



iPhone と iPad の配備 セキュリティの概要



デバイスのセキュリティ

- ・強力なパスコード
- ・パスコードの有効期限
- ・パスコード再利用の履歴
- ・入力を失敗できる回数
- ・無線によるパスコードの適用
- ・高度なパスコードのタイムアウト

iPhone や iPad の中核であるオペレーティングシステム、iOS には、何層ものセキュリティ機能が装備されているので、企業サービスに安全にアクセスしたり、重要なデータを保護することができます。iOS には、データ転送時の強力な暗号化、企業サービスにアクセスするための実績ある認証方式のサポート、デバイスに保存されている全データのハードウェア暗号化などの機能が備わっています。また、パスコードポリシーを使用することでデータを確実に保護します。パスコードポリシーはワイヤレスネットワーク経由で配布し、適用することができます。万が一デバイスが悪意のある人物の手に渡ってしまった場合、ユーザや IT 管理者は、リモートワイプコマンドを実行して機密情報を消去できます。

以下の情報を理解しておく、企業で iOS を使用するにあたって、セキュリティを検討する際に役立ちます。

- ・ **デバイスのセキュリティ**：デバイスの不正使用を防ぐ方法
- ・ **データ保護**：デバイスの紛失または盗難時でも、デバイスに保存されているデータを保護する
- ・ **ネットワーク保護**：ネットワークプロトコルおよびデータ転送時の暗号化
- ・ **アプリケーション保護**：iOS が提供する安全なプラットフォーム

これらの機能がスムーズに連携し、安全なモバイルコンピューティングプラットフォームを提供します。

デバイスのセキュリティ

企業の情報をしっかり保護するには、iPhone や iPad へのアクセスに強力なポリシーを設定することが重要です。デバイスのパスコードは、権限のないアクセスを防ぐ第一の方法となるもので、ワイヤレスで構成し、適用することができます。iOS デバイスは、各ユーザが設定した固有のパスコードを使用して強力な暗号鍵を生成し、デバイス上の E メールやアプリケーションの重要なデータの保護をさらに強化します。加えて iOS には、特定の設定、ポリシー、制限を必要とするエンタープライズ環境でデバイスを構成するための安全な方法が、複数用意されています。その中から柔軟に選択し、権限のあるユーザのための標準レベルの保護を実現できます。

パスコードポリシー

デバイスのパスコードは、権限のないユーザがデバイスに保存されているデータにアクセスしたり、デバイスを不正に使用することを防ぎます。iOS では、タイムアウト時間、パスコードの強度、パスコードの変更頻度など、様々なパスコードの必要条件を選択できるので、セキュリティのニーズを満たすことができます。

次のパスコードポリシーに対応しています。

- ・ デバイスのパスコードが必要
- ・ 単純値を許可
- ・ 英数字の値が必要
- ・ 最小のパスコード長
- ・ 複合文字の最小数
- ・ パスコードの有効期限
- ・ 自動ロックまでの時間
- ・ パスコードの履歴
- ・ デバイスロックの猶予期間
- ・ 入力を失敗できる回数



サポートされている構成可能なポリシーと制限

デバイスの機能

- アプリケーションのインストールを許可
- カメラの使用を許可
- FaceTime を許可
- 画面の取り込みを許可
- ローミング中の自動同期を許可
- 音声ダイヤルを許可
- アプリケーション内での購入を許可
- 購入時に必ずストアパスワードを要求
- マルチプレイヤーゲームを許可
- Game Center に友達の追加を許可

アプリケーション

- YouTube の使用を許可
- iTunes Store の使用を許可
- Safari の使用を許可
- Safari のセキュリティ設定

iCloud

- バックアップを許可
- 書類の同期を許可
- フォトストリームを許可

セキュリティとプライバシー

- 診断データを Apple に送信することを許可
- ユーザーが信頼できない証明書を受け入れることを許可
- 暗号化されたバックアップを強制

コンテンツレート

- 不適切な内容の音楽と Podcast を許可
- レーティングの地域
- 許可されるコンテンツレーティング

ポリシーの適用

前述のポリシーを iPhone や iPad に設定する方法は複数あります。ポリシーを、ユーザがインストールする構成プロファイルに含めて配布することができます。プロファイルは、管理者パスワードがある場合にのみ削除できるように定義できます。また、プロファイルをデバイスにロックし、デバイス上のすべてのコンテンツを完全に消去しない限りプロファイルを削除できないように定義するという方法もあります。さらに、ポリシーをデバイスに直接プッシュできるモバイルデバイス管理 (MDM) ソリューションを使用して、パスコード設定をリモートで構成することもできます。この方法を使えば、ユーザが特定のアクションを実行しなくてもポリシーの適用や更新が可能になります。

また、Microsoft Exchange アカウントにアクセスするようにデバイスが構成されている場合は、Exchange ActiveSync ポリシーがワイヤレスでデバイスにプッシュされます。利用できるポリシーは、Exchange のバージョン (2003、2007、2010) によって異なることに注意してください。実際の構成でサポートされるポリシーの内容については、『Exchange ActiveSync と iOS 搭載デバイス』を参照してください。

安全なデバイスの構成

構成プロファイルは XML ファイルです。これには、デバイス保護ポリシー、制限、VPN 構成情報、Wi-Fi 設定、メールアカウント、カレンダーアカウント、iPhone や iPad とエンタープライズシステムとの関係を許可する認証の資格情報が含まれています。構成プロファイルでパスコードポリシーとデバイス設定を適用することで、組織で規定されているセキュリティ標準に従って適切に社内のデバイスを構成することができます。構成プロファイルを暗号化し、ロックしておけば、設定を削除・変更したり、ほかの人と共有することはできなくなります。

構成プロファイルでは、署名と暗号化の両方を利用できます。構成プロファイルに署名することにより、適用される設定は一切変更できなくなります。また、構成プロファイルを暗号化すると、プロファイルのコンテンツが保護され、対象となるデバイスにのみインストールが許可されます。構成プロファイルは、3DES および AES 128 をサポートする CMS (Cryptographic Message Syntax、RFC 3852) を使用して暗号化されます。

暗号化された構成プロファイルを初めて配布する場合は、構成ユーティリティを使って USB 経由でインストールするか、無線 (OTA) 登録によってインストールします。このほかにも、暗号化された構成プロファイルを添付ファイルとして E メールで配信したり、ユーザがアクセスできるウェブサイトホストしたり、モバイルデバイス管理 (MDM) ソリューションを使用してデバイスにプッシュする、という方法があります。

デバイスの制限

デバイスの制限では、そのデバイスでユーザがアクセスできる機能を設定します。制限する対象は通常、Safari、YouTube、iTunes Store など、ネットワークを利用したアプリケーションですが、アプリケーションのインストールやカメラの使用など、デバイスの機能を制御することもできます。制限を定義することで、要件に応じたデバイスの構成が可能になり、ユーザはビジネス慣行に応じた方法でデバイスを利用できるようになります。制限は、各デバイス上で手動で構成するか、構成プロファイルを使用して適用するか、MDM ソリューションを使用してリモートで適用することができます。また、パスコードポリシーと同様に、カメラとウェブブラウジングの制限も、Microsoft Exchange Server 2007 および 2010 を介してワイヤレスで適用することができます。

デバイスに制限とポリシーを設定できることに加え、iTunes デスクトップアプリケーションも、IT 部門が構成し、管理できます。そうすることで、不適切なコンテンツへのアクセスを禁止したり、ユーザが iTunes からアクセスできるネットワークサービスを定義したり、新しいソフトウェアアップデートをユーザがインストールできるかどうかを設定できるようになります。詳しくは、『iOS 搭載デバイスのための iTunes の配備』を参照してください。

データ保護

- ・ ハードウェア暗号化
- ・ データ保護
- ・ リモートワイブ
- ・ ローカルワイブ
- ・ 構成プロファイルの暗号化
- ・ iTunes のバックアップデータの暗号化

データ保護

会社や顧客の重要な機密情報を扱う環境では、iPhone と iPad に保存されたデータを保護することが重要です。iPhone と iPad では、転送中のデータを暗号化できるほか、デバイスに保存されたすべてのデータをハードウェア暗号化し、Eメールおよびアプリケーションデータも暗号化することで、データ保護をさらに強化します。

万が一、デバイスを紛失したり、盗難された時には、デバイスを無効にし、保存されているデータを消去することが重要です。パスコードの入力に一定回数を超えて失敗した場合にデバイスのデータを消去するポリシーを設定するのも効果的で、デバイスへの不正アクセスを防ぐ重要な手段となります。

暗号化

iPhone と iPad では、ハードウェアベースの暗号化を使用できます。ハードウェア暗号化では、256 ビット AES を使用してデバイスのすべてのデータを保護します。暗号化は常に有効で、ユーザが無効にすることはできません。

また、ユーザのコンピュータの iTunes にバックアップされたデータを暗号化することもできます。これは、ユーザ自身で有効にするか、構成プロファイルのデバイス制限設定を使用して適用します。

iOS はメールで S/MIME をサポートしているため、iPhone と iPad では暗号化された Eメールメッセージを表示したり、送信することができます。Eメールメッセージが複数のアカウント間を移動したり、1つのアカウントで受信したメッセージが別のアカウントに転送されないように、制限を適用することもできます。

データ保護

iPhone と iPad のハードウェア暗号化機能に加え、iOS に組み込まれたデータ保護機能を使用することで、デバイスに保存された Eメールメッセージや添付ファイルをさらに強力に保護することができます。データ保護機能では、各ユーザ固有のデバイスパスコードと iPhone や iPad のハードウェア暗号化を組み合わせることで、強力な暗号鍵を生成します。デバイスがロックされると、この暗号鍵によってデータへのアクセスが禁止され、万が一デバイスを紛失したり、盗難された場合でも、重要な情報をしっかり守ることができます。

データ保護機能を有効にするには、デバイス上でパスコードを設定するだけです。データ保護の効果はパスコードの強度に依存します。そのため、企業のパスコードポリシーを設定する際に、5桁以上の強度の高いパスコードを要求し、適用するようにしておくことが重要です。パスコード設定画面を表示すると、デバイスでデータ保護が有効になっているかどうかを確認できます。モバイルデバイス管理 (MDM) ソリューションでデバイスを照会し、この情報を確認するという方法もあります。

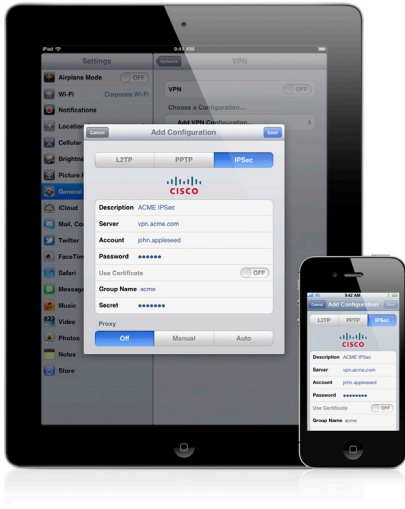
これらのデータ保護 API はアプリケーション開発者も使用でき、社内または商用のアプリケーションのデータを保護するために使用できます。

高度なパスコードのタイムアウト

パスコードの入力に何度も失敗した場合に、自動的にワイブを実行するように iPhone や iPad を構成することができます。間違ったパスコードを何度も入力すると、iOS は長時間使用できなくなります。パスコードの入力に失敗した回数が一定の回数を超えると、デバイス上のすべてのデータと設定が消去されます。

リモートワイブ

iOS は、リモートワイブ機能をサポートしています。万が一デバイスを紛失したり、盗難された場合、管理者またはデバイスの所有者がリモートワイブコマンドを実行して、すべてのデータを消去し、デバイスを無効にすることができます。Exchange アカウントを使用してデバイスが構成されている場合は、管理者が Exchange 管理コンソール (Exchange Server 2007) または Exchange ActiveSync Mobile Administration Web ツール (Exchange Server 2003 または 2007) を使用してリモートワイブを実行できます。Exchange Server 2007 の場合は、OWA (Outlook Web Access) を使用して直接リモートワイブコマンドを実行することもできます。会社で Exchange サービスが使用されていない場合でも、MDM ソリューションからリモートワイブコマンドを実行するという方法もあります。



ネットワーク保護

- Cisco IPSec, L2TP, PPTP VPN のビルトインサポート
- App Store アプリケーションを使用した SSL VPN
- X.509 証明書を使用した SSL/TLS
- 802.1X を使用した WPA/WPA2 Enterprise
- 証明書ベースの認証
- RSA SecurID、CRYPTOCARD

VPN プロトコル

- Cisco IPSec
- L2TP/IPSec
- PPTP
- SSL VPN

認証方法

- パスワード (MSCHAPv2)
- RSA SecurID
- CRYPTOCARD
- X.509 デジタル証明書
- 共有シークレット

802.1X 認証プロトコル

- EAP-TLS
- EAP-TTLS
- EAP-FAST
- EAP-SIM
- PEAP v0, v1
- LEAP

サポートされている証明書フォーマット

iOS は RSA キーを使用した X.509 証明書をサポートしています。 .cer、.crt、.der、.p12、.pfx の拡張子を認識します。

ローカルワイプ

パスコードの入力に一定回数を超えて失敗した場合に、自動的にローカルワイプを実行するようにデバイスを構成することもできます。この構成は、デバイスに強引にアクセスしようとする試みからデータを守る手段となります。パスコードを設定すると、ユーザが、設定から直接ローカルワイプを有効にできます。デフォルトでは、パスコードの入力に 10 回失敗すると自動的にデバイスのデータを消去します。ほかのパスコードポリシーと同様、ワイプされるまでの試行の最大回数は、構成プロファイルまたは MDM サーバで設定するか、Microsoft Exchange ActiveSync ポリシーを使用してワイヤレスで適用することができます。

iCloud

iCloud は、音楽、写真、アプリケーション、カレンダー、書類などを保存して、ユーザのすべてのデバイスに自動的にプッシュします。また、デバイスの設定、アプリケーションのデータ、テキストメッセージや MMS メッセージといった情報を、毎日 Wi-Fi 経由でバックアップします。インターネット経由で送信する際にはコンテンツを暗号化し、保存する際には暗号化したフォーマットを使用し、認証には安全なトークンを使うことにより、ユーザのコンテンツをしっかりと保護します。また、フォトストリーム、書類のシンク、バックアップといった iCloud の機能は、構成プロファイルで無効にできます。iCloud のセキュリティとプライバシーについては、http://support.apple.com/kb/HT4865?viewlocale=ja_JP を参照してください。

ネットワーク保護

モバイルユーザは、世界中のどこからでも企業の情報ネットワークにアクセスできなければなりません。その際には、ユーザの認証と転送中のデータ保護も確実にを行う必要があります。iOS は、定評あるテクノロジーを搭載しているため、Wi-Fi 接続と携帯電話データネットワーク接続の両方で、こうしたセキュリティ目標を達成することができます。

既存のインフラストラクチャに加え、FaceTime のセッションや iMessage での会話も、それぞれエンドツーエンドで暗号化されます。iOS は各ユーザ固有の ID を作成し、コミュニケーションの適切な暗号化、ルーティング、接続を確実に行います。

VPN

多くのエンタープライズ環境では、何らかの形態で仮想プライベートネットワーク (VPN) が構築されています。こうした安全なネットワークサービスがすでに配備されている場合は、通常、最小限の設定と構成だけで、iPhone や iPad を統合することができます。

iOS は、Cisco IPSec、L2TP、PPTP を標準でサポートしているので、一般的に使用されている様々な VPN 環境に統合できます。さらに、Juniper、Cisco、F5 Networks、SonicWALL、Aruba Networks のアプリケーションを使えば、SSL VPN にも対応します。これらのプロトコルに対応するので、機密情報の転送時には、最高レベルの IP ベース暗号化を利用できます。

iOS は、既存の VPN 環境に安全にアクセスできるだけでなく、定評あるユーザ認証方式も採用しています。標準的な X.509 デジタル証明書による認証は、企業のリソースへの効率的なアクセスを可能にし、ハードウェアベースのトークンの代わりとして利用できます。また、証明書認証により、iOS で VPN オンデマンド機能を利用できるため、ユーザに VPN 認証プロセスを意識させることなく、強力な認証によってネットワークサービスにアクセスできるようになります。二要素トークンが必要なエンタープライズ環境では、iOS に RSA SecurID や CRYPTOCARD を統合できます。

iOS は、ネットワークプロキシ構成に加え、スプリット IP トンネリングもサポートしているので、パブリックネットワークドメインへのトラフィックも、プライベートネットワークドメインへのトラフィックも、会社独自のポリシーに従って中継することができます。

SSL/TLS

iOS は、SSL v3 に加え、次世代のインターネットセキュリティ標準である TLS v1.0、1.1、1.2 (Transport Layer Security) もサポートしています。Safari、カレンダー、メール、その他のインターネットを使うアプリケーションは、これらのメカニズムを自動的に開始し、iOS と企業サービスとの間での通信を暗号化します。

WPA/WPA2

iOS は、WPA2 Enterprise をサポートしているので、企業のワイヤレスネットワークへの認証を用いたアクセスが可能になります。WPA2 Enterprise は、128 ビットの AES 暗号化を採用しているため、ユーザが Wi-Fi ネットワーク経由で情報を送受信する際、高いレベルでデータを保護します。iPhone と iPad は 802.1X に対応しているため、様々な RADIUS 認証環境に統合できます。

アプリケーション保護

アプリケーション保護

- ・ランタイム保護
- ・コード署名の強制
- ・キーチェーンサービス
- ・CommonCrypto APIs
- ・アプリケーションのデータ保護

iOS は、セキュリティを重視して設計されたプラットフォームです。例えば、「サンドボックス化」によって、アプリケーションのランタイム保護を実現したり、署名を要求することでアプリケーションの改ざんを防いでいます。さらに、アプリケーションとネットワークサービスの資格情報を、暗号化されたキーチェーンに安全に保存するためのフレームワークもあります。アプリケーション開発者向けには、アプリケーションのデータストアの暗号化に使用できる共通の暗号アーキテクチャが用意されています。

ランタイム保護

デバイス上のアプリケーションは「サンドボックス化」されているため、ほかのアプリケーションの保存データにはアクセスできません。また、システムファイル、リソース、およびカーネルは、ユーザのアプリケーション空間から保護されています。アプリケーションがほかのアプリケーションのデータにアクセスする必要がある場合は、iOS が提供する API とサービスを使用した時のみアクセスできます。コード生成も防ぎます。

コード署名の強制

すべての iOS アプリケーションには署名が義務づけられています。デバイスに内蔵されているアプリケーションには、Apple が署名し、他社製アプリケーションについては、アプリケーション開発者が Apple 発行の証明書を使用して署名しています。これにより、アプリケーションが改ざんや変更が加えられていないことを確認できます。さらに、アプリケーションを前回使用した後に、信頼できない状態になっていないかどうかを確認するためにランタイムチェックが実行されます。

カスタムアプリケーションや社内アプリケーションの使用は、プロビジョニングプロファイルで制御できます。ユーザは、アプリケーションを実行する前に、プロビジョニングプロファイルをインストールする必要があります。プロビジョニングプロファイルのインストールや削除は、MDM ソリューションを使用して、ワイヤレスで行えます。管理者は特定のデバイスに対してアプリケーションの使用を制限することもできます。

安全な認証フレームワーク

iOS には、デジタル ID、ユーザ名、パスワードの格納に使用される、暗号化された安全なキーチェーンが用意されています。キーチェーンのデータは分割されているため、他社製アプリケーションによって格納された資格情報に、別の固有名を持つアプリケーションがアクセスすることはできません。こうしたメカニズムにより、iPhone と iPad に保存された、企業内の様々なアプリケーションとサービスの認証資格情報がしっかり保護されます。

共通の暗号化アーキテクチャ

アプリケーション開発者は、暗号化 API を利用して、アプリケーションデータの保護を強化することができます。データは、AES、RC4、3DES など実績のある方式を利用して対称鍵方式で暗号化されます。さらに、iPhone と iPad には AES 暗号化および SHA1 ハッシュのためのハードウェアアクセラレーションが搭載されているので、アプリケーションのパフォーマンスを最大限に引き出すことができます。

アプリケーションのデータ保護

iPhone と iPad に組み込まれたハードウェア暗号化機能をアプリケーションで使用して、重要なアプリケーションデータをより強力に保護することもできます。アプリケーション開発者は、データを保護したい特定のファイルを指定し、アプリケーションや侵入者がファイルの内容にアクセスできないよう、デバイスがロックされた際にファイルの内容を暗号化するように設定しておけます。

管理対象のアプリケーション

MDM サーバでは、App Store から入手できる他社製アプリケーションと、社内向けアプリケーションを管理できます。アプリケーションを管理対象として設定すれば、デバイス上のアプリケーションとその関連データを MDM サーバから削除できるかどうかを指定できるようになります。また、サーバでは、管理対象のアプリケーションのデータが iTunes や iCloud にバックアップされないようにすることもできます。これにより、IT 部門は機密性の高いビジネス情報を含んでいる可能性のあるアプリケーションを、ユーザが直接ダウンロードしたアプリケーションよりも細かく管理できます。

管理対象のアプリケーションをインストールするために、MDM サーバからデバイスにインストールコマンドが送信されます。管理対象のアプリケーションには、インストール前にユーザによる承認が必要です。管理対象のアプリケーションについて詳しくは、「モバイルデバイス管理の概要」(www.apple.com/jp/iphone/business/integration/mdm)を参照してください。

完全なセキュリティを備えた革新的なデバイス

iPhone と iPad は、転送中または保存されているデータと、iCloud や iTunes へのバックアップ中のデータを暗号化して保護します。ユーザが企業の E メールにアクセスしている時も、個人のウェブサイトを見ている時も、企業ネットワークにアクセスするための認証を行っている時も、iOS は、認証済みのユーザ以外は企業の機密情報にアクセスできないようにします。また、エンタープライズクラスのネットワーク機能とデータ損失防止のための包括的な機能を備えているので、実績のあるモバイルデバイスセキュリティとデータ保護が実装されているという確信を持って iOS デバイスを導入することができます。