SOPHOS

Cybersecurity made simple.

Sophos Mobile

スタートアップガイド (Sophos Central)

製品バージョン: 9.6

目次

1 このドキュメントについて

このドキュメントでは、Sophos Mobile をセットアップし、デバイスを管理する方法について詳しく説明します。

Sophos Central 内の Sophos Mobile 製品を対象にしています。

このドキュメントの他のバージョンは、ソフォス Web サイトのSophos Mobile ドキュメントページを参照してください。

2 導入ステップ

Sophos Mobile の導入ステップは次のとおりです。

1. 任意: Mobile Advanced ライセンスをアクティベートして、Sophos Intercept X for Mobile、Sophos Secure Workspace、および Sophos Secure Email を管理します。
2. 個人設定、サポート問い合わせ先情報、セルフサービス ポータルの設定を構成する。
3. iPhone、iPad、および Mac を管理するための Apple Push Notification Service (APNs) の証明書をアップロードする。
4. 任意: スタンドアロン型 EAS プロキシを設定し、管理型のデバイスからメールサーバーに送信されるメールトラフィックのフィルタリングを行う。
5. コンプライアンスポリシーを作成する。
6. デバイスグループを作成する。
7. デバイスを設定する。
8. セルフサービス ポータルの設定を更新する。
9. セルフサービス ポータルでデバイスの登録をテストする。

3 Mobile Advanced ライセンスのアクティベーション

Mobile Advanced ライセンスでは、Sophos Mobile を使用して Sophos Intercept X for Mobile、Sophos Secure Workspace、および Sophos Secure Email を管理できます。

Mobile Advanced ライセンスのアクティベーションは、Sophos Central Admin で行います。

Sophos Central Admin で、アカウント名 (画面の右上) をクリックして、「**ライセンス**」を選択し、「**アクティベーションコードの適用**」フィールドにライセンスキーを入力します。

キーのアクティベーションが完了するとライセンスの詳細が表示されます。

4 設定

次の設定を行います。

- 個人設定 (管理する OS など)
- サポート問い合わせ先情報
- セルフサービス ポータルの設定

4.1 個人設定の指定

Sophos Mobile Admin に表示される内容を変更することができます。たとえば、言語やタイムゾーン、表示されるデバイスのプラットフォームなどを設定できます。

注
この設定は、現在サインインしている管理者アカウントのみに適用されます。

1. サイドバーのメニューの「**設定**」の下の「**セットアップ > 全般**」をクリックし、「**個人設定**」タブをクリックします。
2. 次の設定を行います。

オプション	説明
タイムゾーン	日時を表示するタイムゾーン。
単位	距離単位 (「**メートル**」または「**ヤード・ポンド**」)。
1ページの表示件数	1ページに表示する最大項目数。
エキスパートモード	この設定によって、次のような追加の機能がオンになります。 • 「**デバイスの表示**」ページに「**カスタムプロパティ**」タブが追加され、デバイスのカスタムプロパティが表示されます。 • 「**デバイスの表示**」ページに、「**内部プロパティ**」タブが追加され、デバイスから報告される追加のプロパティが表示されます。 • 複数のポリシー設定ページに、「**詳細設定**」セクションが追加され、オプションの設定を構成できるようになります。
有効なプラットフォーム	表示されるプラットフォーム。 Sophos Mobile Admin では、選択したプラットフォームに関連するページと設定のみが表示されます。

3. 「**保存**」をクリックします。

4.2 IT 問い合わせ情報の設定

問題や質問がある場合、ユーザーが問い合わせることができるよう、IT の問い合わせ情報を設定します。

ここで入力した情報は、ユーザーのデバイスに表示されます。

1. サイドバーのメニューの「**設定**」の下の「**セットアップ > 全般**」をクリックし、「**IT 問い合わせ**」タブをクリックします。
2. 問い合わせ先の情報を入力します。
3. 「**保存**」をクリックします。

5 Android 管理モードの設定

Android デバイスでは、「**ビジネス向け Android**」または「**デバイス管理機能 (レガシー機能)**」管理モードのいずれかを選択できます。

Android 管理モードを設定するには、次の手順を実行します。

1. サイドバーのメニューの「**設定**」の下の「**セットアップ > Android セットアップ**」を選択し、「**Android**」タブを選択します。
2. 「**管理モード**」で、「**ビジネス向け Android**」を選択します。
3. 「**保存**」をクリックします。

次に、ビジネス向け Android を組織に対して設定します。

5.1 ビジネス向け Android の設定 - 概要

組織で使用するためにビジネス向け Android を設定する場合、次の異なるシナリオから選択できます。ビジネス向け Google Play アカウントのシナリオは、ビジネス向け Android を設定する最も簡単な方法であり、このドキュメントで説明しています。

他のビジネス向け Android のシナリオの詳細については、Sophos Mobile 管理者ヘルプを参照してください。

関連情報

Sophos Mobile 管理者ヘルプ

5.2 ビジネス向け Android (ビジネス向け Google Play アカウントシナリオ) の設定

Sophos Mobile の指示に従って、組織に対するビジネス向け Android を設定できます。

1. サイドバーのメニューの「**設定**」の下の「**セットアップ > Android セットアップ**」を選択し、「**ビジネス向け Android**」タブを選択します。
2. 「**設定**」を選択します。
3. 「**「ビジネス向け Google Play アカウント」シナリオ**」を選択した後、「**次へ**」を選択します。
4. 「**アカウントの登録**」を選択します。
   Google Web サイトにリダイレクトされるので、そこでビジネス向け Android に組織を登録します。
5. Google アカウントで Google Web サイトにサインインします。

   注
   専用の Google アカウントを新規作成することを推奨します。

6. Google Web サイトで、指示に従って組織を登録します。

ヒント
組織名を指定する際、名前に Sophos Mobile を含めることを推奨します。例:

組織名 (Sophos Mobile)

登録手順が完了したら、Google Web サイトから Sophos Mobile にリダイレクトされます。

7. Sophos Mobile で「**セットアップの完了**」を選択して登録処理を完了します。

6 Apple Push Notification Service の証明書

iPhone、iPad、および Mac に組み込まれているモバイルデバイス管理 (MDM) プロトコルを使用するには、iOS Push Notification Service (APNs) を使用して、Sophos Mobile に登録されているデバイスとの通信を可能にする必要があります。

APNs 証明書は 1年間有効です。

6.1 APNs 証明書の作成

1. サイドバーのメニューの「**設定**」の下の「**セットアップ > Apple セットアップ**」をクリックし、「**APNs**」タブをクリックします。
2. 「**APNs 証明書のウィザード**」をクリックします。
3. 「**処理モード**」ページで「**新しい APNs 証明書を作成する**」をクリックします。
4. 「**証明書署名要求 (CSR)**」ページで「**証明書署名要求のダウンロード**」をクリックします。
   「apple.csr」という証明書要求ファイルがローカルコンピュータに保存されます。
5. Apple ID を用意します。既に Apple ID をお持ちの場合でも、Sophos Mobile 用に新しい ID を作成することを推奨します。「**Apple ID**」ページで「**Apple のポータルで Apple ID を作成**」をクリックします。
   「Apple ID を作成」という Apple 社の Web ページが開くので、ここで会社用の Apple ID を作成します。

   注
   作成したアカウントのログイン情報は、担当者がアクセスできる、安全な場所に保管します。このログイン情報は、毎年証明書を更新する際に必要となります。

6. ウィザードの「**Apple ID**」フィールドに新しい Apple ID を入力します。
7. 「**証明書**」ページで「**Apple のポータルで証明書を作成**」をクリックします。
   Apple Push Certificates Portal が開きます。
8. Apple ID でログインし、証明書署名要求ファイル「apple.csr」をアップロードします。
9. 「.pem」という拡張子の APNs 証明書ファイルをダウンロードしてコンピュータに保存します。
10. 「**アップロード**」ページで、「**証明書のアップロード**」をクリックし、Apple Push Certificates Portal から取得した「.pem」ファイルを参照します。
11. 「**保存**」をクリックします。

Sophos Mobile は証明書を読み取り、「**APNs**」タブに証明書情報を表示します。

7 スタンドアロン型 EAS プロキシ

EAS プロキシを設定して、管理対象デバイスのメールサーバーへのアクセスを制御できます。管理対象デバイスのメールトラフィックは、そのプロキシ経由で送信されます。コンプライアンスルールに違反しているデバイスなど、デバイスのメールアクセスをブロックできます。

デバイスは、送受信メールサーバーとして EAS プロキシを使用するように設定する必要があります。EAS プロキシは、デバイスが Sophos Mobile の管理下にあり、必要なポリシーが適用されている場合のみ、実際のメールサーバーにトラフィックを転送します。このため、メールサーバーをインターネットからアクセスできるようにする必要がなく、許可したデバイス (パスコードの設定など、適切に設定されているデバイス) のみがメールサーバーにアクセスできるため、より高いレベルのセキュリティを実現できます。また、特定のデバイスからのアクセスをブロックするように EAS プロキシを設定することもできます。

EAS プロキシは、Sophos Mobile から個別にダウンロード、インストールします。HTTPS Web インターフェース経由で Sophos Mobile サーバーと通信します。

スタンドアロン型 EAS プロキシがサポートするメールサーバーの一覧は、Sophos Mobileリリースノートを参照してください。

注
macOS は ActiveSync プロトコルに対応していないため、Mac からのメールトラフィックを EAS プロキシを使用してフィルタリングすることはできません。

機能

- 複数の Microsoft Exchange メールサーバーや IBM Notes Traveler メールサーバーに対応。各メールサーバーごとに 1つの EAS プロキシのインスタンスを設定できます。
- ロードバランサに対応。スタンドアロン型 EAS プロキシのインスタンスを複数のコンピュータに設定し、ロードバランサを使用して、クライアントからのリクエストを分配することができます。
- 証明書を使用したクライアント認証に対応。認証局 (CA) から証明書を選択できます。クライアント証明書はこの証明書から生成されます。
- PowerShell 経由のメールアクセス制御に対応。この場合、EAS プロキシサービスは、PowerShell 経由でメールサーバーと通信して、管理対象デバイスのメールアクセスを制御します。メールトラフィックは、プロキシ経由ではなく、デバイスからメールサーバーに直接送信されます。詳細は、PowerShell 経由のメールアクセス制御の設定 (p. 13)を参照してください。
- EAS プロキシにはデバイスの状態が 24時間保存されます。アップデートを行っている最中など、Sophos Mobile サーバーがオフライン状態の場合は、メールトラフィックは前回のデバイスの状態に基づいてフィルタリングされます。24時間経過すると、すべてのメールトラフィックがブロックされます。

注
iOS 以外のデバイスの場合、IBM Notes Traveler 特有のプロトコルにより、スタンドアロン EAS プロキシのフィルタリング機能が制限されます。iOS 以外のデバイス上の Traveler クライアントは、リクエストごとにデバイス ID を送信しません。デバイス ID のないリクエストは、Traveler サーバーに送信されますが、EAS プロキシはデバイスが承認されているかどうかを検証できません。

7.1 EAS プロキシのインストーラのダウンロード

1. Sophos Central Admin にサインインして、「**モバイル**」を参照します。
2. サイドバーのメニューの「**設定**」の下の「**セットアップ > Sophos セットアップ**」をクリックし、「**EAS プロキシ**」タブをクリックします。
3. 「**外部サーバー**」で、EAS プロキシのインストーラをダウンロードするリンクをクリックします。

インストーラファイルは、ローカルコンピュータに保存されます。

7.2 スタンドアロン型 EAS プロキシのインストール

前提条件:

- 必要なすべてのメールサーバーにアクセスできること。EAS プロキシのインストーラでは、アクセスできないサーバーへの接続は設定されません。
- EAS プロキシをインストールするコンピュータで管理者権限があること。
- Sophos Mobile サーバーの URL がわかっていること。詳細は、Sophos Mobile サーバー URL の確認 (p. 17)を参照してください。

注
「Sophos Mobile サーバー導入ガイド (英語)」には、スタンドアロン型 EAS プロキシを企業のインフラに統合するアーキテクチャの例が掲載されています。スタンドアロン ESA プロキシのインストールと導入を行う前に、同ガイドを参照することをお勧めします。

1. Sophos Mobile EAS Proxy Setup.exe を実行して、「**Sophos Mobile EAS Proxy - Setup Wizard**」(Sophos Mobile EAS プロキシ - セットアップウィザード) を起動します。
2. 「**Choose Install Location**」(インストール先の選択) ページでインストール先フォルダを選択して、「**Install**」(インストール) をクリックしてインストールを開始します。
   インストールが完了すると、「**Sophos Mobile EAS Proxy - Configuration Wizard**」(Sophos Mobile EAS プロキシ - 設定ウィザード) が自動的に起動されるので、指示に従って設定を行います。
3. 「**Sophos Mobile server configuration**」(Sophos Mobile サーバーの設定) ダイアログで、EAS プロキシが接続する Sophos Mobile サーバーの URL を入力します。

   必要に応じて「**Use proxy server**」（プロキシサーバーの使用） を選択して、EAS プロキシが Sophos Mobile サーバーへの接続に使用するプロキシサーバーを設定します。

   また、「**Use SSL for incoming connections (Clients to EAS Proxy)**」(クライアントから EAS プロキシへの受信接続に SSL を使用) を選択して、クライアントと EAS プロキシ間の通信をセキュリティで保護してください。

また、任意で、「**Use client certificates for authentication**」(認証にクライアント証明書を使用) を選択して、クライアントが、EAS プロキシのアカウント情報のほかに証明書を使用して認証するように設定することもできます。これによって、接続のセキュリティが強化されます。

4. 「**Use SSL for incoming connections (Clients to EAS Proxy)**」(クライアントから EAS プロキシへの受信接続に SSL を使用) を選択している場合は、「**Configure server certificate**」(サーバー証明書の設定) ページが表示されます。このページでは、EAS プロキシへの安全なアクセス (HTTPS) に必要な証明書を作成またはインポートします。

   - 信頼できる証明書がない場合は、「**Create self-signed certificate**」(自己署名証明書の作成) を選択します。
   - 信頼できる証明書がある場合は、「**Import a certificate from a trusted issuer**」(信頼できる発行元からの証明書をインポート) をクリックして、リストから次のいずれかのオプションを選択します。
     - **PKCS12 with certificate, private key and certificate chain (intermediate and CA)**
     - **Separate files for certificate, private key, intermediate and CA certificate**
5. 次に表示されるページで、選択した証明書の種類に応じて該当する証明書情報を入力します。

   注
   自己署名証明書の場合は、クライアントデバイスからアクセス可能なサーバーを指定する必要があります。

6. 「**Use client certificates for authentication**」(クライアントから EAS プロキシへの受信接続に SSL を使用) を選択している場合は、「**SMC client authentication configuration**」(サーバー証明書の設定) ページが表示されます。このページでは、認証局 (CA) からの証明書を選択します。クライアント証明書はこの証明書から生成されます。

   クライアントが接続を試行すると、クライアントの証明書が、ここで指定した CA から生成された証明書かどうかが、EAS プロキシによってチェックされます。
7. 「**EAS Proxy instance setup**」(EAS プロキシ インスタンスのセットアップ) ページで、1つまたは複数の EAS プロキシのインスタンスを設定します。

   - **Instance type** (Secure Email から送信される EWS サブスクリプションのリクエストの許可): 「**EAS proxy**」を選択します。
   - **Instance name**: インスタンスの識別に使用される名前。
   - **Server port** (Secure Email から送信される EWS サブスクリプションのリクエストの許可): 受信メールトラフィック用の EAS プロキシのポート。複数のプロキシのインスタンスを設定する場合は、各インスタンスに対して異なるポートを指定する必要があります。
   - **Require client certificate authentication** (Secure Email から送信される EWS サブスクリプションのリクエストの許可): メールクライアントは、EAS プロキシに接続する際に認証が必要です。
   - **ActiveSync server** (Secure Email から送信される EWS サブスクリプションのリクエストの許可): プロキシのインスタンスが接続する Exchange ActiveSync サーバーのインスタンスの名前や IP アドレス。
   - **SSL** (Secure Email から送信される EWS サブスクリプションのリクエストの許可): プロキシのインスタンスと Exchange ActiveSync サーバー間の通信は、SSL または TLS (サーバーの対応状況に依存) で保護されます。
   - **Allow EWS subscription requests from Secure Email** (Secure Email から送信される EWS サブスクリプションのリクエストの許可): このオプション選択して、iPhone および iPad 上の Sophos Secure Email アプリが、EWS (Exchange Web Service) 経由のプッシュ

通知に登録できるようにします。プッシュ通知は、Sophos Secure Email に関するメッセージを受け取るとデバイスに通知を表示します。

注

- セキュリティ上の理由から、EAS プロキシは、Exchange サーバーの EWS インターフェースへのリクエストすべてをデフォルトでブロックします。このチェックボックスを選択すると、サブスクリプションのリクエストが許可されます。それ以外のリクエストのブロックは解除されません。
- Exchange サーバーの EWS を設定する方法について詳細は、ソフォスのサポートデータベースの文章 127137 を参照してください。

- **Enable Traveler client access** (Secure Email から送信される EWS サブスクリプションのリクエストの許可): このチェックボックスは、iOS 以外のデバイス上の IBM Notes Traveler クライアントにアクセスを許可する必要がある場合のみに選択します。

8. インスタンス情報を入力して、「**Add**」(追加) をクリックしてインスタンスを「**Instances**」(インスタンス) リストに追加します。
   各プロキシのインスタンスに対して、Sophos Mobile サーバーにアップロードが必要な証明書がインストーラによって作成されます。「**Add**」(追加) をクリックすると、証明書のアップロード方法を説明するメッセージウィンドウが表示されます。
9. メッセージウィンドウで、「**OK**」をクリックします。
   これによって、証明書の作成先フォルダがダイアログに表示されます。

注

このダイアログは、該当するインスタンスを選択して、「**EAS Proxy instance setup**」(EAS プロキシ インスタンスのセットアップ) ページの「 **Export config and upload to Sophos Mobile server**」(設定をエクスポートして SMC にアップロード) リンクをクリックしても表示できます。

10. 証明書フォルダの詳細をメモします。この情報は、証明書を Sophos Mobile へアップロードする際に必要になります。
11. 任意: 「**Add**」(追加) を再クリックして、EAS プロキシの追加インスタンスを設定します。
12. 必要な EAS プロキシのインスタンスすべてを設定したら、「**Next**」(次へ) をクリックします。
    入力したサーバーポートがテストされ、Windows ファイアウォールの受信の規則が設定されます。
13. 「**Allowed mail user agents**」(許可するメール ユーザー エージェント) ページで、EAS プロキシへの接続が許可されているメール ユーザー エージェント (つまり、メール クライアント アプリケーション) を指定します。クライアントが、ここで指定されていないメールアプリケーションを使用して EAS プロキシにが接続しようとすると、要求は拒否されます。
    - すべてを許可する場合は、「**Allow all mail user agents**」(すべてのメール ユーザー エージェントを許可する) を選択します。
    - 「**Only allow the specified mail user agents**」(指定したメール ユーザー エージェントのみを許可する) を選択して、一覧からメール ユーザー エージェントを選択します。「**Add**」(追加) をクリックして、許可するエージェントの一覧に追加します。EAS プロキシへの接続を許可するメール ユーザー エージェントすべてに対して、この手順を繰り返します。
14. 「**Sophos Mobile EAS Proxy - Configuration Wizard finished**」(Sophos Mobile EAS Proxy - 設定ウィザードが完了しました) ページで、「**Finish**」(完了) をクリックして設定ウィザードを閉じて、セットアップウィザードに戻ります。

15. セットアップウィザードで、「**Start Sophos Mobile EAS Proxy server now**」(Sophos Mobile EAS プロキシサーバーを今すぐ起動) が選択されていることを確認した後、「**Finish**」(完了) をクリックして設定を完了し、EAS プロキシを初回起動してください。

EAS プロキシの設定を完了するには、各プロキシのインスタンスに対して作成された証明書を Sophos Mobile にアップロードします。

16. Sophos Central Admin にサインインして、「**モバイル**」を参照します。
17. サイドバーのメニューの「**設定**」の下の「**セットアップ > Sophos セットアップ**」をクリックし、「**EAS プロキシ**」タブをクリックします。
18. 「**外部サーバー**」で、「**ファイルのアップロード**」をクリックします。設定中に作成した証明書をアップロードします。

    インスタンスを複数設定した場合は、各インスタンスの証明書についてもこの手順を繰り返します。
19. 「**保存**」をクリックします。
20. Windows で「**サービス**」ダイアログを開いて、「**EASProxy**」サービスを起動します。

これで、スタンドアロン型 EAS プロキシの初期セットアップが完了しました。

注
EAS プロキシのログのエントリは、毎日 EASProxy.log.yyyy-mm-dd という命名規則で作成されるファイルに移動されます。毎日作成されるこのログは自動削除されないため、将来、空きディスク容量が不足する可能性があります。ログファイルをバックアップフォルダに移動する手順を設定することを推奨します。

7.3 PowerShell 経由のメールアクセス制御の設定

スタンドアロンの EAS プロキシを PowerShell モードで設定すると、PowerShell 経由で Exchange メールサーバーに接続し、デバイスのコンプライアンス状態に基づいてメールアクセスを設定します。

PowerShell モードでは、メールトラフィックはプロキシなしで Exchange メールサーバーからデバイスに直接送信されます。通信フローに関する図は、「Sophos Mobile テクニカルガイド」を参照してください。

PowerShell モードの利点:

- Sophos Mobile サーバーで、デバイスからの受信メールトラフィックに対してポートを開放する必要がありません。
- Sophos Mobile に未登録のデバイスによるメールアクセスを阻止することができます。

Exchange メールサーバーは、オンプレミス版の Exchange Server、または Office 365 の一部である Exchange Online のいずれかです。対応しているバージョンは次のとおりです

- Exchange Server 2013
- Exchange Server 2016
- Office 365 (Exchange Online プランを含む)

制約事項
macOS は ActiveSync プロトコルに対応していないため、Mac によるメールアクセスを、PowerShell を使用して制御することはできません。

PowerShell 経由でメールアクセス制御を設定するには、次の手順を実行します。

関連情報

Sophos Mobile テクニカルガイド (Sophos Central) (英語)

PowerShell の設定

1. 任意: 必要に応じて、EAS プロキシをインストールするコンピュータに Windows PowerShell をインストールします。
2. 管理者権限で PowerShell を開き、次のコマンドを実行します。

   Set-ExecutionPolicy RemoteSigned

Exchange Server の場合は、追加の設定が必要です。

3. Exchange 管理シェルを開きます。
4. PowerShell 実行ポリシーを設定します。

   Set-ExecutionPolicy RemoteSigned

5. PowerShell 仮想ディレクトリの名前を取得します。

   Get-PowerShellVirtualDirectory -Server <サーバー名>

   <サーバー名> は、Exchange Server がインストールされているコンピュータの名前です。

   標準インストールでは、PowerShell 仮想ディレクトリは PowerShell (Default Web Site) です。

6. PowerShell 仮想ディレクトリに基本認証を設定します。

   Set-PowerShellVirtualDirectory -Identity "PowerShell (Default Web Site)" -BasicAuthentication $true

関連情報

Windows PowerShell のインストール （Microsoft の文章）

Exchange 管理シェルを開く (Microsoft の文章)

サービスアカウントの作成

サービスアカウントは、PowerShell コマンドの実行に Sophos Mobile が使用する、Exchange メールサーバー上の特別なユーザーアカウントです。

1. 該当する管理コンソールにサインインします。
   - Exchange Server の場合: **Exchange 管理者センター**
   - Exchange Online の場合: **Office 365 管理者センター**
2. ユーザーアカウントを作成します。
   - smc_powershell など、アカウントの用途を明確にするユーザー名を使用します。
   - ユーザーが次回ログオンした際にパスワードの変更を要求する設定をオフにします。
   - 新しいアカウントに、自動的に割り当てられた Office 365 のライセンスを削除します。サービスアカウントにライセンスは必要ありません。
3. 新しいロールグループを作成して、必要なパーミッションを許可します。
   - smc_powershell などのようなロールグループ名を使用します。
   - 「**Mail Recipients**」(メール受信者) ロールおよび「**Organization Client Access**」(組織クライアントアクセス) ロールを追加します。
   - ユーザーアカウントをメンバーとして追加します。

PowerShell 接続の設定

1. スタンドアロンの EAS プロキシをインストールするのと同様に、セットアップアシスタントを使用します。「**EAS Proxy instance setup**」(EAS プロキシ インスタンスのセットアップ) ページで次の設定を行います。
   - **Instance type**: 「**PowerShell Exchange/Office 365**」を選択します。
   - **Instance name**: インスタンスの識別に使用される名前。
   - **Exchange server**: Exchange Server の場合は、サーバーの名前や IP アドレスを入力します。

     Exchange Online の場合、グローバル Office 365 サービスを使用している場合は、outlook.office365.com と入力します。Office 365 Germany など、他のサービスを使用している場合は、Microsoft の文章、Exchange Online PowerShell に接続するでアドレスを参照してください。

     名前にプロトコル「https://」やサフィックス「/powershell-liveid」は指定しないでください。これは、セットアップウィザードによって自動的に追加されます。
   - **Allow all certificates**: EAS プロキシはサーバー証明書を検証しません。Exchange Server を自己署名証明書とともに使用している場合などは、このオプションを選択してください。

     警告
     この設定によって、メールサーバー接続のセキュリティが低下します。 ネットワーク環境で必要な場合のみに選択してください。

   - **Service account**: Exchange Server や Exchange Online 管理コンソールで作成したユーザーアカウントの名前。
   - **Password**: ユーザーアカウントのパスワード。
2. 「**Add**」(追加) をクリックして、「**Instances**」(インスタンス) リストにインスタンスを追加します。
3. PowerShell を使用して他の Exchange Server のインスタンスに接続するには、上記の手順を繰り返します。
4. セットアップを完了します。
5. 任意: 必要に応じて、EAS プロキシが Exchange Server や Exchange Online への接続に使用するプロキシサーバーを設定します。EAS プロキシをインストールしたコンピュータで、「**管理者として実行**」オプションを使用してコマンドプロンプトを開き、次のコマンドを入力します。

   netsh winhttp set proxy <サーバー名または IP>:<ポート>

   警告
   このコマンドによって、システム全体のプロキシが設定されます。コンピュータで実行されている他のプログラムにも影響を与える可能性があります。

関連情報

スタンドアロン型 EAS プロキシのインストール (p. 10)
Exchange Online PowerShell に接続する (Microsoft の文章)

PowerShell 証明書のアップロード

PowerShell を使用した Sophos Mobile への接続の証明書をアップロードします。

1. Sophos Central Admin にサインインして、「**モバイル**」を参照します。
2. サイドバーのメニューの「**設定**」の下の「**セットアップ > Sophos セットアップ**」をクリックし、「**EAS プロキシ**」タブをクリックします。
3. 任意: 「**全般**」で、「**Sophos Secure Email に制限**」を選択して Android および iOS 向けの Sophos Secure Email アプリへのメールアクセスを制限します。
4. 「**外部サーバー**」で、「**ファイルのアップロード**」をクリックします。設定中に作成した証明書をアップロードします。

   インスタンスを複数設定した場合は、各インスタンスの証明書についてもこの手順を繰り返します。
5. 「**保存**」をクリックします。
6. Windows で「**サービス**」ダイアログを開いて、「**EASProxy**」サービスを起動します。

7.4 管理下にないデバイスのメールアクセスのブロック

Sophos Mobile に未登録のデバイスによるメールアクセスを阻止することができます。

前提条件: スタンドアロンの EAS プロキシを PowerShell モードで設定していること。

ここにある手順で Exchange とは、オンプレミス版の Exchange サーバー、または Office 365 に含まれている Exchange Online プランを指します。

管理下にないデバイスが隔離されるように Exchange を設定できます。ユーザーには、デバイスを Sophos Mobile に登録することを指示するメールが送信されます。登録されたデバイスは、隔離から自動的に解除されます。

警告
ここでの設定を運用環境に適用する前に、デバイスが登録済みで、Sophos Mobile と同期できることを確認してください。すべてのデバイスはデフォルトで隔離され、コンプライアンスに準拠していると Sophos Mobile サーバーが判断した場合のみにメールアクセスが許可されます。

また、EAS プロキシがデバイスのコンプライアンス状態を把握していない場合も、登録済みデバイスは隔離されます。これは、デバイスが Sophos Mobile と長期間に渡って同期していない場合、または EAS プロキシが Sophos Mobile サーバーと通信できない場合に発生することが考えられます。

管理下にないデバイスのメールアクセスをブロックする方法は次のとおりです。

1. Exchange 管理シェルを開く (Exchange サーバーを使用している場合）、または Exchange Online PowerShell に接続します。

   詳細は、関連情報のリンクを参照してください。
2. 次のコマンドを実行します (1行に入力)。

```
Set-ActiveSyncOrganizationSettings -DefaultAccessLevel quarantine
-UserMailInsert "デバイスを Sophos Mobile に登録してください。"
```

-UserMailInsert で指定するテキストは、デバイスの隔離時に Exchange によってユーザーに送信される通知メールに追加されます。

一般的なメールアクセス制御の詳細は、Microsoft の文章、許可/ブロック/隔離リストを使用した Exchange ActiveSync デバイスのアクセス制御 (英語) を参照してください。

関連情報

スタンドアロンの EAS プロキシの PowerShell モードでの設定 (p. 13)
スタンドアロンの EAS プロキシを PowerShell モードで設定すると、PowerShell 経由で Exchange メールサーバーに接続し、デバイスのコンプライアンス状態に基づいてメールアクセスを設定します。

Exchange 管理シェルを開く (Microsoft の文章)
Exchange Online PowerShell に接続する (Microsoft の文章)
許可/ブロック/隔離リストを使用した Exchange ActiveSync デバイスのアクセス制御 (Microsoft の文章)

7.5 スタンドアロン型 EAS プロキシサーバーとの接続の設定

Sophos Mobile とスタンドアロン型 EAS プロキシとの接続を設定するには、EAS プロキシのサーバー証明書を Sophos Mobile にアップロードします。証明書は、EAS プロキシのインスタンスを設定する際に生成されます。

スタンドアロン型 EAS プロキシのインストールと設定に関する詳細は、スタンドアロン型 EAS プロキシ (p. 9)を参照してください。

警告
証明書をアップロードする前に EAS プロキシをインストールすると、Sophos Mobile でサーバーとの接続が拒否され、サービスの開始に失敗します。

スタンドアロン型 EAS プロキシの証明書をアプロードする方法は次のとおりです。

1. サイドバーのメニューの「**設定**」の下の「**セットアップ > Sophos セットアップ**」をクリックし、「**EAS プロキシ**」タブをクリックします。
2. 任意: 「**全般**」で、「**Sophos Secure Email に制限**」を選択して Android および iOS 向けの Sophos Secure Email アプリへのメールアクセスを制限します。
3. 「**外部サーバー**」で、「**ファイルのアップロード**」をクリックし、証明書ファイルを参照します。

   複数の EAS プロキシのインスタンスを設定した場合は、すべてのインスタンスについて、この手順を繰り返します。
4. 「**保存**」をクリックします。
5. Windows で「**サービス**」ダイアログを開いて、「**EASProxy**」サービスを起動します。

7.6 Sophos Mobile サーバー URL の確認

スタンドアロンの EAS プロキシを設定するには、Sophos Mobile サーバーの URL が必要です。URL は、Sophos Mobile のシステム設定に表示されます。

1. Sophos Central Admin にサインインして、「**モバイル**」を参照します。

2. サイドバーのメニューの「**設定**」の下の「**セットアップ > Sophos セットアップ**」をクリックし、「**EAS プロキシ**」タブをクリックします。

「**外部サーバー**」で、Sophos Mobile サーバーの URL が表示されます。

8 コンプライアンスポリシー

コンプライアンスポリシーでは以下の設定を行うことができます。

- デバイスに対して特定の設定を許可、禁止、または強制的に適用する。
- コンプライアンスルールに違反した際に実行するアクションを定義する。

コンプライアンスポリシーは、デバイスグループ別に作成・適用できます。このため、管理下のデバイスに異なるレベルのセキュリティを適用することが可能です。

ヒント
会社貸与と私物の両方のデバイスを管理する場合は、少なくともこの 2種類のデバイスに対して異なるコンプライアンスポリシーを指定することを推奨します。

8.1 コンプライアンスポリシーの作成

1. サイドバーのメニューで、「**デバイス設定**」の下の「**コンプライアンスポリシー**」をクリックします。
2. 「**コンプライアンスポリシー**」ページで「**コンプライアンスポリシーの作成**」をクリックした後、ポリシーの基となるテンプレートを選択します。
   - **デフォルトテンプレート**: コンプライアンスルールが選択されていますが、アクションは定義されていません。
   - **PCI テンプレート**、**HIPAA テンプレート**: それぞれ、HIPAA および PCI DSS のセキュリティ基準に基づいた、コンプライアンスルールおよびアクションが選択されています。

   ここでどのテンプレートを選択しても、後で設定できるオプションは同じです。
3. 新しいコンプライアンスポリシーの名前を入力し、必要に応じて説明を入力します。

必要なプラットフォームすべてに対して次の手順を繰り返します。

4. 各タブの「**有効化する**」チェックボックスが選択されていることを確認します。
   このチェックボックスが選択されていないと、対応するプラットフォームに対してコンプライアンスチェックが行われません。
5. 「**ルール**」で選択したプラットフォームに対するコンプライアンスルールを設定します。
   各種のデバイスに対して利用可能なルールの説明は、画面右上の「**ヘルプ**」をクリックします。

注
各コンプライアンスルールには重要度のレベルが設定されており (高、中、低)、青い色のバーで表示されます。重要度のレベルは、ルールの重要性や違反時に実行するアクションを評価するうえで役立ちます。

注
デバイス全体ではなく、Sophos コンテナのみが Sophos Mobile の管理下にあるデバイスの場合は、コンプライアンスルールは一部分のみが適用されます。「**ルールのハイライト表示**」で、項目をハイライト表示する管理タイプを選択します。

6. 「**違反時のアクション**」の下の項目では、ルール違反が発生した場合に実行するアクションを設定します。

オプション	説明
メール接続を拒否	メールへのアクセスを禁止します。 このアクションは、スタンドアロンの EAS プロキシとの接続を設定した場合のみに実行できます。詳細は、スタンドアロン型 EAS プロキシサーバーとの接続の設定 (p. 17)を参照してください。 このアクションは、Android デバイス、iOS デバイス、Windows デバイス、および Windows Mobile デバイスのみに対して実行できます。
コンテナをロック	Sophos Secure Workspace および Secure Email アプリを無効化します。無効化により、これらのアプリで管理されるドキュメント、メール、および Web サイトの閲覧に影響が生じます。 このアクションは、Mobile Advanced ライセンスをアクティベートした場合のみに実行できます。 このアクションは、Android デバイス、iPhone および iPad のみに対して実行できます。
セキュリティ状態の設定	デバイスがこのルールに違反した場合に適用するセキュリティ状態 (**赤**、**黄**、**緑**) を選択します。デバイスが複数のルールに違反した場合は、そのルールに設定されているセキュリティ状態のなかから最も深刻なものが適用されます。 Sophos Mobile は、Sophos Wireless にセキュリティ状態を報告します。Sophos Wireless の設定に応じて、ネットワークアクセスが制限されます。 このアクションは、Synchronized Security をオンにした場合、Android デバイス、iPhone および iPad で使用できます。
警告の作成	警告が送信されます。 送信された警告は、Sophos Central Admin の「**警告**」ページに表示されます。
タスクバンドルの配信	特定のタスクバンドルをデバイスに配信します。 この段階では、この項目は「**なし**」に設定することを推奨します。詳細は、「Sophos Mobile 管理者ヘルプ」を参照してください。 **注意** タスクバンドルを誤って配信すると、デバイスの設定が変更されたり、ワイプされてしまうこともあります。コンプライアンス設定のルールに正しいタスクバンドルを割り当てるには、システムに関する深い知識が必要です。

注
ビジネス向け Android のフル マネージド デバイスが、ポリシーに準拠しなくなると、すべてのアプリが無効になります。

7. 必要なプラットフォームすべての設定が完了したら、「**保存**」をクリックして指定した名前でコンプライアンスポリシーを保存します。

コンプライアンスポリシーはデバイスグループに適用して使用します。この方法は次のセクションで説明します。

9 デバイスグループ

デバイスグループを使用してデバイスを分類することができます。分類することで、個々のデバイスではなく、グループ全体に対してタスクを実行できるため、デバイス管理の効率が上がります。

デバイスは常に 1つのデバイスグループに所属できます。デバイスを Sophos Mobile に追加する際、デバイスグループに割り当てます。

ヒント
1つのグループには、同じプラットフォーム環境のデバイスのみを追加してください。グループを使用して、インストールやその他のプラットフォーム固有のタスクを実行する際に便利です。

9.1 デバイスグループの作成

1. サイドバーのメニューの「**管理**」の下で、「**デバイスグループ**」、「**デバイスの作成**」の順にクリックします。
2. 「**デバイスグループの編集**」ページで、新しいデバイスグループの名前と説明を入力します。
3. 「**コンプライアンスポリシー**」で、会社貸与デバイスと私物デバイスに適用されているコンプライアンスポリシーを選択します。
4. 「**保存**」をクリックします。

注
デバイスグループの設定には、「**iOS の自動登録を有効にする**」というオプションがあります。このオプションを有効にすると、Apple Configurator がインストールされている iPhone および iPad を登録できるようになります。詳細は、「Sophos Mobile 管理者ヘルプ」を参照してください。

新しいデバイスグループが作成され、「**デバイスグループ**」ページに表示されます。

10 デバイスのポリシーの作成

ポリシースタートアップウィザードにより、すべてのプラットフォームに対して基本的なデバイスのポリシーを作成することができます。詳細なポリシーの設定は後から行うことができます。

制約事項
ここでの手順は、Chrome デバイスは対象にしていません。

「**ポリシースタートアップ**」ウィザードを使用してポリシーを作成する方法は次のとおりです。

1. ダッシュボードで、「**作業開始のタスク**」というウィジェットの「**ポリシー スタートアップ ウィザード**」をクリックします。

   ヒント
   ウィジェットが表示されていない場合は、「**ウィジェットの追加 > 作業の開始**」をクリックします。

2. 「**プラットフォーム**」ページで、ポリシーを作成するデバイスのプラットフォームを選択します。
   「**Android**」と「**iOS/iPadOS**」を選択します。
3. **Android** の場合、管理モードを選択できます。
   この設定によって利用できるポリシーの種類が異なります。**ビジネス向け Android**モードを使用することを推奨します。
4. 「**ポリシー**」ページで次の設定を行います。
   a) ポリシー名を入力します。
      選択した各プラットフォームに対して、この名前でポリシーが作成されます。
   b) ポリシーで管理する項目を選択します。
      チェックボックスのチェックを外すと、該当するウィザードの設定ページはスキップされます。スキップされた項目やその他の項目は、後から設定することができます。
      少なくとも「**パスワードの要件**」および「**制限**」を選択することを推奨します。
5. 「**パスワード**」ページで、デバイスのパスワードの要件を設定します。
6. 「**制限**」ページで、デバイスに適用する制限を設定します。たとえば、カメラの使用など、セキュリティ上のリスクになり得るデバイスの機能を制限できます。
7. 「**Wi-Fi**」ページで、組織の Wi-Fi ネットワークへの接続を設定します。
   Wi-Fi ネットワークのセキュリティの種類が、「**WPA/WPA2 PSK**」以外の場合は、後からこの設定を変更することができます。
8. 「**メール**」ページで、組織の Exchange メールサーバーへの接続を設定します。
   プレースホルダ「%_USERNAME_%」および「%_EMAILADDRESS_%」は、デバイスに割り当てられているユーザーの名前とメールアドレスに置き換えられます。
9. 「**完了**」をクリックします。

選択した各プラットフォームに対してポリシーが作成されます。

ポリシーを表示するには、サイドバーのメニューの「**ポリシー**」をクリックして、デバイスのプラットフォームをクリックします。

管理する項目を変更するには、ポリシー名をクリックして「**設定の追加**」をクリックします。

デバイスを登録する前に、まず組織をビジネス向け Android に登録する必要があります。詳細は、「Sophos Mobile 管理者ヘルプ」を参照してください。

11 Android デバイス用のタスクバンドルの作成

管理する Android、iOS、およびその他のデバイスプラットフォームに対して、それぞれ個別のタスクバンドルを作成します。

Android デバイス用の登録タスクバンドルを作成する方法は次のとおりです。

1. サイドバーのメニューの「**デバイス設定**」で、「**タスクバンドル > Android**」を選択します。
2. 「**タスクバンドル**」ページで、「**タスクバンドルの作成**」を選択します。
3. 「**タスクバンドルの編集**」ページで、タスクバンドルの名前、および任意でタスクバンドルの説明を入力します。

   バージョン番号は、タスクバンドルを保存するたびに自動で増えていきます。
4. 任意: 「**違反時にアクションの選択が可能**」を選択した場合、ポリシーに違反したデバイスにタスクバンドルを転送することができます。

   これは、コンプライアンスポリシーで行います。
5. 「**タスクの追加 > 登録**」を選択します。タスクバンドルに登録タスクを追加する手順が表示されます。

   a) 任意: タスクの名前を変更します。

   ここで入力した名前は、デバイスのが登録後に、セルフサービス ポータルに表示されます。

   b) 登録タイプを選択します。

   このタスクバンドルを使用して、ビジネス向け Android のフル マネージド デバイスを登録するには「**フルデバイス**」を選択します。

   c) 次のページで、登録後にデバイスに割り当てるポリシーを選択します。

   選択した登録タイプと一致するポリシーのみが表示されます。

   d) 「**完了**」を選択します。
6. 任意: Exchange、VPN、または Wi-Fi 設定に対して、それぞれ異なるポリシーを設定した場合などは、「**タスクの追加 > ポリシーの割り当て**」を選択して、タスクバンドルにさらにポリシーを追加します。
7. 任意: アプリをインストールしたり、デバイスにメッセージを表示したりする場合は、タスクバンドルにさらにタスクを追加します。
8. 任意: 選択したタスクがインストールされる順序は、タスクのリストの右側にある矢印を使って変更できます。

12 iPhone および iPad 用のタスクバンドルの作成

管理する Android、iOS、およびその他のデバイスプラットフォームに対して、それぞれ個別のタスクバンドルを作成します。

iPhone および iPad 用の登録タスクバンドルを作成する方法は次のとおりです。

1. サイドバーのメニューの「**デバイス設定**」で、「**タスクバンドル > iOS/iPadOS**」を選択します。
2. 「**タスクバンドル**」ページで、「**タスクバンドルの作成**」を選択します。
3. 「**タスクバンドルの編集**」ページで、タスクバンドルの名前、および任意でタスクバンドルの説明を入力します。

   バージョン番号は、タスクバンドルを保存するたびに自動で増えていきます。
4. 任意: 「**違反時にアクションの選択が可能**」を選択した場合、ポリシーに違反したデバイスにタスクバンドルを転送することができます。

   これは、コンプライアンスポリシーで行います。
5. 任意: アプリのインストールに失敗しても、タスクバンドルのプロセスを続行する場合は、「**アプリのインストールの失敗を無視**」を選択します。

   このオプションは、タスクバンドルに「**アプリのインストール**」タスクが含まれている場合のみに使用できます。
6. 「**タスクの追加 > 登録**」を選択します。タスクバンドルに登録タスクを追加する手順が表示されます。

   a) 任意: タスクの名前を変更します。

      ここで入力した名前は、デバイスのが登録後に、セルフサービス ポータルに表示されます。

   b) 登録タイプを選択します。

      このタスクバンドルを使用してフル マネージド デバイスを登録するには「**フル MDM**」を選択します。

   c) 次のページで、登録後にデバイスに割り当てるポリシーを選択します。

      選択した登録タイプと一致するポリシーのみが表示されます。

   d) 「**完了**」を選択します。
7. 任意: Exchange、VPN、または Wi-Fi 設定に対して、それぞれ異なるポリシーを設定した場合などは、「**タスクの追加 > ポリシーの割り当て**」を選択して、タスクバンドルにさらにポリシーを追加します。
8. 任意: アプリをインストールしたり、デバイスにメッセージを表示したりする場合は、タスクバンドルにさらにタスクを追加します。
9. 任意: 選択したタスクがインストールされる順序は、タスクのリストの右側にある矢印を使って変更できます。

13 セルフサービス ポータルの設定の作成

セルフサービス ポータルの設定では、ユーザーが登録できるデバイスの種類、登録の詳細、およびセルフサービス ポータルで実行できるデバイスのアクションを指定します。

ユーザーごとに異なるセルフサービス ポータルの設定を使用できます。これを行うには、ユーザーをユーザーグループに追加し、そのグループを設定に関連付けます。ユーザーグループの詳細については、関連情報を参照してください。

ユーザーが、セルフサービス ポータルの設定に関連付けられている複数のグループに所属している場合は、最も優先度の高い設定が適用されます。

セルフサービス ポータルの設定を作成する方法は次のとおりです。

1. サイドバーのメニューの「**設定**」で、「**セットアップ > セルフサービス ポータル**」を選択します。
2. 「**登録テキスト**」を選択して利用条件と登録後処理テキストを追加します。
   これらのテキストをセルフサービスポータルの設定に追加すると、デバイスの登録前と登録後に、それぞれのテキストが表示されます。
3. 「**セルフサービス ポータルの設定**」ページで、「**追加**」を選択して設定を作成します。
4. 次の設定を行います。

オプション	説明
名前	設定の名前。 セルフサービスポータルで、ユーザーが設定を選択する画面に表示されます。
ユーザーグループ	「**追加**」を選択してユーザーグループを入力します。指定したグループのすべてのメンバーに設定内容が適用されます。
デバイスの最大数	1人のユーザーがセルフサービス ポータルで登録できるデバイスの最大数を選択します。
アクション	「**表示**」を選択して、ユーザーがセルフサービス ポータルで実行できる管理操作を選択します。

5. 「**追加 > Android**」を選択します。
6. 「**プラットフォームの設定**」ダイアログで、次の設定を行います。

オプション	説明
表示名	プラットフォームの設定の名前。 セルフサービスポータルで、ユーザーが登録の種類を選択する画面に表示されます。
説明	プラットフォームの設定の説明。 表示名の横に表示される説明文です。
所有者	この設定で登録されているデバイスの所有者モード (会社または個人)。

オプション	説明
デバイスグループ	デバイスが属するデバイスグループ。
登録パッケージ	作成した Android のタスクバンドルを選択します。
利用条件	登録をする前にセルフサービスポータルに表示するテキスト。 何も表示しない場合は、このフィールドを空白のままにします。 登録を続行するには、ユーザーはテキストの内容に同意する必要があります。
登録後処理テキスト	登録をした後にセルフサービスポータルに表示するテキスト。 何も表示しない場合は、このフィールドを空白のままにします。

7. 「**適用**」を選択して、プラットフォームの設定をセルフサービス ポータルの設定に追加します。
8. 「**追加 > iOS/iPadOS**」を選択して、Android に対して同じステップを繰り返し、設定を行います。
9. 「**セルフサービス ポータルの設定の編集**」ページで、「**保存**」を選択します。

あらかじめ「**Default**」という設定が用意されています。この設定は、もっとも優先度が低く、ユーザーに適合する設定が他にない場合のみに適用されます。

14 セルフサービス ポータルのテストデバイスの登録

セルフサービス ポータルの使用をユーザーに案内する前に、セルフサービス ポータルでデバイスの登録をテストすることを推奨します。

テスト用に作成したユーザーアカウントを使用してセルフサービス ポータルにログインし、Sophos Mobile で管理するすべてのプラットフォームに対して登録のテストを行います。

15 **デバイスの追加**ウィザードの使用

デバイスの追加ウィザードを使用して、新しいデバイスを簡単に登録することができます。画面の案内に従って次の一連の操作を行うことができます。

- Sophos Mobile に新しいデバイスを追加する。
- 任意: デバイスをユーザーに割り当てる。
- デバイスを登録する。
- 任意: タスクバンドルをデバイスに配信する。

1. サイドバーのメニューの「**管理**」の下の「**デバイス**」をクリックして、「**追加 > デバイスの追加ウィザード**」の順にクリックします。

   ヒント
   または、次の方法でウィザードを起動できます。
   - 「**ダッシュボード**」ページから「**デバイスの追加**」ウィジェットをクリックする。
   - Sophos Central Admin のメニューから、「**デバイスの保護 > デバイス登録ウィザードの開始**」をクリックする。

2. 「**ユーザー**」ページで、デバイスを割り当てるユーザーの検索条件を入力します。ユーザーへの割り当てなしでデバイスを登録する場合は、「**ユーザーの割り当てをスキップ**」を選択します。

   注
   文字列の一部を検索できますが、検索文字列が、フィールドの最初の部分にある場合のみに検出されます。たとえば、example という検索文字列は、Example User および example@company.com に一致しますが、user@example.com には一致しません。

3. 「**ユーザーの選択**」ページで、検索条件に一致するユーザーのリストから、必要なユーザーを選択します。
4. 「**デバイスの詳細**」ページで次の設定を行います。

オプション	説明
プラットフォーム	デバイスのプラットフォーム。
名前	Sophos Mobile で管理するデバイスの一意の名前。
説明	デバイスの概略 (任意)。
電話番号	電話番号 (任意)。番号は「+491701234567」など、国際電話番号形式で入力してください。
メールアドレス	登録手順の送信先メールアドレス。 Sophos Central のユーザー管理で設定した、デバイスに割り当てられているユーザーのメールアドレスです。
所有者	デバイスの所有者のタイプ。「**会社**」または「**個人**」のいずれかを選択。

オプション	説明
デバイスグループ	デバイスの割当先グループ。デバイスグループを作成していない場合は、常にリストに表示される「**Default**」というデバイスグループを選択できます。

5. 「**登録タイプ**」ページで、デバイスを登録するか、Sophos コンテナのみを登録するかを選択します。

   「**デバイスの登録**」を選択します。
6. デバイスのプラットフォームに対して設定したタスクバンドルを選択します。
7. 「**登録**」ページで、指示に従って登録の操作を完了します。
8. 登録が問題なく完了したら、「**完了**」をクリックします。

注

- すべてのセクションの設定が終了したら、「**完了**」ボタンが表示される前にウィザードを閉じても問題ありません。登録タスクの作成や処理はバックグラウンドで行われます。

16 用語集

Ad Hoc プロビジョニング プロファイル	自分で開発した iOS アプリに追加する、配布用プロビジョニング プロファイル。これによって、アプリを App Store に公開することなく、登録済みデバイスにインストールすることができます。
登録	Sophos Mobile へのデバイスの登録。
Enterprise App Store	Sophos Mobile サーバーにホストされているアプリのリポジトリ。管理者は、Sophos Mobile Adminを使用して、Enterprise App Store にアプリを追加できます。ユーザーは、Sophos Mobile Control アプリを使用して、追加されたアプリを自分のデバイスにインストールできます。
Mobile Advanced ライセンス	Mobile Advanced ライセンスでは、Sophos Intercept X for Mobile、Sophos Secure Workspace、Sophos Secure Email の一元管理が可能。
プロビジョニング	Sophos Mobile Control アプリをデバイスにインストールするプロセス。
Sophos Central Admin	デバイスの管理に使用する Web インターフェース。
Sophos Central Self Service ポータル	ヘルプデスクの手を煩わせることなく、ユーザー自身でデバイスの登録や、さまざまなタスクを実行できるユーザー向け Web インターフェース。
Sophos Mobile クライアント	Sophos Mobile の管理下のデバイスにインストールされている Sophos Mobile Control アプリ。
Sophos Intercept X for Mobile	Android デバイス、iPhone および iPad 用のセキュリティ対策アプリ。このアプリは Sophos Mobile で一元管理できます (Mobile Advanced ライセンスのアクティベーションが完了している場合に限ります)。
Sophos Secure Email	Android デバイス、iPhone および iPad 用のアプリ。メール、予定表の項目、連絡先などを管理するためのセキュアなコンテナを提供します。このアプリは Sophos Mobile で一元管理できます (Mobile Advanced ライセンスのアクティベーションが完了している場合に限ります)。
Sophos Secure Workspace	Android デバイス、iPhone および iPad 用のアプリ。さまざまなクラウド ストレージ サービス上のファイルや企業が配信するファイルを、参照、管理、編集、共有、暗号化、復号化できるセキュアなワークスペースを提供します。このアプリは Sophos Mobile で一元管理できます

	(Mobile Advanced ライセンスのアクティベーションが完了している場合に限ります)。
タスクバンドル	複数のタスクを 1つのトランザクションとしてまとめるためにパッケージを作成します。デバイスの登録を完了し、社内で利用するために必要なすべてのタスクを 1つにまとめられます。
Team ID	すべての iOS アプリと macOS アプリは、Team ID で署名されます。Team ID は、Apple から開発者ごとに与えられる一意の ID です。

17 サポート

ソフォス製品のテクニカルサポートは、次のような形でご提供しております。

- ユーザー コミュニティ サイト「Sophos Community」(英語) (community.sophos.com/) のご利用。さまざまな問題に関する情報を検索できます。
- ソフォス サポートデータベースのご利用。www.sophos.com/ja-jp/support.aspx
- 製品ドキュメントのダウンロード。www.sophos.com/ja-jp/support/documentation.aspx
- オンラインでのお問い合わせ。https://secure2.sophos.com/ja-jp/support/open-a-support-case.aspx

18 利用条件