スマートフォンネットワークセキュリティ実装ガイド

～スマートフォンの業務利用における安全なネットワーク利用のために～

【第一版】

2012 年 12 月 1 日

日本スマートフォンセキュリティ協会（JSSEC）
技術部会
ネットワークワーキンググループ

文書管理番号 JSSEC-TECN-NW-GD20121201

■制作■

技術部会ネットワークワーキンググループタスクフォース

リーダー	相原弘明	株式会社ネットマークス
メンバー	原田大	NRI セキュアテクノロジーズ株式会社
	山田朋美	NRI セキュアテクノロジーズ株式会社
	清水健	株式会社 EMPRESS SOFTWARE JAPAN
	渡辺龍	KDDI 株式会社
	小熊慶一郎	株式会社 KBIZ
	合田幸司	サイバートラスト株式会社
	谷田部茂	シスコシステムズ合同会社
	山本総夫	ソフトバンク・テクノロジー株式会社
	土屋幸三	ソフトバンク・テクノロジー株式会社
	倉永英久	株式会社大和総研ビジネス・イノベーション
	佐藤導吉	東京システムハウス株式会社
	倉林俊介	トヨタ自動車株式会社
	加治屋繁久	一般社団法人 日本オンラインゲーム協会
	二村廉太	株式会社ネクストジェン
	栃沢直樹	株式会社ネットマークス

（社名五十音順）

文書管理番号 JSSEC-TECN-NW-GD20121201

目 次

1. 実装ガイドの概要 3
1.1. 概要 3
1.2. 想定読者 3

2. 実装ガイドのスコープ 4
2.1. 本ガイドのスコープ 4
2.2. スコープの概念図 5

3. セキュリティ対策の基本的な考え方 6

4. ネットワーク接続時のセキュリティ対策要件 7
4.1. スマートフォンの特性からみたネットワーク接続時のセキュリティ対策 7
4.2. 想定されるネットワーク構成と接続パターン 8
4.3. スマートフォン業務利用時のネットワーク接続パターン 8
4.3.1. パターン１： 携帯電話回線経由、インターネット接続あり 9
4.3.2. パターン２： 携帯電話回線経由、通信事業者閉域網利用 9
4.3.3. パターン３： Wi-Fi 利用 10
4.4. 各接続パターンにおける想定脅威と対策の考え方 10
4.5. スマートフォンをネットワーク接続する際の想定脅威 11
4.6. 接続点別 想定脅威と対策 12
4.7. ネットワークの観点から対処すべき課題 14
4.8. 課題に対する優先度の検討 14
4.9. 課題に対する技術的対策 16

5. 認証 18
5.1. 利用者認証 18
5.1.1. 対策の目的 18
5.1.2. 前提 18
5.1.3. 要件 18
5.1.4. 対策案 18
5.1.5. 対策の実装評価 20
5.2. デバイス認証 24
5.2.1. 対策の目的 24
5.2.2. 前提 24
5.2.3. 要件 24
5.2.4. 対策案 25
5.2.5. 対策の実装評価 26
5.2.6. デバイス認証として電子証明書を使うにあたっての留意点 28

6. アクセスコントロール 30
6.1. 対策の目的 30
6.2. 前提 30
6.3. 要件（対策の方針） 30

6.4. 対策案（対策の手段） 30
6.4.1. アクセスコントロールの方針 30
6.4.2. アクセスコントロールの実装に向けた検討ポイント 33
7. 暗号化 35
7.1. 対策の目的 35
7.2. 前提 35
7.3. 要件 35
7.4. 対策案 35
7.4.1. ファイル暗号化 36
7.4.2. メール暗号化 36
7.4.3. Web サーバ暗号化 36
7.4.4. リモートアクセスにおける暗号化 36
7.4.5. Wi-Fi 環境での暗号化 37
8. 不正 AP 対策 38
8.1. 不正 AP への接続防止 38
8.1.1. 対策の目的 38
8.1.2. 対策の対象 38
8.1.3. 対策案（対策の手段） 38
8.2. 不正 AP の設置防止 39
8.2.1. 対策の目的 39
8.2.2. 対策案 39
9. おわりに 40

1. 実装ガイドの概要

1.1. 概要

タブレット端末を含むスマートフォンの業務利用に際しては、ネットワークを通じて企業や組織（以下、企業と記載）が有する各種の情報システムにアクセスすることが想定されます。スマートフォンをネットワークに接続する方法は複数存在するため、業務要件や用途、想定される脅威への対策などを考慮した上で、最適なネットワークの実装方法を選択する必要があります。

スマートフォンネットワークセキュリティ実装ガイド（以下、本ガイドと記載）は、企業がスマートフォンを業務利用する際に講じるべきネットワークセキュリティ対策の実装方式、及び考慮すべき事項を整理することで、安心してスマートフォンを利用できるネットワークの実現に寄与するものです。

1.2. 想定読者

本ガイドは、主に以下の読者を対象としています。

(1) 企業においてスマートフォンを導入する責任者・企画担当者
(2) 企業においてスマートフォンを導入する際に、ネットワークにおけるセキュリティ対策を策定する責任者・担当者
(3) 企業においてスマートフォンを導入する際に、ネットワークを提案、構築、管理する企業の責任者・担当者

2. 実装ガイドのスコープ

2.1. 本ガイドのスコープ

スマートフォンをとりまくセキュリティ環境には様々な構成要素があり、日本スマートフォンセキュリティ協会（以下、JSSEC と記載）技術部会では、その要素毎のワーキンググループに分かれています。本ガイドは、ネットワークワーキンググループのネットワークタスクフォースにて、スマートフォンがネットワークを介して企業にアクセスする様々な手段におけるセキュリティ上の脅威と、その技術的対策について調査・分析を行い、ガイドラインなどの作成を行なっています。

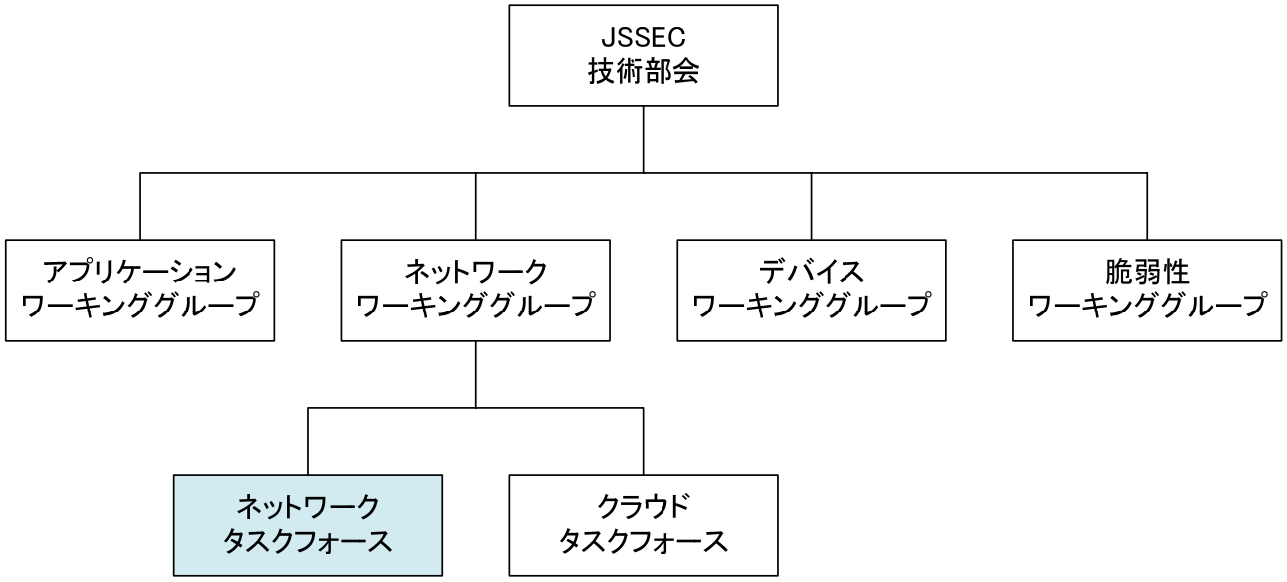

図 2-1　JSSEC 技術部会の組織図と本ガイド執筆組織の位置づけ

2.2. スコープの概念図

スマートフォンのセキュリティ対策は、デバイス、ネットワーク、サービスの観点から網羅的に検討する必要があります。本ガイドが対象とする検討の範囲は、スマートフォンの接続可能なネットワーク、及びその構成要素（ネットワーク関連機器、網／回線）としています。

スマートフォン端末、端末管理サービス、いわゆる MDM（Mobile Device Management）、及びアプリケーションマーケットについては、JSSEC の他のガイドラインで説明していることから、本ガイドの対象には含んでいません。本ガイドのスコープをまとめた概念図を以下に示します。

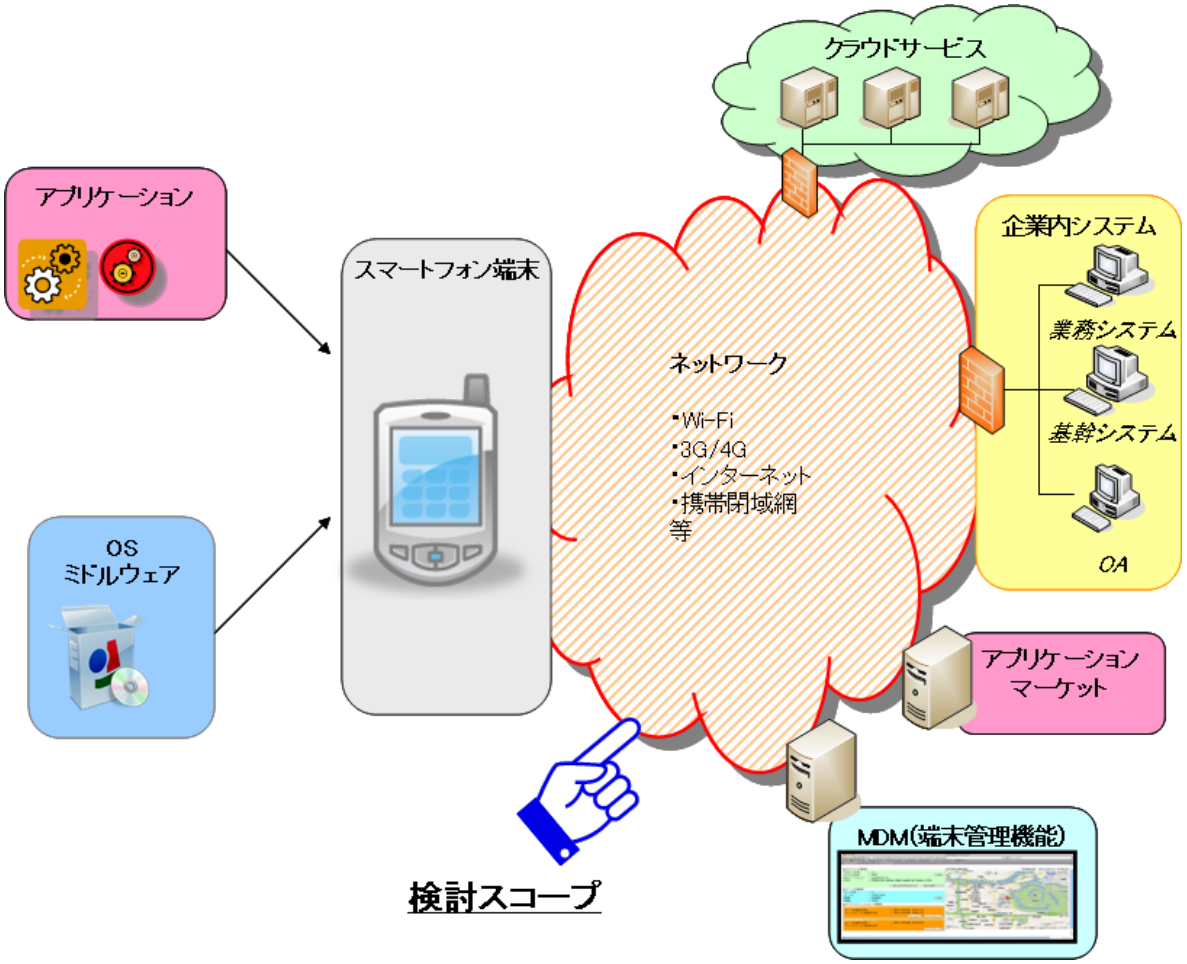

図 2-2　スコープ概念図

3. セキュリティ対策の基本的な考え方

スマートフォンは、現状では性能や機能、業務利用における実績はPCと同じレベルには到達していないものの、ネットワークの利用という観点ではPCに近いと言えます。

このことからセキュリティ面について考察すると、セキュリティ技術や運用ポリシーなど、現状の企業利用においてPCに適用している対策をスマートフォンのセキュリティ管理の基盤として取り入れることが有用であると考えられます。ただし、スマートフォンは、私物デバイスの業務利用（BYOD：Bring Your Own Device）など、PCとの特性の違いから、現状のPCと同様の対策では不十分であるため、スマートフォン特有のセキュリティ対策を見極めることが重要です。

本ガイドでは、既存PCの企業利用におけるネットワーク技術で蓄積されたセキュリティ対策を、いかに適切な形でスマートフォンに適用するかについて考察することを作成方針としています。

4. ネットワーク接続時のセキュリティ対策要件

4.1. スマートフォンの特性からみたネットワーク接続時のセキュリティ対策

スマートフォンの特性からネットワーク接続時のセキュリティ対策を検討する場合、以下の点について考慮する必要があります。

- スマートフォンは、複数のネットワークインターフェースを有しており、通信時には通信の種類（通話/データ通信）や利用環境に応じて最適なインターフェースを利用することができる。
  例：3G/4G, Wi-Fi など
- スマートフォンは、ノート PC などの既存のモバイル機器と比較して携帯性に優れており、いつでもどこでも利用することができる。
  例：自宅, 移動中, 会社の自席, 会議室, 外出先/出張先 など
- スマートフォンは、常時ネットワークに接続されている場合が多く、利用シーンにおいてパブリッククラウドなどの外部サービスの利用頻度が高くなる。
- 企業が保有しているネットワークや利用者が使用するアクセス方式によって、ネットワークへの接続点が変わってくる。
  例：インターネット経由での接続, 通信事業者閉域網経由での接続, Wi-Fi 経由での接続
- デバイスに対する OS やアプリケーションの実装や提供される通信サービスの仕様[1]が統一されておらず、VPN 機能などのネットワークに関するアプリケーションの動作に機種依存が発生している。
- スマートフォンの一部ではテザリング機能[2]を持つものがあり、場所に関係なく Wi-Fi ルータとして利用することができる。
- root 化や Jailbreak[3]されたデバイスをネットワークに接続された場合、実施されたセキュリティ対策が機能しなくなることがある。

上記を考慮した上で、スマートフォンを企業の既存ネットワークに接続する際には、どこに、どのような脅威が発生するのか、既存の脅威にどんな影響が生じるのかを明らかにした上で、必要な対策を洗い出し、実施する必要があります。

本章では、ネットワークの観点から接続パターンを整理することにより、発生しうる脅威、及び対策ポイントを可視化します。

[1] 通信サービスにおいては、利用できるプロトコルの制限などにより VPN などの機能が動作できない場合がある。

[2] スマートフォンの Wi-Fi ルータ機能を利用して、PC などからスマートフォンの携帯電話回線を通じてネットワークに接続する機能。

[3] スマートフォンの管理者権限を取得して、端末製造者の意図とは異なる動作を可能とすること。

4.2. 想定されるネットワーク構成と接続パターン

スマートフォンが有するネットワークインターフェース、アクセス回線網、アクセス先の組み合わせはおおむね以下の通りとなります。これらをもとに、ネットワーク接続パターンを整理します。

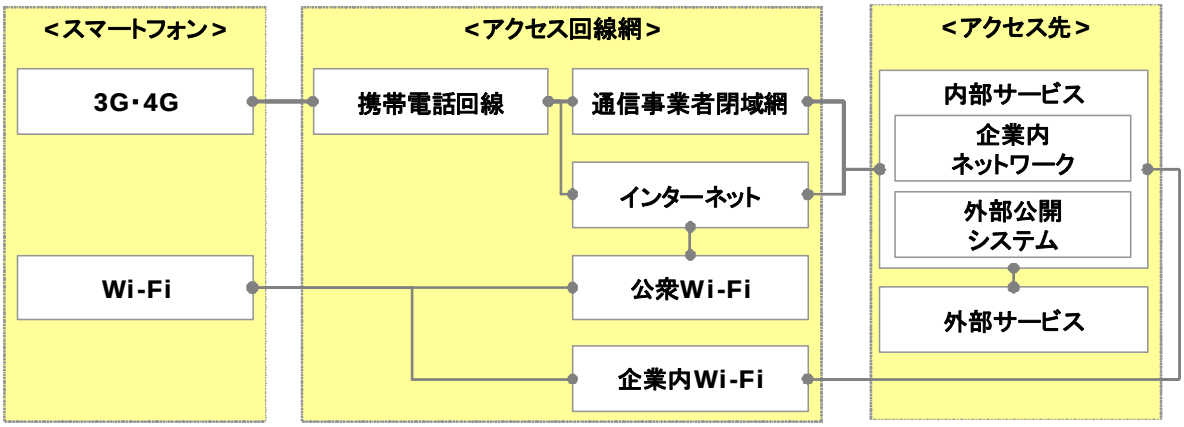

図 4-1 スマートフォンから企業への到達経路

4.3. スマートフォン業務利用時のネットワーク接続パターン

スマートフォンの業務利用時のネットワーク接続パターンを検討するにあたり、以下の内容を利用環境の前提事項とします。

- スマートフォンから利用する情報システムは、企業ホームページなどの「外部公開システム」や「業務システム」といった「内部サービス」、及び「外部サービス」とする。
- 「外部サービス」は、企業のポリシーにより業務利用が許可されたサービスとする（Web アプリケーションを想定）。
- 企業のネットワークを経由してインターネットサービス（Web, Mail など）を利用する場合、フィルタ装置経由とする。
- インターネット経由で内部サービスにアクセスする場合、VPN を利用する。

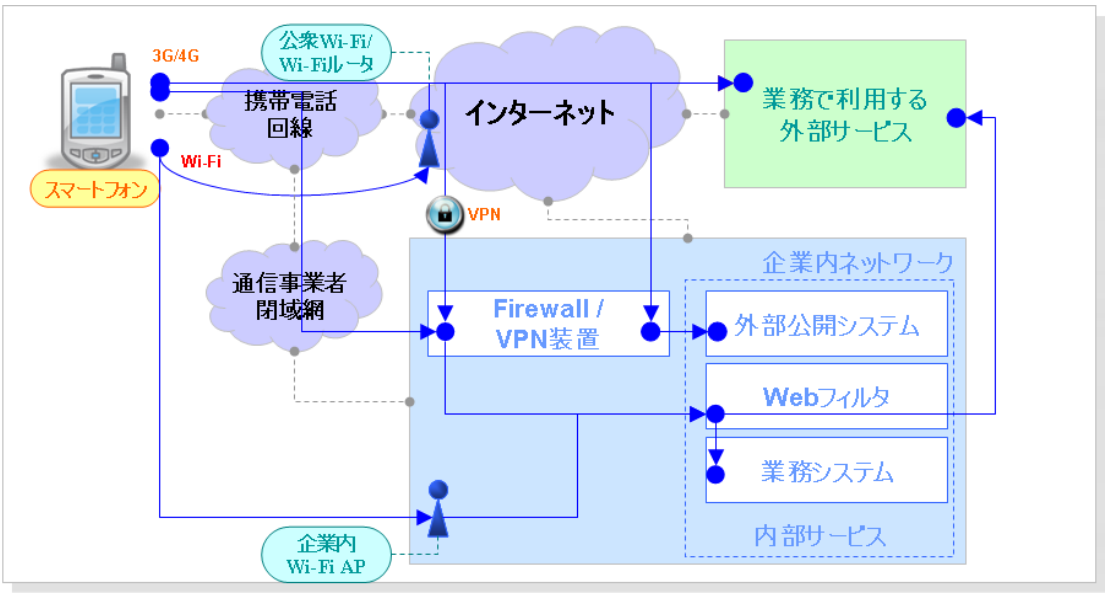

図 4-2　業務利用時の接続パターン

4.3.1. パターン１： 携帯電話回線経由、インターネット接続あり

携帯電話回線（3G/4G など）をアクセス回線として利用し、「内部サービス」及び「外部サービス」へはインターネットを経由してアクセスするパターンです。インターネットと企業内ネットワークとの接続点には境界機器（Firewall）があると想定します。

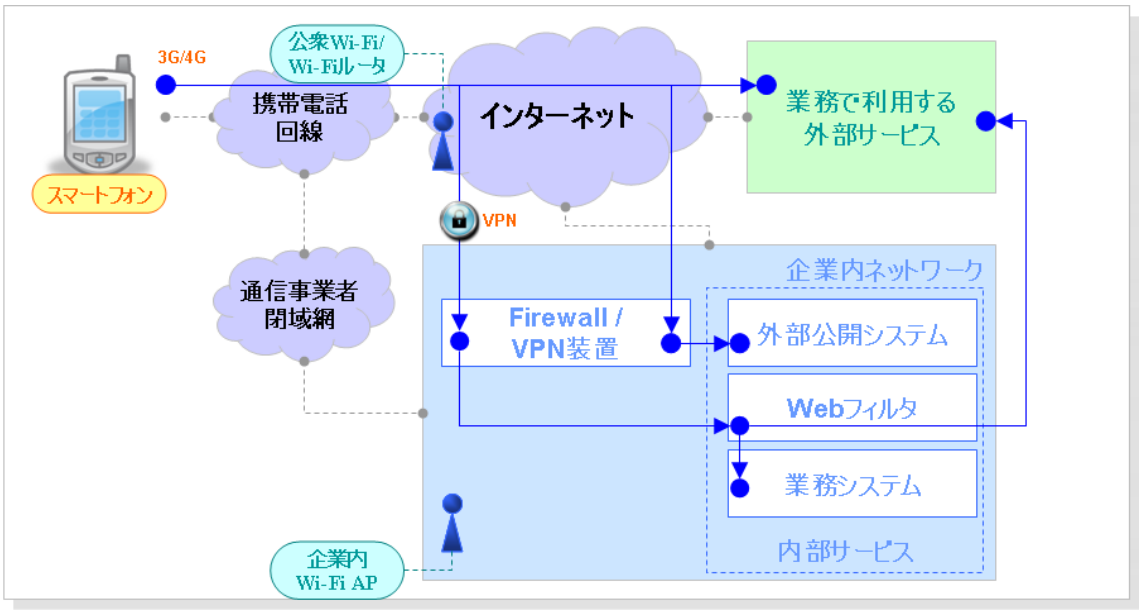

図 4-3　携帯電話回線経由、インターネット接続あり

4.3.2. パターン２： 携帯電話回線経由、通信事業者閉域網利用

企業内ネットワークに接続された通信事業者閉域網をアクセス回線として利用し、「内部サービス」にアクセスするパターンです。「外部サービス」へは内部サービスからインターネットを経由してアクセスします。閉域網接続が可能な Wi-Fi ルータも含み、閉域網と企業内ネットワークとの接続点には境界機器（Firewall）があると想定します。

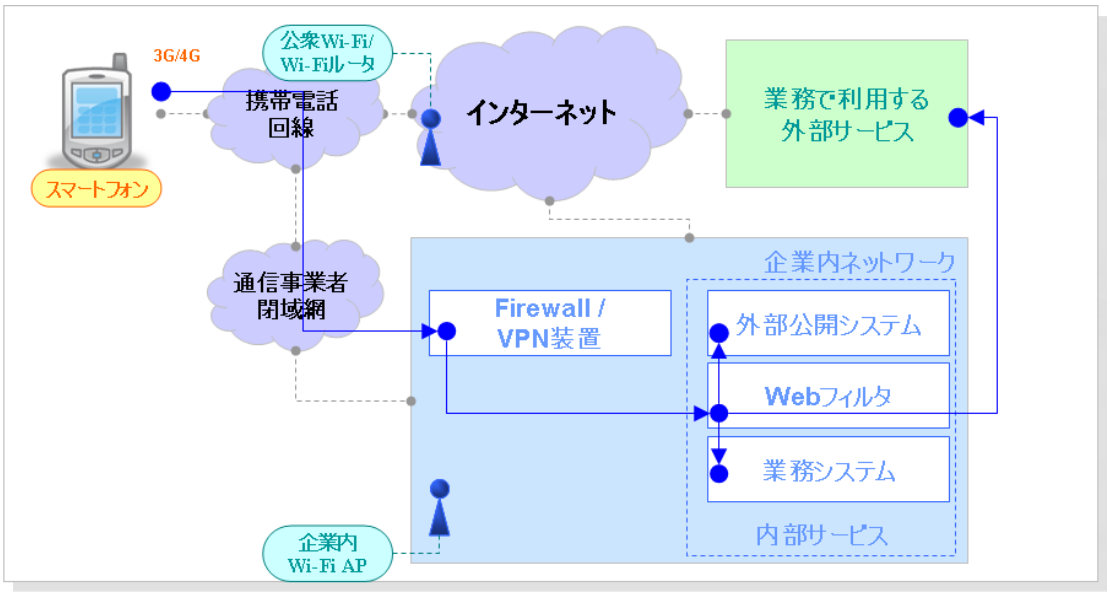

図 4-4　携帯電話回線経由、通信事業者閉域網利用

4.3.3. パターン３： Wi-Fi 利用

企業内 Wi-Fi、公衆 Wi-Fi、Wi-Fi ルータなどをアクセス回線として利用し、「内部サービス」及び「外部サービス」へはインターネットを経由してアクセスするパターンです。携帯電話回線を有する機器については、環境により携帯電話回線、Wi-Fi を使い分けます。一般的なスマートフォン OS の仕様では、Wi-Fi が利用可能な場合には Wi-Fi が優先的に利用され、それ以外の場合には携帯電話回線が利用されています。

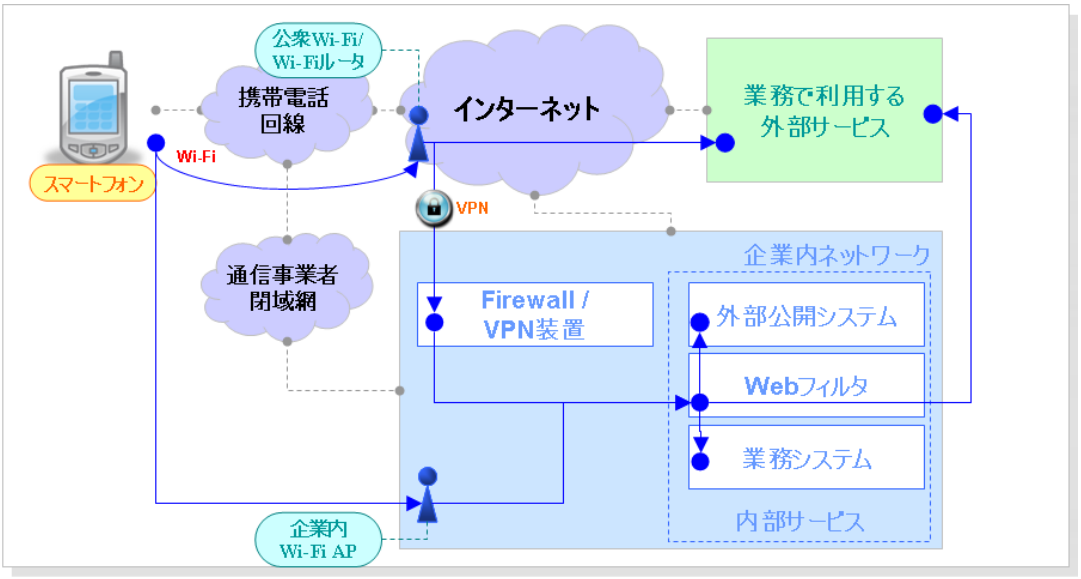

図 4-5　Wi-Fi 利用

4.4. 各接続パターンにおける想定脅威と対策の考え方

各接続パターンにおいて想定される脅威と対策の考え方を以下に示します。

- 利用シーン毎の想定脅威の洗い出しは、JSSEC が公開している「スマートフォン&タブレットの業務利用に関するセキュリティガイドライン」にて整理されている内容のうち、ネットワークに関連するものを引用する。

<引用元> スマートフォン&タブレットの業務利用に関するセキュリティガイドライン
5. 利用シーンから見る脅威と対策 5.6 ネットワークに接続する 5.7 社内ネットワークを利用する 5.8 組織契約の SaaS / ASP サービスを利用する

- 先述の接続パターンにおいて、想定脅威を発生箇所（≒対策実施箇所）に当てはめることで、脅威を可視化する 。
- 対策要件の洗い出し段階においては、対策の実施方法、実現可能性は考慮しない。
- 対策要件の検討に際しては、どのような機器が接続されたとしても安全性が保てるよう考慮する必要がある。このため、スマートフォンそのものの安全性は考慮しない。また、機器の仕様変更の影響がシステム全体の安全性に波及することを防ぐため、接続される機器固有の機能に依存した対策は採用しない。

4.5. スマートフォンをネットワーク接続する際の想定脅威

以上のことから、ネットワーク環境において脅威が存在し、対策を実施する箇所を整理すると以下の通りになります。

(A) 企業内 Wi-Fi との接続点
(B) VPN 接続点（Firewall・VPN 装置）
(C) 携帯電話回線/通信事業者閉域網との接続点
(D) 公衆 Wi-Fi / Wi-Fi ルータとの接続点

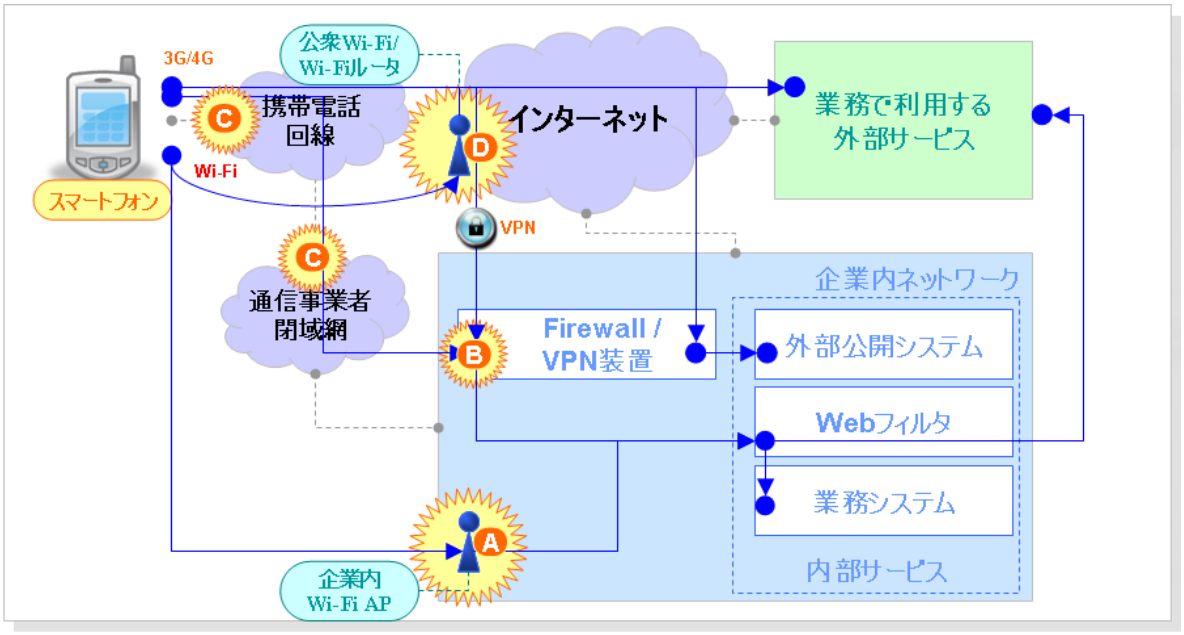

図 4-6　スマートフォンをネットワークに接続する際の想定脅威

4.6. 接続点別 想定脅威と対策

接続点別で考えられる脅威とその対策について、「スマートフォン&タブレットの業務利用に関するセキュリティガイドライン」から抜粋し、その内容を補足します。

表 4-1　接続点別の想定脅威と対策

ID	接続点	脅威	解説(リスク)	対策　または　要件
A	企業内 Wi-Fi AP	なりすまし (利用者)	・権限のない利用者により企業内ネットワークに不正に接続される	・利用者認証の実施[4] - デバイス認証と組み合わせで実施することが望ましい ・アクセスログの取得
		なりすまし （デバイス）	・無許可のデバイスが企業内ネットワークに接続される	・デバイス認証の実施[4] - アクセス先システムなどで利用者認証を実施することが望ましい ・アクセスログの取得
		盗聴	・通信内容を第三者に傍受され、情報が漏洩する	・通信経路の暗号化 ・通信対象データの暗号化 ・重要情報の授受を伴う通信の禁止 - 用途によりアクセス範囲を制限させる
		不正利用	・企業内ネットワークを経由して業務と無関係な通信を行う（業務外利用）	・アクセスログの取得 ・企業内ネットワークにおいて業務外通信を制限（Proxy、URL フィルタなど）
		不正アクセス	・アクセス許可のない/アクセス不要な業務システムにアクセスし、情報を持ち出す	・ネットワークを分離し、ネットワーク間のアクセスを制限 ・アクセスできる業務システムを制限 ・ネットワークの監視 ・アクセスログの取得
		不正 AP 設置	・企業 Wi-Fi を装った偽の AP を利用することにより利用者の情報が漏洩する可能性がある ・無許可の AP が企業内ネットワークに接続される	・企業が管理していないネットワークを利用する場合には通信の暗号化を実施する ・無許可の AP を監視、検出
B	VPN	なりすまし (利用者)	・権限のない利用者が企業内ネットワークに接続する	・利用者認証の実施 ・アクセスログの取得
		なりすまし （デバイス）	・利用者が無許可の機器を企業内ネットワークに接続する	・デバイス認証の実施 ・アクセスログの取得
		機器障害	・ネットワーク機器の障害でサービスが停止する	・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 ・保守サービスへの加入 ・機器の稼動監視
		不正アクセス （脆弱性を利用した攻撃）	・ネットワーク機器の脆弱性を攻撃される	・機器の脆弱性対策の実施 ・アクセスログの取得 ・ネットワークの監視
		不正アクセス （VPN 接続中のテザリング）	・VPN 接続を行うデバイスでテザリング機能を利用され、無許可デバイスがネットワークに接続される	・VPN を利用する機器でのテザリングを禁止

[4] Wi-Fi の場合、デバイスと利用者との両方での多段階認証ができない

ID	接続点	脅威	解説(リスク)	対策　または　要件
C	携帯電話回線 / 通信事業者 閉域網	通信事業者 による 通信規制	・通信事業者により通信規制が行われ、通信しにくくなる	・利用する通信事業者を分散 ・代替通信手段の確保 - 例：3G/4G +公衆 Wi-Fi など
		通信事業者の 回線障害	・通信事業者側の障害により通信ができなくなる	・利用する通信事業者を分散 ・代替通信手段の確保 - 例：3G/4G +公衆 Wi-Fi など
		不正利用	・携帯電話回線を利用して業務と無関係な通信を行う（業務外利用）	・通信事業者が提供するフィルタリングサービスを利用 ※通信事業者のサービスによるフィルタリングサービスについては、企業のポリシーと同一にできない可能性がある
D	公衆 Wi-Fi/ Wi-Fi ルータ	なりすまし （利用者）	・権限のない第三者により、企業が契約している外部サービスを利用される	・外部サービス提供者側で利用者認証を実施 - 企業内の認証システムと連携させるなど ※外部サービス提供者側またはアクセス経路上でデバイス認証を実施 ・アクセスログの取得
		不正利用	・外出先などから企業が契約する外部サービスにアクセスし情報を持ち出す	・外部サービス提供者側でアクセス制限を実施 - アクセス元ネットワークを契約企業のみに限定 ・アクセスログの取得 ※企業側でアクセス元 IP アドレスを絞れることが前提
		不正 AP 設置	・公衆 Wi-Fi を装った偽の AP を利用することにより利用者の情報が漏洩する可能性がある	・企業が管理していないネットワークを利用する場合には通信を暗号化

4.7. ネットワークの観点から対処すべき課題

接続パターン毎に洗い出した想定脅威、対策実施箇所、対策要件を一覧に整理することで、重複を排し、網羅性を確保します。また、情報セキュリティの原則に従い、ある脅威に対して多層的な防御が可能となるよう対策を構成することとします。

表 4-2　接続パターンにおける脅威

脅威		対策実施箇所			
		(A) 企業内 Wi-Fi AP	(B) VPN	(C) 携帯電話回線 閉域網	(D) 公衆Wi-Fi /Wi-Fiルータ
なりすまし	利用者	△	○	－	△
	デバイス	△	○	－	△
盗聴		○	－	－	○
不正利用	業務外利用	○	－	△	－
	外部サービス	－	－	－	○
不正アクセス	対 業務システム	○	○	－	－
	対 ネットワーク機器	－	○	－	○
機器障害		－	○	－	－
通信規制		－	－	○	－
通信事業者の回線障害		－	－	○	－
不正AP設置		－	－	－	○

凡例）○：対策が必要であり対策可能
△：対策が必要であるが対策において一部制限あり
－：対策不要

4.8. 課題に対する優先度の検討

洗い出した対策について、ネットワークの観点から技術的に対処すべきものに焦点を絞って要件を具体化し、対策水準を決定します。

対策水準の決定に際しては、優先度を定めて取り組む必要があります。優先度は、各想定脅威の影響度、対策を実施すべき対象範囲、脅威の発生確率を考慮しなければなりません。JSSEC ネットワークタスクフォースによる、優先度の考え方、及び優先的に対処すべき課題の検討結果を以下に示します。

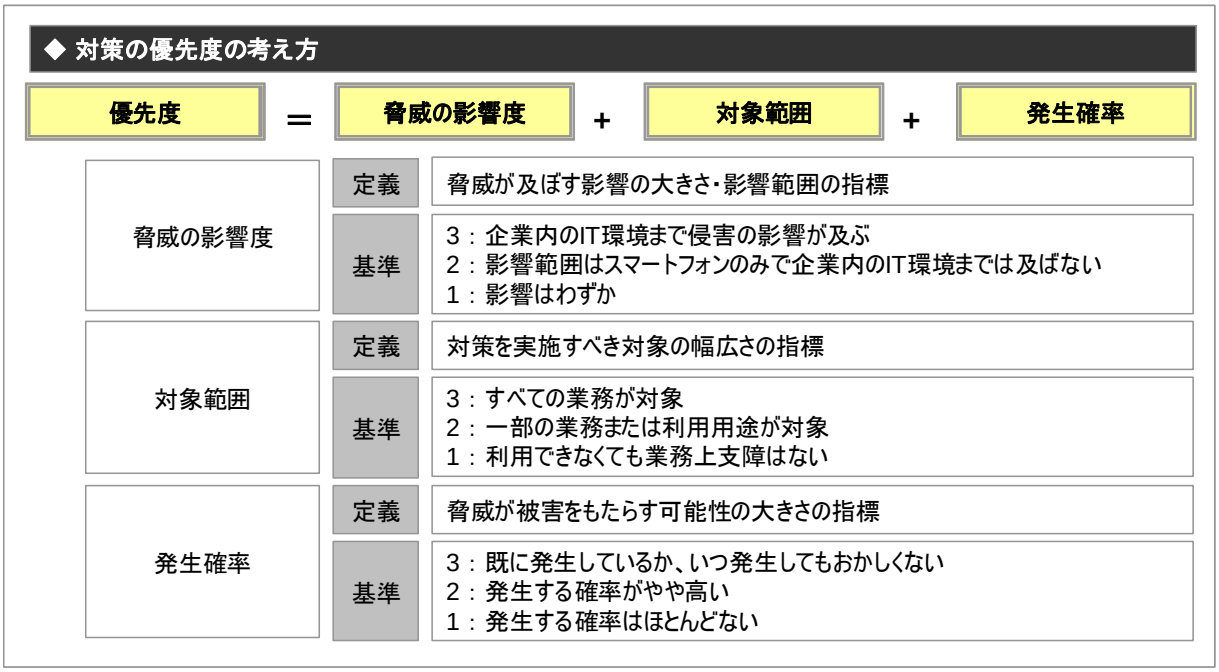

図 4-7　対策の優先度の考え方

表 4-3　対策における総合評価

脅威		優先度				
		脅威の影響度	対象範囲	発生確率	総合	
なりすまし	利用者	3	3	2	8	高
	デバイス	3	3	3	9	高
盗聴		3	3	2	8	高
不正利用	業務外利用	2	3	3	8	高
	外部サービス	3	3	2	8	高
不正アクセス	対 業務システム	3	3	2	8	高
	対 ネットワーク	3	3	2	8	高
機器障害		1	2	2	5	中
通信規制		1	2	2	5	中
通信事業者の回線障害		1	2	3	6	中
不正AP設置		3	3	2	8	高

4.9. 課題に対する技術的対策

ここまでの脅威と対策の検討のうち、優先度の高い以下の 5 項目について技術的な対策を例示し、脅威に対しての対策の関連を表 4-4 に整理します。

(1) なりすまし対策
- 利用者のなりすまし対策として利用者認証を実施する。
- デバイスのなりすまし対策としてデバイスの識別または認証を実施する。
- アクセスした証跡を残すためにアクセスログを取得する。

(2) 盗聴対策
- 通信経路を暗号化する。
- 授受する対象データ自身を暗号化する。

(3) 不正利用対策
- スマートフォンから企業内ネットワークへのアクセス時にアクセス範囲を制限する。
- スマートフォンによる企業内ネットワークを経由した業務外通信を制限する。
- 外部サービスの利用においてスマートフォンからのアクセスを制限する。
- 不正利用の証跡を残すためにアクセスログを取得する。

(4) 不正アクセス対策
- スマートフォンから企業内ネットワークへのアクセス時にアクセス範囲を制限する。
- スマートフォンが接続するネットワークと PC が接続するネットワークとを分離し、スマートフォンからの利用可能なシステムを制限する。
- 企業内システムへのアクセスをプロキシ経由とする。
- 企業内のネットワークを監視する。
- 不正アクセスの証跡を残すためにアクセスログを取得する。

(5) 不正 AP 設置対策
- スマートフォンにおける公衆 Wi-Fi 接続を制限または停止するルールを徹底する。
- 所在が不明な AP への接続を禁止する。
- 公衆 Wi-Fi への接続を制限する場合においては、通信を暗号化するなどの対策について実施する。
- 無許可での企業内ネットワークへの AP 接続を禁止する。
- 企業内のネットワークを監視する。

表 4-5　脅威と対策のマッピング

脅威	対策			
	認証 (利用者及び デバイス)	アクセス コントロール	暗号化	不正AP対策
なりすまし	○			
盗聴			○	
不正利用		○		
不正アクセス		○		
不正AP設置			○	○

次項以降に具体的な対策について記述しますが、ログ及びネットワーク監視については、スマートフォン特有の対策ではないため、具体的な方法については省きます。

5. 認証

5.1. 利用者認証

5.1.1. 対策の目的

企業で認められた利用者であることの証として、利用者認証を実施し、不正な利用者のなりすましによる企業内ネットワークへの不正侵入を防ぐことを目的とします。

基本的な対策は、PC を企業内ネットワークに接続する際に行っている認証方式と同様となりますが、スマートフォンでは携帯性が高いことにより、盗難、紛失の可能性が PC よりも高い点を考慮し、なりすましがされにくい対策を講じる必要があります。

5.1.2. 前提

対策を実施する上で、以下の事項を前提とします。

- ネットワークの接続点（Wi-Fi AP, VPN）において実施する、利用者のなりすまし防止及び検知のための利用者認証について記載する。
- 認証のための識別情報は、アカウント発行時に正当な利用者のみに配布され、利用終了後は遅滞なく停止ないし削除される仕組みがあることを前提とする（不適切なアカウント管理によるリスクは対策検討の対象としない）。
- スマートフォン自体を保護するロック機能は対象としない。
- 運用時の利便性なども考慮する。

5.1.3. 要件

本対策についての要件を以下に記載します。

- 認証により利用者を一意に識別、特定し、認められた利用者以外は企業内ネットワークにアクセスできないこと。
- 利用者の利便性を損なわない方法であること。
- 利用者の識別には独立した 2 つ以上の要素を用いることが望ましい。
- 認証の成功、失敗に関する証跡を取得し、不正利用の検知や、インシデント発生後の追跡が可能となること。

5.1.4. 対策案

利用者の識別または認証の実施方式として以下の方式があります。単独での利用だけでなく、組み合わせて利用することを考慮する必要があります。スマートフォンを導入する企業は、企業規模や利用形態などにより、次章での評価を参考にして対策を講じてください。

(1) 知識による本人確認

記憶などの知識により本人を確認する方法です。パスワードが一般的ですが、漏洩しやすいなどの理由から、一般にパスワードの複雑性、更新頻度などのポリシーは PC と同様にルールを定める必要があります。

さらに、パスワードの利用とともに所有による本人確認などの＋αの要素を盛り込む多要素認証を行うことで認証を強化させることができます。

知識認証に該当する具体的な対策としては以下の方式があります。

・ 固定パスワード

パスワードを記憶することにより、本人を認証する方式。一般的な方式であるが、漏洩しやすいなどの理由から、複雑性や更新頻度などのポリシーを PC と同様にルールを定める必要がある。

・ マトリックス

ワンタイムパスワードの一つで、毎回表示内容が異なるマトリックス表から事前に設定したパターンに従った文字や数字をパスワードとして認証する方法。一般的には PIN と呼ばれる固定パスワードとマトリックスのパターンを記憶しておくことにより、本人を認証する。

・ リスクベース

基本的な動作としては固定パスワードと同様。ただし、アクセス経路やアクセス元が異なるなどの行動パターンを分析して通常と異なる場合はリスクとして判断し、パスワードとは別に本人しか知りえない情報の入力を求めて、本人を認証する。

(2) 所有による本人確認

トークン、メールアドレス、電子証明書などを所有していることで本人を確認する方法です。通常、これらの仕組みでは、盗難や紛失を考慮し、パスワードや PIN などの知識による本人確認と組み合わせて利用されます。

・ トークン

事前に配布したハードウェアやソフトウェアのトークンを所有していることにより本人を認証する方式。トークンには定期的に変化するパスワードが表示され、これによりワンタイムパスワードとなる。通常は紛失や盗難対応のため、表示されたパスワードとは別に PIN と呼ばれる固定パスワードを設定する。多要素認証としてパスワードとトークン（ハードウェア）の二要素を利用する場合、トークンとスマートフォンは物理的に別のものとすることが安全性の面から必要となる。

・ SMTP コールバック

パスワードを電子メールで送付することにより、そのメールアドレスの所有する本人を確認する方法。パスワードは毎回変化させることで、パスワードの使い回しや、盗聴から守ることができる。

・ 電子証明書

電子証明書を所有していることで本人を確認する方法。電子証明書の格納場所として PC やスマートフォンのデバイス内での保管や、スマートカードや NFC を搭載したデバイスへの保管などがある。電子証明書を利用者認証に利用する場合は、秘密鍵の安全管理が必要であることに加え、利用者特定のために利用者と電子証明書の対応関係をネットワーク側で厳密に管理することが必要となる。

(3) 生体による本人確認

利用者自身の生体の特徴により本人を確認する方法です。生体による本人確認方法の主な種類としては指紋、声紋、静脈、顔などがあります。スマートフォンにおいて、これらの認証機能が搭載されているデバイスがほとんどないため、現時点では実用的ではありません。

5.1.5. 対策の実装評価

利用者のなりすまし対策として現時点で考えられる認証方式に対して、利用者の利便性や管理者の運用負荷など、企業利用における検討のポイントについて以下に分析します。なお、以下の比較表に関しては、各認証方式の比較においての相対的評価であり、実際に導入する際の環境、導入製品・サービスにより変動するものと考えられます。レーダーチャートは、システム選定を行う上で「認証強度」、「利便性」、「コスト」、「運用性」の重要度のバランスを分かりやすく明示するためのものであり、必要に応じて複数の対策を組み合わせるなどの選択の一助となることを目的としたものです。

[検討ポイントの定義]

- 認証強度
  当該方式に対する認証強度、なりすましに対する耐性の高さを評価
- 利用者利便性
  当該方式の利用者が、認証時にどの程度容易・スムーズに認証を行えるかを評価
- 初期導入コスト
  企業が当該方式を導入する場合のハードウェア・ソフトウェア・サービスの初期導入費用、及び IT 管理者の導入時稼動コストがどの程度かるかを評価
- 管理運用コスト
  企業が当該方式を導入後、ハードウェア・ソフトウェア・サービスのライセンス・保守サポート費用、及び IT 管理者の運用管理コストがどの程度かるかを評価
- 管理者運用性
  企業が当該方式を導入した場合の IT 管理者の運用管理の煩雑さ、維持するべき管理体制、インシデント発生時の対応などを評価

表 5-1　利用者認証の比較

認証方式		固定パスワード	マトリックス	リスクベース	トークン	SMTPコールバック	電子証明書	生体
認証要素	知識	○	○×2	○	○			
	所有				○	○	○	
	生体							○
強度		定期的な変更等のポリシーに従わない場合は脆弱となる	PIN（固定パスワード）と組み合わせた2要素認証であり、ワンタイムパスワードであることからパスワードの盗聴に強いが、マトリクスイメージを他人に知られないような留意が必要	固定パスワードとともに、リスクを判断し追加認証を行うため、強度は固定パスワードよりも高い	トークンの所有とPIN（固定パスワード）と組み合わせた2要素認証であり、ワンタイムパスワードであることからパスワードの盗聴に強い	メールによりワンタイムパスワードを受け取るため、メールアドレスの所有による認証とともに盗聴にも強い	第三者（パブリック）または管理者（プライベート）にて発行する証明書・秘密鍵で管理を行うため強度は高い	個人の身体的特徴を利用するため高い
		1	2	2	3	2	3	3
利用者 利便性		利便性は高いが、定期的な変更などの徹底が必要	マトリックスとPINを覚えればよく、使い勝手は良い	基本的な操作は固定パスワードと同じで利便性は高い	トークンの持ち歩きが必要	携帯電話の利用により利便性は向上する	証明書の保管場所に依存する為、スマートカードやUSBキーと併用が望ましい	パスワードを覚える必要もなく、利便性は高いが、読取装置によっては持ち歩きが必要となる
		3	2	3	1	2	2	2
初期導入コスト		最も安価に実現可能	専用認証システムのライセンスが必要	専用認証システムのライセンスが必要	専用認証システムのライセンスが必要であり、ユーザに配布するトークンも必要	専用認証システムのライセンスが必要	CA局の構築または証明書サービスの導入が必要	専用認証システムのハードウェアまたはソフトウェアの費用が必要
		3	2	2	1	2	2	1
管理運用コスト		システム的な運用コストは通常の認証サーバの管理のみであるが、パスワード忘れ対策の運用体制または仕組みの費用が必要	ユーザライセンス型製品の場合、それに応じたライセンス保守費用が必要	ユーザライセンス型製品の場合、それに応じたライセンス保守費用が必要	ユーザライセンス型製品の場合、それに応じたライセンス保守費用が必要	ユーザライセンス型製品の場合、それに応じたライセンス保守費用が必要	利用者数に応じたライセンスまたはサービスの費用が発生し、証明書の発行・失効・再発行及びそれに伴う配布などの人件費が必要	ユーザライセンス型製品の場合、それに応じたライセンス保守費用が必要
		3	2	2	2	2	2	2
管理者 運用性		パスワード忘れなどの対応が必要となるが、そのほかの管理は容易	マトリクス忘れ対応が必要であるが、セルフサービスでの対応が可能な製品であれば運用は容易	パスワード忘れ対応が必要	パスワード忘れなどの対応の他、トークンの破損、紛失時対応が必要となる	メールの送受信環境が必要	有効期限があり、失効リストの管理やカードの場合紛失や忘れ対応が必要	本人による初期登録が必要
		3	3	3	1	1	1	2
留意点		パスワードポリシーの実装及び徹底が必要	利用可能なシステム（JAVA等の制限からくる）に制限がある	利用範囲広い	同じデバイスでの利用（ソフトウェアトークンをスマートデバイス自体に導入している場合など）では2要素にならない。	震災時等の一時的な利用も可能であり、これからの市場	証明書の発行、更新、失効などの運用面を考慮する必要がある	認識率（本人拒否、他人受入）の確認が必要であり、高度な個人情報になるため、情報の登録方法や運用性でも留意が必要となる

凡例）　1：標準　2:：やや優れる　3：優れる

(1) 知識による本人確認での評価

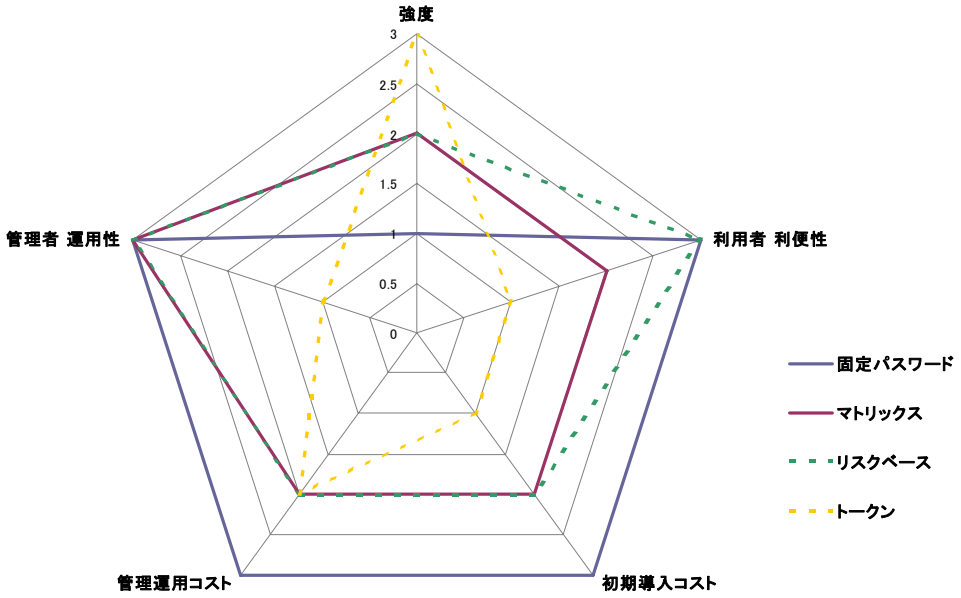

図 5-1　知識による本人確認での評価

(2) 所有による本人確認での評価

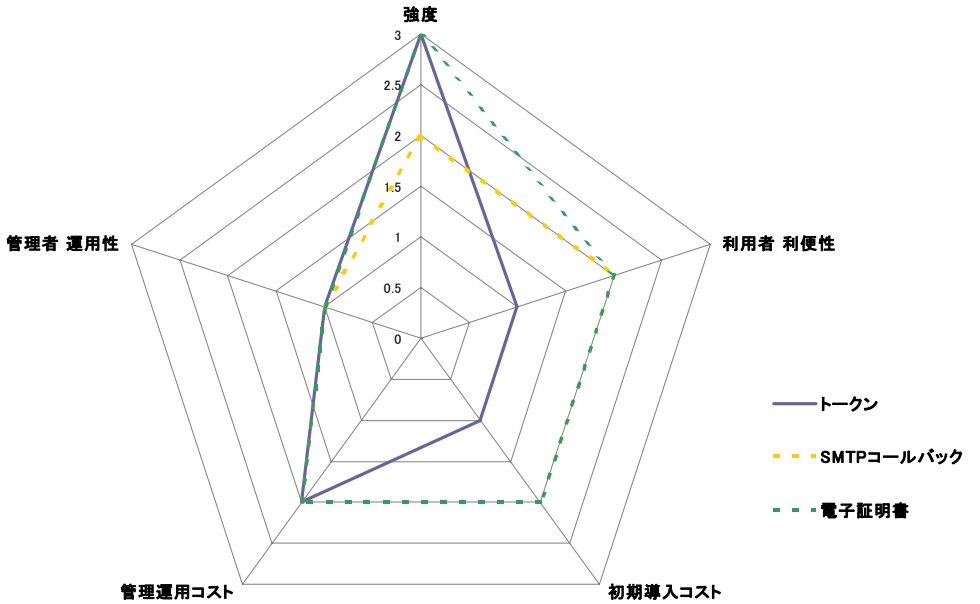

図 5-2　所有による本人確認での評価

(3) 生体による本人確認での評価

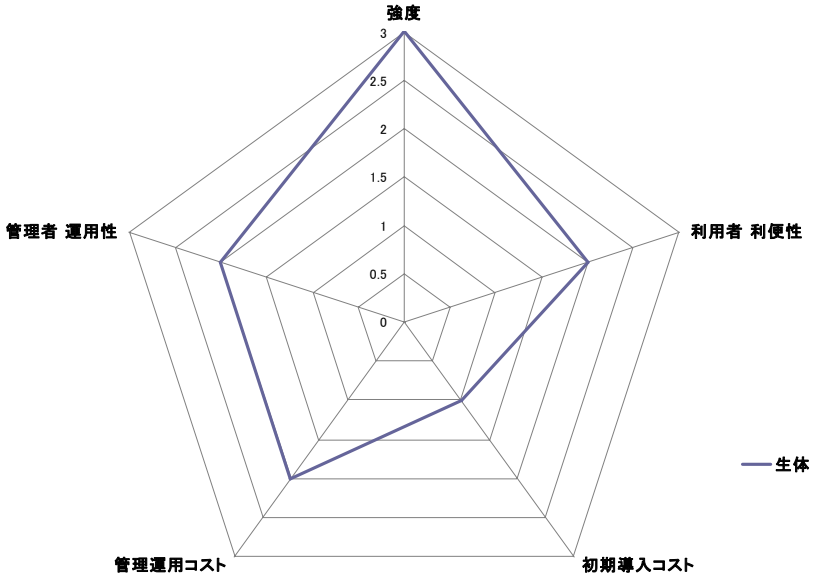

図 5-3　生体による本人確認での評価

5.2. デバイス認証

5.2.1. 対策の目的

企業で認められたスマートフォンであることの証として、デバイスの識別または認証（以下、本ガイドではデバイス認証と記載）を実施し、個人が所有するスマートフォンやなりすましによる企業内ネットワークへの不正侵入を防ぐことを目的とします。

スマートフォンは、PC と比較して携帯性が高く、企業内への持ち込み制限が困難となります。また、ネットワークへの常時接続性、記憶媒体としての特性を有していることから、企業外への情報の持ち出し管理も困難です。それゆえ、企業が承認したデバイスかどうかを判断することが重要となります。

5.2.2. 前提

対策を実施する上で、以下の事項を前提とします。

- ネットワークの接続点（Wi-Fi AP, VPN）において実施する、デバイスのなりすまし防止及び検知のためのデバイス認証について記載する。
- PC とスマートフォンでは、セキュリティ対策のレベルが異なる。
- 企業においては、認められたデバイスのみ接続可能とする。
- デバイスについては、機種変更、破損、水没、紛失なども考慮する。
- 通信手段として携帯電話回線と Wi-Fi の両方を考慮する。
- 運用時の利便性なども考慮する。

5.2.3. 要件

本対策についての要件を以下に記載します。

- 認証によりデバイスを一意に識別、特定し、認められたデバイス以外は接続できないこと。
- 利用者の利便性を損なわない方法であること。
- デバイスの紛失、交換などの運用を考慮すること。認証の成功、失敗に関する証跡の取得し、不正利用の検知や、インシデント発生後の追跡が可能となること。

5.2.4. 対策案

デバイス認証の実施方式として以下の方式があります。単体での利用だけでなく、組み合わせて利用することも考慮する必要があります。スマートフォンを導入する企業は、企業規模や利用形態などにより、次章での評価を参考にして対策を講じてください。

(1) 設定情報（プロファイル情報）

デバイスのプロファイルなどの設定情報と、企業側で設定した情報が合致しているかを確認することで、デバイス認証として代用する手法です。ただし、この対策を採用する場合、一般利用者レベルで設定できる情報は容易に変更できてしまうため、その設定情報が利用者を含め、外部に漏えい及び変更できないようにする対策が必要になります。

例えば、デバイスの Wi-Fi 接続設定を管理者のみが実施し、パスワードを利用者に知らせないことで利用者が意図的にその設定の変更や他への転用を行うことを防ぐことができます。

(2) 電子証明書

デバイスに予め電子証明書と呼ばれる、デバイスを一意に識別するための特殊な形式のファイルを埋め込むことによりデバイスを認証する手法です。

これまで電子証明書は、運用の複雑さやコストの面から、限定的な利用に留まっていましたが、昨今では特にスマートフォンでの利用に最適化され、コスト的にも以前と比べ少ない負担で利用できる状況になっています。また、VPN や Wi-Fi などの様々なネットワーク環境において標準的に利用できるため、非常に利便性が高まっています。デバイスの紛失や、設定情報の外部への流出などが発生した場合においても、デバイスに割り当てた電子証明書のみを失効することが可能なため、個別のデバイスの企業内ネットワークへの接続を制御することが可能です。本手法は他と比べセキュリティ強度が高く推奨できるため、第 5.2.6 章で留意点を記載します。

(3) MAC アドレス

Wi-Fi 接続時のみ有効な、ネットワークインターフェースを識別する固有の値を用いてデバイスを識別する手法です。ただし、MAC アドレスは詐称が容易であるため、単独で利用することは推奨しません。

(4) デバイス固有識別情報

OS が生成する ID、デバイスを識別する ID、電話番号、アプリケーションが独自に発行する ID などを用いてデバイスを識別する手法です。SIM の有無、デバイスの種類、OS の種類によって利用できる情報が異なります。ただし、詐称や偽装の可能性及びこれらの情報の抜き取りなどを考慮し、デバイス固有識別情報の単独での利用は推奨しません。また、SIM に基づいた固有識別情報を利用する場合は、SIM の差し替えが可能なため、なりすましが容易になることに留意する必要があります。このため、将来的には TPM（Trusted Platform Module）のような、デバイスに搭載されたセキュリティチップを活用したデバイス認証を行うことも考えられます。

5.2.5. 対策の実装評価

デバイスのなりすましに対する、現時点で考えられる認証方式について、利用者の利便性や管理者の運用負荷など、企業利用における検討のポイントについて以下に分析します。

なお、以下の比較表に関しては、各認証方式の比較においての相対的評価であり、実際に導入する際の環境、導入製品・サービスにより変動するものと考えられます。レーダーチャートは、システム選定を行う上で「認証強度」、「利便性」、「コスト」、「運用性」の重要度のバランスを分かりやすく明示するためのものであり、必要に応じて複数の対策を組み合わせるなどの選択の一助となることを目的としたものです。

[検討ポイントの定義]

- 認証強度
  当該方式に対する認証強度、なりすましに対する耐性の高さを評価
- 利用者利便性
  当該方式の利用者が、認証時にどの程度容易・スムーズに認証を行えるかを評価
- 初期導入コスト
  企業が当該方式を導入する場合のハードウェア、ソフトウェア、サービスの初期導入費用、及び IT 管理者の導入時稼動コストがどの程度かかるかを評価
- 管理運用コスト
  企業が当該方式を導入後、ハードウェア、ソフトウェア、サービスのライセンス、保守サポート費用、及び IT 管理者の運用管理コストがどの程度かるかを評価
- 管理者運用性
  企業が当該方式を導入した場合の IT 管理者にとっての運用管理の煩雑さ、維持するべき管理体制、インシデント発生時の対応などを評価

また、デバイスが root 化や Jailbreak により管理者権限を奪取されている場合は、セキュリティ強度が下表の通りとならないことに留意ください。

表 5-2　デバイス認証の比較

認証方式	設定情報 （プロファイル情報）	電子証明書	MACアドレス	端末固有識別情報
強度	設定内容を知っていれば複製・再設定することが可能なため、強度は低い	第三者（パブリック）または管理者（プライベート）にて発行する証明書・秘密鍵で管理を行うため強度は高い root化により秘密鍵のExportなどがさらに容易になる可能性があり、強度は低下	MACアドレスの詐称が容易であり、強度は低い	詐称の可能性があり、強度は低い
	1	3	1	1
利用者 利便性	端末に一度設定してしまえば、アクセス毎に認証パスワードなどを入力する必要はない	端末に一度設定してしまえば、アクセス毎に認証パスワードなどを入力する必要はない	アクセス前に管理者にMACアドレスを申請するのみ	アクセス前に管理者に情報を申請するのみ
	3	3	3	3
初期導入コスト	HW/SWの投資がなく、初期導入コストは安価	パブリックCA・プライベートCAともに証明機関に関する投資・導入コストが掛かる	認証デバイス側に情報を登録するのみ	認証デバイス側に情報を登録するのみ（現状VPN・無線APでは端末固有識別情報を認証のトリガーにするシステムはない）
	3	2	2	2
管理運用コスト	設定の管理のみでコストは掛からないが、設定情報を更新する可能性があるため、運用コストがかかる可能性がある	ユーザ数に応じたライセンス（またはサービス）費用が発生する。 証明書の発行・失効・再発行及びそれに伴う配布などの管理者の稼動が掛かる	MACアドレスをゲートウェイ機器に設定・管理する管理者工数が必要	端末固有識別情報をゲートウェイ機器に設定・管理する管理者工数が必要
	2	1	2	2
管理者 運用性	設定プロファイルの管理のみで運用性は高いが、設定変更の可能性もある	証明書の有効期限、失効の管理が必要となるが、それを徹底することにより紛失時の端末のアクセスロックなどに有用	機器交換時などに登録変更が必要	機器交換時などに登録変更が必要
	2	2	2	2
留意点	偽装が容易なため、厳密な端末認証とはいえないことを認識しておく必要あり。他のデバイス認証の仕組みと組み合わせて使うことを推奨	失効や有効期限の管理が必要 秘密鍵がコピーされないよう、管理者はデバイス内での格納状況を把握しておく必要がある。	携帯電話回線(3G回線など)での利用は不可	偽装が可能 機器変更時に登録変更など留意が必要。

凡例）　1：標準　2:：やや優れる　3：優れる

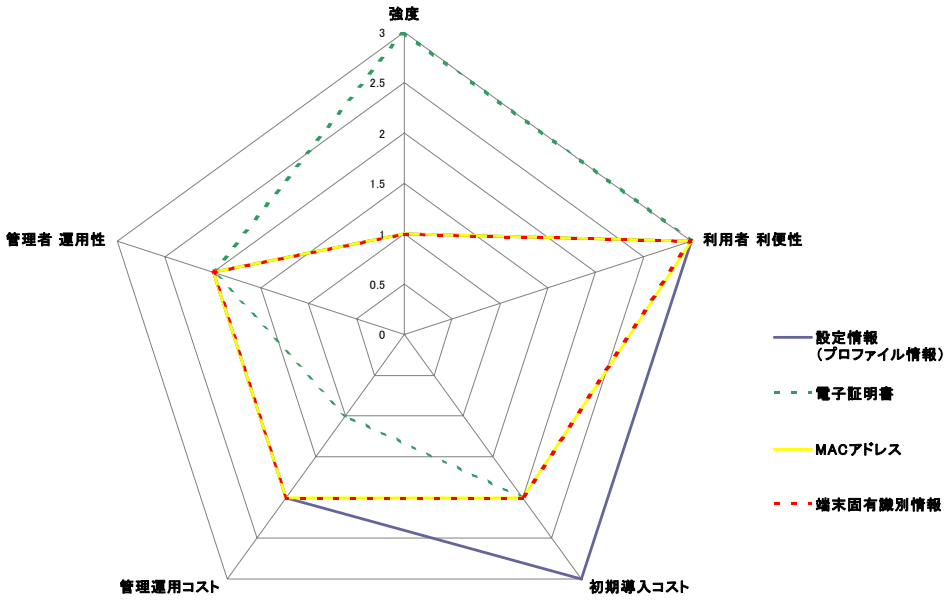

図 5-4　デバイス認証の比較

5.2.6.　デバイス認証として電子証明書を使うにあたっての留意点

電子証明書を利用するなりすまし対策として、デバイス認証と利用者認証の 2 種類がありますが、本章ではデバイス認証に電子証明書を利用する場合の留意点を記載します。

(1) 証明書発行・配付・登録

デバイスのなりすまし対策として最も重要な点が、証明書の発行及び対象のデバイスへの安全な配付と登録作業となります。利用者認証の場合、PKCS#12（秘密鍵と電子証明書を格納したファイル形式の規格）ファイルをデバイスにコピーして登録することが可能ですが、デバイスのなりすまし対策にはなりません。利用者が直接電子証明書に触れることやデバイスに PKCS#12 ファイルが残ってしまう可能性があり、電子証明書が外部に流出するリスクがあるからです。

従って、OS が有するデバイス認証と証明書登録機能の利用や、専用のアプリケーションなどと連携してデバイスに直接電子証明書を登録できる仕組みが必要となります。

※ 登録される電子証明書の格納場所に関しては注意が必要である。本ガイドでは、格納された電子証明書から自由に電子証明書（秘密鍵を含む）を取り出せないことを前提としている。

(2) 更新

スマートフォンに関しては、PC などよりも電子証明書の更新についてライフサイクルを考慮した方法を検討する必要があります。デバイスのライフサイクルと電子証明書の有効期間により、電子証明書の更新は以下の 2 つに大別されます。

ケース 1： デバイスのライフサイクルよりも短い有効期間で電子証明書を更新する。
ケース 2： デバイスのライフサイクルよりも長い有効期間の電子証明書を使うことでデバイスの変更時に電子証明書を更新する。

基本的にスマートフォンは可搬性に優れる一方、破損するリスクや OS のバージョンアップの頻度が高く、PC と比べても比較的ライフサイクルが短いといえます。このため、ケース 2 のようにデバイスの利用期間よりも長い有効期間を持つ電子証明書を登録することによって、電子証明書の「更新」を行わずに運用することが考えられます。

ただし、ケース 1 のように、電子証明書の有効期間よりも長くデバイスを利用する場合、「更新」について考慮が必要です。更新する場合も、「証明書発行・配付・登録」で記載した内容と同様の仕組み（再発行でも可）を有し、配付及び登録の際にはデバイスの認証の仕組みが必要となります。

(3) 再発行

デバイスの初期化や利用者の操作による証明書の削除、デバイスの紛失による証明書の失効など、デバイス側に割り当てられた証明書が利用できなくなった場合に再発行を行います。通常は、新規発行と同様の手順を行いますが、証明書を発行する際には再発行であることの確認作業を含めた運用手順を作成する必要があります。

(4) 失効

電子証明書を利用する最大のメリットは、失効の容易さにあります。他の方式では、不正なデバイスだと判断されても他のデバイスに影響を与えないように該当するデバイスのみを排除することは困難です。しかし、電子証明書では認証局から発行される失効リスト（CRL ：Certificate Revocation List）を確認することで、対象のデバイスのみを企業内ネットワークへ接続することを拒否することができます。

電子証明書を利用する上では、認証局側で対象のデバイスを確認でき失効できることが必要です。また、ネットワーク接続を許可するネットワーク機器側にも失効情報（CRL）の確認ができることが重要な要素となります。

6. アクセスコントロール

6.1. 対策の目的

利用者認証やデバイス認証と組み合わせて適切にアクセス可能な範囲を制御し、管理することにより、意図しない利用者またはデバイスによる企業内ネットワークへの不正なアクセスを防ぐことを目的とします。これにより、情報資産の不正利用を防止することにもつながります。

一般的に、アクセスコントロールはアクセス先のネットワークシステム側で制御しますが、現段階では、スマートフォンに対するセキュリティ対策や企業利用におけるデバイスの管理手法が成熟していません。従って、スマートフォンに対して無条件に PC と同様のアクセス権限を与えることは、企業が定めるセキュリティポリシーに適合しない可能性があります。

このような背景からスマートフォンに対するアクセスコントロールは、従来の PC とは異なる考え方で検討する必要があります。

6.2. 前提

対策を実施する上では、以下の事項を前提として考える必要があります。

- 企業のセキュリティポリシーの中で、スマートフォンの位置付けを明確にして、運用ルールを策定した上でアクセスコントロールの設計を行うことが重要である。
- スマートフォンで利用する企業の内部サービスに存在する個々の情報リソースが、従来 PC で利用している全てのリソースなのか、一部なのかによってアクセスコントロールの重要性が異なる。
- デバイスの通信手段として携帯電話回線と Wi-Fi の両方を考慮する必要があり、それに応じた企業内接続方式とアクセスコントロールの方針を決定する必要がある。

6.3. 要件（対策の方針）

本対策についての要件を以下に記載します。

- 予め定められた経路以外から企業内ネットワークに接続できないようにすること。
- スマートフォンでアクセスできる情報リソースを認証結果に応じて適切に制御できること。また、業務上必要な最低限の情報リソースにのみアクセスを許可することが推奨される。

6.4. 対策案（対策の手段）

スマートフォンを企業内ネットワークに接続する際には、利用者やデバイスを識別して、アクセスする情報リソースの機密レベルに応じたアクセスコントロールを行うことが重要です。企業内ネットワークへのアクセスコントロールの考え方としては以下の方針が考えられます。

(1) 企業内の全ネットワークへのアクセス許可（認証後にアクセスできる情報リソースを制御しない）
(2) スマートフォンの接続可能なネットワークの分離
(3) デバイス認証結果に応じた接続可能なネットワークの制御

6.4.1. アクセスコントロールの方針

(1) 企業内の全ネットワークへのアクセス許可（認証後にアクセスできる情報リソースを制御しない）

現状の企業内アクセス環境を大きく変更することなく、利用者認証だけを行い、スマートフォンには PC と同様のアクセス範囲を提供する場合に採用します。

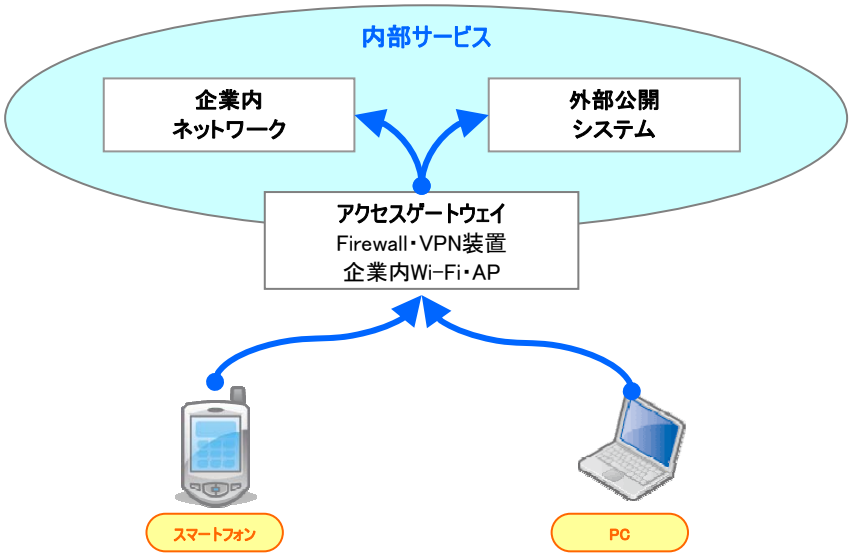

図 6-1　全ネットワークへのアクセス許可構成

(2) スマートフォンの接続可能なネットワークの分離

現状の企業へのアクセス環境を大きく変更することなく、スマートフォンと PC のアクセス範囲を異なるポリシーで制御したい場合に採用することが可能です。スマートフォンアクセス用ネットワークを新設し、スマートフォンはこのネットワークを経由して内部サービスにアクセスを行います。境界 Firewall では、スマートフォンアクセス用ネットワークから特定の情報リソースに対してのみアクセスを許可する Firewall ポリシーを策定する必要があります。また、あわせてスマートフォンから直接内部サービスにアクセスできない仕組みを検討する必要があります。

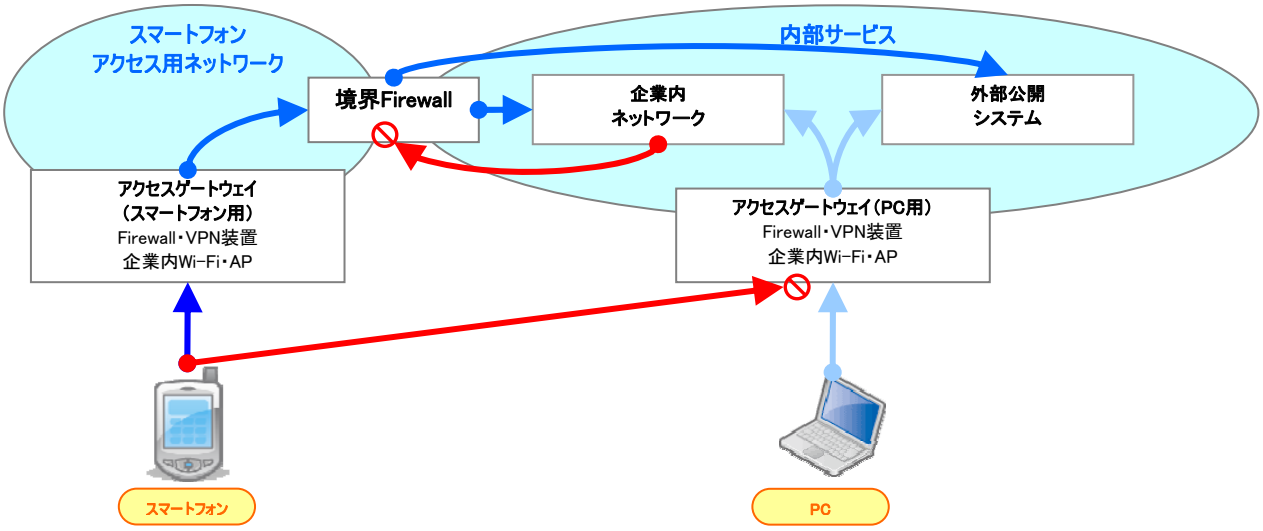

図 6-2　スマートフォンの接続可能なネットワークの分離構成

(3) デバイス認証結果に応じた接続可能なネットワークの制御

スマートフォンと PC のアクセスゲートウェイを統一し、アクセス認証時にデバイスの属性に応じたアクセス範囲の制御を行う場合に採用します。

アクセスゲートウェイを統合することでコスト・運用面の負荷を軽減し、利用者とデバイスの認証属性に応じたきめ細やかなアクセスコントロールが可能となります。

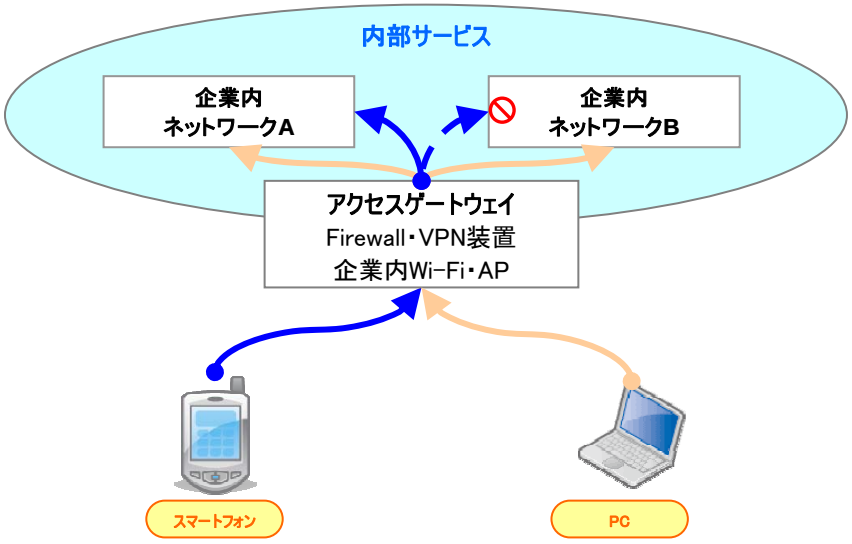

図 6-3　デバイス認証結果に応じた接続可能なネットワークの制御構成

6.4.2. アクセスコントロールの実装に向けた検討ポイント

検討の結果、アクセスコントロールを行う方針とした場合には、認証結果に応じたアクセスコントロールをどのように実装するかを決定する必要があります。一般的な検討のポイントを以下に記載します。

(1) アクセスコントロールの方針決定

利用者･デバイス認証後にスマートフォンがアクセスできる情報リソースの範囲を決定する必要があります。アクセスさせる情報リソースが企業内にどのように点在しているかに応じて、採用できるアクセスコントロールの方針も異なります。一般的な方式を以下に記載します。

表 6-1　アクセスコントロールの方針

アクセス コントロールの方針	アクセス コントロール方式	採用のポイント
企業内の全ネットワークへのアクセス許可	スマートフォンには PC と同様のアクセス範囲を提供する	＜利点＞ ・新たな実装を行うことなく実現できる ＜考慮点＞ ・PC とスマートフォンとのアクセス先を区別することができない
スマートフォンの接続可能なネットワークの分割	スマートフォンアクセス用のセグメントを作成し、Firewall により内部ネットワークへのアクセス範囲を制御する	＜利点＞ ・スマートフォンのアクセスできるネットワークを企業内ネットワークと分割することで比較的容易にアクセスコントロールが可能である ・BYOD 採用時には有効な手段の一つである ＜考慮点＞ ・アクセスゲートウェイを別に用意する必要がある ・スマートフォンが内部ネットワークに直接アクセスできない仕組みを考慮する必要がある
認証結果に応じた接続可能なネットワークの制御	アクセスゲートウェイにて認証結果に応じたアクセス制御を実施する	＜利点＞ ・VPN、Wi-Fi アクセスポイント、リバースプロキシなどでの認証結果に応じて、利用者やデバイス毎のアクセスコントロールが可能 ・BYOD 採用時には有効な手段の一つである ＜考慮点＞ ・アクセス元となる利用者やデバイスとアクセス先となる内部サービスとを紐付けた複雑な制御を行う場合には、より綿密なアクセスルール設計が必要となるため、アクセスゲートウェイ機器の機能を予め確認しておく必要がある

(2) 企業内への接続方式の決定

アクセスコントロールに関するポリシーを決定する際には、対象となる情報リソースに対してどのような方式で接続させるかを決定しておく必要があります。

また、PC とスマートフォンそれぞれのデバイスでアクセスゲートウェイ（3G/4G などの携帯電話回線経由の場合の VPN、Wi-Fi 経由の場合の無線 LAN システム）を分割するか、統一するのかといった課題も挙げられ、その方針によっても接続ポイントとなるアクセスゲートウェイでのアクセスコントロールのポリシーが変ってくるので、十分な検討が必要です。

一般的に企業利用で考えられる接続方式を以下に記載します。

表 6-2　企業内への接続方式

アクセス元	アクセス方式		認可を行う上でのポイント
インターネット経由（携帯電話回線/公衆 Wi-Fi など）	企業外（DMZ）公開	ActiveSync などのアプリケーション対応	スケジュールやメールなど特定のアプリケーションを利用させたい場合に有効（アプリケーションに対応したものに限定される）で、アプリケーションレベルでアクセスさせる情報リソースを柔軟に制御することが可能
		リバースプロキシ	アクセスさせたい情報リソースが特定のアプリケーション（主に企業内及びクラウドサービスへの Web アクセス）のみである場合に有効
	リモートアクセス（VPN）		IPsec、SSL などスマートフォンの機種毎でアクセス方式を選択することが可能。また、認証結果に応じてアクセスさせる情報リソースを IP アドレス単位で制御することが可能
企業内 Wi-Fi 経由	Wi-Fi		アクセス範囲やポリシーに応じて SSID などを分割して、アクセスさせる情報リソースを柔軟に制御することが可能。ただし、多くのアクセスポイントにおいて統合的な管理を行うためには無線 LAN コントローラによる統合管理方式を取ることがセキュリティの統一の観点からも推奨される（機種によっては非管理アクセスポイントを検知する機能を持つものもある）

(3) 認証方式の決定

企業内ネットワークに接続するポイントにおいて適切な認証を行うとともに、認証結果に応じたアクセスコントロールを行うことが重要です。これはスマートフォンだけの範囲で考えるのではなく、従来利用されている PC のアクセスコントロールも含めて俯瞰をした上で考えることが推奨されます。

認証の詳細については、本ガイド第 5 章をご参照ください。

7. 暗号化

7.1. 対策の目的

ネットワーク上を流れるデータを暗号化することで、第三者による盗聴の脅威から情報資産を保護することを目的とします。

7.2. 前提

対策を実施する上で以下の事項を前提とします。

- 暗号化は、盗聴行為から情報を保護するために必要であり、解読時には、鍵を使って暗号文を平文に変換する。従って鍵の情報を全く知らずとも、総当たりの鍵予測を行えば解読は理論上可能となる。暗号鍵の有効期限を設定することにより、総当たり攻撃に対する対策を行うことを前提とする。
- 暗号化の実装方法としては、データ自身を暗号化する方法と通信経路を暗号化する方法がある。（本ガイドでは、メモリカードや内部ストレージなどの記憶媒体の暗号化については言及しない）

7.3. 要件

本対策についての要件を以下に記載します。

- 利用者の利便性を損なわずに実現すること。
- 適切なアルゴリズムを選択できること。
- 暗号強度だけでなくアルゴリズムの選択による装置への影響も考慮すること。

7.4. 対策案

暗号化の実施方式として以下の方式があります。単独での利用だけでなく、組み合わせて利用することを考慮する必要があります。

表 7-1　暗号化一覧

暗号化対象	暗号化区間	プロトコル	スマートフォン 対応状況
ファイル暗号化	End to End	手動	アプリケーション対応
メール暗号化	End to End	S/MIME	OS またはアプリケーション対応
		PGP	アプリケーション対応
Web サーバ暗号化	End to Server	TLS	OS またはアプリケーション対応
リモートアクセス暗号化	End to Network	SSL-VPN	アプリケーション対応
		IPsec	OS（未対応デバイスあり）
		L2TP over IPsec	OS
Wi-Fi 暗号化	End to Network	WEP[5]	OS
		WPA/WPA2	OS

[5] セキュリティ強度が弱いため、推奨しない

7.4.1. ファイル暗号化

通信を行う前にファイルそのものを暗号化します。一般的に共通鍵暗号方式が用いられており、ファイル単位でパスワードを設定します。ファイルに対する暗号処理は、現時点ではスマートフォン OS の機能で提供されておらず、アプリケーションを利用する必要があります。

ファイルの暗号は、エンド・トゥ・エンドでの通信経路及び転送後においても機密を維持することができます。転送対象となる全てのファイルに対しての暗号化は、パスワードの管理が煩雑になることから利用者に対する利便性を損なうため、データの重要性に応じて利用を判断する必要があります。

7.4.2. メール暗号化

メールに対する暗号処理です。スマートフォンにおけるメールの暗号化では S/MIME や PGP などのプロトコルを利用します。S/MIME も PGP も公開鍵暗号方式が採用されており、暗号に加えて電子署名を使用して送信者を明確にすることで安全性を高めています。

スマートフォンに暗号化機能が無い場合でも、暗号化機能を有するメールソトウェアを利用することが可能です。

(1) S/MIME

S/MIME では公開鍵の取扱いをより正当性を高めるために、認証局発行のクライアント証明書を利用します。署名の検証は商用の認証局にて行われます。

(2) PGP

PGP では、Web-of-Trust（信用の輪）という考え方に基づき、当事者間でお互いの公開鍵を交換することにより相手に出すメールデータを暗号化します。

7.4.3. Web サーバ暗号化

Web サーバとの通信の暗号化では主に SSL/TLS が利用されます。ブラウザやアプリケーションなどのクライアントと Web サーバ間の通信での暗号化の実施を決定するのはサーバ側となります。スマートフォンでは、標準で Web ブラウザを実装しており SSL/TLS 通信にも対応しています。

7.4.4. リモートアクセスにおける暗号化

自宅や外出先から企業のネットワークにアクセスする際に通信経路を暗号化し、盗聴行為からデータを保護します。リモートアクセスの方式を以下に記載します。

(1) SSL-VPN

Web サーバ暗号化で説明した SSL/TLS を利用したリモートアクセス方式です。

メールやリモートディスクトップなどに関しては、HTTP プロトコルでカプセル化して暗号化します（以下トンネリング）。PC とは異なり、スマートフォンの場合は Web ブラウザだけではトンネリングの機能が提供できないため、トンネリングに対応した専用アプリケーションが必要となります。

(2) IPsec

IP レイヤで暗号化する技術で、ほぼ全てのプロトコルが暗号化されます。PC の場合は専用のソフトウェアを導入する必要がありますが、スマートフォンでは IPsec クライアント機能が標準でインストールされているものがあります。IPsec の認証には事前共有鍵方式（PSK 方式）と公開鍵暗号方式（RSA 方式）の 2 通りがあります。事前鍵共有方式は予め決めた同じ鍵を共有する方法で同じ文字列の鍵を設定しておきます。公開鍵暗号は暗号通信時に証明書を提示することで共通鍵を生成するので、公開鍵方式の方が、より安全な通信といえます。

(3) L2TP over IPsec

L2TP は OSI モデルのレイヤ 2 でのトンネリングプロトコルです。L2TP は汎用性の高いトンネリングプロトコルですが、暗号化機能を実装していないため、IPsec で暗号化を補っています。なお、スマートフォンによっては、リモートアクセスで利用するプロトコルに L2TP over IPsec のみにしか対応しないモデルもあるので注意が必要です。

7.4.5. Wi-Fi 環境での暗号化

Wi-Fi における暗号化はデバイスから AP までとなります。認証方法、暗号強度によって複数の暗号プロトコルがあり、利用形態により使い分けすることが必要です。

(1) WEP（Wired Equivalent Privacy）

WEP は RC4 というストリーム暗号を用いて実装されています。WEP は導入が比較的容易ですが、暗号強度に問題があることが指摘されおり、デバイスから AP に送られる全パケットの暗号化に同様の鍵を使用しているため、一度鍵が推測されると以後のパケットが解読されてしまう可能性があります。従って、スマートフォンにおいても WEP の利用は推奨しません。

(2) WPA（Wi-Fi Protected Access）／WPA2

WPA は WEP の問題を改善された方式です。利用モードに Enterprise と Personal の 2 つがあり、Enterprise では、IEEE802.1x 認証サーバを使い、利用者毎にキーを配布します。Personal モードでは PSK（事前共有鍵モード）となり IEEE802.1x 認証サーバを必要としません。

WPA2 は従来の WPA の拡張となり、WPA では TKIP という暗号プロトコルを採用していますが、WPA2 では、より強度の高い AES ベースの CCMP という暗号アルゴリズムに対応しています。

Enterprise では認証方式として EAP という拡張プロトコルを利用することができます。なかでも EAP-TLS は証明書を双方向で認証します。多くのスマートフォンが WPA2 と EAP-TLS に対応していることもあり、企業の Wi-Fi 環境においては、WPA2 と EAP-TLS を実装することを推奨します。

8. 不正 AP 対策

8.1. 不正 AP への接続防止

8.1.1. 対策の目的

不正に設置された Wi-Fi AP にスマートフォンが意図せず接続することにより、利用者の通信履歴や情報が収集されるリスクを排除することを目的とします。

公衆 Wi-Fi と同じ SSID とパスフレーズを使って、その公衆 Wi-Fi になりすまし、ハニーポットと同様の動作をすることにより、利用者のスマートフォンが意図せず接続されると情報を詐取される可能性があります。これは公衆 Wi-Fi に限らず、セキュリティ設定のない所有が不明な AP についても同様です。

8.1.2. 対策の対象

- 公衆 Wi-Fi（有償及び無償）
- 偽装公衆 Wi-Fi（ハニーポット）
- 所有が不明な Wi-Fi AP（ハニーポットの可能性）
- 第三者のテザリング端末及び Wi-Fi ルータ

8.1.3. 対策案（対策の手段）

本対策についての要件を以下に記載します。

(1) 業務利用においては、VPN によるネットワーク接続を奨励する

アクセスの度に VPN 接続させるか、自動的に VPN 接続を行える製品を利用する。

(2) 利用者の教育（ルール化）

- 業務利用の際には VPN で接続されていることをチェックする事、あるいは接続操作をする事を義務づける。
- スマートフォンに ID とパスワードを記憶させない。
- 公衆 Wi-Fi のサービスによってはログイン時に Web 表示がサービスポータルとしてのページに転送され、その際に加入者のユーザ名が表示されるので、自分の名前が表示されているかどうかを確認する。
- 多重ログインを許可していない公衆 Wi-Fi サービスでは、ユーザ名/パスワードが漏洩し第三者が利用していると、その旨のメッセージが表示される（ログインできない）。異常があると思える場合、PC から同サービスにアクセスしてパスワードを変更する、もしくは利用を停止するなどの措置が行う。
- 信頼のできる AP 設置場所以外ではスマートフォンの Wi-Fi 設定を無効にする。

(3) 業務用サイト制作においては、HTTPS（SSL）接続を前提として設計する

(4) 業務用アプリケーション制作においては、アプリケーションの起動時、自動的に VPN 接続を行う設計とすることが望ましい

(5) 電子証明書（IEEE802.1x[6]など）で認証するサービスを提供している公衆 Wi-Fi を利用する

8.2. 不正 AP の設置防止

8.2.1. 対策の目的

無許可の AP が企業内ネットワークに接続され、その AP を経由して承認されていないスマートフォンによる企業内ネットワークへの接続防止を目的とします。

8.2.2. 対策案

本対策についての案を以下に記載します。

(1) ルール化

AP 設置に関するルールを整備する。ルールは利用者の勝手な AP 設置を禁止するものであり、設置する場合は、IT 管理者によりセキュリティレベルの確認やアクセスログの可視化が対応されるものとする。

(2) ネットワークの監視

- 不正 AP 検出機能をもった無線 LAN 機器を利用する。
- 企業内ネットワーク全体に対し、事前に登録された MAC アドレスの機器以外の装置が接続されていないかを監視する。

[6] IEEE802.1x 認証では、AP に接続する前に認証が行われるため、接続しようとした AP が偽装 Wi-Fi である場合には正常に認証が終了せずに接続が拒否される。ただし、予めツールや証明書のインストールが必要となる。

9. おわりに

本ガイドで記載した対策については、スマートフォンを利用する際にネットワークの観点から特に優先度の高いものについて整理しました。これ以外に考慮すべき点として以下の事項があります。

(1) root 化または Jailbreak 対応

ネットワーク側で認証・アクセスコントロールを強化しても、デバイスが root 化や Jailbreak された場合、なりすましやマルウェアの感染などの脅威にさらされる可能性が高くなります。ネットワーク側でその対策を行うことが困難であることから、MDM での監視やルールの徹底などにより root 化や Jailbreak されたデバイスを社内に接続させない対応が必要となります。

(2) ネットワーク接続におけるデバイスの依存

PC の場合はデバイス依存の機能や実装が比較的少ないのに対して、スマートフォンの場合は、デバイスや OS、通信アプリケーション、通信サービスの仕様により VPN 機能や Wi-Fi 接続機能において設定が異なっているものや、動作できないものもあります。デバイスやサービスの選定にあっては事前に調査、検証が必要です。

(3) フィルタリング

Web アプリケーションを経由したマルウェアの感染、フィッシング対策としては URL などのフィルタリングが効果的ですが、常時データ通信を ON にしているスマートフォンにおいては、その実装方法についてはいくつかの手段があり、どれを採用するか（または、どのように組み合わせるか）の見極めが必要です。

- ネットワーク側での対応
  - 企業内ネットワークを経由する場合は企業内にてフィルタリングを実施
  - 通信事業者やサービス事業者のサービスを利用する
- デバイス側での対応
  - ウイルス対策・セキュリティソフトベンダーのアプリケーション機能を利用

(4) ネットワーク・端末の見える化

さまざまなデバイスが企業内ネットワークに接続されることから、どのようなデバイスがどのような通信を行っているかを把握する「見える化」も有用です。ネットワーク機器・Firewall の通信ログや IDS/IPS などの侵入検知・防御システムの採用により、特定サーバへの攻撃やマルウェアの感染活動、ボットネットなどへの通信の確認を行うことは、社外で利用する機会の多いスマートフォンを社内で利用する際により効果的なセキュリティ対策となります。また、MDM などのスマートフォン管理の仕組みを導入することで、不正なアプリケーションをインストールしているデバイスの検知や、推奨するアプリケーションの導入を促すなどの効果が見込めます。どちらもリアルタイムでの対策が困難な場合もありますが、インシデントが発生した際に事後の対応がスムーズに行うことが可能となります。

上記に加えて実施すべき対策やネットワークの観点以外での対策（デバイスやアプリケーションなど）も併用して、網羅的に検討することが重要です。また、テクノロジーの進歩やデバイス仕様の変化により、新たな対策手法も出てくるものと考えられますので、継続して情報収集していくことを推奨します。

最後に、新たなデバイスであるスマートフォンの利便性と可能性を損なわないよう、リスクに応じたバランスの良いセキュリティ対策を実施頂くために本ガイドを活用頂ければ幸です。