iPhoneセキュリティ上のトレードオフ

西田圭介（@k24d）

iPhoneのセキュリティ

- デバイスのセキュリティ
  - パスコードポリシー、構成プロファイル
- データのセキュリティ
  - ハードウェア暗号化、データ保護、リモートワイプ
- ネットワークのセキュリティ
  - 各種VPN、Wi-Fi（WPA2 Enterprise）
- アプリのセキュリティ
  - サンドボックス、アプリ署名、キーチェーン

参考：http://www.apple.com/jp/iphone/business/integration/

パスコード

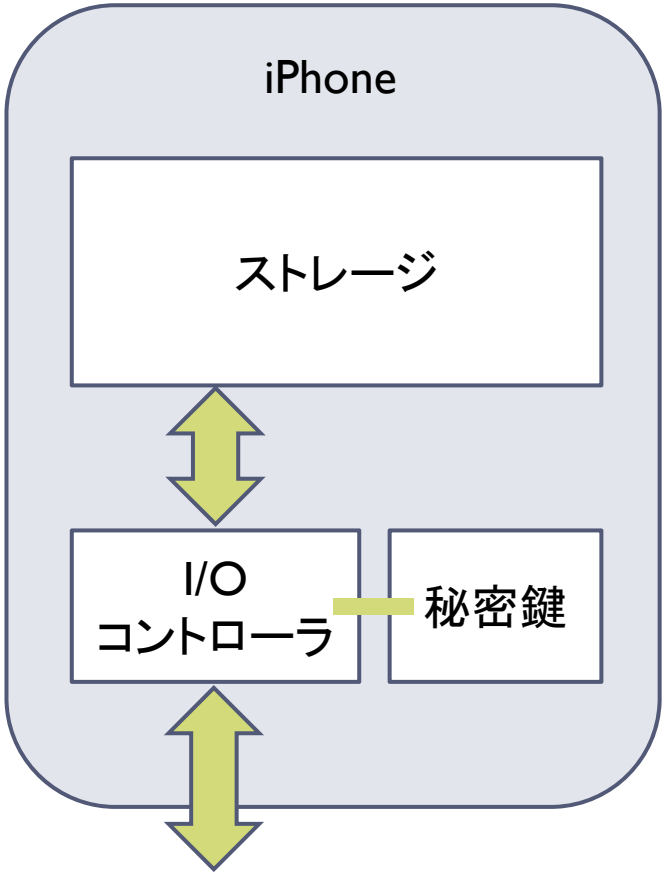
- 管理者がパスコードポリシーを強制可能
  - 長さ、複雑さ、有効期間、etc.
  - 何度も間違えると強制的にワイプ
- ロック画面はカスタマイズ不可能
  - → マルウェアによる影響を受けない

構成プロファイル

- 各種の設定をひとつにまとめたファイル
  - メールアカウント、Wi-Fi、VPN、電子証明書など
  - パスコードポリシー、機能制限など
- 管理者による署名、暗号化が可能
  - アカウント情報の変更、流出を防止
- OTA（Over-The-Air = 無線）による配布
  - サーバからの一括設定が可能

ハードウェア暗号化（iOS 3.x）

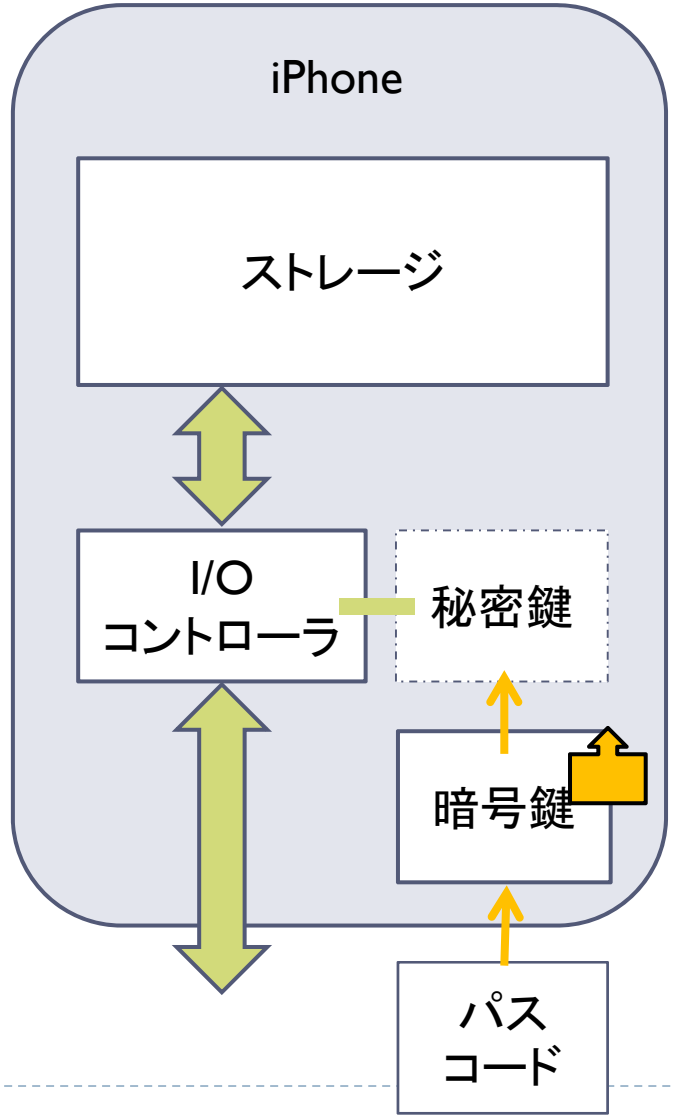
- すべてのディスクI/Oを暗号化
  - iPhone 3GS以降
- ただし・・
  - 秘密鍵はデバイス内にある
  - データは常に復号化される
  - → 情報漏えいを防げない
- 何のためにあるのか？
  - → 高速なワイプ



参考：http://k24d.net/post/12716855652/ios-data-protection

データ保護（iOS 4.x）

- 情報漏えいを防ぐ
  - 秘密鍵そのものを暗号化
  - ユーザのパスコードを利用
  - ロックすると秘密鍵を消去
- 保護すると不便になることも
  - 例： ロック中の音楽再生
  - 例： ロック中のアップロード
- 保護されるデータは一部のみ
  - キーチェーン
  - 標準「メール」アプリ
  - アプリで特別に指定した場合



バックアップ

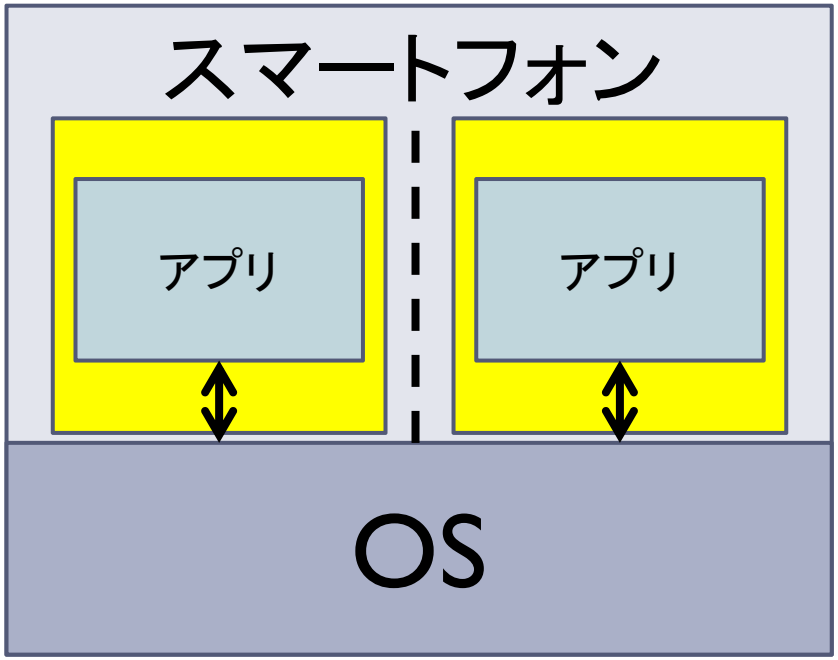
- 暗号化なしの場合
  - 生データがバックアップされる
  - キーチェーンはデバイス固有鍵で暗号化
    - 元デバイスへは復元可能、別デバイスへはコピー不可
- 暗号化ありの場合
  - すべてのデータをパスワードで暗号化
  - キーチェーンもコピー可能になる
    - 一部データを除く（例：証明書の秘密鍵）
- 預託（escrow）キーバッグ
  - データ保護を外すための特殊な鍵
  - → PCのセキュリティも重要

リモートワイプ

- リモートワイプには準備が必要
  - 「iPhoneを探す」
    - 法人単位では管理できない
  - Exchange ActiveSync
    - メールを同期しなければワイプされない
  - MDM（モバイルデバイス管理）
    - MDMサービスへの加入が必要
- 業務アプリのみのワイプも可能（MDM）
  - 管理者が設定したメール、VPN、アプリ等だけ消去

サンドボックス

- アプリの実行空間を分離
  - ファイルシステムの分離
  - 利用できるサービスの制限
- 利点
  - システムを壊さない
  - アプリの依存関係がない
  - データの流出を防げる
- 欠点
  - 管理者権限がない
  - アプリ間の連携が難しい



参考：http://k24d.net/post/12722877231/iphone-anti-virus

アプリ間の連携

- システムデータは共有可能（写真、連絡先、etc.）
- アプリデータ（ファイル）の受け渡しはユーザが指定
  - アプリ間の共有ストレージは、同一開発元でのみ可能
- ファイル単位でデータ保護が可能

- 参考：　Androidでは・・
  - iOSよりも利便性が高い（≒リスクも高い）
  - 例：　インテントにより全アプリにブロードキャスト

バックグラウンド処理

- バックグラウンドで出来るタスクは限定的
  - 音楽、IP電話、位置情報検出、etc.
  - プッシュ通知によりサーバからイベントを送ればよい
- アプリの同時実行を許さない
  - 一つ一つのアプリにリソースを集中
  - バッテリーの節約

- 参考： Androidでは・・
  - プッシュ通知（C2DM）はまだベータ段階
  - アプリ毎にバックグラウンドのサービスを実行可能

参考：http://d.hatena.ne.jp/silvervine/20100423/1272007872

アプリ署名

- Appleが署名したアプリしか実行できない
  - App Store
  - インハウスアプリケーション
  - 開発中のアプリ
- Apple社は署名を失効させることが可能
  - インストール済みのアプリでも起動できなくなる

ウィルス対策

- ウィルスもセキュリティソフトも実行が困難
  - サンドボックスによりアプリが隔離されている
  - アプリを起動しない限りは実行されない
    - バックグラウンドの動作が許されない
- 問題のあるアプリはApp Storeから削除される
  - アプリをコピーできないので拡散しない

- ※iOSのセキュリティはApple社によって守られている
  - ジェイルブレイクすると上記のモデルが破綻