SOPHOS
Security made simple.

Sophos Mobile

スタートアップガイド

製品バージョン: 8.5

目次

1 このガイドについて

このガイドでは、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。

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 Sophos Mobile のライセンス

Sophos Mobile には次の 2種類のライセンスがあります。

- Mobile Standard ライセンス
- Mobile Advanced ライセンス

Mobile Advanced ライセンスでは、Sophos Mobile Security、Sophos Secure Workspace および Sophos Secure Email アプリの管理機能を利用できます。

Sophos Mobile を使用した、Sophos Mobile Security、Sophos Secure Workspace および Sophos Secure Email の管理の詳細は、「Sophos Mobile 管理者ヘルプ」を参照してください。

スーパー管理者は、購入したライセンスをスーパー管理者カスタマーの画面でアクティベートして、各カスタマーに対して、ライセンスを提供するユーザー数を指定できます。

2.1 評価版ライセンス

ソフォスでは Sophos Mobile の無償評価を提供しています。無償評価版はソフォスの Web サイトからお申し込みいただけます。 http://www.sophos.com/ja-jp/products/free-trials/mobile-control.aspx.

評価版ライセンスは 30日間有効で、最大 5名までのユーザーを管理できます。

Sophos Mobile の評価版を初期設定する際に必要となるのは、評価版の利用申し込みの際に登録したメールアドレスのみです。

2.2 評価版ライセンスの正規ライセンスへの更新

評価版ライセンスは、Sophos Mobile で正規版のライセンスキーを入力するだけで正規版ライセンスに更新できます。詳細は、「Sophos Mobile 管理者ヘルプ」を参照してください。

2.3 ライセンスの更新

ライセンスを更新するには、Sophos Mobile で新しいライセンスキーのアクティベーションを行う必要があります。詳細は「Sophos Mobile スーパー管理者向けガイド (英語)」を参照してください。

3 導入ステップ

Sophos Mobile の導入ステップは次のとおりです。

1. スーパー管理者権限で Sophos Mobile Adminにログインします。
2. **開始手順**ウィザードを起動し、Sophos Mobile サーバーの初期設定を行います。

   注
   開始手順ウィザードには評価版ライセンスを要求するオプションも含まれています。

3. ライセンスを確認する。
4. デバイスを管理するための新規カスタマーを作成する。
5. 新規カスタマーに切り替える。
6. 新規カスタマーの管理者を作成し、作成した管理者として Sophos Mobile Adminにログインする。
7. 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。
8. 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。
9. コンプライアンスポリシーを作成する。
10. デバイスグループを作成する。
11. デバイスを設定する。
12. セルフサービス ポータルの設定を更新し、セルフサービス ポータルにテストユーザーを追加する。
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。
    この方法については、「Sophos Mobile スーパー管理者ガイド (英語)」 を参照してください。
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。

4 スーパー管理者としてログイン

初期設定のステップの一部を実行するには、Sophos Mobile Adminのインストール時に設定したスーパー管理者アカウントを使用して Sophos Mobile にログインする必要があります。

1. Sophos Mobile のインストール時に設定した Sophos Mobile Adminの URL を開きます。
2. ログインの画面でスーパー管理者のカスタマー名、ユーザー名、パスワードを入力し、「**ログイン**」をクリックします。

注

スーパー管理者としてログインすると、スーパー管理者のタスクを実行できる専用の Sophos Mobile Admin画面が表示されます。

スーパー管理者としての Sophos Mobile Adminの使用方法の詳細は、「Sophos Mobile スーパー管理者ガイド (英語)」を参照してください。

5 システム設定の構成

インストール後、Sophos Mobile Admin への初回ログイン時に、**開始手順**ウィザードの案内に従ってシステム設定を構成します。

次の情報を入力する必要があります。

- HTTP プロキシサーバーのアドレス (該当する場合)。
- Sophos Mobile のライセンスキー。
- SSL/TLS 証明書。
- SMTP サーバーの認証情報。

注
ここで入力する設定は、すべて「**セットアップ > システム セットアップ**」にて、後から変更することができます。

1. 「**HTTP プロキシ**」ページで、アウトバウンドの HTTP 接続や SSL/TLS 接続に使用するプロキシサーバーのアドレスとポート番号を入力します。
2. 「**ライセンス**」ページで、ライセンスキーを入力するか、または評価版ライセンスをリクエストします。
   - **Standard 版ライセンスキー**: Mobile の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。
   - **Advanced 版ライセンスキー**: Mobile Advanced の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。最初に Mobile のライセンスキーを入力する必要があります。
   - **評価版の請求**: ソフォスの Web サイトから Sophos Mobile のインストーラをダウンロードする際に使用したメールアドレスを入力します。
3. 「**SSL/TLS**」ページで、Sophos Mobile サーバーとクライアントの間の通信内容を暗号化する SSL/TLS 証明書を設定します。
   a) 「**証明書の自動検出**」をクリックします。
      ほとんどの場合、使用中の証明書は自動検出機能で検出できます。
   b) 証明書が自動的に検出されない場合は、手動でアップロードします。「**ファイルのアップロード**」をクリックし、該当する CER 形式または DER 形式の証明書ファイルを選択します。

   ネットワークの構成によっては、インターネットまたは組織内のイントラネットから接続しているクライアントに対して異なる証明書を使用している場合があるため、証明書は 4つまで設定できます。この証明書リストの情報は Sophos Mobile サーバーからクライアントに送信されます。クライアントは、SSL または TLS 接続を確立する際、リストに含まれる証明書が提示された場合のみサーバーを信頼します (Certificate Pinning: 証明書のピン留め)。

   重要
   SSL 証明書を変更または更新した際は、証明書のリストを更新してください。少なくとも 1 つの証明書が常に利用可能な状態になっている必要があります。そうでない場合、信頼できるサーバーがなくなり、クライアントがサーバーに接続できなくなります。

4. 「**SMTP**」ページに SMTP サーバーの詳細とログオンの認証情報を設定します。SMTP を設定します。新しいユーザーにログイン用のアカウント情報をメールで送信するのに必要です。この設定は、メールによるデバイスの登録を行うためにも必要です。

オプション	説明
SMTP ホスト	SMTP サーバーのアドレス。
接続ポート	接続先のサーバーのポート。 **注** 表示される接続タイプ (TLS、SSL、および暗号化なし) では、ポートの標準的な使用を想定しています。どのポートを使用するかに関するガイドラインは、SMTP サーバーのドキュメントを参照してください。
SMTP ユーザー	SMTP サーバーで要求された場合に入力する、接続が許可されているユーザーの名前。
SMTP パスワード	SMTP ユーザーのパスワード。
メール送信元	Sophos Mobile からの送信されるメールの差出人欄に表示されるメールアドレス。
送信者名	差出人欄に表示される送信者の名前。 必要に応じてカスタマーごとに異なる送信者名を設定できますが、異なるメールアドレスは設定できません。詳細は、「Sophos Mobile 管理者ヘルプ」を参照してください。
エラーメールの送信	APNs 証明書の有効期限が切れた場合など、Sophos Mobile からエラーに関するメールを送信できます。
メール受信者	エラーに関するメールを受信するユーザーのメールアドレス。

注
Sophos Mobile は、SMTP 認証に関する OAUTH メカニズムには対応していません。OAUTH を使用するメールプロバイダ (例: Google Gmail) では、Sophos Mobile がサインインを行おうとする動作を安全ではない動作に分類する可能性があります。

5. SMTP の情報を設定したら、「**テストメールの送信**」をクリックしてメールの設定を検証します。
6. 「**完了**」をクリックして**開始手順**ウィザードを完了させます。

6 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。

Sophos Mobile の初期設定の段階で Mobile Advanced ライセンスのアクティベーションを行わなかった場合は、スーパー管理者として後から Sophos Mobile Admin にてアクティベーションを実行できます。

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。

7 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。

  スーパー管理者がカスタマーに対する上限を設定しなかった場合、ライセンスの最大数は、Sophos Mobile サーバーの総数となります。
- **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。
- **対象 URL**: ライセンスが発行されている Sophos Mobile サーバーの URL。

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。

8 カスタマーの作成

この操作を行うには、スーパー管理者として Sophos Mobile Adminにログインする必要があります。

1. サイドバーのメニューの「**管理**」で、「**カスタマー**」をクリックします。
2. 「**カスタマーの作成**」をクリックします。
3. 「**カスタマーの編集**」ページで次の項目を設定します。

オプション	説明
名前	カスタマーの名前。
説明	カスタマーアカウントの概略。
ライセンスの最大数	カスタマーで管理可能なデバイスユーザーと割り当てられていないデバイスの数。
拡張ライセンス	選択した場合、カスタマーは Sophos Mobile を使用して Sophos Mobile Security、Sophos Secure Workspace、Sophos Secure Email アプリを一元管理できるようになります。
有効期限	カスタマーに割り当てられているライセンスの有効期限。この日付を過ぎると、カスタマーで管理するデバイスに対して新しいタスクを作成できなくなります。
アカウントを無効にする	選択した場合、対象のカスタマーのアカウントにログインできなくなります。この設定を有効にした場合でも、スーパー管理者として、画面右上のカスタマーリストから無効化されたカスタマーのビューに切り替えることができます。 無効化したアカウントは「**アカウントを無効にする**」チェックボックスの選択を外すと、もう一度有効化することができます。
有効なプラットフォーム	登録可能なデバイスのプラットフォームを選択します。
デバイスのプライバシー設定	ユーザーが所有するデバイスが盗難・紛失に遭った際、位置情報の取得をユーザーに許可する場合は、「**デバイスの位置情報の取得をユーザーに許可**」を選択します。 管理者に位置情報の取得を許可する場合は、「**デバイスの位置情報の取得を管理者に許可**」を選択します。 「**インストール済みアプリの表示**」を選択して、デバイスの詳細にインストール済みのアプリを表示します。
クローン設定	スーパー管理者アカウントで作成する、すべてのプロファイル、バンドル、パッケージをカスタマーのアカウントで利用できるようにするには、「**設定とパッケージ**」チェックボックスを選択します。
ユーザーディレクトリ	Sophos Mobile で管理するセルフサービス ポータル (SSP) のユーザーのデータソースを選択するオプション。 以下から選択します。

オプション	説明
	• **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。**：選択すると、セルフサービス ポータルのユーザーアカウントを作成することができなくなります。また、LDAP ディレクトリから Sophos Mobile Adminのアカウントを検索することもできなくなります。 • **内部ディレクトリ**: Sophos Mobile Adminとセルフサービス ポータルに対して内部ユーザー管理を使用するようになります。詳細は、「Sophos Mobile 管理者ヘルプ」を参照してください。 • **外部 LDAP ディレクトリ**: 内部ユーザー管理を使用できるほか、LDAP ディレクトリから Sophos Mobile Adminやセルフサービス ポータルのアカウントが検索できるようになります。「**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. 「**保存**」をクリックします。

カスタマーが作成されます。

9 カスタマーの切り替え

前章で作成したカスタマーの初期設定を完了するには、スーパー管理者カスタマーから作成したカスタマーへ切り替える必要があります。

新しいカスタマーのビューに切り替える方法は次のとおりです。

1. スーパー管理者ビューの画面右上で、現在のカスタマー名をクリックして利用できるカスタマーのリストを開きます。

   スーパー管理者は、ドロップダウンリストの上部にアスタリスク付きで表示されます。
2. 前章で作成したカスタマーを選択します。

ビューが作成したカスタマーのビューに切り替わります。このビューは、このカスタマーの監理者としてログインすると表示されるビューです。

10 カスタマーの管理者の作成

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「**管理者の作成**」をクリックします。
3. 「**管理者の編集**」ページで、管理者アカウントの詳細を設定します。
   - カスタマーのユーザーディレクトリに「**外部 LDAP ディレクトリ**」が選択されている場合は、「**LDAP によるユーザー検索**」をクリックして既存の LDAP アカウントを選択できます。
   - カスタマーのユーザーディレクトリに「**内部ディレクトリ**」または「**なし**」が選択されている場合は、「**ログイン名**」、「**名**」、「**姓**」、「**メールアドレス**」、「**パスワード**」欄に情報を入力します。

   ここで指定するパスワードはワンタイムパスワードです。アカウントを作成した後、管理者が最初にログインした際にパスワードの変更を促すメッセージが表示されます。
4. 「**ロール**」リストから「**Administrator**」というユーザーロールを選択します。
5. 「**保存**」をクリックすると、管理者アカウントが作成されます。

カスタマーの設定を進めるには、Sophos Mobile Adminからログアウトし、上記で作成した管理者のアカウント情報 (カスタマー名、ログイン名、ワンタイムパスワード) でログインしなおします。

11 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

11.1 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。

前提条件: 新しいカスタマーに対して作成された管理者として Sophos Mobile Adminにログインしている必要があります。

1. サイドバーのメニューの「**設定**」の下で「**セットアップ > 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	このカスタマーで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**

オプション	説明
	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。 **注** 選択可能なプラットフォームの種類は、スーパー管理者の設定内容によって異なります。詳細は「Sophos Mobile スーパー管理者向けガイド (英語)」を参照してください。

3. 「**保存**」をクリックします。

11.2 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。外部ユーザーの管理については、「Sophos Mobile スーパー管理者向けガイド (英語)」を参照してください。

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。

11.3 サポートへの問い合わせ情報の設定

問題や質問がある場合、ユーザーが組織内のサポート部門に連絡するための問い合わせ先を設定できます。

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. 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。

12 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。

Sophos Mobile では APNs 証明書はカスタマーごとに管理されます。使用する各カスタマーごとに証明書を作成し、アップロードする必要があります。

APNs 証明書は 1年間有効です。

APNs 証明書を更新する際は、同じ証明書を使用しているすべてのカスタマーに対して、スーパー管理者が同時に更新操作を行うことができます。詳細は、「Sophos Mobile 管理者ヘルプ」を参照してください。

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 サーバーへの取得するのに必要な要件と操作手順を説明しています。

12.1 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)

12.2 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 > システム 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。証明書要求ファイルは、カスタマーごとに固有のものです。
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。

13 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。

13.1 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、スーパー管理者が、内部 EAS プロキシまた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、「Sophos Mobile スーパー管理者向けガイド (英語)」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、スーパー管理者がネットワーク 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、「Sophos Mobile スーパー管理者向けガイド (英語)」を参照してください。 このアクションは、Sophos Mobile で Sophos コンテナのみ管理しているデバイスでは実行できません。
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。 **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。

14 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。

14.1 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。

15 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。

注
プラットフォームに応じて、デバイスのプロファイル (Android、iOS)、またはポリシー (macOS、Windows、Windows Mobile) を使用してデバイスの設定を構成します。わかりやすくするために、ここではプロファイルとポリシーのどちらを指す場合でも「ポリシー」という用語を使用します。

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**」を選択します。
3. 「**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。
4. 「**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。
5. 「**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。
   「**デバイスで仕事用データと個人データを分離**」を選択すると、デバイスの OS でサポートされている場合は、個人アプリでの仕事用データの共有 (またはその逆) ができなくなります。
6. 「**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。
7. 「**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。
8. 「**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「**プロファイルとポリシー**」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。

16 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. 任意: 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. 17)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. 「**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。
6. 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。
7. 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。
8. 任意: 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。

9. 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。

17 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. 任意: 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. 17)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. 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. 任意: 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。

18 セルフサービス ポータルの設定

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**」をクリックします。
2. 「**登録テキスト**」をクリックして利用条件と登録後の操作に関する文章を追加します。
   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**」をクリック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**」をクリック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**」をクリックして、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**」をクリックします。
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。 登録の種類を選択するセルフサービスポータルの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	登録するデバイスが、会社のデバイス、あるいは個人のデバイスのどちらであるかを選択します。
デバイスグループ	登録するデバイスを割り当てるグループを選択します。
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を選択します。 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。

オプション	説明
	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を選択します。 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**」をクリックして、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**」をクリックして、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**」をクリックします。

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。

19 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。

注
ここでの手順は、内部ユーザー管理を使用するカスタマーが作成されていることを前提に書かれています。詳細はカスタマーの作成 (p. 9)を参照してください。外部ユーザーの管理については、「Sophos Mobile スーパー管理者向けガイド (英語)」を参照してください。

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。

20 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. 26)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。

21 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。

外部ユーザーの管理については、「Sophos Mobile スーパー管理者向けガイド (英語)」を参照してください。

最大 500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**」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。

22 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 > デバイスウィザードの追加**」の順にクリックします。

   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**」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。
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。 ログインしているカスタマーに対して有効化されているプラットフォームのみ選択できます。
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. 「**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。

注
Mac では、Sophos Mobile の管理対象ユーザーが登録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。

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。

23 用語集

カスタマー	Sophos Mobile 内の分離された管理領域を指します。複数のカスタマーを設定し、各カスタマーのデバイスを独立して管理することができます。この方式は、マルチテナントともいいます。
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、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。
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。

24 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

25 利用条件