

SOPHOS

Security made simple.

Sophos Mobile

ユーザーヘルプ

製品バージョン: 8.1



目次

このヘルプについて.....	1
Sophos Mobile について.....	2
セルフサービス ポータルへのログイン.....	3
初回ログイン.....	3
ログイン.....	3
パスワードの復旧.....	3
ログアウト.....	4
デバイスでの Sophos Mobile のセットアップ.....	5
Android デバイスの登録方法.....	5
iOS デバイスの登録方法.....	5
Mac の登録方法.....	5
Windows Phone と Windows Mobile デバイスの登録方法.....	6
Windows コンピュータの登録方法.....	6
登録後に設定される内容.....	7
セルフサービス ポータルを使用したモバイルデバイスの管理.....	8
デバイスの同期.....	8
コンプライアンス違反の表示.....	8
デバイスのロック.....	9
紛失モードの有効化.....	9
デバイスのパスワードのリセット.....	10
アプリのロックのパスワードのリセット.....	10
Sophos コンテナのパスワードのリセット.....	11
デバイスの位置情報取得.....	11
デバイスのワイプ.....	12
Android の仕事用プロファイルのワイプ.....	12
Sophos Mobile のデバイス管理の再設定.....	13
Sophos Mobile Control アプリの再設定.....	13
デバイスの登録解除.....	14
登録を解除したデバイスの削除.....	15
サポート問い合わせ先情報の表示.....	15
Sophos Mobile Control アプリを使用したモバイルデバイスの管理.....	16
デバイスの同期.....	16
コンプライアンス違反の表示と対処.....	16
アプリのインストール.....	16
仕事用アプリのインストール.....	17
保護対象アプリのロック.....	17
実行が許可されていないアプリの表示.....	18
管理者が送信するメッセージの表示.....	18
デバイスの登録解除.....	18
サポート問い合わせ先情報の表示.....	19
テクニカルサポート.....	20
利用条件.....	21

1 このヘルプについて

このヘルプでは、Sophos Mobile Control アプリの設定と使用方法、および Sophos Mobile のセルフサービス ポータルの使用方法について説明します。

セルフサービス ポータルで利用できる機能は、各システム固有の設定によって異なることがあります。このヘルプで説明する機能の一部をご利用になれない場合もあります。

2 Sophos Mobile について

Sophos Mobile は、スマートフォンやタブレット端末などのモバイルデバイス、さらに Windows 10 を実行している PC、および Mac 用の管理ツールです。アプリやセキュリティ設定を管理し、企業のデータを安全に保ちます。

Sophos Mobile は、サーバーコンポーネントとクライアントコンポーネントから構成されます。

Sophos Mobile はデバイス上の業務データを安全に保ち、デバイスが社内のセキュリティポリシーに準拠していることを確認します。

セルフサービスポータルを使用すれば、ユーザー自身で使用しているデバイスを Sophos Mobile に登録することができます。また、ヘルプデスク担当者の支援なしで、リモートからの位置情報の取得やデバイスのロック、ワイプ、パスワードのリセットを行うことができます。

3 セルフサービス ポータルへのログイン

3.1 初回ログイン

注

初回ログインの手順は、システムの設定によっては、ここで説明する手順と異なる場合があります。ここでの手順は、Sophos Mobile 内のユーザー管理機能で作成されたユーザーを対象にしています。別の方法でユーザーが管理されている場合は、管理者から必要なログイン情報が届きます。

セルフサービス ポータルへのログイン用 Web アドレスは管理者から通知されます。初回ログインの際は、ユーザー情報とアカウントをアクティベートするリンクが記載された、登録メールも届きます。

セルフサービス ポータルに初回ログインする方法は次のとおりです。

1. セルフサービス ポータルの登録メールに記載されている、アカウントのアクティベーション用リンクをクリックします。
Sophos Mobile セルフサービス ポータルが開き、パスワードの設定画面が表示されます。
2. 新しいパスワードを 2回入力して「**パスワードの変更**」をクリックします。
新しいパスワードでログインした状態で「**ホーム**」ページが表示されます。

3.2 ログイン

注

管理者は、たとえば、予定されているシステムのアップグレードやメンテナンスに関する情報などをログイン画面に表示することができます。メッセージはクリックすると全体が表示されます。

1. Web ブラウザで、セルフサービス ポータルを開きます。
2. ログインの画面でログイン情報を入力し、「**ログイン**」をクリックします。

セルフサービス ポータルにログインされます。セルフサービス ポータルの「**ホーム**」ページが表示されます。

3.3 パスワードの復旧

Sophos Mobile セルフサービス ポータルのログイン用パスワードを忘れた場合は、セルフサービス ポータルのログインダイアログで、「**パスワードを忘れた場合**」をクリックして、パスワードをリセットできます。

3.4 ログアウト

セルフサービス ポータルからログアウトするには、メニューバーのユーザー名をクリックし、「ログアウト」を選択します。

4 デバイスでの Sophos Mobile のセットアップ

デバイスの登録は、セルフサービス ポータルから簡単に行うことができます。

注

セルフサービス ポータルを使用して登録できるデバイスの数は、企業ポリシーによって制限されている場合があります。この場合、登録済みのデバイスの数が指定数に達すると、それ以上デバイスを登録することができなくなります。

1. セルフサービス ポータルで「**デバイスの新規登録**」をクリックします。
2. 画面の指示に従って、デバイスを Sophos Mobile に登録します。

4.1 Android デバイスの登録方法

登録は、大きく 2つのステップで行います。

1. Sophos Mobile Control アプリをデバイスにインストールします。
2. デバイスにインストールしたアプリを設定します。

詳しい手順は、管理者から届くメールを参照してください。セルフサービス ポータルからデバイスを登録する場合は、画面に手順が表示されます。

4.2 iOS デバイスの登録方法

登録は、大きく 2つのステップで行います。

1. Sophos Mobile Control アプリをデバイスにインストールします。
2. デバイスにインストールしたアプリを設定します。

詳しい手順は、管理者から届くメールを参照してください。セルフサービス ポータルからデバイスを登録する場合は、画面に手順が表示されます。

4.3 Mac の登録方法

Sophos Mobile に Mac を登録するには、登録ポリシーをインストールする必要があります。

詳しい手順は、管理者から届くメールを参照してください。セルフサービス ポータルからデバイスを登録する場合は、画面に手順が表示されます。

重要

Sophos Mobile は、登録手順を実行する際に Mac にログインしていたユーザーを管理します。このユーザーを後で変更することはできません。

ヒント

管理者によって Mac に適用された設定を表示するには、「システム環境設定」の下で、「プロファイル」をクリックします。

4.4 Windows Phone と Windows Mobile デバイスの登録方法

登録は、大きく 3つのステップで行います。

1. Sophos Mobile Control アプリをデバイスにインストールします。
2. デバイスにインストールしたアプリを設定します。
3. デバイス上のデバイス管理エージェントを設定します。

詳しい手順は、管理者から届くメールを参照してください。セルフサービス ポータルからデバイスを登録する場合は、画面に手順が表示されます。

4.5 Windows コンピュータの登録方法

Windows コンピュータを Sophos Mobile に登録するには、デバイスでデバイス管理エージェントを設定する必要があります。

詳しい手順は、管理者から届くメールを参照してください。セルフサービス ポータルからデバイスを登録する場合は、画面に手順が表示されます。

5 登録後に設定される内容

デバイスが Sophos Mobile に登録されると、デバイスにインストールされた設定プロファイルの内容に応じて、以下が設定されることがあります。

- 新しいアプリケーションが追加されることがあります。
- デバイスにインストールするアプリが、管理者によって指定されることがあります。アプリの確認とインストールを行うには、デバイスで Sophos Mobile Control アプリを開き、「[アプリ](#)」をタップします。詳細は、[アプリのインストール](#) (p. 16)を参照してください。
- デバイス上のカメラ、YouTube、アプリストアなどのアプリケーションが利用できなくなることがあります。
- 企業のメールサーバーに接続できるように、デバイスのメールアプリケーションがあらかじめ設定されることがあります。
- デバイスが企業ポリシーに違反すると (ポリシーに準拠していないアプリがインストールされた場合など)、Sophos Mobile の通知アイコンが表示されます。(iOS を使用している場合、デバイスに通知を表示する方法についてはアップルの製品ドキュメントを参照してください。)Sophos Mobile Control アプリでは、すべての違反を表示できます。詳細は、[コンプライアンス違反の表示と対処](#) (p. 16)を参照してください。また、登録済みのデバイスで発生しているコンプライアンス違反をセルフサービス ポータルで表示することもできます。詳細は、[コンプライアンス違反の表示](#) (p. 8)を参照してください。
- 管理者がデバイス上の特定のアプリに対して、アプリのロックを設定した場合、設定後のアプリ初回起動時にパスワードを設定する必要があります。ここで設定するパスワードは、以後、対象のアプリを起動する際やデバイスがロックされた後に、毎回入力する必要があります。保護対象アプリは、Sophos Mobile Control アプリで表示できます。すべての保護対象アプリを一度にロックすることもできます。詳細は、[保護対象アプリのロック](#) (p. 17)を参照してください。
- Sophos Mobile Control アプリでメールのパスワードを入力するようメッセージが表示されることがあります。
- Samsung Knox 対応の Android デバイスの場合、Samsung Knox の使用許諾契約への同意するようメッセージが表示されることがあります。これは、ソフォスの MDM 機能をデバイスに登録するには必須です。Samsung Knox ライセンスは無料です。Samsung Knox Premium ライセンスは必要ありません。
- Android デバイスの登録作業中に仕事用プロファイルを作成した場合、デバイス全体ではなく、このプロファイルのみが Sophos Mobile によって管理されます。個人のデータやアプリは制御されません。仕事用プロファイルの詳細は、[ビジネス向け Android ヘルプ \(外部リンク\)](#) を参照してください。
- Sophos コンテナのみを登録した場合、Sophos Mobile は、個人のデータやアプリなど、Sophos コンテナ外のデータにはアクセスしません。

注

登録を解除した結果として、デバイスから設定が削除されると、すべてのデータ (メール、予定表の項目、連絡先) や追加された管理対象アプリも削除されます。

6 セルフサービス ポータルを使用したモバイルデバイスの管理

Sophos Mobile にデバイスが登録されると、セルフサービス ポータルを使用して管理が行えるようになります。

6.1 デバイスの同期

注

この機能は、特定の機種デバイスに対応していない、または、管理者によって無効化されている場合があります。

セルフサービス ポータルを使用して、お使いのデバイスと Sophos Mobile サーバーを手動で同期することができます。

この操作は、たとえば、以下のような状況で役立ちます。

- デバイスの電源が長期間オフになっていたため、サーバーと同期されていない。この場合、デバイスはポリシーに準拠していないため、たとえば、メールの受信などができなくなります。デバイスを再度ポリシーに準拠させるには、Sophos Mobile サーバーと同期させる必要があります。
- デバイスが他の何らかの理由（禁止するアプリを含むなど）でポリシーに準拠しておらず、企業ポリシーに準拠するためにはデバイスでの変更が必要である。必要な変更を行った後、Sophos Mobile サーバーとデバイスを同期させる必要があります。

デバイスを手動で同期する方法は次のとおりです。

1. セルフサービスポータルで、「**マイ デバイス**」をクリックして、該当するデバイスをクリックします。
2. 「**アクション**」、「**データの更新**」の順にクリックします。

6.2 コンプライアンス違反の表示

注

この機能は、特定の機種デバイスに対応していない、または、管理者によって無効化されている場合があります。

使用しているデバイスのコンプライアンス違反をセルフサービス ポータルで確認することができます。

1. セルフサービスポータルで、「**マイ デバイス**」をクリックして、該当するデバイスをクリックします。
2. 「**コンプライアンス状態**」をクリックします。
「**コンプライアンス状態**」は、デバイスがコンプライアンスに準拠していない場合のみに表示されます。

コンプライアンス準拠に必要なアクションをデバイスで実行します。

6.3 デバイスのロック

注

この機能は、特定の機種 of デバイスに対応していない、または、管理者によって無効化されている場合があります。

盗難・紛失にあった場合、デバイスをリモートからロックできます。

1. セルフサービスポータルで、「**マイ デバイス**」をクリックして、該当するデバイスをクリックします。
2. 「**アクション**」、「**ロック**」の順にクリックします。

iOS デバイスの場合、デバイスのロックが完了した後、画面に表示するメッセージ (半角文字の場合 300文字以内) を入力できます。たとえば、デバイスの拾得者に対して連絡先を知らせるメッセージなどを入力できます。「**表示する電話番号**」フィールドに電話番号を入力すると、タップするだけで発信できるリンクとして、ロックされた画面のメッセージに表示されます。

Mac の場合、ロック解除するために Mac で入力が必要な 6桁の PIN を設定します。

デバイスが現在のパスワードでロックされます。Mac の場合はシステムロック PIN でロックされます。

6.4 紛失モードの有効化

注

このセクションの内容は、iOS デバイスのみを対象にしています。

盗難・紛失にあった場合、iOS デバイスを紛失モードに切り替えることができます。

紛失モードに切り替えたデバイスで実行できるのは次の操作のみです。

- 管理者が設定した電話番号に発信する。
- 緊急通話を行う。

重要

セルフサービスポータルで紛失モードに切り替えた場合、iCloud で無効にすることはできません。また、その逆も同様です。

紛失モードを有効に設定する方法は次のとおりです。

1. セルフサービスポータルで、「**マイ デバイス**」をクリックして、該当するデバイスをクリックします。
2. 「**アクション**」、「**紛失モードの有効化**」の順にクリックします。
3. 次の設定を行います。

オプション	説明
ロック画面のメッセージ	画面ロック時に表示されるテキスト。
ロック画面の電話番号	画面ロック時にかけることのできる電話番号。
脚注	画面ロック時に画面の下に表示される脚注。 脚注を設定しない場合、管理者に問い合わせることを指示する標準のメッセージが表示されます。

4. 操作を確定します。デバイスで、ただちに紛失モードが有効になります。

デバイスで紛失モードが有効になっている場合、セルフサービス ポータルで次の操作を行うことができます。

- デバイスの位置情報を確認するには、「位置情報取得 (Locate)」を使用します。
- デバイスで音を鳴らすには、「紛失モードのサウンドの再生」を使用します。
- 紛失モードを無効に設定するには、「紛失モードの無効化」を使用します。

6.5 デバイスのパスワードのリセット

注

この機能は、特定の機種種のデバイスに対応していない、または、管理者によって無効化されている場合があります。

デバイスのパスワードをセルフサービス ポータルからリモートでリセットできます。

1. セルフサービスポータルで、「マイ デバイス」をクリックして、該当するデバイスをクリックします。
2. 「アクション」、「パスワードのリセット」の順にクリックします。
3. 表示されるメッセージを確定するか、または手順に従います。
Android、Windows、および Windows Mobile デバイスの場合は、自動で新しいパスワードが作成され、セルフサービス ポータルに表示されます。iOS の場合は、デバイスロックに使用する新しいパスワードを入力します。

デバイスがロックされますが、入力した新しいパスワードでロックを解除できます。

6.6 アプリのロックのパスワードのリセット

注

このセクションの内容は、Android デバイスのみを対象にしています。

管理者がデバイス上の特定のアプリに対して、アプリのロックを設定した場合、設定後のアプリ初回起動時にパスワードを設定する必要があります。ここで設定するパスワードは、アプリを起動する際やデバイスがロックされた後に毎回入力する必要があります。パスワードはセルフサービス ポータルでリセットできます。

1. セルフサービスポータルで、「マイ デバイス」をクリックして、該当するデバイスをクリックします。

2. 「アクション」、「アプリのロックパスワードのリセット」の順にクリックします。
3. ダイアログボックスで、「新しいパスワード」フィールドに新しいパスワードを入力し、確認入力します。
4. 「パスワードのリセット」をクリックします。

6.7 Sophos コンテナのパスワードのリセット

注

この機能は、管理者によってデバイスに Sophos コンテナがインストールされている場合のみに利用できます。

Sophos コンテナのパスワードは、セルフサービス ポータルからリモートでリセットできます。このパスワードは、Sophos Secure Workspace と Sophos Secure Email の両方のアプリで使用します。

1. セルフサービスポータルで、「マイ デバイス」をクリックして、該当するデバイスをクリックします。
2. 「アクション」、「Sophos コンテナのパスワードのリセット」の順にクリックします。

Sophos コンテナのパスワードが削除されます。新しいパスワードを設定してください。

6.8 デバイスの位置情報取得

注

この機能は、特定の機種種のデバイスに対応していない、または、管理者によって無効化されている場合があります。

盗難・紛失にあった場合、Google マップでデバイスの現在地を表示できます。

注

iOS や Windows Mobile デバイスの場合、デバイスでメッセージが確認されないと現在地を表示できないため、位置情報取得機能は限られた範囲での利用となります。

1. デバイスの位置情報サービスがオンになっており、Sophos Mobile Control アプリで位置情報の使用が許可されていることを確認してください。
2. セルフサービスポータルで、「マイ デバイス」をクリックして、該当するデバイスをクリックします。
3. 「アクション」、「位置情報の取得」の順にクリックします。
タスクが作成されデバイスに送信されます。
4. デバイスの詳細で、「現在位置」をクリックすると、デバイスの位置が Google マップに表示されます。

6.9 デバイスのワイプ

注

この機能は、特定の機種デバイスに対応していない、または、管理者によって無効化されている場合があります。

注

このセクションの内容は、仕事用プロファイルのみが Sophos Mobile で管理されている Android デバイスには当てはまりません。このようなデバイス上の仕事用プロファイルをワイプする場合は、[Android の仕事用プロファイルのワイプ](#) (p. 12)を参照してください。

盗難・紛失にあった場合、デバイスをリモートからワイプする (出荷時の状態に戻す) ことができます。ワイプが必要かどうかがよくわからない場合は、社内のサポート部門にお問い合わせください。

重要

デバイスをワイプすると、すべてのデータが削除されます。この操作は元に戻せません。

1. セルフサービスポータルで、「マイ デバイス」をクリックして、該当するデバイスをクリックします。
2. 「アクション」、「ワイプ」の順にクリックします。
Mac の場合、ワイプされた後に、Mac をロック解除するために入力が必要な 6桁の PIN を設定します。

デバイスは出荷時の状態にリセットされます。すべてのデータが削除されます。

6.10 Android の仕事用プロファイルのワイプ

Sophos Mobile によって仕事用プロファイルのみが管理されている Android デバイスが盗難・紛失にあった場合、リモートでデバイスから仕事用プロファイルを削除できます。この操作を実行すると、Sophos Mobile Control アプリを含む、すべての仕事用アプリやデータがデバイスから削除されます。個人のデータやアプリは削除されません。Android の仕事用プロファイルをワイプするべきか判断しかねる場合は、社内のサポート部門に問い合わせてください。

重要

仕事用プロファイルをデバイスから削除した場合、元に戻すことはできません。

1. セルフサービスポータルで、「マイ デバイス」をクリックして、該当するデバイスをクリックします。
2. 「アクション」、「Android の仕事用プロファイルのワイプ」の順にクリックします。
仕事用プロファイルが削除されます。デバイスの Sophos Mobile への登録が解除されました。

6.11 Sophos Mobile のデバイス管理の再設定

セルフサービスポータルや Sophos Mobile Control アプリを使用せずに、手動で Sophos Mobile のデバイス管理機能を無効にした場合、デバイスはセルフサービスポータルの管理下にあるデバイスのリストに表示されたままとなります。デバイスを管理下に置くには、デバイスを再設定する必要があります。

1. セルフサービスポータルで、「マイ デバイス」をクリックして、該当するデバイスをクリックします。
2. 「アクション」、「再設定」の順にクリックします。
管理下にあるデバイスの場合には登録が解除されるという警告メッセージが表示されます。

デバイスが Sophos Mobile サーバーへの接続を開始します。デバイスの通信速度によっては、再設定が開始するまで時間がかかることがあります。

デバイスでの [Sophos Mobile のセットアップ](#) (p. 5)に記載されている手順に沿って登録処理を行います。処理が完了すると、デバイスが再び Sophos Mobile に登録されます。

6.12 Sophos Mobile Control アプリの再設定

注

このセクションの内容は、iOS デバイスと Windows Mobile デバイスのみを対象にしています。

管理下のデバイスから Sophos Mobile Control アプリが誤ってアンインストールされてしまった場合は、次の手順を実行する必要があります。

- アプリを再インストールします。
- アプリを再設定し、Sophos Mobile サーバーに接続し直します。

注

このセクションの内容は、デバイスの Sophos Mobile デバイス管理 (MDM) アカウントも削除されている場合には当てはまりません。そのような場合は、デバイスを再設定する必要があります。詳細は、「[Sophos Mobile のデバイス管理の再設定](#) (p. 13)」を参照してください。

Sophos Mobile Control アプリを再設定する方法は次のとおりです。

1. セルフサービスポータルで、「マイ デバイス」をクリックして、該当するデバイスをクリックします。
2. 「アクション」、「SMC アプリの再設定」の順にクリックします。
詳細な手順が記載されたページが表示されます。
3. Sophos Mobile Control アプリを使用して、表示されている QR コードを読み取るか、表示されている設定の詳細を手動で入力します。

Sophos Mobile Control アプリが、再び Sophos Mobile サーバーに接続されます。

6.13 デバイスの登録解除

注

このセクションの内容は、仕事用プロファイルのみが Sophos Mobile で管理されている Android デバイスには当てはまりません。そのようなデバイスを登録解除する場合は、[Android の仕事用プロファイルのワイプ](#) (p. 12)を参照してください。

セルフサービス ポータルを使用して、デバイスを Sophos Mobile の登録から解除することができます。登録の解除は、新しいデバイスを取得したなどの理由で、管理下にあるデバイスを使用しなくなった場合に行います。

重要

登録を解除したデバイスを元に戻すことはできません。

1. セルフサービスポータルで、「**マイ デバイス**」をクリックして、該当するデバイスをクリックします。
2. 「**アクション**」、「**登録解除**」の順にクリックします。

デバイスが、デバイス管理から登録解除されます。これにより以下の影響があります。

- Android デバイスの場合:
 - Sophos Mobile Control のデバイス管理機能が無効化されます。
 - Sophos Samsung Plugin のデバイス管理機能が無効化されます (インストールされていた場合)。
 - アプリからすべてのデータが削除されますが、アプリはデバイスに残ります。必要な場合は、Sophos Mobile Control アプリを手動でアンインストールしてください。
 - Sophos コンテナアプリ (Sophos Secure Workspace および Sophos Secure Email) と Sophos Mobile Security アプリはリセットされます。
- ビジネス向け Android (デバイス所有者モード) で Sophos Mobile Control に登録している Android デバイスの場合:
 - デバイスがワイプされます。
- iPhone および iPad の場合:
 - MDM の基本プロファイルや、その他のプロファイル、および Sophos Mobile によってインストールされた管理対象アプリがすべて削除されます。
 - Sophos Mobile Control アプリがアンインストールされます。
 - デバイスに指定されていた制限内容が解除されます。
 - Sophos Mobile によって設定されたアカウントおよび関連したデータはすべて削除されます。これには企業メールも含まれます。
 - Sophos Mobile から取得したアプリ (「管理対象アプリ」と呼ばれます) はすべて削除されません。
 - Sophos Mobile から取得した証明書はすべて削除されます。
 - Sophos コンテナアプリ (Sophos Secure Workspace および Sophos Secure Email) はリセットされます。
- Mac の場合:
 - Sophos Mobile によってインストールされた登録ポリシー、およびその他のデバイス/ユーザーポリシーはすべて削除されます。

- デバイスに指定されていた制限内容が解除されます。
- Sophos Mobile によって設定されたアカウントおよび関連したデータはすべて削除されます。これには企業メールも含まれます。
- Sophos Mobile から取得した証明書はすべて削除されます。
- Windows Phone デバイスと Windows Mobile デバイスの場合:
 - Sophos Mobile Control アプリとすべてのポリシーがデバイスから削除されます。
 - サーバーへのログインデータや、サーバーから受信した他のデータすべてが削除されます。
- Windows コンピュータの場合:
 - デバイスから Sophos Mobile のデバイス管理 (MDM) アカウントが削除されます。
 - サーバーへのログインデータや、サーバーから受信した他のデータすべてが削除されます。

6.14 登録を解除したデバイスの削除

デバイスは、登録解除またはワイプした後、セルフサービス ポータルを使用して、管理システムから削除することができます。

1. セルフサービスポータルで、「マイ デバイス」をクリックして、該当するデバイスをクリックします。
2. 「アクション」、「削除」の順にクリックします。

削除したデバイスがデバイスの一覧に表示されなくなります。

6.15 サポート問い合わせ先情報の表示

テクニカルサポートの問い合わせ先情報やその他の情報をセルフサービス ポータルで確認することができます。

メニューバーの「サポート」をクリックします。

「サポート」ページが開き、テクニカルサポートの問い合わせ先情報や追加情報が確認できます。

7 Sophos Mobile Control アプリを使用したモバイルデバイスの管理

Sophos Mobile にデバイスを登録し、Sophos Mobile Control アプリがインストールされると、次のセクションで説明する操作が Sophos Mobile Control アプリで実行できるようになります。ほとんどの機能の利用にはインターネットへの接続環境が必要です。

7.1 デバイスの同期

Sophos Mobile Control アプリでは、手動でデバイスを Sophos Mobile サーバーと同期させることができます。

この操作は、たとえば、以下のような状況で役立ちます。

- デバイスの電源が長期間オフになっていたため、サーバーと同期されていない。この場合、デバイスがポリシーに準拠していないため、たとえば、デバイスでメールを受信することなどができなくなります。デバイスをもう一度ポリシーに準拠させるには、Sophos Mobile サーバーと同期する必要があります。
- デバイスが他の何らかの理由 (禁止するアプリを含むなど) でポリシーに準拠しておらず、企業ポリシーに準拠するためにはデバイスでの変更が必要である。必要な変更を行った後、Sophos Mobile サーバーとデバイスを同期する必要があります。

デバイスを手動で同期する方法は次のとおりです。

1. デバイスで Sophos Mobile Control アプリを開きます。
2. ダッシュボードで「**今すぐ同期**」をタップします。

7.2 コンプライアンス違反の表示と対処

デバイスが企業ポリシーに違反すると (禁止するアプリがインストールされた場合など)、Sophos Mobile の通知アイコンがデバイスに表示されます。

Sophos Mobile Control アプリでは、次の手順ですべての違反を表示できます。

1. デバイスで Sophos Mobile Control アプリを開きます。
2. ダッシュボードで、デバイスのコンプライアンス状態が表示されている最上部の項目をタップします。
コンプライアンス違反の一覧が表示されます。
3. 違反項目の横の「**今すぐ対処**」をタップし、手順に従ってコンプライアンス違反に対処します。

7.3 アプリのインストール

注

Sophos Mobile で仕事用プロファイルのみを管理している Android デバイスの場合は、[仕事用アプリのインストール](#) (p. 17) を参照してください。

デバイスにインストールするアプリは、管理者によって指定されている場合があります。指定されているアプリは、Sophos Mobile Control アプリから直接インストールできます。

1. デバイスで Sophos Mobile Control アプリを開きます。
2. ダッシュボードで「アプリ」をタップします。
3. インストールするアプリをタップし、手順に従ってインストールします。

注

デバイスの種類によっては、管理者がアプリを直接デバイスにインストールすることもあります。この場合、確認メッセージが表示されない場合もあります。

7.4 仕事用アプリのインストール

注

このセクションの内容は、仕事用プロファイルのみが Sophos Mobile で管理されている Android デバイスを対象にしています。

デバイスにインストールする仕事用アプリは、管理者によって指定されている場合があります。指定されているアプリは、Google Play ストア アプリから仕事用プロファイルにインストールできます。

1. デバイスで、ブリーフケースのマークが付いている Google Play ストア アプリをタップします。
2. インストールするアプリを参照します。
3. アプリのページで、「インストール」をタップし、表示されるインストール手順に従います。

注

仕事用アプリは、確認メッセージなしで、管理者が直接デバイスにインストールしたり、アンインストールしたりすることがあります。

7.5 保護対象アプリのロック

注

このセクションの内容は、Android デバイスのみを対象にしています。

管理者がデバイス上の特定のアプリに対して、アプリのロックを設定した場合、設定後のアプリ初回起動時にパスワードを設定する必要があります。設定後、アプリはパスワードで保護されます。パスワードは、アプリを起動する際やデバイスがロックされた後に毎回入力する必要があります。保護対象アプリは、Sophos Mobile Control アプリで表示できます。すべての保護対象アプリを一度にロックすることもできます。この操作は、他の人にデバイスを貸す場合など、保護対象アプリが使用されないようにロックできるため便利です。

注

パスワードはセルフサービス ポータルでリセットできます。

1. デバイスで Sophos Mobile Control アプリを開きます。

2. ダッシュボードで「**アプリのロック**」をタップします。
「**保護対象アプリ**」の下に管理者が設定した保護対象アプリがすべて表示されます。
3. 「**一覧にあるアプリをロック**」をタップします。

7.6 実行が許可されていないアプリの表示

注

このセクションの内容は、Android デバイスのみを対象にしています。

管理者が特定のアプリに対して**アプリ コントロール**を設定している場合、対象のアプリをデバイスで実行することはできません。実行できないアプリは、Sophos Mobile Control アプリで表示できません。

1. デバイスで Sophos Mobile Control アプリを開きます。
2. ダッシュボードで「**アプリ コントロール**」をタップします。
「**アプリ コントロール**」の下に実行が許可されていないアプリの一覧が表示されます。

7.7 管理者が送信するメッセージの表示

管理者は、ユーザーのデバイスにメッセージを送信することができます。メッセージが届くと、通知が表示されます。受信したメッセージは、Sophos Mobile Control アプリで閲覧できます。

1. デバイスで Sophos Mobile Control アプリを開きます。
2. ダッシュボードで「**メッセージ**」をタップします。
これまでに受信したすべてのメッセージが表示されます。メッセージは個別に削除できます。

ヒント

メッセージの受信の通知をタップして Sophos Mobile Control アプリを開きます。

注

Sophos Mobile 4 で管理が行われている場合、メッセージを「**メッセージ**」に表示させるには、通知を確認する必要があります。






7.8 デバイスの登録解除

注

この機能は、特定の機種デバイスに対応していない、または、管理者によって無効化されている場合があります。

Sophos Mobile Control アプリを使用して、デバイスを Sophos Mobile から登録解除することができます。登録を解除すると、サーバーとの接続が切断され、すべての関連データが削除されますが、Sophos Mobile Control アプリはアンインストールされません。

デバイスの登録を解除するには、デバイス上の Sophos Mobile Control アプリを開き、次の操作を実行します。

- Android の場合:
 - a) ダッシュボードのタイトルバーのメニューキー  をタップし、「バージョン情報」をタップします。
 - b) 「バージョン情報」で「登録解除」をタップします。
- iOS の場合:
 - a) ダッシュボードのタイトルバーで、「バージョン情報 」、「登録解除」の順にタップします。
- Windows Mobile の場合、Sophos Mobile Control 2017 アプリで次の手順を実行します。
 - a) ダッシュボードのタイトルバーの「サポート 」をタップします。
 - b) 「サポート」のタイトルバーで、「登録解除 」をタップします。
- Windows Phone および Windows Mobile の場合、Sophos Mobile Control アプリで次の手順を実行します。
 - a) ダッシュボードで「設定」をタップします。
 - b) 「設定」の一番下のメニューキー  をタップし、「登録解除」をタップします。

7.9 サポート問い合わせ先情報の表示

Sophos Mobile Control アプリでは、テクニカルサポートの問い合わせ先情報やその他の情報を表示することができます。

1. デバイスで Sophos Mobile Control アプリを開きます。
2. ダッシュボードで「サポート」をタップします。

ヒント

「メール」、「電話番号」、「携帯電話番号」フィールドのいずれかをタップし、社内のサポート担当者にメールを送信したり、電話をかけたりすることができます。

8 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わせ。 <https://secure2.sophos.com/ja-jp/support/contact-support/support-query.aspx>

9 利用条件

Copyright © 2018 Sophos Limited. All rights reserved. この出版物の一部または全部を、電子的、機械的な方法、写真複写、録音、その他いかなる形や方法においても、使用許諾契約の条項に準じてドキュメントを複製することを許可されている、もしくは著作権所有者からの事前の書面による許可がある場合以外、無断に複製、復元できるシステムに保存、または送信することを禁じます。

Sophos、Sophos Anti-Virus および SafeGuard は、Sophos Limited、Sophos Group および Utimaco Safeware AG の登録商標です。その他記載されている会社名、製品名は、各社の登録商標または商標です。