情報セキュリティガバナンス協議会

スマートデバイス、SNS 等への対応方針に関する

報告書

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

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。また、震災に伴い、在宅勤務制度の導入や見直しが検討されており、その中で、自宅等における業務環境を確保する手段として、私物機器（携帯、PC 等）の業務利用も検討課題とされる可能性があります。

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ないため、手放しで導入を容認するわけにはいきません。導入のメリットとリスクを勘案して導入することが重要となってきます。スマートフォンやタブレット端末、SNS などの新しい 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り、それに対し、会員各社がどのようなスタンスで対応しているかを共有することは、今後の方針を考える上で有効です。

そこで私たちは、アンケートや事例分析等を通じて、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の共有によって、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取りまとめました。

最初に、情報セキュリティ対策の実効性を上げるためにはどのような組織体制や外部委託先の管理が考えられるかを整理した上で、第 2 章では会員各社に対するアンケート調査の結果を踏まえて想定リスクとその対策について検討しました。また第 3 章では、実際にセキュリティ対策を導入する際に利便性とセキュリティのバランスが重要となってくることから、これらをどのように考えてバランスさせればよいのかを検討しました。続く第 4 章は、スマートデバイスの普及とともに急速に利用が広がっている SNS 利用の周辺リスクについて検討を加えました。最後の第 5 章では、新しい IT 端末・メディアの活用に関するリスクについての教育や啓発活動の重要性についてまとめています。

今後の皆様方が、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. 組織のあり方

最初に情報セキュリティを所管する組織のあり方について整理したいと思います。そこで本章では、スマートデバイスを活用する際に情報セキュリティガバナンスを確立するための組織のあり方について示すことにします。

1.1 情報セキュリティ管理態勢について

1.1.1 組織体制

人、物、金は昔から経営資源としてよく言われてきていますが、今では情報もまた重要な経営資源の一つと考えられるようになってきました。このような重要性を増した情報についてのリスクに対する全社的統括管理体制についてはいくつかの方法が考えられます。全社的統括管理体制としては、

１．委員会方式

２．専門部署方式

３．委員会方式と専門部署方式の併用

が考えられますが、ここでは、１．委員会方式と２．専門部署方式の特徴について簡単に説明いたします。

(1)委員会方式

委員会方式は、トップマネジメントを委員長とする CSR 委員会、リスク管理委員会、情報セキュリティ管理委員会等の委員会で情報セキュリティを全社的かつ組織横断的に統括管理する方式です。

情報を取り扱う部署には、情報セキュリティ管理責任者、管理者を設置して現場を統括管理します。

(2)専門部署方式

専門部署方式は、経営資源である「情報」の管理を専門に行う部署を設置する方法です。「人」は人事部、「物」は総務部、「金」は財務部として組織を設置するのと同様の方式です。この専門部署方式には、情報セキュリティ管理専門部署を一つ設置しそこで集中して管理する方法（単独部署方式）と、情報セキュリティに関連する複数部署で連携して管理する方法（複数部署連携方式）の二つがあります。「情報」の管理を専門部署が行う方式です。

① 単独部署方式

情報セキュリティ管理専門部署として、システム的な技術的安全管理措置の企画・推進

を含む各種安全管理措置（組織的安全管理措置、人的安全管理措置、物理的安全管理措置等）の実施を単独部署が推進する組織体制です。情報システムの安全管理措置の推進も同一部署で所管するため、実効性のある管理策の推進が可能となります。

また、単独部署方式は、情報セキュリティ管理責任部署が明確となり、管理手続・マニュアルの整備、教育・研修、情報漏えい対策の実施、事故対応等一連の情報セキュリティ管理策の実施が一部署で可能となり、強力かつ先進的な組織体制です。

一方で、業務の効率化の阻害要因となるような過剰な管理に陥りがちな組織体制でもあり、セキュリティの強化と業務効率のバランスを勘案した運営がポイントとなります。

スマートデバイスのセキュリティの企画・推進の他、情報システム全般の情報セキュリティ全般の企画・推進を単独部署で推進できるメリットがあります。

情報を取り扱う部署には、情報セキュリティ管理責任者、管理者を設置して現場を統括管理します。（委員会方式と同様）

② 複数部署連携方式

全社を組織横断的にコントロールしている部署（例えば企画部、リスク統括部等）が情報セキュリティ管理の役割を担い全社的に統括します。

情報システム部門はシステムリスク管理部署として、情報セキュリティ統括部署と連携し情報漏えいに対する技術的安全管理措置を実施します。

情報セキュリティ管理部署が複数存在するため、役割分担、責任の所在が不明確になりがちです。「不作為の罪」を起こさないよう取りまとめ部署を決定し、責任を明確にすることが重要です。

情報を取り扱う部署には、情報セキュリティ管理責任者、管理者を設置して現場を統括管理します。（委員会方式と同様）

(3)組織体制の整備を実践するための管理策

ここでは、組織体制の整備を実践するための管理策として、経済産業省「個人情報保護ガイドライン」における「個人データの安全管理措置を講じるための組織体制の整備」を実践するために講じることが望まれる手法を例示します。

・ 従業者の役割・責任の明確化

従業者の役割・責任を職務分掌規程、職務権限規程等の内部規程、契約書、職務記述書等に具体的に定めます。

・ マネジメントレベルの情報管理責任者の設置

・ データの取扱い（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・

廃棄等の作業）における作業責任者の設置及び作業担当者の限定
- データを取り扱う情報システム運用責任者の設置及び担当者の限定
- データの取扱いに係わるそれぞれの部署の役割と責任の明確化
- 監査責任者の設置
- 監査実施体制の整備
- データの取扱いに関する規程等に違反している事実又は兆候があることに気づいた場合の、管理者等への報告連絡体制の整備
- データの漏えい等（漏えい、滅失又はき損）の事故が発生した場合、又は発生の可能性が高いと判断した場合の、管理者等への報告連絡体制の整備
- 漏えい等の事故による影響を受ける可能性のある本人への情報提供体制の整備
- 漏えい等の事故発生時における主務大臣等に対する報告体制の整備

1.1.2 管理規程の整備・運用

情報セキュリティ管理態勢の整備は、組織・体制の整備の他、各種管理規程を整備し、規程を浸透させ、遵守していくことが必要です。整備すべき規程類は以下のとおりです。

- 「情報」の取扱いに関する規程等の整備と遵守
  「紙」文書、電話、FAX、電子メール、Web サイト、USB メモリ等の電子記憶媒体、スマートデバイス、SNS 等利用時の管理基準

- 「情報システム」の安全管理措置に関する規程等の整備と遵守
  情報システムへのアクセスコントロール、情報システムで取り扱うデータ及びデータ伝送経路での暗号化、重要データへのアクセス記録の取得・分析・保管、コンピュータウイルス対策、サイバー攻撃対策、標的型メール対策、情報システムのリスク評価、OS・Web アプリケーション・ネットワークの脆弱性診断等のセキュリティ基準の他、情報システムの開発管理基準・運用管理基準

- 「建物、部屋、保管庫等」の安全管理に関する規程等の整備と遵守
  入退室管理システムの導入、重要な情報の施錠管理等物理的な安全管理措置

- 情報・データの取扱いを委託する場合の運用
  委託先の選定基準、委託契約書のひな型、委託先における情報・データの取扱い状況を確認するためのチェックリスト等の整備と遵守

1.2 スマートデバイスの管理態勢について

スマートデバイスのための特別な情報セキュリティ管理態勢は特段必要としません。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ます。

しかしながら、スマートデバイス固有の特性から、以下を明確にすることが重要です。

1.2.1 役割・責任の明確化

スマートデバイスの管理項目とその管理部署の候補を以下に参考として例示します。

(1) スマートデバイス現物の管理

- スマートデバイス現物の統括管理、利用部署向けの運用・管理ルールの整備

  → 総務部、システム部門
- 個人所有のスマートデバイス（BYOD）の利用可否判断

  → 情報セキュリティ管理部署
- スマートデバイスの紛失、盗難に関わるリモートロック等の初動、事故の当局報告等全社的な対応ルールの整備

  → 情報セキュリティ管理部署

(2) システム環境管理

- MDM 設定内容の決定等のセキュリティポリシーの決定

  → 情報セキュリティ管理部署
- PC と同等の機能を保有するため、インターネット接続、社内ネットワーク接続に関わるネットワークセキュリティ、ウイルス対策機能等セキュリティ機能の実装

  → システム部門
- 電話帳（電話番号、メールアドレス、その他の個人情報）、アプリに入力したデータ等スマートデバイスに保有するデータの管理、利用部署における運用・管理ルールの整備

  → 情報セキュリティ管理部署
- スマートデバイスのキッティング、MDM の導入、社内システムへの接続

  → システム部門

(3) ソフトウェアの管理

- 共通アプリケーション、OS 等の管理。メールシステム、スケジュール管理システム、Web ブラウザ、経路検索アプリ等、スマートデバイス利用者全員が利用できる機能の

管理

→ システム部門

・ 特定業務をサポートするアプリケーションの管理

→ （目的・安全性の審査、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

(4) その他

・利用部署からのスマートデバイス利用申請の受付、故障・紛失の一次受付窓口、利用者向け操作・業務利用方法・セキュリティ等の教育等、現場利用者のサポート・ヘルプデスク体制の整備

→ 導入企画した部署

以上、スマートデバイスの管理対象と管理部署を表 1-1 に整理します。

表 1-1　スマートデバイスの管理対象と管理部署

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） （承認後の管理）	情報セキュリティ管理部署 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

1.3 外部委託先管理

1.3.1 外部委託先のガバナンスのポイント

情報システムの開発や運用をすべて自社だけで完結している組織はほとんどないと思います。開発や運用のうちの一部の業務については外部の事業者に委託していることでしょ

う。情報システムの開発や運用で外部委託先を活用している場合は、委託元である自社の管理態勢を整備することが前提となりますが、組織体制の整備の他、スマートデバイスの管理規程の整備が必要です。

その上で、以下の外部委託に関わる意思決定、リスク評価を実施し、総合的な判断が必要です。

1.3.2 外部委託の可否判断

業務上のノウハウの外部流出リスク、機密情報・その他機密性の高い情報漏えいリスク等、総合的な観点で外部委託に関わるリスクを評価・コントロールした上で、外部委託の可否判断が必要です。委託業務の遂行にあたりスマートデバイスを利用する場合は、委託元の資産、委託先の資産にかかわらず、スマートデバイスからの情報漏えいリスクを評価し、外部委託の可否判断が必要です。

1.3.3 委託先の選定

委託先の選定は、下記の観点で総合的な検討が必要です。

(1)委託先の業務遂行力

・業務品質、納期の遵守、委託費用、業務ノウハウ、人材、設備等
・委託業務の遂行にあたりスマートデバイスを利用する場合は、委託元の資産、委託先の資産にかかわらず、委託元の管理規程に基づきスマートデバイスからの情報漏えいリスクの評価を実施し、リスクが存在するはその軽減策実施の実現性を評価する必要があります。

(2)情報漏えいリスク

下記について、委託元である自社の基準の充足度が判断材料となります。

- 組織的安全管理措置
- 人的安全管理措置
- 技術的安全管理措置

(3)委託先の業務継続力

委託先を容易に代替できる業務の場合は評価不要ですが、情報システムの保守等、継続的に委託を行う場合は、十分な検討が必要です。委託業務の遂行にあたりスマートデバイスを利用する場合は、委託元の資産、委託先の資産にかかわらず、利用者への情報セキュリティ研修が繰り返し実施されていることを定期的に確認することが必要です。

(4)委託中の管理

委託先選定時と同様の観点で、定期的にモニタリングの実施が望まれます。

1.3.4 スマートデバイスを利用する外部委託業務事例

(1)委託業務の概要

作業を外部委託する場合、その作業状況を委託元が確認する手段としてスマートデバイスを利用します。委託先担当者は作業の進捗状況をスマートデバイスで撮影し、その写真を委託元に送信します。委託元はその写真を進捗の管理及び検査等に使用し、作業実績として保管します。

(2)委託先管理の概要

スマートデバイスは委託元が貸与し、個人所有のスマートデバイス等の利用は認めていません。スマートデバイスの利用については、委託元の管理基準を適用しています。具体的には以下のとおりです。

- 外部持ち出し時は、持ち出し管理簿による管理を実施
- 事務所に持ち帰ったスマートデバイスは、管理者が施錠保管
- 定期的にスマートデバイス現物の棚卸しを実施

(3)委託元管理の概要

委託元の管理基準に基づき、委託先に対して以下を実施しています。

- 利用者からスマートデバイスの利用誓約書を徴収
- 利用状況を定期的にモニタリング実施
- MDMの導入により紛失・盗難時のセキュリティを確保

(4)情報漏えいリスクへの対応

撮影した写真は送信後、自動的に消去される仕組みであり、取り扱う情報の機密性、紛失・盗難時のリスクを勘案した対策が取られています。

(5)盗難、紛失、情報漏えいの対応

盗難、紛失及び情報漏えいがあった場合、委託元ルールに基づき、委託先責任者は委託元責任者に連絡をします。委託元では格納されている資産の重要度に応じて、対策を取りますが、個人情報、お客様情報等、機密度の高い情報については危機管理委員会を開きます。

2. 想定リスクとその対策

本章では、スマートデバイスを活用する際に想定されるリスクとその対策について、アンケート調査を基にした分析結果を示します。

2.1 本章の目的、背景

前章 1.2.1 では､スマートデバイスの管理体制について､その整備要件を説明しました。スマートデバイスの導入においては、それらを使用する際のリスクを認識し、その対策を講じ、安心・安全に活用する必要があります。

リスクは例えば「情報漏えい」に関する事件、事故として顕在化してきますが、この影響は、スマートデバイスを導入した企業だけでなく、これを使用する役職員や、情報を共有する顧客の不利益にまで及ぶため、社会的責任としても回避する対策が求められています。

本章では、当協議会に参加する各社の導入事例を対象に「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ので、その結果を紹介します。

なお、本章での検討範囲は、会社支給の機器として社員に貸与する場合を想定していますが、使用事例としては個人所有機器の利用も一部含まれています。

2.2 アンケートの実施と結果

アンケートは当協議会に参加する企業の中で、スマートデバイスの導入を実施、あるいは検討している企業に協力を求めました。

調査項目と回答結果の概要は以下のとおりです。

(1)アンケートの調査項目

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

(2) 回答結果

① 11 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
・技術的対策 ⇒ 36 例
・人的対策 ⇒ 14 例
・ルール整備 ⇒ 20 例

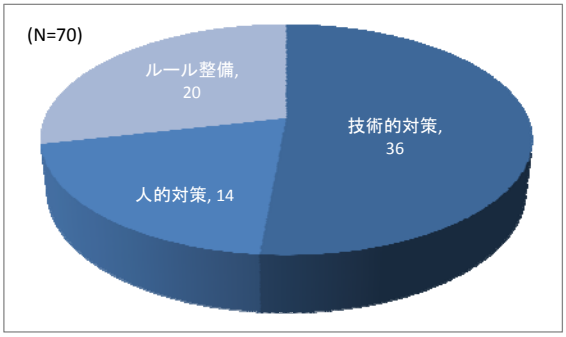


図 2-1 アンケート調査で対象とした対策事例

2.3 （アンケート結果に基づく）想定リスク

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っています。

(ア)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
(イ)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
(ウ)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、2.2 (2)－③で得られた回答 53 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。

(1)情報漏えい又は情報喪失リスク

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

(2)コスト増加のリスク

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

(3)規程違反リスク

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

上記(1)の「情報漏えい・喪失」は、①から⑤のようないくつかの要因により、機密情報や個人情報が外部に開示されてしまい、データを取り戻すことができなくなることを想定したもので、結果として顧客への迷惑、さらには損害賠償の訴訟にまで発展しうるものです。失った信用を取り戻すには多大な労力と時間が必要となります。

また、(2)の「コスト増加」は、スマートデバイスの導入により、それまでの携帯電話では実現できなかった機能・アプリを利用することが可能となり、ユーザの通信費用の増大や、使用に関する問い合わせ窓口体制（ヘルプデスク）の強化に要するコストが増えることを想定したものです。

さらに、(3)の「規程違反」は、就業規則だけでは縛りきれず、またシステム的な対策の限界を超えてしまうような、例えば業務時間以外の使用や、会社支給機器での私的利用、濫用、あるいは、社員教育ではカバーしきれない委託先での管理不備などから発生する事象を想定したものです。

2.4 （アンケート結果に基づく）対策

次に各社が実施又は予定している対策案の整理を行うため、2.2 (2)－④で得られた回答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。

(1) 技術的対策

① MDM（Mobile Device Management）に委ねられる対策
② 企業固有の対策機能

(2) 人的対策

① 教育
② 台帳管理など

(3) ルールの整備

① 機器使用・運用ルール
② 就業規則など

上記(1)の「技術的対策」は、MDM の導入で実現できるものが多く、後述する「2.5 対策の検討」のベースとなるものです。

MDM は、一般的に以下の機能で構成されています。
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

通常は、各ベンダーから製品として提供（SaaS 型が主流）されるものの中で、自社に適用する設定を選んで導入する形式を取りますが、スマートデバイスの利用目的によっては独自に構築し、必要なセキュリティに特化した構成にする場合もあります。
クラウド型サービスに比べオンプレミス型はコストが高く付きますが、痒いところに手が届く対応が可能となります。

スマートデバイスの導入台数や利用開始までのリード期間の大小においても、MDM の導入形式は検討する必要があります。

企業固有の対策としては、VDI（Virtual Desktop Infrastructure）やデータのリセット

機能（端末電源 off 時にデータ・設定情報を初期状態に戻す）の導入など、データを端末に保存させない技術が採用されています。

これは、機器紛失・盗難の際にデータ漏えいを防止する効果的な対策となります。

また、(2)の「人的対策」の一つは、社員教育（操作説明、セキュリティ教育）によって、技術的には対応が難しい部分、又は個人的なモラルのレベル維持を図るものです。

その他には、機器・データの持ち出し管理簿を用いて、社員のデータ管理意識を高めると共に、紛失・盗難の際に、どのデータがなくなったかが即座に判明することで、その後の対策が迅速にとれるようになります。

さらに、(3)の「ルールの整備」は、スマートデバイスの使用手順を会社の規程として縛ることで、上記の(1)「技術的対策」の実行にも、(2)「人的対策」の整備・適用にもセキュリティのレベルを維持させることを側面から支持するものとなります。

2.5 対策の検討

スマートデバイスの導入において、その目的や導入規模は企業により異なります。2.3 のアンケート結果でも紹介したように、スマートデバイスで扱う情報は、電子メール（事務連絡を想定）やスケジューラのように機密性の低いものから、モバイル PC で実現しているようなアプリケーションを搭載し、取引業務を処理した場合の個人情報・顧客情報など機密性の高いものまで様々ですが、リスク対策を検討するにはこれら情報の重要度を踏まえて、リスクを受け入れる部分と対策を講じる部分を整理する必要があります。

表 2-1　導入目的と対策は、導入目的・規模・情報の重要度とそれに見合う対策の軽重を紐付け、「基本的対策」と「拡張的対策」の関連性をまとめたものです。

アンケートの結果からは、技術的対策として MDM 機能を用いることが有効であり、その適用範囲を検討することが重要となっています。

表 2-1　導入目的と対策

	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 災上発生時の対応手順 VPN環境の構築 アカウント管理

2.5.1 基本的対策

会社のメールやスケジューラは、オフィス外で最も活用されるツールですが、これに対しては、MDM 機能の中の、パスワード管理や紛失時の遠隔ロック機能だけでも十分な対策となります。

一方、MDM でカバーしない手順は、ユーザ自ら対処（例えばバージョンアップの更新、ウイルスパターンファイルの更新など）する必要があり、セキュリティ管理上のばらつきはリスクの受入部分と認識して運用していくこととなります。

2.5.2 拡張的対策

スマートデバイスには、各種「アプリ」や、セキュアな通信環境を構築することにより、業務用アプリケーションの機能を処理する仕組みを搭載することができます。

例えば、モバイル PC で利用できる認証業務や Web 系取引業務、さらには一般消費者を対象とした SNS 活用の営業業務の実装などですが、これに対するリスク対策では、基本的対策をベースに拡張的に対策を施す必要が出てきます。

MDM 機能の中の端末認証、暗号化、データバックアップなどまで適用範囲を広げて設定を行います。

また、導入が全社規模（数十台から数百台）と多い場合や、委託先へも貸与するような

場合は、端末の共通のキッティングや、初期教育においても個別指導ではなく、e-learning を利用した均一で広範な指導が必要となると共に、紛失・盗難、SNS を利用することによる「炎上」への対応など、それなりの投資が必要となります。

本章ではアンケート結果に基づいてリスクと対策の整理をしてきましたが、この対策への投資バランスについては、次章「3 利便性とセキュリティのバランス」で整理、分類して説明します。

コラム「BYOD 導入する際の企業における課題と対策の留意点」

本コラムでは、BYOD（Bring Your Own Device）の現状と企業における BYOD 導入時の課題とその対策の留意点を取り上げています。

●BYOD とその現状

BYOD とは、端的に言い切ってしまえば私有デバイスを業務活用することです。従来からも PC においても同様の議論がされていました。近年、スマートフォンやタブレット PC が急速に普及したことにより、スマートデバイスにおける BYOD 利用の導入が一部企業で始まっており、その他の企業でも盛んにその導入の是非が検討されています。

BYOD は、東日本大震災後の BCP（事業継続計画）対策としても注目され、また「いつでも」「どこでも」働ける多様な働き方を推進するワークライフバランスの向上の観点からも注目されている手法の一つです。

海外でも同様の議論は既に行われているようです。米国、英国などの BYOD 導入率は、日本に比べて高いようです。日本でもスマートフォンなどの個人所有が急増している中、私有端末で業務を遂行できれば利便性が高まると考えるのは自然なことです。

しかし、IDC Japan 株式会社の調査結果によると、スマートフォンでは BYOD を認めない：42.9%、BYOD 検討していない：7.5%であり、タブレットでは BYOD 認めない：48.0%、BYOD 検討していない：8.5%であり、いずれも半数以上の企業が BYOD 利用を考えていない状況です。[1]

日本では個人情報保護法の施行をきっかけに、多くの企業が情報漏えいの事故を起こさないように、ノート PC 等の持ち出し制限など、厳格な情報セキュリティ対策を実施してきていることもあり、保守的な風土が根付いてしまっているのかもしれません。

●企業における BYOD 導入時の課題

企業が BYOD を導入するにあたっての課題としてよく挙げられるのが、「セキュリティ」と「労務管理」の２つのリスクです。これらの課題が解決していないために BYOD の導入に踏み切れていない企業は少なくないと思われます。

まず「セキュリティ」ですが、主な懸念事項は情報漏えいでしょう。端末の紛失／盗難、誤操作、マルウェア感染などにより、「お客様情報や会社の機密情報を漏えいしてしまう」という懸念です。社有のノート PC や USB メモリのセキュリティ管理に既に多くの投資をし、対策を講じてきた情報システム部門としては、私有デバイスの利用を認めることについての抵抗感がかなりあるのではないかと考えます。

次に「労務管理」ですが、労務管理を管轄する人事部門の立場として、労働時間外に私

[1] 2013 年 国内 BYOD 利用実態調査結果を発表　2013 年 1 月 17 日 IDC Japan 株式会社 、http://www.idcjapan.co.jp/Press/Current/20130117Apr.html

有デバイスで会社の業務をしてしまう「労働関連法令に関するコンプライアンス上の問題」が課題となっています。

しかしながら、BYOD の導入は、企業と従業員の両方にメリットをもたらす面もあることをやはり忘れてはならないでしょう。企業としてはデバイス導入コストが削減されます。一方、従業員も私有と社有の複数台のデバイスを持ち歩かずにすみます。いつでもどこでも業務が遂行できる利便性、生産性向上という大きなメリットを両者とも受けられるのではないでしょうか。

●BYOD 導入時に企業が考慮する対策例

従来、私有デバイスを認めていなかった企業が BYOD を導入する場合の重要な点は、情報セキュリティアーキテクチャに大きな影響を与える方針変更をするということを経営者が認識することです。つまり、経営者による従来の情報セキュリティガバナンスの考え方を大きく転換する意思決定とも言えるのです。

具体的な一例としては、私有デバイス業務利用禁止という従来ルールから方針を転換することが挙げられます。また、BYOD を一部の従業員に限定する場合、全従業員への一律のルール適用から脱却して、特定の領域・従業員への個別ルール適用という考え方への切替えが必要な企業もあるかもしれません。

その上で、情報漏えいリスクに対しては、端末に情報を残さないシステム的な制限や、BYOD 向けの MDM ソリューションの利用により、個人データと会社データを隔離し、紛失時は会社データを遠隔消去するなどの手段を講じる対策を導入することも考えられます。

また労務管理リスクに対しては、端末の利用状況をモニタリングし、定期的にログを監査して、問題があれば速やかに是正するなどの運用管理体制を整備することも考えられます。

その他、従業員には必要な教育を実施し、誓約書を取得するなどの対応も必要になるかもしれません。また、私有デバイスによるセキュリティインシデントの発生リスクを低減させるため、役職、セキュリティ意識、IT リテラシーなど個人の資質の観点で、私物端末利用を許可する従業員を限定することも考えられます。

さらに、通信費、マルウェア対策アプリや業務中の端末紛失・破損などの費用負担の問題など、事前に詳細な検討を十分にしておく必要があるでしょう。

3. 利便性とセキュリティのバランス

本章では、スマートデバイスの利便性を活用しつつ、情報セキュリティガバナンスを確立するための考え方を示します。

3.1 利便性とセキュリティ対策の関係

システムを構築する際には、そのシステムが果たすべき目的から、必要となる情報資産とその情報資産の利用方法が決まります。この両者が決まると、そのシステムが抱えるリスクが明らかとなり、これにいかに対応していくかを検討することになります。

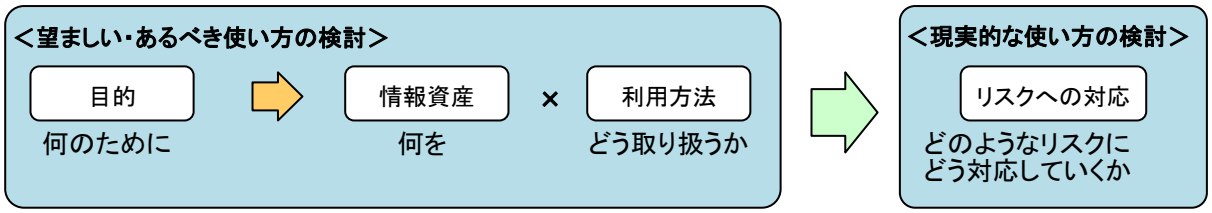


図 3-1　スマートデバイスの使い方の検討

基本的にセキュリティ対策にかかる費用はリスクの大きさに依存します。リスクは、情報資産の持つ価値と､その情報資産がさらされる危険度により決まります｡その危険度が、すなわち利用方法によるのです。利用方法の重要な要素は利便性です。特にインターネットの普及を経て、近年のスマートデバイスの出現が危険度を加速度的に増加させており、利便性の高さがすなわち危険度の高さといっても過言ではない状況です。

コストを一定として考えた場合、基本的に利便性（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となります。

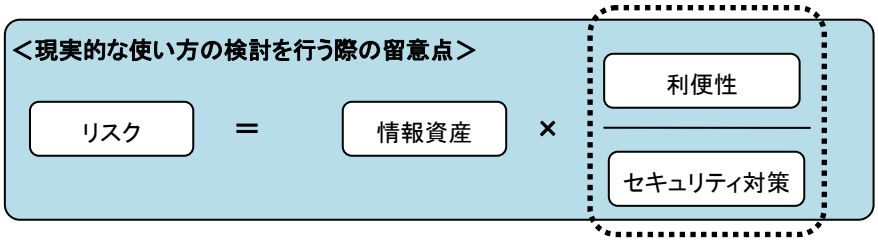
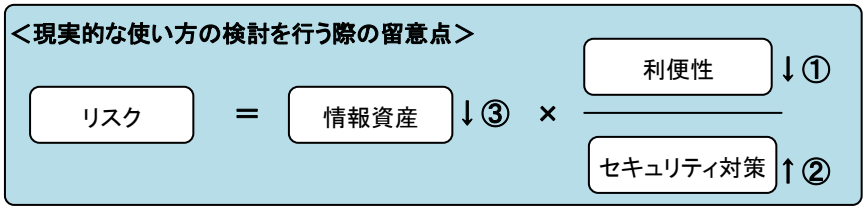


図 3-2　利便性とセキュリティ対策のトレードオフ

3.2 バランスの考え方

利便性とセキュリティ対策のバランスを考える際に重要なことは、まずは対象となる情報資産に目を向けるということです。情報資産の価値が高いほど、取扱いに注意が必要です。顧客情報、中でもクレジットなどお金に関する情報や、個人属性などのセンシティブな情報は、厳重に取り扱う必要があります。よって、重要な情報資産を取り扱う際には、その価値を守るためのその他の情報よりさらに強度の高い対策が必要となります。一方、時刻表や企業プロフィールなどの広く公知の情報は秘匿する必要がありませんので、情報漏えい対策は必要ないといえるでしょう。

重要な情報資産を使い勝手よく利用したいというニーズは絶えず存在しますが、現時点で安全かつ安価に実現する方法はありません。重要な情報資産を扱う場合には、まず安全を優先することが望ましいでしょう。逆説的に言えば、利便性を追求する必要があるのであれば、できる限り取り扱う情報資産を限定し、重要な情報資産を取り扱わないようにすることが望ましいといえます。どうしても重要な情報資産を利便性よく活用したいということになれば、少しでも取り扱う情報資産を減らし、取り扱う要員も限定し、さらに十分な対策を施した上で、それが本当に目的に適うのか否かを検証することが必要です。



リスクを回避する手段
① 利便性をある程度我慢する
② セキュリティ対策の強度を上げる
③ 情報資産そのものを減らす
※①③なしでは、コストが際限なく必要となる可能性がある。

図 3-3 リスクを回避する手段

3.3 目的とリスクに応じたバランスの最適化

ビジネスにおいて取り扱う主な情報資産について、利便性とセキュリティ対策のバランスの観点から考えられる具体的なアプローチをまとめてみました。

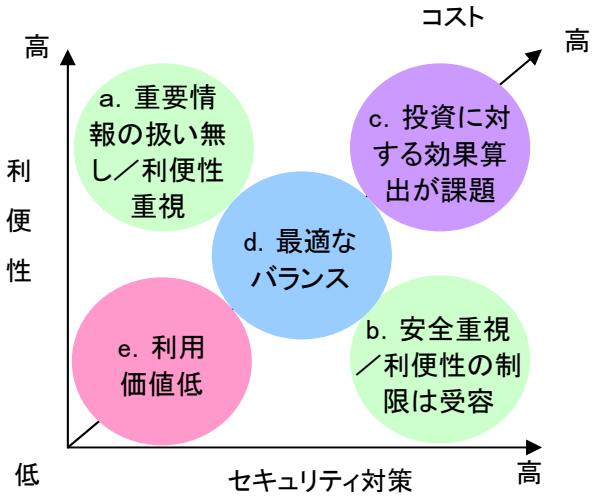


図 3-4　利便性とセキュリティ対策の考え方

・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。　（図 3-4 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。（図 3-4 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。（図 3-4 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。（図 3-4 d.）

これらを踏まえ、具体的にどのようなセキュリティ対策が考えられるか、それによって利便性がどう制限されるのかを一覧にまとめて後述します。

3.4 セキュリティ対策のレベルと利便性の関係

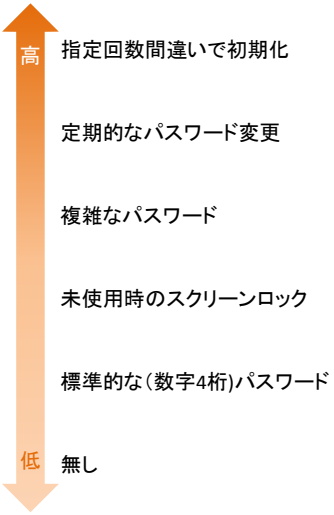
情報資産に対する主なセキュリティ対策について、利便性とのバランスの考え方をまとめました。

3.4.1 パスワード

指定回数で初期化設定をした場合、意図しない操作により初期化されることがあり、管理者の工数が増加する可能性がありますが、盗難や紛失時の情報漏えい対策としては効果的です。

パスワード設定をした場合、その長さや文字種別の多さによりセキュリティは向上しますが、利用する時に煩雑になります。また、定期的なパスワード変更を行うことで、更なるセキュリティの向上につながりますが、パスワード忘れにより利用できなくなる可能性が高くなります。

パスワード設定無しで利用すれば、誰でも簡単に利用可能となり、利便性は向上しますが、盗難や紛失した時のリスクが極めて高くなります。



3.4.2 ウイルス対策

マルウェア対策やウイルス対策アプリを導入することにより、各種操作が遅くなることがありますが、操作性への大きな影響はありません。

Android 端末では、ウイルスに感染し情報漏えいにつながる危険性があるため、対策アプリを導入して利用する方が良いとされています。一方、iOS に関してはウイルスに感染する可能性がほとんどなく、ウイルス対策アプリも存在しないため、対策アプリ無しで利用することが一般的です。ただし、業務アプリ等を開発する場合は、iOS は制限事項が多く Android は自由に開発できるという特性があります。

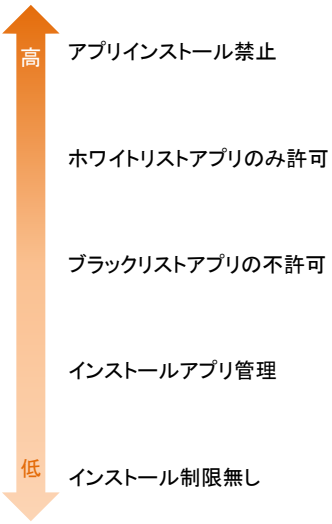
3.4.3 アプリ制限

キッティング時に必要なアプリをインストールしてから端末を配布することにより、ユーザによるアプリインストールの禁止やホワイトリスト化によるアプリインストール制限は可能です。

しかし、その他の市販や無料のアプリを利用する場合は、申請等が必要になり簡単に利用できなくなります。その反面、ウイルス感染や私的利用の抑制には効果的です。

ブラックリスト化により、利用できないアプリを制限することも可能ですが、ブラックリストアプリの登録を頻繁に行う必要があり、メンテナンス工数が増加します。

アプリのインストール制限無しで利用する場合でも、インストールされたアプリ一覧を管理することにより私的利用の抑制にはなりますが、ウイルス感染の予防には効果はありません。

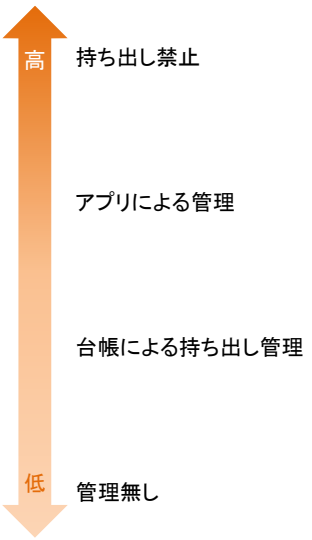


3.4.4 端末管理

会議室専用端末や生産ライン用端末等として利用するならば持ち出し制限も可能ですが、営業支援ツール等の端末として利用する場合は、社外での利用は必須です。

台帳で管理することも可能ですが、記入漏れ等により管理できない端末が発生するため、MDM アプリで管理するのが一般的です。

端末管理を行わずに利用した場合は、盗難や紛失時の端末特定ができないため、セキュリティリスクが高くなります。



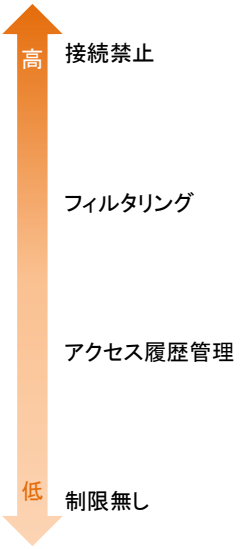
3.4.5 インターネット接続

インターネット接続を禁止することは、ウイルス感染やマルウェア感染の対策にはある程度効果的ですが、利用用途は会議室端末や生産指示端末等など極めて限定的となります。

フィルタリングによる対策も効果はありますが、利用できる情報が制限されてしまいます。

アクセス履歴を管理することにより、自由に情報取得ができ私的利用の監視も行えます。しかし、予防的なセキュリティ対策としての効果はありません。

情報端末として活用するには、制限なく利用する方が利点を損ないませんが、セキュリティリスクは高くなります。



3.4.6 社内ネットワーク接続

社内ネットワークへの接続を禁止することにより、情報漏えいのリスク低減やウイルス感染被害の社内への拡散防止に効果があります。しかし、社内の業務アプリ利用や情報共有を行う場合に、インターネット経由で行う必要があり、技術的なハードルが高くなります。

社内接続の運用方法や接続方法をルール化し、許可された端末のみ接続可能とすることで、比較的安全に社内接続を行うことができます。

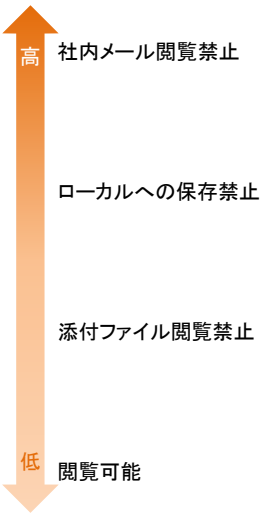
制限無しで、社内ネットワークへ接続を許可した場合は、情報漏えいのリスクが大きくなります。また、ウイルス感染やマルウェア感染の被害が発生した場合に、社内全体に被害が広がる可能性があります。

3.4.7 社内メール閲覧

社内メールの閲覧を禁止することにより、メールに起因する情報漏えいの可能性はなくなりますが、情報端末としての利便性が損なわれます。

端末へのデータ保存や添付ファイルの閲覧を禁止すれば、ある一定の効果は発揮しますが、ショルダーハック等の「覗き見防止策」を検討する必要があります。

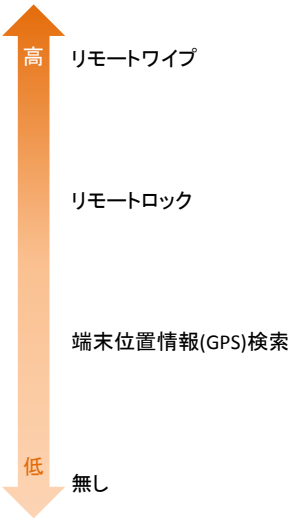
自由に閲覧可能とすることで、情報端末としての特性を発揮できますが、情報漏えいリスクは高くなります。



3.4.8 盗難、紛失時の遠隔制御

MDM アプリで、リモートロックやリモートワイプを利用する方法が一般的です。また、GPS による端末の所在地確認を行うことも可能です。

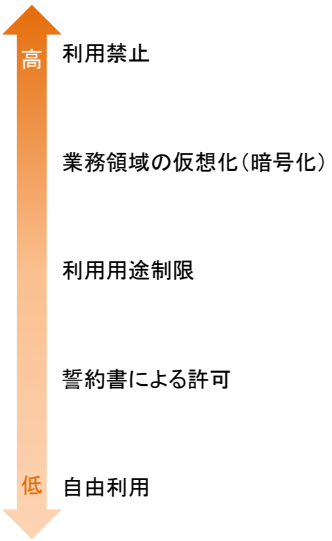
MDM アプリをインストールしたことによる利便性への影響はほとんどありませんが、MDM アプリのライセンス費用が必要となります。



3.4.9 私有端末の利用制限

私有端末の利用を禁止し、セキュリティ対策及び管理の徹底された社用端末に限定することで、セキュリティは向上しますが、利用者は複数台の端末を持ち運びする必要があります。

私用端末の業務利用(BYOD)を許可することにより、複数台の端末を持ち運ぶ煩わしさはなくなりますが、私用領域と社用領域の分離や、扱える情報を限定する必要があります。誓約書による許可や自由利用により、私有端末の利活用につながりますが、利用者のモラルに頼る部分が大きく、教育や規則の整備が重要になります。



3.4.10 まとめ

上記の各セキュリティ対策の強度については、各対策を単独で行った場合の評価となります。実利用環境においては、それぞれのセキュリティ対策を組み合わせて実施することにより、様々なセキュリティリスクへ対応する必要があります。

また、これらの評価は現時点での評価となり、今後の技術の進歩や情勢の変化により必要とされるセキュリティ対策は変化していきます。利便性とセキュリティのバランスも、時代の流れに即して考えていく必要があるため、定期的に見直しを行っていく必要があります。

コラム「情報漏えいリスクとの付き合い方」

スマートフォンの普及率が上昇しています。携帯電話からスマートフォンに乗り換えた当初は、「操作が難しい」という意見や「バッテリーの持ちが悪い」等の苦情もあるようですが、しばらくすると、ユーザ自身の慣れや工夫でこれらの問題を解決し、「便利」「楽しい」という意見が大半を占めるようです。またメーカーの日々の努力により新機種・新機能が続々と発表され、今後も乗り換えが進むことは間違いなさそうです。

確かに携帯電話と機能比較すると、スマートフォンでできることが格段に増えました。今までより、より「便利」「楽しい」のですから普及していくのは必然であり何ら問題もありません。

ところが**会社で利用する**ことを考えると乗り越えなければならないいくつかの問題があります。通信コストの問題、端末のキッティング・配布・サポートの問題、それから**セキュリティの問題**は、企業での普及を阻害する大きな原因となっています。せっかくの便利なツールです。うまく活用することはできないのでしょうか。情報漏えいリスクを軽減するソリューションも数多く登場しています。

結論から言えば、**「各企業のセキュリティ方針により、スマートフォンの利便性と情報漏えいリスクを考察し、バランスを取ることが重要」**ということになります。業界や会社毎に状況も違いますし、考え方は違って当然です。例えるならセキュリティ方針は、各家庭における教育方針に近いのかと思います。家庭によって、しつけに厳しい家庭もあれば、比較的寛容な家庭もあります。これは考え方の違いであり、いちがいに良い悪いとは言えません。それから隣の家庭はどうしているのか気になるという点も似ているようです。

スマートフォンは「便利」というだけでなく「楽しい」ものだと思います。個人的には、スマートフォンを初めて購入した時の**「楽しさ」・「ワクワク感」を大切にしたい**と思います。さてどのように役立てましょうか。

コラム「スマートデバイスの管理、技術でできないこと」

本コラムでは、経営者の皆様や IT には詳しくないがスマートデバイスの導入を検討しなければいけない担当者の皆様が導入や運用を設計する際に、押さえておくべきポイントをいくつか挙げています。

スマートデバイスにはたくさんの危険がありつつも、何でも解決できる“魔法の杖”のようなソリューション広告が出ていることもありますが、実際に“何ができて、何ができないか（教育やルールでカバーすべきか）”の理解を深めることが、スマートデバイス活用のポイントとなります。スマートデバイスを管理する際、次の三点を理解することが重要です。

・ネットワークを利用する技術的管理策
・OS や業者の特性に基づく技術的管理策
・技術的な過渡期であるスマートデバイス

●ネットワークを利用する技術的管理策

スマートデバイスのセキュリティを守る上では、コンピュータウイルスのような悪意のあるプログラムの侵入を検知し防ぐこと、利用者自身が勝手にアプリケーションを導入したり、情報を外部に送信したりすることを防ぐこと、盗難や紛失時に、遠隔操作でデータを削除したり、位置を特定すること等が主な管理策として挙げられます。

こうした機能はパソコンと同様のフィルタリングソフトやウイルス対策ソフト、MDM、暗号化ソフトといったソリューションとして提供されています。MDM によっては複数の機能を有するものもありますので、<u>一言に MDM といっても、どこまでの機能が提供されているかはソフトの仕様によります。</u>

特徴的なことは機能の多くがスマートデバイスの特徴である“常にネットワーク（携帯電話の回線や無線 LAN）につながることができる”ことを利用していることです。

例えば紛失したとしてもネットワークがつながる環境であれば、速やかに位置情報を特定し、データを消去することができます。こうしたことは出先では利用者が自分でネットワークにつないでいたノートパソコンでは実現が困難でした。

また、デバイス内にデータが残ることが盗難や紛失、不正利用の中でリスクがあると考える場合には、VDI（Virtual Desktop Infrastructure）と呼ばれるようなネットワークを通じで、必要な機能にアクセスするようなソリューションも多く登場しています。これはネットワークの速度が飛躍的に向上したことにより、例えば会社にあるパソコンの画面をスマートデバイス上に呼び出して、あたかも会社のパソコンを操作しているかのように外出先で業務を行うことも可能となっています。（逆に外出先で利用できる機能を制限する、といったことも可能です）

一方、<u>ネットワークが届かない環境では、期待する機能が利用できない</u>可能性があります。実際、スマートデバイスを不正に取得した人間が SIM カード（携帯電話の通信に使わ

れる部品）を抜き取ってしまうと、遠隔からの制御が機能しないことなどは、実際の紛失ケースでも発生しています。

●OS や業者の特性に基づく技術的管理策

次に OS や、業者が考え方によって、必要な技術的管理策が異なる場合があります。

現在では iOS（iPhone や iPod）にはウイルス対策ソフトはほぼ皆無ですが、Android では様々なウイルスが確認され、また多くのウイルス対策ソフトが提供されています。これは Apple 社が iOS に導入するアプリケーションに対して審査を実施しており、不正な改造がなければウイルスを導入する余地がないという設計に基づいているためです。

一方 Android では、アプリケーションを作った人間は特に審査もなく自分の作ったものを公開することができます。Google が提供する正規のマーケットでウイルスが混入したアプリケーションが配布されていたこともありました。

iOS は一見安全ではありますが、攻撃者（ウイルス作成者）の技術革新により、ウイルスを iOS に侵入させる仕組みが確立された場合や利用者が OS を不正に改造していた場合、発見が困難になるため、不正改造を制限する仕組み（MDM 等）の導入や、必要な情報を定期的に入手し、新たな脅威が発現した場合に適切に対応することが求められます。また、会社が利用したい独自のアプリケーションを iOS に導入するためには、多少の敷居の高さがあることを理解する必要があります。

Android では、MDM 等の技術対策で導入可能なアプリケーションを制限する、もしくは、携帯電話のキャリア等が審査したアプリケーションのみを利用許可する等の**運用ルールを利用者に教育する等の技術以外の対策**が求められることがあります。

また、Android では利用者が容量を拡張するために SD メモリ等の外部記憶媒体を利用することができる機種もありますが、現行のほとんどの機種では標準機能では外部記憶媒体の暗号化ができず、紛失や盗難をされた場合にデータを簡単に読み取られてしまう恐れがあります。

●技術的な過渡期であるスマートデバイス

本コラム執筆時点でも、OS のバージョンアップや新しい機種では、過去の技術的な弱点がしっかりと補完されています。

スマートデバイスは技術的に過渡期ですし、また Microsoft 等が新たなスマートデバイス用 OS を発表する等のニュースも世間をにぎわせています。

技術的な過渡期であるデバイスを組織に導入する場合、異なる機種、異なるバージョンの混在を許さず、全体として一定のセキュリティレベルを担保するか、組織として最低限求めるセキュリティレベルをしっかりと考えた上で、機能の向上などをメリットとしてとらえ、多様な機種やバージョンの混在を自明のものとした運用体制を構築すべきかは組織として考えるべき導入の際に考えるべき事項です。

4. SNS 利用の周辺リスク

本章では、スマートデバイスの普及とともにその利用が急速に広がっているソーシャルネットワーキングサービス（SNS）について、その利用の際のリスクと効果的な対策について説明したいと思います。

4.1 SNS の利用状況

近年、SNS は猛烈な勢いで普及しています。企業は情報漏えいに備えて様々なセキュリティ対策を施しますが、従業員の倫理観が大きく影響する SNS での不用意な発言等に対する対策は手付かずの状態です。守秘義務に関する研修や誓約書といった一般的なコンプライアンス対策を従業員に対して実施したとしても各従業員の倫理観や意識に依存する部分も多く、どのようにして再発を防止するのかは、企業における大きな課題となっています。企業は、社員の SNS 利用におけるガイドラインを作成するなどして対応を始めていますが、単に形式だけを整えても実効性がないことは、様々な事件を見れば明らかです。

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。「ソーシャルメディアはバーチャルではなくリアルである」こと、「SNS での発言に伴うリスクがある」ことを理解しておくことは最低限必要でしょう。

ここで言う「正しい知識」には、「Twitter での友人への書き込みが、電車の中やエレベーターの中での会話以上に危険な、広範囲に伝達される可能性があること」、「友人への何気ない書き込みによって、自らが働く会社ばかりか、自らの生活にまで重大な影響を及ぼすことがあるという、従来の伝達手段にはなかった甚大な影響力を有する」という認識も含まれます。

そして、企業の対策は、この正しい知識の周知を図り、SNS による発言が、公の場での発言と同じ意味を持つことを十分に理解してもらった上で、企業人が公の席で守るべき最低限のルール“自分が職場で見聞きした顧客等のプライベートな情報を話したりしない”、“社会常識に反した偏った意見を表明しない”、“誤解を招きそうな発言を行わない等”を順守するよう教育することに尽きます。

つまり、SNS 利用の際には、「自分の名前と、会社名を明記した名札を胸につけて、公の席で発言できないようなことは、その相手が誰かに関わりなく発信しない」という、極めて「当たり前」のことを、以下に紹介する会社を巻き込む SNS トラブル実例を交えながら社員に徹底していくということです。

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。

4.2 悪気ない Twitter での「つぶやき」が事件に発展

あるホテルで起こった事件では、ホテル内のレストランの女性アルバイトが「著名なサッカー選手と女性タレントがレストランに来て今夜二人で泊まるらしい」と友人にツイートし、この情報が蔓延・拡大し炎上、当該アルバイトの個人情報がネット上で開示されてしまった他、ホテルへの批判が集中し、最終的には、ホテル総支配人による公式ホームページでの正式な謝罪にまで発展しました。

つぶやきの内容は彼女にしてみれば、友人とのいつもの会話と変わらなかったのかもしれません。しかし、それが Twitter を通して行われたことによって、大事件に発展してしまったわけです。

このホテルでは、きちんと顧客情報の守秘義務に関する研修や誓約書の提出といった、一般にコンプライアンス上必要とされることをきちんと実施していました。しかし、当該アルバイトにとっての「つぶやき」は、単なる友人への報告であり、このように情報が第三者に拡散するなど予想すらしておらず、研修や誓約書によって禁止された行為と結びつかなかったのです。

Twitter が引き起こした事件の最大の特徴は、「情報の伝播速度が従来のメディアをはるかに超えて瞬く間に分散拡大するという点」、「従前の企業不祥事における従業員の多くが、悪いと知りつつ違法な行為を行っていたのと異なり、Twitter の発信者に悪いことをしているという自覚が全くないという点」です。

それでは、企業はどのような対策を取ることができるのでしょうか。

社員に対し、Twitter、Facebook 等の SNS は従来の枠を超えた全く新しい情報発信ツールであって、日ごろ活用しているメールとは異なり、開示した友人以外にも急速かつ無限定に伝達・拡散する可能性を持つものであることを、実例を挙げて徹底して教育することが重要です。SNS の仕組みといった抽象論・機能論だけではなく、個別事件の詳細を説明し、生の事実を実感してもらうことが効果的です。

SNS を巡る事件・事故の主な原因を分析すると、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、一般のメールと同じように考えているということです。であれば、その意識を修正すること、つまりその点に関する認識の誤りを是正する教育こそが事故防止の対策となります。

4.3 SNS を利用した販促の落とし穴

「Twitter で、一方的に宣伝メッセージが送られてくるので不愉快です。一体どう言うことですか？」こんな問い合わせが会社に殺到しました。ワインにちなんだエッセーを募

集する販促キャンペーンの告知に、Twitter を利用したのが反感を招いた原因でした。

ユーザが投稿したキーワードに反応して自動でメッセージを返信する BOT と呼ばれる仕組みを使って、Twitter で「ワイン」というキーワードを使うと、「ワインにまつわる思い出のエッセーを募集しています」などというメッセージが自動的に送られるものでしたが、この自動で送られる宣伝メッセージが消費者の反感を買ってしまいました。

ネット上の“炎上”は一向に収まる気配がなかったので、Twitter 上のアカウントを停止してキャンペーンを中止しましたが、個人情報漏えい事故のように、誰かに被害を与えたわけでもないので、ホームページにおわびを出すことはしませんでした。

それが今度は「不祥事を隠蔽するとは何事か」とネット上で新たなバッシングの材料となり、さらに炎上しました。マスコミにも面白おかしく取上げられ、“鎮火”に手間取り、キャンペーンは失敗し、関連商品の売上は大きく落ち込む結果となりました。

ネット上で炎上を防ぐためにはどのような対策が必要なのでしょうか。

炎上する前には、必ず、一定の苦情等の書き込みが寄せられるようになり、それが SNS の持つ伝播力によって急速に拡大していきます。したがって、その火種の段階を少しでも早く把握することが炎上を防ぐことになります。そのために Web のモニタリングを行います。Web の直接監視という方法と併せ、最初に様々なクレームが入ってくる、企業のお客様相談窓口での情報収集も行います。従来のメディアに比べて極めて伝播速度の速い SNS を端緒とするクレームの場合は、時間との勝負になるので注意が必要です。

炎上の火種を見つけたら、直ちに広範な情報収集を行い、自然鎮火を期待できないと判断したら、素早く企業として、事実調査の発表や謝罪などの意見表明を Twitter の公式アカウントや Facebook の企業ページなど、問題発生の端緒となった SNS を活用して発信します。もちろん、自社のホームページでも正式の見解を公表して、同時に Twitter や Facebook からの発信でリンクを貼ります。プレスリリースや記者会見まで行うかどうかは、事件の深刻さの度合い等、状況に応じて考えます。

また、お客様相談窓口での対応の不備が、さらにネット上で取上げられて、問題とされることも多いことから、リアルの世界におけるお客様相談窓口での対応と、ネット上での事故対応を十分にリンクさせることが必要になります。事故対応における意見表明のポイントは、「事実」を誠実に開示し続けるということであり、批判等に対して、直接の「反論」や「釈明」は行わないことです。

4.4 怖い「なりすまし」

SNS を使った「なりすまし」が多発しています。Twitter で偽アカウントを使い、有名企業の社長になりすましたユーザが現れたり、また別の有名企業の取締役を名乗るユーザが Twitter で特定の人物を批判したりするような内容の書き込みを行い騒動となりました。

さらに、ある企業の社員が SNS のグーグル＋で「採用担当者」を装い、実在しない「30歳の専門学校生」を面接しているという虚偽の「面接の実況中継」を配信して炎上した事例もあります。

SNS を活用したソーシャルリクルーティングにおいても、第三者が偽りの採用ページを立ち上げたり、偽アカウントを使って企業の社長やリクルーター社員になりすましたりすることで、トラブルが発生した事例もあります。

また、なりすましとは違いますが、ソーシャルリクルーティングでは、リクルーター社員が SNS を使って就職希望者とコミュニケーションを図るという手法が取られますが、リクルーター社員の個人的な発言が企業の公式見解と受け止められたり、リクルーター社員が、就職希望者からの質問や書き込みを無視する態度を示したり、企業に対する批判的な内容の書き込みに対して強く反論したり、相手を攻撃・非難するような内容の書き込みを行うなどの不適切な対応をした場合、リクルーター社員のアカウントや企業のサイトが炎上して、却って企業の評判に傷をつけてしまう恐れがあります。

このような事態を防ぐためには企業がするべきことは何でしょうか。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に、「ソーシャルメディアポリシー」を公表します。ソーシャルメディアポリシーとは、企業のソーシャルメディアの利用方針を示すものです。通常、ソーシャルメディアポリシーには、企業及び自社従業員がソーシャルメディアを利用する際の基本的姿勢、公式ページや公式アカウント、問い合わせ窓口などが掲載されます。ソーシャルメディアポリシーに公式ページや公式アカウントが表示されていれば、なりすましが現れた場合でも、ソーシャルメディアポリシーを見て確認をすれば、すぐになりすましであることが発覚します。

また、社員が発信する情報はあくまで社員個人の見解によるものであり、企業としての公式の見解は企業の公式ページで公表する旨を表明しておくことで、誤解や混乱の発生を防止することもできます。

さらに、問い合わせ窓口を明示しておくことで、何か問題のある書き込み等がなされた場合にも、すぐに企業がその事実を把握することができ、早期に対応を取ることが可能となります。

4.5 ソーシャルメディアハラスメント

ソーシャルメディアハラスメントは、いわゆるソーシャル時代の新たな悩みとして今年に入って注目されています。ソーシャルメディアハラスメントの典型例として、Facebook のような実名登録制の SNS で上司に友達申請され、SNS 上で上司に気を使わなくてはならなくなる、というような状況を挙げることができます。「いいね！」ボタンを押すなどしてやたらと絡んできたり、自分に絡んでほしいと要求してきたりして気疲れの元になるこ

とが問題に発展します。「上司から友達申請がきたら、断りづらい。でもプライベートのことや、個人的なつながりまで知られてしまいイヤだ。」、「見たくない上司の書き込みをいつも見せられる。“いいね”を押さないといけない気がして、憂鬱になる。」、「仕事の愚痴をついつい書いていたら、SNS 上で説教された。」というような声も聞かれ、上司や先輩からすれば、「親しみの気持ち」「仲良くなりたい」といった気持ちからですが部下はそうは受け取りません。この気持ちのズレがハラスメント（ソーシャルハラスメント）問題に発展することを認識しなければならないと思います。

企業としては、「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してソーシャルメディアに職場関係が持ち込まれて、ハラスメントに発展しないようにしていくことが必要です。

4.6 SNS 疲れ

SNS を利用していると精神的疲労や身体的疲労を感じたり、又はその疲れに気づかずに隠れ疲労になったりしてしまうことがあります。
日本で最もネットが見られている時間は、深夜 12 時～1 時までというデータがありますが、もう少しだけと思い返信していたり会話が盛り上がったりすると、3 時や 4 時になってしまうということもよくあることです。

好きでやっているので気にならないようですが、本人が気づかないうちに深刻なほど疲れがたまってしまうことがあります。このような状態になると倦怠感が抜けない、昼間の集中力に欠ける、頭がボーっとするなどの症状が現れ、業務の効率が低下してしまいます。

また、Twitter を活用して企業の情報発信をしているような業務利用のケースでは、名も知らぬユーザから非難されたり、罵詈雑言を吐かれたりすることもよくあり、情報発信を行っている企業担当者がそうした声にまともに取り合っているうちに、対応について悩んで、最悪、鬱を発症してしまいます。

いずれのケースでも「SNS 疲れ」は、労働効率の低下や、従業員のメンタル問題への発展など企業のリスクに直結する問題になってきています。

企業としては、「SNS 疲れ」が企業にとってリスクとなり得ることを認識し、従業員に対しては具体的な事例を通じて適度な利用を促すこと、企業活動における SNS 利用に潜むこのようなリスクに対し、担当者の精神的なケアに配慮することが必要になってきています。

5. 教育・啓発

本章では、スマートデバイスや SNS を利用する際の教育・啓発の状況について示します。

スマートデバイスや SNS を業務利用する場合はもちろん、私的に利用する場合でも使い方を誤ると、情報セキュリティ事故が発生し社業に悪い影響を与えかねません。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。情報セキュリティガバナンス協議会では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。

5.1 教育・啓発手法

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す。

5.2 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）や、警察への届出・社への報告などの手続きが多くの会社で取上げられています。また、営業情報・個人情報の流失・紛失・盗難の危険性や事故の際の影響なども取上げており、各社とも情報セキュリティ事故を教育のポイントとしています。その他では自社の規則・ルール、利用に関する手続きなどの説明もよくなされているようです。

表 5-1　スマートデバイスの教育内容

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	★★★
紛失・盗難の危険性	★★
スマートフォン利用に関する申請・届出方法	★★
個人情報の流失の危険性	★★
事故が起きた時の影響（金額、業務負荷の増大）	★★
ウイルス感染の危険	★
紛失の際の弁償方法	★
GPS 機能で移動履歴が明かされる場合がある	

★★★多くの会社で説明　★★半分程度の会社で説明　★あまり取上げられていない
（★が付いていない設問は､アンケートでは各社とも取上げていないと回答されたもの）

5.3 SNS の教育内容

不特定多数に閲覧されている可能性、転載（リツイート等）による情報の拡散、一度公開した情報の削除の難しさなど､SNS の特性から生じる危険性を認識した上で利用するよう注意喚起しています。SNS 上で法令違反の発言をしない、他社・個人への批判中傷をしない、などの SNS の基本的マナー教育も行われています。

不適切発言による炎上の危険性はもちろん、個人の発言が社の見解とみなされてしまう危険性や私的発言により社が謝罪する場合があるなど個人の発言が会社にも影響を及ぼす危険性も取上げられています。

表 5-2　SNS の教育内容

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	★★★
不適切な SNS での発言による炎上	★★
私的な SNS の不適切な発言により、社が謝罪する場合がある	★★
SNS に一度公開した情報は完全な削除が難しい	★★
SNS は転載（リツイート等）で情報が拡散する場合がある	★★
SNS に関する自社の規則・ルール	★★
SNS では私的活動か会社の活動か明確にする必要がある	★★
SNS 投稿の個人の見解が社の見解とみなされる場合がある	★★
SNS で法令違反の発言をしない	★★
SNS の抽象的な発言でも業務内容を特定されてしまうことがある	★★
SNS を私的活動で発言する場合は社名を記載してはいけない（又は、投稿する時は社名を明かさなければならない）など社名記載に関するルール	★★
匿名による投稿でも推察され投稿者の個人情報がさらされる危険性	★★
SNS による情報発信は適切に行わないと、攻撃を受け炎上する場合がある	★★
公開設定ミスにより想定者以外から閲覧される危険	★
非公開で発言しても転載されることで公開されてしまうことがある	★
事故が起きた時の影響（金額、業務負荷の増大）	★
SNS の中には身分を詐称した「なりすまし」が紛れていることがある	★
会社の業務で SNS を投稿する場合は申請が必要	★
SNS に熱中するあまり精神的・身体的疲労を生じ業務に支障が出る危険	
SNS の友達申請の強要や閲覧の強要はソーシャルハラスメント	

★★★多くの会社で説明　★★半分程度の会社で説明　★あまり取上げられていない
（★が付いていない設問は、アンケートでは各社とも取上げていないと回答されたもの）

5.4 今後の課題

企業として必要なことを伝える知識付与型の研修は必要ですが、SNS は個人の裁量部分が大きいことから、さらに意識変革につなげていくことが求められます。

周辺リスクでもふれていますが、SNS は従来の枠を超えた情報発信ツールであり、発信の仕方によっては本人の意図しない事故やトラブルになってしまいます。これらのリスクを本当に認識するためには、最近起きている様々な事故・事件を参考に、従業員がこれを

自分も起こしかねない問題としてとらえ、気づき納得してもらうことが必要です。これにより SNS の正しい使い方が継続され、SNS の面白さがさらに享受できます。

また SNS に熱中するあまり精神的・身体的疲労を生じ業務に支障が出る危険性やソーシャルハラスメント についてはまだどの会社も研修プログラムに取入れておらず、これからのテーマと言えそうです。特に、職場におけるハラスメントとそれが起因するうつ病を始めとする精神障害は増える傾向にありますので、本テーマとは関係ありませんが注意を払う必要があります。

コラム「SNS を活用するためのマナー」

SNS はマーケティング・コミュニケーションの有効な手法として、各企業の業務上の活用や私的活用が盛んになっています。mixi、Twitter、Facebook などに加え、YouTube、USTREAM、ニコニコ動画などの動画サービス、GREE やモバゲーなどのゲーム系サービスも一般的に SNS として扱われますが、SNS の特性をよく理解して活用すればこれはこれで大変有効な広告媒体といえます。

では、SNS を道路に例えた場合上手に走行するマナー（もしくはルール）というのはあるのでしょうか。まとまったオーソライズされたものはありませんが、過去の炎上事例から、業務上の活用において最低限こうしなければ炎上しなかったのではないかというものをまとめたものがあります。(技術的な対応を除きます。)

炎上させないための「べからず集」[2]

・運営者の身分や企業との関係性を隠すべからず
・不誠実、不公平な対応はするべからず
・各種法令を違反するべからず（道交法や薬事法など）
・不謹慎な発言はするべからず
・他社批判をするべからず
・オンライン・オフラインの対応を区別するべからず

言われてみれば当たり前のことです。私的活用であれば、１番目を外し、代わりに「業務上知り得たこと（社外秘）を公表すべからず」とすれば経験的には納得がいきます。

マナーを守っているにもかかわらず炎上してしまったらどうするのか。過失があるなら率直に謝り、言いがかりであれば毅然と真摯に対応します。対応が間違っていなければ、いずれ沈静化するはずです。炎上しないにこしたことはありませんが、過度に炎上を恐れる必要もありません。

そして何より大切なことは、ユーザや消費者の声を真摯に受け止め、積極的な対話を行っていくことです。SNS のリスクを十分踏まえた上で上手に活用していくことが、ネット時代に求められているのです。

[2] 『「炎上」させないための「べからず集」』http://marketingis.jp/archives/1938

コラム「「Twitter」被害の今昔」

Twitter が登場したのは、マーケティング・コミュニケーションの効果的な手法の一つとしてブログが注目を集めたのとほぼ同時期です。

ブログは、それなりの継続性、文章力、訴求効果などが求められるためその運営は労力・コストがかかるのに対し、「ミニブログ」と呼ばれる Twitter はその瞬間の気持ち(感情) を 140 文字以内という短い言葉で伝え共有することが目的のため、正しく使っている限り気楽な手間のかからないコミュニケーションの一手段と言えます。

では、かつて企業では Twitter 被害に類する問題はなかったのでしょうか。次のような事例が思い起こされます。

①エレベーターやロビーでの立ち話（噂話等）が他部門の人間に聞かれ、社内に部外秘（個人情報含む）の情報が拡散

②居酒屋で会社の営業情報を話題にし、それが他社に盗み聞きされ漏えい

これらの対策はどちらかというと、従業員のしつけという観点から新人教育や部門内会議での周知徹底や酒席を含む OJT で再発防止が図られました。

Twitter はもともと不特定多数の人間との感情共有であるため、事例で言う第三者を最初から大量に含んでおり、感情共有の醍醐味とリスクはセットです。特定の人間との感情共有であれば、発信者の内容訂正もきき、相手が制止してくれることもありますが、Twitter にその機能はありません。

Twitter の私的利用を「イソップ寓話」に置き直してみると・・・

ミダス王はロバの耳をしていてそれを隠していました。いつも通っている床屋はそのことを知っていたが口止めされていました。ところが遂に我慢できなくなって井戸の奥に向かって『王様の耳はロバの耳！』（業務上知り得た秘密）と叫ぶと、その声が井戸という井戸に伝わり皆にそれが知られてしまいました。

この井戸を Twitter に置き直すとわかりやすくなります。

企業は、「Twitter 炎上事例」を従業員に説明し、その被害の詳細を明らかにして自覚を促すことが第一歩となります。理解で終わることなく自分の問題として納得し意識変革・行動変革に結び付ける契機としなければなりません。

あまり紹介されていませんが従業員（発信者）個人の被害（制裁）も相当なものがあります。**本人の身分、履歴、写真、家族の状況などプライバシーが SNS に掲載され、削除しても即 UP されるなど心身ともに傷つく例が散見されます。イソップ寓話ではミダス王と民衆は床屋を許しますが、SNS では民衆は発信者を許しません。いつまでも発信者のプライバシーが晒し者になり、期限のない「ネットハラスメント」の被害者となる場合があります。**

軽率な行動の帰結として、企業も従業員も自覚する必要があります。

コラム「なぜ、人は SNS を使うのか」

Twitter や Facebook 等のソーシャルメディアを通じた情報漏えいや炎上が懸念される一方、若い世代を中心に急速に普及していることは紛れもない事実です。

とはいえ、ソーシャルメディアを利用していない方からすると、“自分の日記を人に見せて楽しいのか”“電話やメールで十分”、という意見も多く、**“使う人間”と“使わない人間”のギャップは大きいよう**に思えます。

本コラムでは、ソーシャルメディアを使う人間にとってのメリットを挙げてみました。

●情報を入手する手段として使う

情報感度の高い人間が様々な情報をリアルタイムに公開してくれるため、**自分の欲しい情報をすぐに入手できる手段として非常に有効**です。

実際に東日本大震災では大手マスメディアが報道しない地域のスーパーの在庫情報や被災地の知人の安否等を迅速に共有する手段として評価を高めました。また、**自治体や政府も情報共有手段としての SNS に注目し、防災の分野においては積極的な活用を推奨しています。**

一方でデマや風評被害が拡散しやすいことも事実ですが、スマートデバイスという“いつでもどこでも情報を入手・発信できる道具”を結びついたことで、情報を入手できる速度や量は飛躍的に高まっています。

また、国際的には**欧米を中心として名刺（ビジネスカード）代わりに Facebook でつながる、というケースも増えています。**実名のコミュニケーションであるため、今後の連絡には“SNS の方が便利”という新しい常識ができつつあります。

このように、SNS によって**必ずしも全員が自分の情報を外部に公開しているわけではなく、知人の近況や自分の趣味、場合によっては仕事関連の情報を迅速に入手するための道具として価値を見出している方も多い**です。

●ライフログ（備忘録）として使う

自分のアイデアや気になったことをすべて覚えていられる方がほとんどいません。

SNS 等のサービスは、パソコンであろうが、スマートフォンであろうがどのデバイスからでもアクセスができますし、また、検索も容易です。

日記やインターネットで見つけた気になること、買いたいもの等を SNS に記録しておくことで、後で容易に検索することができたり、移動中のスマートフォンでインターネットを見ながら見つけた仕事上のヒントを、後で家や会社のパソコンであらためて見返したり、といった利用方法にメリットを感じている方も多いです。

他人に公開せずに自分だけの備忘録にすることもできますし、食事や読書、スポーツの記録等、趣味などに合わせたサービスもあります。

●反応とつながりを満たす手段として使う

人間には“人とつながりたい”という根源的な欲求があるようです。

また、どのような活動であれ“他人に見られている”という環境に身をおくことは目標の達成率を高める傾向があります。

一人でダイエットをするよりも有志をつのって一緒にダイエットをした方が達成効果は高いようです。これはお互いの存在を意識することで途中放棄することを防ぐ“仕組み”であり、“自分の活動に誰かが反応してくれる”ことをモチベーションに返る仕組みであったりします。

個人の利用においても、企業の利用においても、SNS を通じて“誰かとつながっている”“反応がある”ことに、潜在的な欲求を満たしているという要素があるといえます。

●感情を速やかに伝える手段として使う

“簡単”かつ“すぐ”に感情を伝えることができる手段である、ということは SNS の一つの特徴です。手紙やメールでも、すぐに返事が返ってくることはビジネスで重視される点でもある一方、うまい文章が書けなかったり、表現が稚拙であったりするとコミュニケーションを阻害してしまう場合もあります。

例えば Facebook の「いいね！」ボタンは、共感という反応を簡単に相手に伝えられる手段であり、LINE はスタンプと呼ばれる喜怒哀楽を表現できる画像を絵文字代わりに利用することで人気となっています。(文章よりも顔文字、顔文字よりも画像の方が、より簡単に自分の感情を表現できる、ということです)

手紙がメールにとって代わられてきているように、**今日のコミュニケーションはより即時性を求められるようになっており、それを実現する道具としてスマートデバイスが、また、実現するサービスとして SNS が注目を集めるようになってきた**、ということは事実です。

●自己表現欲求を満たす手段として使う

ネットワークを介して、居住している地域や場合によっては国籍も超えて交流できる場ができたことは、**自分の存在価値や市場価値を PR する場**としても活用されるようになりました。自分の考えやスキルをうまく外部に認識してもらうことができれば自分や所属する組織の価値向上につながります。

また、“愚痴”や“批判”もネガティブではありますが、“自分の考えの正しさ”や“他人や世間の間違い”の表明することで自己の欲求を満たす手段ですし、“ここだけの話”のような自分しか知らない情報を他人に開示することも、“こんな情報を知っている自分”の価値を他人に認めてもらいたい、という欲求の表れと言えます。

“上司の無責任で愚痴る”のも“昨日、街で芸能人を見た”も、根っこの部分は、自己の欲求を満たす表現の表れであり、その場所が、**近所の居酒屋からいつでもアクセスできるネットの空間に変わってきた**、と言えるのかもしれません。

まとめ

この報告書では、スマートデバイスを含む情報セキュリティの管理の話から、スマートデバイスにまつわるリスク、そしてその対策についてアンケート等の結果を踏まえて議論してきました。また、スマートデバイスの普及とともに急速に利用が広がっている SNS 利用の周辺リスクについても検討しました。そして最後は普及・啓発の重要性や具体的な対策例についてもふれました。内容についてはいかがでしたでしょうか。

網羅性が不十分と感じた方もいるかもしれません。各論点の深掘りが不十分と感じた方もいるかもしれません。各章毎のつながりが不明確でばらばら感があると感じた方もいるかもしれません。正直なところ、そのような指摘はそのとおりだと思っています。この報告書はワーキンググループの「メンバー全員」で分担して執筆したものです。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。「現場」ならではのすばらしい内容になっていると自負しています。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。

20 年ほど前のことですが PC が普及し始めた頃、「一人一台 PC を買い与えるのか」という議論があったように思います。今では当然のように一人一台の PC が与えられています。スマートデバイスも使うか使わないのかという時代ではなく、使うのは当たり前でどのように有効に使うのか、どこまで使いこなせるのかというのが話題の中心になっていくのでしょう。そして、あと数年もたてばこの報告書でいろいろと議論されたことも「そういう時代もあったなぁ」と振り返るような「当たり前のこと」になっているのかもしれません。そういう時代になった時、「そういう時代になったのはこの報告書があったからだ」と私たちはそのとき思うことでしょう。スマートデバイスや SNS の普及時にみんなで知恵を集めて考えたことがやがて現場での実践となって定着していくのです。

繰り返しになりますが、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。読者のみなさん、是非目を通して活用してください。

最後に、ワーキンググループのみなさん、事務局のみなさん、ありがとうございました。こんなすばらしい報告書ができました。ありがとう。

主査　丸山　満彦

用語集

スマートデバイス

多様な用途に使用可能な多機能端末。本報告書では、スマートフォンやタブレット端末の総称として用いています。

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。

クラウド

情報システム（アプリケーション、ミドルウェア、OS、ハードウエア等）を、ネットワークを通じ、サービスの形で必要に応じて利用すること。

オンプレミス

情報システムを自社の設備に導入・設置し、運用すること。

SaaS（Software as a Service）

ユーザが必要とするソフトウェアの機能だけをサービスとして配布し､利用できるようにした形態。

VDI（Virtual Desktop Infrastructure：仮想デスクトップインフラ）

クライアントPCからデスクトップ環境を分離し、サーバ上の仮想環境に集約するもの。

BYOD（Bring Your Own Device：私的デバイス活用）

従業員が私物のスマートデバイス等を企業に持ち込んで業務利用すること。

BCP（Business Continuity Plan：事業継続計画）

自然災害等、事業が存続できなくなるリスクを事前に想定・分析し、最低限の業務や、復旧時間・対応策等を事前に策定しておく行動計画のこと。

キッティング

情報システムの新規導入時、各種機器の組立や配置・配線、必要なソフトウェアのインストール、各種設定等を行う作業のこと。

ブラックリスト／ホワイトリスト

ホワイトリストは事前に登録したもののみフィルタを通し、ブラックリストは登録したもののみフィルタを通さない仕組み。

リモートワイプ

スマートデバイスが保存しているデータを、遠隔地から通信回線経由で消去したり、無効化したりする手法

炎上

ネット用語でサイトの管理者やコンテンツの提供者に対して批判的な書き込みが殺到すること。

検討メンバー

■メンバー

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
富士ゼロックス株式会社	今村　光
一般社団法人日本コンプライアンス推進協会	上村　広志

（社名五十音順）

（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