スマートデバイス、SNS等への対応方針

2013年3月

情報セキュリティガバナンス協議会

目次

はじめに

■　背景

スマートフォンやタブレット端末、SNSなど、新しいIT端末・メディアが登場すると、組織によっては、業務の効率化や他社との差別化をもたらす鍵としてユーザ部門が導入を求めるケースが見られます。

これらは、メリットも期待できる反面、セキュリティ上の課題も少なくありません。新しいIT端末・メディアや、私物機器の業務利用に関して、どのようなリスクがあるか理解し、それに対して適切に対応することで、情報セキュリティガバナンスを確立することが必要です。

■　目的

ワーキンググループ（WG）では、アンケートや事例分析等を通じて、協議会会員各社におけるスマートフォン、タブレット端末導入事例（活用方法、情報セキュリティガバナンスの観点からのセキュリティ対策の考え方、情報セキュリティ対策等）を整理し、ビジネスにおける付加価値の向上と情報セキュリティへの配慮を両立させた、効果的な活用に関する知見をまとめました。

これらの知見によって、読者の方々が自社の効果的な対策に結び付けることを目的として、本報告書を作成しました。

今後、皆様方がスマートデバイスやSNS等を活用する場合の参考となれば幸いです。

1.想定リスクとその対策①調査項目と調査結果

■　協議会会員各社のスマートデバイス導入事例を対象に「想定されるリスク」及び「その対策」についてアンケートを実施し、リスクベースの検討を行いました。

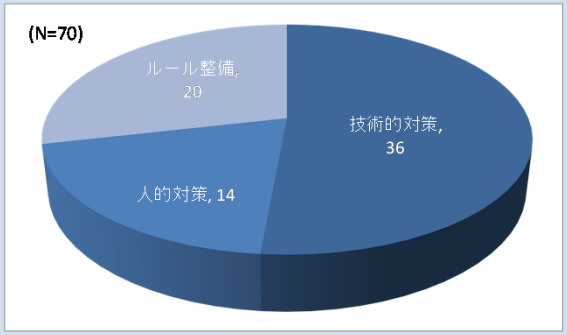
アンケート調査項目

①　企業属性
　（業種、規模、端末台数）
②　リスクに関する項目
　（社有／私有、利用範囲、
　取扱情報、接続形態）
③　導入目的
④　利用用途、利用シーン
⑤　想定するリスク
⑥　セキュリティ対策のポイント
⑦　実施している対策
- 技術的対策
- 人的対策
- ルール整備

アンケート調査結果

①11社（17事業拠点）から回答
- スマートフォン（Android系）⇒　2,164台導入
- スマートフォン（iPhone系）　⇒　2,176台導入
- タブレット型端末　⇒　2,372台導入

②私有機器の使用を認めている企業　⇒　2社
③想定されるリスク　又は　事象事例　⇒　53例
④対策案　又は　対策事例　⇒　70例



１.想定リスクとその対策②利用シーンとリスク

- 協議会会員へのアンケートでは、スマートデバイスを社屋内利用と社外持ち出し利用の両者を想定していますが、その主な使い方（利用シーン）は次のような結果となりました。
  - 自社の電子メール、スケジューラなど機密性が低く、事務連絡情報に類するもの
  - 顧客への商品説明資料、サーバ内のデータ参照など業務処理に類するもの
  - 撮影した現場（証跡）写真、売上情報参照など機密情報・個人情報に類するもの
- このような利用目的を背景として、発生が想定されるリスクの整理を行うため、アンケートで得られた「想定されるリスク　又は　事象事例」回答53例を分類すると、以下の3つの項目に分けることができました。

スマートデバイス利用時に発生が想定されるリスク

情報漏えい　又は 情報喪失リスク	コスト増加のリスク	規定違反リスク
①紛失・盗難 ②不正接続・不正設定 ③外部からの攻撃 （ウイルス感染など） ④盗聴 ⑤データ消失	①問い合わせ対応体制の 構築・整備・運営 ②導入・運用コスト	①労務規程に係わる 管理規則違反 ②私的利用（公私混同） ③不適切な使用

1.想定リスクとその対策③対策

■　協議会会員各社が実施又は予定している対策案の整理を行うため、アンケートで得られた対策案又は対策事例回答70例を分類してみると、以下の3つの項目に分けることができました。

スマートデバイス利用時の対策分類

技術的対策	人的対策	ルールの整備
①MDMに委ねられる対策 ②企業固有の対策機能	①教育 ②台帳管理など	①機器使用・運用ルール ②就業規則など

【技術的対策】

①セキュリティ管理
＝　パスワードの有効期限設定、遠隔操作による機能ロック

②ポリシー管理　＝アプリケーションの利用制限、メールやVPNの設定

③インベントリ管理　＝　シリアル番号、ユーザ名、アドレス、証明書情報

④ソフトウェア配布・管理　＝　構成プロファイル、クライアント証明書

これらの機能はMDM*1で実現できるものが多くあります。

*1）MDM（Mobile Device Management：モバイル端末管理）
大量のスマートデバイスを効率的、かつセキュリティを確保して活用するための管理ツール。

1.想定リスクとその対策④まとめ

- スマートデバイスの導入目的によって、導入規模や取り扱う情報の重要度が異なります。
- 技術的対策としてMDMに搭載された機能を用いることが有効であり、導入規模や情報の重要度に応じて機能の適用範囲を検討することが重要です。

スマートデバイスの適用範囲に応じた対策の考え方

	利用シーン (アンケート結果)	導入規模	情報の重要度 (アンケート結果)	対策 (アンケート結果　＋　一般的対策)
基本的対策	全社電子メール スケジューラー イントラ閲覧	特定部署 数十台導入	アドレス帳 事務連絡メール	【端末管理】 MDMによる基本設定 ユーザによるバージョンアップ、ファイル更新 【端末の初期設定】 利用部門毎、個人 【教育・啓蒙】 個別説明
拡張的対策	認証業務 WEB系取引業務 SNSによる対応 写真撮影	全社導入 委託先への貸与	取引情報 認証・決裁情報 機密情報 個人情報	【端末管理】 MDMによる集中管理 自社要件によるMDMの構築 【端末の初期設定】 共有キッティング 【教育・啓蒙】 e-learning 【その他】 紛失・盗難時の対応手順、炎上発生時の対応手順 VPN環境の構築、アカウント管理

2.情報セキュリティガバナンス確立のための留意点①組織のあり方

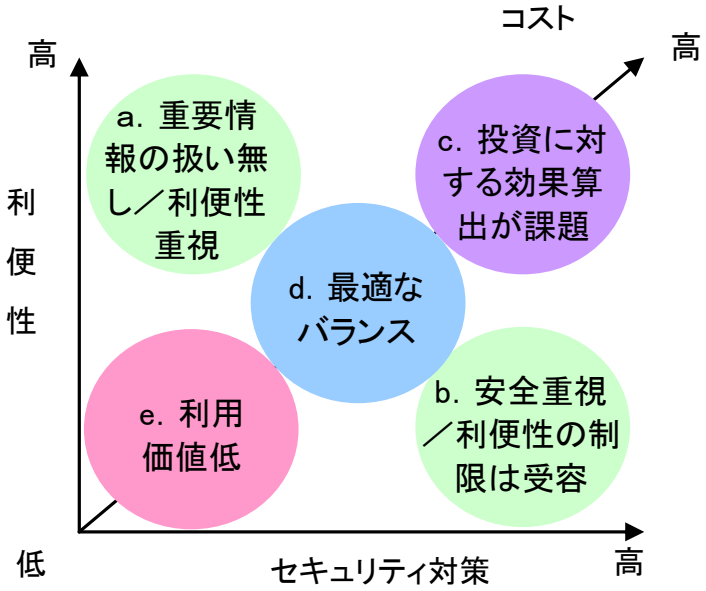
■　協議会会員会社の事例では、既存の情報セキュリティ管理態勢の枠組みにスマートデバイスを当てはめることで管理態勢は確立できるということがわかりました。

■　しかしながら、スマートデバイス固有の特性から、役割・責任について、以下の管理項目に対して管理部署を明確にすることが重要です。

管理項目	内容	管理部署
スマートデバイス現物の管理	現物の統括管理、 利用部署向け運用・管理ルール整備	総務部、システム部門
	BYOD利用可否判断	情報セキュリティ管理部署
	事故発生時の全社ルール整備	情報セキュリティ管理部署
システム環境管理	セキュリティポリシー決定	情報セキュリティ管理部署
	セキュリティ機能の実装	システム部門
	データ管理、 利用部署向け運用・管理ルールの整備	情報セキュリティ管理部署
	キッティング、MDMの導入、 社内システムへの接続	システム部門
ソフトウェアの管理	利用者共通機能の管理	システム部門
	特定業務アプリケーションの管理 （目的・安全性審査、利用可否判断）	情報セキュリティ管理部署
	（承認後の管理）	申請部署
その他	サポート・ヘルプデスク体制整備	導入企画した部署

2.情報セキュリティガバナンス確立のための留意点
②利便性とセキュリティのバランス

■　セキュリティに対するコストを一定として考えた場合、利便性（使い勝手）とセキュリティ対策（安全な利用）は両立せず、トレードオフの関係になりがちです。現実的なリスクへの対応を考えた場合、この両者をいかにうまくコントロールし、バランスを取るかが重要です。



・公開情報（企業Webページ、時刻表情報、製品カタログ等）
　事業所以外の場所においても迅速に情報を取得することが目的。重要情報は扱わず、利便性を追求します。（a）

・極秘情報（機密情報、個人情報等）
　安全に利用する必要あり。利便性の制限はやむを得ません。（b）

・重要情報（会計、営業情報等）
　決裁や、営業情報閲覧など。迅速さが求められる範囲がどこまでなのか、必要な対象者はどれほどかといった詳細な検討を行わないと費用が際限なく必要になるので注意が必要です。（c）

・社外秘情報(メール、企業内掲示板等)
　必要最小限の情報に絞り込んだ上で、リスクに備えた対策を施す必要があります。（d）

2.情報セキュリティガバナンス確立のための留意点
③周辺リスク（SNS）

■　SNSは、従来の枠を超えた新しい情報発信ツールであり、開示した友人以外にも際限なく伝達・拡散する可能性を持つものです。SNSを利用する者は、SNSに関する正しい知識を持つことが重要です。

■　従前のような、情報は適切に扱わなければならない、仮に情報漏えいした場合には厳しい制裁を受けるといった、情報漏えいの防止そのものを目的とした教育ではなく、SNSという新しい情報伝達手段の特性に関する理解を深める教育を行うことが重要になります。

SNSのリスクへの対策（例）

事例	対策（例）
①悪気ないつぶやきが事件に発展（炎上等）	・実例を挙げて徹底して教育することが重要。 ・SNSを親しい友人・知人に対する近況報告や個人的意見開示のツールとして考えている意識を修正。
②SNSを利用した販促の落とし穴（販促メールでユーザが不愉快に）	・Webモニタリング等、火種の段階で早期に検知。 ・自然鎮火を期待できない場合、事実調査の発表や謝罪などの意見表明を問題発生の端緒となったSNSを活用して発信。自社のホームページで正式見解を公表。 ・お客様相談窓口での対応も重要。
③怖い「なりすまし」（偽アカウント等）	・なりすまし行為や、社員個人の意見が企業としての活動でないことや公式の意見でないことを証明するための「ソーシャルメディアポリシー」の公表。
④ソーシャルメディアハラスメント（上司からの友達申請等）	・「相手の立場や気持ちになってよく考えよう」「断りたいと思ったら断ってもいい」というハラスメント防止の考え方は、SNSにも当てはまることを従業員に周知。
⑤SNS疲れ（精神的・身体的疲労、業務での外部対応の悩み）	・「SNS疲れ」が企業にとってリスクとなり得ることを認識。 ・従業員に対して具体的な事例を通じて適度な利用を促す。 ・担当者の精神的なケアに配慮。

2.情報セキュリティガバナンス確立のための留意点④教育・啓発

- 安全にスマートデバイス・SNSを利用するためには教育・啓発活動が欠かせません。
- 各社がどのように教育・啓発活動取組んでいるかメンバーにアンケートを取り傾向を分析しました。
- スマートデバイス・SNSに対する教育は、会社によりまだまだ温度差がありますが、できるところから少しずつ取り組んでいます。例えば、ガイドライン等を作成し、利用者へ注意喚起しています。教育・啓発手法は他に集合研修、説明会、e-learning、イントラネット掲示板・社内ホームページの利用、部署毎での説明DVDの上映、誓約書の取得など多岐に渡りました。

多くの会社で説明されている教育内容

スマートデバイスの教育内容	
紛失・盗難の際の安全管理策（リモートロック、リモートワイプ）	★★★
紛失・盗難の際の手続き（警察へ届出、社への報告など）	★★★
スマートフォンに関する自社の規則・ルール	★★★
営業情報の流失の危険	★★★

SNSの教育内容	
SNS投稿は自身の発言が不特定多数に閲覧されている可能性がある	★★★
他社・個人への批判中傷をしない	★★★

まとめ

■　本報告書では、協議会会員企業に対するアンケート調査を通じて、スマートデバイスやSNS利用の際のリスクと対策を整理し、情報セキュリティガバナンスの確立に向けた留意点として「組織のあり方」「利便性とセキュリティのバランス」「周辺リスク」「教育・啓発」についてとりまとめました。

■　本報告書はWGの「メンバー全員」で分担して執筆したものです。 網羅性や各論点の深掘りが不十分な点や、各章毎のつながりが不明確な部分もあるかもしれません。
しかし、日々、スマートデバイスやSNSのリスクと対策に立ち向かっている「現場」の人が定時後に自主的に集まって執筆した現場の人の思いが詰まった報告書です。

もっとこういう意見もあるよという方がおられましたら是非一緒にやりましょう。現場のみなさんの力が結集すれば、さらによいものができるでしょう。

「スマートデバイス、SNS等への対応方針に関する検討」（2012年度WG2）　メンバー

■　メンバー（社名五十音順）

株式会社インフォセック	松本　照吾
株式会社ジェイティービー	戸田　磨（副主査）
清水建設株式会社	武井　英明
住友商事株式会社	北方　孝好
積水化学工業株式会社	平尾　安明
株式会社高島屋	上原　佳都雄（副主査）
デロイトトーマツリスクサービス株式会社	丸山　満彦（主査）
株式会社電通	山下　実
東京ガス株式会社	廣川　千里
日本コムシス株式会社	中島　敏郎
一般社団法人日本コンプライアンス推進協会	上村　広志
富士ゼロックス株式会社	今村　光

（事務局）

株式会社三菱総合研究所	川口　修司
株式会社三菱総合研究所	江連　三香
株式会社三菱総合研究所	井上　信吾