SOPHOS

Cybersecurity made simple.

Sophos Mobile インストールガイド

製品バージョン: 9.6

目次

1 このガイドについて

このガイドでは、Sophos Mobile 9.6 のインストールおよび設定の方法について説明しています。また、既にインストールされている Sophos Mobile をアップデートする方法についても説明しています。

特に記載されていない限り、すべての手順は、Microsoft Windows Server の管理者または管理グループのユーザーとして実行する必要があります。

2 Sophos Mobile について

Sophos Mobile

Sophos Mobile は、モバイルデバイスのセキュリティ管理に割けるリソースが限られている企業に最適な EMM ソリューションです。直感的に使用できるクラウド管理型の Sophos Central Admin コンソールで、エンドポイント、ネットワーク、サーバーと併せて、モバイルデバイスのセキュリティ対策も一元的に管理することができます。セキュア・コンテナ アプリや、iOS、iPadOS、ビジネス向け Android、Samsung Knox に対応するモバイル OS のコンテナ化機能で、デバイス上の機密性が高い企業データを個人データから確実に分離します。

トップレベルのデータ保護機能を備えているだけでなく、さまざまなセキュリティ機能を網羅していることや、費用対効果が非常に高いこと、また管理機能が柔軟であることも特長です。Sophos Mobile を使えば、モバイルデバイスの使用を許可して生産性を向上する一方で、企業データを保護し、個人のプライバシーを守ることも可能です。

Sophos Intercept X for Mobile

Sophos Intercept X for Mobile は、パフォーマンやバッテリーの持ちに影響を与えることなくデバイスを保護します。業界トップレベルのマルウェア対策テクノロジーを駆使し、Sophos Intercept X for Mobile は実績あるマルウェア/ウイルス対策をはじめ、業務上不要と思われるアプリケーションの検出、プライバシー/セキュリティアドバイザー、盗難・紛失対策、Web プロテクションなど、さまざまな機能を提供します。

Sophos Secure Workspace

Sophos Secure Workspace は、モバイルコンテンツ管理アプリです。コンテナ化機能が搭載されており、業務文書ファイルや Web コンテンツを安全に管理、配布、保護することができます。セキュアなコンテナ環境内で Office 形式の文書ファイルを編集できるため、暗号化されたコンテンツが復号化されず安全に保たれます。フィッシング対策テクノロジーを使って、文書ファイル内の悪質なリンクやコンテンツからユーザーを保護します。

Sophos Mobile の管理者は、あらかじめ設定したコンプライアンス違反時のルールに応じて、管理下にあるデバイスのコンテンツへのアクセスを簡単に制限することができます。Sophos SafeGuard Encryption との併用で、ローカルやクラウド上に保存されている暗号化済みファイルを、Windows、Mac、iPhone、iPad、Android など、異なるデバイス間でシームレスに共有できるようになります。

Sophos Secure Email

Sophos Secure Email は、セキュアコンテナなど、さまざまな機能を装備したアプリで、Sophos Mobile で管理した場合、モバイルデバイス上の業務データ (ビジネス用のメール / 予定表 / 連絡先など) と個人データの領域を分離することができます。すべての企業情報は、AES-256 を使用して暗号化され、コンプライアンスルールに違反したデバイスのアクセスは、簡単にブロックすることができます。また、管理者は、業務メールの一貫したセキュリティポリシーを、さまざまなデバイスと OS 環境に適用することができます。

3 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 Intercept X for Mobile、Sophos Secure Workspace、Sophos Secure Email の一元管理が可能。

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。

3.1 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。

3.2 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。

3.3 ライセンスの更新

ライセンスを更新するには、Sophos Mobile Admin 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。

4 Sophos Mobile の設定

このセクションでは、Sophos Mobile サーバーを新規インストールする方法について説明します。既にインストールされているサーバーをアップデートする方法は、Sophos Mobile のアップデート (p. 26)を参照してください。

4.1 インストールの前提要件

Sophos Mobile サーバーをインストールする前に、次の前提条件を確認してください。

- 「Sophos Mobile サーバー展開ガイド」を読んでいること。このドキュメントには、Sophos Mobile サーバーを組織のインフラに統合するアーキテクチャの例や、サイジングのガイドライン、必要となるネットワークポート / プロトコルなどが記載されています。
- 「Sophos Mobile リリースノート」を読み、Sophos Mobile サーバーをホストするサーバー、管理対象のデバイス、その他関連するコンポーネントが Sophos Mobile でサポートされていることが検証済みであること。
- Sophos Mobile サーバー用の SSL/TLS 証明書があること。
- IIS (インターネット インフォメーション サービス)、あるいは 80番または 443番ポートを使用するその他のアプリケーションがサーバーコンピュータにインストールされていないこと。
- サーバーコンピュータの DNS 名がインターネットで名前解決できること。
- ユーザーアカウントが LDAP ディレクトリに保存されている場合は、セルフサービスポータルの使用を許可されているユーザーを含む 1 つまたは複数の LDAP グループがあること。

既存のデータベースサーバーで Sophos Mobile データベースを管理する場合は、次の前提条件を満たしている必要があります。

- Microsoft SQL Server または Microsoft SQL Server Express の場合:
  - Windows 認証または SQL Server 認証が使用されていること。
  - TCP/IP が有効であること。
  - SQL Server Browser サービスが有効になっていること。
  - SQL へのログインに使用するアカウントの言語が英語に設定されていること。
- Microsoft SQL Server Express の場合:
  - SQL 管理ツールがインストールされていること。

関連タスク

SSL/TLS 証明書の要求 (p. 6)
ソフォスの製品には、Sophos Mobile の EAS プロキシの SSL/TLS 証明書要求を作成する SSL Certificate Wizard (SSL 証明書ウィザード) が含まれています。

関連情報

Sophos Mobile サーバー展開ガイド (英語)
Sophos Mobile リリースノート

4.2 システム環境の要件

Sophos Mobile のインストーラは、一連のテストを実行して、システム環境が Sophos Mobile の要件すべてを満たしていることを確認します。

必須要件

Sophos Mobile インストーラは、次の条件が満たされている場合のみに起動します。

- ローカル管理者アカウントでコンピュータにサインインしています。
- Sophos Mobile は、コンピュータの OS に対応しています。
- コンピュータに少なくとも 1つのネットワークアダプタがあります。
- コンピュータに少なくとも 4GB の RAM が搭載されています。
- Microsoft Internet Information Services (IIS) Web サーバーは、コンピュータで無効化されています。
- コンピュータで HTTP/S ポート 80、443 および 818 を使用できます。
- コンピュータは、次の Web サービスに接続できます。
  - Apple Push Notification Service (APNs)
  - Google Firebase Cloud Messaging (FCM)
  - Google reCAPTCHA
  - Windows プッシュ通知サービス (WNS)
  - Sophos サービス

任意の要件

Sophos Mobile の一部の機能は、コンピュータが次の Web サービスに接続できる場合のみに使用できます。

- Apple Volume Purchase Program (VPP)
- Apple iTunes
- Apple アクティベーションロックのバイパス
- Apple Device Enrollment Program (DEP)
- Google ビジネス向け Android
- Microsoft Azure
- TeamViewer

4.3 SSL/TLS 証明書の要求

ソフォスの製品には、Sophos Mobile の EAS プロキシの SSL/TLS 証明書要求を作成する SSL Certificate Wizard (SSL 証明書ウィザード) が含まれています。

%MDM_HOME%¥tools¥Wizard というフォルダからウィザードを実行するか、www.sophos.com/mysophos からウィザードをダウンロードします。

注
自己署名証明書や、自己認証局 (CA) で発行した証明書を使用している場合は、次の制限があります。

- デバイスを Sophos Mobile に登録する前に、自己署名証明書または自己認証局による証明書をデバイスに手動インストールする必要があります。この操作を実行しないと、Sophos Mobile Control アプリによってサーバーが信頼されず、接続が拒否されます。グローバルに信頼されている CA 発行の証明書の場合、この手動インストールは必要ありません。
- Sophos Mobile サーバー上の APK ファイルから Android アプリをインストールすることはできません。
- Android ゼロタッチ登録、または Samsung Knox Mobile Enrollment を使用することはできません。
- Sophos Mobile 設定ウィザードまたは SSL 証明書ウィザードで作成されなかった自己署名証明書を使用する場合は、アップル社の文章 iOS 13 および macOS 10.15 における信頼済み証明書の要件を参照してください。

SSL/TLS 証明書を要求するには以下を実行します。

- Sophos Mobile SSL Certificate Wizard.exeファイルを実行して、SSL Certificate Wizard (SSL 証明書ウィザード) を起動します。

  ウィザードの指示に従ってインストールを行います。以下の指示に従って、必要な情報を入力します。

  a) 証明書のベンダーでコピー＆ペースト機能がサポートされている場合は、「**Upload CSR**」(CSR のアップロード) ページで、「**Open CSR**」(CSR を開く) ボタンをクリックして、CSR ファイルを開くことができます。

  b) 「**Import Certificate Files**」(証明書ファイルのインポート) ページで、「**Upload CSR**」(CSR のアップロード) でダウンロードした CA 証明書を、「**Select CA certificate file**」(CA ファイルの選択) フィールドに入力します。

  c) 「**Certificate created**」(作成された証明書) ページに、作成された証明書の保存場所が表示されます。Sophos Mobile を設定する際は、この保存場所を参照する必要があります。

注
証明書ファイルを含むフォルダのバックアップを作成するようにしてください。

関連情報
iOS 13 および macOS 10.15 における信頼済み証明書の要件 (外部リンク)

4.4 Sophos Mobile サーバーのインストールと設定

前提条件:

- Sophos Mobile を既存のデータベースに接続する場合は、インストールを開始する前にデータベースのアカウント情報が手元にあることを確認してください。また、新しいデータストア、ユーザーアカウント、およびデータレコードを作成するための十分な権限があることを確認してください。
- データベースをローカルに保存していない場合は、データベースサーバーの接続ポートにアクセスできる必要があります。デフォルトのポートは、TCP 1433 (Microsoft SQL Server の場合) および TCP 3306 (MySQL) です。また、Sophos Mobile サーバーで使用するデータベースアクセス用の管理者アカウントも必要です。

1. ローカル管理者権限を持つユーザーアカウントで Windows にサインインします。
2. Sophos Mobile インストーラを起動します。
3. 「**System Property Checks**」(システムプロパティの確認) ページで、「**Check**」(チェック) をクリックして、システム環境が、Sophos Mobile のすべての要件を満たしていることを確認します。詳細は、システム環境の要件 (p. 5)を参照してください。

   テスト結果のレポートは、「**Report**」(レポート) をクリックして生成できます。
4. 「**Choose Install Location**」(インストール先の選択) ページで、Sophos Mobile サーバーのインストール先フォルダを選択します。
5. 「**Database Type Selection**」(データベースの種類の選択) ページで、使用するデータベースの種類を次から選択します。

   - **Install and use Microsoft SQL Server Express** (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): Microsoft SQL Server Express がインストールされ、Sophos Mobile との使用に必要な設定が行われます。
   - **Use existing Microsoft SQL Server installation** (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): 既にインストールされている Microsoft SQL Server を使用して、Sophos Mobile 用の新しいデータベースが作成されます。
   - **Use existing MySQL installation** (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): 既にインストールされている MySQL を使用して、Sophos Mobile 用の新しいデータベースが作成されます。
6. 「**Database Settings**」(データベースの設定) ページで、データベースのログイン情報を入力します。

   注
   「**Use SQL Server Authentication**」(SQL Server 認証を使用する) オプションを選択した場合は、SQL ログイン言語が英語に設定されていることを確認してください。詳細は、SQL ログイン言語の変更 (p. 10)を参照してください。

7. 「**Database Selection**」(データベースの選択) ページで、「**Create a new database named**」(名前付きの新しいデータベースを作成) をクリックして、作成するデータベースの名前 (例: SMCDB など) を入力します。
8. 「**Database Configuration**」(データベースの設定) ページで、データベース作成の進行に関するメッセージが表示されます。
   正常にデータベースが作成され、データが追加されたら、「**Next**」(次へ) をクリックして続行します。

9. データベースへの接続に Windows 認証を選択した場合は、「**Set service credentials**」(サービス用アカウント情報の設定) が表示されるので、Sophos Mobile のサービスを実行する Windows のアカウントを設定します。

   Local System アカウントまたは任意のユーザーアカウントを指定できます。ユーザーアカウントを使用する場合は、<コンピュータ名>¥<ユーザー名> または <ドメイン名>¥<ユーザー名> という形式で入力します。

   インストーラによって、データベースに対するアクセス権がアカウントに付与されます。

   注
   セキュリティ上の理由から、制限付きでアクセスが許可されているユーザーとして Sophos Mobile サービスを実行することを推奨します。このユーザーアカウントに必要な属性は次のとおりです。

   - ユーザーアカウントは、Sophos Mobile がインストールされているコンピュータ上のローカル Windows アカウントであること。
   - ユーザーは、「ユーザー」グループを含む、いかなるグループにも所属していないこと。
   - ユーザーは SQL データベースにアクセスでき、必要な変更権限を持っていること。MS-SQL データベースの場合、このためには、db_datareader および db_datawriter ロールのメンバーでなくてはなりません。

10. 「**Configure super admin account**」(スーパー管理者アカウントの設定) ページで、スーパー管理者アカウントの詳細を設定します。

    スーパー管理者アカウントは、カスタマーの管理を実行するために使用し、日々のデバイス管理には使用しないようにしてください。スーパー管理者は、スーパー管理者のカスタマーにログインして、新しいカスタマーの事前設定を行ったり、既存のカスタマーに対して設定を強制適用したりすることができます。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。

    注
    スーパー管理者のアカウント情報は、Sophos Mobile Admin に最初にログインする際に必要です。インストール後、Sophos Mobile Admin に、スーパー管理者をさらに追加できます。

11. 「**Configure external server name**」(外部サーバー名の設定) ページで、Sophos Mobile サーバー名 (例: smc.mycompany.com) を入力します。

    注
    管理下にあるデバイスが名前解決できるサーバー名を入力する必要があります。

12. 「**Configure server certificate**」(サーバー証明書の設定) ページで、Web サーバーへの安全なアクセス (HTTPS) に必要な証明書をインポートします。

    - 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、ドロップダウンリストからオプションを選択します。
    - 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。

注
ソフォスの製品には、Sophos Mobile の SSL/TLS 証明書要求を作成する SSL Certificate Wizard (SSL 証明書ウィザード) が含まれています。詳細は、SSL/TLS 証明書の要求 (p. 6)を参照してください。

13. 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、管理下にある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。

14. 「**Server Information**」(サーバー情報) ページでサーバー情報を検証し、「**Next**」(次へ) をクリックして、サーバーと設定の処理を続行します。
15. インストールが完了すると、「**Sophos Mobile Control - Installation finished**」(Sophos Mobile - インストールが完了しました) のダイアログボックスが表示されます。「**Start Sophos Mobile server now**」(Sophos Mobile サーバーを今すぐ起動) が選択されていることを確認し、「**Finish**」(完了) をクリックすると Sophos Mobile のサービスがはじめて起動します。

注
サービスが開始した後、Sophos Mobile の Web インターフェースが使用可能になるまでに数分間かかります。

インストール後は、次の初期設定を行う必要があります。

- 使用しているドメイン名に転送されたリクエストのみを許可するように、Sophos Mobile Web サーバーを設定します。詳細は、Sophos Mobile Web サーバーの設定 (p. 9)を参照してください。
- Sophos Mobile Admin に初回ログインして、**開始手順**ウィザードを起動します。詳細は、「Sophos Mobile スタートアップガイド」を参照してください。
- iPhone、iPad、および Mac の場合は、Apple Push Notification サービスの証明書を取得する必要があります。詳細は、「Sophos Mobile スタートアップガイド」を参照してください。
- 必要に応じて、スタンドアロン型 EAS プロキシを設定してメールのフィルタリングを行うこともできます。詳細は、スタンドアロン型 EAS プロキシ (p. 11)を参照してください。

4.5 Sophos Mobile Web サーバーの設定

Sophos Mobile には、Sophos Mobile Admin とセルフサービス ポータル Web アプリケーションのコンテンツへのアクセスを提供する、Web サーバーコンポーネントが含まれています。Web サーバーは、使用している環境に対して最適化するように設定できます。

Web サーバーへの HTTP リクエストのヘッダには、リクエストを処理する Web アプリケーションを指定する Host フィールドがあります。攻撃者は Host フィールドの値を変更して、意図しない処理を実行することが可能です。

インストール後、Sophos Mobile の Web サーバーコンポーネントは、Host フィールドの値を確認しません。使用しているドメイン名に転送されたリクエストのみを許可するように、Web サーバーを設定することを推奨します。

1. Sophos Mobile サーバーのインストール先コンピュータで、次のスクリプトを実行します。%MDM_HOME%¥tools¥HostValidationUndertowFilter¥addModule.bat

%MDM_HOME% は、Sophos Mobile のインストールフォルダで置き換えます。

2. %MDM_HOME%¥wildfly¥standalone¥configuration¥smc-config.xml ファイルをテキストエディタで開き、次のセクションを検索します。

```
<filter name="hostheadervalidation" ...>
   <param name="allowedHosts" value="localhost"/>
</filter>
```

3. localhost の後ろに、Sophos Mobile Admin とセルフサービス ポータル用のドメイン名を追加します。

   たとえば、ドメイン名が smc.example.com の場合は、該当する行を次のように変更します。

```
<param name="allowedHosts" value="localhost,smc.example.com"/>
```

   複数のドメイン名で Sophos Mobile サーバーにアクセスできる場合は、カンマで区切ってすべてのドメイン名を入力してください。

4. smc-config.xml ファイルを保存します。
5. Sophos Mobile サービスを再起動します。

4.6 SQL ログイン言語の変更

Sophos Mobile サーバーで、SQL Server 認証を使用してデータベースに接続するよう設定した場合は、SQL ログイン言語を英語に設定する必要があります。それ以外の言語を設定すると、Sophos Mobile サービスの起動時にエラーが発生します。

このトピックでは、SQL ログイン言語を英語に変更する方法について説明します。

1. Sophos Mobile サービスを停止します。
2. サーバー上の SQL Management Studio を開き、「**Security > Logins**」(セキュリティ - ログイン) を選択します。
3. 「**General**」(全般) ページの「**Login Properties**」(ログインのプロパティ) で、「**Default language**」(デフォルト言語) を英語に設定し、「**OK**」をクリックして変更内容を保存します。
4. Sophos Mobile サービスを再起動します。

5 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 2種類あります。

- Sophos Mobile と同時に自動インストールされる内部 EAS プロキシ。Microsoft Exchange、および iOS デバイスや Samsung Knox デバイス用の IBM Notes Traveler で使用される ActiveSync の受信トラフィックに対応しています。
- 個別にダウンロードして、インストールできるスタンドアロン型 EAS プロキシ。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
パフォーマンス上の理由から、500台以上のクライアントデバイスを管理する必要がある場合、社内バージョンの代わりにスタンドアロンの EAS プロキシサーバーを使用することを推奨します。

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

スタンドアロン型 EAS プロキシは、内部 EAS プロキシと比較して、次のような追加機能があります。

- iOS 以外 (Android など) のデバイス用の IBM Notes Traveler に対応。このようなデバイス用の Lotus Traveler クライアントは、内部 EAS プロキシでは対応していない (ActiveSync ではない) プロトコルを使用します。
- 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. 17)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。

5.1 EAS プロキシを使用するシナリオ

注
このセクションに記載されている情報のほかに、スタンドアロン型 EAS プロキシサーバーを企業のインフラに統合するアーキテクチャの例が、「Sophos Mobile サーバー導入ガイド (英語)」に掲載されています。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。

iOS 以外のデバイス向けの IBM Notes Traveler (旧称 IBM Lotus Notes Traveler) を使用している場合

内部 EAS プロキシは、Microsoft Exchange や iPhone および iPad 向け Lotus Traveler で使用する ActiveSync プロトコルのみに対応しているため、このシナリオでは不適切です。Android など、iOS 以外のデバイス向けの IBM Notes Traveler では、スタンドアロン型 EAS プロキシで対応している別のプロトコルが使用されます。

iOS 以外のデバイスでは、専用の Lotus Traveler クライアントソフトウェアが必要になります。このソフトウェアは、<Traveler サーバー>/servlet/traveler または Lotus Traveler のファイルシステムから取得できます。Lotus Traveler クライアントソフトウェアは、Sophos Mobile の「アプリのインストール」や「アプリのアンインストール」機能を使用して、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できます。設定は手動で実行する必要があります。

複数のバックエンドサーバーに対応する場合

スタンドアロン型 EAS プロキシを使用すると、バックエンド メールシステムの複数のインスタンスを設定できます。各インスタンスには、受信方向の TCP ポートが必要です。各ポートは異なるバックエンドに接続できます。各 EAS プロキシインスタンスごとに URL が 1つ必要です。

EAS に対して負荷分散を設定する場合

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。

このシナリオでは、HTTP に対する既存のロードバランサが必要になります。

クライアント証明書を使用した認証を使用する場合

このような環境では既存の PKI が必要で、CA 証明書の公開部分は EAS プロキシで設定する必要があります。

500台以上のデバイスを管理する必要がある場合

パフォーマンス上の理由から、500台以上のクライアントデバイスを管理する必要がある場合、社内バージョンの代わりにスタンドアロンの EAS プロキシサーバーを使用することを推奨します。

5.2 EAS プロキシのインストーラのダウンロード

1. スーパー管理者権限で Sophos Mobile Admin にサインインします。
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。

5.3 スタンドアロン型 EAS プロキシのインストール

前提条件:

- Sophos Mobile がインストール・設定されていること。
- 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 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。

   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。

   注意
   「**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。

   注
   ソフォスの製品には、Sophos Mobile の EAS プロキシの SSL/TLS 証明書要求を作成する SSL Certificate Wizard (SSL 証明書ウィザード) が含まれています。詳細は、SSL/TLS 証明書の要求 (p. 6)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)**
     - **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. スーパー管理者権限で Sophos Mobile Admin にサインインします。
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。

5.4 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 導入ガイド」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 サーバー展開ガイド (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
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. スーパー管理者権限で Sophos Mobile Admin にサインインします。
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。

5.5 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. 17)
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)

6 負荷分散と HA (高可用性)

Sophos Mobile では、HA 環境を設定できます。1つの Sophos Mobile ノードで障害が発生しても、引き続き外部から SMC サービスにアクセスできるので、タスクの処理が継続されます。この設定には、該当するノードに DNS ラウンドロビンを使用して、クライアントとブラウザのセッションを分散する負荷分散が必要です。

以下のセクションは、Sophos Mobile のクラスタ化を設定し、Sophos UTM で負荷分散を設定する方法について説明しています。

6.1 要件

- 各 Sophos Mobile サーバーノードに対して、1台の Windows サーバーが必要です。
- すべてのノードが同じネットワーク上にある必要があります。
- 1台の Microsoft SQL/MySQL データベースサーバーやクラスタが必要です。
- 負荷分散のために、Sophos UTM や Apache リバースプロキシ (mod_proxy) が必要です。ロード バランサは、永続的なセッションクッキーと正式な SSL/TLS Web サーバー証明書に対応する必要があります。

注
インストール要件の詳細は、「Sophos Mobile 9.6 リリースノート (英語)」を参照してください。

アーキテクチャ

3 ノードの Sophos Mobile クラスタの例は、「Sophos Mobile サーバー導入ガイド (英語)」を参照してください。

各 Sophos Mobile サーバーノード間のマルチキャスト通信には、任意で異なるネットワークを使用することもできます。使用するネットワークインターフェースは、1つ目のノードの設定 (p. 22)で説明されているように、クラスタの設定時に選択できます。VLAN を使用することもできます。

注
テスト目的で別の Sophos Mobile クラスタを稼働する場合は、異なるネットワークが必要になります。

ポートとプロトコル

以下の表は、Sophos Mobile サーバーの各ノード間の通信に必要なポートとプロトコルの一覧です。

プロトコル	ポート	転送先
TCP	7600、8181、57600	<受信>
TCP	7600、8181、57600	<送信>
UDP	45700	<受信>

サーバー証明書

Sophos Mobile をセットアップする際、Sophos Mobile Control アプリが Sophos Mobile サーバーへのセキュアな接続を確立できるように、SSL/TLS Web サーバーの証明書を設定します。グローバルに信頼されている認証局 (CA) によって発行されている証明書の使用を推奨します。ただし、ロードバランサの背後に複数の Sophos Mobile サーバーノードがあるクラスタ環境では、そのような証明書の使用が難しいこともあります。その場合は、代わりに自己署名証明書を使用してください。

関連タスク

SSL/TLS 証明書の要求 (p. 6)
ソフォスの製品には、Sophos Mobile の EAS プロキシの SSL/TLS 証明書要求を作成する SSL Certificate Wizard (SSL 証明書ウィザード) が含まれています。

6.2 クラスタノードの設定

クラスタ環境を設定するには、Sophos Mobile サーバーのインストールと設定 (p. 7)の説明に従って、1つ目のノードをインストールします。クラスタは、その後、**設定ウィザード**を使用して有効化します。

それ以外のノードについては、1つ目のノードの作成時に作成したデータベースを選択後、クラスタを有効化する必要があります。

注
また、既存の SMC サーバーをクラスタ用に設定して、ノードを追加して環境を拡張することもできます。

6.2.1 1つ目のノードの設定

1. Sophos Mobile サーバーのインストールと設定 (p. 7)の説明に従って、Sophos Mobile をインストールして、作成したデータベースの名前をメモします。追加のノードをインストールする際は、このデータベースを指定します。
2. インストールの最後に、「**Sophos Mobile - Installation finished**」(Sophos Mobile - インストールが完了しました) ダイアログで、「**Start Sophos Mobile server now**」(Sophos Mobile サーバーを今すぐ起動する) オプションを選択解除します。

注
Sophos Mobile サービスが既に起動されている場合は、この後に説明する設定の過程で、自動的に停止され、再起動されます。または、Sophos Mobile のシステムトレイ アイコンのメニューから、手動でサービスを停止することができます。

3. サーバーで「**スタート**」をクリックして、「**Sophos Mobile**」を開き、「**SMC Configuration Wizard**」(SMC 設定ウィザード) をクリックします。
4. 「Sophos Mobile Configuration Wizard」(設定ウィザード) の「**Welcome**」(ようこそ) ページが表示されます。「**Next**」(次へ) をクリックします。
5. 「**Database Selection**」(設定の選択) ページで、「**Skip database configuration**」(クラスタサポートの設定) を選択し、「**Next**」(次へ) をクリックします。
6. 「**Choose configuration steps**」(設定の選択) ページで、「**Configure cluster support**」(クラスタサポートの設定) を選択し、「**Next**」(次へ) をクリックします。
7. 「**Cluster Configuration**」(クラスタの設定) ページで、使用可能なネットワークインターフェースのドロップダウンリストを使用して、設定する サーバーのノードと他のノード間のマルチキャスト通信に使用するインターフェースを選択します。
8. 設定ウィザードの残りをクリックして進めます。SMC サービスの起動を確認するメッセージが表示されたら「**Yes**」(はい) をクリックします。
これで、SMC サーバーの 1つ目のノードの設定が完了しました。「**Sophos Mobile - Configuration Wizard finished**」(Sophos Mobile - 設定ウィザードが完了しました) ダイアログで、「**Finish**」(完了) をクリックします。

6.2.2 追加のノードの設定

1. Sophos Mobile サーバーのインストールと設定 (p. 7)の説明に従って、Sophos Mobile のインストールを開始します。
2. 「**Database selection**」(データベースの選択) ダイアログで、1つ目のノードにインストールした際に作成したデータベースを選択して、「**Next**」(次へ) をクリックします。
「**Database configuration**」(データベースの設定) ダイアログボックスが表示されます。設定処理の進行状況が表示されます。
3. 「**Database configuration**」(データベースの設定) ページで、設定が完了するまで待ちます。その後、「**Next**」(次へ) をクリックします。
4. 「**Choose configuration steps**」(設定の選択) ページで、「**Configure cluster support**」(クラスタサポートの設定) を選択し、「**Next**」(次へ) をクリックします。
5. 「**Configure server certificate**」(サーバー証明書の設定) ページで、Sophos Mobile サーバーのインストールと設定 (p. 7)の説明に従って自己署名証明書を作成し、「**Next**」(次へ) をクリックします。
6. 「**Cluster Configuration**」(クラスタの設定) ページで、使用可能なネットワークインターフェースのドロップダウンリストを使用して、設定する Sophos Mobile サーバーのノードのインターフェースを選択します。次に、「**Next**」(次へ) をクリックします。
7. 設定ウィザードの残りをクリックして進めます。「**Sophos Mobile - Installation finished**」(Sophos Mobile - インストールが完了しました) ページで、「**Start Sophos Mobile server now**」(Sophos Mobile サーバーを今すぐ起動する) を選択して、設定したクラスタノードを起動します。
8. 1つ目のノードで、使用しているドメイン名に転送されたリクエストのみを、Sophos Mobile の Web サーバーコンポーネントで許可するように設定した場合は、他のノードすべてに対しても同様の設定を行います。詳細は、Sophos Mobile Web サーバーの設定 (p. 9)を参照してください。

さらにノードを設定するには、この手順を繰り返します。

6.3 Sophos UTM を使用した負荷分散の設定

このトピックでは、クラスタ化した複数の Sophos Mobile サーバーノードに対して、Sophos UTM をロードバランサとして設定する方法について説明します。Sophos UTM の設定方法の詳細は、Sophos UTM のドキュメントを参照してください。

注

- Sophos UTM を使用してクラスタを設定するには、**Sophos Webserver Protection** サブスクリプションを含む Sophos UTM ライセンスが必要です。
- この後に説明する手順では、管理下にあるデバイスと、Sophos UTM で設定する仮想 Web サーバー間の通信を保護する証明書を指定します。操作を簡単にするため、Sophos Mobile サーバーで使用した証明書と同じ証明書を使用することを推奨します (SSL/TLS 証明書の要求 (p. 6)を参照)。自己署名証明書を使用した場合は、必ずその証明書を使用する必要があります。

1. Sophos UTM WebAdmin にログインします。
2. WebAdmin のメニューの「**Webserver Protection**」で、「**Web アプリケーションファイアウォール > リアル Web サーバー**」タブを選択します。
3. 「**新規リアル Web サーバー**」をクリックして、SMC ノードを作成します。
4. 「**新規リアル Web サーバー**」ダイアログで、次の設定を入力します。
   a) **名前**: Web サーバーの説明的な名前を入力します (例: SMC ノード)。
   b) **ホスト**: ホストを選択または追加します。ホストを選択するには、「**ホスト**」フィールドの横にあるフォルダアイコンをクリックします。使用可能なホストの一覧からホストを「**ホスト**」フィールドにドラッグします。
      オブジェクトの追加方法の詳細は、「UTM 管理ガイド」の「Network Definitions」(ネットワークオブジェクト) を参照してください。
   c) **タイプ**: 「**暗号化 (HTTPS)**」を選択します。
   「**保存**」をクリックして設定を保存します。
   各 Sophos Mobile サーバーのノードに対して、上記の手順を繰り返してください。
5. WebAdmin のメニューの「**Webserver Protection**」で、「**証明書管理 > 証明書**」タブを選択します。
6. 「**新規証明書**」をクリックして、SSL/TLS Web サーバー証明書をアップロードします。
7. 「**証明書を追加**」ダイアログで、次の設定を入力します。
   a) **名前**: 証明書の説明的な名前を入力します。
   b) **メソッド**: 「**アップロード**」を選択します。
   c) **ファイルタイプ**: 「**PKCS#12 (証明書+CA)**」を選択します。
   d) **パスワード**: 証明書ファイルのパスワードを入力します。
   e) **ファイル**: 「**ファイル**」ボックスの横にあるフォルダアイコンをクリックし、アップロードする証明書を選択して、「**アップロード開始**」をクリックします。
   「**保存**」をクリックして設定を保存します。証明書は、「**証明書**」の一覧に追加されます。
8. WebAdmin のメニューの「**Webserver Protection**」で、「**Web アプリケーションファイアウォール > 仮想 Web サーバー**」タブを選択します。
9. 「**新規仮想 Web サーバー**」をクリックして、クラスタ用の仮想 Web サーバーを追加します。
10. 「**新規仮想 Web サーバー**」ダイアログボックスで、次の設定を入力します。

a) **名前**: 仮想 Web サーバーの説明的な名前を入力します (例: SMC クラスタ)。

b) 「**インターフェース**」リストから、外部からこのクラスタにアクセスするための WAN インターフェースを選択します。

c) **タイプ**: 「**暗号化 (HTTPS) とリダイレクト**」を選択します。

d) 「**証明書**」リストから、先ほどアップロードした Web サーバーの証明書を選択します。

e) **ドメイン** (ワイルドカード証明書 (複数のサブドメインで使用可能な公開鍵証明書) を使用する場合のみ): shop.example.com など、Web サーバーが管理するドメインを入力するか、**アクション**アイコンを使用して、ドメイン名の一覧をインポートします。

ドメイン名は、必ず FQDN で入力してください。

*.mydomain.com など、ドメインのプレフィックスとしてアスタリスク (*) を使用できます。ワイルドカード文字を含むドメインは、フォールバック設定として扱われます。ドメイン名にワイルドカード文字を含む仮想 Web サーバーは、より具体的なドメイン名の仮想 Web サーバーがない場合のみに使用されます。

例: a.b.c に送信されたクライアントリクエストは、a.b.c に一致します。それがない場合は、*.b.c、そして *.c の順に一致します。

f) **リアル Web サーバー**: 先ほど作成した SMC ノードを選択します。

注
ファイアウォールのプロファイルは選択しないようにしてください。

「**保存**」をクリックして設定を保存します。サーバーは、「**仮想 Web サーバー**」の一覧に追加されます。

11. 仮想 Web サーバーを有効化します。

新規仮想 Web サーバーはデフォルトで無効になっています。トグルスイッチをクリックして、仮想 Web サーバーを有効化します。トグルスイッチの色は、グレー (無効) から緑色 (有効) に切り替わります。

12. 「**サイトパスルーティング**」タブを選択します。
13. 「**仮想 Web サーバー**」の一覧で、追加した仮想 Web サーバーを参照して、「**編集**」をクリックします。
14. 「**サイトパスルートの編集**」ダイアログボックスで、「**詳細**」をクリックして、「**スティッキーセッション cookie を有効化する**」を選択します。
「**保存**」をクリックして設定を保存します。

7 Sophos Mobile のアップデート

Sophos Mobile サーバーのインストールは、バージョン 9 および 9.5 から直接バージョン 9.6 にアップデートすることができます。

これより古いバージョンは、まず Sophos Mobile 9 にアップデートする必要があります。詳細は、Sophos Mobile 9 の製品ドキュメントを参照してください。

7.1 Sophos Mobile サーバーのアップデート

Sophos Mobile サーバーのインストールをバージョン 9.6 にアップデートするには、Sophos Mobile 9.6 のインストーラを起動して手順に従ってください。アップデートが必要な既存のインストール環境は自動的に検出されます。

アップデートが開始される前に、システムプロパティの確認が実行されます。すべての確認が成功すると、アップデートを続行できます。データベースとファイルは、ユーザーの操作なしで自動的にアップデートされます。アップデートが完了すると、Sophos Mobile サービスが再開します。

注
Sophos Mobile サーバーをはじめてインストールしたときに Windows 認証を使用した場合は、「**Start Sophos Mobile server now**」(Sophos Mobile サーバーを今すぐ起動) のチェックボックスはグレーアウト表示されます。サービスは手動で開始する必要があります。

7.2 アップデート後のタスク

7.2.1 Sophos Mobile Web サーバーの再設定

使用しているドメイン名に転送されたリクエストのみを、Sophos Mobile の Web サーバーコンポーネントで許可するように設定した場合は、Sophos Mobile をアップデート後、その操作を繰り返す必要があります。詳細は、Sophos Mobile Web サーバーの設定 (p. 9)を参照してください。

7.3 サーバークラスタのアップデート

Sophos Mobile サーバーのノードのクラスタをアップデートする際は、すべてのノードが常に同じバージョンで稼働しているとともに、サーバーのバージョンとデータベースのバージョンが一致していなければなりません。次の手順を実行します。

1. 該当するコンピュータ上の Sophos Mobile サービスを停止して、すべてのサーバーのノードをシャットダウンします。
2. Sophos Mobile サーバーのアップデート (p. 26)の説明に従って、最初のノードをアップデートします。
   これと同時にデータベースもアップデートされます。
3. アップデートしたサーバーのノードを起動し、問題なくアップデートされていることを確認します。
4. 残りのサーバーのノードをアップデートします。

ヒント
スタンドアロン型 EAS プロキシを使用している場合は、すべての Sophos Mobile サーバーのノードが停止していても、管理下のデバイスはメールサーバーにアクセスできます。これは、Sophos Mobile サーバーに接続されていない際、デバイスのステータスが最長 60分間、EAS プロキシに一時保存されるためです。

7.4 スタンドアロン型 EAS プロキシのアップデート

スタンドアロン型 EAS プロキシをアップデートするには、EAS プロキシのインストーラを起動して画面の案内に従ってください。アップデートが必要な既存のインストール環境は自動的に検出されます。

ロードバランサの背後で構成されている EAS プロキシサーバーのノードのクラスタを使用している場合は、各ノードを任意の順序で個別にアップデートします。

ヒント
同時にすべての EAS プロキシサーバーのノードを停止しないでください。アップデートの際にすべて同時に停止すると、管理下のデバイスのメール通信が中断されます。

8 技術情報

8.1 Sophos Mobile サーバーの機能

Sophos Mobile サーバーは、Sophos Mobile 製品のコアコンポーネントです。主な機能は次のとおりです。

- サーバーはインターネットに接続します。
- サーバーでは、高い可用性の環境を設定できます。
- 管理者は、Web インターフェースを使用してサーバーを制御します。
- エンドユーザーは、セルフサービス ポータルを使用して自身のデバイスを登録できます。または、自動登録の準備が完了したデバイスを管理者から取得することもできます。
- 管理下にあるデバイスは、HTTPS 経由でサーバーと同期します。
- 既存の Microsoft SQL Server や MySQL データベースを使用して、デバイスやアプリケーション情報を保存できます。または、Sophos Mobile のインストーラで、Microsoft SQL Server Express を使用して新しいデータベースを作成できます。
- データベースは、同じコンピュータまたは別のコンピュータに保存でき、データベースクラスタを使用できます。
- サーバーは、複数のテナントのセットアップに対応しており、同じサーバーで複数のカスタマーを設定できます。
- メールアクセスは、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実行できます。スタンドアロン型 EAS プロキシの場合は、HTTPS 経由で SMC サーバーにアクセスする必要があります。

Sophos Mobile サーバーは、Java EE (Enterprise Edition) 環境に対応するように開発されています。十分にテストされている、業界標準の WildFly アプリケーションサーバー環境にインストールし、実行できます。

サーバーは、仮想環境にインストールすることもできます。

8.2 Sophos Mobile Web インターフェース

8.2.1 Sophos Mobile の管理インターフェース

Sophos Mobile は、ログインとセッション管理で安全に接続できる Web インターフェースを使用して管理します。パスワードポリシーを適用できます。アクセス制御では、複数のユーザーロールを使用できます。各ロールには異なるアクセス権限が付与されています。ユーザー 1名につき 1つのロールのみを割り当てることができます。

詳細は、「Sophos Mobile 管理者ヘルプ」を参照してください。

8.2.2 スーパー管理者インターフェース

スーパー管理者は、カスタマーを設定・管理して、デバイス管理を行うために使用されます。最初のスーパー管理者アカウントは、Sophos Mobile のセットアップ時に作成されます。詳細は、Sophos Mobile サーバーのインストールと設定 (p. 7)を参照してください。

スーパー管理者は、同様に Sophos Mobile のセットアップ時に作成される「スーパー管理者カスタマー」としてログオンします。スーパー管理者カスタマーとしてログオンすると、Sophos Mobile Admin にスーパー管理者タスクを実行するための専用画面が表示されます。

8.2.3 セルフサービス ポータル

セルフサービス ポータルは、ログインとセッション、およびパスワードポリシーで保護されています。アカウントは、Sophos Mobile の管理者が設定する必要があり、任意のテナントに関連付けることができます。セルフサービス ポータルを使用して、エンドユーザーは Sophos Mobile に自分でデバイスを登録することができます。エンドユーザーは、遠隔操作でのリモートやワイプなど、自分のデバイスに対してタスクを実行することもできます。実行できるタスクの種類は、デバイスのプラットフォームと設定に依存します。管理者は、エンドユーザーがセルフサービス ポータルで実行できる機能を設定できます。

セルフサービス ポータルをエンドユーザー用に設定する方法の詳細は、「Sophos Mobile 管理者ヘルプ」を参照してください。

9 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

10 利用条件