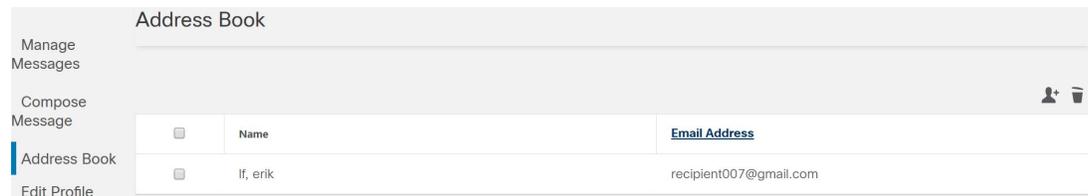
- ステップ1 左側のペインの **[Address Book]** アイコンをクリックして、アドレス帳を開きます。
- ステップ2 編集するアドレスの横にある **[Edit]** アイコンをクリックします。
- ステップ3 連絡先の姓、名、またはメールアドレスを編集し、**[Save]** をクリックします。

メッセージへのアドレス帳の電子メールアドレスの追加

手順

- ステップ1 **[To:]** フィールドをクリックするか、左側ペインの **[Address Book]** アイコンをクリックしてアドレス帳を開きます。

[To]フィールドをクリックすると、アドレス帳が開き、メッセージにメールアドレスを追加できます。



(注) [CC]および[BCC]フィールドをクリックしてアドレス帳を表示し、メッセージにメールアドレスを追加することもできます。

ステップ2 電子メールの宛先となる連絡先のメールアドレスをクリックします。[Compose Message] ページが開き、選択したアドレスが [To:] フィールドに指定されます。

ステップ3 メッセージ（および必要なその他のフィールド）を入力し、[Send] をクリックします。

メッセージの管理

左側のナビゲーションメニューにある [Manage Messages] をクリックして、送信済みの暗号化されたメッセージを管理できます。メッセージを管理する場合は、最初に検索を実行して、送信されたメッセージを取得します。次に、検索結果を使用して、メッセージの詳細の表示、メッセージのロックとロック解除、またはメッセージの有効期限の指定を行います。次の操作を実行できます。

- [すべての送信済みメッセージの取得 \(20 ページ\)](#)
- [特定のメッセージの取得 \(21 ページ\)](#)



(注) メッセージの管理では、送信済みメッセージの詳細を確認したり、アクセスを制限できますが、メッセージの内容を表示することはできません。

すべての送信済みメッセージの取得

送信したすべてのセキュリティで保護されたメッセージリストを取得するには、次のようにします。

手順

ステップ1 左側のナビゲーションメニューから [Manage Messages] をクリックします。[Search Sent Messages] ページが開きます。

ステップ2 **[Keyword]** フィールドは空欄にします。

ステップ3 **[検索 (Search)]** ボタンをクリックします。

ページ下部の結果リストに送信済みメッセージが表示されます。カラムの見出しをクリックすると、表示を並び替えることができます。1ページにつき最大で25件の送信済みメッセージを表示できます。その他のメッセージを表示するには、リンクをクリックします。

特定のメッセージの取得

送信済みのセキュリティで保護されたメッセージのサブセットを検索するには、基本検索または詳細検索を実行します。

基本検索

基本検索を実行する場合、検索するメッセージの **[To]** または **[Subject]** フィールドに含まれているキーワード文字列を入力します。キーワードは大小文字を区別しません。また、どのような文字の組み合わせ（単語の一部、単語、語句など）でも使用できます。

基本検索の実行方法：

手順

ステップ1 左側のナビゲーションメニューから **[Manage Messages]** をクリックします。

ステップ2 **[Keyword]** フィールドに文字列を入力します。

ステップ3 **[検索 (Search)]** ボタンをクリックします。

結果リストには、検索条件に一致するメッセージが表示されます。メッセージが検索条件に一致するのは、

入力したキーワード文字列が **[To]** または **[Subject]** フィールドに含まれている場合です。たとえば、「test」というキーワードで検索した場合、**[To]** または **[Subject]** フィールドに次のような文字列を含むメッセージが結果リストに表示されます。

- test
- TESTS
- testing
- smartest

詳細検索

詳細検索では、キーワード、日付の範囲、メッセージのステータスなどに基づいて検索結果を絞ることができます。

詳細検索の実行方法：

手順

ステップ 1 左側のナビゲーションメニューから **[Manage Messages]** をクリックします。

ステップ 2 **[Advanced Search]** リンクをクリックします。

ステップ 3 指定したい検索条件のフィールドに入力します。

ステップ 4 **[検索 (Search)]** ボタンをクリックします。

次の表は、詳細検索で指定できる条件です。

表 3:

フィールド	説明
Keyword 1	<p>基本検索と同様に、キーワードを入力します。対応するドロップダウンリストを使用して、検索するメッセージデータを指定します。メッセージの [宛先 (To)] フィールド、[件名 (Subject)] フィールド、[ロックされた理由 (Locked Reason)] テキスト、または [試行失敗数 (Failed Attempts)] データを検索できます。</p> <p>たとえば、「機密 (Confidential)」というキーワードを入力し、[件名 (Subject)] を選択することで、[件名 (Subject)] フィールドに「機密 (Confidential)」という言葉が含まれている送信済みメッセージを検索できます。</p>
Keyword 2	<p>キーワード文字列を入力してから、対応するドロップダウンリストを使用して、検索するメッセージデータを指定します。[To] フィールド、[Subject] フィールド、[Locked Reason] テキスト、または [Failed Attempts] データを検索できます。</p> <p>たとえば、「3」と入力し、[試行失敗数 (Failed Attempts)] を選択することで、受信者が 3 回開封を試みて失敗し、ロックされたメッセージを検索できます。</p>

フィールド	説明
[Date From] および [Date To]	検索条件の日付範囲を指定するには、[Date From] および [Date To] フィールドへ日付を入力し、対応するドロップダウンリストからメッセージのステータスを選択します。指定した日付範囲内に送信または開封されたメッセージ、または期限が切れたメッセージを検索できます。設定しない場合は、前月に送信されたメッセージが表示されます。
Status	ステータスに基づいて検索結果を絞るには、メッセージのステータスを選択します。オプションには、[All]、[Opened]、[Unopened]、[Locked]、[Expired]があります。デフォルトは[All]です。

詳細検索の条件を組み合わせて、検索結果を絞り込むことができます。検索条件に含めない場合は、そのフィールドを空欄にしてください。[Status] フィールドのみが必須です。

詳細検索では、「OR」演算子ではなく「AND」演算子を使用して検索条件を組み合わせます。たとえば、[キーワード1 (Keyword 1)] と [キーワード2 (Keyword 2)] フィールドに入力した場合、どちらか片方ではなく、両方のフィールドの条件と一致するメッセージが表示されます。

メッセージの詳細の表示

検索を実行すると、検索条件に一致するメッセージの詳細が結果リストに表示されます。詳細には、受信者のメールアドレス、件名、およびメッセージの送信日時と最初に開封した日時があります。また、メッセージのロックステータスや有効期限も表示されます。すべての時間はグリニッジ標準時 (GMT) で表示されます。

結果リストでは、セキュリティで保護されたメッセージの各受信者がそれぞれ別の行に表示されます。たとえば、暗号化されたメッセージを3人の受信者へ送信した場合、そのメッセージには3行表示されます。

結果リストでメッセージのロックステータスや有効期限を変更できます。ロックの詳細については、[メッセージのロック \(24 ページ\)](#) および [メッセージのロック解除 \(25 ページ\)](#) を参照してください。有効期限の詳細については、次を参照してください。[メッセージの有効期限を設定する \(25 ページ\)](#)

各メッセージの詳細を表示する

それぞれのメッセージの詳細を個別に表示するには、結果リストの件名をクリックします。[Update Sent Message] ページが表示されます。ここでは、結果リストの情報とほぼ同じ詳細情

報が表示されていますが、それに加えてメッセージのロックステータスに関する追加情報が含まれています。

[Update Sent Message] ページには、[To] フィールドにリストされている受信者が初めてメッセージを開封した日時が表示されています。受信者がまだメッセージを開封していない場合は、[Opened Date] フィールドは空白です。

各メッセージの詳細画面では、南京錠アイコンをクリックして、[To] フィールドの受信者のロックステータスを変更できます。また、カレンダーアイコンをクリックして受信者に対するメッセージの有効期限も設定できます。ロックステータスや有効期限を変更したら、[Save] をクリックして変更内容を保存してください。

メッセージをロック/ロック解除する

このトピックでは、次の情報を提供します。

- [メッセージのロック](#) (24 ページ)
- [メッセージのロック解除](#) (25 ページ)

メッセージのロック

受信者がメッセージを開封できないように、送信済みメッセージをロックできます。メッセージがロックされると、受信者はそのメッセージを開封して、暗号化された内容を表示できなくなります。メッセージのロックは受信者ごとに行います。そのため、特定の受信者に対してメッセージをロックできます。

1 つまたは複数のメッセージをロックする方法：

手順

-
- ステップ 1** 左側のナビゲーションメニューから **[Manage Messages]** をクリックします。
 - ステップ 2** **[検索 (Search)]** をクリックしてすべての送信済みメッセージを表示するか、基本検索または詳細検索を実行して、特定のメッセージを表示します。
 - ステップ 3** 結果リストから、ロックするメッセージのチェックボックスをオンにします。

(注) 複数の宛先にメッセージを送信した場合、同じメッセージが複数の行に表示される場合があります。メッセージをロックしたい受信者のチェックボックスをそれぞれオンにします。
 - ステップ 4** 結果リストの上にある **[Lock/Unlock Message]** アイコンをクリックします。[Update Sent Messages] ページが開きます。
 - ステップ 5** **[Lock all selected messages]** オプションが選択されていることを確認してください。
 - ステップ 6** 必要に応じて、メッセージをロックした理由を入力します。

受信者がセキュアメッセージを表示すると、このロックした理由が示されます。

ステップ7 [更新 (Update)] をクリックします。

(注) ロックした理由を指定した場合、受信者がセキュアメッセージを表示しようとする
と、理由が表示されます。ロックした理由の内容を変更する場合は、メッセージの
ロック手順に従って、新しい理由を入力して [Update] をクリックしてください。

セキュアメッセージがロックされると、結果リストの [ロック済み (Locked)] 列に鍵アイコン
が表示されます。

メッセージのロック解除

メッセージのロックを解除する方法：

手順

ステップ1 左側のナビゲーションメニューから [Manage Messages] をクリックします。

ステップ2 [検索 (Search)] をクリックしてすべての送信済みメッセージを表示するか、基本検索または
詳細検索を実行して、特定のメッセージを表示します。

ステップ3 結果リストから、ロックを解除するメッセージのチェックボックスをオンにします。

ステップ4 メッセージの受信者が複数いる場合は、受信者ごとにチェックボックスを選択してください。

ステップ5 結果リストの上にある [Lock/Unlock Message] アイコンをクリックします。[Update Sent Messages]
ページが開きます。

ステップ6 [Unlock selected messages] オプションを選択します。

ステップ7 [更新] をクリックします。

(注) 各メッセージの詳細画面でも、メッセージのロックステータスを変更できます。ロック
ステータスを変更した後は、[Save] をクリックしてください。各メッセージの詳細
表示画面の詳細については、[各メッセージの詳細を表示する \(23 ページ\)](#) を参照し
てください。

メッセージの有効期限を設定する

受信者が特定の日付以降にメッセージを開封できないように、メッセージの有効期限を設定で
きます。通常、有効期限には将来の日付を設定します。メッセージの有効期限日が過ぎると、
受信者はそのメッセージを開封して、暗号化された内容を表示できなくなります。受信者が
メッセージを表示しようすると、メッセージの有効期限が過ぎていることを知らせる通知が
表示されます。

メッセージの管理では、メッセージの有効期限を設定、変更、削除できます。結果リストの
メッセージ情報には、すでに有効期限が切れたメッセージの有効期限日時が赤色で表示されま
す。すべての時間はグリニッジ標準時 (GMT) で表示されます。

メッセージの有効期限を削除する

メッセージの有効期限の設定または変更方法：

手順

-
- ステップ 1** 左側のナビゲーションメニューから **[Manage Messages]** をクリックします。
 - ステップ 2** **[検索 (Search)]** をクリックしてすべての送信済みメッセージを表示するか、基本検索または詳細検索を実行して、特定のメッセージを表示します。
 - ステップ 3** 結果リストから、更新するメッセージのチェックボックスをオンにします。メッセージの受信者が複数いる場合は、該当する受信者の行ごとにチェックボックスをオンにしてください。
 - ステップ 4** 結果リストの上に表示されている **[Update Expiration For Messages]** アイコンをクリックします。**[Update Sent Messages]** ページが開きます。
 - ステップ 5** メッセージの有効期限日時を入力するか、カレンダーアイコンをクリックして有効期限を選択します。
 - ステップ 6** 入力する時間はグリニッジ標準時 (GMT) であることに注意してください。
 - ステップ 7** **[更新]** をクリックします。メッセージの有効期限が結果リストの **[Expires]** カラムに表示されます。
-

メッセージの有効期限を削除する

メッセージの有効期限を削除する方法：

手順

-
- ステップ 1** 左側のナビゲーションメニューから **[Manage Messages]** をクリックします。
 - ステップ 2** **[検索 (Search)]** をクリックしてすべての送信済みメッセージを表示するか、基本検索または詳細検索を実行して、特定のメッセージを表示します。
 - ステップ 3** 結果リストから、更新するメッセージのチェックボックスをオンにします。
 - ステップ 4** メッセージの受信者が複数いる場合は、該当する受信者の行ごとにチェックボックスをオンにしてください。
 - ステップ 5** 結果リストの上に表示されている **[Update Expiration For Messages]** アイコンをクリックします。**[Update Sent Messages]** ページが開きます。
 - ステップ 6** **[New expiration date]** フィールドのテキストを削除します。
 - ステップ 7** **[更新]** をクリックします。

(注) 注：各メッセージの詳細表示画面でも、メッセージの有効期限を設定または削除できません。有効期限を入力または削除したら、**[Save]** をクリックして変更内容を保存してください。各メッセージの詳細表示画面の詳細については、[各メッセージの詳細を表示する \(23 ページ\)](#) を参照してください。

プロフィールの編集

左側のナビゲーションメニューの [プロフィールの編集 (Edit Profile)] を選択すると、Cisco Secure Email Encryption Service (Encryption Service) を使用してユーザーアカウント情報を更新できます。[Edit Profile] ページを更新した後にユーザーアカウントのパスワードを入力し、[Save Profile] をクリックして変更内容を保存します。

実行できるタスクは次のとおりです。

- [ローカルタイムゾーンの設定 \(27 ページ\)](#)
- [個人の詳細と設定の編集 \(27 ページ\)](#)

ローカルタイムゾーンの設定

タイムゾーンは現在のロケーションに基づいて自動的に設定されます。あらかじめタイムゾーンを設定している場合は、自動検出は有効になりません。また、[Time Zone] ドロップダウンメニューから優先タイムゾーンを選択することでタイムゾーンを変更できます。

送信するすべてのメッセージについて、タイムスタンプをローカルタイムゾーンと目的のフォーマット (12 時間または 24 時間) に設定できます。

ローカルタイムゾーンの設定方法：

手順

- ステップ 1 左側のペインで、[Edit Profile] アイコンをクリックします。[Edit Profile] ページが開きます。
- ステップ 2 [Time Zone] ドロップダウンメニューから適切な値を選択します。
- ステップ 3 [Time Format] ドロップダウンメニューから 12 時間または 24 時間を選択します。
- ステップ 4 パスワードを入力して変更を確認します。
- ステップ 5 [Save Profile] をクリックします。

個人の詳細と設定の編集

下図に示すように、次のフィールドで個人の詳細を編集できます。

Edit Profile

Personal Details

First Name*

Last Name*

Email Address

Language

New Password

Confirm Password

Enter a minimum of 8 characters or numbers. Passwords are case-sensitive. Your password must contain both letters and numbers.

If you enter a new password, after your profile is updated you will be required to log in again using your new password.

Time

Time Format

Select to view time in 12- or 24-hour format.

Time Zone

The time zone is set automatically based on your current location. If you have set the time zone previously, the auto-detection will not be enabled. You can also change it by selecting the preferred time zone from the drop-down list. Make sure to save your profile.

Preferences

Auto-open Secure Messages.

BCC me on messages that I send.

Request Read Receipt: Let me know when recipients open their messages.

Please enter your current password to confirm profile changes.

Password*

[Save Profile](#)



(注) デフォルトでは、名前と姓は Encryption Service アカウントから取得されます。

Encryption Service パスワードをリセットし、[プロファイルの保存 (Save Profile)] をクリックすると、Encryption Service アカウントがログアウトされます。その場合は、新しいパスワードを使用して Encryption Service アカウントに再ログインする必要があります。

また、[設定 (Preferences)] の下部にある [パスワード (Password)] に Encryption Service のパスワードを入力し、[プロファイルの保存 (Save Profile)] をクリックして設定することもできます。



第 3 章

セキュアメッセージに関する問題のトラブルシューティング

この章では、次の項目について説明します。

- [トラブルシューティングのヒント \(29 ページ\)](#)
- [関連リソース \(33 ページ\)](#)

トラブルシューティングのヒント

このセクションでは、セキュアメッセージの開封に関する問題のトラブルシューティングのヒントを紹介します。

問題：[開く (Open)] ボタンがメッセージに表示されない、または正常に機能しない

[Open] ボタンが表示されないか正常に機能しない場合、いくつかの原因が考えられます。たとえば、メールアドレスが Cisco Secure Email Encryption Service のユーザーアカウントに関連付けられていない場合は、メッセージに [開く (Open)] ボタンではなく [登録 (Register)] ボタンが表示されることがあります。また、[開く (Open)] ボタンが正常に機能しない場合は、ご使用のコンピュータで Java または JavaScript の実行が設定されていないか、送信中にメッセージが変更された可能性があります。



ヒント メッセージに [登録 (Register)] ボタンが表示されている場合はそれをクリックし、メッセージを受信したメールアドレスに新しいユーザーアカウントを作成してください。



ヒント そのメールアドレスにすでにユーザーアカウントを作成している場合は、パスワードを入力して [オンラインで開く (Open Online)] リンクをクリックし、別の方法でメッセージを開封します。

問題：メールアドレスが [To:] フィールドに表示されない



ヒント [オンラインで開く (Open Online)] を使用しても開封できない場合は、mobile@res.cisco.com 宛てにメッセージを転送してください。サービスから一定期間有効なリンクを含むメールメッセージが送信され、そのリンクをクリックすると、ご使用のコンピュータまたは携帯情報端末 (PDA) で Web ブラウザを介してメッセージを安全に読むことができます。[オンラインで開く (Open Online)] を使用した開封方法や、[転送により開く (Open by Forwarding)] を使用して開封する方法の詳細については、次の URL からセキュアメッセージのオンラインヘルプをご覧ください。 <https://res.cisco.com/websafe/help?topic=RegEnvelope>

問題：メールアドレスが [To:] フィールドに表示されない

セキュアメッセージが複数の宛先に送信された場合には、ユーザーのメールアドレスが [宛先： (To:)] フィールドにすぐに表示されない可能性があります。



ヒント [To:] フィールドの矢印をクリックして、ドロップダウンメニューから自分のメールアドレスを選択してください。



ヒント BCC の宛先としてセキュアメッセージを受信した場合は、[宛先： (To:)] フィールドのドロップダウンメニューにメールアドレスが表示されません。その場合は、[Address not listed] オプションを選択します。次に自分のメールアドレスを入力して [Submit] をクリックし、[To:] フィールドに追加します。

問題：セキュアメッセージが正常に表示されない

暗号化された添付ファイルを開くときに、セキュアメッセージが正しく表示されない場合があります。たとえば、ファイルに不要なテキストまたは HTML マークアップ (<!--、--> など) が含まれている場合もあります。



ヒント セキュアメッセージの表示に問題がある場合は、mobile@res.cisco.com にメッセージを転送してください。Cisco Secure Email Encryption Service からリンクが記載されたメッセージが送信されます。このリンクをクリックすると、暗号化されたメッセージを表示することができます。

問題：メッセージの処理速度が遅い、または停止する

セキュアメッセージの表示や開封の際に、接続問題などが原因で、メッセージ処理が中断される場合があります。その場合は、ツールを読み込み中またはメッセージの復号解読を実行中であることを示す通知が、セキュアメッセージの下に表示されます。数分間待ってもメッセージ

が開かない場合は、処理速度が遅くなっているか、処理が停止した可能性、または添付ファイルのサイズが非常に大きい可能性があります。



ヒント 処理速度が遅くなったり停止した場合は、パスワードを再度入力し、[開く (Open)] をクリックしてください。



ヒント [開く (Open)] を使用しても開封できない場合は、mobile@res.cisco.com宛にセキュアメッセージを転送してください。Cisco Secure Email Encryption Service からリンクが記載されたメッセージが送信されます。このリンクをクリックすると、暗号化されたメッセージを表示することができます。

問題：パスワードを忘れた、またはパスワードが機能しない

パスワードを思い出せない、または覚えているパスワードが正しくない場合は、パスワードをリセットしてください。



ヒント パスワードを忘れた場合は、セキュアメッセージの [パスワードを忘れた場合 (Forgot Password?)] ボタンをクリックして、パスワードをリセットします。Cisco Secure Message Service から、アカウントに関連付けられているメールアドレスに「新しいパスワード (New Password)」というメッセージが送信されます。新しいパスワードメッセージには [Create New Password] ページへのリンクが表示されます。このリンクをクリックすると、新しいパスワードを作成するためのブラウザにリダイレクトされます。アカウントへのログインやセキュアメッセージを開封する際、ここで設定したパスワードを使用します。パスワードをリセットするたびに、Encryption Service アカウントに関連付けられているメールアドレスに通知メールが送信されます。パスワードのリセット時には、セキュリティに関する質問は不要になりました。

会社でシングルサインオン (SAML) ログインを使用できるように設定されている場合に、パスワードを忘れたり紛失したりした際には、そのサポートグループに連絡してパスワードを手またはリセットしてください。



ヒント Cisco Secure Email Encryption Service のパスワードでは、大文字と小文字が区別されます。覚えているパスワードが正しくない場合は、間違っ **て Caps Lock** キーを押していないかを確認してください。それでも問題が解決しない場合は、セキュアメッセージの [パスワードを忘れた場合 (Forgot Password?)] ボタンをクリックして、パスワードをリセットしてください。Cisco Secure Email Encryption Service から、アカウントに関連付けられているメールアドレスに「新しいパスワード (New Password)」というメッセージが送信されます。

問題 : Microsoft OWA 2007 の互換性

互換性を確保するために、OWA 2007 Encryption Service Secure Mail Recipients 用の Microsoft パッチをインストールしてください。

受信した Secure Email Encryption Service のセキュアメッセージを Microsoft OWA 2007 を使用して開封する場合は、サーバー側の管理オプションの設定で HTML/XML フィルタを無効にする必要があります。この HTML フィルタのオプションは、まだリリースされていない Microsoft Exchange 2007 SP1 Rollup 8 で公式にリリースされる予定で、Microsoft ユーザーは Microsoft から暫定的なパッチを入手できます。Microsoft カスタマーサービスとサポートに問い合わせる方法とタイミングについては、次のサイトをご確認ください。

<https://support.microsoft.com/en-us/help/295539>

問題 : 左側のナビゲーションメニューに [Compose Message] リンクが表示されない

アカウント管理者は、[Secure Compose] へのアクセスを無効にできます。アカウント管理者がこの機能を無効にしている場合は、左側のナビゲーションメニューに [メッセージの作成 (Compose Message)] リンクが表示されず、Encryption Service の Web サイトからセキュリティで保護されたメッセージを送信できません。

問題 : セキュアな電子メール（プレーンテキストまたは HTML）でアクセント付き文字が正しくレンダリングされない

問題 : 特定の外国語のアクセント付き文字がメッセージコンテンツで使用されている場合、プレーンテキストまたは HTML 形式のセキュアな電子メールが正しくレンダリングされません。現在、アクセント付き文字は、メッセージの内容に黒いひし形または疑問符 (?) として表示されます。

解決策 : Microsoft Outlook で発信メッセージのエンコーディングオプションを「西ヨーロッパ言語 (Windows)」から「Unicode (UTF-8)」に切り替える必要があります。

手順 :

1. Microsoft Outlook で [File] > [Outlook Options] > [Advanced] > [International Options] セクションに移動します。
2. 発信メッセージの優先エンコーディングオプションとして [Unicode (UTF-8)] を選択します。
3. [Automatically select encoding for outbound messages] チェックボックスをオフにします。

関連リソース

Cisco Secure Email Encryption Service およびセキュアメッセージの詳細については、次の関連リソースを参照してください。

セキュアメッセージのヘルプ

サービスの概要やセキュアメッセージのさまざまな開封方法については、次の URL からセキュアメッセージのヘルプページをご覧ください。

<https://res.cisco.com/websafe/help?topic=RegEnvelope>

FAQ

暗号化された電子メールの開封、Cisco Secure Email Encryption Service への登録、最適なブラウザ設定などに関する一般的な質問の答えは、次の URL の「よく寄せられる質問 (FAQ)」ページからご覧いただけます。

<https://res.cisco.com/websafe/help?topic=FAQ>

カスタマー サポート

Cisco Secure Email Encryption Service のカスタマーサポートにお問い合わせの際は、次のアドレスまでメールをお送りください。

support@res.cisco.com



(注) 電子メールおよび Web チャットで現在使用できる言語は英語とフランス語です。フランス語のサポートは、平日の東部標準時間の午前 8 時から午後 5 時までご利用いただけます。



索引

S

Securedoc.html ファイル [2](#)
説明 [2](#)

あ

アクティブ化 [12](#)
 ユーザーアカウント [12](#)
 電子メールメッセージ [12](#)
アドレスフィールド [6](#)
 説明 [6](#)

か

カスタマー サポート [33](#)
 連絡先情報 [33](#)

せ

セキュア メッセージ [13](#)
 開封の手順 [13](#)

セキュアメッセージ [2, 6, 8, 12-13, 30](#)
 オンライン ヘルプ [6](#)
 コンポーネント [6](#)
 開封の手順 [8, 12](#)
 概要 [2](#)
 処理の問題 [30](#)
 表示の問題 [30](#)
 用途 [2, 13](#)

と

トラブルシューティング [29](#)
 エンベロープの問題 [29](#)

は

パスワード [6, 31](#)
 field [6](#)

め

メッセージのセキュリティレベル [6](#)
 説明 [6](#)

