私有スマートデバイス取扱規程サンプル第2版及びスマートデバイス・セキュリティポリシーサンプル第2版解説書

CSAJ Computer Software Association of Japan
一般社団法人コンピュータソフトウェア協会

contents

1 はじめに

１．本解説書の目的

本解説書は BYOD（Bring　Your　Own　Device）と言われる、従業員私有のIT機器特にスマートフォンやタブレットPCを業務利用するに当たり、企業が事前に決めておくべき規程やポリシーを解説したものです。これからBYODへの取り組みを行う企業、あるいはすでに実施している企業においてBYODによるリスクを低減、回避するために「規程サンプル」及び「セキュリティポリシーサンプル」とともに提供いたします。

企業では、競争力の向上やコスト削減の目的で長年にわたりIT機器を利用してきました。どの様な目的でIT機器が使われるかは各社の業務内容、規模、IT化への取り組み度合い、時代など多くの要因によって様々ですが、企業では業務に使用するIT機器は企業側で調達し従業員に使わせるという形態が多かったように思います。しかしながら昨今、私物のIT機器を職場内に持ち込み業務に利用する形態が欧米を中心にみられるようになりました。その背景には、IT機器の小型化や低価格化が進み個人でのIT機器所有が増えた事、電話の機能とパソコンの機能を併せ持つ「スマートフォン」「タブレット」の普及、回線速度の向上、クラウドサービスなど携帯機器から利用しやすいサービスの増加が考えられます。

BYODで業務を行う事には多くのメリットがあると言われています。従業員が複数のIT機器を携帯せず、自身の使いなれた物で業務を行うことによる効率アップや、場所・時間にとらわれず業務を行える点、企業側にとっては機器の初期コストの低下が可能になる、機器のメンテナンスを企業が行う必要がなくなる等のコスト削減効果のほかに、震災以降注目される在宅によるワークスタイルの実現も可能になるかもしれません。さらに積極的に考えれば、いつでもどこでも好きな時に業務する新たなライフワークスタイルを実現する可能性が高まります。

一方で私有機器に企業の情報が保存されることや、セキュリティ強度をコントロールしにくい個人用IT機器からの社内ネットワークアクセスによるセキュリティの懸念が発生します。また労務時間の自由度向上は労務管理の困難さもはらみ、新たな労使間の課題が生まれることもあるでしょう。

このような状況からコンピュータソフトウェア協会セキュリティ(BYOD)研究会では、企業がBYODの取り組みを行う際にどのような点を検討し、事前に取り決めをしておくことが必要なのかを議論し規程とポリシーをサンプルとともに用意いたしました。

ITの技術的な側面よりもむしろ従業者と企業の関係性の中で検討すべきところ、決めておくべき事を中心にまとめました。

既にそのような取り決めがある場合には自社の規程類の見直しに、まだそれらがない場合には参考にしていただき、より効果的なBYOD導入を実現していただきたいと願うものであります。

2．本解説書の構成

本解説書は就業規則の一部に相当する「私有スマートデバイス取扱規程サンプル第2版」及びガイドラインに相当する「スマートデバイス・セキュリティポリシーサンプル第2版」をそれぞれ解説し、いくつかのトピックについては「コラム」と言う形で記載しました。また巻末にはBYODを導入する企業の手助けとなるであろうソフトウェアを紹介しています。

ただし、本解説書の情報は本解説書執筆時点の情報であり、ご参照いただく時点の情報とは異なる可能性もありますのでご留意ください。

3．本解説書を利用するにあたって

本解説書及び各種サンプルは、特定の前提条件を想定し記載されたものです。それぞれの記載内容が必ずしも参照される各社の状況にそのまま合致するものとは限りませんが、各条項や項目にあげた事象についての検討がなされているかについて確認していただくことをお勧めします。

また本解説書を除く各サンプルについては、改変しての利用が行いやすいよう著作権の設定をいたしました。

なお、「規程サンプル」及び「セキュリティポリシーサンプル」の策定にあたり、専門家の立場からアドバイザーとして多大なご協力を賜りました鈴木　雅一 氏（ピー・エム・ピー株式会社　代表取締役 特定社会保険労務士 HIS認証コンサルタント）と中山　裕人 氏（ブレークモア法律事務所　弁護士）に、心から御礼申し上げます。

2013年7月
一般社団法人コンピュータソフトウェア協会
セキュリティ(BYOD)研究会　主査　小屋　晋吾

2 サンプル規定・ポリシーの前提条件

2.1 対象社員

役員を含む社員（正社員、契約社員、嘱託社員、パートタイマー、アルバイト）

2.2 対象機器・OSなどシステム条件

使用可能端末、OSについて制限あり。但しサンプル中には特定の端末、OSの記載はしていない。

2.3 対象業務

特定の業務を対象とせず。

2.4 使用を許可される条件

以下の条件をすべて満たした場合に使用が可能となる。
・対象社員であること
・所定のフォームに則った許可申請を提出、承認されること
・会社が実施する所定の教育プログラムを受講し受講報告書を提出すること
また使用許可を得た後に標準導入するソフトウェアを規定しており、それらソフトウェアの導入が必須とされている。

2.5 可能な作業（動作）

電子メールの閲覧、業務で使用する情報資産、顧客情報、業務アプリケーションの使用など及びVPN、有線・無線LAN等への接続。

2.6 禁止されている作業（動作）

・端末の改造（JailBreakやRoot化など）
・私的アカウントで使用するアプリケーションやサービスへの企業の情報資産、営業秘密のデータ転送、共有
・サンプル上は具体的な表記はしていないが一部機能制限を行うエリアがある旨の表示あり
・サンプル上は具体的な表記はしていないがスマートデバイス持ち込み制限エリアがある旨の表示あり
・会社から電子証明書を配布する場合、電子証明書の削除、複製、保存、譲渡、貸与、公開等
・MDMを利用している場合、そのソフトウェアや設定ファイル等の削除・変更など

2.7 管理の為に使用しているツール

・MDMについては使用の場合、不使用の場合を併記した。

2.8 スマートデバイスの利用方法の定義

「スマートデバイス取扱規程 第4条」では、対象となるスマートデバイスの利用方法として、当社が指定する経路／方法で自社のネットワーク（LAN）に接続し、スマートデバイス本体の画面にて情報の閲覧／加工を行う事を利用することを想定している。
そのため、スマートデバイスが一般的に備えている下記の様な機能については、「スマートデバイス取扱規程」の定義外である。これらの機能の利用については、スマートデバイスの利用許可とは分離して別途定義する必要がある。

・wifiルーターとしての利用（テザリング）
インターネットへの接続経路を他の端末へ提供する利用方法である。そのため、当社が指定する以外の経路を提供する事になるため、本規定で想定している利用方法から外れる。情報セキュリティマネジメントシステムの観点からは、アクセス制御方針として定義される事項である。

・リムーバブルメディアとしての利用
外部記憶装置としてデータを保存する利用方法であるため、本規定で想定している利用方法から外れる。ＵＳＢメモリなど、リムーブバブルメディアの取扱規程と同様に定義する必要がある。

3 私有スマートデバイス取扱規程サンプル第2版解説

3.1 第1条　目的

従業員が私有の携帯用機器を職場に持ち込み、それを業務に利用することを一般的にBYOD（Bring your own device、ビーワィオーディ）と呼ぶが、本規程では、私有の携帯用機器の内、スマートフォン、タブレットなどのスマートデバイスに範囲を限定した。会社がこれを認める場合に規定しておかなければならない事項について、規程サンプルおよびポリシーサンプルとして作成したものである。
私有スマートデバイスの利用を会社が認めることで、利用者は自分の普段使い慣れた機器をいつでもどこでも利用できることになる。会社側としては、業務の効率化や災害時における安否確認などで迅速な対応が期待でき、導入や教育などにかかるコストを抑える効果が期待できる。しかしながら、私有スマートデバイスを利用して会社の情報システムや情報資産にアクセスすることによるリスクも、想定しておかなければならない。例えば、私有スマートデバイスの紛失時や情報漏えい時に、どのように対応していくかといったセキュリティ対策の検討が必要である。なお、私有スマートデバイスの利用にあたっては、個人情報保護や機密情報取り扱いなどを定めた社内規程や手順書との整合性についても検討いただきたい。

3.2 第2条　対象

委託事業者、派遣社員に対して原則禁止としているが、許可する場合は委託事業者、派遣元事業者との基本契約や、本人との誓約書として遵守事項を盛り込むなどの対応を検討いただきたい。

3.3 第3条　定義

「スマートフォン、タブレット等の携行可能な情報通信機器もしくは当社が判断した機器」といった抽象的な記載としているが、規程ということで特定のメーカ名、製品名の記載を避けた。具体的にはiPhone、iPad、Android、Android Tablet、Windows Tabletなどを想定しているが、対象機器を限定する場合など状況に応じ記載方法を検討いただきたい。また、将来的にはウェアラブル、時計、眼鏡などの形態が考えられる事から、「もしくは当社が判断した機器」としている。

3.4 第4条　利用許可

私有スマートデバイスの利用は、希望する者が上長承認のもと利用申請を行い、会社が承認した場合のみ許可する申請・承認形態とした。「新規」、「機器追加」、「解除」の３パターンの申請書と、会社が利用許可を決定した際に使用する「決定通知書」を用意しているので参考にされたい。例えば、利用者が機種変更を行う際は「解除」申請の後、「新規」申請とする。「機器追加」は、２台目以降のスマートデバイス申請で利用いただきたい。申請書には、「希望する利用範囲」と「同意事項」を掲載しているので、状況に合わせ加筆・修正いただきたい。なお、私有スマートデバイスの利用を会社が認めたことによる、時間外の業務利用など労務管理の考慮が必要である。
第4項は、例えば社員等が前職（仮にA社とする）で得た営業秘密等の情報を私有スマートデバイスに保有し、かつその情報をもとに営業行為などを行っていた場合、自社がA社から訴えられるリスク（自社は社

員等が営業秘密を持っていることを知りながら利用させていたのではないかなど）を回避するために入れている。
教育については、別途条項を定めて詳述してもよい。以下の条項案では、定期的に教育訓練を行うことを想定している。
（教育訓練）
第X条　当社は、社員に対し私有スマートデバイスの利用に必要な知識、技能、資質の向上を図るため、定期的に必要な教育訓練を行う。
2　社員は、当社から私有スマートデバイスに関する教育訓練を受講するよう指示された場合には、特段の事由がない限り指示された教育訓練を受け、受講報告書を提出しなければならない。

3.5 第5条　費用負担

会社は「費用を一切負担しない」との立場をとっているが、MDM（Mobile Device Management）やセキュリティ対策製品の導入、業務アプリのインストールなど、状況により会社負担を考慮する必要がある。
発信時に特定の番号を付加することで、通話費用を会社払いにするサービス等の利用も可能である。
なお、労働者に情報通信機器等、作業用品その他の負担をさせる定めをする場合には、当該事項について就業規則に規程しなければならないことが労働基準法第89条3項に定められているため、第5条を入れる場合には、就業規則との紐づけが必須になります（常時十人以上の労働者を使用する使用者の場合）。

3.6 第6条　善管注意義務

BYODでは、業務に私有スマートデバイスを利用することから、本条ではその私有スマートデバイスの管理・運用に対し、社員の善管注意義務を求めるものである。
第1項では個人情報保護、不正競争防止、情報管理に関する一般的な知識を前提に、業務上の管理、運用を求めている。これらの一般的な知識については、当然、個人によってばらつきが生じることから、解釈の違いが起こる恐れがある。従って、第4条4項の「私有スマートデバイスに係る教育プログラム」が重要となろう。教育プログラムでは、個人情報保護法、不正競争防止法、情報管理規程での「守るべき事柄」、「守られなかった際に発生する企業の金銭的な被害や信用の失墜」、「罰則規定」、「規範的な行動指針」等の分かりやすい事例解説が必要である。個人情報保護法については消費者庁[1]、不正競争防止法については経済産業省[2]に詳しい資料があるので参考にされたい。
第2項は、情報セキュリティにおける環境変化が激しいことから、利用者に対して最新の規定を常に理解することを要件としている。本規程の改訂は就業規則の改訂となるため、労働者（社員）に周知したときに効力が発生するので留意されたい（労働基準法第106条[3]）。なお、厚生労働省の定める周知方法は、以下の通りである。

・常時各作業場の見やすい場所へ掲示し、又は備え付けること
・書面を労働者に交付すること
・磁気テープ、磁気ディスクその他これらに準ずる物に記録し、かつ、各作業場に労働者が当該記録の内容を常時確認できる機器を設置すること

第3項は、業務とプライベートの情報、データの分離を求めるものである。スマートデバイスの情報は多くがクラウドサービス等の外部記憶域に保存されることから、社外秘情報とプライベート情報の混在を許してしまうと、個人ごとに社外秘情報が異なるクラウドサービスに広く拡散してしまう。そのため、情報漏えい等のインシデントが発生した際の原因究明や対策が困難になる可能性が高い。企業が利用許可した外

[1]消費者庁 http://www.caa.go.jp/seikatsu/kojin/gimon-kaitou.html
[2]経済産業省 http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/2012hontai.pdf
[3]労働基準法 第 106 条　使用者は、この法律及びこれに基づく命令の要旨、就業規則（略）を、常時各作業場の見やすい場所へ掲示し、又は備え付けること、書面を交付することその他の厚生労働省令で定める方法によつて、労働者に周知させなければならない。（第二項略）

部ストレージにおいても、同一アカウントに業務情報とプライベート情報を混在させず、アカウントを分けて利用させることが重要である。
他方、社外に広く告知するような社外秘ではない情報については、厳しい分別を求めることでBYODの利点を損なう可能性もある。「業務で利用する情報」の具体的な定義を明示し、「守るべき情報」とそれ以外の情報の基準を示し、迷ったら「守るべき情報」に区分させると良い。
第4項は、上長等への報告義務を課している。ポリシーにも「紛失」や「セキュリティ対策」のところで遵守すべき対応を詳述しているが、就業規則と紐づく取扱規程にも記載した。

3.7 第7条　監査

本条は、規程遵守の状況を企業が把握するための監査権を規定するものである。
企業が監査権を有することで規程の遵守が期待できるとともに、インシデントの怖れや発生における原因究明等が可能となる。一方で、監査におけるプライベート情報へのアクセスについては、企業の業務や取り扱う情報の特性に応じて規定されるべきである。この場合は、「業務情報の保存状態の開示」を「すべての情報の保存状態の開示」等にすればよい。但し、「すべての情報の保存状態の開示」とした際は、社員と事前の明示的な合意がなされていないとトラブルの原因となることが考えられる。利用申請書等での記述、教育カリキュラムでの確認等に留意されたい。

3.8 第8条　緊急措置

本条は、情報漏えいや不正アクセスなどのインシデント発生における私有スマートデバイスの利用解除について定める。情報システムや顧客データの保護のために企業が必要と判断された場合は、BYODの利用を解除し、運用を停止できるものである。
第2項は、社員の規程違反やマルウェアなどの感染等によって規程違反状態と考えられる場合の、社員の行うべき対応について規定しており、報告およびデータの削除措置などを義務化している。インシデント発生では、被害の拡散の防止において初動の措置が重要となるが、そのためには一定のITリテラシーが必要である。第4条第4項の教育において、マルウェアへの感染ケースやフィッシングサイト等の手口を解説し、初動の重要性を理解させ、組織全体で適切な措置を講じられる体制を整えることが重要である。
第3項は、削除対象となるデータに個人のデータが含まれることを明示するものである。
第4項は、インシデント発生時における上長の行動を定めたものである。BYOD導入によってインシデント発生の可能性は高まることが予想されるため、情報システム部門や管理部門だけでなく、全社的な素早い対応が可能な体制が重要である。部門の管理職に一定の行動規範を求めることで、リテラシーの底上げを図り、適切な措置を期待するものでもある。
第5項は、インシデント発生時に企業が私有スマートデバイスに対して強制的にデータ消去などができる権利を定めている。社員が削除を拒否した場合や、出張先などでスマートデバイスを紛失し、社員自らが適切な措置を講じることができない場合を担保している。教育や利用許可の際には、どのような状況で本項が適用されるかを解説するとよい。

3.9 第9条　免責

本条は、BYODでの利用責任が社員にあること、企業は免責されることを定める。スマートデバイスはプライベートな利用を含めて常時携帯されることから、持ち出しNote PCなどに比べて紛失の可能性が高く、企業が管理者として果たせる範囲が狭く、運用リスクを負わせるのは酷というべきである。一方で社員は、免責条項に納得がいかなければ私有スマートデバイスを利用しなければよい。
他方、企業が社員に適切な情報システムを提供せず、BYODを社員に押し付け、その上で一方的に企業の債務を免責する等は、逆に社員にとって酷であり、条項の規程をもってしても無効と判断されよう。

3.10 第10条　懲戒

本条は、懲戒を定める。違反とされる事項、本人の弁明、事実認定の機関、懲戒の種類を明示している。
本規程が実行されることを望むものではなく、あくまでも抑止として機能すべきものであり、また、懲戒処分におけるトラブルを未然に防止するためにも、規程違反のケースを分かりやすく解説することが重要である。
なお、懲戒の実施には、罪刑法定主義に基づき「理由となる事項」、「懲戒の種類・程度」、「就業規則の周知」が必要であり、単に本規程を取締役会で決議しただけでは効力を発しないことに留意すべきである。
懲罰委員会が設置されていない場合の条項案
（懲戒）
第10条　私有するスマートデバイスで当社の情報システムに接続する社員は、以下の事項に該当した場合、本人の弁明等、所定の手続きを経て、戒告、けん責、減給、出勤停止、降格、諭旨解雇、懲戒解雇の懲戒処分を決定し、これを実施する。

3.11 第11条　損害賠償

本条は、社員に対する企業の損害賠償請求権を規定するものである。
実際にBYODの運用結果、本人の不注意で大規模な個人情報漏えいを起こしてしまう可能性はあり、その場合、企業が実害を被るだけでなく、企業をとりまくステークホルダー（例えば、株主、他の社員、取引先、顧客）も大きな被害を受けることになり、公正の観点からは損害賠償請求はあってしかるべきというものである。
一方で、個人の賠償には限度があり、必ずしも企業の損害が補填されるとは限らない。前条の懲戒も含め、損害賠償のケースとなるような行為、事態を周知し、社員と組織の自戒を求め、BYODの適切な運用を期待する。

3.12 第12条　相談窓口

本条は、私有スマートデバイス取扱規程への疑問、運用上、制度上の疑義解消の窓口について規定する。
BYODの利用シーンは様々であり、スマートデバイスの発達や利用者の創意工夫によってより効果的な活用は容易に考えられる。一方で規程が想定しておらず、活用事例が規程違反となることも想定できる。業務遂行にかかる普遍的な価値、例えば平穏な業務環境の維持や就業態度などを定める一般的な就業規則と異なり、本規程は技術の発達によってよりよい解決策を求めるものであり、また、こうした機関（情報セキュリティ委員会等）の設置によって社員の利用リスクを軽減するべきである。

3.13 第13条　施行、改訂

本条は就業規則の施行、改訂を規定する。
労働契約法により、使用者が一方的に就業規則を変更しても、労働者の不利益に労働条件を変更することはできず、また、その変更が合理的で就業規則を周知させることが企業の義務となっている。
情報セキュリティ委員会及び取締役会ではこれらの労働法規上の規定を十分理解した上で、適切な措置を講じる必要があることに留意されたい。
本規定では、情報セキュリティ委員会が起案部門、取締役会が意志決定機関として記述しているが、実態に合わせ、適宜、変更されたい。
以下は、起案、決定機関を記述しない場合の条項案である。
（施行期日、改訂）
第13条　本規程は、平成XX年XX月XX日から施行する。

2　　当社は、必要に応じて本規程を改訂することができる。

3　　当社は、本条第1項の改訂にあたり、社員に対して改訂の周知徹底をはからなくてはならない。

4 スマートデバイス・セキュリティポリシーサンプル第1版解説

4.1 対象機器・OS

本項は、対象機器とOS、およびそのメンテナンスを規定している。
パターン１はMDMを利用している場合で、指示に基づきバージョンアップ等を実施することとしている。これは、会社がパッチ適用での弊害をテストすることを前提としている。テスト実施がない場合は、パターン2を参考されたい。
パターン２はMDMを利用していない場合で、最新のパッチを適用、バージョンアップについては、会社の指示に基づく、とした。バージョンアップでVPN等の会社指定のアプリケーションが動作しない、OSのダウングレードが困難な場合があるためである。MDMを搭載していない場合、リモート・ワイプの強制ができないことから、リモート・ワイプの利用設定も求めている。

会社の情報を私有スマートデバイスで運用させるに当たり、様々なリスクをコントロールする必要がある。リスクコントロールの一環として、利用させる機器やOSを限定する事が有効である。また、OSを含むソフトウェアには後述する「脆弱性」が存在するため、最新のバージョン、セキュリティパッチを適用する事が望ましい。

・対象となる機器とOSの種類
BYODの対象となる機器としては、スマートフォンやノート型のパソコンなどが当てはまるが、スマートフォンは、従来の携帯電話と比べて各メーカそれぞれのハードウェアとOSの違いがあり、それぞれに対してセキュリティの考え方や対処方法に留意する必要がある。
以下は、日本の市場で提供されている主なOS の種類一覧と、スマートデバイスを含めた特徴となる。

表 4-1

OSの種類	提供会社	特徴
iOS（iPhone/iPad）	Apple	Apple がデバイスとOSを1社で提供している。また、機器に合わせたOSおよびパッチを提供している。アプリは審査されたものだけが掲載される公式マーケットからのみインストールが許可されている。
Android	Google	Google が提供するOSで各メーカが独自にカスタマイズしてデバイスを提供している。OS バージョンが同一でも機種依存性があり、市場に複数のOSおよびパッチが存在している。また、アプリにおいては公式マーケットだけでなく、複数のアプリマーケットからのインストールおよびユーザ自身でインストールも可能である。
Windows 10	Microsoft	Microsoft がPC、タブレット、スマートフォン向けのOSとして1社が提供している。従来通りユーザ自身でアプリケーションをインストールでき、それらアプリへの検査機能は特にない。但しWindows ストアアプリに関してはMicrosoftで審査したものを公式マーケットからのみインストールが許可されている。

・OSのアップデートの重要性
OSやソフトウェアには、プログラム上の不具合や不適切な設計などが原因となる「脆弱性」が存在し、セキュリティ上のリスクがある。脆弱性には、動作不安定といった許容できるものから、悪意ある操作、

攻撃されるような危険なものも存在する。脆弱性に対しては、開発メーカより提供される「修正プログラムまたはパッチファイル」を定期的にアップデート（更新）する必要がある。
ただし、サポート期限が切れて修正プログラムが提供されなくなったソフトウェアやOSを使い続けることは非常に危険であるため、早急に新しいソフトウェアへのアップグレードや新たなソフトウェアへの切り替え、代替措置を含めた利用停止などの対策を検討する必要がある。

・アプリの入手方法（アプリマーケット）
電話、メール、スケジュールなどスマートフォンで利用する機能は全てアプリであり、スマートフォンの機能の有無は、アプリをインストールした数によって決まる。また、スマートフォンに保管されているデータ（連絡帳、メール、写真等）は、企業、個人の区別することが困難であるため、データの保護を保つためには、アプリの共有制御は必要不可欠となる。
スマートデバイスのアプリは、デバイスの出荷時に予め提供されているものと、利用者がアプリマーケットからダウンロードして利用するものがある。マーケットは、各OS提供元、または通信事業者やデバイスメーカなどが提供しているものがある。マーケットによってはアプリを審査し不正な物や違法性のある物は掲載しないようにしているが、すべてのマーケットで十分な審査が行われているとは限らない。悪意のあるアプリケーションによって重要なデータが漏えいする危険性がある。そのため、信頼のおけるマーケットを選択して使用させることが必要である。また、無料で利用できるアプリの数も多く、パソコンと比較してユーザ自身がアプリケーションを容易に導入してしまうことを考慮しておく必要がある。無料のアプリやコンテンツには、悪意のあるアプリケーションによって情報漏えいしてしまうものに加え、他者の著作権を侵害している場合もあるため注意が必要である。

4.2 標準導入ソフトウェア

本項は、業務利用のためのソフトウェアを会社が指定する場合の規定である。
私有スマートデバイスを会社業務で使用させるに当たり、会社のセキュリティポリシーを守り、円滑かつ安全に運用する為には、会社が管理を行うことを支援するアプリケーションの導入が不可欠である。またコミュニケーションツールなどの統一も必要となるので、共通に使用するアプリを標準導入ソフトウェアとし、ここに導入の義務付けを規定する。

（参考）以下、各デバイスに準じたセキュリティ製品を紹介する。

表 4-2

	iOS	Android	Windows 10 Mobile	Windows 10
アンチウイルス	不正アプリのリスクが低く製品がほぼ存在しない。	トレンドマイクロ社 ウイルスバスターモバイル/Trend Micro Mobile Security	不正アプリのリスクが低く製品が存在しない。	トレンドマイクロ社 ウイルスバスタークラウド
モバイルデバイス管理（MDM）	インヴェンティット社 MobiConnect トレンドマイクロ社 Trend Micro Mobile Security	インヴェンティット社 MobiConnect トレンドマイクロ社 Trend Micro Mobile Security	マイクロソフト社 SystemCenter	マイクロソフト社 SystemCenter
暗号化ソフト	OS標準機能 方式256AES	3.0からのみ搭載 方式：AES 非公開 東京システムハウス社 K2filemanagerEE	OS標準搭載 方式：AES 128, 256	Proに標準搭載 方式：AES 128, 256
電子会議クライアント	Cisco社 WebEx SSL 、AES 暗号化			
遠隔データ消去	OS標準機能 （アカウントごとに端末を個々に操作）、集中管理を数る場合にはMDMを利用			ワンビ社 トラストデリート

・ワンビ社　トラストデリート
盗難・紛失したパソコンのデータ漏えいを防止するためにインターネットまたは広域ワイヤレスネットーワーク（SMS）を介して電源の入っていないパソコンを強制的に起動して、ロックおよび消去できるSaaS型サービス。
・インヴェンティット社　MobiConnect
デバイスの遠隔ロック&ワイプ、ポリシー&各種設定が可能。iOS固有のセキュリティ課題も独自技術で解決。アプリ配布や位置情報取得等のIT資産管理機能も備えたスマートフォン・タブレット向けMDMクラウドサービス。
・東京システムハウス社　K2filemanagerEE
スマートデバイス専用の暗号化ソフト。ファイル書き込み時に自動的に暗号化されるので、手間無くセキュアな環境を構築できる。暗号方式は、総務省と経産省が公表する電子政府推奨暗号に選定されている。
・トレンドマイクロ社　Trend Micro Mobile Security
モバイル端末に対する不正プログラム対策やweb脅威策などのデバイスセキュリティ対策とモバイルデバイス管理など企業におけるスマートフォンやタブレット端末を集中管理し安全に運用するソフトウェア。
・トレンドマイクロ社　ウイルスバスターモバイル
Android端末において単独で動作する、紛失/盗難対策、不正アプリ対策、Web脅威対策、ペアレンタルコントロールなどがひとつ入った総合セキュリティアプリ。
・トレンドマイクロ社　ウイルスバスタークラウド
Windows、Mac において単独で動作する、不正プログラム対策、web脅威対策、URLフィルタリングはじめSNSに対する脅威対策など様々な脅威に対応する総合セキュリティ対策ソフトウェア

4.3 リムーバブルメディア

本項は、リムーバブルメディアが利用可能なスマートデバイスに対する規定である。リムーバブルメディアは、メディア単体の抜き取りが可能であるため、端末本体をパスワード等で守っても、情報漏えいの可能性がある。
パターン1は利用を禁止している。パターン2は限定的に利用を認め、その条件として暗号化を義務づけ、紛失時の対応を規定している。

繰り返しになるが、リムーバブルメディアの最大のリスクは、簡単に抜き取る事が可能で、記録されている情報を一般的なPCで閲覧出来てしまう事である。これはMDMでも完全に防ぐ事が出来ないため、抜き取られてもデータを安全に保つ観点が必要となる。対策としては「暗号化」が有効である。

一方、リムーバブルメディアの使用を禁止する場合の注意点として、私的利用において利便性を損なう可能性がある事を（ユーザビリティの話題だが）考慮しておきたい。
故障時や機種変更時にSDカードを使えない点や、SDカード挿入口があるテレビやプリンタなど他機器との連携サービスの利用において、ユーザによっては不便を感じる可能性があるので、想定をしておくと良いだろう。
また、リムーバブルメディア搭載端末でリムーバブルメディアを装着せずに利用すると、標準的機能でも使えないケースがある（例IS15SHではリムーバブルメディアを抜いた状態でカメラ画像を保存できない）ので注意されたい。

主なスマートデバイスのリムーバブルメディアの有無について紹介する。

リムーバブルメディアの有無はスマートデバイスの機種で決まるので、「リムーバルメディアの取り扱いについての方針」と「対象機種」は合わせて決めると良いだろう。

4.4 導入ソフトウェア他

本項は、ソフトウェアの導入について規定している。
スマートデバイスは、構成プロファイル等によってセキュリティポリシーを維持しているが、これらの改造や変更を禁止している。また、私的利用ソフトウェアについては、端末メーカ、OSベンダ、キャリアが提供している安全と思われるアプリケーションストアからのインストールだけを認め、それ以外のアプリケーションストアから入手したソフトウェアのインストールを禁止している。
MDM利用の場合、MDMを削除されると会社からの制御が不可能となるため、削除禁止を規定している。

・不正アプリの存在
スマートフォンのアプリを導入の際に、スマートフォン内のデータベースへのアクセス許可を求めて許可をすることで、他のアプリのデータや機能などへのアクセスができるようになる。特に、アプリ間でのデータ共有に関しては、スマートフォン特有の仕組みとなっており、その共有する仕組みを利用することで、スマートフォン内のデータを外部に転送したり、データを消去したりする、悪意あるプログラムが多く存在する。

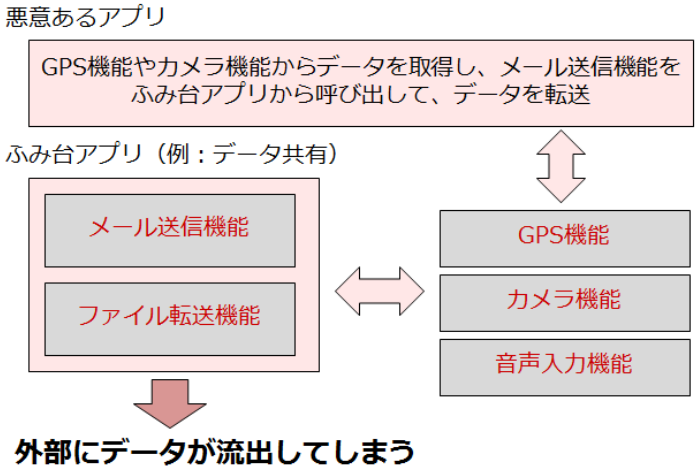


図 4-1

前述の通り、アプリが権限を取得するタイミングは、アプリのインストール時である。アプリのインストール時に、OSにより、アプリ同士や入出力デバイスの利用権限を許可するか否かを確認する画面が表示される。利用者はアプリが要求している権限を確認し、最終的に許可（＝インストール）するかどうかを決定する。
利用者を騙して情報取得する悪意あるアプリは様々な権限を要求するため、業務アプリは連絡先、位置情報、カメラ、アルバムとの共有を原則認めない設定を推奨する。または、業務でカメラ等を利用する場合には、個人で利用するアプリでは許可を認めない排他的な運用を推奨する。

・SNSソフト利用の注意点
現在、SNSの利用者は世界中で増加しており、法人においても、新しいコミュニケーション・ツールとして、商品やサービスの改善に利用しようとする動きが見られる。一方で、法人アカウントによるSNS上の発言などがユーザの非難を集めてしまう事例も少なくない。ここではSNS利用時に想定される脅威と対策について紹介する。

・偽アカウント、架空アカウントの作成

SNSには本人確認が徹底されていないサービスもあり、実在の人物・組織の名前を使った偽のアカウントや、架空のアカウントで投稿されているケースもある。偽のアカウントや架空のアカウントを悪用して、不正リンクの投稿などが行われる事例もあるので、SNSで関わるアカウントの相手が本物であるかどうかは、慎重に確認する必要がある。

SNSサービスによっては、本人確認が行われた上で公式アカウントとして登録されているものもある。特に公的機関や企業、著名人などの情報を購読する場合には、まず公式アカウントが存在するかを、それぞれの機関のホームページなどで確認してみる。直接の知人や公式アカウント以外のアカウントで、本人確認ができない場合には、安易にフォロー（購読）したり、友達になったりしないようにする。

・短縮URLの悪用

短縮URLは、SNSで文字数の制約上URLを短縮して表示する外部のサービスである。本来のURLよりも文字列が短くなり、見た目にも扱いやすくなる。しかし、一見しただけではどのようなサイトにリンクされているかわからないことから、この機能を悪用してフィッシング詐欺やワンクリック詐欺などの悪性ホームページに誘導する手口が確認されているので、短縮URLをクリックする際には注意が必要である。

・スパムアプリケーション

SNSのアプリケーションの中には、インストールの際に、連絡先情報へアクセスする許可を求めてくるものがある。このようなアプリケーションの中には、個人の連絡先情報を収集して、収集したメールアドレスに迷惑メールなどを送りつけることなどを目的としているものもある。連絡先情報へアクセスするアプリケーションで、作成者の身元やその利用目的がよくわからないものは、使用をしないこととする。

・プライバシー情報の書き込み

友人間のコミュニケーションを目的としてSNSを利用している場合であっても、プライバシー設定が不十分であったり、友人から引用されることなどにより、書きこんだ情報が思わぬ形で拡散する危険性がある。インターネット上に情報が公開されていることに変わりはないということを念頭に置いて、書き込む内容には十分注意をしながら利用することが大切である。

・SNSへの写真掲載による意図しない位置情報の流出

最近のGPS機能のついたスマートフォンやデジタルカメラで撮影した写真には、設定によっては、目に見えない形で、撮影日時、撮影した場所の位置情報（GPS情報）、カメラの機種名など、さまざまな情報が含まれている場合がある。SNSに、こうした位置情報付きの写真をよく確認せずに掲載してしまうと、自分の自宅や居場所が他人に特定されてしまう危険性があり、迷惑行為やストーカー被害などの犯罪被害にあう可能性もあるため、十分注意が必要である。

写真にどのような情報が含まれているか調べる方法はいくつかあるが、これらを表示するための専用アプリケーションを利用すると、事前に確認ができる。写真に含まれている情報を編集・削除できるアプリケーションもある。位置情報もプライバシー情報であるということを十分理解して、むやみに位置情報をつけて写真を投稿しないようにする。

・SNSの怪しい投稿のリンク

SNSは誰でも投稿することができることから、怪しいリンク（ワンクリック詐欺、フィッシング詐欺など）に誘導される危険性がある。投稿した人が実在の信頼できる人であったとしても、他の人が投稿した内容をそのまま再投稿する場合もあるので、元々の情報の発信元の信頼性を意識することが大切である。

4.5 データ共有の制限

本項は、データ共有の制限を規定した。
スマートデバイスは、グループウェア、電子メール、ストレージサービス、SNS、名刺交換サービスなど多彩なデータ共有、交換方法が提供されているが、会社の情報資産・営業機密については、原則として共有禁止し、但し書きで共有可能なデータと許可するソフトウェアを指定している。ソフトウェア毎に共有禁止データを指定する場合は、なお書きで個々に指定すればよい。

Windows パソコンとスマートデバイスとでは情報の量からすれば、圧倒的にWindowsパソコンの方が多いといえるが、スマートデバイスが情報漏えいのリスクが大きいのは保持しているデータが直接的に個人情報になるものが多いことと、常にネットワークに接続されているためである。前述のクラウド環境における「データ転送」、ネットワークに接続しているときに、情報を自動的に同期してクラウド環境に保持することが一般化されてきている。
主な個人情報
・メールやメールアドレス
・ブラウザなどに登録されたIDやパスワード
・閲覧記録
・位置情報
「アプリ本来の機能では必要性がないと思われる権限を要求するケースは注意が必要。広告を伴うようなアプリで端末の設定情報を読み取る権限を要求するような場合や、逆に具体的な権限を明示しないような場合もあり、十分な確認が難しい場合もある」

・OS別の危険性
Androidを搭載する端末ではGoogleアカウントとの連携も問題だ。Androidマーケット上のアプリをダウンロードするには、まずGoogleアカウントを作成し、ログインする必要がある。このアカウントはGmailと共通で、これさえあればWeb版のAndroidマーケットからもアプリを購入できる。購入したアプリは端末へとプッシュ配信される。
対策の基本はPCに同じ、ただしAndroidでは困難な場合もある。開発元のAppleやMicrosoftが提供する修正パッチをユーザがこまめに適用する基本的な方法の徹底を推奨する。
以下に、iOS6.0、Android 4.0でのデータ共有設定の制限を行うための手順を説明する。

4.6 機能制限

本項は、スマートデバイスの機能制限について規定している。スマートデバイスは、電話、カメラ、録音・再生等の機能があり、これらの機能を利用して個人情報や営業秘密の持出、送信が可能である。そのため、個人情報が収納されているエリア（書庫、サーバールーム等）での会社が指定した機能について制限を加えるものである。スマートデバイス制限エリアでの機能制限が困難な場合は、本項を削除し、4.7持込制限だけとすればよい。
MDMでは、機能の制限を加えることができることから、パターン1とパターン2に分け規定してある。

スマートデバイスはもともと多機能なうえ、アプリを追加すればさらに使い道を拡張できる。そのため、エンドユーザーの裁量に任せて野放図に利用させればセキュリティリスクは増大しまた、業務以外に使うことでかえって生産性を損なうことにもなりかねない。
そうした不正利用を防止するために、デバイス制御やアプリ利用制限などの機能制限の必要性について、十分に考慮する必要がある。

デバイス制御は、カメラやBluetooth、無線LAN、SDカード等のうち、業務に不要なものを無効化する機能である。
アプリの利用制限は、管理者が許可したアプリのみを利用可能にするホワイトリスト方式や、反対に、使わせたくないアプリを登録するブラックリスト方式で行う。
これらの機能制限は、本体の設定やMDMなどの管理システムで強制的に制限を行うことも可能だが、BYODの場合は私有スマートデバイスであるため、取扱規程やポリシーを活用して制限することになる。

機能制限として考慮すべき事例は以下の通り
・カメラ機能、録音機能の利用可否
事務所など業務エリア内での利用を禁止する、利用禁止エリアを設定するなど。（後述の持ち込み制限との兼ね合いで検討）
・業務時間中、もしくは社内ネットワークからのSNSの利用制限
Facebook、mixi、twitter、LINEなど。ただし、会社の広報活動や、業務上認められる利用方法であれば可とするなどの考慮が必要。
もしくは、プロキシやファイアウォールなどの制限で、アクセスを制御することも一つの案として検討。
・インターネットストレージなど、社外へのデータ保存
（Evernoteや各種クラウドサービスなど）
・テザリング機能の利用可否
スマートデバイス本体をWi-Fiルーターとして利用して他の端末がインターネット接続を利用する場合は、インターネット接続を利用する各端末のインターネット接続ルールに従わなければならない。
・外部記憶装置としての利用可否
PCなどに接続してデータをスマートデバイスに保存する事は、USBメモリなど外部記憶装置の利用ルールに従わなければならない。

4.7 持込制限

スマートデバイスは、写真や録画、録音の機能や、アプリを追加することにより様々な機能を追加する事が可能である。また、それらの機能を利用して情報を記録し、インターネットを通じてそれらの情報を拡散することが容易であり、情報漏えいの危険性は高い。
また、個人が別の目的で様々な機能を使用していたとしても、情報漏えいにつながる行動であると誤解を生じる場合がある。
したがって、重要情報を扱うなどの特定の場所においては、利用制限以前に持込制限を行うことで情報漏えいを防止するとともに、利用者に対する不要な疑いを事前に回避することが重要である。
これは、自社内に限らず、訪問先企業でも同様（利用や持込を禁止されることがある）であり、特に持込制限されていない場所においても、写真や録画、録音などの機能を利用する場合は、利用の可否を確認した上で利用するよう、社員へ啓発することが望ましい。

4.8 パスワード・ID

本項は、パスワード・IDについて規定したものである。
一般的にスマートデバイスでは4桁の数字のパスコードもしくはパスワードなしが規定値となっている端末が多い。BYODにおいてパスワードなしは論外として4桁のパスコードでは、紛失した際にパスコードがブレークされる可能性が高いと云わざるを得ない。端末がブレークした場合、ブラウザにキャッシュされたパスワードでアプリケーションへのアクセスが可能となり、また、電子メールの閲覧、なりすましによる送信などのインシデントが発生する可能性が高くなる。パスコードが4桁固定でない、というだけで攻撃側の推測が困難になることから、この点は大変重要である。一方で、複雑で長大なパスワードはメモ書

きなどでの流出の可能性が高くなる懸念がある。使用するアプリケーションからの情報漏えいリスクを検討し、「4.9 ロック」と併せた強度設計をすることが重要である。
なお、生体認証を備えたスマートフォンも販売されているが、生体認証に失敗した場合はパスコード4桁という設定が一般的である。紛失・盗難の際のブレークを考えると、生体認証の有無にかかわらずパスコードの強度を評価すべきである。
その他、ログオンパスワードとサービスを受ける際のパスワードを別なものとする、個人利用のサービスでは、会社のメールアドレスをIDとして利用しないことを規定した。

さて、スマートフォンが企業システムの端末として深く広く浸透しつつある現状を鑑みると、PCに課すパスワード強度と同等レベルを維持することは、もはや当然の措置であり、スマートフォンだけ使い勝手を優先するのは本末転倒といえよう。
しかし、アプリケーションもあまり制限したくない、使い勝手もある程度は確保したい、ということであれば、数字6桁以上として、ログインに3回連続で失敗した場合はリモートワイプを強制する等の設定を検討するべきである。本項は、桁数、複雑さ、推測困難性を規定しているが、情報漏えいの観点からいえば、後述のロックおよびワイプ設定と組み合わせて総合的な強度を維持するためである。
基本的な考え方は、スマートフォンの役割はもはやPCと同等と捉え、桁数は8桁以上、複雑さは文字、数字の混在、同じ文字・数字が連続しない、連続して増減しない、推測困難性は、近しい第三者が推測容易な生年月日、氏名、名前を使用してはならない、とした。（桁数と強度の関係については、コラムを参照）

4.9 ロック

本項は、パスワード・ID規定に関連するロックについて規定した。
ログインに5回連続で失敗した場合は、端末がロックされるとしている。一般的には10回程度が既定値として設定されているが、パスワードの上位10位で全体の15%を占める等のデータもあることから、短い設定値とした。リスクに応じて設定値を変更するとよい。なお、機種によっては構成プロファイルツール等でないと設定できない場合があり、留意されたい。

スマートデバイスは、本体に機密性の高いデータを保持しており、かつ、ネットワーク経由で様々な情報にアクセスするための入り口となり得るので、情報保護の観点から本体にパスワードロックを施すことの必要性は、自明である。
また、紛失や盗難の際、悪意を持った者がパスワード破りを行う可能性があるため、パスワード入力を特定の回数間違えた場合には、デバイスやアカウント自体をロックアウトすることにより本体を利用不可にするとともに、「4.11 データ消去」で規定しているデータ消去もしくはリモート・ワイプを実行することにより、情報を保護する仕組みとしている。
なお、ログインの連続失敗回数の設定や、スマートデバイスを一定時間放置した場合のパスワード再入力の設定などは、各社のセキュリティポリシーや規定等に準じて、適宜変更されたい。

4.10 電子証明書

本項は、デバイスを特定するための電子証明書、クライアントを特定するための電子証明書の利用規程である。
電子証明書は削除が可能であり、生成の方法によっては複製が可能であることから、なりすましの可能性がある。そのため、これらの行為を禁止している。

以下に、電子証明書の説明と、電子証明書を使用しなければならないシーンや電子証明書を取り扱う上での注意点について解説する。

（1）電子証明書とは？

サーバや利用者が確かに実在し、正当であることを第三者機関（認証局：CA局）が認証し、真正であることを証明するための電子データである。

サーバや利用者の認証や電子署名、暗号に使用される。

（2）電子証明書を利用するメリット

利用者を認証する方法としてID・パスワードを使用して認証する方法がよく利用されるが、電子証明書に比べパスワードは解析しやすく、利用者やサーバに成りすまされる可能性が高い。

電子証明書を利用して認証を行うと、秘密鍵を所有している利用者やサーバのみが認証される。秘密鍵は認証の際に通信経路を流れず、認証の際に署名技術により通信相手が正しいことを確認するために、ID・パスワード方式に比べて解析がより困難になる。

利用するアプリケーションによっては電子署名が施されたアプリケーションも存在し、悪意を持った攻撃者による改ざんがなされていないかをチェックする用途にも使用される。

また、利用者本人が入力したデータであることを証明（原本保証）したい場合などは、電子署名により実現が可能である。

（3）BYODでの利用シーン

無線LANを接続するための端末認証、VPN接続を行う際のクライアント認証、SSL接続を行う際の相互認証等に利用される。

通信経路上に機密情報等、漏えいすることで悪影響を及ぼすデータを流す場合、無線LANやVPN接続、SSL認証を使用する際には電子証明書を利用することを検討する必要がある。電子証明書の使用が必要と認められた場合は、その旨をポリシー上に記載し、それを遵守する。

※その他、クライアントで使用される業務システム等のアプリケーションの仕様に依存して、電子証明書が利用されるケースがある。

（4）電子証明書の取り扱い

電子証明書が漏えいするということは、攻撃者がその利用者に成りすましてシステムに入り込まれる可能性があるので、取り扱いには十分注意する必要がある。

ポリシーには、以下の内容について規定する必要がある。

電子証明書は厳重に管理するとともに、以下の行為を禁止する。

・電子証明書の削除の禁止
・複製保存、譲渡・貸与・公開・送信の禁止
・指定以外のデバイスへのインポートを禁止
・利用目的以外の使用を禁止

ＳＤカード等の電子メディアによる電子証明書の受け渡しを行う場合は、使用後は以下のいずれかの方法により、電子メディアに保存された電子証明書が再利用できない様にする。

・データ消去ツールを使用してRAWレベルでのデータ消去
・電子メディア自体を第三者が利用できない施錠された場所へ保管

（5）電子証明書のインポート方法について

（参考）電子証明書のインポート方法には以下のようなものがある。

表 4-3

インポート種類	内容	メリット	デメリット
OTA(Over The Air)を含むインターネットからのインポート	Webサイトやアプリを経由してインターネットから電子証明書をインポート。	利用者のスキルに依存しない。	インターネットに繋がっていなければインポートできない。導入漏れの可能性がある。
MDM（Mobile Device Management）	MDMを管理する管理者が各クライアントに向けて強制的に電子証明書を配付する。	利用者が電子証明書について意識する必要がない。導入漏れの可能性が低い。	MDMが入っていない端末には入れることができない。インターネットにつながっている必要がある。アプリの種類によっては対応できない可能性もある。
電子メールへの添付	管理者が電子証明書を添付したメールを各端末に送信し、メールを受け取った利用者が個々に証明書をインポートする。	事前の手間がかからず、容易に実施できる。	通信経路で漏洩する可能性がある。添付ファイルが保存できれば利用者が複製を入手可能。利用者の手間が発生する。導入漏れの可能性がある。
SDカード等の電子メディアを使用	SDカード等の電子メディアに電子証明書を入れて各端末に電子証明書を登録する方法。	事前の手間がかからず、容易に実施できる。インターネットを経由しないので、インターネットからの漏えいがない。	利用者が容易に複製を入手可能。利用者にインポートの手間が発生する。導入漏れの可能性がある。

インポート方法によっては、同じ電子証明書を複数デバイスにインポートできるなどの脆弱性が発生したり、導入漏れの可能性があったりするため、指定の手順に従って導入するようにポリシーに明記する。

4.11 改造禁止

本項は、OSの改造によるJail Break、Root化の禁止規定である（ハードウェアの改造については、考慮していない）。

スマートデバイスは、一般のPCと同様にユーザ権限に応じて動作する仕組みが搭載されている。これにより不正なアクセスを防止しているが、改造されたスマートデバイスの場合は、アクセス制御が正常に働かないために、諸問題を引き起こす可能性がある。

注目すべきは、“OSの改造自体が決して難しく無い“と言う点である。Webで検索すればその方法が書かれたページが沢山出てくるほどだ。

改造端末に起因した事例として有名なのが、「IOS_IKEE.D(*1)」である。

これは改造されたiPhoneに対して感染するウイルスで、iPhone内のデータを攻撃者から参照可能な状態にしてしまう。つまり、端末は丸裸となる。

改造によって発生する被害としては、以下が想定できる。

・端末内の電話帳データ、カメラで撮影した画像、SNSなどのアカウント等を読み取り、外部サーバへ送信
・通話内容を盗聴（記録）し、外部サーバへ送信
・大量のメール（迷惑メール）を送信
・電話帳に登録されている相手へ電話発信
・端末が故障し利用不能

中古品のリスクについても触れておく。私有スマートデバイスの場合は、中古で購入した可能性も排除できない。中古品はその時点で改造品である可能性があり、前述の通りリスクを伴うので、積極的に確認を

行うなど、何らかの対策が必要だろう。また、ユーザが改造したい理由が必ずしも悪意を伴う訳では無い点にも留意しておきたい。ここで詳細説明は割愛するが、「自分だけのデザインにしたい」等の軽い感覚で実施されるケースがありそうだ。

(*1) TREND MICROのセキュリティ情報
http://about-threats.trendmicro.com/malware.aspx?language=jp&name=IOS_IKEE.D

4.12 メール・ショートメッセージ

本項は、別途「メール運用規程」がある場合、私有スマートデバイスでも「メール運用規程」を遵守させるものである。
BYODで業務利用をする場合、メールは最もよく使われるサービスのひとつとして挙げられる。しかし、同時に会社の情報資産を外部と簡単にやり取りができるITサービスとして位置づけられ、適切な運用に基づき安全なメール利用を促すことが重要である。

私有でも、会社支給でもその端末を業務利用する以上、スマートデバイスにおいても既存のメールの運用規定に準拠した運用を行うことが重要である。もし、そのような規定がない場合、早急に以下に挙げるようなポイントで規定を作り、ユーザに周知する必要がある。

一般にメール運用規定に検討される項目としては、1. 機密情報や個人情報の送信に関する規定、2. 私用アドレスへの転送禁止、3. メール利用の監視や監査の実施、4. セキュリティ対策をされた環境からのみ使用を許可、などがある。ここでは特にスマートデバイス特有の状況も踏まえ、それぞれの項目を解説する。

（1）機密情報や個人情報の送信の禁止

この規定は、機密事項管理規定などに定義される文書の重要度に関する分類と、その扱いなどにも密接に関係する。一般には、個人情報や機密度の高い文書はメールでの送信を基本的には禁止すべきであるが、もし共有する必要のある場合は、認証、暗号化などセキュリティ対策の施された方法を用意し、それを以って行うことも検討すべき事項である。
スマートデバイスでは、メールの添付ファイルなどがメールクライアントの中にとどまらないケースがある。例えば、Android デバイスなどでは、ほかのアプリケーションなどからもアクセス可能な領域にキャッシュ、保存されるような仕様であり、取り扱いに注意が必要だ。ファイルの暗号化、ファイルを開くためのパスワードによる保護、さらには、メールへの添付ではなく例えば web ベースのセキュアな場所を介したデータの交換などの手段も、有効な対策として検討する必要がある。

（2）私用アドレスへの転送禁止

業務用のメールを私用のアドレスへ転送することを禁止するのは、よくある運用規定のひとつである。ただし、スマートデバイス、特に私有のスマートデバイスを使った場合、少し注意が必要である。一般に、デフォルトのメールクライアントは複数のアカウントを登録することができ、業務用のアカウントと私用のアカウントを混同して利用しないよう、注意を促すことが必要である。また、それだけでは不十分だとみなす場合、業務用に別のメールクライアントを利用することを促すことや、端末のある領域内だけで業務のためのアプリケーションを利用できるような、コンテナ化のソリューションの導入検討も効果的である。

（3）メール利用の監視や監査の実施

電子メールを適切に業務のために利用しているか、会社側が監視や監査を実施したいと考える管理者もいるかもしれないが、過去の判例などからも社員のプライバシーに配慮した運用が必要である。私用メールの頻度や悪質さなど一定の基準を設け、職務専念義務違反などで処分できるように規定を定めることと、

その事実確認のために会社側が監視を行う場合があることなどを明示した規定を作ることが重要である。また、このような運用を行っていることを社員にも広く周知しておくことで、違反行為への抑止力にもなりえる。
なお、私有スマートデバイスの場合でもメールサーバ側で行えることの違いはないが、私有スマートデバイスからの利用状況の確認や認められていない端末からのアクセスがないかの確認など、どのような端末からメールサーバへアクセスしているのかのアクセスログなどの分析も重要である。

（4）セキュリティ対策をされた環境からのみ使用を許可
不正プログラムを送付しないよう、ウイルス対策ソフトウェアなどでセキュリティ対策された端末からのみ利用を認めるといった規定で運用されている例も多い。しかし、スマートデバイスでは、例えば Android であれば限られたリソースしか使えないことにより、Android を標的にした不正プログラムのみ検出することが一般的であるし、iOS であればそもそもそのようなセキュリティアプリケーションは存在しない。したがって、不正プログラムの検出については、メールサーバで不正プログラムが添付されていないかなどの確認を行う必要がある。
またスマートデバイスの場合、不正プログラム対策だけではなく、モバイルデバイス管理もセキュリティ上重要な対策であるが、モバイルデバイス管理上のポリシーに準拠した（例えば、パスワードがポリシーどおり設定されており、禁止アプリケーションがインストールされていない）端末だけをメールサーバにアクセスさせるなどのコントロールができるものもあり、より安全な運用の検討も必要である。

4.13 紛失

本項は、紛失の際の具体的な行動、措置を規定したものである。
紛失した場合、立ち寄った箇所を捜索するなどの行動も尊重するが、（バックアップを前提に）即座にリモート・ワイプを実施することが最も優先されるべきである。
本項の実効性を担保するためには、端末からの情報漏えいが発生した場合の重大性（信用の毀損、謝罪・損害賠償等費用負担、信用回復のための行動コスト）を算定し、社員に企業の存続に関わる重大事であることに理解を求める必要がある。
また、万一、社員がリモート・ワイプを実施しなかった場合に備えて、会社の権利を留保している。
なお、会社としてはリモート・ワイプの操作方法のドキュメント整備等をするとともに、紛失→リモート・ワイプ実施で実害がない場合は、懲罰を加えるべきではない。懲罰的な対応をとることで、社員が萎縮し紛失の事実を隠蔽するリスクには、十分な配慮が必要である。

スマートデバイスの紛失時は、スマートデバイス内のデータの漏えいを防ぐ必要がある。対応としては、遠隔地からデータの削除などが実行できるリモート・ワイプが一般的である。

リモート・ワイプを実施する際のポイントは、「早く実施する」ということである。
電池が切れれば実施不能となるし、悪意の第三者に渡れば何をされるか分からないからだ。また、スマートデバイスがネットワークに繋がらない場所にあると、やはりリモート・ワイプは実施出来ない。「暗号化」など他の対策も合わせて実施する必要があるだろう。

紛失時の対応手順として、“報告の順番”についても注意したい。フィーチャーフォン時代の慣習もあってか、紛失時にまずキャリアに電話をして、利用停止措置をするケースがある。しかしこれでは、前述のリモート・ワイプ等の遠隔操作が出来なくなってしまうので、留意されたい。

紛失時には素早くかつ正しい順番で対応する事が求められる。そのため、日頃の教育も重要である点を認識されたい。

4.14 データ消去

本項は、データ消去、リモート・ワイプを実施する際の条件を規定したものである。
パスワードの連続ミスについては、リモート・ワイプ、退職・機種変更等で利用しなくなった場合はデータ消去となる。なお、これらの操作に伴うリスクは、社員側の負担としている。

スマートデバイスの盗難、紛失に備えて以下の対策を行い、データの漏えいや不正利用がないように適切に運用することが重要である。
・本体および外部記憶媒体のデータ領域を暗号化する。
・アプリケーションの動き（データ保存場所、データの公開範囲等）を調べる。
・業務専用の保存場所を決める。
・利用者には保存場所を選択させないようにする。
・可能な限りデータを区分する（プライベートと業務の保存場所の区分）。

ただし、個人所有のデバイスをBYODとして企業で利用する場合に、個人所有のデータと企業の業務データを区別して利用することは、デバイスの利便性を考慮すると難しい面があることと、情報単体で考えても所有権の有無を判断するのは非常に困難である。
さらに、デバイスに保存されている設定情報には、会社へのネットワーク接続設定や業務リソースへのアクセスを行うためのIDやパスワードが存在するため、デバイスにあるすべての情報を消去できるようにしておくことが重要である。
特に以下の事象のように、企業の業務データや会社へのネットワーク接続設定などの情報が漏えいする危険性があるときには、利用者へデバイスにあるデータそのものを消去することを同意させたうえで、デバイスのデータを消去する必要がある。
・パスワード入力を特定回数間違えた場合、本体を初期化する。
・退職時、利用終了時には全ての業務データの保存場所に対し、データを削除したことを明示させる。
・紛失・盗難時にリモート・ワイプ機能でデータを消去させる。
スマートデバイスは、OS標準機能、通信会社やMDMで提供されるリモート・ワイプ機能を用いることで、デバイスを工場出荷状態にして利用者データを含めてデバイス全体のデータを消去することができる。ただし、Windows８ で動作するノートパソコンやタブレット端末を紛失・盗難した際には、遠隔から指示、もしくは時限的にデータの復元ができなくなるように特定の処理方法でのデータ消去を行う必要がある。

※参考情報
・ハードディスク、SSDの消去方法
　米国　NIST SP-800-88　　上書き1回方式
　米国　国防総省 Unclassified Computer Hard Drive Disposition　　上書き3回方式

4.15 私有データのバックアップ

本項は、リモート・ワイプの実施を前提にバックアップを強制する規定である。バックアップに関わる費用およびリスクは社員の負担としている。

私有スマートデバイスを利用する場合、スマートデバイス内には業務データと私有データが共存することになる。業務データの漏えいを防ぐためには、事故が起こった場合などにデータを削除する必要性に迫られるが、あらゆるケースを想定すると私有データだけを残す（消さない）ことは難しい。労使間のトラブルを避けるためにも、私有データは利用者に定期的にバックアップを取るようにお願いしておきたい。

バックアップの保存先としては、SDカードやクラウドサーバ、パソコンなどが考えられるが、ここでは保存時の漏えいリスクが少ない“パソコン”に保存する方法を紹介する。

iPhoneの場合は、以下の手順によってバックアップが可能である。
(1)iPhoneとパソコンをUSBケーブルで接続する。
(2)iTunesを起動する。
(3)画面の右上に表示されたiPhoneをクリックする。
(4)「今すぐバックアップ」ボタンをクリックする。
(5)バックアップが開始され、写真、連絡先、アプリケーションなどが保存される。
※詳細は下記「iOS：バックアップ方法」を参照されたい。
http://support.apple.com/kb/ht1766?viewlocale=ja_JP&locale=ja_JP

Androidの場合は、以下の要領でバックアップが可能である。
(1)スマートデバイスとパソコン（windows3.1以上）をUSBケーブルで接続する。
(2)パソコンのマイコンピュータを開くと、スマートデバイスの端末名が表示される。
(3)コピーしたいフォルダやファイルを（パソコン内の保存したい先に）ドラッグ＆ドロップする。
スマートデバイス内のファイルの存在場所については、Androidの構成に依存するので、概ねどの機種も似た場所（※1）となる。例えば、docomo Optimus LIFE L-02Eの場合では、以下のパスが（パソコン上で）表示される。
a)ブラウザからのダウンロードしたファイルの場所
　マイコンピュータ¥L-02E¥SDカード¥Download¥
b)Gmail添付ファイルの場所
　マイコンピュータ¥L-02E¥内部ストレージ¥Download¥
c)カメラで撮影した画像ファイルの場所
　マイコンピュータ¥L-02E¥SDカード¥DCIM¥Camera¥
（※1）利用するスマートデバイスやパソコン等の環境によって、詳細は異なるので、
　必要に応じて各種マニュアル類を参照頂きたい。

Android端末ではこの他に、adb(Android Debug Bridge)を利用したバックアップやマーケットアプリ（GooglePlayで入手可能）を使ったバックアップがあり、これらの方法では住所録などアプリのデータを保存する事も可能である。必要に応じて検討すると良い。

4.16 セキュリティ対策

BYODの対象となるスマートデバイスのセキュリティ対策について解説する。

BYODの対象となるスマートデバイスには、4-2「標準導入ソフトウェア」で解説したようなセキュリティ対策ソフトウェアの導入を検討すべきである。その目的と考え方について解説する。
下記の対策とあわせて、違反時の報告ルールなども規定し、社内でのセキュリティモラルを徹底することが望ましい。

（1）BYODの機器管理
モバイルデバイス管理（MDM）およびモバイルアプリケーション管理（MAM）ソフトウェアを設定して、モバイルデバイスとセキュリティ状態を管理する。MDMとMAMのソフトウェアはセキュリティを細かく管理することができるので、BYODを導入する場合は、機器のセキュリティ状態管理として使用することが望ましい。

（2）マルウェア対策

会社で認定したアンチマルウェアソフトのインストールを義務化するなど、アンチマルウェアソフトの導入を検討すべきである。新しいノートPCを手に入れたら必ずアンチウイルスソフトを入れるのと同じで、新しいスマートデバイスには必ず何らかのアンチマルウェアソフトを設定することが望ましい。MDMやMAMのソフトウェアでアンチマルウェアソフトをチェックし、設定されていないデバイスからのアクセスを禁止（遮断）するなどの対策をとることを検討すべきである。

（3）暗号化対策

スマートデバイス（記憶域）もしくはデータの暗号化を利用する。

会社のデータをスマートデバイス（記憶域）に保存したりアクセスしたりする際には、暗号化ソフトウェアを使用させる。また、内蔵デバイス以外に、リムーバブルメディア等が接続できる機種の場合は、リムーバブルメディア自体の暗号化や格納するデータを暗号化できるソフトウェアの利用をおこなうことが望ましい。

（4）スマートデバイス仮想化基盤

会社のデータをスマートデバイスに保存させたくない場合には、ネットワーク利用が前提となるが、端末内にはデータが残らない、スマートデバイス仮想化基盤の利用を検討すべきである。スマートデバイスに導入した専用アプリケーションから、サーバ上にあるスマートデバイス向けの仮想環境を利用するため、BYODでも個人利用と業務利用を明確に分けて使用させることができる。BYODの場合には、OSが多岐に渡るため、マルチOSに対応していることが望ましい。

4.17 データ転送

会社データの転送は、原則禁止としており、どこかに会社データを転送する必要がある場合は、例えば会社のPC（社内ネットワーク接続PC）から送ることをルール化するなどの対策を検討する必要がある。

また、会社データを含むバックアップの設定を、機器の自動バックアップサイトなどへおこなわないようにすることも重要である。BYODで利用する機器のバックアップは、企業のセキュリティポリシーにもよるが、会社のPCやサーバなどにおこなえるよう設定することも、一つの方法である。

4.18 監査

スマートデバイスの利用状況・利用内容の監査について解説する。

（1）スマートデバイスの状態監査

スマートデバイスが、規定どおりに利用（使用）されているか、定期的な現物確認、もしくはMDMなどを利用して自動的に利用状況を確認する。

（2）ログファイルの監査

ログとしては、監査ログ、システムログ、イベントログがあり、ファイル、共有リソース、アカウントに対する不正なアクセスや怪しいアクセスがなかったか、定期的にチェックする。できれば、インベントリ収集ソフトなどを利用して、不正アクセス時に自動的にアラートが送られるような対策をおこなっておくと良い。最小限のログ監査としては、「ログファイルの存在をチェックする」だけでも、ハッカーなどの進入チェックができる。

（ハッカーは証跡を消す習性があるので、ログが不自然に削除されていたら、なんらかの攻撃の可能性があったと思える）

監査の観点としては、以下のような項目がある。

⑴不正なアプリ（利用禁止アプリ・ＯＳ会社か認可していないアプリ）が入っていないか
⑵改造（JailbraekやRoot化）をおこなって、開発者権限、管理者権限で認可されていないソフトウェアを利用していないか
⑶規定したセキュリティ対策がきちんと施されているか
⑷規定したソフトウェアがきちんと入っているか
⑸会社のデータが、スマートデバイス（記憶域）に保存されていないか
⑹ファイルアクセスのログ確認

5 コラム

5.1 効果的な教育について

BYODを導入した企業のリスクとは、個人のスマートデバイスからの情報漏えいである。スマートデバイスは常時携帯されることから、紛失・盗難の可能性は極めて高いといわざるを得ない。従って、BYOD導入にあたっての社員向けの教育は、紛失・盗難があり得るということを前提に、情報漏えいによる企業被害を最小化することを目的にすべきである。
では、情報漏えいの企業被害を最小化するにはどうすればよいか？以下、本コラムの筆者の私案であるが、効果的な教育方法について提案したい。

(1)個人情報と会社情報を分別させ、会社情報の重要度棚卸を実査させ、どの程度の重要情報を持っているかを明確にさせる。
(2)どの程度の流出が起こりうるか、下記資料をもとにグループで検討させ、実際に落とした場合、どのような結果になるか予想させる。
(3)グループ毎に「重要と判断する会社情報」が広く社会に公開されてしまった場合の、金銭的被害について、損害賠償額、事業機会の損失額、信用回復にかかる費用の3点について試算させる。グループ、担当セクションによって異なると思われるが、バラツキがあってよい。
(4)事業部門やセクションの損益をシミュレートさせ、会社全体規模として、雇用を維持できるか検討させる。
(5)企業としての行動指針を、規定およびポリシーをもとに説明し、遵守の重要性を理解させる。

資料としては、以下を参照されたい。
・情報漏えいをおこした際の損害賠償額
日本ネットワークセキュリティ協会「2013年情報セキュリティインシデントに関する調査報告書」[4]
・50台のスマートフォンを意図的に落とし、戻ってくるか、情報漏えいが起こるかの社会的実験
シマンテックスマートフォンハニースティックプロジェクト[5]
・位置検索は限界も　スマホ紛失、都内７カ所で実験
日経プラスワン2013年4月6日付[6]
また、キャリア各社も紛失の際の行動指針をホームページで公開しているので、参考資料として提示するのも良い。

au	http://www.au.kddi.com/support/mobile/trouble/loss
NTT docomo	http://www.nttdocomo.co.jp/support/trouble/lost/index.html
SOFTBANK	http://www.softbank.jp/mobile/support/lost/

また、BYODでの紛失は個人的な損害が発生し、個人情報の漏えいも起こりえる。その意味では、企業も個人も（不注意が原因となったとはいえ）、被害者であることに変わりはない。
ところが、会社側が始末書や戒告などの懲戒を設定している場合、これらに対抗するために秘匿する可能性があり、これが原因となってリモート・ワイプ等の措置が遅れる可能性がある。

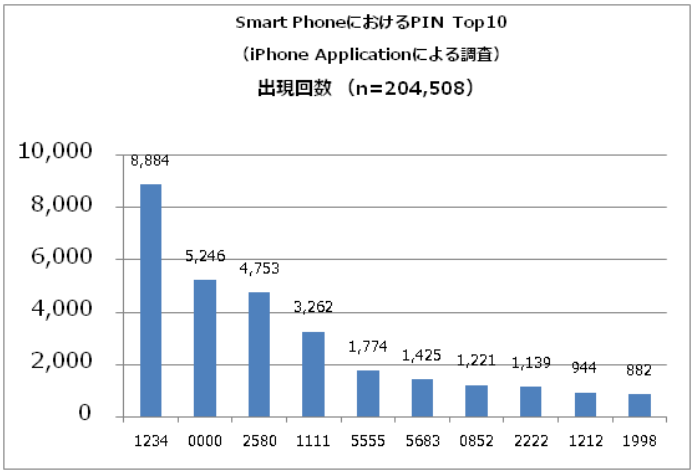
[4] http://www.jnsa.org/result/incident/ index.html
[5] http://www.symantec.com/connect/blogs/symantec-smartphone-honey-stick-project
[6] http://www.nikkei.com/article/DGXDZO53625570V00C13A4W03201/?df=2

従って、紛失・盗難にあたっては、企業・個人情報の漏えいを防ぐという意味で、まずは会社と社員は協働して行動するべきである。さらに（重過失[7] が認められない場合は）懲戒に代わって、紛失に至った状況や情報管理の実態を広く企業内で共有し、再発防止の具体策策定に努めさせるべきである。

5.2 パスワードの強度について

パスワードによる認証システムは、パスワードの長さや複雑さだけでなく、認証失敗の際のロックアウトや、認証システムのアーキテクチャ全体で強度を評価するべきだが、本コラムでは長さと複雑さにおける問題を提起したい。

一般に、パスワードは8文字以上で大文字、小文字、数字、記号を混ぜた複雑なものが推奨されることが多い。ISOキーボードのキートップには94種の文字が刻印されており、94種すべての利用が許されたパスワードの組み合わせは、94の8乗となる。その数は6095兆という膨大な組み合わせであり、一般的には解析は甚だ困難と思える。しかし、米国国立標準技術研究所（NIST）の電子認証に関するガイドラインでは、ユーザが自分で自由に設定した際のパスワードの強度（同書がエントロピーと呼んでいる組み合わせ数）を18bit（2の18乗＝262,144）と評価している。一方で、辞書規則と組み合わせ規則を適用させると5桁であってもその強度は20bit＝1,048,576 としており、ユーザが自由に設定したパスワードの5倍の組み合わせがあると評価している。ここでいう辞書規則とは、5万語程度の英語辞書に搭載されている単語を排除するということであり、組み合わせ規則とは、小文字、大文字、およびアルファベット以外の数字、記号を選択するよう求めるというものである。つまり、8桁であってもユーザが自由に選択した場合は、「11111111」や「password」といった単純なパスワードが設定されてしまい類推が容易であり、5桁の「m&4Q#」のほうが類推は困難ということである。



実際に、600万ユニークユーザの内91%がTop1000のパスワードを使用[8]しており、4.7%が「password」、8.5% が 「 password 」 もしくは「123456」、9.8%が「123456」もしくは「12345678」であるという。 iPhone では母数204,508 の15%がTop10のパスワードを使用しているという調査がある。また、年（西暦）にも相関があり、誕生日や学校を卒業した年を利用する者が多いのではないか、とされている。実際にシステム構築に当たってServerをインストールする際などは「password」や複雑なものにしたとしても「P@ssw0rd」などを使うことが経験的に多い。これらの安直なパスワードを集めて辞書化し、攻撃されることを想定する必要がある。

ところで、スマートフォンではソフトウェアキーボードであることから、大文字、小文字の入力はよいとしても、記号や数字をいれるとなると画面の切り替えが必要となり操作が煩雑になる。電話をかける度に「P@ssw0rd」を入力するとなると甚だ使い勝手が悪く、こうした組み合わせを3ヶ月毎に考えて変更せよ、というのは運用上些かの無理が生じるのではないだろうか。では、スマートデバイスの理想的なパスワードとは何か？

まず、スマートフォンはLogonされてしまえば、電子メール、DropBoxなどのリソースには簡単に入れる（パスワードの再設定も自由だ）し、VPN接続も場合によっては可能となってしまう。Webアプリのパスワードはブラウザがキャッシュしており、このような場合はすべて突き抜けてしまう事となるリスクがある。パスワードの強度と情報漏えいはトレードオフの関係にあることを念頭におかなければならない。

[7]自己管理不能な状態（泥酔酩酊した）など。
[8] Mark Burnett（2011）

となれば、少なくとも4桁のパスコードについては、その運用を止めるべきである。これは「0000」や「2580」などの単純なパスコードを招くことから危険である、という考え方による。もしくはこれらを許す代わりに、運用ではメールだけを許可し、個人情報等を含むデータはメール本文には書かずに添付ファイルとし、添付ファイルには複雑なパスワードを必須とするなどを検討する。
次に、英小文字、英大文字の組み合わせで8桁以上とする。この場合アプリケーションの制限はなしとするが、紛失しやすいという特徴を踏まえ、3回以上連続してミス入力されればロックする、5回以上連続してミス入力されればリモート・ワイプを実行するようにし、これらの設定は強制監査するのである。もしくは、数字6桁として、3回連続してミス入力されればリモートワイプを実行、設定は強制監査するという考え方もある。
これらの条件を厳しいと思われるなら、金曜日の夜にスマートフォンを紛失し、月曜日の朝に紛失に気がついて、社内アプリケーションのパスワードを変更、リモート・ワイプが実行できるまでの60～72時間程度は攻撃から耐えうる認証システムの導入を検討するべきだろう。

5.3 MDM製品とは

MDM(Mobile Device Management：モバイルデバイス管理)は、通常Google社のAndroid OS、Apple社のiOS、Microsoft社のモバイルデバイス向けWindowsOS、BlackBerry社のBlackberryOS等を搭載したスマートフォンやタブレットPCといった従来の携帯電話やノートPCには分類されない新しいモバイルデバイスを管理運用するためのシステム全般を指す言葉である。
MDMが一般に求められる機能は、モバイルデバイスの「遠隔での操作制御」、「設定管理」「利用情報収集」の3点である。まず、「遠隔での操作制御」はモバイルデバイス紛失等に際し、”ワイプ（デバイス内のデータの一部または全部を削除すること）”および”ロック（デバイスを一時的に利用できなくすること）”を主な機能として提供されている。次に「遠隔での設定」とは、パスワード強制化やデバイス内蔵のカメラや特定のアプリケーション等を利用できなくするといった所謂「セキュリティポリシー」の設定はもちろん、デバイス利用時に必要となるメール、WifiネットワークやVPN設定といった煩雑な設定作業を、デバイス利用者に負担をかけずに一元的にシステム管理者が行うことである。最後に「利用情報収集」とは、デバイスが企業の運用ルールに則り正しく利用されているかという観点からインストールされているアプリケーションや、そのアプリケーションやモバイルデバイスの利用頻度といった情報を遠隔で収集管理することである。
さて、情報セキュリティ目的で導入されるMDMは、実際のスマートフォンやタブレットPCが紛失、盗難に際しどのように利用されているのであろうか、つまりモバイルデバイスの利用者はデバイス紛失に際し、どのような行動に出るのだろうか。米国ジュニパーネットワークス社が2011年に「モバイル脅威に関するレポート2010/2011」の中でモバイルデバイス紛失の際の利用者の行動について紹介している。
彼らの調査では、2010年中でMDMにモバイルデバイスを登録し、利用している法人、個人を問わず利用者のうち20 人に1 人がモバイルデバイスを紛失している。また、モバイルデバイスを紛失した利用者のうち3分の1の利用者がMDMの位置情報取得機能を利用して紛失した自分のデバイスの場所を表示した。また、デバイスを紛失し、位置情報取得を操作した利用者のうち77%は、自分のデバイスを利用できないようにロック操作を遠隔で行っている。紛失したデバイスへロック操作を遠隔で行った利用者のうちで、30%はロック解除操作をおこなっていない。それは、紛失デバイスが見つからなかったことに他ならないにも関わらず、紛失デバイスへ遠隔ロック操作を行った利用者のうち21%しか遠隔でのワイプ操作を行っていないとしている。つまり、MDMに登録しているにも関わらず、紛失したモバイルデバイスの利用者のうち66%強は紛失後でもMDMを利用したセキュリティアクションを起こしておらず、また、セキュリティアクションを起こした利用者でさえ、その2%強の利用者はデバイスが見つかっていないにも関わらず、デバイス内のデータを消去していないという結果となる。
日本におけるMDM利用においても、例えば企業ルールとしてモバイルデバイス紛失時には即座に遠隔ワイプ操作を行うという規程がある場合に、デバイスを紛失したにも関わらずその事実を企業に届け出ないまま利用者が紛失したデバイスを探し、時間の経過とともに情報漏えいリスクを増大させるような危うい実例がしばしば見かけられる。

MDMの他に、情報セキュリティの目的で導入を検討される仕組みとしては、MAM（Mobile Application Management：モバイルアプリケーション管理）がある。MAMは、モバイルデバイスで利用する業務アプリケーションなどが、安全に使えるようにアプリケーションや通信を制限する仕組みであるが、その種類は大きく２つに分類できる。１つはコンテナ型と呼ばれるもので、モバイルデバイスの業務アプリケーション内部に業務データを保持する方式だ。業務データはアプリケーション内で保持しているため、必要に応じて、特定データのみを選択して消去することができる。もう１つは、画面転送型といって、サーバ上で仮想環境を動作させ、モバイルデバイスには専用アプリケーション経由で画面のみを表示させる方式である。この方式の場合、モバイルデバイス内部には業務データが格納されていないため、万が一デバイスを盗難・紛失してしまった場合でも、データを消去する必要はない。ただし、快適に業務を行うためには、ある程度整備されたネットワーク環境が必要となる。MAMを利用する場合には、実施させる業務の内容や、それぞれの方式のメリット/デメリットを考慮した上で、導入を検討してほしい。
スマートフォンやタブレットPCは、デスクトップPCやノートブックPCと異なり普段持ち歩いているデバイスであり、利用者にはより身近なツールであるがゆえ、企業から配布されたデバイスであっても利用者は自分の所有物と混同しがちである。しかしながら、企業業務で利用している以上、そこで取り扱われる情報は企業資産であり、その情報流失によって企業が大きなダメージを負うということを利用者に今一度認識させる必要がある。企業におけるモバイルデバイス利用にあたり、セキュリティ対策としてのMDMを利用することはもちろん、デバイス紛失時の迅速なセキュリティ対処の必要性をデバイス利用者自身に自覚させなければ企業の情報資産がセキュリティリスクに晒され続ける、といった初歩的なセキュリティリテラシー向上のための教育プログラムの実施が合わせて求められる。

5.4 内部犯行抑止のための考察

内部の人間が起こす情報漏えい

企業からの情報漏えいを論じる時、すぐに浮かぶのは外部からの攻撃による漏えい事件である。特に昨今は「標的型攻撃」「ログイン試行」等により多くの企業・団体から個人情報や営業機密が漏えいしているとの報道を目にすることが多い。しかし、一方、外部からの攻撃ではない、つまり組織内部の人間による漏えいもまた発生している。経済産業省が平成２５年３月に発表した「営業秘密の管理実態に関するアンケート調査」によれば、過去5年間に人を通じた情報漏えいがあったと答えた企業が15.8%、わからないと答えた企業が16.2%存在した。主な内訳としては「中途退職者（正規社員）による漏えい（50.3%）」、「現職従業員のミスによる漏えい（26.9%）」、「金銭目的等の動機を持った現職従業員による漏えい（10.9%）」と報告されている。営業秘密の漏えいは多くのケースで企業競争力の低下を招く。経営者としては見過ごせないリスクのはずであるが、対策はなかなか進まない。
経済産業省は、平成２６年８月に経済団体に対して個人情報保護法等の遵守に関する周知徹底を要請した。これは平成２６年７月に教育関係事業者において、内部関係者の不正行為により極めて多数の個人情報が漏えいするという事案が発生したことに起因するものである。その周知徹底を要請する文書では、参考情報として独立行政法人情報処理推進機構（IPA）が策定した「組織における内部不正防止ガイドライン」が紹介されている。このガイドラインには、内部関係者による不正行為が行われないように組織として対応するにはどうすればいいか記載されているので参考にしてほしい。
環境犯罪学の中で、コーエンとフェルソンは「ルーチンアクティビティセオリー（日常行動理論、1979年発表）」において、「犯意を持つ行為者」と、「ふさわしいターゲット」「（抑制力のある）監視者の不在」この３条件が揃ったときに犯罪が発生すると説いている。企業内部においても内部犯行を防ぎ社員を守るため、上記３条件を揃えないような施策が必要となって来ているのではないだろうか。
日本は欧米に比べて犯罪の少ない国といわれており、その理由はいくつかあるが、「単一民族に近く中流意識による満足度が比較的高い」「家族や職場地域への帰属意識が強く”ウチ””ムラ”に恥をかかせてはならないという規範意識が強い」という理由は、核家族化、昨今のグローバライゼーション、終身雇用制度の崩壊により徐々に失われつつあるのではないか。例えば、転職に当たり自分の価値を高める方策として、前属の企業内情報を利用したいという意思が起こる可能性がある。利用したい情報が企業外持ち出し禁止

であれば（往々にしてこういう場合はそのような情報が多いが）、その者は犯意を持つ行為者に変貌する。企業が競争力を維持し、広くグローバルで活躍するためにも、再度セキュリティ及び企業と従業員とのあり方を見直す時期にあるのかもしれない。

6 スマートデバイスに関わるセキュリティ製品・サービス紹介

CSAJ正会員及び賛助会員へ平成25年6月11日～6月19日の期間、スマートデバイスに関わるセキュリティ製品・サービスの募集を行い、掲載申し込みがあった該当製品・サービスは以下の通り。詳細は、各問い合わせ先へ直接連絡してください。

表 6-1

製品分類	暗号化ソフト
会社名	東京システムハウス株式会社
製品名	K2filemanagerEE
製品特長	スマートデバイス専用の暗号化ソフト。ファイル書き込み時に自動的に暗号化されるので、手間無くセキュアな環境を構築できます。暗号方式は、総務省と経産省が公表する電子政府推奨暗号に選定されています。
製品紹介URL	http://www.tsh-world.co.jp/ks/product/android/k2fmee.html
お問合先	担当：渡部　和也（わたなべ　かずや） 電話：03-3493-5761　　E-mail：k-watanabe@tsh-world.co.jp

表 6-2

製品分類	MDM、アンチウイルス、遠隔データ消去、Webフィルタリング（すべて含む）
会社名	トレンドマイクロ株式会社
製品名	Trend Micro Mobile Security
製品特長	スマートフォンやタブレット端末の不正プログラムやweb脅威の対策とアプリケーションや端末の構成などのMDMをワンストップで提供するモバイルセキュリティソリューション。
製品紹介URL	http://www.trendmicro.co.jp/tmms/
お問合先	http://jp.trendmicro.com/jp/about/contact/ 法人お問合せ窓口　　電話番号: 03-5334-3601 （月曜日～金曜日の9：00～12：00、13：00～18：00、ただし祝祭日および、その振替日を除きます）

表 6-3

製品分類	パスワード管理
会社名	トレンドマイクロ株式会社
製品名	トレンドマイクロ　パスワードマネージャー
製品特長	webサイトのログインIDとパスワードを自動で暗号化しクラウド上で保管するサービス。PCからもモバイル端末からも利用でき、webサイトに簡単に自動的にログインできます。
製品紹介URL	http://safe.trendmicro.jp/products/pwmgr.aspx
お問合先	以下URLをご参照ください。 http://jp.trendmicro.com/jp/about/contact/

表 6-4

製品分類	モバイル用バックアップサービス
会社名	トレンドマイクロ株式会社
製品名	トレンドマイクロ セーフバックアップ
製品特長	Android端末のデータを連絡先、カレンダー、写真、音楽などの項目ごとにクラウド上に保存できるバックアップサービス。機種変更などにより新たな端末へデータを復旧することも可能です。
製品紹介URL	http://safe.trendmicro.jp/products/sa.aspx
お問合先	以下URLをご参照ください。 http://jp.trendmicro.com/jp/about/contact/

表 6-5

製品分類	アンチウイルス
会社名	日本事務器株式会社
製品名	ウイルスバスタービジネスセキュリティサービス あんしんプラス
製品特長	PCとスマートデバイスをまとめて一元管理する法人向けSaaS型セキュリティ対策サービス。クラウド上のいつも最新のパターンファイルで、端末の利用場所を問わず、新たな脅威からいち早く防御可能です。
製品紹介URL	http://www.anshinplus.jp/service/virus.html
お問合先	担当：西浪 一雅（事業推進本部 プラットフォームソリューション事業推進部） 電話：050-3000-1523 E-mail：seplus@njc.co.jp お問い合わせフォーム https://form.njc.co.jp/webapp/form/14798_exv_145/index.do

表 6-6

製品分類	企業向けチャット・メッセージングソリューション
会社名	株式会社レジェンド・アプリケーションズ
製品名	LaKeelMessenger（ラキール・メッセンジャー）
製品特長	企業利用に特化したチャットツールです。社外での利用ポリシー、ログ監査等の機能により安全なコミュニケーションを実現します。
製品紹介URL	http://messenger.lakeel.com
お問合先	プロダクト営業グループ 担当：片石 電話：03-6203-0571 E－Mail：tecs-support@legendapl.com

表 6-7

製品分類	デバイス利用時の本人認証
会社名	ウィッツェル株式会社
製品名	Cyber-SIGN for Android（端末ロック）
製品特長	Android端末の電源オン時に、手書き署名照合（生体個人認証）による本人確認を行う事で、端末の不正利用や、端末の盗難・紛失時の情報漏洩防止を行う事が出来るアプリケーションソフトウェアです。
製品紹介URL	http://www.witswell.co.jp/cybersign/
お問合先	担当：舟山 浩司（WWパートナーズ部門 BDMグループ） 電話：03-5212-7123 E－Mail：koji.funayama@witswell.co.jp

表 6-8

製品分類	MDM
会社名	販売代理店 ： 株式会社インテリジェント ウェイブ 開発メーカ ： インヴェンティット株式会社
製品名	MobiConnect
製品特長	デバイスの遠隔ロック&ワイプ、ポリシー&各種設定が可能。iOS固有のセキュリティ課題も独自技術で解決。アプリ配布や位置情報取得等のIT資産管理機能も充実したスマートフォン・タブレットPC向けMDMクラウドサービス。
製品紹介URL	http://www.mobi-connect.net/
お問合先	株式会社インテリジェント ウェイブ 第一営業本部 第二営業部 E-mail： cwatsales@iwi.co.jp

表 6-9

製品分類	MDM
会社名	販売代理店 ： 株式会社インテリジェント ウェイブ 開発メーカ ： インヴェンティット株式会社
製品名	IT-MOM
製品特長	遠隔ロック&ワイプ、ポリシー&各種設定等のセキュリティ機能およびIT資産管理機能を提供。用途に合わせて既存システムとの連携が可能。MDMクラウドサービス「MobiConnnect」のオンプレミス版ソフトウェア。
製品紹介URL	http://www.mobi-connect.net/
お問合先	株式会社インテリジェント ウェイブ 第一営業本部 第二営業部 E-mail： cwatsales@iwi.co.jp

表 6-10

製品分類	盗難・紛失パソコンのデータ遠隔消去ソリューション
会社名	ワンビ株式会社
製品名	TRUST DELETE Biz（トラストデリート ビズ）
製品特長	盗難・紛失したパソコンのデータを遠隔から消去して、重要なデータの漏えいを防止します。起動していないパソコンにおいても、携帯通信網を利用し電源を投入しデータを消去します。
製品紹介URL	http://www.onebe.co.jp/
お問合先	営業部 担当：藤原 電話：03-6909-0305 E－Mail：mailto:info_ml@onebe.co.jp

表 6-11

製品分類	アンチウイルス・MDM（リモートロック、ワイプ）・デバイス証明書
会社名	株式会社 日立ソリューションズ
製品名	スマートフォン セキュリティ統制サービス
製品特長	スマホやタブレットを利用する際に必要な、モバイルデバイスマネジメント(MDM)、マルウェア対策、デバイス認証を提供します。 24時間365日リモートロック・ワイプが可能。
製品紹介URL	http://www.hitachi-solutions.co.jp/smartphone_so/
お問合先	https://www.hitachi-solutions.co.jp/inquiry/

表 6-12

製品分類	リモートロック・リモートワイプ・盗難紛失対策
会社名	株式会社 日立ソリューションズ
製品名	モバイルPC 盗難・紛失対策サービス
製品特長	PCに対してリモートロック・ワイプが24時間365日可能です。盗難にあったPCの回収支援も行います。本サービスを実現するソフトウェアが、モバイルPCから故意に削除されても自動的に復元されるため、常に管理することが可能です。
製品紹介URL	http://www.hitachi-solutions.co.jp/antitheft/
お問合先	https://www.hitachi-solutions.co.jp/inquiry/

表 6-13

製品分類	リモートデスクトップ
会社名	株式会社 日立ソリューションズ
製品名	Array DesktopDirect
製品特長	様々なスマートデバイスからオフィスのPCに接続可能なリモートデスクトップ環境を実現します。接続元スマートデバイスにデータが残らない、デバイス個体識別が可能、などの機能によりBYODにも適用可能です。
製品紹介URL	http://www.hitachi-solutions.co.jp/array/sp/dtd/about.html
お問合先	https://www.hitachi-solutions.co.jp/inquiry/

表 6-14

製品分類	無線LANシステム
会社名	株式会社 日立ソリューションズ
製品名	Arubaシリーズ
製品特長	小～大規模企業、学校、公共など幅広いお客様に導入実績のある無線LANシステムです。複数の認証方式やユーザ毎のアクセス権限設定などセキュリティ機能が充実。最新のIEEE802.11acにも対応し、セキュアで安定した無線LAN環境を提供します。
製品紹介URL	http://www.hitachi-solutions.co.jp/aruba/sp/
お問合先	https://www.hitachi-solutions.co.jp/inquiry/

表 6-15

製品分類	次世代ファイアウォール
会社名	株式会社 日立ソリューションズ
製品名	パロアルトネットワークス PAシリーズ
製品特長	社内LANに接続したスマートデバイスの通信を可視化し、ユーザが利用できるアプリケーションの通信を制御することができます。情報漏えいの危険があるアプリケーションの利用を制限できるので、BYODにも対応できます。
製品紹介URL	http://www.hitachi-solutions.co.jp/paloalto/sp/
お問合先	https://www.hitachi-solutions.co.jp/inquiry/

表 6-16

製品分類	スマートデバイスの暗号
会社名	株式会社 日立ソリューションズ
製品名	秘文AE SmartDevice Encryption
製品特長	スマートデバイスの内蔵データやmicroSDカードのデータを暗号化。万一の盗難・紛失の際に第三者にデータを見られることを防止します。 秘文シリーズはスマートデバイスをビジネスで安全・安心に利用できる環境をご提供します。
製品紹介URL	http://www.hitachi-solutions.co.jp/hibun/sp/product/ae_sde.html
お問合先	https://www.hitachi-solutions.co.jp/inquiry/

表 6-17

製品分類	スマートデバイスの認証
会社名	株式会社 日立ソリューションズ
製品名	静紋JS1
製品特長	スマートデバイスで指静脈を使用した認証が行えます。静紋JS1は重さわずか35グラムの指静脈認証装置。スマートデバイスで、偽造・改ざんが困難な指静脈を使用した、高セキュリティなユーザ認証を実現します。
製品紹介URL	http://www.hitachi-solutions.co.jp/johmon/sp/product/feature_03.html
お問合先	https://www.hitachi-solutions.co.jp/inquiry/

表 6-18

製品分類	スマートデバイスの認証
会社名	株式会社 日立ソリューションズ
製品名	AUthentiGate Android ICカード認証パッケージ
製品特長	Andoroid端末でICカードによる認証を実現。 認証に特別な装置の追加は不要です。社員証、交通系カードなど既存のICカード（FeliCa、MIFARE）をNFC対応のAndroid端末にかざすだけで認証が行えます。
製品紹介URL	http://www.hitachi-solutions.co.jp/AUthentiGate/sp/product/androidcardauth.html
お問合先	https://www.hitachi-solutions.co.jp/inquiry/

表 6-19

製品分類	スマートデバイス仮想化基盤
会社名	株式会社 日立ソリューションズ
製品名	Avast Virtual Mobile Platform
製品特長	サーバ上に仮想スマートデバイスを構築し、それを手元のモバイル端末からリモートアクセスすることで、スマートデバイスをセキュアに業務で利用可能です。業務エリアとプライベートエリアが分離されるため、BYODの課題を解決します。
製品紹介URL	http://www.hitachi-solutions.co.jp/remotium/lp/
お問合先	https://www.hitachi-solutions.co.jp/inquiry/

表 6-20

製品分類	端末認証用電子証明書サービス
会社名	サイバートラスト株式会社
製品名	サイバートラスト デバイスID
製品特長	企業および組織が許可した端末のみをネットワークに接続させるための、端末認証を実現するデバイス認証用証明書発行管理サービス。
製品紹介URL	https://www.cybertrust.ne.jp/MDM/deviceid/index.html
お問合先	サイバートラスト株式会社 電話：03-6234-3800

7 研究会メンバー一覧

主査	小屋　晋吾*	トレンドマイクロ株式会社　執行役員 統合政策担当
主査代理	転法輪　浩昭*	トレンドマイクロ株式会社　マーケティング本部 エンタープライズマーケティング部 担当課長代理 プロダクトマネージャー
メンバー	板東　直樹*	アップデート テクノロジー株式会社　代表取締役社長
	井潟　博彦	株式会社アルゴグラフィックス　取締役 執行役員 管理統括部 統括部長
	山形　浩一*	インヴェンティット株式会社　執行役員営業本部本部長
	野寺　鐘太郎	インヴェンティット株式会社　事業企画部長
	DIKDIK SETIA PERMANA*	株式会社インフィニテック　米沢営業所 開発1課 課長
	近藤　伸明*	株式会社神戸デジタル・ラボ　セキュリティソリューション事業部 シニアコンサルタント 情報セキュリティスペシャリスト
	寺川　英信*	株式会社大和コンピューター　企画管理本部 経営企画部 上席マネージャー
	西原　由貴雄*	東京システムハウス株式会社　ビジネスイノベーション事業部 モバイルビジネス部　部長
	国枝　直之*	日本事務器株式会社　内部統制部 部長
	浅野　利也*	日本事務器株式会社　経営企画部　IT企画グループ シニアエキスパート
	谷川　智久	日本システム開発株式会社　取締役 情報システム部 部長
	脇坂　隆則*	株式会社日立ソリューションズ　九州地区本部 本部長
	久保田　裕介	株式会社ミック　総務部 係長
	加藤　貴*	ワンビ株式会社　代表取締役社長
	勝原　雄介	ワンビ株式会社　営業部
事務局	戸島　拓生	一般社団法人コンピュータソフトウェア協会　業務課 係長
	鈴木　啓紹	一般社団法人コンピュータソフトウェア協会　業務課 主任

※敬称略、メンバーは社名五十音順
※部署・役職は平成25年6月時点
※「*」は、執筆メンバー
＜平成25年6月時点のメンバー一覧＞

8 第2版校正メンバー一覧

主査	小屋　晋吾	トレンドマイクロ株式会社
主査代理	転法輪　浩昭	トレンドマイクロ株式会社
メンバー	板東　直樹	アップデート テクノロジー株式会社
	寺川　英信	株式会社大和コンピューター
	国枝　直之	日本事務器株式会社
	浅野　利也	日本事務器株式会社
	中川　克幸	株式会社日立ソリューションズ
事務局	戸島　拓生	一般社団法人コンピュータソフトウェア協会

※敬称略、メンバーは社名五十音順
※所属は平成27年9月時点

私有スマートデバイス取扱規程サンプル第2版及びスマートデバイス・セキュリティポリシーサンプル第2版解説書

2013年7月11日　第1版
2016年1月26日　第2版
発行・著作　一般社団法人コンピュータソフトウェア協会

Computer Software Association of Japan
一般社団法人コンピュータソフトウェア協会
モバイル利活用ワーキンググループ
（旧セキュリティ（BYOD）研究会）
〒107-0052　東京都港区赤坂1-3-6
赤坂グレースビル4F
TEL：03-3560-8440　FAX：03-3560-8441
URL：http://www.csaj.jp/