日本スマートフォンセキュリティフォーラム
-スマートフォンを安心して利用出来る社会へ-

技術部会
ネットワークWG
進捗報告

2011年11月7日

サブリーダ　相原弘明

Agenda

- **ネットワークWGの目的**
- **活動課題**
- **タスクフォース (TF) メンバー**
- **ネットワークWGのスコープ**
- **検討プロセス**
- **進め方**
- **個別課題の検討**
- **成果物の目次とスケジュール**
- **成果物抜粋**

ネットワークWGの目的

- 目的
  - スマートフォンのネットワーク観点から、セキュリティ課題の検討を行うワーキンググループ

- リーダ/サブリーダ
  - ネットワークWGリーダー
    清水(新日本無線株式会社)
  - ネットワークWGサブリーダー
    相原(株式会社ネットマークス)

活動課題

- **第1回WGでの募集により提案された課題案**
  - **① スマートフォンの業務利用における技術的課題の解決支援**
  - **② Wi-Fi や VPN（に限らず認証を利用するもの）での動作確認**
  - **③ 端末・個人認証によるネットワーク安全性保証ソリューションの検討**
  - **④ スマートフォンを利用するにあたってのネットワーク環境で必要となるセキュリティ対策に関する実装ガイド提供**
  - **⑤ ワイヤレス技術やセンシング技術による、M2P／P2M認証（ｻｰﾋﾞｽ認証）**の検討と検証。**（**：Machine-to-Person / Person-to-Machine）**
- **結論　(第2回WGで報告)**
  - **「スマートフォンセキュリティ実装ガイド（ネットワーク認証編/認可編）」**
  - **スマートフォン監視（盗難・紛失・置忘れの未然対策）**

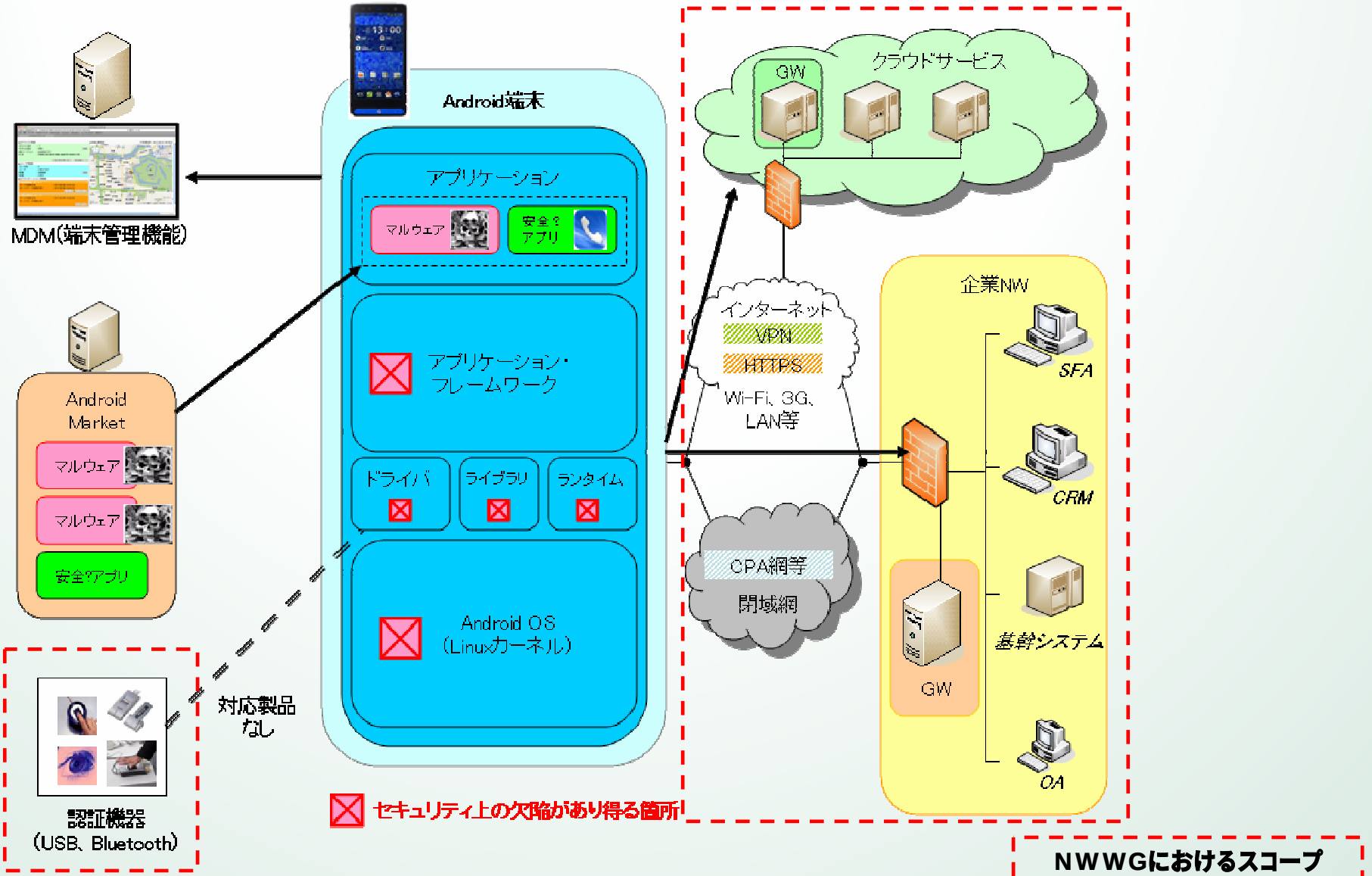
タスクフォースメンバー(TF)

TFを募集して活動課題を推進しています。

- トヨタ自動車株式会社：倉林
- サイバートラスト株式会社：合田
- 株式会社大和総研ビジネス・イノベーション：倉永
- 株式会社ＫＢＩＺ：小熊
- ＮＲＩセキュアテクノロジーズ株式会社：原田
- 株式会社ネクストジェン：二村
- 株式会社KDDI研究所：渡辺
- 新日本無線株式会社：鈴木
- 株式会社ネットマークス：栃沢
- ネットワークWGリーダー：清水(新日本無線株式会社)
- ネットワークWGサブリーダー：相原(株式会社ネットマークス)

※随時募集を継続　　(敬称略)

ネットワークWGのスコープ



検討プロセス

WGとTFをそれぞれ月1回開催

- WG　4回
  - 7/26　第1回WG開催
    - 課題テーマの募集結果とその説明
    - 検討メンバーとしてのタスクフォース（TF)募集
  - 8/30　第2回WG開催
    - TFメンバー紹介
    - 課題テーマの説明
  - 9/27　第3回WG開催
    - 課題テーマに対する方針説明と課題検討
  - 10/31　第4回WG開催
    - 課題の検討
- TF　4回開催
  - 8/8、9/13、9/22、10/14

進め方

- 方針とゴールの共有
  - それぞれの環境、立場、目的の異なるメンバーが参画している為、TFとしての方針とゴールを議論し、共有することが重要。
- 利用部会で公開されたガイドラインをブレイクダウン
- PCとの違いを整理
  - PCでのセキュリティ対策との対比
  - PCで必要だが、スマホでは不要な対策／スマホでは必要だがPCでは不要な対策
  - PCにはない、将来的に必要なセキュリティ対策
- ネットワーク構成・接続パターンを整理
  - ガイドラインを元に整理
- 個別課題の検討

個別課題の検討

- 当初設定した課題とは別に当WGまたは他WGにて提案された個別課題についても検討中。
  - 公衆Wi-Fiの偽装に対する脅威と対策
  - VPN接続中にテザリング機能を利用した場合、そこに接続される機器（スマホ・PC他）はVPNを経由して社内に接続可能かを検討
  - 総務省において10/19「スマートフォン・クラウドセキュリティ研究会」が開催された。それを受けてJSSECでもクラウドタスクフォースをネットワークWG内で立ち上げることを検討

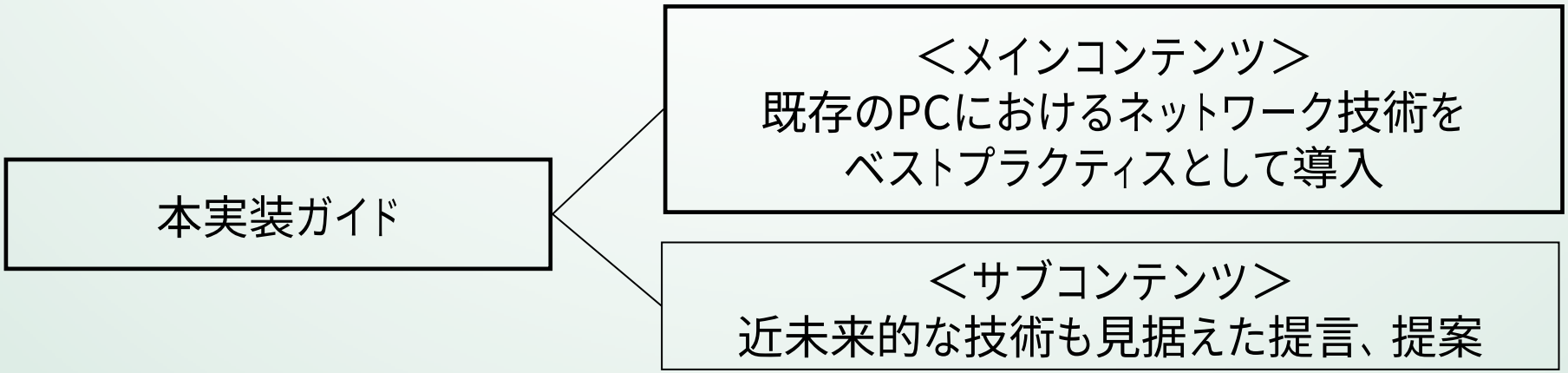
成果物の目次とスケジュール

- 1章：スマートフォンでのセキュリティ対策の考え方
  - 概要、スコープ設定、想定読者
  - 実装ガイド作成方針
- 2章：ネットワーク接続時のセキュリティ脅威と対策要件
  - 想定されるネットワーク構成と接続パターン
  - スマートフォンをネットワーク接続する際の想定脅威
- 3章：ネットワーク接続時に実施すべき技術的対策
  - 利用者認証
  - デバイス認証
- 4章：技術的対策の現状と課題
- 5章：検証報告

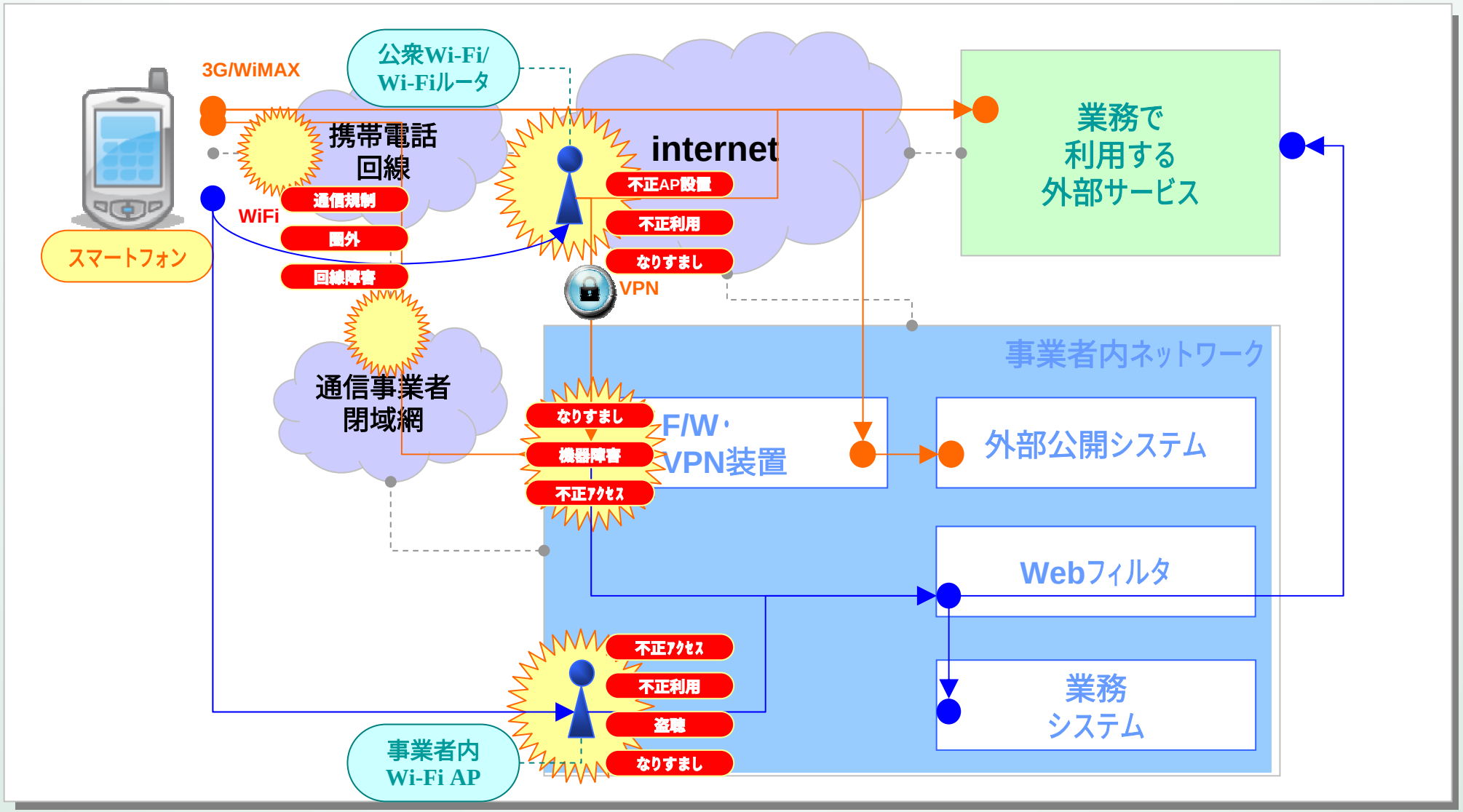
赤字の部分をまとめて12月中にα版を作成予定

【抜粋】実装ガイド作成方針

- 2011年現時点においては、スマートフォンは「性能の劣るPC＋α」である。
- 従って、特にネットワークという、端末の外にあるドメインにおけるセキュリティは、今のPC向けガイドラインをベストプラクティスとして活用することが有効であると考える。ただし、スマートフォンは性能面でPCに劣る点を考慮し、これを補う施策を採り入れる必要がある。
- 今後のスマートフォンの技術発展により、PCとの共通領域が増えるだけではなく、 スマートフォンの特性や独自機能も随時追加されていくと予測する。
- そのような将来像も見据えながら、近未来的な技術の必要性も現状のガイドから盛り込んでおくことは、本ガイドを長期間にわたって活用可能なものとすることを考慮した場合、非常に重要な観点になると考える。



【抜粋】スマートフォンをネットワーク接続する際の想定脅威



【抜粋】脅威と対策のマトリクスと優先度設定

- マトリクスにより整理した優先度に従い、まずは「成りすまし」「盗聴」「不正AP」に関する対策の具体化を実施する。

脅威		対策実施箇所 (A) 事業者内 Wi-Fi AP	(B) VPN	(C) 閉域網	(D) 公衆Wi-Fi /Wi-Fiルータ	実施すべき対策(要件) 技術的対策	備考・その他の対策	優先度 脅威の影響度	対象範囲	対策の実現性	総合		考慮事項
成りすまし	利用者	△	○	-	△	・利用者認証の実施 ・アクセスログ取得	※Wi-Fiでは多段階認証は不可 ※Wi-Fiで利用者認証を実施する場合、無許可デバイス無断接続防止は困難	3	3	3	9	高	・スマートフォンの業務利用を考える上でのベースラインであると考えられる。
	デバイス	△	○	-	△	・デバイス認証の実施 ・アクセスログの取得	※Wi-Fiでは多段階認証は不可 ※Wi-Fiでデバイス認証を実施する場合、アクセス先システムで利用者認証を実施	3	3	3	9	高	
盗聴		○	-	-	○	・通信の暗号化 ・データの暗号化	・重要情報の授受を伴う通信の禁止 └ 用途、アクセス範囲の制限による	3	3	3	9	高	
不正利用	業務外利用	○	-	-	-	・アクセスログの取得 ・業務外通信の制限(Proxy/URLフィルタ等)		2	3	2	7	中	・取り扱うデータの重要度、アクセス範囲等を考慮して実施判断されるべきものと考えられる。
	外部サービス	-	-	-	○	・サービス提供者によるアクセス制限	※ 事業者側でアクセス元IPを限定できることが前提	3	3	2	8	中	
不正アクセス	対 業務システム	○	-	-	-	・業務システムへのアクセス制限(NW/AP分離) ・アクセスログの取得 ・不正アクセス監視		3	3	2	8	中	
	対 ネットワーク機器	-	○	-	○	・機器の脆弱性対策 ・アクセスログの取得 ・不正アクセス監視	・ANY接続の禁止 ・VPN接続時のテザリング ・暗号化強方式の強度をあげる	3	3	2	8	中	
機器障害		-	○	-	-	・機器の冗長化による可用性向上 ・代替アクセス手段の確保 ・機器の稼動監視	・保守サービスへの加入	2	2	2	6	低	・中核業務で利用する場合、考慮する必要あり
通信規制		-	-	○	-		・通信事業者の分散(？) ・複数の通信手段を有するデバイスの選定	2	2	2	6	低	
圏外		-	-	○	-		・デバイスを利用する地域をカバーできる通信事業者を選定	2	2	2	6	低	
通信事業者の回線障害		-	-	○	-		・通信事業者の分散(？) ・複数の通信手段を有するデバイスの選定	2	2	2	6	低	
不正AP設置		-	-	-	○	・通信の暗号化 (組織の管理外のAPを利用する場合)	・重要情報の送受信を行う場合、公衆Wi-Fiの利用禁止	3	3	1	7	高	※ 影響が大きいため対策の検討が急務