BYODのリスク分析
～個人スマホを社則で縛るのはナンセンス～

KDDI研究所
竹森 敬祐 （Ph.D）

BYODって、リスク分析の積み上げです。
リスク低減の施策と許容レベルを考慮し、
何を何処まで許可すべきか考えます。

本音はコスト削減。でも安全も維持したい。

BYOD vs 安全性：社内規則で縛れるの？！

■ 会社と社員の相互理解
- ◆ 会社は社員スマホの通信費の一部を負担する。
  - ⇒ 負担の代償として、社員に依頼できそうな／すべき規則を交渉。

■ 依頼できそうな／すべき規則
- ◆ パスワード／パターンロック：効果＝紛失時の情報漏洩防止
  - ⇒ 個人利用においても必要性ですね。
  - ⇒ パターンロックなら導入の敷居は低いです。
- ◆ USBデバッグOFF：効果＝紛失時の情報漏洩防止
  - ⇒ 一般的な利用シーンで、USB経由でPC接続する必要はない。

■ 会社の費用負担で依頼できそう？
- ◆ MDMの導入：効果＝ロック・ワイプ・暗号化などの基本対策
  - ⇒ 法人領域のみを管理することを了解して貰う。

BYOD vs 安全性：社内規則で縛れるの？！

■ 依頼できそうにないこと

- ◆ 様々なOS／端末がある中で、購入OS／端末を規定できない。
  ⇒ 安全度の低いOSを基準に、対策・リスク分析を行う。
- ◆ 盗撮カメラで逮捕者や、アドレス帳等の情報送信アプリもあるが、個人スマホに対するアプリのインストール制限はやりすぎです。
  ⇒ アプリの脅威を許容できますか？
- ◆ セキュリティソフトは有料であったり効果を発揮できない側面が。
  ⇒ マルウェア感染やJailbreakツールの導入で、標的型攻撃を担える端末がいることを想定した、法人NWの設計が必要。
- ◆ WiFi／USBテザリング機能を持ち、社内PCがスマホを経由して、インターネットに直接繋がる。
  ⇒ 社内でのテザリングを防ぐ施策が必要。
- ◆ 端末内の情報は、個人所有のものがある。
  ⇒ 紛失時にリモートワイプを拒否されることを前提にする。

スマホ・タブレットの特徴（1）

■ オープンOS端末のパッチ

◆ 脆弱性へのパッチ配布が、端末ベンダに任されている。

パッチの整合性検査に時間を要し、配布が遅い・無い。

但し、昨今の傾向として脆弱性を狙うマルウェアは少ない。

■ OSベンダ主導のパッチ

◆ OSベンダがパッチを統一的に配布する。

パッチは迅速に配布され、最新の状態に保ちやすい。

スマホ・タブレットの特徴(2)

■ 情報収集モジュール

◆ 無料アプリの45%が情報を外部送信している(KDDI研調べ2011)。

件(率)/400	送信情報
50件(12.5%)	OS生成 ID
57件(14.3%)	端末ID(IMEI)
7件(1.8%)	加入者ID(IMSI)
0件(0.0%)	SIMシリアルID(ICCID)
7件(1.8%)	メールアドレス
87件(21.8%)	OS生成IDのハッシュ値
4件(1.0%)	IMEIのハッシュ値
4件(1.0%)	電話番号
32件(8.0%)	位置(緯度・経度)
3件(0.8%)	インストールアプリ一覧

■ プライバシ保護型OS

◆ 送信される情報は限られる。

◆ 送信する情報を利用者が制限することができる。

スマホ・タブレットの特徴（3）

■ オープンOS向けマルウェア

◆ 出現数　PC：オープンOS ＝400：1　（カスペルスキー2011統計）

◆ Marketから駆除されると、感染の拡大が止まる。

知らないうちにマルウェア感染する確率はPCよりもかなり低い。

マルウェアの多くは、非公式Marketにある。

■ OSベンダ管理型向けマルウェア

◆ Makertに厳格な審査があり、マルウェアは殆ど出現していない。

知らないうちに感染する脅威は、殆どない。

利用者がJailbreakした端末は、踏み台になっている?!

KDDI R&D LABS

BYODのリスク分析
～個人スマホを社則で縛るのはナンセンス～

KDDI研究所
竹森 敬祐 （Ph.D）

BYODって、リスク分析の積み上げです。
リスク低減の施策と許容レベルを考慮し、
何を何処まで許可すべきか考えます。

本音はコスト削減。でも安全も維持したい。

KDDI R&D LABS

リスクウェアの整理

◆ スマホに生じるリスクの殆どは、アプリの導入・利用に起因する。

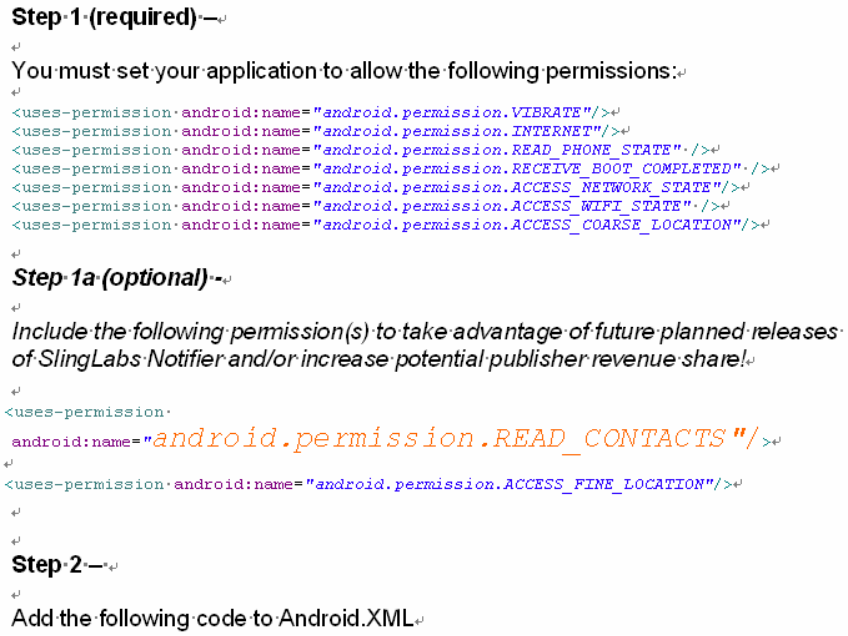
分類	定義	具体例	
		悪性アプリ 参考：現時点の日本における脅威レベル	設計ミス・迷惑なアプリ 参考：現時点の日本における脅威レベル
情報漏洩	・勝手に利用者情報を送信するアプリ	・スパイウェア 主に海外の非公式配信サイトに掲載され日本の利用者への感染は殆ど無い。（脅威小） ・情報漏洩型の悪性Webサイト 悪性Webサイト閲覧による攻撃スクリプトの実行を通じた情報漏洩が想定される。（脅威小）	・説明/許諾のない情報収集 主にターゲティング広告の為であり、脅迫などの実被害の報告は無い。（脅威中） ・ファイル操作の設計ミスによる情報漏洩 外部から端末内ファイルを読み取れてしまう設計ミスのアプリがある。（脅威小）
不正課金	・勝手に料金の生じるサービスを利用するアプリ ・利用者を騙して金銭を要求するアプリ	・プレミアムSMS 日本にプレミアムSMSのサービスは無く実被害無し（脅威小） ・振込め/ワンクリック詐欺 多くは日本の成人向けWebサイトに掲載され自動感染は無いが、騙され易い。（脅威中）	・説明/許諾のないSMSの利用 リモート制御のためのSMS通信等であり、悪意の制御には至っていない。（脅威小）
踏み台	・端末を外部から不正に制御するアプリ	・ボット/バックドア 多くは海外の非公式配信サイトに掲載され、日本の利用者の感染は殆ど無い。（脅威小）	対象外
脱獄 （ﾊｯｷﾝｸﾞ）	・OS/ライブラリ/アプリ等の脆弱性を突くアプリ ・他のアプリが作った裏口や特権を利用するアプリ	・アタック 多くは海外の非公式配信サイトに掲載され、日本の利用者の感染は殆ど無い。（脅威小）	・制限された権限/コマンドの利用 非開放機能の活用であり直接的な被害は少ない。（脅威小）
悪用	・使い方によっては、法令に抵触するアプリ	対象外	・盗撮(消音)カメラ/ビデオ 使い方によっては被害者が出てしまう、もしくは機密情報の漏洩に至る。（脅威中）

KDDI R&D LABS

アプリによる情報送信の問題

- 端末から何らかの情報を送信するアプリ　181/400件（45%）
  - 適切な説明を経て情報収集しているアプリ　白17/181件（10%）
  - 不適切な説明のまま情報収集しているアプリ　灰7/181件（4%）
  - 勝手に情報送信しているアプリ　黒157/181件（86%）

情報収集モジュール



Step 1 (required) –

You must set your application to allow the following permissions:

```
<uses-permission android:name="android.permission.VIBRATE"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
```

Step 1a (optional) -

Include the following permission(s) to take advantage of future planned releases of SlingLabs Notifier and/or increase potential publisher revenue share!

```
<uses-permission
android:name="android.permission.READ_CONTACTS"/>
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
```

Step 2 –

Add the following code to Android.XML

- 悩ましい実態
  - 情報送信アプリが多過ぎ、スパイウェアの判断がつかない（放置）。
  - アドレス帳も収集されることを前提にする。

KDDI R&D LABS

スマホが管理する情報の一例

スマホから送信できる利用者を特定する情報および各種識別子（ID）

種別	詳細
利用者を特定する情報	氏名、アドレス帳で管理される情報、メールアドレス
個体を識別する情報（ID）	OSが生成するID、端末ID（IMEI：d14桁）、加入者ID（IMSI：d14桁）、SIMシリアルID（ICCID：d19桁）、電話番号（d11桁）、認証チケット、アプリが独自に発行するID、MACアドレス、OSやサービスへのログインアカウント、IPアドレスなど

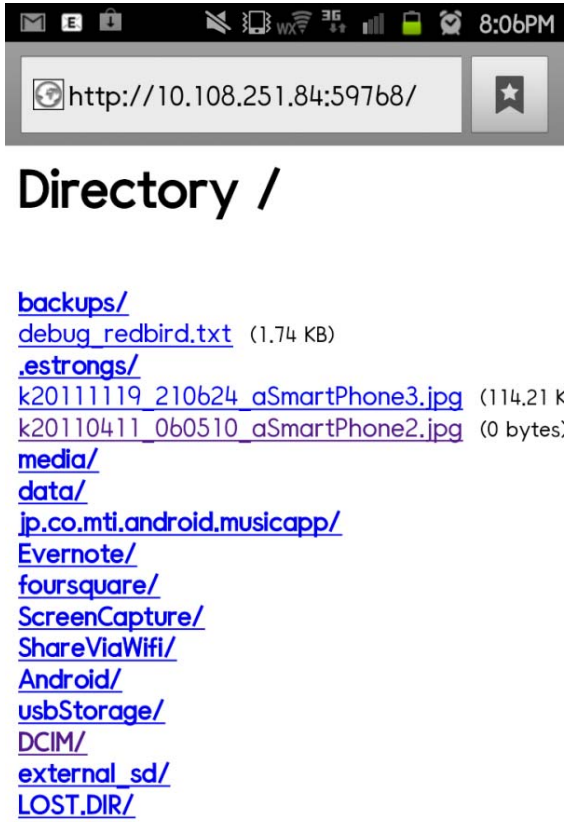
スマホから送信できるプライバシ情報

種別	詳細
利用履歴	位置情報、通話・メールの履歴、Webのブックマーク・閲覧履歴など
アプリ	アプリの一覧・利用履歴、アプリの管理データなど

設計ミス：SDカード上のファイルの公開

- ファイル操作アプリ
  - ファイルを閲覧・操作するアプリを使うと、バックドアが開いてSDカード上のファイルが外部に公開される。

⇒ 開発者の設計ミスで情報漏洩が生じる。



他人のAndroid端末のSDカードを閲覧できている。

悪性アプリ：振込め／ワンクリック詐欺

■ 非公式アプリ配信サイト

◆ 日本の成人向けWebサイトに偽の再生アプリが置かれた。

⇒「提供元不明アプリ」をデフォルト設定（OFF）にしておけば安心。

迷惑なアプリ：盗撮（消音）カメラ

■ 迷惑なアプリとは

◆ 利用者の使い方次第で、第三者に迷惑をかけるアプリのこと。

◆ 消音カメラは、盗撮で被害者が出るなど社会問題になっている。

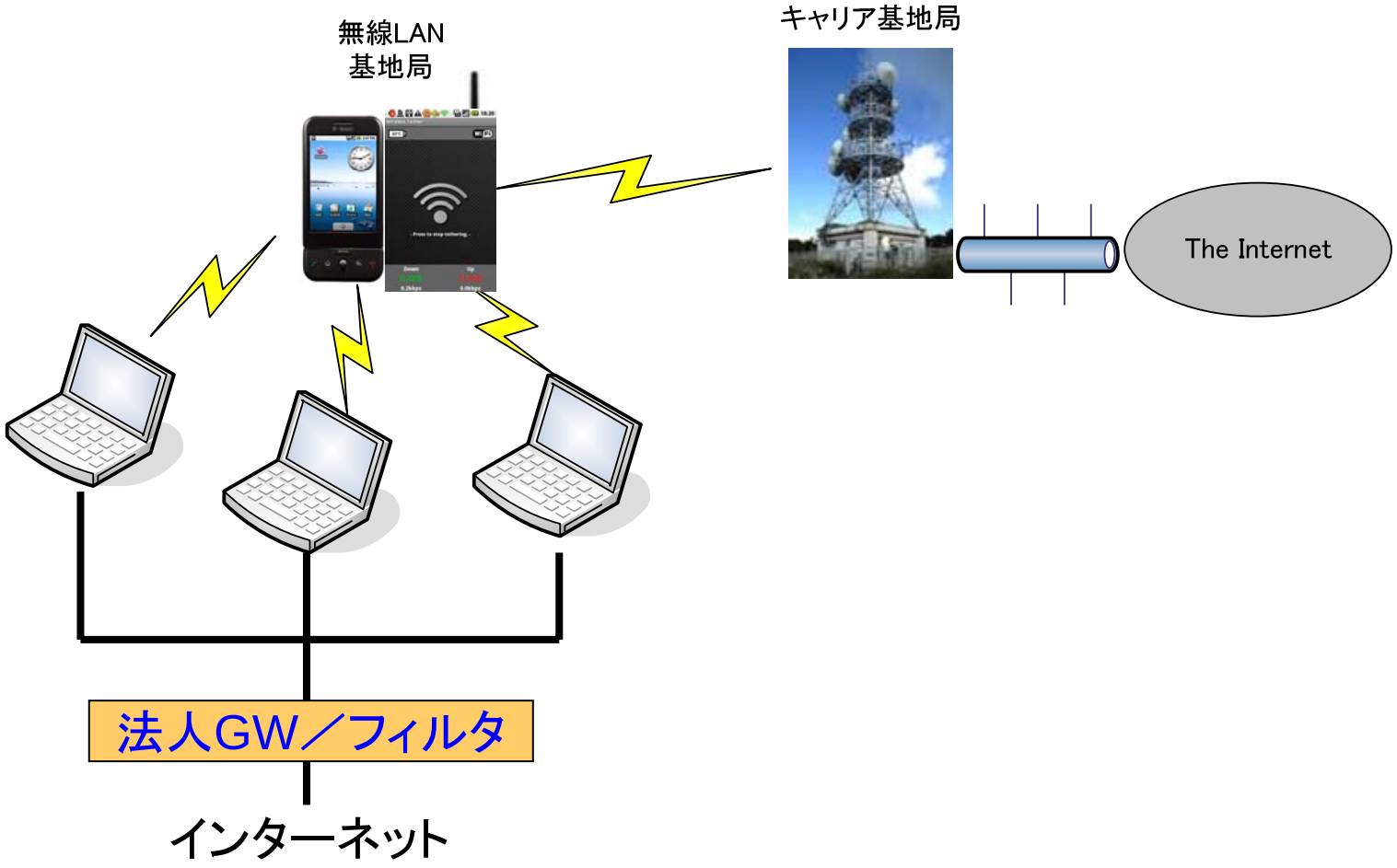
- 正しい使い方
  - 動物を撮影する。
  - 撮影許可のある美術館で撮影する。

- 問題のある使い方
  - 駅で盗撮をする。
  - 工場や研究施設を盗撮する。
  - 書籍を電子万引きする。

http://t0.gstatic.com/images?q=tbn:ANd9GcTuDn7nvVDQNPN3tDVOBtGaK3h-YM9AbowFtPUvxn6GtAO15wkoftTQnjkOhA

制限された機能：テザリング

- テザリングとは
  - スマホが無線LANルータになり、インターネットへ直接繋がる。



BYODのリスク分析
～個人スマホを社則で縛るのはナンセンス～

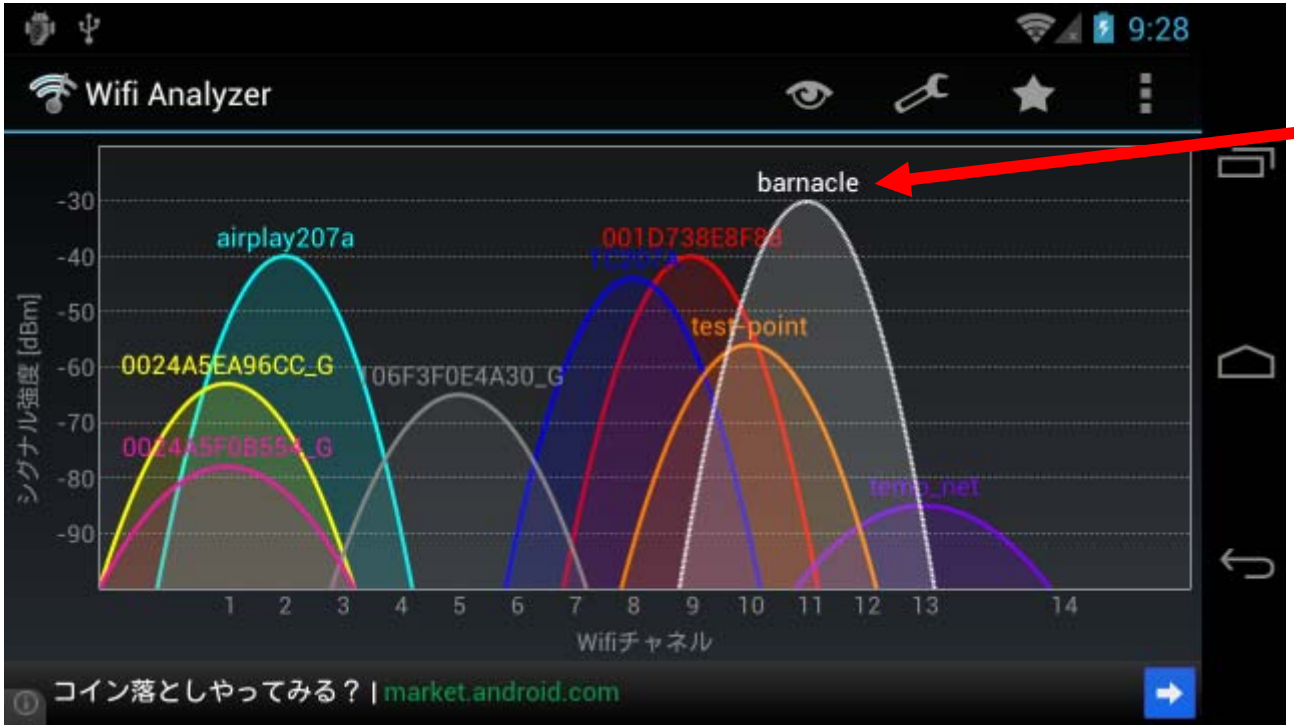
KDDI研究所
竹森 敬祐 （Ph.D）

BYODって、リスク分析の積み上げです。
リスク低減の施策と許容レベルを考慮し、
何を何処まで許可すべきか考えます。

本音はコスト削減。でも安全も維持したい。

かってなWiFiアクセスポイント（AP）を探し出す

- 社内LANからネットへのバックドア対策
  - USBテザリングを防ぐため、USBデバックのOFFを規定する。
  - スマホをWiFi-AP化して、法人GWを通過しないネット通信を防ぐ。
    ⇒ WiFi Analyzerを使って、強度が高く、知らないWiFi-APを探査。



スマホでWiFi-AP（barnacleアプリ）を立てたもの。

「KDDI 3LM」でのBYOD:個人端末を法人契約枠へ

KDDI 3LM Security

企業管理アプリ

- 業務アプリ
- セキュリティソフト
- グループウェア（Exchange）
- など

- データ強制暗号化
- 端末からアプリ削除の禁止
- コピー＆ペースト制限
- 指定アプリデータの削除

業務利用と個人利用のアプリを別管理

個人利用アプリ

- ゲーム
- SNS
- E-mail
- 電話
- SMS
- など

- 利用制限なし



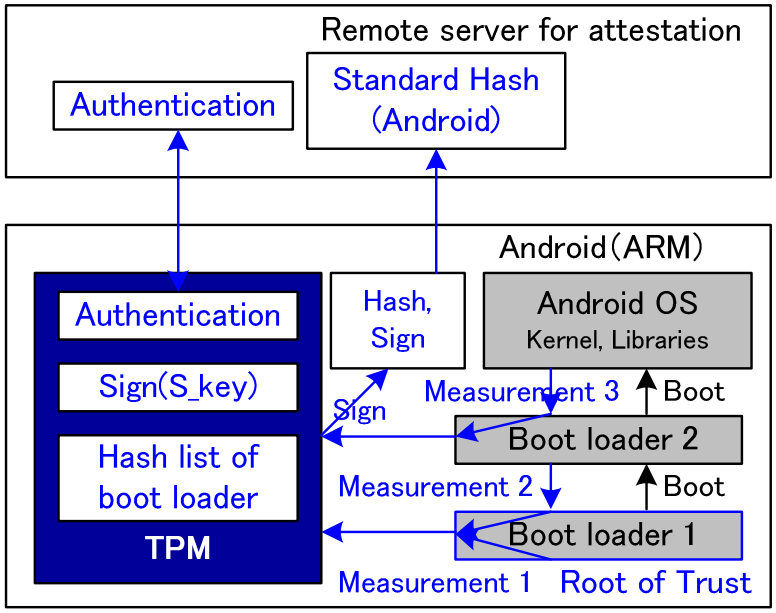
業務アプリやセキュリティなど企業管理が必要なアプリケーションを別管理。
またロック・ワイプなど個人利用で有効な機能も利用可能に！

KDDI R&D LABS

検疫研究：Android（ARM）＋TPMのセキュアブート

■ セキュアブート
- ◆ Android搭載のARMボードにTPMを接続して、認証・完全性検証を試作。
- ◆ 端末起動時に、ブートローダ、Android OS、アプリの状態を測定。
- ◆ 測定結果を、遠隔の状態管理局に送付し、完全性を検証する。

⇒ 重要サービスへの接続の際に、認証・完全性検証をH/Wレベルで実現。



セキュアブートの手順

実装例

BYODのリスク分析
～個人スマホを社則で縛るのはナンセンス～

KDDI研究所
竹森 敬祐 （Ph.D）

BYODって、リスク分析の積み上げです。
リスク低減の施策と許容レベルを考慮し、
何を何処まで許可すべきか考えます。

本音はコスト削減。でも安全も維持したい。

復習：BYODの前提条件

- 社員にお願いできそうなこと
  - パスワード／パターンロックを掛けて貰う。
  - USB接続機能をOFFにする。

- もう少しだけ社員にお願いできそうなこと
  - root権限奪取（Jailbreak）しない。
  - アドレス帳に社員やお客様の情報を入力しない。
  - 紛失時には通信事業者に依頼して、リモートロックを掛けて貰う。
  - 会社側の費用負担で、会社用アプリ保護にMDMを適用して貰う。

↓

上記以上に期待はできないでしょう。

↓

次項から設計とリスク分析の一例を紹介します。

KDDI R&D LABS

リスク分析の一例：許容範囲を考える

■ 電話の発着信
- ◆ 電話帳に社員やお客様情報を登録せず、単なる電話として利用。
  ⇒ 発着信履歴の漏洩（確率：低）×TEL番（影響：低）＝リスク：低

■ メールの送受信
- ◆ パスワード入力型のWebメールを使う。
  ⇒ メールサーバ侵入（確率：低）×内容（影響：大）＝リスク：中
- ◆ MDMを適用して専用のメールアプリを使う。
  ⇒ 紛失時に漏洩（確率：低）×内容（影響：大）＝リスク：中

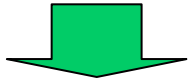
■ 業務システム・アプリ
- ◆ LANの外側にパスワード入力型Webベース業務システムを設置。
  ⇒ サーバ侵入（確率：低）×内容（影響：大）＝リスク：中
- ◆ MDMを適用して端末内の業務用アプリを用いる。
  ⇒ 紛失時に漏洩（確率：低）×内容（影響：大）＝リスク：中

KDDI R&D LABS

その他の案

- デフォルト安全なOSに限定する
  - 安全性の高いOSであれば認める。
    ⇒ 紛失時に漏洩（確率：小）×内容（影響：大）＝リスク：中
    （パスワードロックでROM全体が暗号化されている。）

- オープンOS端末にはMDMを別途法人契約する
  - MDMでディスクの暗号化、ワイプの同意が得られれば認める。
    ⇒ 紛失時に漏洩（確率：低）×内容（影響：大）＝リスク：中
    （KDDI-3LMセキュリティを導入すれば、ロック・ワイプ・暗号化できる。）



上記の2つの施策を並行して打てるのはauだけ♪

この資料、営業トークだったのか？！

KDDI R&D LABS