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

～日本のスマートフォンとビジネスマン達の輝ける未来のために～

【β版】

２０１２年4月１２日

日本スマートフォンセキュリティフォーラム（JSSEC）
技術部会
ネットワークワーキンググループ
クラウドタスクフォース

文書管理番号 JSSEC-TECN-CL-GD20120412

■制作■

技術部会 ネットワークワーキンググループ クラウドタスクフォース

リーダー	倉永 英久	株式会社大和総研ビジネス・イノベーション
メンバー	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	新日本無線株式会社
	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

（社名五十音順）

※ JSSEC ならびに執筆関係者は、本ガイドに関するいかなる責任も負うものではありません。全ては自己責任にて対策などをお願いします。
※ 本ガイドに登場する商品名・サービス名は、一般に各社の商標または登録商標です。
※ 社内文書などに引用する場合、著作権法で認められた引用の範囲内でご利用ください。また、その際は必ず出典を明記してください。
※ 本ガイドは 2012 年 4 月時点のものであり、記載された内容は今後変更の可能性があります。

文書管理番号 JSSEC-TECN-CL-GD20120412

目 次

1. はじめに 3
1.1. 本ガイドの目的 3
1.2. 本ガイドのスコープ 3
1.3. 本ガイドの対象読者 6
1.4. 本ガイドの構成 6
1.5. 用語集 7

2. スマートフォンの業務利用における考え方 8
2.1. 本章の位置づけ 8
2.2. 背景 8
2.3. システムセキュリティの検討 10
2.3.1. 保護対象の明確化 10
2.3.2. 脅威の洗い出し 10
2.3.3. 対策に関する本資料のアプローチ 12
2.4. システムアーキテクチャの検討 13
2.4.1. システムアーキテクチャ概念図 13
2.4.2. 端末の支給方法について 14
2.4.3. 業務システムの取得方法について 15
2.5. スマートフォンと業務システムに関する考察 16

3. クラウドサービスセキュリティガイド 17
3.1. 本章の位置づけ 17
3.2. クラウドサービス利用のステップ 18
3.3. クラウドサービス選定チェックリスト 20
3.4. 技術紹介 21
3.4.1. 最低限必要なセキュリティ対策 21
3.4.2. IP アドレスによるアクセス制限 21
3.4.3. シングルサインオンによる認証 22
3.4.4. クライアント証明書による認証 22
3.4.5. 端末固有情報による認証 22

4. 社内システムセキュリティガイド 23
4.1. 本章の位置づけ 23
4.2. 社内システムのセキュリティ対策導入ステップ 23
4.3. 社内システムのセキュリティ対策におけるポイント 24
4.4. 技術紹介 25
4.4.1. ３要素認証 25
4.4.2. マルウェア対策（サーバー型） 26
4.4.3. シンクライアント 27
4.4.4. リバースプロキシ 29

All rights reserved (c) Japan Smartphone Security Association

5. システムインテグレーションガイド 30
5.1. 本章の位置づけ 30
5.2. ソリューション紹介 31
5.2.1. 紙媒体持ち出しリスクの低減ソリューション 31
5.2.2. ３要素認証応用ソリューション 32
5.2.3. ビジネスインテリジェンス MDM ソリューション 34
6. おわりに 35
6.1. 今回のまとめ 35
6.2. 今後の課題 35
6.3. 今後の進め方 35
6.4. 今後の目標 35

All rights reserved (c) Japan Smartphone Security Association

1. はじめに

1.1. 本ガイドの目的

日本スマートフォンセキュリティフォーラム（以下、JSSEC）では、2011 年 5 月の発足以来、「スマートフォンやスマートタブレット（以下、スマートフォン）」の提供者／開発者／利用者などの、各企業が集まり、スマートフォンのセキュリティ向上に向けて様々な観点から調査・分析を行い、ガイドラインや提言の形で利用者などに公開してきました。

そのような活動の成果物の一つとして、2011 年 12 月に公開された『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』（以下、セキュリティガイドライン）があります。このセキュリティガイドラインでは、主にスマートフォンを業務で利用する際のセキュリティ上の注意事項を、スマートフォンの特性や、利用シーンに応じて、整理・分類し、対策について基本方針を提示しています。

本ガイドは、このセキュリティガイドラインの基本方針を技術的な面からさらに具体化して検討を行いました。その際に、業務システムとして近年 SaaS / PaaS / IaaS など様々な形で利用されている「クラウドサービス」と、オンプレミス型も含めた「社内システム」に注目し、スマートフォンの業務利用におけるセキュリティ向上策についてまとめました。

本ガイドがスマートフォンから業務システムを利用する際のセキュリティ対策として参考になり、業務効率の改善に貢献できれば幸いです。

1.2. 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、JSSEC 技術部会ではその要素ごとにワーキンググループに分かれて調査・分析およびガイドラインの作成を行っています。

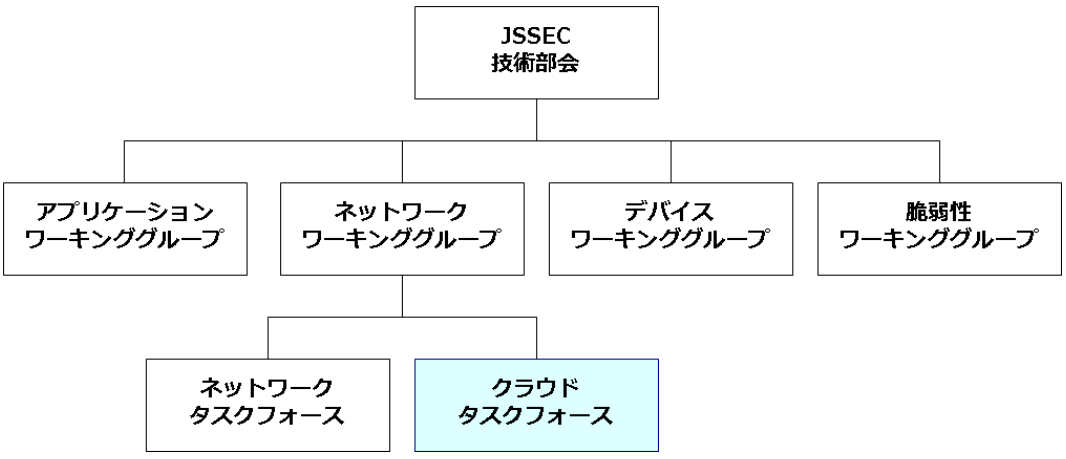


図 1-1　JSSEC 技術部会の組織

All rights reserved (c) Japan Smartphone Security Association

以下に、スマートフォンをとりまくセキュリティ環境の概念図を示します。

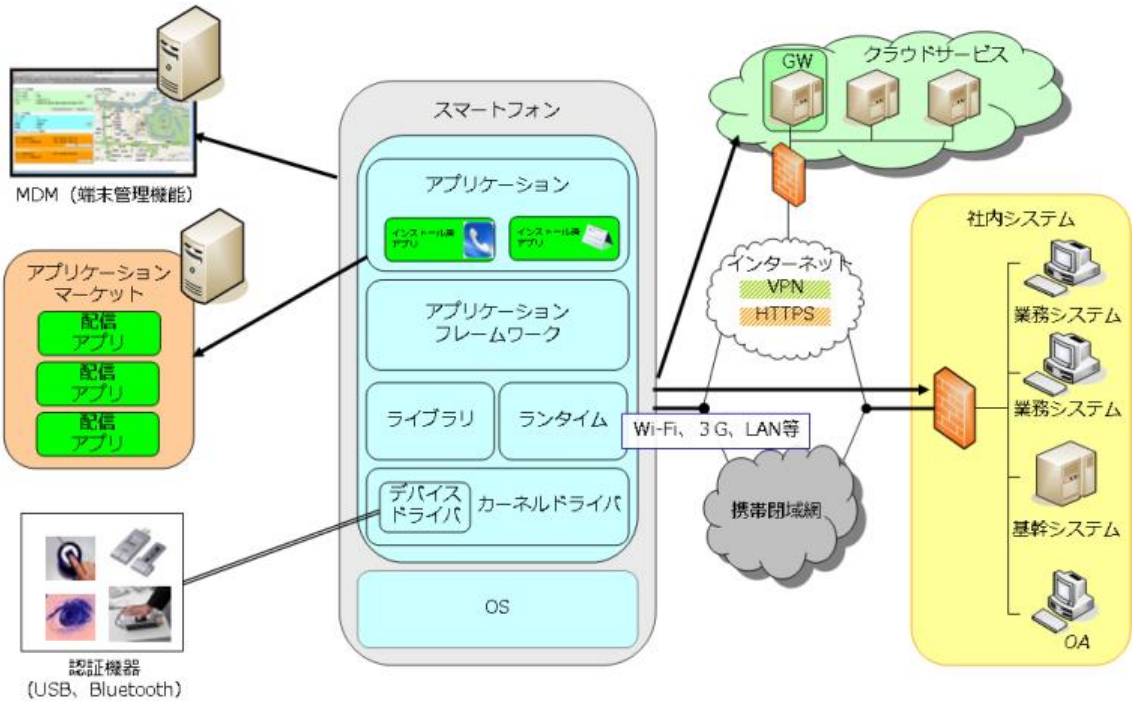


図 1-2　スマートフォンをとりまくセキュリティ環境の概念図

スマートフォンから見た場合、データの送信先は「クラウドサービス」であっても「社内システム」であっても意識されることはありません。そのため、クラウドタスクフォースでは「クラウドサービス」と「社内システム」をまとめて「業務システム」として、スコープ（対象の範囲）としました。

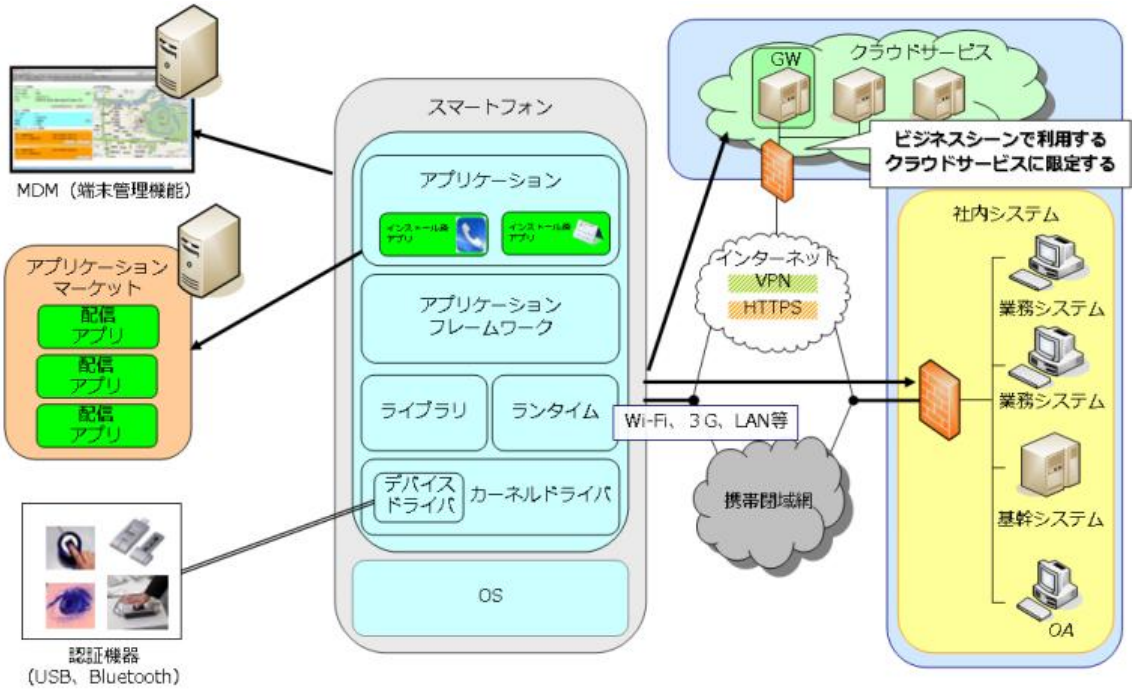


図 1-3　クラウドタスクフォースで対象とするスコープ

All rights reserved (c) Japan Smartphone Security Association

なお、スマートフォンから「クラウドサービス」「社内システム」までの通信経路についてはネットワークタスクフォースのスコープとなっています。通信経路におけるセキュリティ対策についてはネットワークタスクフォースからの公開資料をご参照ください。

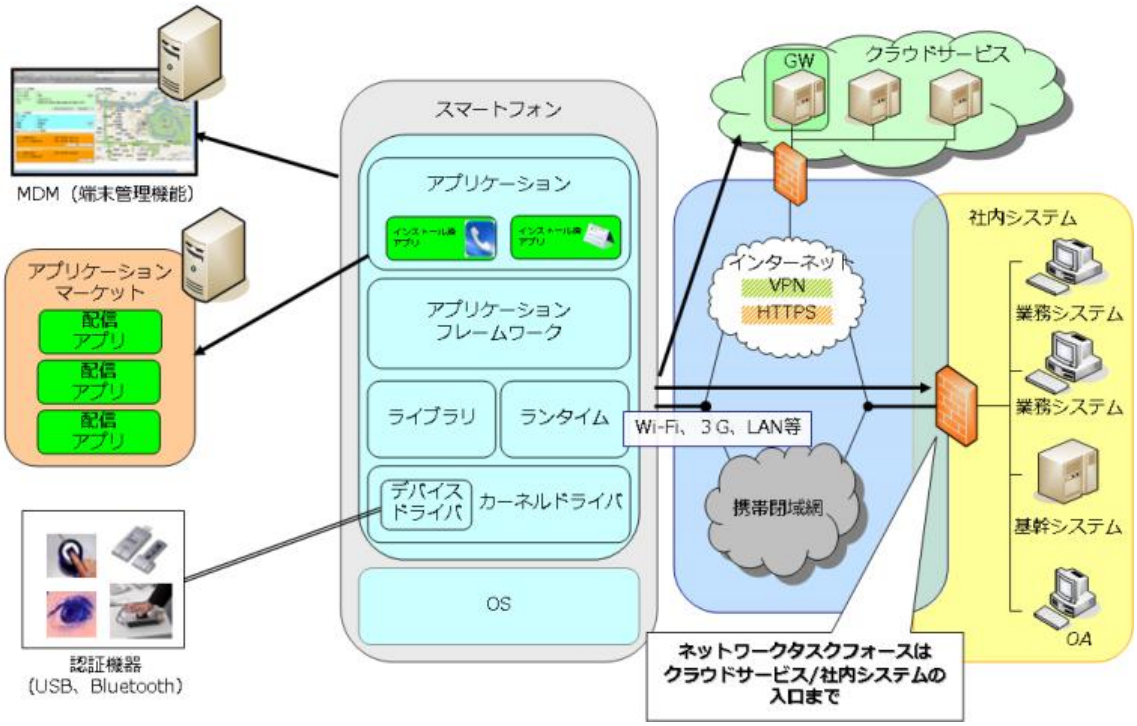


図 1-4　ネットワークタスクフォースで対象とするスコープ

All rights reserved (c) Japan Smartphone Security Association

1.3. 本ガイドの対象読者

本ガイドでは読者として、主に以下の立場の方を想定しています。

- 企業や組織においてスマートフォンの業務利用を検討する責任者・企画担当者
- 企業や組織においてスマートフォンの業務利用を検討する際にセキュリティポリシーを策定する責任者・担当者
- 企業や組織においてスマートフォンの業務利用を検討する際に業務システムの RFP や要求事項などを作成する担当者
- 上記の方からの要望に応じて、スマートフォンを活用した業務システムについて提案・開発・導入を行う担当者

1.4. 本ガイドの構成

本ガイドでは、スマートフォンから業務システムを安全に利用するための技術的要件を以下の構成でまとめました。

2 章では、セキュリティを検討する際の考え方について説明します。その際に保護する対象と脅威を明確にし、「クラウドサービス」とオンプレミス型の「社内システム」との違いについても説明します。

3章では、「クラウドサービス」のセキュリティ対策として重要な技術について紹介します。どのような「クラウドサービス」を安全と判断して良いかチェックリストを提示します。

4章では、オンプレミス型の「社内システム」へのセキュリティ対策として重要な技術について紹介し、それぞれについてどのような脅威を解決できるのかをまとめます。

5 章では、スマートフォンから業務システムを安全に利活用するソリューションについて紹介します。その際に、どのような要求に対して適合するか、構築においてどのような点に注意が必要か、またどのような機能拡張が可能なのか、についても合わせて紹介します。

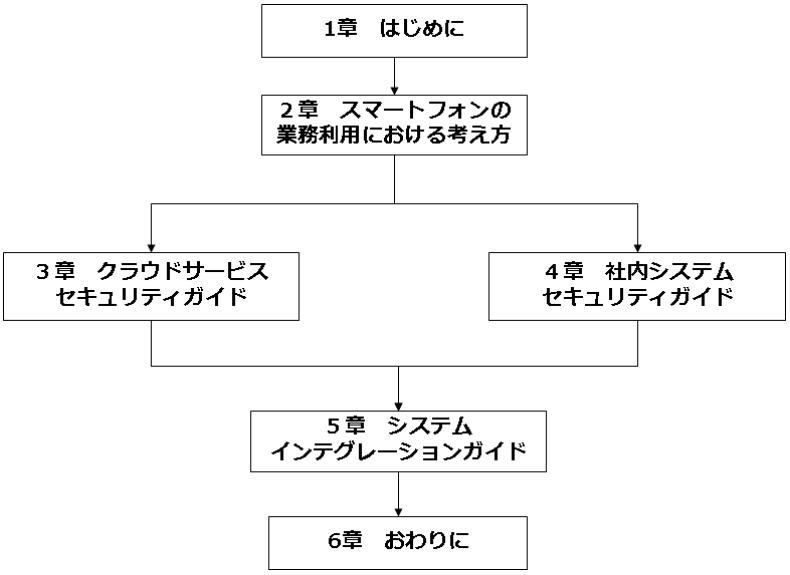


図 1-5　本ガイドの構成

All rights reserved (c) Japan Smartphone Security Association

1.5. 用語集

本ガイドで頻繁に使用される用語について以下に説明します。

表 1-1　用語集

用語	解説
スマートフォン	本ガイドは OS として iOS または Android、Windows Phone、BlackBerry を搭載した携帯端末およびタブレット端末を合わせたものを「スマートフォン」と呼びます。 （※本ガイドに記載の対策技術が、適用できない OS もあります。）
脅威	企業の情報資産に害を与える可能性がある望ましくない状況を発生させる要因のことを「脅威」と呼びます。
セキュリティシステム	企業の情報資産に対する安全性向上を実現するシステムです。物理セキュリティシステム、ネットワークセキュリティシステム、ホストセキュリティシステム、アプリケーションセキュリティシステム、データセキュリティシステムがあります。
業務システム	企業において役職員が業務を行うために使用する情報システムを「業務システム」と呼びます。なお、業務システムには以下の「クラウドサービス」と「社内システム」の２種類があるものとします。
クラウドサービス	業務システムのうち、パブリッククラウド上で稼動している情報システムを「クラウドサービス」と呼びます。パブリッククラウドとは、マルチテナントで動作しており、基本的にカスタマイズはせず、利用企業へ共通の機能を提供する SaaS や PaaS を想定しています。また、本ガイドでは「クラウドサービス」はビジネスシーンにおいて利用するものを対象とし、コンシューマ利用のサービスは対象としないこととします。
社内システム	業務システムのうち、導入企業専用に構築または開発された情報システムを「社内システム」と呼びます。稼動している設備は、オンプレミス型以外にホスティングや IaaS、場合によっては PaaS を利用している場合も想定しています。

本ガイドにおける「業務システム」「クラウドサービス」「社内システム」のスコープについて、概念図を以下に示します。

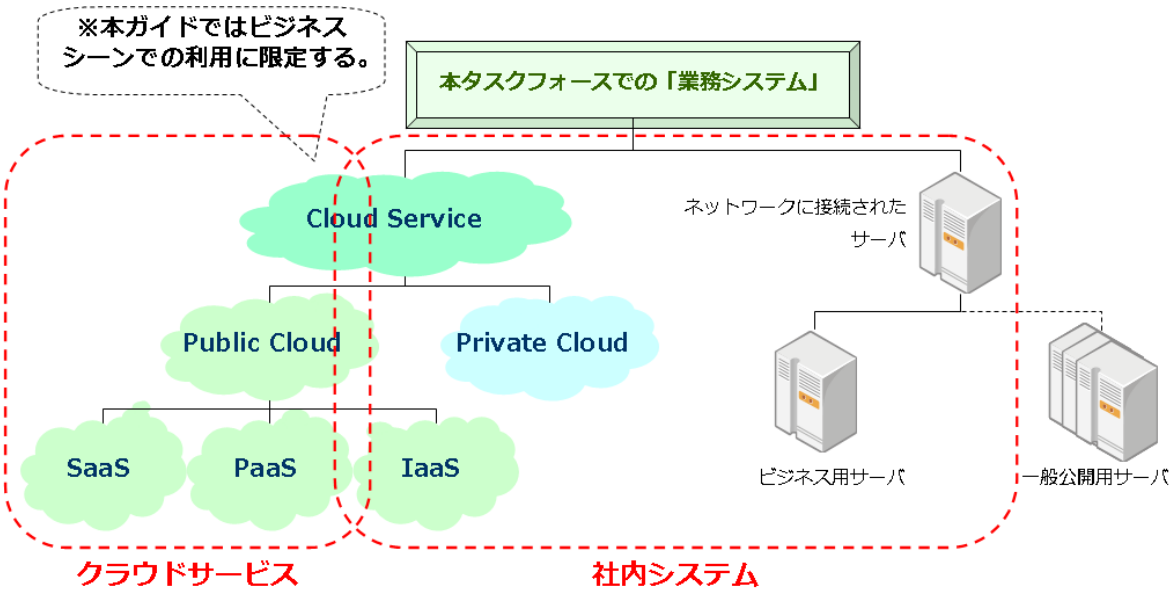


図 1-6　本ガイドにおける「業務システム」「クラウドサービス」「社内システム」の概念図

All rights reserved (c) Japan Smartphone Security Association

2. スマートフォンの業務利用における考え方

2.1. 本章の位置づけ

本章では以後の３～５章の前提となるスマートフォンの業務利用における考え方について、以下の順で説明します。

まず、「2.2 節 背景」でスマートフォンの業務利用における市場動向などを紹介します。

次に「2.3 節 システムセキュリティの検討」で「保護対象の把握→脅威の洗い出し→対策の検討」の順にセキュリティの考え方を説明します。

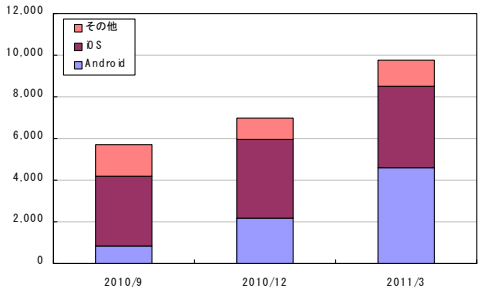
「2.4 節 システムアーキテクチャの検討」では具体的なシステム検討の手順を示します。

最後に「2.5 節 スマートフォンと業務システムに関する考察」では、ここまでの整理から、スマートフォンと業務システムの関係についてまとめ、今後の動向の予想について紹介します。

2.2. 背景

最初にスマートフォンの業務利用における市場動向などを紹介します。

（1）スマートフォンに関する現状

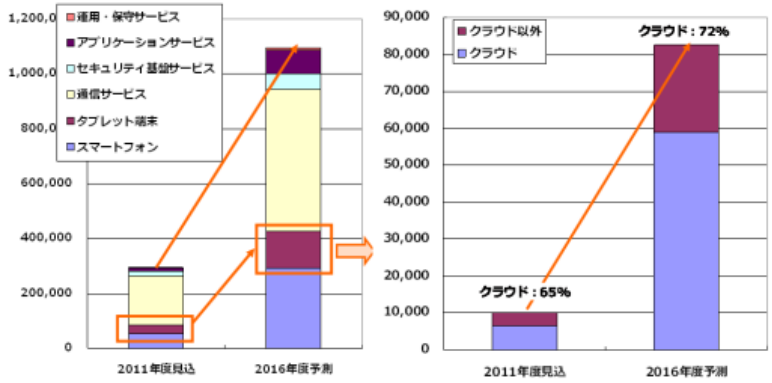


解説

Android、iOS、その他 OS 合わせて、スマートフォンの国内利用者数は 4 半期単位で急増しています。また、OS については Android の比率が大きく増加しています。

図 2-1　スマートフォンの国内利用者数（出典：2012 年 コムスコア・ジャパン株式会社）

（2）スマートフォンのビジネス市場（2011 年→2016 年）



解説

スマートフォン向けのビジネス市場は今後大きく拡大する見込みとなっています。また、その中でもクラウドサービスを利用する比率が高くなることが想定されます。

図 2-2　スマートフォンのビジネス市場規模（左）とその中のアプリケーション市場規模（右）
（出典：富士キメラ総研　2012 法人向けスマートデバイス関連ビジネスの全貌）

All rights reserved (c) Japan Smartphone Security Association

（3）ビジネスにおけるスマートフォン導入上の課題

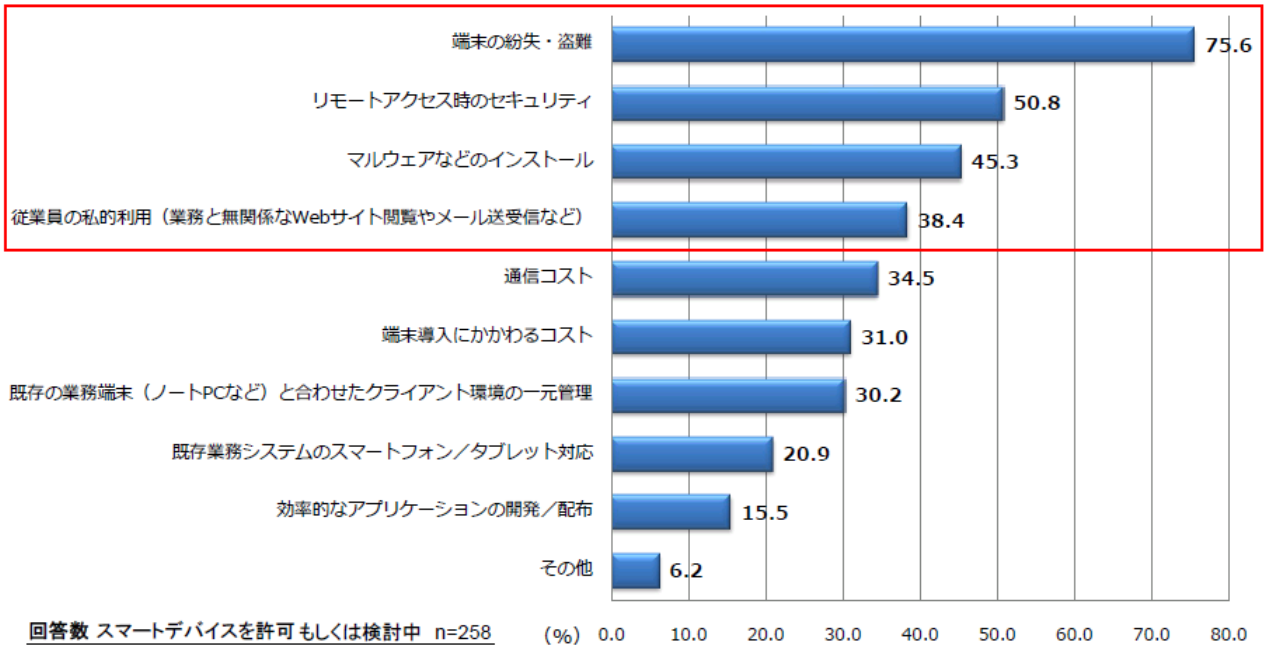


図 2-3　スマートフォンの導入を許可しているもしくは許可を検討している企業の心配事項

（出典：TechTarget ジャパン　44.6%の企業はスマートデバイス導入も、「端末の紛失・盗難」に不安）
http://techtarget.itmedia.co.jp/tt/news/1106/29/news03.html

解説

導入に際しての懸念事項として上位 4 件がセキュリティに関するものが挙げられています。

（4）セキュリティ問題の現状と、その中での JSSEC の役割

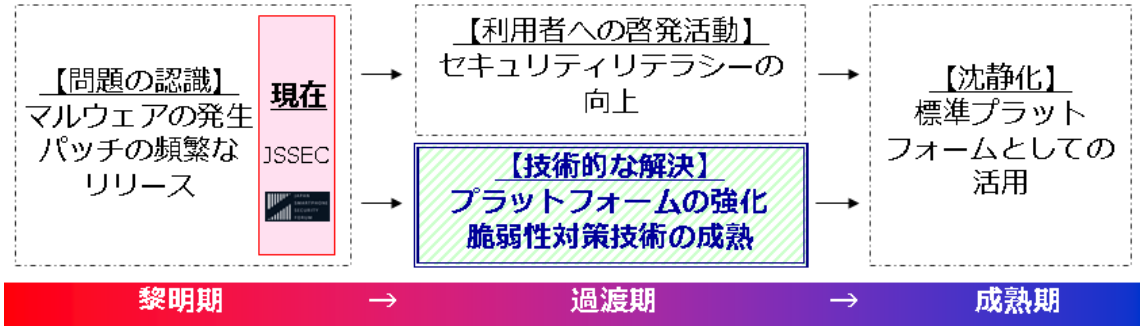


図 2-4　JSSEC 技術部会が担当している役割

解説

JSSEC 技術部会ではプラットフォームの強化や脆弱性対策技術の成熟化など、技術的な解決策の検討と提言の作成を目標として活動を進めています。

これらの背景をふまえつつ、次節以降では実際にスマートフォンを企業に導入する際に行うべきセキュリティ対策の検討手順について、順を追って説明していきます。

All rights reserved (c) Japan Smartphone Security Association

2.3. システムセキュリティの検討

2.3.1. 保護対象の明確化

セキュリティ対策を検討するにあたり、最初に何を守るかを明らかにする必要があります。その際に使用する分類基準の例を以下に示します。この中から例えば「レベル３以上のものはセキュリティ保護対象とする」というように評価と選定を行い、安全と呼べる基準を明確にします。

表 2-1　企業の情報資産の分類例

分類	概要	顧客情報の例	技術情報の例	経営情報の例
レベル４	経営に甚大な損失・事業の継続に深刻な影響を及ぼす	多数または、機微な情報を含む顧客情報	新製品に関する情報	中長期的な経営に関する情報
レベル３	経営に多大な損失を及ぼす	個人情報を含む顧客情報	図面やノウハウなど、製造に関する情報	経理に関する情報
レベル２	経営に軽微な損失を及ぼす。	非公開の顧客情報（組織など個人情報を含まない）	公開予定の情報（特許申請中の情報など）	人事に関する情報
レベル１	経営にも損失を生じない。	公開の情報（取引先社名など）	公開の情報（特許情報など）	公開の情報（売上など）

※情報資産の分類については、JIS Q27002:2006 で標準化されている基準等もあります。どのような基準を適用するかは、自社の文書管理規定やセキュリティポリシーとも照らし合わせて判断してください。

2.3.2. 脅威の洗い出し

次にスマートフォンの業務利用における脅威を明らかにします。セキュリティガイドラインの「利用シーン別対策チェックシート」（p.28～31）から、業務システムに関して想定される脅威を抽出しました。

表 2-2　セキュリティガイドラインから抜粋した業務利用シーンにおける脅威一覧

分類	利用シーン	脅威
社内システム	SaaS/ASP サービスを利用する	不正利用／なりすまし
	アプリケーションを利用する（ネイティブ）	誤操作／知識不足／マルウェア／不具合
	アプリケーションを利用する（WEB）	誤操作／知識不足／設定ミス／外部からの攻撃
クラウドサービス	アドレス帳を利用する	誤操作／知識不足／プライベートデータの混在
	メールを利用する	不正利用／誤操作／プライベートデータの混在
	スケジュールを利用する	誤操作／知識不足／私的利用
	バックアップを取る／同期する	誤操作／知識不足／業務データの混在
	アプリケーションを利用する（ネイティブ）	誤操作／知識不足／マルウェア／プライベートデータの混在
	アプリケーションを利用する（WEB）	誤操作／知識不足／マルウェア／プライベートデータの混在

表 2-2 において「知識不足」「誤操作」「不正利用」という脅威が頻出しています。JNSA の調査によると、パソコンと比較した場合、携帯電話は約 2 倍程度の紛失の確率があります。アドレス帳や通話履歴など、企業にとって重要なデータを保持していることを考慮すると、「紛失」も重大な脅威となり得ます。（なお、会社貸与端末の方が紛失しやすいという調査結果もあります。）

表 2-3　紛失・盗難の年間発生確率

調査対象	年間発生確率
携帯電話	6.5%
パソコン	3.5%
USB メモリ	4.5%

（出典：JNSA　情報セキュリティインシデントに関する調査報告書 ～発生確率編～から抜粋 ）

また、JNSA の個人情報漏えいに関する調査からもインシデント（事故）の８割前後は「知識不足」「誤操作」「不正利用」「紛失」によるものと考えることができます

All rights reserved (c) Japan Smartphone Security Association

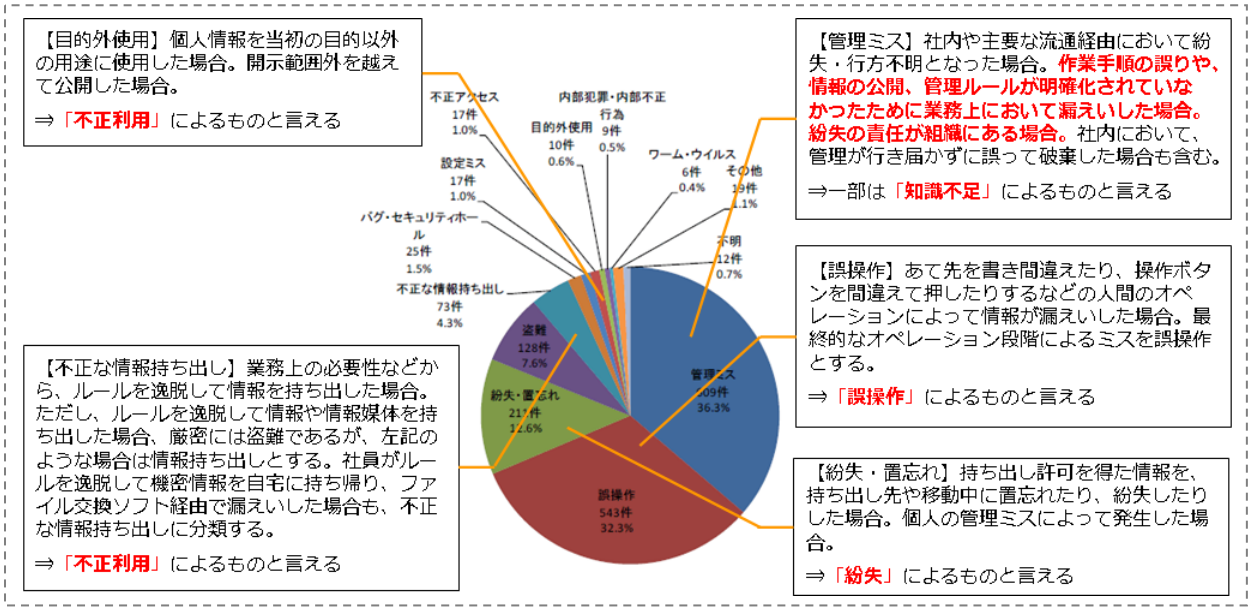
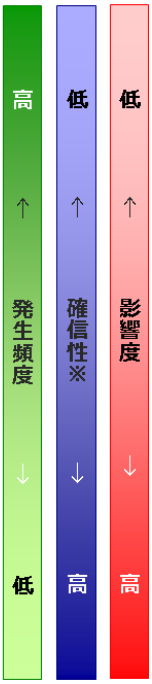


図 2-5　セキュリティインシデントにおける原因分析

（出典：JNSA　2010 年 情報セキュリティインシデントに関する調査報告書　～個人情報漏えい編～）

これらの脅威についてスマートフォンでの具体的なインシデント例を以下に挙げます。

脅威	具体的なインシデント例	イメージ
知識不足	・運用ルールを知らない ・知らずにアドレス帳が同期される ・パッチ情報の見逃し ・管理手順が不明確	運用ルールを知らない
誤操作	・メールの誤送信 ・アプリケーションの操作ミス	メールの誤送信
紛失	・紛失 ・盗難	紛失
不正利用	・画面キャプチャの取得と保存 ・アドレス帳への個人情報の登録 ・安易なパスワード設定 ・設定されたMDMの解除	画面キャプチャの取得と保存

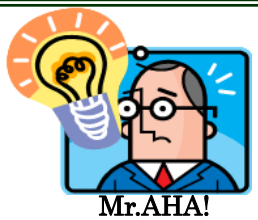


※確信性…行為に及ぶにあたり、その行為の結果（影響）を本人がどれだけ理解（予測）しているか

図 2-6　スマートフォンにおける４大脅威

【重要なポイント】

業務でのスマートフォン利用においても
「知識不足」「誤操作」「紛失」「不正利用」が、
４大脅威と考えることができます。



All rights reserved (c) Japan Smartphone Security Association

2.3.3. 対策に関する本資料のアプローチ

守る対象と脅威が明確になったら、次に対策を検討します。セキュリティ対策には、運用を含む管理的対策と、セキュリティシステムを含む技術的対策がありますが、一般的に管理的対策を先に考えることが重要となります。なお、管理的対策の概要は「セキュリティガイドライン」をご参照ください。

しかし、人が運用するものには必ず「ルールの逸脱」が存在します。特に、スマートフォンではこの「ルールの逸脱」が重要な問題になると想定されます。それはなぜでしょうか？

（1） 一般的に、モバイルデバイスの利便性と安全性は相反する関係があり、利便性を優先すれば安全性が損なわれ、安全性を優先すれば利便性が損なわれこととなります。その中で求められる安全なレベルを維持しつつ、投資対効果が最大になる様に、適切なポイントでバランスを取る事が重要です。

（2） 携帯電話がスマートフォンになることで、取り扱う情報資産が多くなり、利便性が向上しました。その結果として、より利便性を求める利用者とより情報資産の安全性を求める管理者との間で利害が一致しない状況となりました。

そのため、スマートフォンの業務利用においては、セキュリティシステムの役割が非常に重要になると考えます。セキュリティシステムはいわば「重し」となって、安全性と利便性の最適なバランスを実現するための存在といえます。

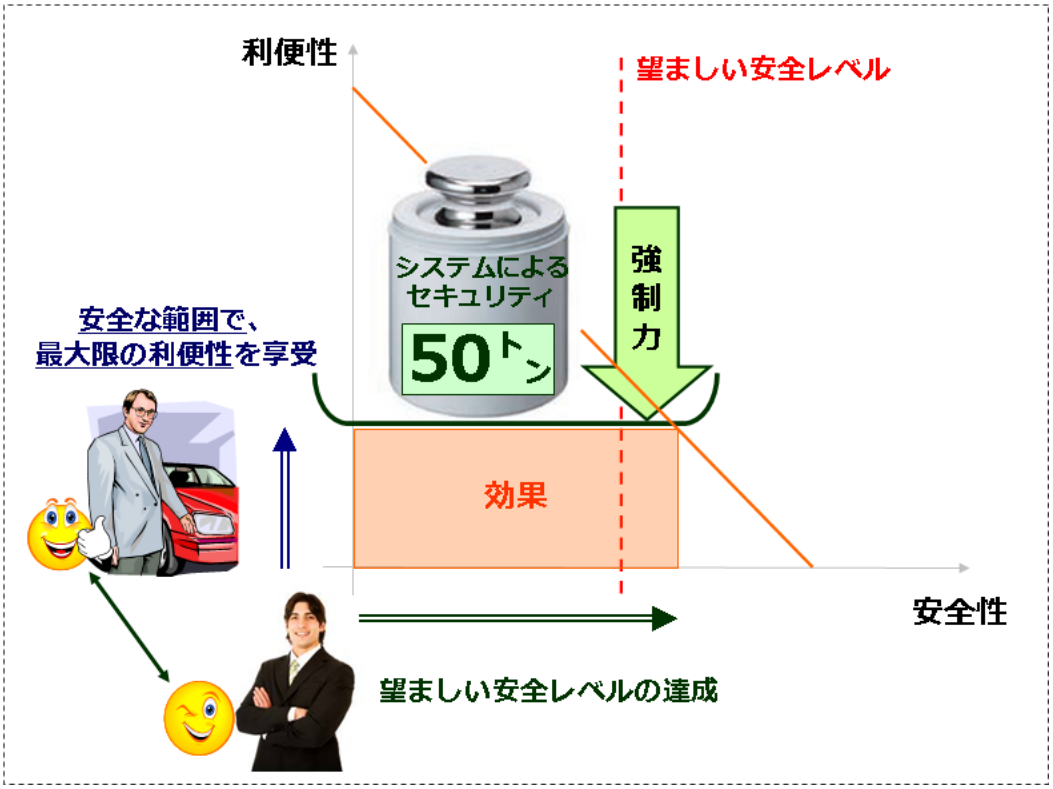


図 2-7　スマートフォンにおけるセキュリティシステムの役割（イメージ）

【重要なポイント】

セキュリティシステム導入の目的は「強制力によって利便性を損なう事」ではありません。
「安全かつ最大限の利便性を提供する事」です。

All rights reserved (c) Japan Smartphone Security Association

2.4. システムアーキテクチャの検討

本節では、「安全かつ最大限の利便性を提供するセキュリティシステム」の検討手順について具体的に説明します。

セキュリティシステムの導入にあたり重要な要件は、求められる安全性と利便性のバランス、そして投資可能なコストです。このコストについて大きな影響があるのが、以下の２つの要素です。

（１） 端末の支給方法：会社貸与か、個人所有の業務利用（以下、BYOD：Bring Your Own Device）か
（２） 業務システムの取得方法：「クラウドサービス」か、「社内システム」か

それぞれの選択肢のメリットとデメリットについては 2.4.2 項と 2.4.3 項で説明します。

【重要なポイント】

端末の支給方法と業務システムの取得方法を
適切に検討する事で、
安全性・利便性・コストの最適な構成を決める事ができます。

2.4.1. システムアーキテクチャ概念図

「端末の支給方法」と「業務システムの取得方法」のバランスについて検討するにあたり、これらの組み合わせについて概念図を示します。

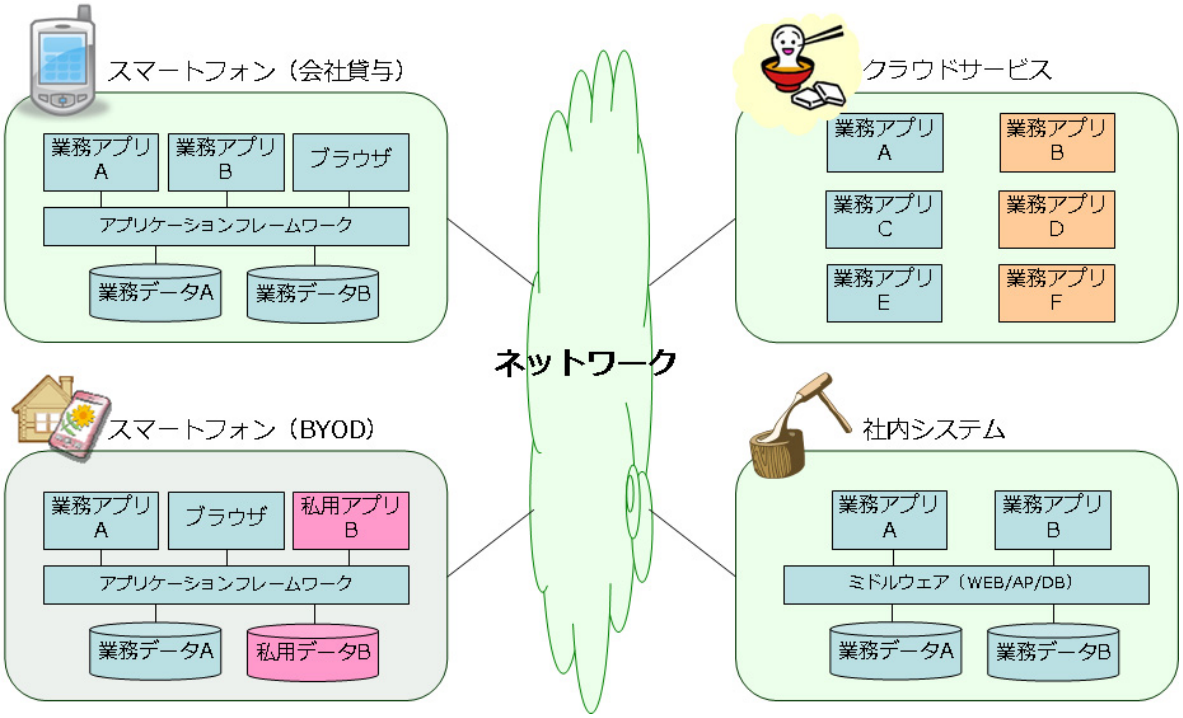


図 2-8　システムアーキテクチャ概念図

All rights reserved (c) Japan Smartphone Security Association

2.4.2. 端末の支給方法について

端末の支給方法については会社貸与だけではなく、BYOD も状況によって有力な選択肢となります。

※重要：本ガイドではどちらかを推奨するものではありません。

表 2-4　端末の支給方法

分類		説明	メリット	デメリット
	会社貸与	企業が初期費と月額費を支払って通信事業者と契約し、社員に端末を配布する	管理性が高い	機種のバージョンアップが追い付かない
	BYOD	個人が契約した端末を業務でも利用できるようにする	コストダウンが図れる 使い慣れているため、業務効率の改善効果が高い	管理性が低い

端末の支給方法に応じた主なセキュリティ対策と対策技術例を以下に挙げます。

表 2-5　端末の支給方法に応じたセキュリティ対策と技術例

支給方法	目的	セキュリティ対策	対策技術例
会社貸与	情報漏えい防止	パスワード義務化	構成プロファイル配布（※1）
			MDM（※2）
			3 要素認証
		画面キャプチャー禁止	構成プロファイル配布（※1）
			MDM（※2）
			3 要素認証
		マルウェア対策	マルウェア対策ソフト
		紛失盗難対策	盗難対策ソフト（※2）
		アドレス帳検疫	3 要素認証
	端末管理	IT 資産管理	MDM（※2）
		モラル管理	構成プロファイル配布（※1）
BYOD	情報漏えい防止	パスワード義務化	構成プロファイル配布（※1）
			3 要素認証
		画面キャプチャー禁止	構成プロファイル配布（※1）
			3 要素認証
		マルウェア対策	マルウェア対策ソフト
		紛失盗難対策	盗難対策ソフト（※2）
		アドレス帳検疫	3 要素認証

※1　構成プロファイル配布によるセキュリティポリシーの適用は iOS のみ対応しています。（2012 年 4 月時点）。

※2　MDM および盗難対策ソフトについては、近日リリース予定のデバイスワーキンググループの公開資料をご参照ください。

「3 要素認証」「マルウェア対策ソフト」については 4 章で紹介します。

【重要なポイント】

どちらの支給方法もメリットとデメリットがあります。
また、業務の内容や使用頻度に応じて両方を使い分けることも有効な場合があります。従って、適切なセキュリティ対策を取りながら最適な配分を検討することが重要です。

All rights reserved (c) Japan Smartphone Security Association

2.4.3. 業務システムの取得方法について

業務システムについても端末支給方法と同様に、メリット・デメリットを把握した上で、適切に組み合わせることが重要です。

表 2-6　業務システムの取得方法

分類		説明	メリット	デメリット
	クラウドサービス	パブリッククラウドまたは外部サーバ上で稼動しているシステム	コストが安い 短期利用が可能 セキュリティがサービスに含まれている（※）	管理性が低い （外部依存のため）
	社内システム	導入企業専用で構築または開発されたシステム	管理性が高い （全体をコントロールできる）	コストが高い （カスタマイズのため） 長期利用が前提

※重要：クラウドサービスが提供するセキュリティについては、サービスごとに十分なチェックが必要です。詳細は 3.3 節をご参照ください。

業務システムの取得方法に応じた主なセキュリティ対策と対策技術例を以下に挙げます。

表 2-7　業務システムの取得方法に応じたセキュリティ対策と対策技術の例

取得方法	目的	セキュリティ対策	対策技術例
クラウドサービス	サービスレベル確認	SLA（特にセキュリティ管理基準）	セキュリティチェックリスト
	不正アクセス防止	認証	パスワード認証
			IP アドレス認証
			シングルサインオン
			端末証明書による認証
			端末固有情報による認証
	データ保護	暗号化	SSL
			VPN
社内システム	不正アクセス防止	認証	パスワード認証（※）
			シングルサインオン（※）
			端末証明書による認証（※）
			端末固有情報による認証（※）
	アクセス範囲の制御	アクセスコントロール	LDAP（※）
	データ保護	暗号化	SSL（※）
			VPN（※）
		データ保存禁止	リバースプロキシ
			シンクライアント
		画面キャプチャー禁止	構成プロファイル（iOS）
			３要素認証

※社内システムにおける記載の対策技術については、ノート PC によるリモートアクセス技術と同等の技術が利用可能です。

上記、青字の技術については 3 章、赤字の技術については 4 章で紹介します。

【重要なポイント】

「クラウドサービス」については、セキュリティ管理基準の確認、「社内システム」についてはセキュリティポリシーに応じた対策の設計および実装が重要となります。

All rights reserved (c) Japan Smartphone Security Association

2.5. スマートフォンと業務システムに関する考察

本章のまとめとして、スマートフォンと業務システムの関係について整理します。

1.2 節で書いたように、スマートフォンから見た場合、通信先の業務システムが「クラウドサービス」であっても「社内システム」であっても意識される事はありません。そして、今後のスマートフォン活用の重要なポイントは、使用する場所（国や地域）も、使用する端末（BYOD も含む）も意識せずに利用できることではないかと考えます。

そのように考えた場合、スマートフォンはコミュニケーションやプレゼンテーションに強みのある「フロントエンドの端末」であり、業務システムは情報の保存場所（ストレージ）や計算処理（コンピューティング）に強みのある「バックエンドの支援サービス」と総称することができると言えます。

図 2-9　スマートフォンと業務システムの役割分担（イメージ）

今後は「BYOD」や「クラウド」といったキーワードにとらわれない、柔軟で多様なサービスやソリューションが登場することが期待されます。その状況では、フロントエンドの端末とバックエンドの支援サービス、それぞれの得意分野を有効に活用し、適切な役割を考える事が業務システムの設計において重要となるでしょう。

そして、いつでもどこからでもアクセスできる業務システムにおいて、安全な利用を実現するセキュリティ技術とは何かを考える事が、スマートフォンの活用において非常に重要なポイントになると考えています。

【ワンポイント】

スマートフォンの業務利用においてはスマートフォンと
業務システムの適切な役割分担が重要であるため、これを
MObile & Cloud Hybrid Integration（ MOCHI ）と名づけ、
本ガイドでは餅をイメージキャラクターとして使用しています。

All rights reserved (c) Japan Smartphone Security Association

3. クラウドサービスセキュリティガイド

3.1. 本章の位置づけ

２章では、スマートフォンのセキュリティを実現する手段として、「クラウドサービス」には以下の特徴があると紹介しました。

表 3-1　クラウドサービスのメリットとデメリット

分類		説明	メリット	デメリット
	クラウドサービス	パブリッククラウドまたは外部サーバ上で稼動しているシステム	コストが安い 短期利用が可能（柔軟性がある） セキュリティもサービスに含まれている	管理性が低い （外部依存のため）

「クラウドサービス」は「所有」から「利用」へ IT リソースを大きく転換できることからスマートフォンの活用の有無に関わらず、導入が進んでいます。「クラウドサービス」を使用するメリットを以下に挙げます。

（１）　IT リソースの調達に関わる負担の軽減
- 機器（サーバ、ストレージ、ネットワーク等）の調達（選定、設置、設定等）が不要
- サービスアプリケーションの調達（選定、開発、設定等）が不要
- 期間限定の業務や、自社開発サービスの稼動までの一時的な利用も可能

（２）　IT リソースの運用に関わる負担の軽減
- 機器やサービスアプリケーションの稼動に係わる各種の運用（OS やアプリケーションのアップデート、トラブル対策・対応、バックアップ、ライセンス管理等）が不要
- ユーザーサポートに関わる各種の運用（アカウント等の運用管理、ヘルプデスク等）負担の軽減
- セキュリティ対策の運用（ウイルス対策、不正アクセス対策、ログ監視等）が不要

また 2011 年に発生した東日本大震災およびその後の電力不足の問題が発生し、BCP の観点からも利用が進んでいます。特に、東日本大震災の際は、クラウドサービス事業者が無償で提供したこともあり、短期的に外部サービスを利用するケースも多くありました。

このように、「クラウドサービス」の利用には多くのメリットがありますが、幾つかの課題もあります。

本章では、これらの課題を認識して頂くために準備段階からサービスの終了までの各フェーズに分けて説明します。

All rights reserved (c) Japan Smartphone Security Association

3.2. クラウドサービス利用のステップ

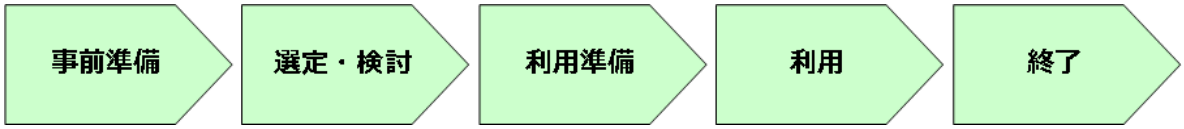


図 3-1　クラウドサービス利用のステップ

企業は多岐にわたる法令の遵守、情報公開、公正な取引など高い企業倫理が求められ、社内規定やセキュリティポリシーを定めています。

「クラウドサービス」を利用するということは、情報資産の保管先や運用の一部に社外リソースを利用するということです。社内規定・情報セキュリティポリシーや運用にまつわるリスクとメリット、コストを踏まえて選定することが重要ですので、事前準備の段階でできる限り検討しておく必要があります。

表 3-2　クラウドサービス利用時の注意すべきポイント

フェーズ	項目	注意すべきポイント
事前準備	クラウドサービスの利用目的・対象業務の設定	取扱うデータの重要度
		コンプライアンス上のリスク
		セキュリティポリシーとの整合性
選定・検討	クラウドサービスが利用目的・対象業務に合致しているか	クラウドサービスの動作
		データの管理
	クラウドサービスおよび提供事業者の信頼性（SLA 等を含め）	実績・情報公開度
		サービスレベル
利用準備	既存サービスとの互換性	データの移行
		管理項目（アカウント等）
運用	クラウドサービスに関わる各種の管理と運用	管理項目の運用
		データの管理（バックアップ等）
		障害時の対応方法
終了	データの削除	クラウドサービス終了時の事業者側でのデータ削除の証明
	データの移管	クラウドサービスの移管を想定し、終了時のデータの入手

（1）　事前準備

「クラウドサービス」の利用目的・対象業務を明確にし、そのサービスにおいて取り扱う情報の重要度を定義します。重要度により、セキュリティポリシーとの整合性（情報漏えい事故への対応等）、コンプライアンスの対応等が異なると想定され、「クラウドサービス」に要求する仕様が変わる可能性があります。以下にコンプライアンス上のリスクの例を挙げます。

- クラウドサービスを利用することにより、リスクマネジメントの方針・体制・運用の方法が変わる可能性があります。
- 個人情報保護法におけるガイドラインにおいて、個人情報の委託に係わる指針を定義しているガイドラインが関係する可能性があります。
- 国外のデータセンターを利用するクラウドサービスや、クラウドサービスを海外で使用する場合、貿易関連法（外国為替、外国貿易法）を遵守する必要があります。
  ※サービス事業者が国外の事業者であるなど、国外のデータセンター（PaaS/IaaS も含む）の場合、監査において、それぞれの国の法律が適用される可能性があります。
- その他、対象業務（対象データ）によりｅ－文書法など考慮しなければならない法律があれば遵守する必要があります。

All rights reserved (c) Japan Smartphone Security Association

（2） 選定・検討

「クラウドサービス」の選定にあたっては、利用目的・対象業務に合致するかどうかに加え、それ以外にもデータ（クラウドサービス上に保持される）の取り扱いにも考慮する必要があります。例えば、個人情報が含まれている場合、個人情報保護に関するガイドラインにおいて規定された技術的対策を満たしているか、例えば、営業機密が含まれている場合、機密情報として管理できるかなどです。

クラウドサービス事業者の信頼性については、事業者の実績や評判を評価します。また「クラウドサービス」の信頼性については、サービス稼動実績などを評価します。

IPA（独立行政法人情報処理推進機構）が作成した「クラウド事業者による情報開示の参照ガイド」では事業者から提供されることが望ましい項目が網羅されているので、参照して下さい。また、FMMC（一般財団法人マルチメディア振興センター）が行う「ASP・SaaS 安全・信頼性に係る情報開示認定制度」は、事業者やサービスを比較、評価、選択する際に必要な「安全・信頼性の情報開示基準を満たしているサービス」を認定する制度です。認定を受けたサービスは、事業者情報を含めた詳細情報が公表されていますので、参考にして下さい。

表 3-3 クラウドサービスの選定にあたり、参考となるガイドライン一覧

公開主体	公開月	名称
経済産業省	2008/01	SaaS 向け SLA ガイドライン
総務省	2008/01	ASP・SaaS における情報セキュリティ対策ガイドライン
経済産業省	2011/04	クラウドサービスの利用者のための情報セキュリティガイドライン
IPA	2011/04	中小企業のためのクラウドサービス安全利用の手引き
IPA	2011/04	クラウド事業者による情報開示の参照ガイド
ASPIC	2011/07	クラウドサービス利用者の保護とコンプライアンス保護のためのガイド

具体的に必要なセキュリティ対策技術については 3.3 節以降をご参照ください。

（3） 利用準備

「クラウドサービス」を選定した後、導入にあたり、利用の準備を行います。ユーザーへの教育やヘルプデスクの用意、データの準備やバックアップ体制・方法などを検討します。

利用時には、「社内システム」と違い運用をクラウドサービス事業者が行うことから、さまざまな業務（監視、障害対応、バックアップ、保守）の運用方法が変わります。サービスのバージョンアップひとつとっても、適用はクラウドサービス事業者の都合によります。運用がどのように変わり、ユーザーへのサービス提供にどのように影響するのか、確認して、情報システム部門の対応を検討します。また、障害発生時（サービスの障害だけでなく、情報漏えい発生時も含め）のクラウドサービス事業者も含めたサポート体制（連絡先や受付時間等）を確認しておくとよいでしょう。

（4） 利用

クラウド事業者が事前に契約したサービスレベルに準じた運用を行っているか、レポート等を使用して定期的に確認します。また、クラウドのメンテナンスのために対応が必要となる場合があります。

（5） 終了

「クラウドサービス」の終了時には、クラウドサービス側の完全なデータの削除が必須です。事業者

All rights reserved (c) Japan Smartphone Security Association

がデータを削除したことの証明を入手できるように契約時に確認することを推奨します。また、対象業務（サービス）を「社内システム」、他の「クラウドサービス」に切替える場合、当該事業者からデータを提供してもらえるように契約時に確認することを推奨します。

3.3. クラウドサービス選定チェックリスト

以降の節では、「クラウドサービス」を選定する際に重要となるセキュリティ技術について紹介します。最初に、それらセキュリティの技術についてチェックリストを以下にまとめます。

表 3-4　クラウドサービスのセキュリティチェックリスト

項番号	技術名	重要度
3.4.1	パスワードによる認証	◎
	通信経路の暗号化	◎
	アクセスログの記録と提供	◎
3.4.2	IP アドレスによるアクセス制限	○
3.4.3	シングルサインオンによる認証	○
3.4.4	クライアント証明書による認証	○
3.4.5	端末固有情報による認証	△

◎：必須　　○：推奨　　△：推奨（課題あり）

上記の表において、必須（◎）の技術については、どのような「クラウドサービス」を利用する場合も必ず必要な技術となります。

推奨の技術（○、△）については、必須技術と併せて利用する事により、さらにセキュリティを向上できる技術となります。

これらセキュリティ技術に対応した「クラウドサービス」を選定する事による脅威への効果は以下のようになります。

表 3-5　４大脅威への効果

脅威	本技術による効果
知識不足	クラウド事業者がユーザー向けマニュアルなどを用意しているので教育が容易です。また、操作性が標準的で初心者にも使いやすいという利点もあります。
誤操作	データがクラウド上に保存されるため、誤操作による影響が限られていると考える事ができます。
紛失	データがクラウドサービス上に保存されているため、紛失・盗難があってもクラウドサービス上でデータ保護対策を取る事ができます。
不正利用	データがクラウド上にあるため、利用履歴をすべてログに記録しておくことが可能となり、不正の抑止力となります。

All rights reserved (c) Japan Smartphone Security Association

3.4. 技術紹介

3.4.1. 最低限必要なセキュリティ対策

「クラウドサービス」を利用するにあたり最低限必要なセキュリティ対策として以下の３つが挙げられます。

（１）パスワードによる認証
（２）通信経路の暗号化
（３）アクセスログの記録と提供

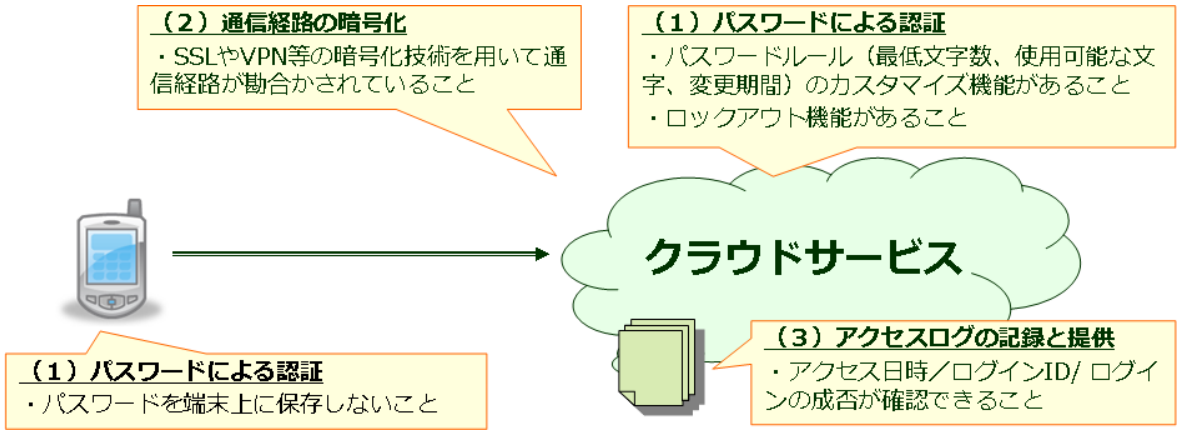


図 3-2　クラウドサービス利用にあたり最低限必要なセキュリティ技術

3.4.2. IP アドレスによるアクセス制限

「クラウドサービス」にアクセスする前に必ず、「社内システム」に VPN 接続した上で、プロキシサーバなどを経由して特定の IP アドレスからアクセスするようにします。「社内システム」が必要となりますが、IP アドレスによるアクセス制限に対応している「クラウドサービス」は比較的多いため、多様なサービスが利用可能となります。なお、携帯電話網でも携帯電話事業者が提供している閉域網サービスの場合、IP アドレスが特定できる場合もあります。

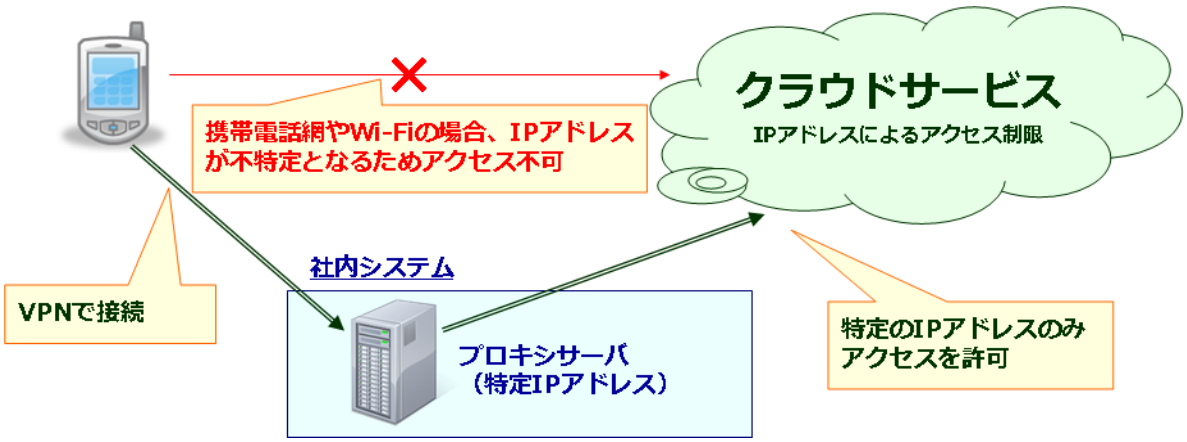


図 3-3　IP アドレスによるアクセス制限

All rights reserved (c) Japan Smartphone Security Association

3.4.3. シングルサインオンによる認証

クラウドサービス側で SAML などのシングルサインオン認証に対応している場合は、自社設備、または外部のシングルサインオンサービスを利用することで、一元化した認証によるアクセスが可能となります。

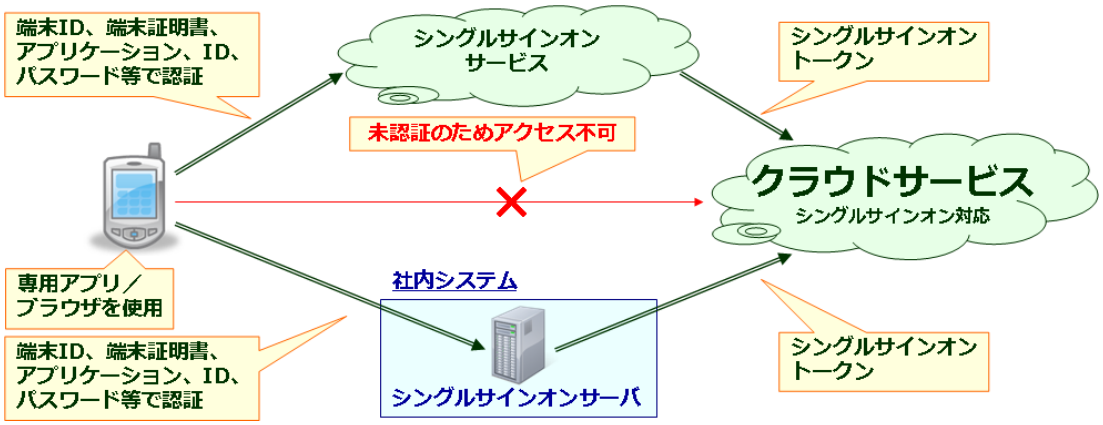


図 3-4　シングルサインオンによる認証

3.4.4. クライアント証明書による認証

クラウドサービス側で証明書認証に対応している場合は、事前にクライアント証明書をクラウドに登録しておくことで証明書認証によるアクセスが可能となります。

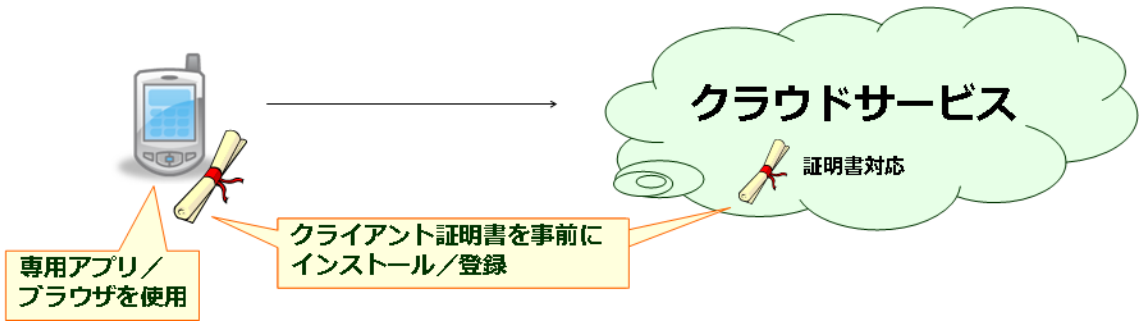


図 3-5　クライアント証明書による認証

3.4.5. 端末固有情報による認証

業務利用で事前にアクセス端末が特定できている場合、端末固有番号（IMEI／IMSI など）のハッシュ値を登録することで認証を行うことも可能です。ただし、現時点では一部 OS・端末の場合、これら端末固有番号（IMEI／IMSI など）を改変できてしまい、セキュリティホールとなりうるため注意が必要です。

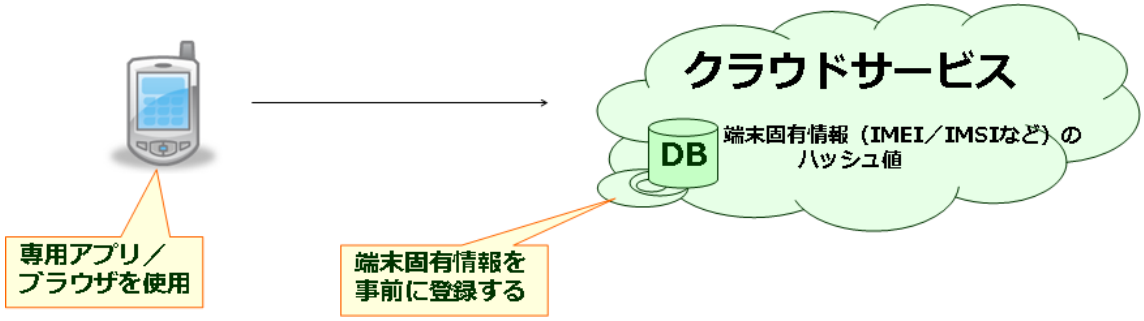


図 3-6　端末固有情報による認証

All rights reserved (c) Japan Smartphone Security Association

4. 社内システムセキュリティガイド

4.1. 本章の位置づけ

２章では、スマートフォンのセキュリティを実現する手段として、「社内システム」には以下の特徴があると紹介しました。

表 4-1　社内システムのメリットとデメリット

分類		説明	メリット	デメリット
	社内システム	導入企業専用で構築または開発されたシステム	管理レベルが高い 既存資源が活用できる	コストが高い （カスタマイズなため） 長期利用が前提

「社内システム」のセキュリティ対策は、コンピュータが導入された当初の物理的セキュリティ対策から始まり、その後の OA 環境のネットワーク化、インターネットとの接続を経て様々な技術が導入されてきました。

オフィス内でのフリーアドレス化や在宅勤務など、様々なワークスタイルが導入されてきている中で、リモートアクセス、認証、マルウェア対策など社内ネットワークへの接続とセキュリティ対策についてより重要度が増してきています。

4.2. 社内システムのセキュリティ対策導入ステップ

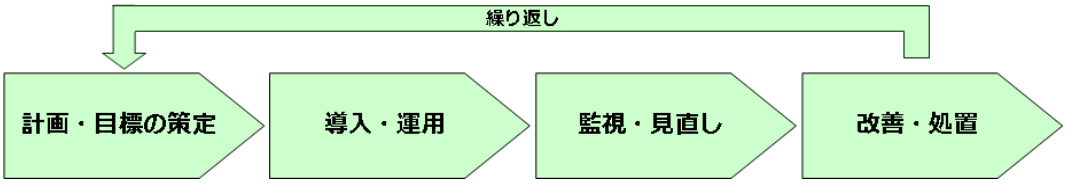


図 4-1　社内システムのセキュリティ対策導入ステップ

「社内システム」のセキュリティ対策導入プロセスとしては、ISMS（情報セキュリティ管理システム）が一般的に広く採用されています。ISMS に準じた検討プロセスの概要を以下に示します。

表 4-2　社内システムのセキュリティ対策導入時の注意すべきポイント

フェーズ	項目	注意すべきポイント
計画・ 目標の策定	情報セキュリティ基本方針の策定	アクセスポリシーの策定
		体制の策定
		防御方針の策定
		改善プロセスの策定
導入・運用	リスク分析・評価・目標設定 リスク対策の策定	リスク評価方式の策定 リスクの低減・保有・回避・移転・受容の判断
	運用	セキュリティ方針に則った運用実態の確認
監視。見直し	監査 プロセスの評価 基本方針の見直し	監査計画の策定
		監査の実施
改善・処置	プロセスの改善	改善計画の策定
		改善実施の判断

※ISMS による検討プロセスの詳細は各 ISMS 解説書をご参照ください。

All rights reserved (c) Japan Smartphone Security Association

4.3. 社内システムのセキュリティ対策におけるポイント

スマートフォン導入における「社内システム」のセキュリティ対策については、ノート PC 導入の際に活用した技術と同等の技術が利用可能です。ただし、ノート PC とスマートフォンの特性の違いについて、十分に理解し、その特性に応じた対策を実施することが重要です。

以下にノート PC とスマートフォンの主な特性の違いを挙げます。そして、以降の節でこれらに対して有効なセキュリティ対策技術を紹介します。

（1） BYOD

従来のノート PC ではなかった BYOD による端末利用の場合、端末を完全にコントロールするような対策を取る事が難しい場合があります。

⇒「３要素認証」、「シンクライアント」

（2） リソース不足

スマートフォンでは、CPU の処理能力や電池容量などノート PC よりもリソースの制限が厳しいケースがほとんどです。そのため常駐型のアプリケーションの稼動に制約があります。

⇒「マルウェア対策（サーバー型）」、「シンクライアント」

（3） データの多様性

位置情報や通話履歴など、アプリケーションから利用できるデータの多様性が大きく増しています。また、業務資料など重要な資料を持ち出す機会も多くなります。これはマルウェアによる情報漏えいによる影響が大きくなる事を意味しています。

⇒「マルウェア対策」、「シンクライアント」

（4） ユーザーインターフェースの違い

タッチパネルで操作する事が多いスマートフォンでは、マウスとキーボードを前提としている PC 型のユーザーインターフェースが適切ではなく、誤操作による情報漏えいを招く場合があります。

⇒「リバースプロキシ」

なお、これらの技術は単独で使用するだけではなく、組み合わせることによって、より高度なセキュリティを実現することが可能です。

All rights reserved (c) Japan Smartphone Security Association

4.4. 技術紹介

4.4.1. ３要素認証

表 4-3　４大脅威への効果

脅威	本技術による効果
知識不足	利用者が運用ルールを把握していなくても、セキュリティシステムがルールを強制することにより社内データの安全を守る事ができます。
誤操作	誤操作により端末設定が意図しない変更をされた場合はアクセス制限することによりセキュリティを保つ事ができます。
紛失	端末内にデータが保存されない環境を担保できるため、紛失してもデータが漏えいしません。
不正利用	不正利用された場合は社内システムへのアクセスを拒否する事ができるため、ポリシーを強制することができます。

従来の端末単体常時監視ではセキュリティの設定が維持されていることを保証できず、一方で MDM による監視では、ユーザーがオフにできる、監視のタイムラグがあるなどの課題があります。

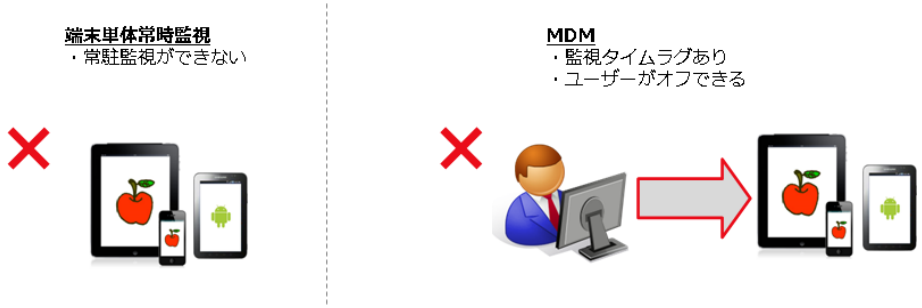


図 4-2　従来型監視技術の課題

それに対して 3 要素認証では、認証時に端末のセキュリティステータスを確認することにより、端末のセキュリティが不正な状態では社内へのアクセスを拒否することにより、情報漏えい防止に効果を発します。

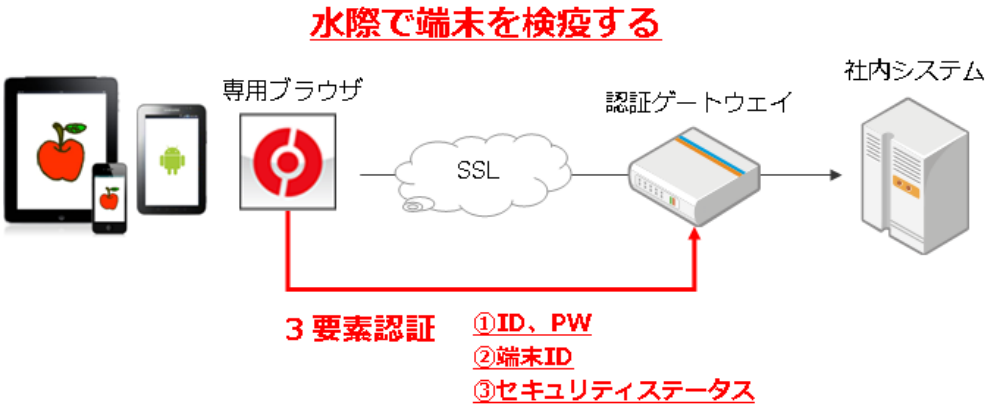


図 4-3　３要素認証技術による解決

【重要なポイント】

端末をクリーンにするという MDM のアプローチとは逆に、
クリーンな状況であると認定しないと社内に接続しないという発想

All rights reserved (c) Japan Smartphone Security Association

4.4.2. マルウェア対策（サーバー型）

表 4-4　4 大脅威への効果

脅威	本技術による効果
知識不足	電池消費や操作上の不便さを気にせずにマルウェア対策を行う事ができるため危険なアプリケーションのインストールを防ぐ事ができます。
誤操作	パターンファイルを必ず更新できるため、更新漏れによるチェック漏れを防ぐ事ができます。
紛失	―
不正利用	インストールされたアプリケーションリストがサーバーに保存されるため、不正利用を監視・検知することができます。

従来の PC で使用していたマルウェア対策はスマートフォンでも同様に利用可能ですが、CPU や電池容量などリソースが限られているスマートフォンでは利便性を損なう場合があります。そのような場合に有効な技術としてマルウェア対策（サーバー型）があります。なお、本技術はオンプレミスのサーバー型だけではなく、クラウド型のサービスとしても提供されています。

特徴

（1）　低消費電力

アプリケーションのインストール、アンインストール時、およびクラウドとの通信時にのみ動作し、それ以外はスリープ状態です。また、ウイルス情報や解析エンジンはサーバー側にあり、スキャンもサーバーで行います。端末側での動作を最小限にすることで、消費電力を低減します。

（2）　未知/新種不正アプリケーションへの対応

クラウド上で端末がインストールしたアプリケーションの履歴を管理しているため、インストール時にはマルウェアと判断されなかったアプリケーションが、後にマルウェアと判断した場合、さかのぼって該当ユーザーに警告する、「さかのぼり検知」が可能です。検知エンジンは、アプリケーションを構成する部品（メタデータ）で検知をする「ヒューリスティック検知」を使用することにより、一部分を変更しながら増殖する、亜種や変種のマルウェアにも素早く対応が可能です。また、該当するアプリケーションがアンインストールされてしまっている場合でも通知を行うことができます。

（3）　クラウドでの一括管理による端末負荷の軽減

ウイルス情報（シグネチャ）の管理は、サーバーで行います。そのため全てのユーザーが常に最新の「ウイルス情報」 を共有するので、端末ごとの更新は不要です。また、端末がインストールしているアプリケーションの情報も、サーバーで一括管理されています。既に登録されているアプリケーションを他の端末がインストールしようとした際には、スキャンをせずに「安全」「危険」を判断することが可能です。

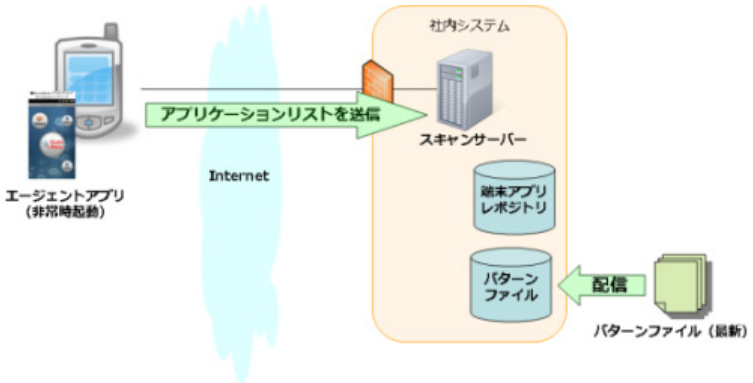


図 4-4　マルウェア対策（サーバー型）による解決

All rights reserved (c) Japan Smartphone Security Association

4.4.3. シンクライアント

表 4-5　4 大脅威への効果

脅威	本技術による効果
知識不足	社内のデスクトップ PC の環境と同一の環境を利用した業務遂行が可能となるため、追加の利用者教育を最小限に抑えることが可能です。
誤操作	社内システムと同様のユーザーインターフェースを提供するため従来の操作感で使用できます。
紛失	情報をスマートフォン側にダウンロードすることができないため、万が一紛失した場合も情報の漏えいを防止することが可能です。
不正利用	社内システムのセキュリティ対策がそのまま適用されるため、不正利用のリスクを社内と同等レベルに低減することが可能です。

コンセプト

スマートフォンをシンクライアントとして、社内のデスクトップ環境を利用します。それによって、スマートフォンからの社内システム（社内リソース全て）の利用を、社内デスクトップ環境と同一にすることができます。

特徴

一般的なシンクライアントと同様に、スマートフォン側への情報の持ち出しを防止します。また、スマートフォン用に社内システムアプリケーションの開発を実施せずに済むため、導入コストが低く抑えられます。業務システムの利用方法が、社内デスクトップ環境と同様であるため、利用者側への追加の教育が最小限に抑えられます。

適用性の高い導入ケース

業務システムが多く存在している場合であっても、既存の業務システムに手を入れることなく、セキュアなアクセスが可能となる場合があります。特に、業務システムのスマートフォン向けのカスタマイズが困難な場合に有効です。

利用手順

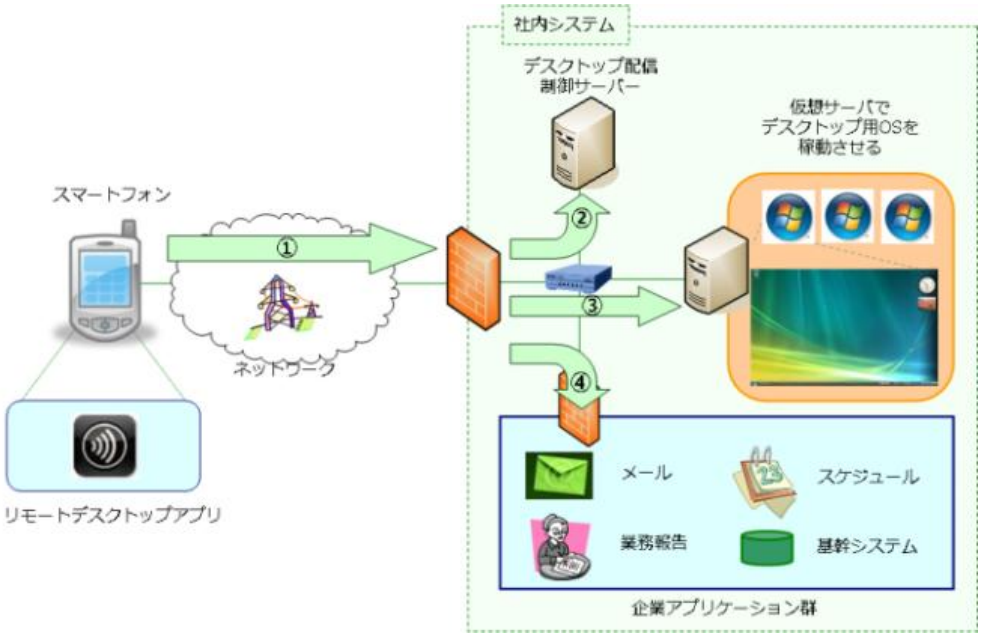


図 4-5　シンクライアントの利用手順

All rights reserved (c) Japan Smartphone Security Association

①社内システムに VPN で接続します。
②端末の認証を行い、識別された端末・ユーザー情報によって、デスクトップ配信制御サーバーから適切なデスクトップ環境が選択されます。
③サーバー上で稼動している仮想デスクトップ OS に接続します。
④仮想デスクトップ経由で、社内の企業アプリケーションを利用する事が可能となります。
※手順②、③を省略し、スマートフォンから社内のデスクトップに直接接続する方法も可能です。

課題

スマートフォンによるシンクライアント利用については、現状では主に Windows 系 OS をスマートフォンから操作することで、社内デスクトップと同様の環境を外部からアクセス可能とするケースが多いようです。ただし、Windows は原則としてマウスとキーボードを前提とした OS およびユーザーインターフェースとなっており、スマートフォンのような小型のディスプレイからタッチ操作によって利用する事は想定されていないため、スマートフォンからは操作が難しいという課題があります。

この問題の解決のために、スマートフォン利用を想定した OS によるリモートデスクトップの提供が期待されています。

図 4-6　シンクライアントの現状の課題

現在においては、タブレットなど比較的画面サイズの大きい端末において、従来の Windows アプリケーションを短い準備期間で利用可能としたい場合に、有効な技術と位置づけられます。その場合も導入に際して操作感に問題が無いか、十分な検証が必要と考えています。

All rights reserved (c) Japan Smartphone Security Association

4.4.4. リバースプロキシ

表 4-6　4 大脅威への効果

脅威	本技術による効果
知識不足	端末アプリ上の 1 つのアプリを業務システムの入り口とすることで、思わぬ操作による端末経由のデータ漏えいを未然に防ぐことができます。
誤操作	リバースプロキシが提供するスマートフォン向けユーザーインターフェースにより、フリックやピンチイン・ピンチアウトなど、コンシューマ向けアプリと同じ操作感で使用する事ができます。
紛失	リバースプロキシは認証・認可を必ず行うため、紛失した端末からのアクセスを拒否する事ができます。
不正利用	操作は全てリバースプロキシ経由で行われるため、業務システムへのアクセスはすべて記録を残すことが可能であり、抑止力となります。

リバースプロキシはスマートフォン専用の技術ではなく、外部からアクセスのある一般的なネットワークにおいて、内部サーバーの代わりに応答することによりセキュリティを高める際に用いられます。

特徴

リバースプロキシは、不特定多数のクライアントから寄せられる要求に対して、応答を肩代わりすることにより特定のサーバーの負担を軽減したり、アクセスを制限することにより特定のサーバーのセキュリティを高めたりする目的に用いられます。一般的に SSL または VPN の機能を持っており、社内システムの入り口とすることで防御が一段階増やすことが可能となります。また、リバースプロキシに認証・認可の機能を持たせることもでき、背後に複数台のサーバーがある場合には認証・認可を行うことでシングルサインオンを実現することもできます。

スマートフォンに特化したリバースプロキシの特徴として、本来 PC 向けに作成された WEB ページをスマートフォンの画面サイズ・ユーザーインターフェースに適合するように自動で変換する「コンテンツ変換」機能を持つことにより、さらに低コストでスマートフォンからのリモートアクセスを実現する機能を持つものも存在します。

適用性の高い導入ケースとしてはメールやイントラなど既存の業務システムが存在していて、スマートフォン専用の設備を用意したくない場合に、リバースプロキシを導入することで、既存の業務システムに手を入れることなく、セキュアなアクセスが可能となる場合があります。

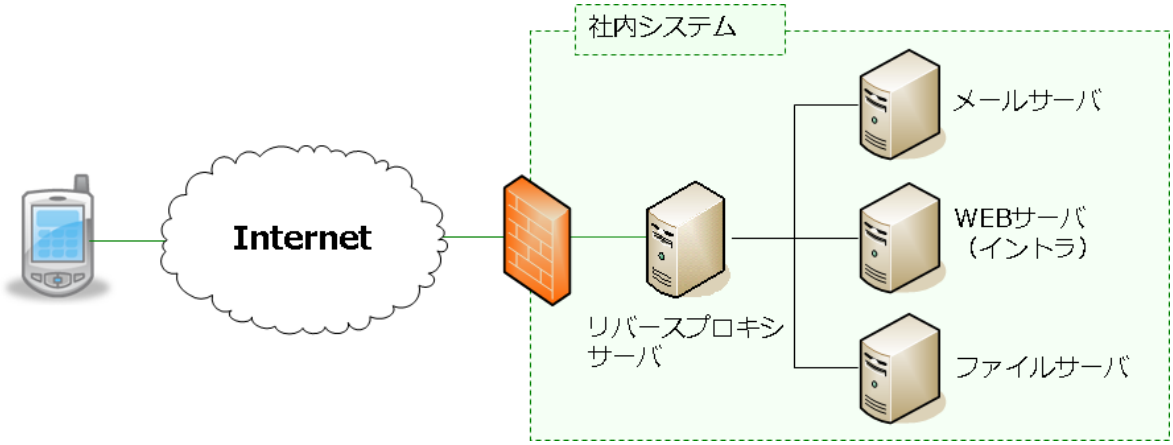


図 4-7　リバースプロキシ導入イメージ

All rights reserved (c) Japan Smartphone Security Association

5. システムインテグレーションガイド

5.1. 本章の位置づけ

3 章および 4 章では、スマートフォンのセキュリティを実現する業務システムとして「クラウドサービス」と「社内システム」に分類し、それぞれのセキュリティに関して考慮すべき点についてまとめました。

2.5 節で、スマートフォンはコミュニケーションやプレゼンテーションに強みのある「フロントエンドの端末」であり、スマートフォンからみた業務システムは、情報の保存場所（ストレージ）や計算処理（コンピューティング）に強みのある「バックエンドの支援サービス」と総称することができると記載しました。そして、今後はさらに柔軟で多様なサービスやソリューションが登場することが期待されます。

そこで、本章ではスマートフォンと「クラウドサービス」によって、どのように業務の効率化を実現できるか、モデルとなるソリューションについて紹介します。これらのソリューションでは本ガイドの 3 章および 4 章で紹介した技術を使用して安全性にも配慮しています。

これらの情報がスマートフォンを利用した業務改善の新しいヒントとなり、セキュリティ対策と合わせて、それぞれの企業の状況に合わせてソリューションの検討をする際のお役に立てればと考えています。

All rights reserved (c) Japan Smartphone Security Association

5.2. ソリューション紹介

5.2.1. 紙媒体持ち出しリスクの低減ソリューション

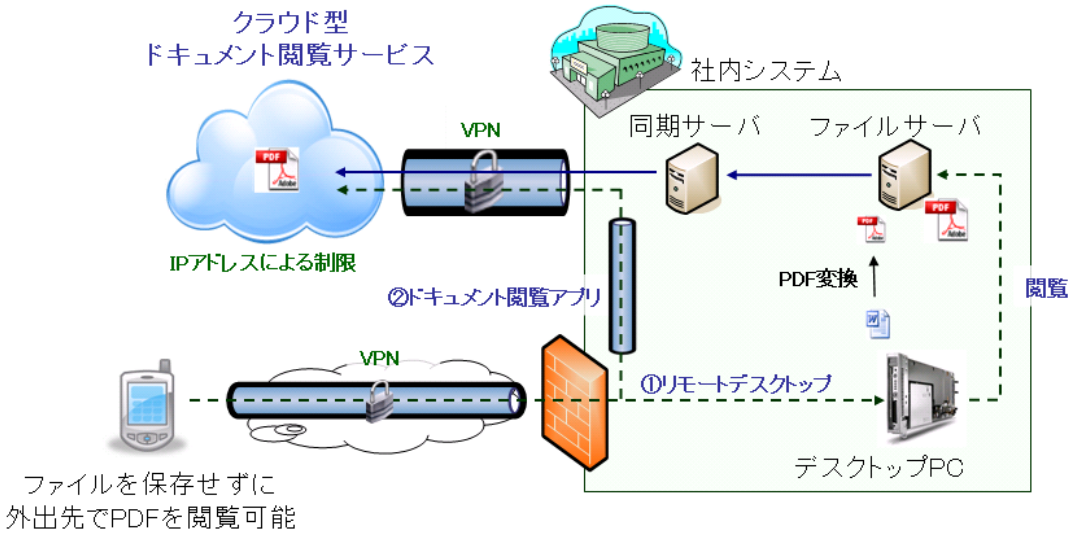


図 5-1　紙媒体持ち出しソリューションの概要

（1）　適用

社内の機密文書を紙媒体で持ち出すことによるリスクを低減するためのソリューションです。

（2）　説明

機密文書を紙媒体で持ち出すことを防ぐために、社外で文書閲覧が必要な場合には会社からスマートフォンを貸与します。

使用方法は以下の２通りです。

① VPN により暗号化された経路上で社内の PC へリモートデスクトップ接続をおこない、文書を閲覧する。
② 文書をクラウドサービスに同期または転送し、ドキュメント閲覧アプリを使用してスマートフォンから閲覧する。

（3）　導入上のポイント

紙媒体の持ち出しは、制御が難しく、どのような資料がいつ漏れたかを追うのは大変難しいです。スマートフォンをこのような使用方法とすることで“データを持ち出さない”という考え方ができるようになります。

（4）　拡張ポイント

使用方法②においては、文書がクラウドサービス内に保存されるため、時限機能を使って一定時間が経ったら文書を削除する仕組みが導入できるとセキュリティ強度が高くなります。

All rights reserved (c) Japan Smartphone Security Association

5.2.2. ３要素認証応用ソリューション

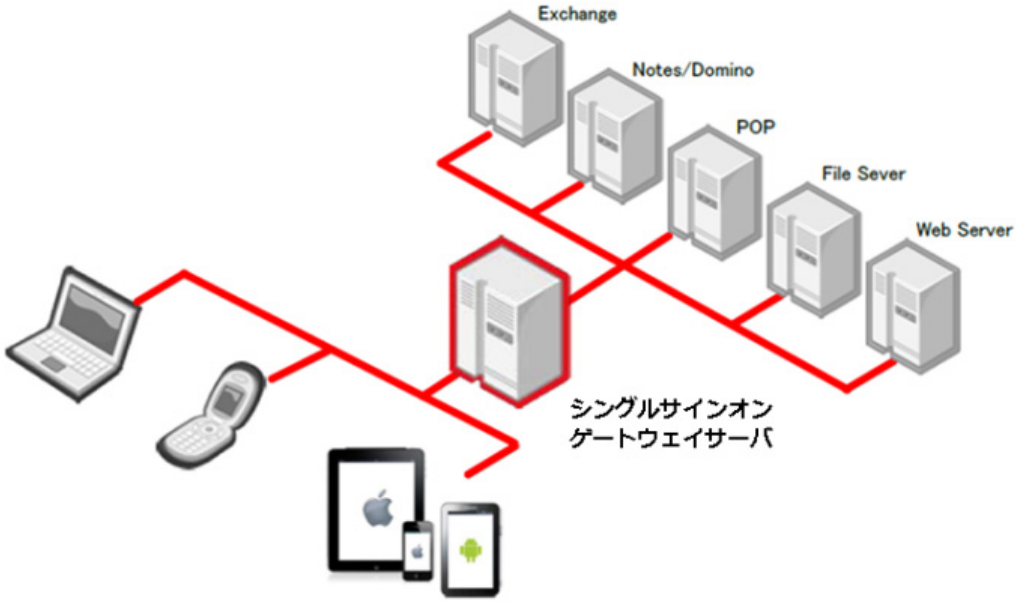


図 5-2　３要素認証応用ソリューションの概要

（１）　適用

端末側でのセキュリティ制御が難しい BYOD での導入に適しています。

（２）　説明

このソリューションは以下の４つの特徴があります。

・　基本機能

各コンテンツのデータを変換するハブ機能を基本機能とします。スマートフォンにおいては、各端末のブラウザに応じた HTML に変換する機能を提供しています。

・　シングルサインオン

サーバーを経由して、スマートフォンから社内のグループウェア、ファイルサーバ、Web 化された社内システムにシングルサインオンを行います。

・　３要素認証

スマートフォン上のブラウザアプリは認証時に、　①ID/PWD ②端末 ID　③セキュリティステータス　の３つの要素を認証要素とします。セキュリティステータスとは「マルウェア対策ソフトおよび MDM アプリがインストールされていること」「デバッグモードで PC に接続されていないこと」「既定の構成プロファイルが存在すること（iOS の場合)」「ジェイルブレイクのおそれが少ない OS バージョンであること（iOS)」であり、接続後は、「画面キャプチャー禁止」「コピーペースト禁止」「ファイルダウンロード禁止」「印刷禁止」「PC へのデータ移送禁止」を実現します。

・　デュアルポリシー

個人所有端末（BYOD）は情報漏えい禁止のポリシー、会社貸与端末は MDM と組み合わせることにより情報漏えいだけでなくモラル管理や端末の資産管理を行うポリシーという複数のセキュリティポリシーを同一基盤で運用することが可能です。

All rights reserved (c) Japan Smartphone Security Association

（3） 導入上のポイント

このソリューションによるポイントは以下の２つになります。

・ 新しい脆弱性に迅速に対応しやすい

端末のセキュリティレベルを高く保つことは一般的に困難ですが、端末がセキュリティ的に脆弱である可能性があることを発見する事は比較的容易です。そのため、新しい脆弱性が発見された時に迅速な対応を行う事が可能です。

・ 他のセキュリティシステムのカバーできない部分をカバーできる

３要素認証は、MDM やマルウェア対策ソフトなど、既存セキュリティシステムが前提としていないケースでもセキュリティを担保できることをコンセプトとしています。そのため、他の技術と組み合わせながらセキュリティ対策を万全にすることが可能となります。

図 5-3　３要素認証応用ソリューションのポイント

（4） 拡張ポイント

MDM やマルウェア対策と併用することにより、さらに強固なセキュリティを実現する事ができます。

All rights reserved (c) Japan Smartphone Security Association

5.2.3. ビジネスインテリジェンス MDM ソリューション

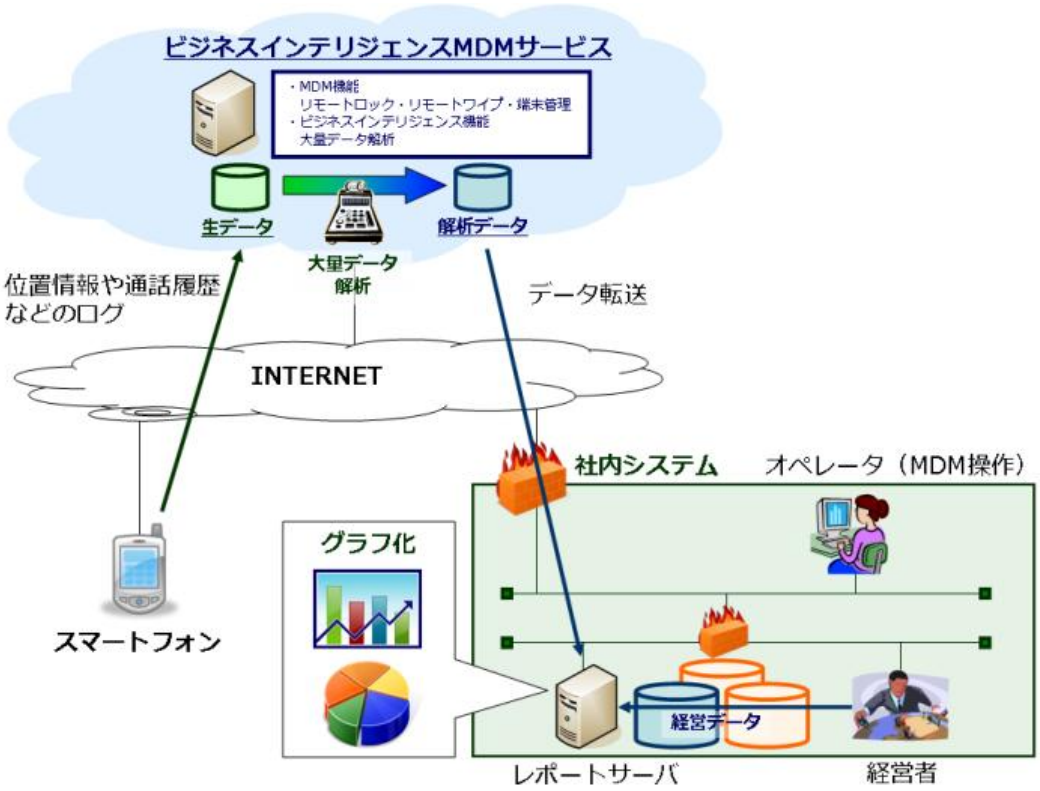


図 5-4　ビジネスインテリジェンス MDM ソリューションの概要

（1）　適用

スマートフォンを活用して業務の更なる効率化を目指す場合に有効となるソリューションです。

（2）　説明

営業外交員などに貸与したスマートフォンの位置情報や通話履歴などの利用ログをクラウドサービス上で集計・解析し、社内システムにある既存のデータマートと統合します。このデータをビジネスインテリジェンスツール（以後、BI ツール）を活用して可視化することで、業務改善のための切り口を見つけます。

（3）　導入上のポイント

クラウドサービスをデータの一時保管先としてだけではなく、大きな計算能力のある集計用インフラとして活用する事により、本来高負荷で高価な設備が必要となりがちな BI ツールの活用を促進します。

（4）　拡張ポイント

BI ツールのパッケージや、営業支援システムや顧客管理システム、経営支援システムなどの既存社内システムと統合することにより、業務改善のためのより効率的な集計・解析が可能となります。

All rights reserved (c) Japan Smartphone Security Association

6. おわりに

6.1. 今回のまとめ

このガイドではスマートフォンと業務システムについて現状を整理し、現時点でのセキュリティ技術とその応用事例について紹介しました。今回紹介した技術およびソリューションが実際に利用可能なすべてではありませんが、これらの技術を用いることでスマートフォンを安全に業務利用できることが理解いただけたのではないかと考えています。

6.2. 今後の課題

スマートフォン技術や市場動向に合わせて、セキュリティに対する考え方（２章）や具体的な技術・ソリューション（３章～５章）は、定期的なブラッシュアップが必要と考えています。最終的な到達点は、スマートフォンを活用したシステムインテグレーションにおける考え方とベストプラクティス集としたいと考えています。

6.3. 今後の進め方

本ガイドは今後の技術動向などを踏まえて定期的に更新したいと考えています。

6.4. 今後の目標

クラウドタスクフォースという活動においてスマートフォンとクラウドとの関係や、セキュリティに関する検討と議論を進めてきた中で、スマートフォンを企業導入するにあたり「社内システムとクラウドの組み合わせ方」や「スマートフォンと業務システムの役割分担」について、大量かつ重要なノウハウがある、ということを発見しつつあります。

世界においてスマートフォンが全盛となった現在、デバイス・ネットワーク・ソリューションは既にワールドワイドです。今、セキュリティにおいてメイドインジャパンの「キメ細やかな」ソリューションを確立することができれば、それはそのまま世界に打って出る武器となるだろうと考えています。

それを目標として我々はスマートフォンのビジネス利用に関するノウハウを「積極的」かつ「迅速」に、「深め」「広め」ていくことで、日本の ICT ソリューションをグローバルに広めていきたいと考えています。

All rights reserved (c) Japan Smartphone Security Association