SOPHOS
Security made simple.

Sophos Mobile as a Service

スタートアップガイド

製品バージョン: 8

目次

1 このガイドについて

このガイドでは、Sophos Mobile as a Service をセットアップし、デバイスを管理する方法について説明します。

管理方法の詳細については、「Sophos Mobile 管理者ヘルプ」を参照してください。

このガイドは、モバイルデバイスの最も一般的なプラットフォームである、Android と iOS を対象としています。サポートされている他の OS についても、このガイドの説明と同様の方法で設定を行うことができます。

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. パスワードをリセットし、Sophos Mobile Adminにログインし、管理者のユーザー名を変更する。
2. オプション: Sophos Mobile Security、Sophos Secure Workspace および Sophos Secure Email アプリを管理するために、Mobile Advanced ライセンスのアクティベーションを行う。
3. ライセンスを確認する。
4. 個人設定、管理者アカウントに対するパスワードポリシー、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。
5. iOS デバイスを管理するための Apple Push Notification Service (APNs) の証明書をアップロードする。
6. オプション: 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。
7. オプション: サードパーティ製の NAC (ネットワーク アクセス コントロール) システムとのインターフェースを設定する。
8. コンプライアンスポリシーを作成する。
9. デバイスグループを作成する。
10. デバイスを設定する。
11. セルフサービス ポータルの設定を更新する。
12. ユーザー管理を設定する。
13. 内部ユーザー管理を使用する場合: ユーザーを追加する。ユーザーは新規作成することも、ユーザーのリストをアップロードすることもできます。
14. 外部ユーザー管理を使用する場合: LDAP ディレクトリとの接続を設定する。
15. 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 パスワードの変更

セキュリティ上の理由から、Sophos Mobile Adminへの初回ログイン時にパスワードをリセットすることをお勧めします。

1. Web ブラウザで Sophos Mobile Adminを開きます。
2. 「**ログイン**」ダイアログで、「**パスワードを忘れた場合**」をクリックします。
3. 「**パスワードのリセット**」ダイアログで、Sophos Mobile as a Service のアカウントのアクティベーションを案内するメールに記載されている「**カスタマー**」と「**ユーザー**」を入力し、「**パスワードのリセット**」をクリックします。
   パスワードのリセット用リンクを含むメールが送信されます。
4. リンクをクリックして「**パスワードの変更**」ダイアログを開きます。
5. 新しいパスワードを入力し、「**パスワードの変更**」をクリックします。
   パスワードが変更されます。次回コンソールにログインする際は、必ずこのパスワードでログインします。

注
パスワードポリシーは、たとえばパスワードに最低限含めなくてはならない小文字、大文字、記号の文字数などを設定し、推測しやすいパスワードを設定できないように変更することを推奨します。詳細は、パスワードポリシーの設定 (p. 8)を参照してください。

4 ログイン名の変更

セキュリティ上の理由から、Sophos Mobile Adminに初回ログインした後、管理者のログイン名を変更することを推奨します。

1. サイドバーのメニューの「**設定**」の下で、「**セットアップ > 管理者**」の順にクリックします。
2. 「**管理者の表示**」ページで、ログイン名の右側に表示される青い逆三角マークをクリックし、「**編集**」をクリックします。
3. 「**管理者の編集**」ページで、「**ログイン名**」フィールドに新しいログイン名を入力します。
4. オプション: 他の項目の設定内容を変更します。
   - **名**
   - **姓**
   - **メールアドレス**
5. 「**保存**」をクリックします。

アカウント情報が変更されます。次回 Sophos Mobile Adminにログインする際は、必ず新しいログイン名でログインします。

5 Mobile Advanced ライセンスのアクティベーション

Mobile Advanced ライセンスをお持ちの場合は、Sophos Mobile を使用して Sophos Mobile Security、Sophos Secure Workspace、Sophos Secure Email アプリを一元管理することができます。

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

1. サイドバーのメニューの「**設定**」の下で、「**セットアップ > システムセットアップ**」の順にクリックします。
2. 「**ライセンス**」タブの「**Advanced 版ライセンスキー**」にライセンスキーを入力し、「**アクティベート**」をクリックします。

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。

6 ライセンスの確認

Sophos Mobile のライセンス体系はユーザー単位です。1つのユーザーライセンスで、ユーザーに割り当てられているすべてのデバイスを保護できます。ユーザーに割り当てられていないデバイスは、1台につき 1つのライセンスが必要です。

利用可能なライセンスを確認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**」の下で、「**セットアップ > システムセットアップ**」の順にクリックします。
2. 「**システムセットアップ**」ページで「**ライセンス**」タブをクリックします。

次の情報が表示されます。

- **ライセンスの最大数**: 管理可能なデバイスユーザー (および割り当てられていないデバイス) の最大数。
- **使用中のライセンス数**: 現在使用されているライセンスの数。
- **有効期限**: ライセンスの有効期限。

表示されるライセンス情報に関する質問やご不明な点は、ソフォス営業部までお問い合わせください。

7 設定

次の設定を行います。

- 個人設定 (管理する OS など)
- パスワードポリシー
- 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

7.1 個人設定の指定

Sophos Mobile Adminをより効率よく使用するため、使用するプラットフォームのみが GUI に表示されるようにカスタマイズできます。

注
ここで、プラットフォームを指定した場合、現在ログインしているユーザーだけに対して表示される画面が変更されます。ここで機能を無効にすることはできません。

1. サイドバーのメニューの「**設定**」の下で「**セットアップ > 全般**」の順にクリックし、「**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
言語	Sophos Mobile Adminの表示言語を選択します。
タイムゾーン	画面に表示する日時のタイムゾーンを選択します。
単位	距離単位を選択します (「**メートル**」または「**ヤード・ポンド**」法)。
1ページの表示件数	1ページに表示するデータの最大件数を選択します。
デバイスの詳細をすべて表示	デバイスに関するすべての詳細情報を表示する場合は、このチェックボックスを選択します。「**カスタムプロパティ**」タブと「**内部プロパティ**」タブが「**デバイスの表示**」ページに追加されます。
有効なプラットフォーム	管理するプラットフォームを選択します。 • **Android** • **Android Things** • **iOS** • **Windows Mobile** (Windows Phone 8.1 および Windows 10 Mobile OS など) • **Windows** • **Windows IoT** 選択したプラットフォームに基づいて、Sophos Mobile Adminの GUI が調整されます。選択したプラットフォームに関連する画面や機能のみが表示されます。

3. 「**保存**」をクリックします。

7.2 パスワードポリシーの設定

パスワードのセキュリティを強化するには、Sophos Mobile Adminのユーザーとセルフサービスポータルに対してパスワードポリシーを設定します。

> **注**
> パスワードポリシーは、外部 LDAP ディレクトリのユーザーには適用されません。

1. サイドバーのメニューの「**設定**」の下で、「**セットアップ > 全般**」の順にクリックし、「**パスワードポリシー**」タブをクリックします。
2. 「**ルール**」の下では、パスワードに最低限含めなければならない小文字や数字の数など、パスワード要件を指定できます。
3. 「**設定**」の下では次の項目を設定します。
   a) **パスワードの変更頻度 (日数)**: パスワードの有効期限が切れるまでの日数 (1 ~ 730 の値) を入力します。何も入力しない場合、パスワードの有効期限は無期限になります。
   b) **過去のパスワード利用制限回数**: 1～10 までの間の値を選択します。「---」を選択した場合、無制限になります。
   c) **ログインの最大試行回数**: アカウントがロックされるまでのログインの失敗回数 (1～10) を選択します。「---」を選択した場合、ログインの失敗が無制限に許可されます。
4. 「**保存**」をクリックします。

7.3 サポート問い合わせ先情報の設定

ユーザーからの問い合わせに対応するテクニカルサポートの問い合わせ先や問い合わせ方法に関する情報を設定できます。ここで入力する情報は、Sophos Mobile Control アプリとセルフサービス ポータルに表示されます。

1. サイドバーのメニューの「**設定**」の下で、「**セットアップ > 全般**」の順にクリックし、「**サポート問い合わせ**」タブをクリックします。
2. 必要なサポート問い合わせ情報を入力します。
3. 「**保存**」をクリックします。

7.4 セルフサービス ポータルの設定

1. サイドバーメニューの「**設定**」の下で、「**セットアップ > セルフサービス ポータル**」の順にクリックします。
   「**セルフサービス ポータル**」ページが開きます。
2. 必要に応じて、「**設定**」タブでセルフサービス ポータルを設定します。

   この時点で適用する設定がよくわからない場合は、デフォルトの設定を使用することを推奨します。

   設定の詳細については、画面右上の「**ヘルプ**」ボタンをクリックしてください。
3. 「**利用条件**」タブで「**編集**」をクリックしてモバイルポリシーの免責事項や同意テキストを入力します。

このメッセージはデバイスの登録を開始する際に表示されます。ユーザーは登録を実行する前に内容に同意する必要があります。

> **ヒント**
> エディタのツールバーを利用して簡単な HTML 形式のテキストを編集できます。次のステップで説明する「ポストインストール用テキスト」も同様です。

4. 任意: 「**ポストインストール用テキスト**」タブで、「**編集**」をクリックしてデバイスの登録が終了する際に表示するメッセージを入力します。
   たとえば、デバイスの登録後にユーザーが行う必要のある操作の手順などを設定できます。
5. 「**保存**」をクリックします。

8 Apple Push Notification Service の証明書

iOS や macOS デバイス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。

以下のセクションでは、独自のクライアント証明書を使用して APNs サーバーへ接続するのに必要な要件と操作手順を説明しています。

8.1 要件

Apple Push Notification Service (APNs) と通信を行うには、以下の TCP ポートへの送受信接続を許可する必要があります。

- Sophos Mobile サーバーが接続するサーバー: gateway.push.apple.com:2195 TCP (17.0.0.0/8)
- Wi-Fi のみで接続する各 iOS デバイスが接続するサーバー: *.push.apple.com:5223 TCP (17.0.0.0/8)

8.2 APNs 証明書の作成

1. サイドバーのメニューの「**設定**」で、「**セットアップ > システム セットアップ**」の順に展開し、「**APNs**」タブをクリックします。
   タブに表示されている説明に従って、Apple から証明書をリクエストし、Sophos Mobile にアップロードします。
2. 「**証明書署名要求のダウンロード**」ステップで、「**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。
3. 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 の作成**」ステップで、「**新しい Apple ID の作成**」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。

4. 「**APNs**」タブの上部の「**Apple ID**」フィールドに新しい Apple ID を入力しておくと、必要なときに参照できます。
   毎年証明書を更新する際、常に同じ Apple ID を使用する必要があります。

5. 「**APNs 証明書の作成または更新**」ステップで、「**Apple Push Certificates Portal**」をクリックします。

   Apple Push Certificates Portal が開きます。
6. 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。
7. 「.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。
8. 「**APNs 証明書のアップロード**」ステップで、「**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。
9. 「**保存**」をクリックすると、APNs 証明書が Sophos Mobile に追加されます。

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。

9 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。

スタンドアロン型 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。

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、内部 EAS プロキシまたはスタンドアロン型 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. 16)を参照してください。

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認証されているかどうかを検証できません。

9.1 EAS プロキシのインストーラのダウンロード

1. Sophos Mobile Adminにログインします。
2. サイドバーのメニューの「**設定**」の下で、「**セットアップ > システムセットアップ**」の順にクリックし、「**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。

9.2 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。

注
「Sophos Mobile 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 SMC サーバーの URL を入力します。

   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。

   Sophos Mobile サーバーが複数の証明書を EAS プロキシに提示する場合は、「**Allow all certificates**」(すべての証明書を許可する) を選択します。これは、たとえば、ロードバランサの後ろに複数のインスタンスがあり、各インスタンスで異なる証明書が使用されている場合などです。このオプションを選択すると、EAS プロキシは、Sophos Mobile サーバーからの証明書すべてを受け入れます。

重要
「**Allow all certificates**」(すべての証明書を許可する) オプションを選択すると、サーバー通信のセキュリティレベルが低下するため、ネットワーク環境で必要となる場合のみに選択することを強く推奨します。

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) を選択済みの場合は、「**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。

注
SSL Certificate Wizard (SSL 証明書ウィザード) を MySophos からダウンロードして、Sophos Mobile の EAS プロキシの SSL/TLS 証明書要求を作成できます。

ソフォス製品のソフトウェアをダウンロードする方法については、ソフォスのサポートデータベースの文章 111195 を参照してください。

   - 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) (証明書、秘密鍵、および証明書チェーンを含む PKCS12 (中間および CA))
     - **Separate files for certificate, private key, intermediate and CA certificate** (証明書、秘密鍵、 中間証明書および CA 証明書への個別ファイル)
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**」(認証にクライアント証明書を使用) を選択済みの場合は、「**SMC client authentication configuration**」(SMC クライアント認証の設定) 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** (インスタンスの種類): 「**EAS proxy**」(EAS プロキシ) を選択します。
   - **Instance name** (インスタンス名): インスタンスの識別に使用される名前。
   - **Server port** (サーバーポート): 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** (クライアント証明書を使用した認証が必要): 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** (ActiveSync サーバー): 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**: 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): このオプションを選択して、iOS デバイス上の 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。

- **Enable Traveler client access** (Traveler クライアントのアクセスを有効にする) : 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 Sophos Mobile サーバーにアップロード) 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. オプション: 「**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、Sophos Mobile 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 Mobile Adminにログインします。
17. 「**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。セットアップウィザードを使用して作成した PowerShell 接続用の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。
18. 「**保存**」をクリックします。
19. 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。

9.3 PowerShell 経由のメールアクセス制御の設定

PowerShell を使用した、Exchange サーバーや Office 365 サーバーへの接続を設定できます。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、デバイスからメールサーバーに直接送信されます。プロキシ経由では送信されません。

注
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 接続を使用したシナリオのメリットは次のとおりです。

- デバイスは、Exchange サーバーと直接通信します。
- サーバーで、管理対象デバイスからの受信メールトラフィック用のポートを開放する必要がありません。

対応しているメールサーバーは次のとおりです。

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

PowerShell をセットアップする方法は次のとおりです。

1。PowerShell を設定します。
2。Exchange サーバーまたは Office 365 にサービスアカウントを作成します。Sophos Mobile は、このアカウントを使用して PowerShell コマンドを実行します。
3。Exchange または Office 365 への 1つまたは複数の PowerShell の接続インスタンスをセットアップします。
4。インスタンスの証明書を Sophos Mobile にアップロードします。

PowerShell の設定

1. EAS プロキシのインストール先コンピュータで、管理者権限で Windows PowerShell を開き、次のように入力します。

```
PS C:¥Windows¥system32> Set-ExecutionPolicy RemoteSigned
```

> **注**
> PowerShell がない場合は、マイクロソフトの文章、Windows PowerShell のインストール (外部リンク) にある説明に従ってインストールします。

2. ローカル Exchange サーバーを接続する場合は、そのコンピュータで、管理者権限で Windows PowerShell を開いて、先ほどと同じコマンドを入力します。

```
PS C:¥Windows¥system32> Set-ExecutionPolicy RemoteSigned
```

> **注**
> この手順は、Office 365 では不要です。

サービスアカウントの作成

3. 該当する管理コンソールにログインします。
   - Exchange Server 2010 の場合: **Exchange 管理コンソール**
   - Exchange Server 2013/2016 の場合: **Exchange 管理者センター**
   - Office 365 の場合: **Office 365 管理者センター**
4. ユーザーアカウントを作成します。Sophos Mobile は、このアカウントをサービスアカウントとして使用して、PowerShell コマンドを実行します。
   - 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無効にします。
   - 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。
5. 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。
   - サービスアカウントをメンバーとして追加します。

PowerShell 接続のセットアップ

6. スタンドアロン型 EAS プロキシをセットアップするのと同様に、セットアップウィザードを使用します。ウィザードの「**EAS Proxy instance setup**」(EAS プロキシのインスタンスのセットアップ) で、次のオプションを設定します。

- **Instance type** (インスタンスの種類): 「**PowerShell Exchange/Office 365**」を選択します。
- **Instance name** (インスタンス名): インスタンスの識別に使用される名前。
- **Exchange server** (Exchange サーバー): Exchange サーバーの名前や IP アドレス (Exchange サーバーのローカルインストールの場合)、または outlook.office365.com (Office 365 の場合)。プレフィックス https:// やサフィックス /powershell は指定しないでください。自動的に追加されます。
- **Allow all certificates** (すべての証明書を許可する): Exchange サーバーが提示する証明書は確認されません。これは、たとえば、自己署名証明書が Exchange サーバーにインストールされている場合などに使用できます。「**Allow all certificates**」(すべての証明書を許可する) オプションを選択すると、サーバー通信のセキュリティレベルが低下するため、ネットワーク環境で必要となる場合のみに選択することを強く推奨します。
- **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): このオプションを選択して、iOS デバイス上の 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。

- **Service account** (サービスアカウント): Exchange 管理コンソールや Office 365 管理者センターで作成したユーザーアカウントの名前。
- **Password** (パスワード): ユーザーアカウントのパスワード。

7. 「**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。
8. 任意: PowerShell を使用して他の Exchange サーバーや Office 365 サーバーに接続するには、上記の手順を繰り返します。
9. スタンドアロン型 EAS プロキシのインストール (p. 13)の説明に従ってセットアップウィザードを完了します。

証明書のアップロード

10. Sophos Mobile Adminにログインします。
11. サイドバーのメニューの「**設定**」で、「**セットアップ > システム セットアップ**」の順に展開し、「**EAS プロキシ**」タブをクリックします。
12. オプション: 「**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。
    これにより、他のメールアプリがメールサーバーに接続することを防ぎます。
13. 「**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。セットアップウィザードを使用して作成した PowerShell 接続用の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。
14. 「**保存**」をクリックします。
15. 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、PowerShell 接続の初期セットアップが完了しました。デバイスがコンプライアンスルールに違反している場合、管理対象デバイスと Exchange サーバーや Office 365 サーバー間のメールトラ

フィックはブロックされます。個別のデバイスは、デバイスへのメールアクセスモードを「**拒否**」に指定してブロックできます。

注
メールアクセスがブロックされると、Exchange サーバーの設定によっては、デバイスは通知を受信します。

9.4 内部 EAS プロキシサーバーとの接続の設定

1. サイドバーのメニューの「**設定**」で、「**セットアップ > システム セットアップ**」の順に展開し、「**EAS プロキシ**」タブをクリックします。
2. オプション: 「**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。
   これにより、他のメールアプリがメールサーバーに接続することを防ぎます。
3. 「**内部サーバー**」で、Exchange サーバーまたはグループウェアサーバーの URL を「**Exchange サーバー/グループウェアサーバーの URL**」テキストフィールドに入力します。
4. 「**SSL/TLS の使用**」を選択し、セキュアな接続を試用するようにします。
5. 「**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**」を選択して、iOS デバイス上の 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。
   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。
6. 「**接続の確認**」をクリックし、接続をテストします。
   サーバーに接続できない場合は、メッセージが表示されます。
7. 「**保存**」をクリックします。

9.5 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。

重要
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ッ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**」で、「**セットアップ > システム セットアップ**」の順に展開し、「**EAS プロキシ**」タブをクリックします。

2. オプション: 「**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。
   これにより、他のメールアプリがメールサーバーに接続することを防ぎます。
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。

10 ネットワーク アクセス コントロールの設定

Sophos Mobile には、サードパーティ製の NAC (ネットワーク アクセス コントロール) システムとの連携に必要なインターフェースが搭載されています。NAC システムとの接続を設定すれば、SMC のデバイスやそのコンプライアンスステータスのリストを NAC 側で取得できるようになります。また、このセクションの説明に従ってネットワーク アクセス コントロールを設定すれば、特定のコンプライアンスルールに違反した場合にネットワークへのアクセスを禁止するコンプライアンスポリシーを後から指定することができます。

コンプライアンスポリシーの定義方法の詳細は、「Sophos Mobile 管理者ヘルプ」を参照してください。

ネットワーク アクセス コントロールを設定する方法は以下のとおりです。

1. サイドバーのメニューの「**設定**」の下で、「**セットアップ > システムセットアップ**」の順にクリックし、「**ネットワーク アクセス コントロール**」タブをクリックします。
2. リストから利用可能な NAC システムを選択します。

   - **Sophos UTM**

     Sophos UTM (バージョン 9.2 以降) との連携を有効にするオプションです。連携には UTM 側の設定も必要です。Sophos UTM の WebAdmin インターフェースの「**管理 > Sophos Mobile**」で、SMC サーバーの URL と管理アカウントの情報を指定してください。詳細は、「Sophos UTM 管理ガイド」を参照してください。

   - **Cisco ISE**

     Cisco ISE との連携を有効にするオプションです。次の設定を行います。

ユーザー名	Cisco ISE で指定する必要のあるユーザー名。Cisco ISE が Sophos Mobile にログインするときに使用するユーザー名です。
パスワード	Sophos Mobile にログインするためのパスワードを入力します。
パスワードの確認	パスワードを再入力します。
ブロックしたデバイスのリダイレクトページ	デバイスにネットワークへのアクセスが許可されないときに表示する URL。 セルフサービス ポータルの URL、またはセルフサービス ポータルへのリンクを含む情報画面の URL を指定することを推奨します。

     ここで入力した Sophos Mobile サーバーの URL とログイン情報を使用して NAC インターフェースに接続するように、Cisco ISE でも関連する設定を行う必要があります。

   - **Check Point**

     Check Point (バージョン R77.10 以降) との連携を有効にするオプションです。次の設定を行います。

ユーザー名	Check Point で指定しなくてはならないユーザー名。Check Point が Sophos Mobile にログインするときに使用するユーザー名です。
パスワード	Sophos Mobile にログインするためのパスワードを入力します。
パスワードの確認	パスワードを再入力します。

Check Point のサポート記事、MDM cooperative enforcement for Mobile clients (英語) の説明に従って、Check Point Mobile Access Gateway で、セキュリティゲートウェイの特定の構成を設定する必要があります。

- **Web サービス**

  サードパーティの NAC システムに Web サービスインターフェースへのアクセスを許可する場合に選択します。

  Sophos Mobile には、MAC アドレスやネットワークアクセスのステータスを提供する、RESTful Web サービス インターフェースが搭載されています。

  サードパーティの NAC システムは、Sophos Mobile の管理者アカウントのログイン情報を使用して、このインターフェースに接続することができます。

  Web サービスインターフェースの導入の詳細は、「Sophos Mobile ネットワーク アクセス コントロール インターフェース ガイド (英語)」を参照してください。

- **カスタム**

  証明書ベースでの NAC インターフェースへのアクセスを設定する場合に選択します。

  > **注**
  > 「**カスタム**」という古いオプションの使用は推奨しません。このオプションは今後の製品リリースで削除する予定です。代わりに「**Web サービス**」オプションを使用してサードパーティの NAC システムを Sophos Mobile に接続します。

  「**ファイルのアップロード**」をクリックしてサードパーティ製 NAC システムの証明書を参照します。証明書がアップロードされ、一覧に表示されます。

  Sophos Mobile サーバーでアップロードした証明書を用いて認証が行われ、該当するサードパーティの NAC システムに NAC インターフェースへの接続が許可されます。

3. 「**ネットワーク アクセス コントロール**」タブで「**保存**」をクリックします。

11 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。

11.1 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. 19)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 デバイスおよび iOS デバイスのみに対して実行できます。
ネットワーク接続を拒否	ネットワークへのアクセスを禁止します。 このアクションは、ネットワーク アクセス コントロールを設定した場合のみに実行できます。詳細は、ネットワーク アクセス コントロールの設定 (p. 21)を参照してください。
警告の作成	警告が作成されます。 生成された警告は、「**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。 このアクションは、Android デバイス、iOS デバイス、macOS デバイス、および Windows デバイスのみに対して実行できます。 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。

オプション	説明
	重要 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。

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**」ページに新しいコンプライアンスポリシーが表示されます。

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。

12 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。

12.1 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 iOS デバイス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。

13 iOS デバイスの設定

13.1 iOS デバイス用のプロファイルの作成

ここでは、iOS デバイスの初期設定のためのプロファイルを作成します。

以下の項目に対しては個別のプロファイルを設定することを推奨します。

- パスワードポリシーと制限
- Exchange アカウントの設定 (必要に応じて)
- VPN 設定 (必要に応じて)
- Wi-Fi 設定 (必要に応じて)
- ルート証明書とクライアント証明書 (必要に応じて)

注

Sophos Mobile では、次の 2種類の方法で iOS デバイス用のプロファイルを作成できます。

- Sophos Mobile Adminから手動でプロファイルを作成する。
- Apple Configurator で作成したプロファイルをインポートする。

このセクションでは、Sophos Mobile Adminでプロファイルを作成する方法について説明します。Apple Configurator で作成したプロファイルをインポートする方法についての詳細は、「Sophos Mobile 管理者ヘルプ」を参照してください。

iOS デバイスのパスワードポリシーと制限のプロファイルを作成する方法は以下のとおりです。

1. サイドバーのメニューの「**デバイス設定**」で、「**プロファイルとポリシー > iOS**」をクリックします。
2. 「**プロファイルとポリシー**」ページで、「**作成 > デバイスのプロファイル**」の順にクリックします。
3. 「**プロファイルの編集**」ページで次の項目を設定します。
   a) **名前**: プロファイル名を入力します。セルフサービス ポータルでの登録に適用するプロファイルを作成する場合は、「iOS SSP プロファイル」という名前を指定することを推奨します。
   b) **所属**: 会社名などプロファイルに対する所属名を入力します。
   c) **説明**: ベースプロファイルなどプロファイルの概略を入力します。
4. プロファイルにパスワードポリシーを追加するには、「**設定の追加**」をクリックして「**パスワードポリシー**」を選択します。
5. 「**パスワードポリシー**」ページで必要な項目を設定します。
   設定の詳細については、画面右上の「**ヘルプ**」ボタンをクリックしてください。
6. 「**適用**」をクリックして設定内容を保存します。
   「**パスワードポリシー**」の設定が「**プロファイルの編集**」ページの「**設定**」の下に表示されます。
7. プロファイルに制限を追加するには、もう一度「**設定の追加**」をクリックして「**制限**」を選択します。
8. 「**制限**」ページで必要な制限項目を選択します。
   制限項目のなかには特定の機種やバージョンの iOS のみに適用可能なものもあります。この要件は各制限項目の右横に表示されます。

設定の詳細については、画面右上の「**ヘルプ**」ボタンをクリックしてください。

9. 「**適用**」をクリックして設定内容を保存します。
「**制限**」の設定が「**プロファイルの編集**」ページの「**設定**」の下に表示されます。
10. 「**プロファイルの編集**」ページで「**保存**」をクリックしてプロファイルを保存します。

プロファイルが「**プロファイルとポリシー**」ページに表示され、iOS デバイスに配信できるようになります。

必要に応じて、Exchange アカウント、VPN、および Wi-Fi の設定、あるいはルート証明書やクライアント証明書のインストールを定義するプロファイルを追加で作成します。

13.2 iOS デバイス用のタスクバンドルの作成

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**」をクリックします。
2. 「**タスクバンドル**」ページで、「**タスクバンドルの作成**」をクリックします。
「**タスクバンドルの編集**」ページが表示されます。
3. 該当するフィールドに、新しいタスクバンドルの名前と、必要に応じて説明を入力します。
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. オプション: コンプライアンスルール違反時に、デバイスにタスクバンドルを配信する場合は、「**違反時にアクションの選択が可能**」を選択します。詳細は、コンプライアンスポリシー (p. 23)を参照してください。

> **注**
> 既存のタスクバンドルを編集する場合で、そのタスクバンドルが既に違反時のアクションとして使用されているときは、このオプションは無効になります。

5. オプション: iOS のタスクバンドルで、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ない場合、無効に設定されます。
6. 「**タスクの作成**」をクリックして「**登録**」を選択し、タスク名を入力します。「**適用**」をクリックしてタスクを作成します。
ここで入力した名前は、タスクが処理されている間、セルフサービス ポータルに表示されます。
7. もう一度「**タスクの作成**」をクリックして「**プロファイルのインストールまたはポリシーの割り当て**」を選択します。タスク名に「パスワードポリシーのプロファイルのインストール」など、わかりやすい名前を入力し、先に作成したプロファイルを選択します。「**適用**」をクリックしてタスクを作成します。
8. Exchange、VPN、または Wi-Fi の設定のプロファイルを作成した場合は、各プロファイルについても上記の手順を繰り返します。
9. オプション: タスクバンドルにその他のタスクを追加します。

> **ヒント**
> 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ソート矢印を使って設定できます。

10. 必要なタスクすべてをタスクバンドルに追加したら、「**タスクバンドルの編集**」ページで「**保存**」をクリックします。

作成したタスクバンドルは、これで配信する準備ができました。「**タスクバンドル**」ページに作成したタスクバンドルが表示されます。

14 Android デバイスの設定

14.1 Android デバイス用のプロファイルの作成

ここでは、Android デバイスの初期構成のためのプロファイルを作成します。

以下の項目に対しては個別のプロファイルを設定することを推奨します。

- パスワードポリシーと制限
- Exchange アカウントの設定 (必要に応じて)
- VPN 設定 (必要に応じて)
- Wi-Fi 設定 (必要に応じて)
- ルート証明書とクライアント証明書 (必要に応じて)

1. サイドバーのメニューの「**デバイス設定**」で、「**プロファイル、ポリシー > Android**」の順に展開します。
2. 「**プロファイルとポリシー**」ページで、「**作成 > デバイスのプロファイル**」の順にクリックします。
3. 「**プロファイルの編集**」ページで次の項目を設定します。
   a) **名前**: プロファイル名を入力します。セルフサービスポータルでの登録に適用するプロファイルを作成する場合は、「Android SSP プロファイル」という名前を指定することを推奨します。
   b) オプション: **説明**: ベースプロファイルなどプロファイルの概略を入力します。
4. プロファイルにパスワードポリシーを追加するには、「**設定の追加**」をクリックして「**パスワードポリシー**」を選択します。
   「**パスワードポリシー**」ページが開きます。
5. 「**パスワードの種類**」フィールドで、定義するパスワードの種類 (例:「**複雑なパスワード**」) を選択します。
6. 必要な項目を設定します。
   表示される設定項目は選択したパスワードの種類によって異なります。すべての設定の詳細を表示するには、画面右上の「**ヘルプ**」ボタンをクリックしてください。
7. 「**適用**」をクリックして設定内容を保存します。
   「**パスワードポリシー**」の設定が「**プロファイルの編集**」ページの「**設定**」の下に表示されます。
8. プロファイルに制限を追加するには、もう一度「**設定の追加**」をクリックして「**制限**」を選択します。
9. 「**制限**」ページで必要な制限項目を選択します。
   制限項目のなかには特定の機種やバージョンの Android のみに適用可能なものもあります。この要件は各制限項目の右横に表示されます。
   設定の詳細については、画面右上の「**ヘルプ**」ボタンをクリックしてください。
10. 「**適用**」をクリックして設定内容を保存します。
    「**制限**」の設定が「**プロファイルの編集**」ページの「**設定**」の下に表示されます。
11. 「**プロファイルの編集**」ページで「**保存**」をクリックしてプロファイルを保存します。

プロファイルが「**プロファイルとポリシー**」ページに表示され、Android デバイスに配信できるようになります。

必要に応じて、Exchange アカウント、VPN、および Wi-Fi の設定、あるいはルート証明書やクライアント証明書のインストールを定義するプロファイルを追加で作成します。

14.2 Android デバイス用のタスクバンドルの作成

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**」の順に展開します。
2. 「**タスクバンドル**」ページで、「**タスクバンドルの作成**」をクリックします。
   「**タスクバンドルの編集**」ページが表示されます。
3. 該当するフィールドに、新しいタスクバンドルの名前と、必要に応じて説明を入力します。
   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. オプション: コンプライアンスルール違反時に、デバイスにタスクバンドルを配信する場合は、「**違反時にアクションの選択が可能**」を選択します。詳細は、コンプライアンスポリシー (p. 23)を参照してください。

   注
   既存のタスクバンドルを編集する場合で、そのタスクバンドルが既に違反時のアクションとして使用されているときは、このオプションは無効になります。

5. オプション: iOS のタスクバンドルで、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ない場合、無効に設定されます。
6. 「**タスクの作成**」をクリックして「**登録**」を選択し、タスク名を入力します。「**適用**」をクリックしてタスクを作成します。
   ここで入力した名前は、タスクが処理されている間、セルフサービス ポータルに表示されます。
7. もう一度「**タスクの作成**」をクリックして「**プロファイルのインストールまたはポリシーの割り当て**」を選択します。タスク名に「パスワードポリシーのプロファイルのインストール」など、わかりやすい名前を入力し、先に作成したプロファイルを選択します。「**適用**」をクリックしてタスクを作成します。
8. Exchange、VPN、または Wi-Fi の設定のプロファイルを作成した場合は、各プロファイルについても上記の手順を繰り返します。
9. オプション: タスクバンドルにその他のタスクを追加します。

   ヒント
   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ソート矢印を使って設定できます。

10. 必要なタスクすべてをタスクバンドルに追加したら、「**タスクバンドルの編集**」ページで「**保存**」をクリックします。

作成したタスクバンドルは、これで配信する準備ができました。「**タスクバンドル**」ページに作成したタスクバンドルが表示されます。

15 セルフサービス ポータルの設定の更新

セルフサービス ポータルで登録したユーザーのデバイスに転送するタスクバンドルを作成した後は、「セルフサービス ポータル」タブのグループ設定で、そのタスクバンドルを指定する必要があります。

1. サイドバーのメニューの「**設定**」の下で「**セットアップ > セルフサービス ポータル**」の順にクリックし、「**グループの設定**」タブを開きます。
2. 「**Default**」のグループ設定をクリックします。
「**グループ設定の編集**」ダイアログボックスが開きます。
3. 「**初期パッケージ - 会社貸与デバイス**」および「**初期パッケージ - 私物デバイス**」のリストで、Android および iOS デバイス用に作成したタスクバンドルを選択します。
4. セルフサービス ポータルで利用できるようにするプラットフォームに対して「**有効**」チェックボックスを選択します。
5. 「**追加先デバイスグループ**」リストから、セルフサービス ポータルから登録したデバイスを追加するグループを選択します。
6. 「**適用**」をクリックします。
7. 「**グループの設定**」タブで「**保存**」をクリックします。

16 ユーザー管理の設定

Sophos Mobile では、Sophos Mobile Adminやセルフサービス ポータルのユーザーアカウントは、次のいずれかの方法で管理できます。

- 内部ユーザー管理の場合、Sophos Mobile Adminでユーザーを手動で追加するか、CSV (カンマ区切り) 形式のファイルからユーザーを一括インポートしてユーザーを作成できます。
- 外部ユーザー管理: 既存の LDAP ディレクトリに接続し、グループメンバーシップに基づいて、グループやプロファイルにデバイスを追加します。

注

- デバイスにユーザーを割り当てた後で、ユーザー管理方法を変更することはできません。
- 外部ユーザー管理では LDAPS (LDAP over SSL/TLS) 環境が必要です。Sophos Mobile では、デフォルトの LDAPS ポート 636 を使用して LDAP サーバーへの接続を行います。

ユーザー管理方法を選択するには以下の手順を実行します。

1. サイドバーのメニューの「**設定**」の下で、「**セットアップ > システムセットアップ**」の順にクリックし、「**ユーザー設定**」タブをクリックします。
2. Sophos Mobile Adminとセルフサービス ポータル (SSP) のユーザーアカウントのデータソースを選択します。
   - 内部ユーザー管理を使用するには「**内部ディレクトリ**」を選択します。
   - 内部ユーザー管理を使用しない場合や、内部ユーザー管理と併用する場合は、「**外部 LDAP ディレクトリ**」を選択します。
3. 「**外部 LDAP ディレクトリ**」を選択した場合は、「**外部 LDAP の設定**」をクリックしてサーバーの詳細を指定します。詳細は、外部ディレクトリの接続の設定 (p. 36)を参照してください。
4. 「**保存**」をクリックします。

注

設定内容を保存すると、選択したユーザー管理方法のみが「**ユーザー設定**」タブに表示されるようになります。後から選択内容を変更する場合は、いったん「**なし。 SSP、ユーザー固有のプロファイル、LDAP 管理者は利用できません。**」を選択して保存すると、再びすべてのオプションが表示されるようになります。

17 内部ユーザー管理の使用

17.1 セルフサービス ポータルのテストユーザーの作成

セルフサービス ポータル (SSP) でのプロビジョニングをテストするために、テスト用の SSP ユーザーアカウントを作成します。作成した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、デバイスの登録をテストします。

セルフサービス ポータルのテスト用アカウント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「**管理**」の下の「**ユーザー**」をクリックして、「**ユーザーの作成**」をクリックします。
2. 必要な項目を設定します。
   「**登録メールの送信**」が選択されていることを確認します。
3. 「**保存**」をクリックします。

ユーザーがセルフサービス ポータルユーザーのリストに追加され、設定画面で指定したメールアドレスに、登録メールが送信されます。

17.2 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。

セルフサービス ポータルのテストユーザーの作成 (p. 34)で作成したテスト用の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。

17.3 Sophos Mobile へのユーザーのインポート

セルフサービス ポータルのデバイス登録をテストしたら、ユーザーのリストを Sophos Mobile にインポートできます。

ユーザーのインポートは、内部ユーザー管理を選択している場合のみが対象です。外部ユーザー管理の場合、特定の LDAP グループに属するすべてのユーザーはシステムにログインできます。

最大 300名のセルフサービス ポータルの新規ユーザーを、文字コードが UTF-8 CSV (カンマ区切り) ファイルから一括インポートして、追加できます。

注
CSV ファイルの編集には、テキストエディタを使用してください。Microsoft Excel を使用すると、入力した値が正しく表示されない場合があります。ファイルを保存する際は、拡張子が .csv になっていることを確認してください。

ヒント
正しい列名と列の順序の例として、「**ユーザーのインポート**」ページからサンプルファイルをダウンロードできます。

CSV ファイルからユーザーをインポートする方法は次のとおりです。

1. サイドバーのメニューの「**管理**」の下の「**ユーザー**」をクリックして、「**ユーザーのインポート**」をクリックします。
2. 「**ユーザーのインポート**」ページで「**登録メールの送信**」を選択します。
3. 「**ファイルのアップロード**」をクリックして用意した CSV ファイルを参照します。
   ファイルから項目が読み込まれ、画面に表示されます。
4. データの形式が正しくない場合や、データに不整合がある場合は、ファイル全体が取り込めなくなります。この場合、問題のある項目の右側に表示されるエラーメッセージを確認し、CSV ファイルの内容を修正したら、ファイルをアップロードしなおします。
5. 「**完了**」をクリックしてユーザーアカウントを作成します。

ユーザーがインポートされ、「**ユーザーの表示**」ページに表示されます。セルフサービス ポータルのログイン情報が記載されたメールがユーザーに届きます。

18 外部ユーザー管理の使用

18.1 外部ディレクトリの接続の設定

外部の LDAP ディレクトリを使用して Sophos Mobile Adminとセルフサービス ポータルのユーザーアカウントを管理する場合は、Sophos Mobile から LDAP サーバーのデータを取得できるようディレクトリとの接続を設定する必要があります。

注
LDAP ディレクトリと Sophos Mobile は同期されません。Sophos Mobile は、ユーザー情報を参照する目的のみで LDAP ディレクトリにアクセスします。LDAP ユーザーの変更は、Sophos Mobile のデータベースに反映されません。また、その逆も反映されません。

1. サイドバーのメニューの「**設定**」の下で、「**セットアップ > システムセットアップ**」の順にクリックし、「**ユーザー設定**」タブをクリックします。
2. 「**外部 LDAP ディレクトリ**」を選択します。
3. 「**外部 LDAP の設定**」をクリックして、サーバーの詳細を指定します。
4. 「**サーバーの詳細**」ページで次の項目を設定します。
   a) 「**LDAP の種類**」フィールドで、LDAP サーバーの種類を選択します。
      - **Active Directory**
      - **IBM Domino**
      - **NetIQ eDirectory**
      - **Red Hat Directory Server**
      - **Zimbra**

   b) 「**プライマリ URL**」フィールドに、プライマリ ディレクトリ サーバーの URL を入力します。サーバーの IP アドレスやサーバー名を入力できます。SSL または TLS (サーバーの対応状況に依存)でサーバーに接続するには、「**SSL/TLS**」を選択します。Sophos Mobile as a Service の場合、「**SSL/TLS**」の選択を外すことはできません。
   c) オプション: 「**セカンダリ URL**」フィールドに、プライマリサーバーに接続できない場合のフォールバック設定として、セカンダリ ディレクトリ サーバーの URL を入力します。サーバーの IP アドレスやサーバー名を入力できます。SSL または TLS (サーバーの対応状況に依存)でサーバーに接続するには、「**SSL/TLS**」を選択します。Sophos Mobile as a Service の場合、「**SSL/TLS**」の選択を外すことはできません。
   d) 「**ユーザー**」フィールドにディレクトリサーバーで検索するアカウントを入力します。Sophos Mobile ではディレクトリサーバーへの接続にアカウント情報が使用されます。

      Active Directory の場合はドメインも入力する必要があります。次の形式で入力してください。

      - <ドメイン名>¥<ユーザー名>
      - <ユーザー名>@<ドメイン名>.<ドメインコード>

注
セキュリティ上の理由から、ディレクトリサーバーに対して読み取り権限のみを持ち、書き込み権限を持たないユーザーを指定することを推奨します。

e) 「**パスワード**」フィールドにユーザーのパスワードを入力します。
「**次へ**」をクリックします。

5. 「**検索のベース**」ページで、検索ベースの DN (Distinguished Name) を入力します。
検索ベースは、ユーザーやグループの検索を開始する外部ディレクトリの場所です。
6. 「**検索フィールド**」では、プロファイルやポリシーの %_USERNAME_% や %_EMAILADDRESS_% を表示するために使用するディレクトリのフィールドを設定します。必要なフィールド名を入力するか、または「**ユーザー名**」と「**メール**」リストから選択します。

注
リストには、現在 LDAP ディレクトリに接続しているユーザー (前述のステップ 4.d (p. 36) で指定) に対して設定されているフィールドのみが表示されます。たとえば、ユーザーに対してメールのフィールドが設定されていない場合などは、「**メール**」フィールドに必要な値を手動で入力する必要があります。

Active Directory の場合、フィールドに対応する属性は以下のとおりです。

- **ユーザー名**: sAMAccountName
- **名**: givenName
- **姓**: sn
- **メール**: mail

7. 「**SSP 設定**」ページで、セルフサービス ポータルへのログインを許可するユーザーを指定します。次のいずれかの方法で「**LDAP ディレクトリグループ**」フィールドに関連する情報を入力します。
   - アスタリスク「*」を入力すると、LDAP ディレクトリグループのメンバーすべてに、セルフサービス ポータルへのログインが許可されます。

     注
     「*」は、すべてのユーザーでなく、すべてのグループを指します。LDAP ディレクトリグループに所属していないユーザーは含まれません。

   - ディレクトリサーバーで定義されているグループ名を入力すると、グループのすべてのメンバーにセルフサービス ポータルへのログインが許可されます。グループ名を入力したら、「**グループの名前解決**」をクリックしてグループ名を識別名 (DN: Distinguished Name) として表示します。
   - 入力欄を空白のままにすると、ディレクトリサーバーに登録されているすべてのユーザーがセルフサービス ポータルにログインできなくなります。セルフサービス ポータルではなく、Sophos Mobile Adminに対する外部ユーザー管理を有効にする場合は、このように設定してください。

> **注**
> ここで指定するグループは、「**セルフサービス ポータル**」ページの「**グループの設定**」タブで指定するユーザーグループに関連しません。SSP ページでは、各ユーザーグループに対する、タスクバンドル、Sophos Mobile のグループメンバーシップ、有効なデバイスのプラットフォームなどを指定します。
>
> セルフサービス ポータルのグループ設定の詳細は、「Sophos Mobile 管理者ヘルプ」を参照してください。

8. 「**適用**」をクリックします。
9. 「**ユーザー設定**」タブで「**保存**」をクリックします。

18.2 LDAP ユーザーのデバイス登録テスト

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。

LDAP アカウントの認証情報でセルフサービス ポータルにログインし、Sophos Mobile で管理するすべてのモバイルプラットフォームに対して登録のテストを行います。

19 デバイスの登録ウィザードを使用したデバイスの新規登録と割り当て

デバイスの新規登録は、デバイス登録ウィザードを利用すると、簡単に登録できます。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。

デバイスの登録ウィザードを起動する方法は次のとおりです。

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 > 登録ウィザード**」をクリックします。

> **ヒント**
> ウィザードは「**ダッシュボード**」ページからも起動できます。その場合は「**デバイスの追加**」というウィジェットをクリックします。

2. 「**ユーザー検索情報の入力**」画面で、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。
3. 検索条件を入力すると、一致するユーザーが画面に表示されます。必要なユーザーを選択します。
4. 「**デバイスの詳細**」画面で、次の項目を設定します。

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。 カスタマーのユーザー管理を設定している場合は、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。 ユーザー管理を設定していない場合は、ここにメールアドレスを入力してください。
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。
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. デバイスの登録後に配信するタスクバンドルを選択します。または、タスクバンドルの配信なしでデバイスを登録する場合は、「**デバイスの登録のみ**」を選択します。

「**次へ**」をクリックすると、デバイスが Sophos Mobile に追加されます。

6. 「**登録**」画面で、指示に従って登録の操作を完了します。

> **注**
> Mac では、Sophos Mobile の管理対象ユーザーが登録手順を実行する必要があります。登録プロファイルをインストールする際、ユーザーは管理者パスワードを入力する必要があります。

7. 登録の操作が正常に完了したら「**完了**」をクリックしてデバイスの登録ウィザードを閉じます。

> **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。

20 用語集

デバイス	管理対象デバイス (スマートフォン、タブレットや Windows 10 デバイスなど)。
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、このようなアプリを自分のデバイスにインストールできます。
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。
セルフサービス 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。
Mobile Advanced ライセンス	Mobile Advanced ライセンスでは、Sophos Mobile を使用した Sophos Mobile Security、Sophos Secure Workspace、Sophos Secure Email アプリの一元管理が可能。
SMSec	Sophos Mobile Security の略称。
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 Mobile コンソール	デバイスの管理に使用する Web インターフェース。
Sophos Mobile Security	Android デバイス向け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 および iOS 搭載デバイス用のアプリ。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 および iOS 搭載デバイス用のアプリ。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。

21 テクニカルサポート

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せ。 https://secure2.sophos.com/ja-jp/support/contact-support/support-query.aspx

22 利用条件

最終更新日: 20171212