技術部会 ネットワークWG 活動報告

2012年5月24日

ネットワークWGリーダ　　相原弘明
(株式会社ネットマークス)

Agenda

1．ネットワークWG　活動報告

2．ネットワークタスクフォース　活動報告

3．クラウドタスクフォース　活動報告

1.ネットワークWG　目的と構成

- 目的

  スマートフォンセキュリティにおける

  ネットワーク観点から、セキュリティ課題の検討を行う。

- 構成

  以下の2つのタスクフォース(TF)で構成

  ①ネットワークタスクフォース

  ②クラウドタスクフォース

1.ネットワークWG　活動テーマ【発足時】

①『スマートフォンネットワークセキュリティ実装ガイド』の
　作成及び公開

②個別課題検討
- クラウドセキュリティ
- 公衆Wi-Fiの偽装
- テザリング中のVPN接続

③ネットワーク接続検証
- VPN接続検証

2．ネットワークタスクフォース

2.ネットワークTF　参加メンバー

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
相原弘明	株式会社ネットマークス

2.ネットワークTF　実装ガイドについて

『スマートフォンネットワークセキュリティ実装ガイド』

に関するリリース状況の報告と今後の予定

2.実装ガイドの目次

1章：実装ガイドの概要
2章：実装ガイドのスコープ
3章：セキュリティ対策の基本的な考え方
4章：ネットワーク接続時のセキュリティ対策要件
5章：認証
6章：アクセスコントロール
7章：暗号化
8章：不正AP対策
9章：おわりに

2.実装ガイドの概要

- 概要

  スマートフォンネットワークセキュリティ実装ガイドは、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。

- 想定読者

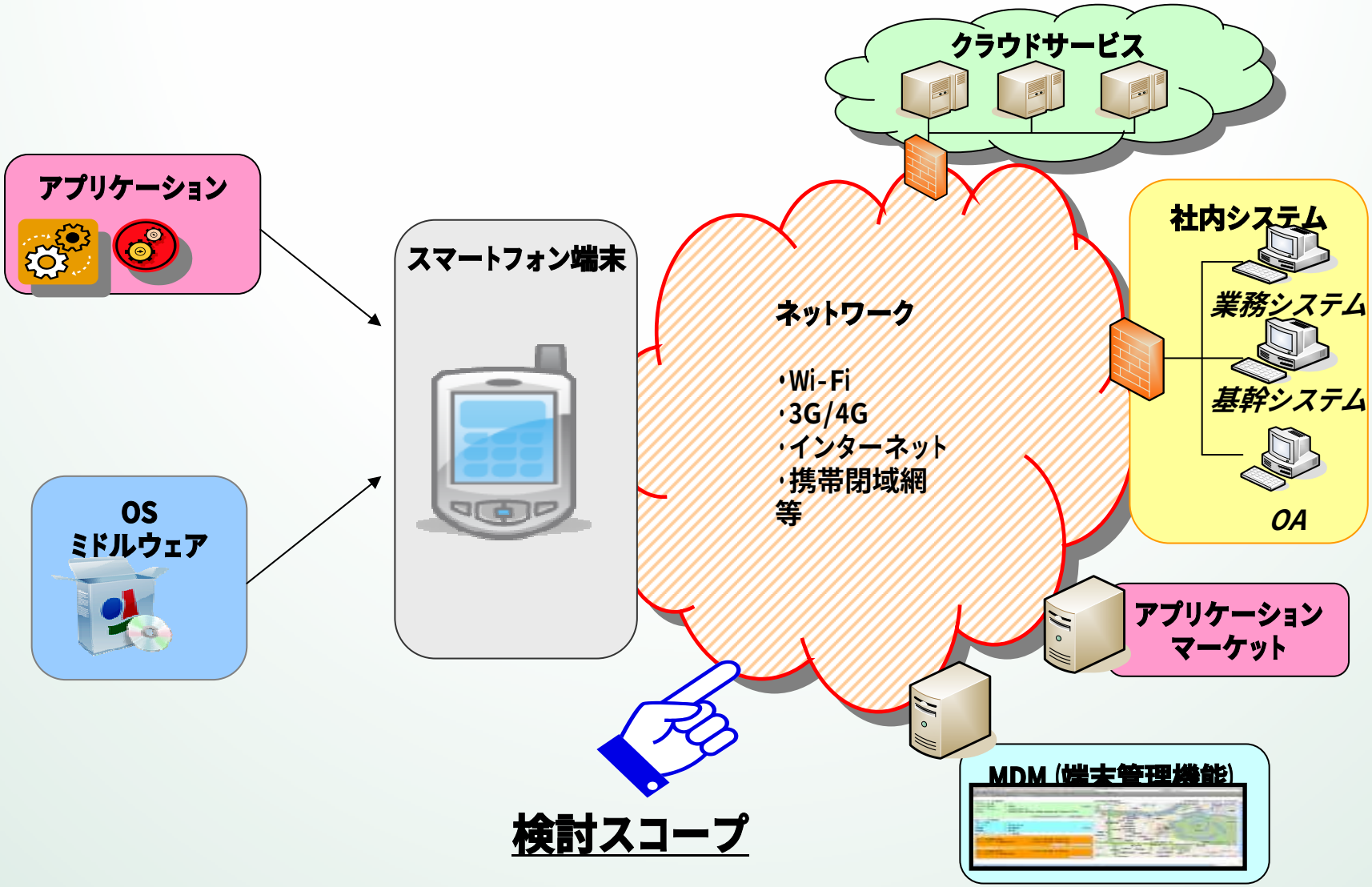
  本ガイドは、主に以下の読者を対象としています。

  (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.ネットワークセキュリティ対策の考え方

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蓄積されたセキュリティ対策を、スマートフォンの特性を考慮しながら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。

2.対策検討の流れ

① スマートフォンの接続形態の洗い出し

② 接続形態毎の発生箇所とその脅威を整理

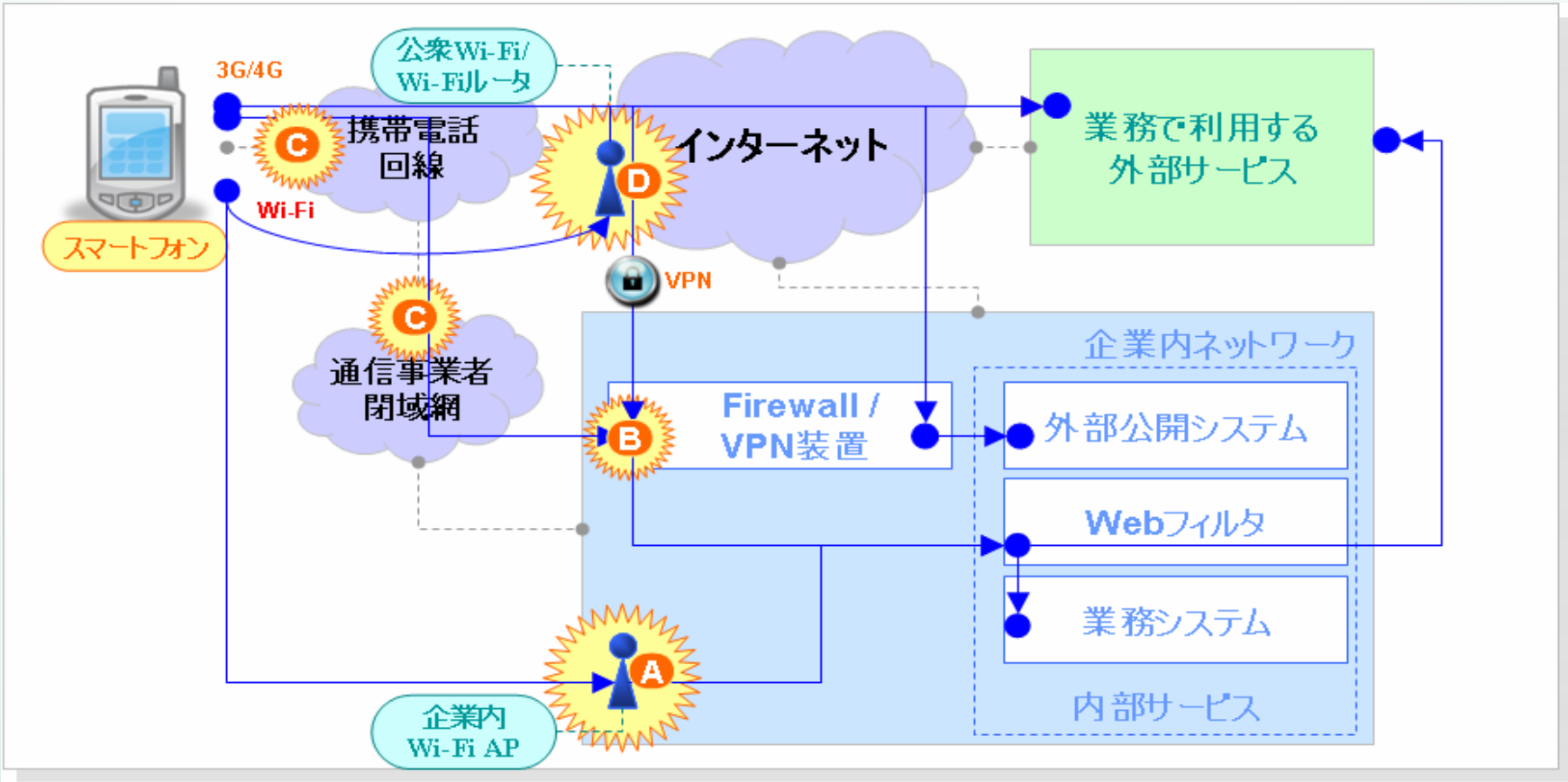
③ 脅威に対する対策

④ 対策に対する優先度の設定

⑤ 優先度の高い対策に対する対策方式例

2. ネットワーク接続時の脅威存在箇所

<脅威が存在する箇所>
(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



2. ネットワーク接続点での脅威

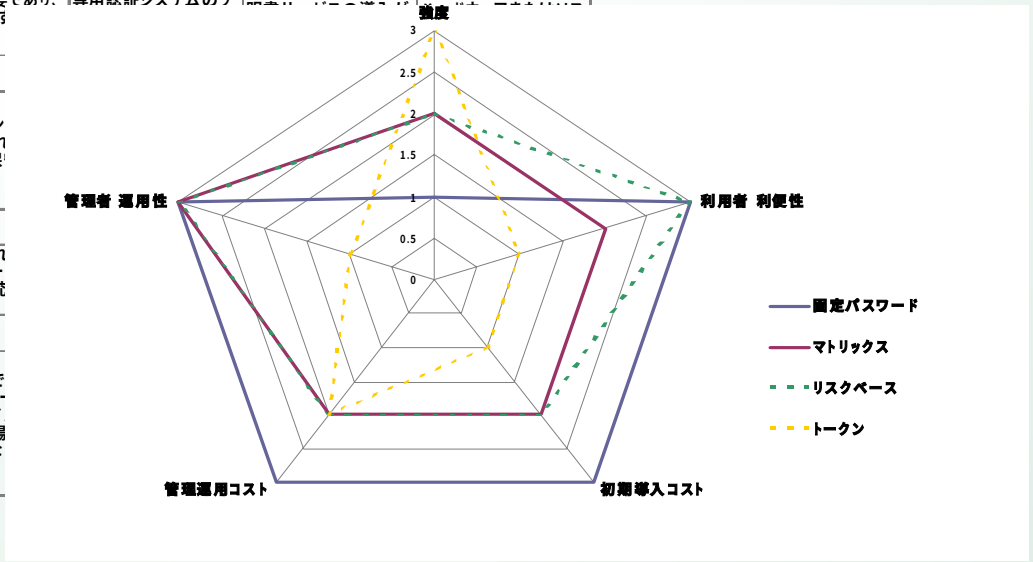
脅威		対策実施箇所			
		(A) 企業内 Wi-Fi AP	(B) VPN (Firewall・VPN 装置)	(C) 携帯電話回 線閉域網	(D) 公衆Wi-Fi /Wi-Fiルータ
なりすまし	利用者	△	○	-	△
	デバイス	△	○	-	△
盗聴		○	-	-	○
不正利用	業務外利用	○	-	△	-
	外部サービス	-	-	-	○
不正アクセス	対 業務システム	○	○	-	-
	対 ネットワーク機器	-	○	○	○
機器障害		-	○	-	-
通信規制		-	-	○	-
圏外		-	-	○	-
通信事業者の回線障害		-	-	○	-
不正AP設置		-	-	-	○

2.脅威に対する対策

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(ルール化等)
なりすまし	○			
盗聴			○	
不正利用		○		
不正アクセス		○		
不正AP設置			○	○

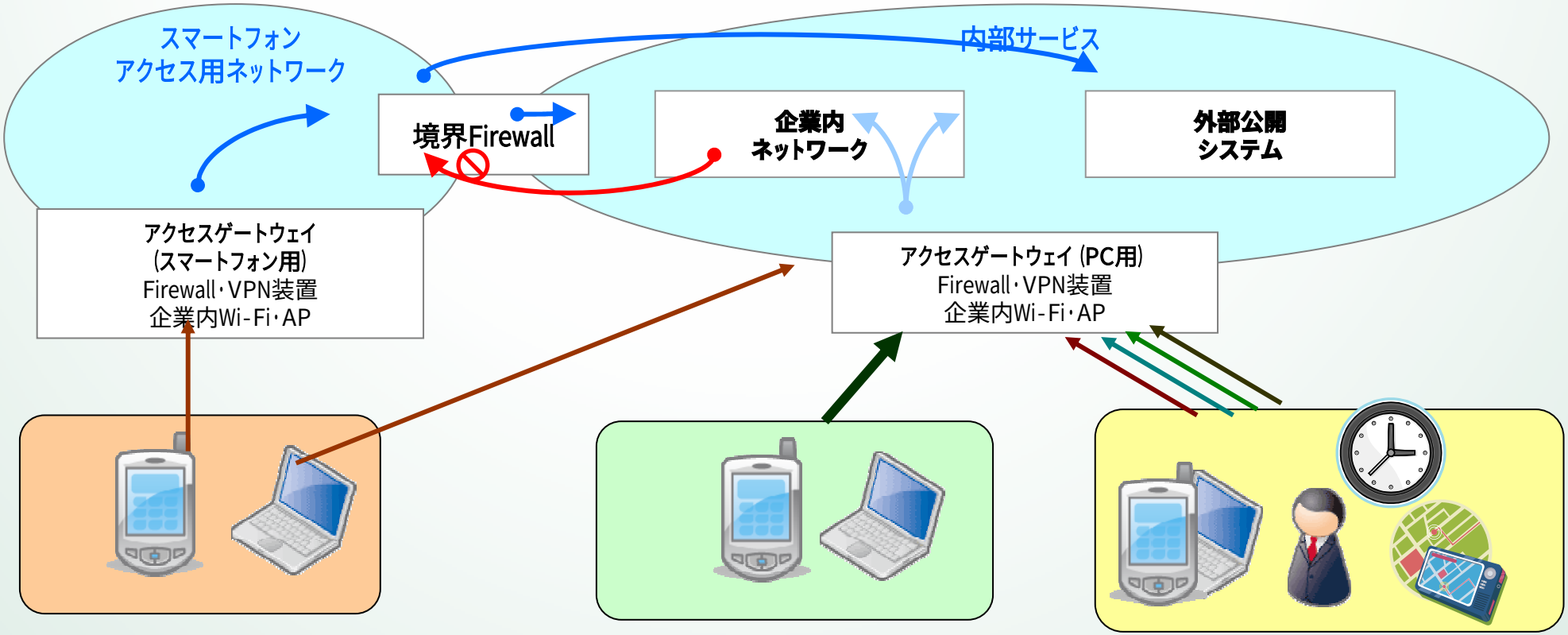
2.認証対策での実装方式比較(例)

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	CA局の構築または証	専用認証システムの
		3	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	ユーザライセン品の場合、それたライセンス保が必要			
		3	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	パスワード忘れ対応が必要	パスワード忘れ対応の他、トー損、紛失時対応となる			
		3	3	3	1			
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等の制限からくら）に制限がある	利用範囲広い	同じデバイスで（ソフトウェアトスマートデバイ導入している場では2要素にな			



凡例） 1:標準 2:優れる 3:特に優れる

2. 3つのアクセスコントロールの考え方(例)

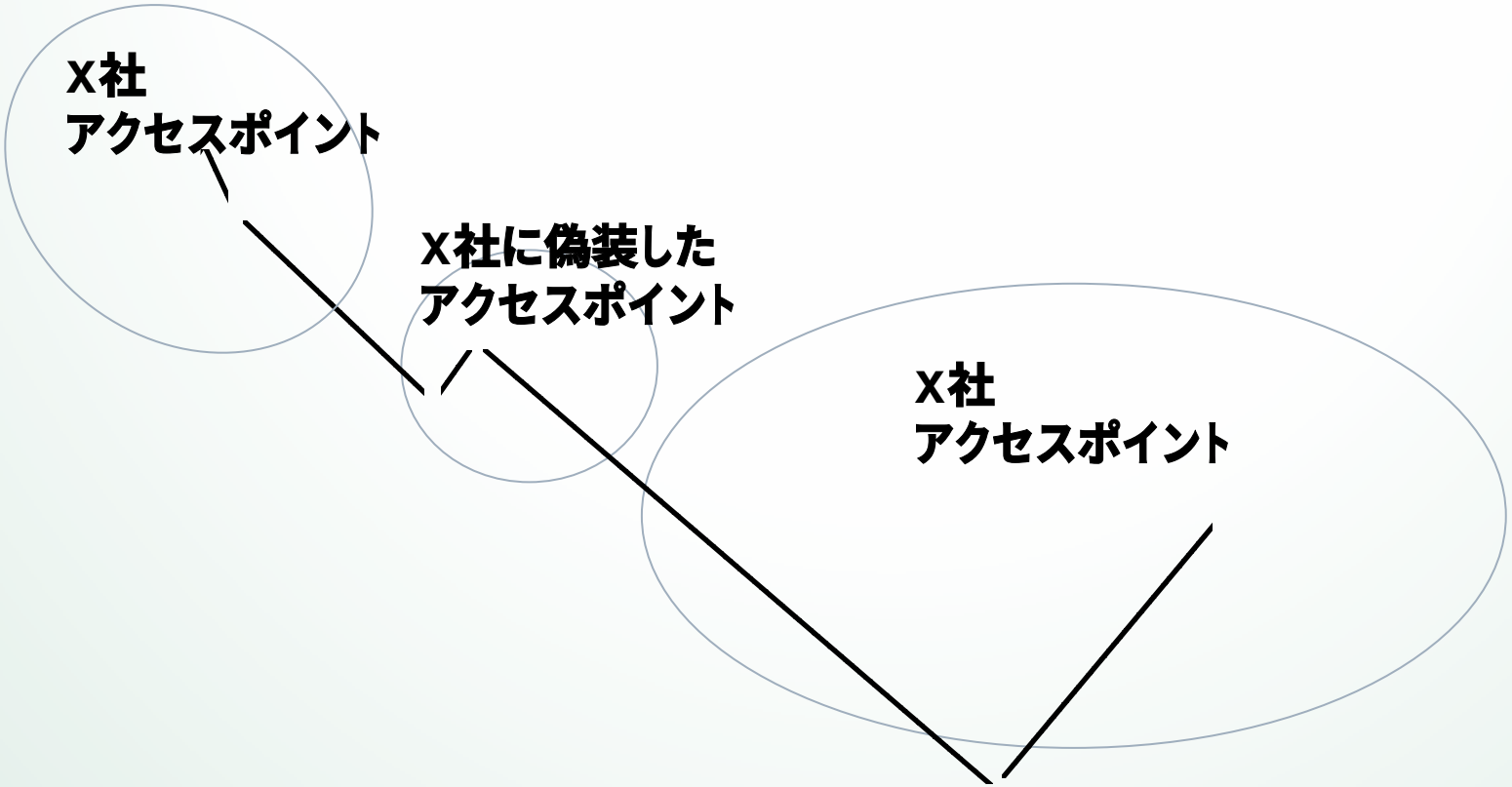


②スマートフォン用のネットワークを分離

①PCとスマートフォン用を同等の扱い

③デバイスや利用者、利用場所や時間に応じた制御

2.不正APへの接続防止対策



例えば、移動経路にX社に偽装したアクセスポイントがあると、スマートフォンの設定によっては自動的に接続してしまう。これにより通信の内容を盗聴される可能性がある。

2.不正APへの接続防止対策（例）

（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

・VPN利用のルール化や自動的にVPN接続を行えるサードパーティ製品の利用

（2）公衆Wi-Fi事業会社提供している接続用アプリケーションの利用

（3）信頼のできるAP設置場所以外ではWi-Fi設定を無効化

（4）802.1xで認証するサービスを提供している公衆Wi-Fiを利用

（5）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

（6）業務用アプリケーション制作では、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

2.ネットワークTF　今後の予定

①本ガイドのβ版公開と初版に向けての対応

②ネットワーク接続検証に向けた調整
- VPN接続検証
- テザリング中のVPN接続

③個別課題検討
発生毎に検討

3．クラウドタスクフォース

3.クラウドタスクフォース

『スマートフォンの業務利用における
クラウド活用ガイド』【β版】

に関するリリースの報告と今後の予定

3.クラウドタスクフォース参加メンバー

倉永 英久	株式会社大和総研ビジネス・イノベーション
本多 規克	アルプスシステムインテグレーション株式会社
野尻 泰正	株式会社イーグリッド
高野 篤	株式会社イーグリッド
加藤 雅和	株式会社NTTデータMSE
近藤 伸明	株式会社神戸デジタル・ラボ
雲井 卓	株式会社神戸デジタル・ラボ
吉田 晋	株式会社コネクトワン
中山 聡	株式会社CSIソリューションズ
谷田部 茂	シスコシステムズ合同会社
清水 健	株式会社 EMPRESS SOFTWARE JAPAN
三木 英夫	セコムトラストシステムズ株式会社
棚橋 佑子	セコムトラストシステムズ株式会社
倉林 俊介	トヨタ自動車株式会社
松村 啓	日本電気株式会社
相原 弘明	株式会社ネットマークス

3.クラウドタスクフォースの成果

2012年4月12日
『スマートフォンの業務利用における
クラウド活用ガイド』
【β版】 公開

3. 公開概要

『スマートフォンの業務利用におけるクラウド活用ガイド』【β版】

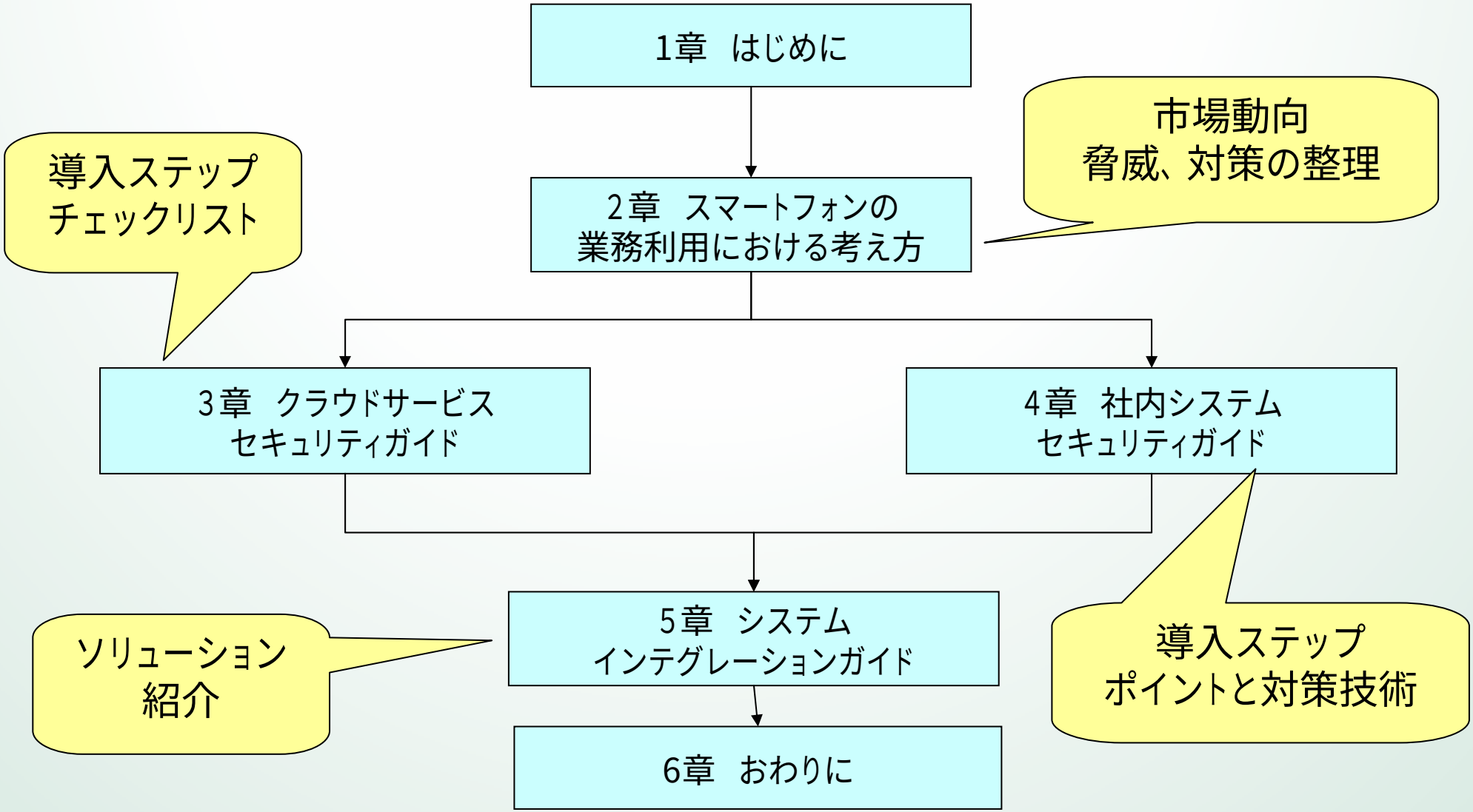
MObile & Cloud Hybrid Integration
（MOCHI）

1，リスク分析（統計ベース）

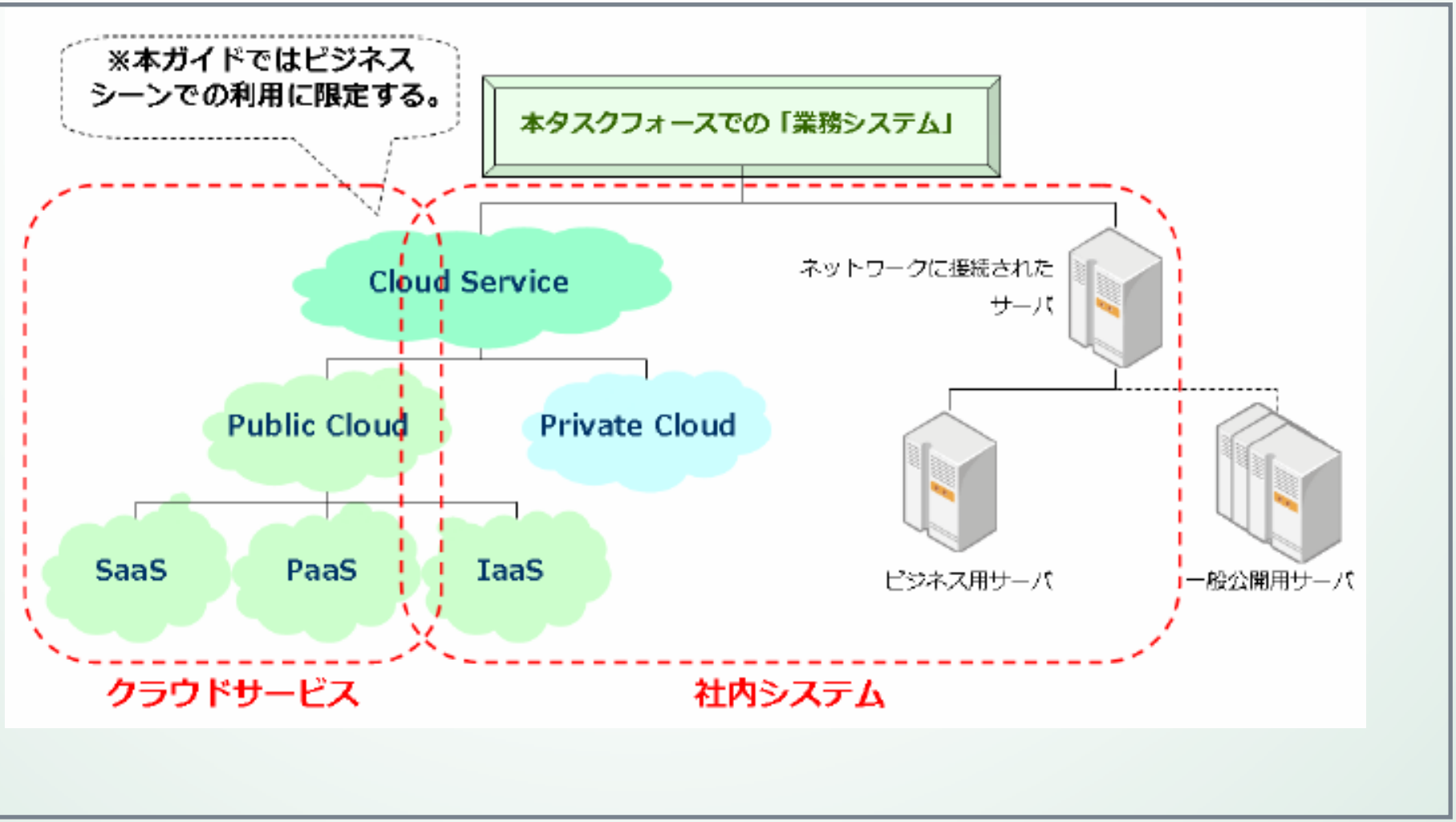
2，セキュリティ指針
（クラウドサービスと社内システム）

3，技術事例

3. ガイドの構成

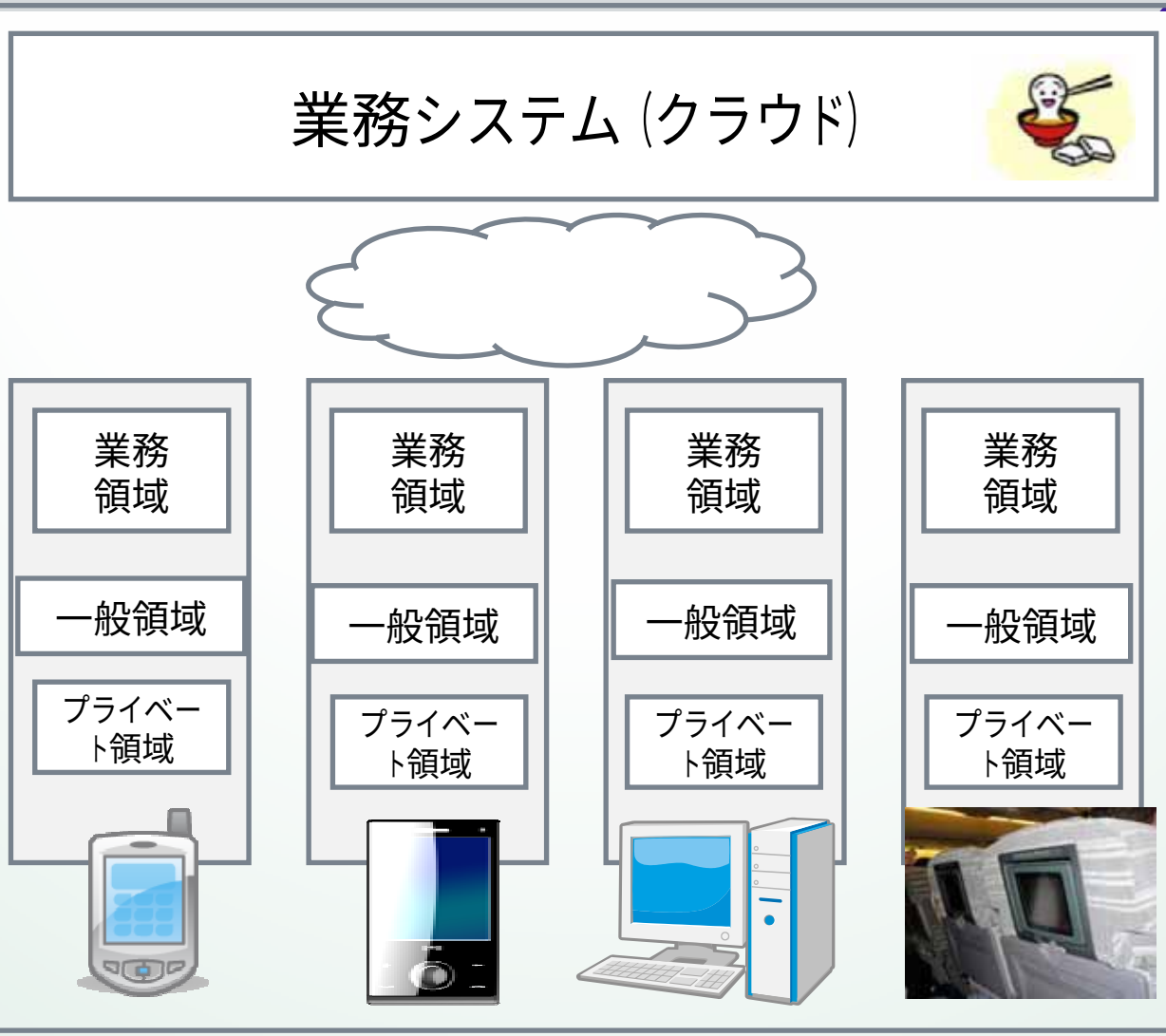


3.β版でのクラウドの定義



「スマートフォンとクラウドの組み合わせ」についてのセキュリティ視点が不明確であった。

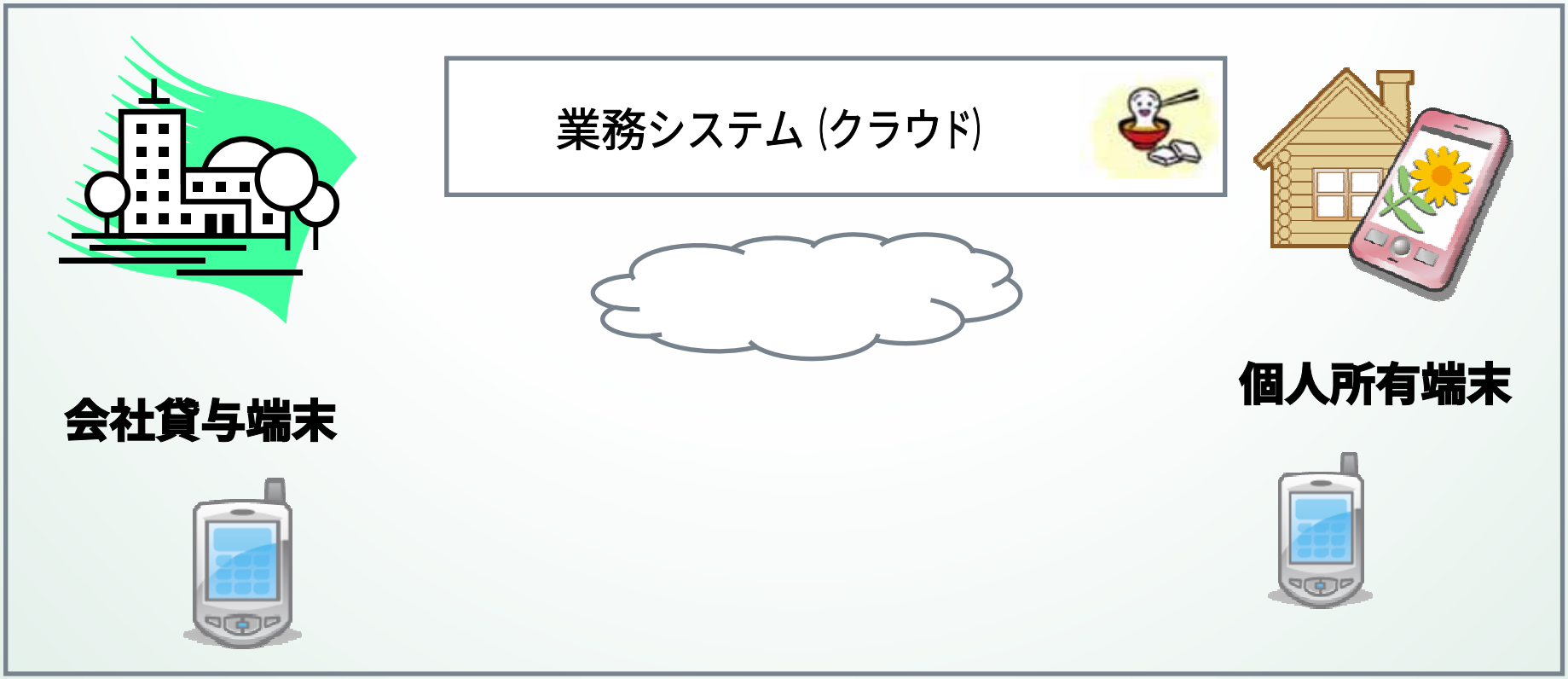
3.初版に向けてのクラウドの定義



「クラウド」とはどのOSどの端末でも、同一のIT環境にアクセスできる技術のこと

3.クラウドTFの目的

どのOSでも、どの端末でも、包括的にセキュリティを
保つために必要なセキュリティガイドの構築を行う



例）
■会社貸与端末と個人所有端末が混在して運用しなければならない場合、どういうセキュリティが必要か
■iOS, Andorid, WindowsのOSが混在して運用しなければならない場合、どういうセキュリティが必要か

3.クラウドTFの目的

ガチガチポリシー

・会社配布端末に限定
・OSも一種類に限定
・可能な限りの権限は
　システム管理者の配下に

リベラルポリシー

・端末の所有者の制限なし
・OSの制限なし
・端末管理は会社は関与せず
　所有者の自己責任で行う

二極化する運用方針

世の中に認知されつつある領域

・どういうリスクが考えられるのか
・どういう運用方法が推奨されるのか
・どういう技術が世の中にあるのか

まだ明確な指針が見えていない領域
‖
クラウドTFで求められるガイドライン領域