JEITA

IS－12－技標－2

セキュリティ市場・技術調査報告書

2012年3月

一般社団法人 電子情報技術産業協会

はじめに

本報告書は、セキュリティ市場・技術調査専門委員会が、「企業における新たな IT 活用の方向性と情報セキュリティ」に関する調査を行い報告するものである。

注目すべき IT 領域として、市場性とビジネスへのインパクトからスマートフォンとクラウド・コンピューティングについて、市場動向や活用事例から新たなセキュリティ課題の検討を行った。一昨年本委員会で調査したクラウドサービスは本格的に市場を形成しつつあり 1,000 億円を超える市場規模でさらに大きく成長が見込まれている。

スマートフォンは昨年から急速に広がり、国内でも携帯電話の 10%を超え、さらにタブレット端末などとあわせて新たなモバイル端末として企業内でも積極的に採用が進められている。しかし、このような新しい IT 環境は、新たなセキュリティの問題、プライバシーの問題を生み出している。

また、企業を取り巻く社会状況として、2011 年は日本全体に大きな影響を与えた東日本大震災がおこり、多くの企業が大きな被害の中で事業継続の試練に立たされ、その後も復興に向けた努力を続けている。非常時の情報セキュリティの観点から企業活動への脅威と対策を検討した。

もうひとつ、2011 年に注目されたこととして、企業や組織を対象としたサイバー攻撃があった。フィクションの世界のことのように感じられていたサイバー攻撃が現実に社会インフラへ影響を及ぼすような脅威になる現実が企業にも突き付けられているようである。まだまだ検討が始まったばかりではあるがこの脅威にどのように対処していくべきかを共有していきたい。

これらの ICT の動向や社会状況からも企業活動を行う上で、重要となる情報通信技術を確実に安全に利用するために、各々の企業がどのような技術を活用し、そのためにどういったセキュリティ対策を取っていくべきか、方針検討の一助となることを目指した。

本調査報告書の作成にあたり、視察およびヒアリングにご協力いただいた企業や有識者の方々、そして当専門委員会の関係の皆様に深く感謝の意を表すとともに、本報告者が関係の方々に活用され、今後のビジネスの更なる発展に寄与できれば幸いである。

2012 年 3 月

セキュリティ市場・技術調査専門委員会
委員長　平木　博史

セキュリティ市場・技術調査専門委員会名簿

（敬称略・順不同）

委員長	平木博史	㈱リコー
副委員長	武本　敏	㈱日立製作所
委員	福島孝文	東芝テック㈱
〃	池田政弘	富士ゼロックス㈱
〃	池田恵一	富士通㈱
〃	白石節男	富士通㈱
〃	米田　健	三菱電機㈱
〃	畠山有子	三菱電機㈱
〃	遠藤　淳	三菱電機インフォメーションテクノロジー㈱
〃	佐藤　淳	㈱リコー
オブザーバ	川口修司	㈱三菱総合研究所
〃	江連三香	㈱三菱総合研究所
事務局	吉田　晃	（社）電子情報技術産業協会

目　次

第1章　企業における IT 活用の動向とセキュリティ

1.1 クラウド・コンピューティング

1.1.1 市場動向、活用事例

クラウドサービスの 2010 年の市場規模は 454 億円で、2015 年には 2010 年比 4.3 倍の 1,947 億円になると予測されている。また、市場成長率は、2010 年が前年比 45.3%増となり、2011 年は 50%近い成長率が見込まれる。その後は低下する見通しとなっている[1]（図 1.1-1）。

適用先としては、個別カスタマイズや他のシステムとの連携をそれほど必要としない、グループウェアサービスやソーシャルアプリケーションサービス、SaaS 型セキュリティサービス等の活用、また、それらの基盤としての PaaS や IaaS の活用等が伸びてきている。ただし、これまで多くの企業において想定してなかった、東日本大震災により表面化した津波や原発事故に関するリスクへの対応としてのクラウド・コンピューティングの活用が見込まれることから、クラウド化のポイントや規模等は大きく変化するのではないかと考えられる。例えば、原子力発電所から遠い位置に存在するデータセンタを指定した上でのクラウドを活用したバックアップなどの冗長化構成や Desktop as a Service などの事業継続計画（BCP: Business Continuity Plan）に関する需要に大きな伸びがある。

クラウド・コンピューティングは有効な手段であり、その市場が伸びている一方で、導入の際の個別カスタマイズ費等により、導入のメリットとされていた「コスト削減効果」が大きく期待できない場合がある。そのため、クラウド・コンピューティング導入を行わないことを決定した企業が増加してきている。これは、既存システムのクラウド化の際に、既存業務の改革に踏み切れない日本企業特有の問題であると考えられる。クラウド化は事業継続の観点においても非常に有効な手段の一つである一方で、クラウド化に際して固有のカスタマイズを実施した上で導入をした企業では、非常時の際のシステムの再構築に多くのリソース（人員、時間、費用など）を必要としてしまい、迅速な事業復旧の妨げとなる可能性がある。

[1] 東日本大震災による影響は考慮されていない。

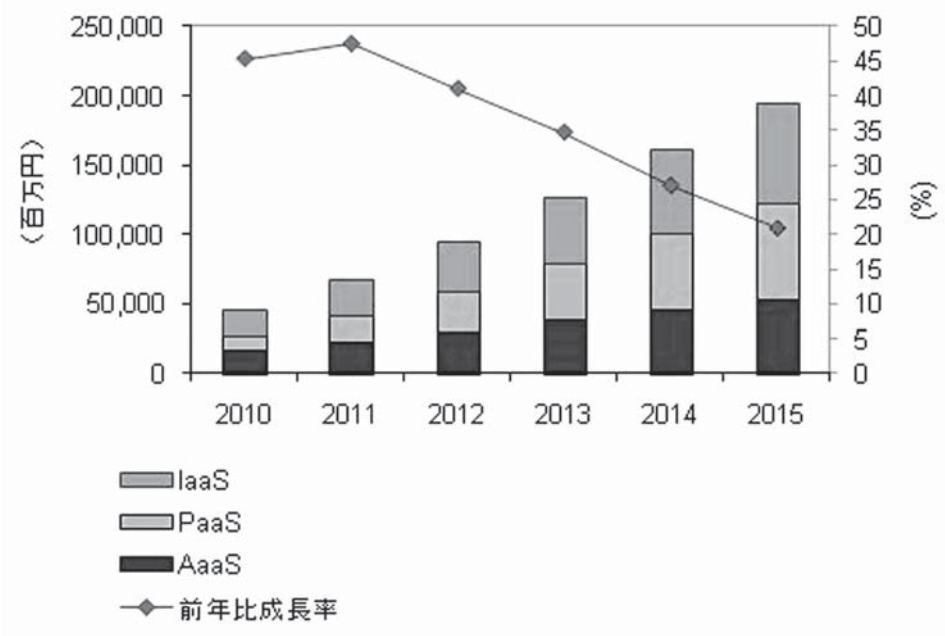


図 1.1-1　国内クラウドサービス市場 セグメント別売上額予測、2010 年～2015 年[2]

1.1.2 セキュリティ課題

クラウド・コンピューティングの黎明期から、そのセキュリティは大きな課題として扱われており、多くのガイドラインやホワイトペーパーなどが公開されている。特に、機密性に関するリスクはクラウドサービスを利用するユーザにとって重要度の高いリスクとして認識されている。

これは、クラウドサービス事業者のセキュリティ対策状況を把握すること、その中でも特に、システム管理者や他ユーザへの情報漏えい対策を確認することが困難であること等に起因していると考えられる。これらの課題について、以下にそれぞれ述べる。

1) クラウドサービス事業者のセキュリティ対策状況の把握

一般に、クラウドサービス利用契約前にクラウドサービス事業者のセキュリティ対策状況を把握することは困難である（契約後であれば契約の範囲内でクラウド事業者に対する監査を行うことなどが可能な場合がある）が、そのニーズは根強く存在する。

そこで、クラウドサービス事業者では、ユーザ向けに「情報セキュリティ報告書」や、各種ホワイトペーパーなどを公開するとともに、クラウドセキュリティ強化ソリューションなどを準備している。また、事業者内部向けには、セキュリティ対策状況を自動的に把握するツールの導入などが進められている。

また、複数社・サービスでシステムを構成している場合（SaaS のインフラとして PaaS

[2] IDC Japan（2011 年 4 月）http://www.itmedia.co.jp/enterprise/articles/1104/04/news047.html http://enterprisezine.jp/article/detail/3049

や IaaS を利用している場合など）では、それぞれがセキュリティを担保できる範囲が異なっており、サービス全体としてのセキュリティ対策状況を把握することは非常に難しい。

そこで、米国政府では、FedRAMP[3]という政府によるクラウドサービス利用の際の、クラウドサービスのセキュリティ評価・認証プログラムが進行している。当該プログラムでは、評価・認証を受けたサービスのみを政府調達可能とすることにより、政府によるクラウドサービスの利用を安全なものとしている。

2) クラウドサービスにおける情報漏えい対策（プライバシー保護）

近年、ビッグデータの分析・利活用が進んでいる。例えば、多くのサービスにおいて、クラウド・コンピューティング環境を利用した情報の管理・分析が行われており、広告やマーケティング等に活用されている。このような場合には、情報漏えいに備えて、個々のサービスにおいて適切にデータの匿名化が行われており、個々のサービスの情報が漏えいした場合でも、個人のプライバシー情報の漏えいにつながらないようにしている。その一方で、複数のサービスにおいて情報漏えいがあった場合には、それらを組み合わせて分析することにより、個人のプライバシー情報漏えいにつながる可能性がある。そのため、ビッグデータの分析・利活用には、適切な情報漏えい対策が必須となる。

一般に、情報漏えい対策としては、不正アクセス対策とともに、データの暗号化が用いられることが多いが、当該データを処理する場合には復号する必要があり、その際の情報漏えいは避けられない。また、データ暗号化を行う場合には、その暗号鍵管理等の運用が複雑になってしまう。

そこで、暗号化したまま処理を可能とする「準同型暗号」や、アクセスコントロールと暗号化を一体化させた「関数型暗号」、暗号鍵管理の負荷を下げる「再暗号化技術」などが実用化に向けて研究開発されている。特に「準同型暗号」では、すべての演算を暗号化したまま行うことは困難であるが、機能を絞ることにより実用度を高めてきている。

また、従来の入口対策（不正アクセスされないための対策）に加えて、近年では出口対策（不正アクセスされても情報漏えいさせないための対策）を行うことにより、機密性を担保する方法が取られることが増えてきている。

[3] http://www.gsa.gov/portal/category/102371

1.2 スマートフォン

1.2.1 市場動向、活用事例

スマートフォンの 2011 年の市場規模は出荷台数で 2,005 万台、2015 年には 3,454 万台になると予測されている[4]（図 1.2-1）。業務用スマートフォンの導入状況は、導入済みは 7.7%、導入検討中は 36.9%で全体の 44.6%となっており、半数近くが業務にスマートフォンを活用したいと考えていることがわかる。これは、端末の選択肢の増加、業務アプリケーションの増加、自社開発環境の整備等が進展してきたためで、今後、ますます企業でのスマートフォンの利用が進展すると予測される。

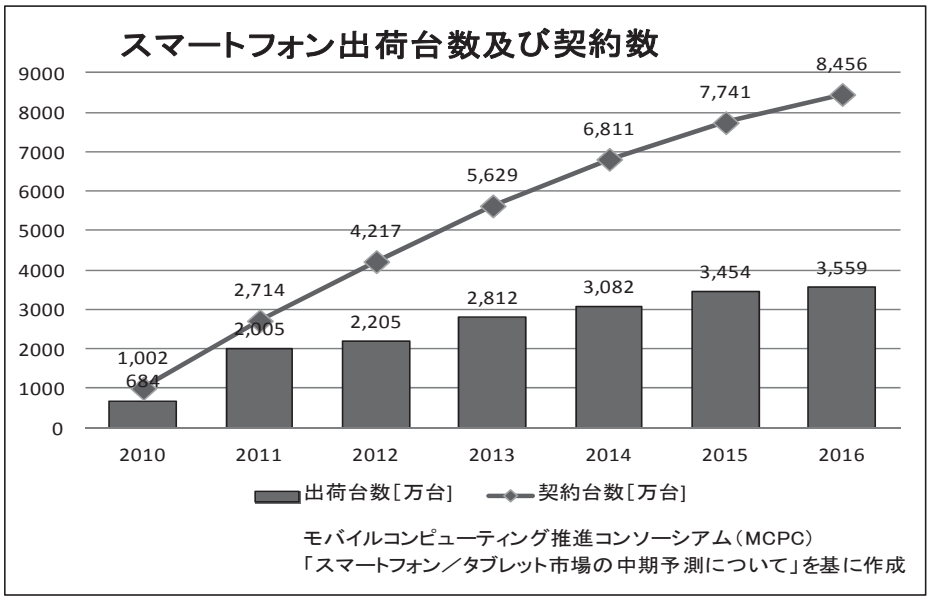


図 1.2-1　スマートフォンの出荷台数および契約数

スマートフォンを業務に導入を検討している企業は、大企業よりも中堅／中小企業の方が高い割合になっている。また、業務用スマートフォンの導入のきっかけとしては「業界での業務用スマートフォンの導入が進んでいるので、自社でも積極的に取り入れた」といったもので、およそ過半数に達している。このことから、業務アプリの充実や導入事例が増えてくるとともに、今後、ますますスマートフォンを業務に導入する企業が増えてくると考えられる。

業務でのスマートフォンの利用目的も「社内コミュニケーションの円滑化」から「営業・渉外の効率化」に変化してきており、単なるコミュニケーションツールから、より社外に持ち出してビジネスに直結するツールとして利用されることがわかる（具体的事例は MRI

[4] 「スマートフォン／タブレット市場の中期予測について」モバイルコンピューティング推進コンソーシアム（MCPC）http://www.mcpc-jp.org/news/index.htm

報告書「1.2　スマートフォンの導入事例」を参照のこと)。これらの導入事例でもわかる通り、スマートフォンで取り扱うデータは顧客情報や知財情報、企業情報（財務、従業員情報など含む）など重要度が高い情報である。また、スマートフォンは社外で利用する事例が多いことからも携行先での紛失や盗難には気を付ける必要がある。調査（MRI 報告書「1.2 スマートフォン　市場動向⑥」）によると、調査対象企業の 7 割がスマートフォンなどの携帯端末の対する依存度が 1 年前よりも高くなっており、半数以上は携帯端末の紛失・盗難による情報漏えいを課題ととらえている。紛失または盗難に遭った携帯端末上のデータは、顧客データが 4 割、企業の知的所有権に係わる情報 3 割など、重要な情報が多いことがわかる。

業務へのスマートフォンの導入割合が大企業よりも中堅／中小企業の方が高い一つの理由に導入コストの問題がある。大企業では業務用スマートフォンの導入に中小企業より大きな導入コストがかかる。そこで、業務へのスマートフォンの導入コストを低減させるとともに、使い慣れた端末を利用して利用者の利便性が向上できるなどのメリットから、個人のスマートフォンを業務に利用したいという要望もある。しかし、スマートフォンを導入済みの企業、今後導入予定の企業の過半数が個人用スマートフォンの業務利用を認めていない。また、個人でスマートフォンを持つ利用者が増加しているが、企業でのスマートフォン利用に対するポリシーや規定整備が遅れているケースも少なくない。

スマートフォンを業務に利用している企業の 60%以上が、利便性の向上、業務の効率化、そしてビジネスの機会損失防止に役立っている。しかし、40%弱の企業は何らかの不満を持っている。その不満の理由は、「既存システムとの適合性が悪い」、「紛失の可能性が高い」、「ネットワークセキュリティの理由で利用できる機能に制限を加えている」などで、多機能なスマートフォン本来の利点を活用し切れていない点である。

スマートフォンは、紛失リスクやセキュリティの解決、導入コストの問題などが解決できれば、業務でのスマートフォンの活用がさらに進展する可能性があると言える。

1.2.2 セキュリティ課題

スマートフォンは利便性の向上、業務の効率化、ビジネスの機会損失防止などのメリットが大きいことから、業務利用が加速されていくと考えられる。業務での利用が増大されてスマートフォン上で重要な情報が扱われるようになってくると、それらの情報を狙う攻撃者も必然的に増加してくる。従来の多機能携帯電話は機種毎に異なる仕様を持ち、利用者の作ったプログラムを動作させることが難しいなどから、ほとんど攻撃対象にはならなかった。しかし、スマートフォンは共通の仕様を提供する OS を搭載するとともに、利用者が自由にアプリケーションを追加することや、アプリケーションの開発も自由にすることができるようになっている。これは PC とその性格が似ていると言える。また、PC 以上に、カメラ機能、GPS、加速度センサ、マイクロフォンなどのデバイスを搭載しており、

スマートフォンの存在している位置情報や周囲環境情報を収集するセンサとして利用できるので、PC 以上の情報が得られる可能性が高いと言える。

スマートフォンは、一度に取り扱える情報量は多くはないが、通信情報の他に位置情報や画像情報などの機微情報が多いので、これらの機微情報が漏えいすると、企業や利用者にとって大きなダメージを与える可能性がある。スマートフォンのセキュリティ対策はまだ不十分であり、PC と同等あるいはそれ以上にセキュリティに対して気を付けなければならないと言える。

特に、OS として Android を使った端末については IPA が 2011 年 1 月に「Android OS を標的としたウイルスに関する注意喚起」を公開するなどしているが、その後も Android 端末を狙ったウイルスは増加傾向にある（図 1.2-2）。そして、徐々に機能も高度化してきている。

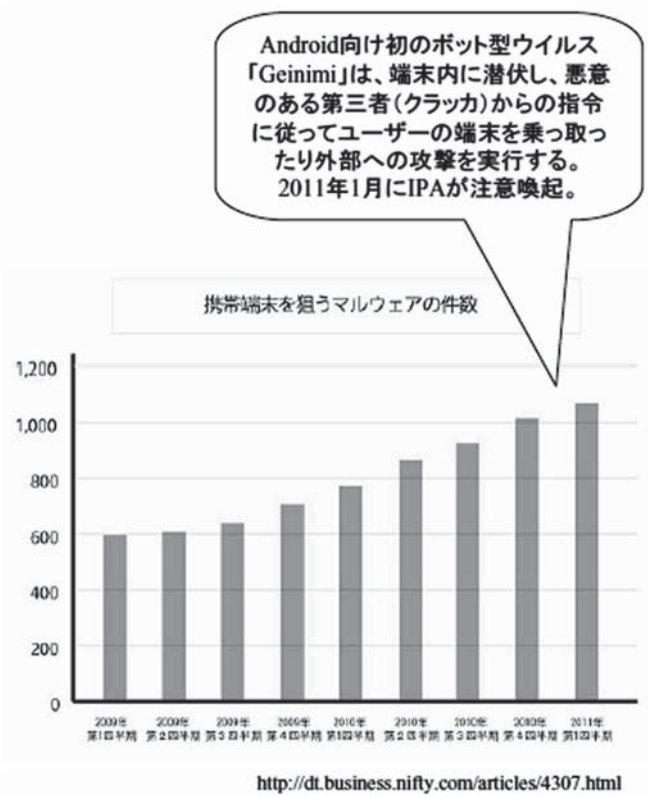


図 1.2-2　携帯端末を狙うマルウェアの件数

企業が業務でスマートフォンを利用する場合に考慮しなければならないセキュリティ課題は大きく分類すると次の 4 つがある。

1）スマートフォンの紛失や盗難

・スマートフォンに保管されている重要情報の漏えい

・攻撃者に企業への侵入口を提供してしまう

2) 不正プログラム（マルウェアを含む）からの情報漏えい

・不正なプログラムが勝手に導入されて情報を漏えいさせる

・GPS やカメラで居所や行動を不正に特定される

3) 意図しない接続による重要情報の流出

・SNS を利用する際に誤って企業の重要情報を書き込んでしまう

・アクセス先が確認できずにフィッシングされて情報を流失させてしまう

・アプリケーションの動作がわからないまま利用して、誤って情報を流失させてしまう

4) OS のバージョンアップ

・OS の脆弱性修正のタイムラグを攻撃されて情報が漏えいする

特に不正プログラムによって、知らないうちに GPS やカメラが動作して不正に位置情報が取得される可能性もあるので注意する必要がある。

不正プログラムに対する考え方は、それぞれのスマートフォンに搭載されている OS によって異なっている。スマートフォンの OS として iOS(iPhone)、Android OS、BlackBerry、WindowsPhone（旧 WindowsMobile）等がある。

iOS(iPhone)や WindowsPhone アプリでは、AppStore や Windows Phone Market Place と呼ばれる公式なマーケットプレイスでアプリケーションが審査されており、不審なアプリケーションを検知し、利用者の端末に不正プログラムがインストールされることを防げる。また、OS のバージョンアップも同時に可能であり、迅速な脆弱性対策が可能である。このため iPhone, WindowsPhone は、現在のところセキュリティ上比較的安全な端末と言える。しかし、Android 端末で利用される AndroidMarket[5]は、悪意のあるプログラムを自動的にスキャンする仕組みが導入されてはいるが、AppStore と比べて事前審査をする仕組みがない。このため、動作が不審なアプリケーションや、安全に作成されていないアプリケーションがインストールされないようにすることができない。アプリケーションの善し悪しは利用者が自らが判断して、端末にインストールするか否かを決める必要がある。また、Android OS に脆弱性が発見された場合のバージョンアップは、端末メーカーにより提供されるので、メーカー毎にリリース時期がばらつき、バージョンアップのタイミングが遅くなることがある。これにより、脆弱性が残されたまま利用される Android 端末も多く存在することになる。

Android 用のウイルス対策ソフトも何種類か市場に登場しているが、システム領域のウイルスや不正をチェックすることができない。さらに Android 用ウイルス対策ソフトは、アプリケーションとして動作しているのでそれ自身の動作を止めることは比較的容易にで

[5] Android Market は、2012 年 3 月より Google Play の一部として統合された。Android アプリ開発の為の審査プロセスやポリシーは従来と同じである。

きるので、ウイルス対策ソフトを導入していても安全とは言い切れない。

スマートフォンなどで用いられる OS 別の脅威を表 1.2-1 に示す。

表 1.2-1　携帯端末 OS 別脅威

OS	OS提供元	展開モデル	特徴	マーケットの特徴
iOS(iPhone)	Apple Inc.	垂直統合型 ・OS、 ・デバイス ・アプリケーションマーケット	・iPhone/iPad上でのみ稼動し、最新バージョンの適用が容易。 ・基本的に安全 ・Jailbreak（脱獄、サードパーティアプリをインストール可能とし、ファームウェアを書き換える）を実行させるサイトに注意が必要。	・App Store ・Appleがアプリケーションを審査。アプリケーションの配布や使用時は、Apple社が発行の証明書が必要
Android	Google	水平分業型 ・OS ・デバイス ・アプリケーションマーケット	・デバイスの選択肢が豊富。オープンソースのOSであり、基本的には、各デバイスメーカーが独自に開発したデバイスにカスタマイズして搭載。OSバージョンが同一でも機種依存がある。 ・2009年からウィルスなどの不正プログラム（マルウェア）が急増してきた。 ・現在の不正プログラムは利用者自らがインストールする行為に起因するが、今後、自動的にインストールされてしまうエクスプロイトが出現する恐れがある。	・Android Market ・Googleは審査せず、その活用は利用者或いはデバイスメーカーにゆだねられる(自動的に悪意あるプログラムをスキャンして排除しているが、アプリケーションの善し悪しは利用者が自ら判断する必要がある)
BlackBerry	Research In Motion（RIM）	垂直統合型 ・OS、 ・デバイス ・アプリケーションマーケット	・現在はBlackBerry上でのみ稼動 ・基本的に安全。 ・出所が不明だったり、危険なアプリケーションやはインストールできない。 ・デバイスとして、FIPS140-1/2やCommonCriteriaなどのセキュリティ認証を取得している。	・App World ・RIMがアプリケーションを審査
WindowsPhone	Microsoft	水平分業型 ・OS ・デバイス ・アプリケーションマーケット	・METRO UIとExchange等による管理機能搭載。 ・Windows OSと同様の脅威が存在。 ・対策にもノウハウがあり、セキュリティ対策ソフトも充実	・Marketplace ・Microsoftがアプリケーションを審査

スマートフォンは登場して間もないこともあり、前述のようなセキュリティ課題が多くある。スマートフォンに不正プログラムが入り込むと、顧客情報（個人情報、プライバシー情報）や企業情報（知財、経営、居場所情報）などの機微重要な情報が漏えいする可能性がある。これにより、顧客や企業の行動が悪意を持った者に筒抜けになる可能性がある。これらの機微情報が悪用された場合には甚大な被害が予測される。また、顧客情報が漏えいした場合は賠償金の請求リスクも発生する。スマートフォンが利用できなくなると業務が実施できないなど経営的な損失が発生する。また、テロリストなどにこれらの機微情報が渡った場合には顧客、企業の経済的な損失だけでなく会社、人命が危険に曝されることも考えられる。このようなことからも、スマートフォンの業務への導入に関してはセキュリティ課題を十分に考慮して、予めセキュリティ対策を考えておく必要がある。

第2章 企業における脅威の顕在化

2.1 東日本大震災の影響

2.1.1 震災に対する BCP の評価

2011 年 3 月に発生した東日本大震災では、これまでにない広範囲に、被害が及ぶ結果となった。直接的な被害の大きかった岩手・宮城・福島・茨城の 4 県以外に本社を置く企業へのアンケート（図 2.1-1）[6]によれば、回答企業の約半数 44%では「業務は停止しなかった」との回答であるのに対し、他の 55%では何らかの業務が停止した結果となっている（「重要な業務が停止」26%、「一部（重要でない）業務が停止」29%）。また、重要な業務が停止した企業の 21%では、業務停止の期間が「1 ヶ月以上」と回答されており、長期にわたり業務に影響を受けた企業もあったことが窺える。

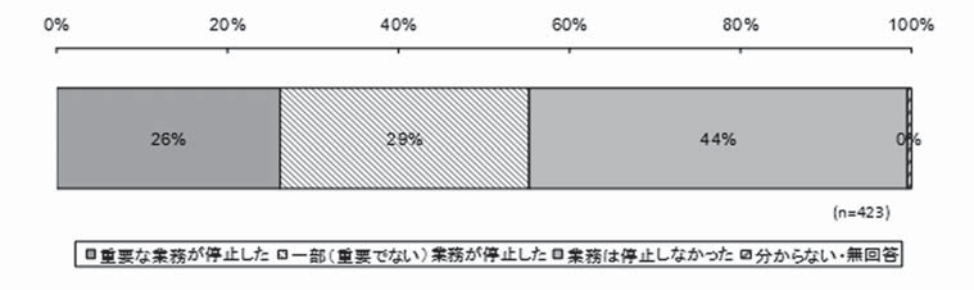


図 2.1-1　重要業務の停止状況

業務停止の主な理由は、「停電」、「業務に必要な生産拠点が利用できなかった」、「取引先の業務停止などにより必要な調達・供給が行えなかった」であり、計画停電やサプライチェーンの機能低下が大きな原因となっている。

さらに、これらの企業の約 2/3 が震災時に BCP を策定済み／策定中であったが、そのうち 9 割以上の企業で「BCP が有効に機能しなかった」という結果となっている（図 2.1-2）。（BCP 策定状況は、49%が「策定済み」、17%が「策定中」。BCP への評価は、「十分に機能した」企業は僅か 7%にとどまるのみ、「概ね機能したが一部に問題があった」が 78%、「ほとんど機能しなかった」は 15%にも上っている。）

[6] 「東日本大震災の影響と BCP（事業継続計画）に関するアンケート調査結果」株式会社野村総合研究所（2011 年 6 月 30 日）　http://www.nri.co.jp/news/2011/110630_1.html

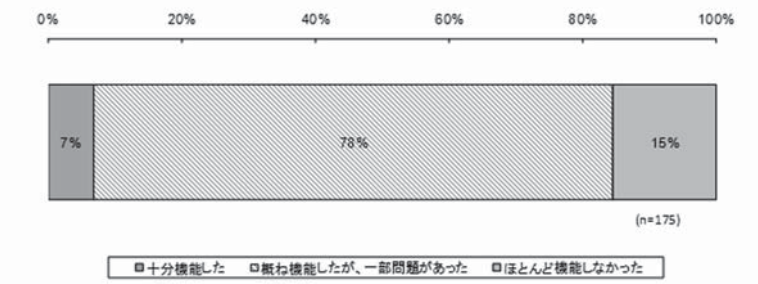


図 2.1-2　自社の BCP に対する評価（BCP の対象となる被害のあった企業で集計）

また、同アンケートでは、今後の BCP の見直しとして、「サプライチェーンの再構築」、「社員の安否確認システムの導入」、「システムに対する防災対策」だけでなく、「リモートオフィス環境の整備」、「本社などオフィスの分散」といった“１拠点が災害で機能しなくなった場合の可用性の確保”も重要な見直し要素となっていることがわかる。

2.1.2 非常時におけるセキュリティ課題

東日本大震災では、電源・サーバ・PC・通信インフラ等の企業インフラも大きな損害を受けており、これによるセキュリティ上の問題も発生している。サーバ機器内の重要データの消失や流出（漏えい）、入退室管理システムや監視システム等が停電により機能停止した、といった問題である。

また、震災後の BCP の課題として顕在化した「バックアップサイトの確保」や「リモートオフィス環境の整備」をクラウドで検討する企業も増えてくると見込まれる。実際、震災後の業務機能回復のサポートとして、安否確認、情報共有、情報発信、メールサーバ・グループウェア・WEB 会議等がクラウドで無償提供され活用されたケースもあり[7]、今後の有効な対応策として検討されると想定される。

その他にも、プライバシー保護における問題として、人命優先のため震災直後は一時的にプライバシー保護が全くない状況も容認されるが、一方で過剰なプライバシー保護により現場で混乱発生するなどの問題もあった。

非常時の場合を考慮して検討すべきセキュリティ課題を以下にまとめる。

1）非常時を考慮したセキュリティ対策のあり方

情報漏えい（情報流失）や不正アクセスへの対策、停電等によりセキュリティ対策の機

[7] 「震災時の緊急支援に役立てられたクラウドサービスの事例と、復旧･復興に向けたクラウドサービス安全利用に関する資料の公開」独立行政法人情報処理推進機構（2011 年 12 月 19 日）http://www.ipa.go.jp/security/cloud/cloud_sinsai_R1.html

能が停止した場合の対応､非常時に備えたバックアップサイト･冗長化の整備等について、検討が必要である。

2) 非常時における企業インフラのあり方

サーバ・PC・通信インフラが被害を受けた際に、事業継続の観点から、どこまでの代替使用を認めるか。リモートオフィス環境やバックアップ環境の整備と合わせ、非常時における個人デバイスの使用可否、スマートフォンや SNS などの新しいインフラの活用の範囲をどうするか、また、バックアップサイトの確保やリモートオフィスの整備などでクラウドを活用する場合、クラウド活用時のリスク、セキュリティ課題についても評価が必要である。

3) 非常時におけるプライバシー保護のあり方

非常時においては、プライバシー保護よりも安否確認が優先される場合も発生する。プライバシー情報取り扱いの範囲や規定を緩和し、一定条件のもと活用を認める等のしくみも重要であり[8]、予めそれらを規定しておくことが混乱を低減することにつながる。

[8] 「東北地方太平洋沖地震等に際しての住民基本台帳ネットワークシステムの活用について」総務省自治行政局住民制度課（平成 23 年 3 月 23 日）http://www.cas.go.jp/jp/seisaku/jouhouwg/renkei/dai3/sankou4.pdf

2.2 サイバー攻撃の状況

2.2.1 サイバー攻撃の動向

2011 年は、政府機関や防衛産業企業等に対する「サイバー攻撃」が相次いで発生し、大きく報道された。2011 年に発生した主なサイバー攻撃事例を、表 2.2-1 に示す。ネットワークサービスが停止したり、大量の個人情報が漏えいしたりするなど、大きな被害をもたらしていることがわかる。

また、サイバー攻撃を行う攻撃者の動機も変化している。自己満足のためのいたずらや売名行為、能力の誇示ではなく、数年前から金銭目的や組織活動の妨害に変化している。

金銭目的の場合は、組織内の機密情報や個人情報など価値のある情報が狙われており、これらを窃取されることで大きな被害を及ぼすことになる。

政治的・思想的な動機による組織活動の妨害や社会的混乱を狙ったサイバー攻撃の事例も増えてきている。標的となる組織に対して、何らかの打撃を与えること自体を目的とするケースもある。米国では、国防長官が、サイバー空間を第五の戦場として位置づけ、サイバー攻撃を戦争行為と見なす旨の発言をしている。今後、攻撃の激化、被害の深刻化も懸念される。

表 2.2-1　2011 年に発生した主なサイバー攻撃事例

企業・組織名	時期	サイバー攻撃の内容
ソニーコンピュータエンタテイメントアメリカ	4 月	「Play Station Network (PSN)」が不正アクセスを受けて停止。約 2460 万件の SOE アカウントと約 1 万 2700 件のクレジットカード/デビットカードの番号と有効期限情報、オーストリアとドイツ、オランダ、スペインユーザの約 1 万 700 件のダイレクトデビットカードの購入履歴情報が流出
米シティグループ	5 月	ネットバンキングシステムにハッカーが侵入。北米地域 36 万人分のカード口座が影響
米グーグル	6 月	電子メールサービス「gmail」利用者数百人がメールの内容を盗み見られる
衆議院	7 月	議員パソコンや衆議院内サーバがウイルスに感染し、議員ら利用者の ID とパスワードが盗難
参議院	8 月	議員パソコンや参院内サーバがウイルスに感染し、全議員・秘書と管理者用の計 700 件強のパスワードが流出
三菱重工業	9 月	本社や工場、研究所など 11 拠点にあるサーバと従業員のパソコン約 80 台がウイルスに感染

2.2.2 標的型攻撃とは

今回のサイバー攻撃では、一部で特定の組織や個人を狙った「標的型攻撃」という手法を用いていることが特徴としてあげられる。情報処理推進機構(IPA)では、これを「新しいタイプの攻撃」と呼び[9] 、海外では、「APT (Advanced Persistent Threats)：高度かつ継続的な脅威」とも呼ばれている。特に標的型メール攻撃の被害が顕在化している。標的型メール攻撃のプロセスを以下に紹介する[10] 。

【攻撃のプロセス】

（攻撃準備）

攻撃対象組織や狙うべき弱い部分の事前調査

（事前攻撃）

1) 信頼できる組織や個人を騙った巧妙な標的型攻撃メールの送付

2) 特定の情報窃取を目的とした業種や組織への執拗な攻撃

（本攻撃）

3) メールの添付ファイルの開封やURLのクリックによるウイルスの一次感染
ウイルスは普段使っているアプリケーションソフトウェアの脆弱性(ゼロデイを含む)を悪用しているケースが多い。

4) 感染ウイルスによる外部の攻撃指令サーバとの通信

5) ウイルスの増強・変身や新たな攻撃プログラムのダウンロード

6) 組織システム内での潜伏・拡散・侵攻・探索

7) 機密情報や個人情報等の窃取

8) 外部の攻撃者への窃取情報の送出

標的型攻撃は、実メールを悪用したり、信頼できる実組織を騙ったりするなど、攻撃を見分けることが困難であり、”persistent(しつこい、持続する)”という名前の通り、長期に渡って、執拗に情報探索活動を行い、目的の情報を窃取するという特徴がある。

標的型攻撃に対抗するためには、従来の対策だけでは不十分であり、新しい対策が必要となる。

2.2.3 政府機関等の取組

このようなサイバー攻撃による被害の発生を受け、政府機関を中心に、サイバー攻撃に

[9] 「組織の重要情報の窃取を目的としたサイバー攻撃に関する注意喚起」
独立行政法人情報処理推進機構　http://www.ipa.go.jp/about/press/pdf/110920press.pdf

[10] 「標的型サイバー攻撃の事例分析と対策レポート」独立行政法人情報処理推進機構
http://www.ipa.go.jp/security/fy23/reports/measures/documents/report20120120.pdf

関する手法や事例などの情報を共有し、被害の発生や拡大を防ぐための取組が進んでいる。主な取組を表 2.2-2 に示す。

表 2.2-2　政府機関等における取組

取組	概要
サイバー情報共有イニシアティブ(J-CSIP[11])	経済産業省主管の下、サイバー攻撃による被害拡大防止のため、重工、重電等、重要インフラで利用される機器の製造業者を中心に情報共有と早期対応の場として設立
情報セキュリティ政策会議	官民連携等を通じて企業等の情報セキュリティ対策を強化するため、政府調達に際してのセキュリティ要件、政府の情報提供の在り方等を検討する分科会の設置[12]
防衛省 調達におけるセキュリティ基準	従来から定めていた、調達時のセキュリティ基準を、防衛関連企業に対するサイバー攻撃の発生を受け、規則を一部改正[13]
サイバーインテリジェンス情報共有ネットワーク	警察庁を中心に、サイバー攻撃の標的となる恐れのある事業者（全国で約 4000）との連携を強化し、サイバー攻撃事案の情報を集約・分析し、事業者に対し注意喚起を実施[14]
日本セキュリティオペレーション事業者協議会(ISOG-J[15]) 標的型攻撃対策検討 WG	ISOG-J は、セキュリティオペレーションに携わる事業者の団体。標的型攻撃の実態調査およびその防御策について検討、実証実験を行う WG を立ち上げ

[11] Initiative for Cyber Security Information sharing Partnership of Japan
[12] http://www.nisc.go.jp/conference/seisaku/dai28/pdf/28seisakupress.pdf
[13]「防衛関連企業における情報セキュリティ確保について」防衛省
http://www.mod.go.jp/j/approach/others/security/security.html
[14]「サイバーインテリジェンス対策に係る警察の取組について
http://www.npa.go.jp/keibi/biki3/230804kouhou.pdf
[15] Information Security Operation providers Group Japan

第3章　求められる情報セキュリティ対策

3.1 クラウド利用時の課題

3.1.1 複数クラウド利用時の課題

NIST SP500-291 NIST Cloud Computing Standards Roadmap によれば、クラウドサービスは単一のものから、複数のクラウドサービスを統合したサービスであるマルチプルクラウドサービスへ変遷すると記載されている。その形態としては、単一事業者内の複数の SaaS の連携を実現する場合や、複数の SaaS 事業者に跨がる連携サービスを実現する場合、SaaS 事業者が PaaS や IaaS を利用する場合など、多岐にわたるが、ここでは、最も課題が顕在化する「複数の SaaS 事業者に跨がる連携サービスを実現する場合」にフォーカスし、主要な 3 つの課題について対策を述べる。

（1）課題１：他事業者のセキュリティ対策状況の悪化による波及

複数の SaaS 事業者により一つのサービスが提供されている場合、一つの事業者のセキュリティ対策状態が悪化した場合、サービス全体としてのセキュリティ対策状態の悪化となってしまう。その結果として、全体として脆弱な状態でサービスを継続することとなってしまい、セキュリティ事故が発生してしまうリスクが高まってしまう。

このような事態を避けるためにも、サービス提供に係る SaaS 事業者間またはクラウドサービスブローカ等による、継続的なセキュリティ状態の監視（可視化）や情報共有等が必要となる。

また、実際にインシデントが発生した場合に問題を切り分けるための適切な仕組み作り（事業者間でユーザの状態遷移をトレースする仕組み等）も重要となる。

（2）課題２：ID 連携の信頼性の確保

複数の SaaS 事業者により一つのサービスが提供されている場合、それぞれの SaaS 事業者に対して ID を作成するのではなく、一つの ID を連携させて利用することが一般的である（ここでは ID をユーザの識別子と属性情報の組み合わせを言う）。一般的なシングルサインオンは同一事業者内のシステムに適用されていることが多い一方で、複数のクラウドサービス事業者間に跨がる ID 連携を実現する場合には、Identity Provider と SaaS 事業者の間の信頼関係作りがカギとなる。

そのためにも、NIST SP800-63「電子的認証に関するガイドライン」や、近年 OpenID ファウンデーションなどで検討が進められているトラストフレームワークの検討成果を適切に取り入れた、技術面・運用面の双方からの ID 連携の仕組み作りが重要となる。特に技術的には、連携されてくる ID の信頼性を定量化する仕組み（level of assurance）が重要である。

また、複数サービスでの ID 連携を行う場合には、サービス利用開始時の ID 連携は当然であるが、サービス利用終了時のシングルログアウトを確実に行う仕組みを持つことにより様々なセキュリティの課題の解決やサーバのリソース解放につながる。

（3）課題３：プライバシー保護を実現する技術

1.1.2 項にも述べた通り、クラウド・コンピューティングを活用したサービスの市場拡大や、ビッグデータの分析・利活用が進むにつれ、利用者のプライバシー情報漏えいのリスクが高まっており、適切な情報漏えい対策が求められている。

クラウドサービスを対象としたプライバシー保護のための暗号化技術は、様々なものが開発されている。それに加え、データの匿名化のための技術として、k-匿名化[16] やトークナイゼーションなどのように様々なものが研究・開発されてきており、実用化されているものもある。

・暗号化：データを可逆状態で秘匿処理を行う。処理時には復号する必要がある。
・匿名化：データを不可逆に抽象化することにより個人と紐付かない様にする。
　　そのまま処理可能。

これらは、システムの要件（処理速度等）や特性（データに求める精度等）によって適切に使い分ける必要がある。

3.2 スマートフォンの企業活用

スマートフォンを企業で安全に活用するためには、1.2 節で提示したセキュリティ課題を解決する必要がある。

（1）課題１：スマートフォンの紛失や盗難への対策

スマートフォンの紛失や盗難における対策としては、パスワードによるスマートフォンの利用者認証や、リモート（遠隔）によるスマートフォンのロック、重要なデータの暗号化、スマートフォンの真正性確保などの技術的な対策の他、セキュリティポリシーの整備と遵守の徹底、利用者へのセキュリティ教育などが有効である。また、スマートフォンの遠隔ロックや遠隔初期化や自動的にデータを消去、パスワードポリシーが設定できる MDM(Mobile Device Management)や MDP(Mobile Data Protection)等の管理ツールの導入といった手段が有効である。しかし、私物のスマートフォンの利用を許可した場合の運用では MDM や MDP での管理ができないケースもある。万が一、紛失・盗難にあった場合には、業務が停止しないように大事なデータはスマートフォン以外の別の場所にバックアップを取っておく必要がある。バックアップ媒体もセキュリティ対策をしておく必要が

[16] 与えられたデータから k 人にまでしか特定できないようにする不可逆の匿名化技術。

ある。また、紛失したスマートフォン以外の端末装置でも業務が継続できるように、業務データをクラウドネットワークに保管し、様々な端末装置から業務データを活用できるようにすることも考えるべきである（マルチデバイス対応)。

紛失・盗難に遭ったスマートフォンが戻ってきた場合でも、システムが改ざんされている可能性があるので、直ぐに業務には利用しないで、完全な初期化を実施した上で利用を十分に検討する必要がある。また、スマートフォンの OS やアプリケーションが改ざんされた場合には起動しなかったり、自動で正しい OS やアプリケーションに修正されるなどの真正性確保のための方法が取られることが望ましい。また、業務に必要なデータは改ざんや不正な読み出しが行われないようなハードウェアを利用することも良い。このようなスマートフォンを利用することで、紛失・盗難にあってもセキュリティ上の脅威が低減するので安心である。

（2）課題２：不正プログラムからの情報漏えい対策

スマートフォンに不正プログラム（マルウェア）が入り込むと、スマートフォンの OS の脆弱性を悪用する不正プログラムや、不正プログラム自身の機能により、重要な情報の漏えいや、業務が停止するなどの脅威があるので十分な対策を行う必要がある。

不正プログラムがスマートフォンにインストールされる要因としては、興味本位でインストールしたアプリケーションに不正プログラムが仕込まれていてインストールされた、Web サイトを閲覧したら勝手に不正プログラムがインストールされた、目を離した隙に他人により不正プログラムがインストールされた、などがある。

第１の対策として､不正プログラム自身がインストールされないようにすることである。不正プログラムがインストールされることを防止するために、①アプリケーションは信頼できる場所からインストールする、②提供元不明のアプリケーションはインストールしない、③アプリケーションをインストールする際にどの情報や機能にアクセスするのかを確認して必要なアクセス以外は許可しない、などの方法を取る。

第２の対策として、不正プログラムの動作を禁止することである。そのために、スマートフォン用のセキュリティ対策ソフトを利用することも考える。PC では、セキュリティ対策ソフトが一般的になってきたが､スマートフォンではまだ普及しているとは言えない。しかし、Android OS などではその構造上、セキュリティ対策ソフトを停止することが可能であるので、過信してはいけない。

第 3 の対策として、セキュリティ強度が高いスマートフォンを利用することである。1.2.2 項で述べたように iPhone や WindowsPhone では公式のマーケットプレイスで不正プログラムの検出を行っており､比較的不正プログラムがインストールし難くなっている。このため比較的にセキュリティ強度が強いと言える。逆に、Android 端末では現在のとこ

ろ利便性が優先されており、様々な情報や機能にアクセスできるようになっているので、不正プログラムにとっても活動がしやすくなっている。

セキュリティ面で他のスマートフォンに遅れを取っていたAndroid OSであるが、2012年1月には、米国家安全保障局（NSA）が、Androidのセキュリティ強化版となる「Security Enhanced（SE） Android : SE Android」のパブリックリリースを公開したなど、Androidにおいてもセキュリティは強化されてきている。

スマートフォンのOS(iOS、Android、WindowsPhone)はソフトウェアであるため、OS自身が改ざんされセキュリティ機能がバイパスされる恐れがある。このため、OS やアプリケーションをハードウェアで保護すると言う取組がスマートフォンでも進んできている。PCではTPM(Trusted Platform Module)といったISO化されている安価なハードウェアセキュリティチップを利用してOSやアプリケーション、データ等を改ざんから保護している（真正性の確保）。スマートフォンでもPCと同様にハードウェアベースのセキュリティチップを利用して真正性を確保する仕組みを搭載する動きがある。ただし、改ざんから保護すると言うことは、利用者が便利なアプリケーションを容易にインストールすることができなくなり利便性が低下するということにもなる。セキュリティ確保と利便性の確保のために、最近ではスマートフォンに2つのOSをインストールして、セキュリティを強化した部分（セキュア領域）と、セキュリティは低下しているが比較的自由にアプリケーションをインストールでき利便性を高めた領域（ノンセキュア領域）に分けるような端末も開発されている。また、同様な機能を一つのOS内で実現するOSも開発が進んでいる。今後は、より一層セキュリティが強化され業務に利用できるようなスマートフォンが登場すると思われる。

（3）課題3：意図しない接続による重要情報の流出対策

スマートフォンを業務に利用する場合には、企業で定めたセキュリティポリシーに合わせた運用を確実に実施することが基本である。

業務で SNS などを利用する場合には、誤って重要な情報を漏えいさせないように、スマートフォンで利用するアプリケーションを制限するなどの対策が必要となる。昨今のSNS（例えばTwitterやFacebookなど）では多くのSNS用のアプリケーションが提供されている。これらのアプリケーションは SNS に保管されているデータやスマートフォンを便利に使うためのものであり、場合によって不本意にセキュリティがないアプリケーションに渡され、SNS から情報が流失することもある。このため、SNS 用アプリケーションの利用を制限するあるいは利用しない、利用されるデータに制限を加える、などの方法を取るのが良い。

スマートフォンにどのような情報が格納されているのかを常に把握することも必要とな

る。私物スマートフォンを利用する場合には所有者のプライバシー情報も把握する必要があるので、管理・運用とプライバシー保護の両方に配慮する必要があるので、ガバナンスの観点から言うと、業務には会社から支給されたスマートフォンを利用する方が安全である。

さらには、スマートフォンに格納されているデータそれぞれに、利用できるアプリケーションを限定するような仕組みを導入することを考えるのも良い。昨今では、常に暗号化したままデータ処理を行う技術（再暗号化技術など）の研究開発が進んでおり、この技術を利用すると、特定の業務アプリケーションや特定の利用者だけがデータを利用することができるので、意図しない情報の流失を防げるようになる。その他、誤った操作により情報を漏えいさせることを防止するためにアプリケーションの画面やユーザインターフェースなどを統一することや、SNS を利用する際のポリシーを策定し、セキュリティ意識を向上させることも重要である[17]。

（4）課題 4：OS のバージョンアップの対策

OS のバージョンアップはスマートフォンの OS 種類毎に異なることは、表 1.2-1 に示した通りである。OS のバージョンアップのセキュリティ課題は、セキュリティに脆弱性が発見された場合に早急に脆弱性が修正されるか否かがポイントとなる。脆弱性が発見されてもなかなかそれが修正されなければ、その脆弱性を突いて攻撃され情報が流失する可能性がある。

iOS(iPhone)や WindowsPhone では OS 開発元の Apple 社や Microsoft 社が提供する脆弱性修正パッチをこまめに適用する基本的な方法の徹底をする。一方、Android では基本的に製造メーカーが提供する脆弱性修正パッチや OS バージョンアップによるアップデートを適用する以外に方法がない。また、各社とも異なったハードウェア上で OS がカスタマイズされているので、脆弱性修正パッチや OS のアップデートは製造メーカーによりリリース時期が異なる。ハードウェアの制約から OS のバージョンアップができず、脆弱性が修正されない可能性もありえる。このため、業務にスマートフォンを導入するためには導入している端末メーカーから出される脆弱性情報の収集を定期的に実施し、脆弱性修正パッチを確実に導入することが必要である。また、万が一を考え、前述の課題 1～3 の対策を導入することが望ましいと言える。

スマートフォンによる利便性・生産性の向上は、企業としては無視できないものになってきている。このため、セキュリティ対策の有無に関わらず、今後もますます業務で利用されていくと考える。セキュリティを厳しくしすぎるとスマートフォンの良さである利便

[17] ソーシャルメディアポリシーが各社で作成されつつある
http://web-tan.forum.impressrd.jp/e/2010/05/25/8041

性や生産性が生かせなくなってしまう。このようなことから企業ではスマートフォン利用におけるセキュリティと利便性のバランスを考慮したセキュリティポリシーを策定することが必須となる。また、業務でスマートフォンを使わないとしても、個人利用のスマートフォンがセキュリティ上の脅威にならないようにするためにも、セキュリティポリシーではスマートフォンの利用について記述をすると共に、従業員に対してもセキュリティ教育をすることが必須である。しかし、ガバナンスを効率よく実施するためには業務利用するスマートフォンはやはり会社支給のものが望ましいと言える。スマートフォンを企業で利用するためのポリシーや運用環境整備に関しては、日本スマートフォンセキュリティフォーラム(JSSEC)で作成したガイドラインが参考になる[18]。

3.3 非常時を考慮したセキュリティ対策の考え方

非常時を考慮したセキュリティ対策として、

・非常時の機器流失や機能停止を考慮したセキュリティポリシーの見直し

・被災地域のインフラが壊滅的な打撃を受けることを考慮した BCP の見直し

が必要である。

（1）課題１：セキュリティポリシーの見直し

機密性・完全性・可用性を確保する物理セキュリティ・情報セキュリティの規定は、セキュリティポリシーに記載される。今回の東日本大震災のような非常時を考慮した場合、セキュリティポリシーに以下 3 点の考慮が新たに必要となる。

緊急時における対策緩和・代替策への切替が主な観点であるが、対応範囲をどこまでとするか、どの段階で・どう戻すのかといった検討も重要である。

1) 機器流失を考慮したバックアップやセキュリティ対策

東日本大震災では、システムが津波で流されるといった事態も多々発生した。データを格納する機器が破損した場合だけでなく、流失した場合の影響を考慮した規定の見直しが必要と考えられる。

機器流失の際に情報の喪失が許容されない場合は、クラウド環境等も活用したリモートバックアップ対策を必須とするだけでなく、機器流失の際に情報漏えいが許容されない場合はデータの暗号化を行う必要がある。

さらに、今回の震災では、バックアップから実際にデータを復旧させることが難しかった場合も多く見受けられた。システム復旧方法についても、事前に十分に検証しておくべ

[18] 「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」
http://www.jssec.org/dl/guidelines2011_v1.0.pdf

きである。また、システム復旧を容易に行えるという観点でのアプリケーションのあり方・カスタマイズ範囲のあり方等も検討しておくべきであろう。

2) 代替策の規定

停電等で入退室管理システムなどの各種セキュリティシステムが機能しなくなった場合も考慮した規定の見直しや代替策の検討が必要である。入退室管理システムの例では、情報の重要性によっては警備員でカバーする等の代替策である。

従来より、短期間の停電対策は検討されているが、停電が長期間にわたる場合や計画停電も含めた観点での対応の検討・見直しが、新たに必要である。

3) 制限事項の非常時における解除

企業インフラが機能喪失した場合にも事業継続性を確保するため、「民間クラウド環境の利用」や「個人 PC 端末利用」等、通常は機密性の観点から制限される事項でも許容する必要がある。

また、今回の東日本大震災では、在宅勤務を認めるケースも多々見受けられた。「在宅勤務の許容」、「在宅勤務の環境整備」といった観点での見直しも必要と考えられる。

（2）課題２：BCP の見直し

非常時の際にも、BCP を迅速に発動し、BCP が十分に機能できるようにするために、以下 3 点の考慮が必要となる。

1) プライオリティ、目標復旧期間の明確化

BCP 策定においては、影響度の評価（重要業務の決定、目標復旧期間・目標復旧レベルの設定）を予め決定しておくことが重要である[19]が、その絞り込みが適切になされていないために、今回の震災時に BCP がうまく機能しない場合もあった。

BCP が機能するためには、業務停止・データ消失がどこまで許容できるのか、事業内容・事業環境を踏まえ、予め個々の業務について評価し、プライオリティ（どの業務から）、RTO（どのくらいの期間で復旧させるかの目標）を見直すことが重要である。

2) BCP の対象範囲の見直し

今回の震災では、従来の災害と比べ、インフラ機能低下期間の長期化、サプライチェーンの影響範囲の広範さなどのため、本来の企業活動の機能回復には一企業の機能回復だけでは困難となった場合も多く見られた。

BCP 見直しの際、事業継続に関わる範囲として、自社のみでなく、取引先や、場合によ

[19]「IT サービス継続ガイドライン」経済産業省（平成 20 年 9 月）
http://www.meti.go.jp/policy/netsecurity/downloadfiles/itsc_gl.pdf

っては利用者まで含めた広い範囲で見直すことも必要である。

3) 迅速な BCP 発動のための対策

安否確認・被害状況の把握に時間がかかったり BCP 関連資料が喪失したために、そもそも BCP の発動自体が速やかに行えなかった場合も見受けられている。

BCP を適切に発動するためには、BCP 発動権限の現地への委譲、本社・支社・現場レベル等の BCP の階層化、BCP 関連資料へのアクセス手段の確保、といった観点での見直しが必要であり、さらに、混乱なく BCP 発動を行うために、平常時から訓練し、対応力を強化しておくことが重要である。

また、システムやデータ自体を喪失した場合でも事業継続性を確保できるよう、バックアップサイトを確保し、移行方法も含め、事前に十分に検証しておくべきである。

4) 非常時のプライバシー保護

東日本大震災の直後では、過剰なプライバシー保護による非効率な業務を強いられることにより現場では様々な混乱が発生するなど、プライバシー保護に関する様々な問題が発生している。

一方で、非常時には、プライバシーよりも人命が優先されるため、東日本大震災の直後ではプライバシーが全くない状態も散見されたが、復興後のことまで考慮すると、望ましい状態とは言えない。

これは、非常時におけるプライバシー情報の利用規程を明確にしていなかったことなどが原因と考えられる。

従って、各組織の BCP では、非常時のプライバシー保護の考え方や、それに基づく非常時に利用するサービス（安否確認サービスや避難者管理システム等）を明確にするとともに、定期的な教育・訓練を行うことにより、非常時に混乱を生じないようにすることが重要となる。

3.4 標的型攻撃への技術的対策

3.4.1 標的型攻撃対策の考え方

2.2 節で述べた通り、標的型攻撃は、様々な手法を駆使し、セキュリティ対策の状況に合わせて、巧妙かつ執拗に行われる。このような攻撃に対抗するためには、個々のクライアントだけではなく、サーバ・ネットワーク等、システム全体での多層的な対策が必要となる。標的型攻撃対策の全体像を、表 3.4-1 に示す。

表 3.4-1　標的型攻撃対策の全体像[20]

No	項目	対策内容
1	ネットワークの入口と経路での防御	・ファイアウォール ・最新のウイルス対策ソフト (ネットワーク・サーバ・クライアント) ・侵入検知システム／防止システム ・通信路の暗号化 (Virtual Private Network などの利用) ・ネットワーク構造／設計 (重要なサーバに対するルート制御)
2	脆弱性対策	・OS やサーバソフトウェアの定期的な脆弱性診断 ・ウェブサイトで使用している OS やサーバソフトウェアに関する脆弱性情報の時期を逸しない収集とパッチの反映 ・ウェブアプリケーションへの脆弱性の作り込みの回避 ・ウェブアプリケーションの定期的な脆弱性診断 ・ウェブアプリケーションファイアウォール(WAF)
3	標的型攻撃ルートでの対策	・スパムフィルター／URL フィルター ・外部メディア利用規則、強制利用抑止
4	ウイルス活動の阻害および抑止(出口対策)	・端末間、他部署間のネットワーク通信の制限 (ウイルスの組織内蔓延抑止) ・組織の端末からの外部通信はプロキシを経由させる等の経路制御 ・組織内ネットワーク量の監視(異常さを早期に検知しウイルスの蔓延を早期に発見) ・知財等のある重要サーバはインターネットから隔離
5	アクセス制御	・ユーザ認証 ・アクセスするプログラムの特定(ホワイトリスト化)
6	情報の暗号化	・暗号／暗号鍵管理
7	システム監視、ログ分析	・ネットワークログ取得・分析 ・サーバログ取得・分析 ・アクセスログの監査(DB 監査ツール等)

[20]「標的型攻撃/新しいタイプの攻撃の実態と対策」（独立行政法人情報処理推進機構）
http://www.ipa.go.jp/security/J-CSIP/documents/presentation2.pdf

8	管理統制およびコンテンジェンシープラン	・セキュリティポリシー ・海外を含むグループ会社間でのセキュリティガバナンス ・危機対応体制の整備

ここであげられている対策のうち、ファイアウォールやウイルス対策など、外部からの攻撃をインターネットの入口で防ぐ対策の導入は進んでいる。しかし、標的型攻撃ではゼロデイの脆弱性が狙われたり、対策ソフトで検知できないウイルスを使用されたりする場合があり、ウイルス感染等の被害を完全に防ぐことは困難である。

従って、仮にウイルスに感染したとしても重要な情報を窃取されないため、No.4 の出口対策が重要となる。

3.4.2 出口対策

ウイルスは、自身の状態やどのような情報が存在するかなどを、攻撃者に対し通知しようと外部と通信を行う。このような外部への通信を検知し、止めることが出口対策である。つまり、出口対策とは、標的型攻撃により、ウイルス等に感染し内部システムに侵入されたとしても、重要情報を外部に持ち出させないようにするというセキュリティ対策である。出口対策については、IPA から発行されているガイド[21]が参考になる。ガイドに記載されている出口対策について、表 3.4-2 に示す。

表 3.4-2　出口対策

No	対策	実装手法
1	サービス通信経路設計	1. ファイアウォールの外向き通信の遮断ルール設定 2. ファイアウォールの遮断ログ監視
2	ブラウザ通信パターンを模倣する http 通信検知機能の設計	http メソッド利用バックドア通信の遮断
3	RAT[22] の内部 proxy 通信(CONNECT 接続)の検知遮断設計	RAT の CONNECT 確立通信の特徴を利用した内部 proxy ログでの監視
4	最重要部のインターネット直接接続の分離設計	最重要部がインターネットへ直接接続しないように VLAN 等で設計

[21] 「「新しいタイプの攻撃」の対策に向けた設計・運用ガイド」
http://www.ipa.go.jp/security/vuln/newattack.html

[22] Remote Access Trojan リモートアクセス型トロイの木馬

5	重要攻撃目標サーバの防護	1. AD[23]を管理する管理セグメントを防護する 2. 利用者から見える AD のサービスに対するパッチ当て
6	SW 等での VLAN ネットワーク分離設計	利用者セグメントと管理セグメントを分離設計する等
7	容量負荷監視による感染活動の検出	スイッチ等の負荷やログ容量等における異常検知を行い、セキュリティ部門と連携する
8	P2P 到達範囲の限定設計	No.4、6 の対策に加え、不要な RPC 通信の排除を目的としたネットワーク設計

[23] Active Directory

第4章　今後の IT 活用の方向

第 3 章で記述されているように、クラウドサービスとスマートフォン利用に必要なセキュリティ対策が適用されることによって、これらをセキュリティ対策そのものに活用してゆくことが可能になる。

このことにより、これまで大企業でしか実施できなかったようなセキュリティ対策をより多くの企業に適用することが可能となり、あわせて構築・展開費用を低減することが期待される。クラウドサービスとスマートフォンによって利用可能になると考えられるセキュリティ施策には次のようなものがある。

4.1 セキュリティ教育・訓練

従業員へのセキュリティ教育は企業が実施すべき施策の基本であり、常に新しい脅威への対応も含めて定期的に実施することが必要である。常に出現する新たな脅威への対峙方法については、個々の企業が教材を作成して展開するよりも、スマートフォンで学習可能なクラウドサービスとしてセキュリティ教育や対応訓練を実施することによって、最新の情報をタイムリーに教育し訓練を実施することができる。特に、サイバー攻撃における企業への攻撃型メールへの対策などにおいては、ユーザ教育として実施すべき内容が多く、学習や訓練によって備えることは、結果として企業のセキュリティ耐性を高める上で有効となると思われる。

4.2 脆弱性検出・回避

従業員へのセキュリティ教育は、企業におけるセキュリティ対策の基本施策であるが、一方で教育による脅威への対応には限界がある。そのため、情報セキュリティ対策の標準化と自動化を実現するための試みが進められている。特に、米国 NIST が開発したセキュリティ設定共通化手順「SCAP： Security Content Automation Protocol」は、下記 6 つの標準仕様書から構成されている。

- 脆弱性を識別するための CVE（共通脆弱性識別子）
- セキュリティ設定を識別するための CCE（共通セキュリティ設定一覧）
- 製品を識別するための CPE（C 共通プラットフォーム一覧）
- 脆弱性の深刻度を評価するための CVSS（共通脆弱性評価システム）
- チェックリスト記述のための XCCDF（セキュリティ設定チェックリスト記述形式）
- 脆弱性やセキュリティ設定をチェックするための OVAL（セキュリティ検査言語）

これらについては、IPA から活用事例が紹介され[24]、セキュリティ対策の重要技術として認識が高まっている。この脆弱性検出・回避の施策を構築する際に、クライアントやサーバに搭載するセキュリティエージェントが脆弱性を自動検出するクラウドサービスと連携して検疫システムを構成したり、脆弱性検出時の警告をスマートフォンに通知するなど、セキュリティ対策を施したクラウドサービスやスマートフォンを活用することにより、より広く利用可能な対策として普及してゆくことが予想される。

4.3 BCP 支援

BCP 支援に有効とされる IT 活用は、「グローバルなバックアップサイトの確保」および「リモートオフィス環境の整備」ということが明らかとなった。「グローバルなバックアップサイトの確保」の実現に関して、技術面ではリストアを確実に実施するための施策が課題であり、制度面ではバックアップを行う際に関係する規制の確認などである。海外のサイトにバックアップするような場合、個人情報を出し入れする際の規制の有無など、サービス加入時に利用規約や関連する法律を確かめながら選択する必要がある。「リモートオフィス環境の整備」においては、非常時にも使用可能なシステムをセキュリティ対策済みのスマートフォンやクラウドサービス用いて構築し、常時利用するといった対応が考えられる。このような施策は、拠点が海外にある企業への ICT 環境構築などにも効果がある。

IT 活用以外にも、BCP への対策としては、想定外の事態に備えた教育や対応訓練が有効という評価結果が出ていることから、これらが汎用なサービスとして提供され、企業で活用されることは非常時への対策として有効であると考えられる。

[24] 「脆弱性対策の標準仕様 SCAP の仕組み」セミナー開催のお知らせ（独立行政法人情報処理推進機構）
http://www.ipa.go.jp/security/vuln/seminar/lab_semi_scap_2011_4.html

表 4.3-1　セキュリティ課題の解決による今後の IT 活用の方向

課題	セキュリティ教育	脆弱性検出・回避	BCP 支援
技術的な活用	■ 高度化する攻撃型メール等サイバー攻撃の迅速な分析と対応施策の展開 ■ 信頼のおけるコンテンツを保証する署名技術	■ SCAP 実装時のクラウドサービス、スマートフォン有効活用 ■ 脆弱性の自動回避に伴う、システム安定性の保証	■ バックアップされたデータのリストア作業の品質保証 ■ 定常稼働時と非常時のデータの互換性確保
運用・制度面の活用	■ 国の機関を中心としたセキュリティ専門家の育成 ■ 専門家同士が所属組織の制約を越えて協業可能な体制の構築	■ 国の機関による、脆弱性検出・回避自動化システムの検証機構および監査体制構築 ■ SCAP の国際標準化（X.1500 化）	■ 個人情報を消去したことを第三者が確認する等のプライバシー保護制度 ■ ヨーロッパでは、プライバシーコミッション制度有り

表 4.3-1 のように、クラウドサービスとスマートフォンを活用したセキュリティ施策の普及に伴い、これまでセキュリティ面の不安があって適用できなかった領域への IT 活用が促進されることが予想される。

おわりに

本年度の調査にて、企業における新たな IT 技術として注目され、実際に活用が進んでいるクラウドサービスとスマートフォンについて、セキュリティ上の課題と対策を検討した。また、災害時の BCP の対策の一つとして紹介した。

実際の災害の中で BCP の有効性とともに問題点も多く見つかっている。本報告書での指摘も項目としては既知のことであるが、実際の BCP 発動に際しての課題を確認し、BCP の見直しをするとともに、実効性を高めるための訓練をしていただきたい。

一方でサイバー攻撃は、ウイルス対策といった従来のセキュリティ対策では対処できない新たな脅威に変化しており、出口対策と従業員への教育訓練の重要性を指摘した。官民共同の研究成果を企業に素早く展開していく必要性がある。

今後の IT 活用の方向性として、クラウドサービスとスマートフォンを活用したセキュリティ対策を提案した。解決しなければならない課題はあるが、段階的に実現することで JEITA 会員企業のみならず多くの企業において、変化する IT 環境をより安心・安全に活用した企業活動を行い、合わせて情報セキュリティ産業が発展していくことを期待する。

報告書

企業における新たなIT活用の方向性と情報セキュリティに関する調査

2012年2月24日

株式会社三菱総合研究所
情報通信政策研究本部　クラウドセキュリティグループ

目次

0．1 調査背景と目的

■ 調査の背景

- 企業の経済活動のグローバル化やサプライチェーンの高度化・複雑化等、ビジネスにおける環境が大きく変化する中、クラウド等の新たなITの活用やiPadやスマートフォン等新たな端末の導入と共に、企業における情報セキュリティの新たな脅威も刻々と変化している。特に情報保護については、外部からの攻撃や標的型メール等の脅威の広がりに加え、内部における情報管理も重要になっている。
- また、3.11以降、多くの企業においてリスクマネジメントに関する再検討がなされているところであり、脅威に対するリスクの評価と、それに伴う対策についても順次見直しがなされることと考えられる。さらには、夏の電力需要の増加に伴う計画停電等の対応等に迫られることにより、業務継続のための新たなITの活用がなされることも予想される。

調査の目的

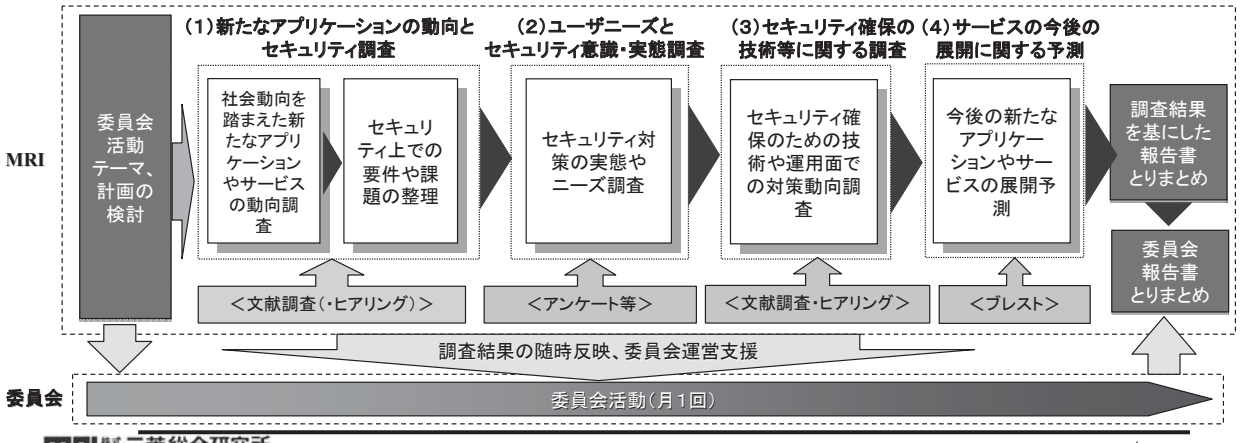
- 本調査は、企業のビジネス環境の変化とITや端末の変化、さらには3.11という環境変化を踏まえた新たな脅威の動向について現状を調査し、特に求められる情報セキュリティ面の課題について明確化する。そして、企業におけるニーズや対策状況を踏まえ、それらの課題を解決する技術や運用面も含めた対策の状況を調査し、今後の新たなサービスの展開とセキュリティ確保のあり方について検討を行う。具体的には、以下の項目を明らかにすることを目指す。
  - 新たなアプリケーションやサービスの動向
  - 求められるセキュリティ機能
  - ユーザのニーズと対策の状況
  - 課題を解決するセキュリティ技術等
  - 新たなアプリケーションやサービスの展開とセキュリティ確保のあり方

0．2 調査フロー

■ 調査フローは以下の通りとする。

（1）ビジネスのグローバル化やサプライチェーンの進化、あるいは3.11以降の環境変化等、近年求められる新たなアプリケーションやサービスの動向を調査し、その中で要求されるセキュリティ面の要件や課題を整理する。
（2）新たなアプリケーションやサービスに対するユーザの導入意向や導入実態、あるいはサービスに対するニーズを把握すると共に、セキュリティに関する意識と対策の実態を調査し、新たなアプリケーションの普及と共に顕在化することが予想されるセキュリティ面での課題を明確化する。
（3）（2）で明らかとなったセキュリティ面での課題を解決するための、新しい技術や運用面での対策等を調査する。
（4）セキュリティの課題解決により、今後、新たなアプリケーションやサービスがどのように社会展開するか予測を行う。
（5）以上の調査結果を基に、報告書のとりまとめを行う。

本調査のフロー

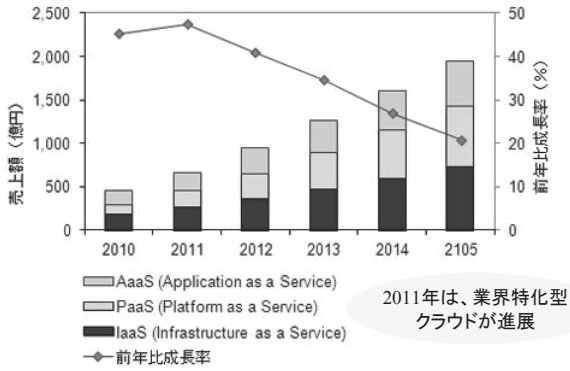


第1章　企業におけるIT活用の動向とセキュリティ課題

1．1　クラウド・コンピューティング　（1）市場動向①

■　2015年の国内クラウドサービス市場は1947億円。2010年は、特にコラボレーティブアプリケーション（電子メール、グループウェア、情報共有：Microsoft BPOS、Exchange Online、IBM LotusLive、Google Apps　等）や、ソーシャルアプリケーションの稼働基盤としての採用事例が多数。SaaSの牽引は中小企業。大企業での事例も徐々に出現。震災の影響は加味されていないが、震災もBCP、コミュニケーションの観点から追い風になる見込み。（IDC Japan, 2011年4月）
■　一方、成長率のピークは2011年と予測。2011年はクラウドベンダの淘汰が進む可能性も。
■　また、2009年の国内プライベートクラウド市場の市場規模は984億円。今後は500万円未満の小規模案件が増加する見込み。（IDC Japan, 2010年9月）

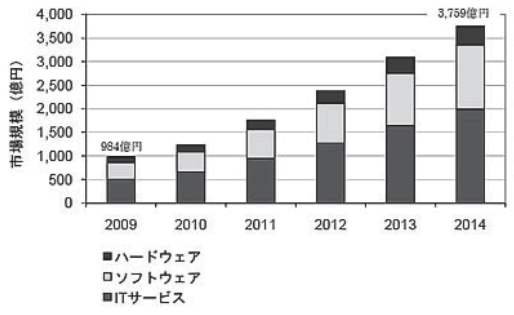
国内クラウドサービス市場



2011年は、業界特化型クラウドが進展

IDC Japan（2011年4月）
http://www.itmedia.co.jp/enterprise/articles/1104/04/news047.html
http://enterprisezine.jp/article/detail/3049

国内プライベートクラウド市場



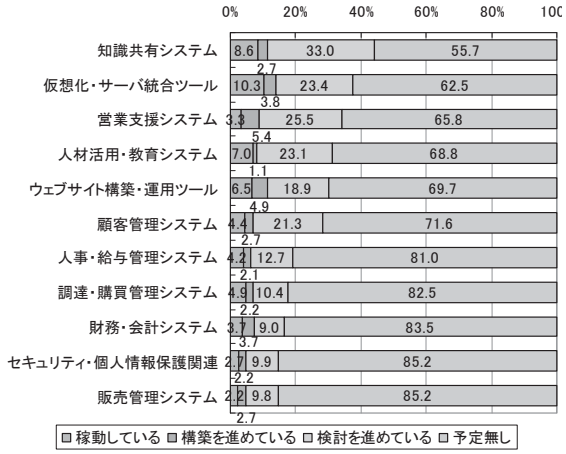
Note：2009年は実績値、2010年以降は予測

IDC Japan（2010年9月）
http://japan.zdnet.com/virtualization/analysis/20419377/

1．1 クラウド・コンピューティング （1）市場動向②

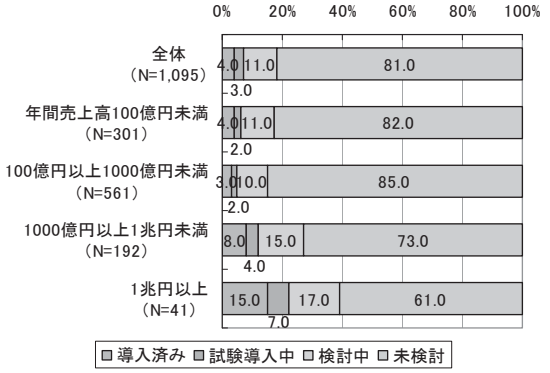
■ CIO調査によると、グループウェアなどの知識共有でクラウドが進むと予測される。
■ 情報システムユーザ協会の調査によると、ソーシャルメディアを導入している企業は7%に留まる（社内外を含む）。
ソーシャルメディアのメリットを理解しつつも、全社としての利用には現時点では二の足を踏む企業は多い。

クラウド導入の検討や構築・稼動の有無
（2011年版CIO調査）



日経情報ストラテジー（2011年6月）

企業におけるソーシャルメディアの導入検討状況



日経コンピュータ（2011年5月26日）

1．1 クラウド・コンピューティング （1）市場動向③

■ クラウドコンピューティングのアプリケーションとして組織内SNSの利用が進展している。
■ 企業向けソフトウェアベンダや大手クラウド事業者によるソーシャルメディア機能の取り込みが急速に進展。
- 大量の情報から自身に必要な情報を漏らさず得るためにソーシャルメディアが有効と判断
- 短期・不定期な協業支援に適している

■ 日本のIT市場の成長が年1%と予測される中、コラボレーションを含むCCC（Contents、Communication、Collaboration）分野が年14%以上の成長を続けるという予測も。（Gartner、2010年4月）
■ 日本企業による海外企業の買収、新興市場への進出等グローバル化や、スマートフォンやクラウドサービスの充実も背景。

ソフトウェア大手のソーシャルメディア対応製品の開発・強化方針

利用者の行動に関する情報を次々に表示

企業名	中核製品名	特徴	連携する自社製品やクラウドサービス
IBM	Vulcan	**アクティビティストリーム**の連携モジュールを提供し、様々な製品/サービスに組み込めるようにする	Lotus Notes，同Connections、他社のグループウェア、社外のクラウドサービスなど
SAP	Stream Work	アクティビティストリームを備え、SAPのアプリケーションに組み込んだり、社外のクラウドサービスと連携できるようにする	Sales OnDemand, Google Docs, Evernote, box など
オラクル	On Track	アクティビティストリームを備え、オラクルのアプリケーションやミドルウェアに組み込めるようにする	WebCenter Suite, CRM On Demand, Beehive など
セールスフォースドットコム	Chatter	Twitterに似たUIで、利用者の発言やデータオブジェクトなどの更新をリアルタイムに把握できる	Force.comで開発したSaaS全般
マイクロソフト	Office	SharePoint向けに開発したソーシャル機能を、他の自社製品にも組み込む	Exchange Server, Lync, Outlook など

日経コンピュータ（2011年5月26日）

エンタープライズ・ソーシャルテクノロジーの構成要素

ソーシャルグラフ：
友人、現在、過去の上司・部下といった人間関係・つながり
プロフィール：
自己紹介。写真、出身地、経歴、住所、所属部署などの基本情報を共有
コミュニティ：
同じ趣味・興味などによる集まり・サークル
ブログ：
日記・日報
マイクロブログ（ツイッター）：
ブログよりも短文で現在の状況を書き込むもの
ウィキ：
参加者全員が共同で編集できる用語集・マニュアルなど
タグ：
文書・動画などに対するしおり機能
アクティビティストリーム：
行動履歴。位置情報なども付加し、誰がどこで何をしたかを記録し、自分で確認したり、他者が閲覧できたりする

日経情報ストラテジー（2011年2月）

1．1 クラウド・コンピューティング （2）活用事例①

キリン
～ 全体のコスト削減を意識した業務システムの全面刷新 ～

システム概要:
・2015年を目処に業務システム基盤を全面刷新。「仮想化」と「オープン化」が柱。
・サーバ仮想化は約1000台のサーバのうちWindowsやLinuxが稼動しているもの。既に600台が仮想化、35台の物理サーバに集約済。
・仮想化ソフトはVmwareの「vSphere」と日本マイクロソフトの「Hyper-V」を利用。I/Oの負荷が小さい情報系システムを中心に。
・オープン化は、2012年半ばを目処にメインフレーム上の約20種類のアプリケーションをUNIXに移行。
・2015年頃は、仮想化や外部クラウド利用、ミドルウェアの刷新などを実施予定。

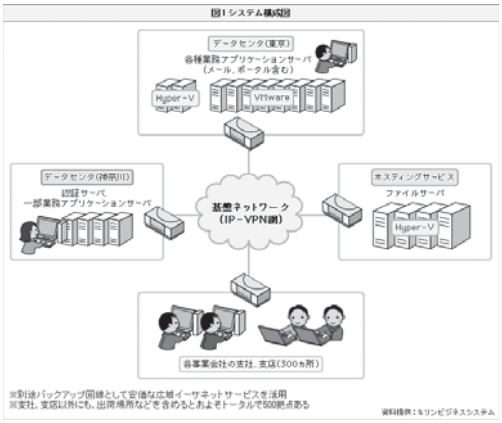
導入目的:
・長期経営構想「キリン・グループ・ビジョン2015」（売上高3兆円、営業利益率10%以上）の実現のために、グループ各社の事業を支えるITサービスをタイムリーかつ効率的に提供。

導入効果:
・データセンターの消費電力を2008年時点の660万kWから600万kWに削減。

構築のポイント:
全体最適化を意識。物理サーバのコストやソフトウェアライセンスなどを加味したうえで、固定資産やリースなどを織り交ぜながら全体でのコスト圧縮を常に考える。

おいしさを笑顔に KIRIN

構築後に気付いた点:
・ネットワークの負荷やI/O部分がパフォーマンスのボトルネックになる。（センタ内のストレージとサーバ間、ブレードサーバを含めたラック内） ユーザが体感するレベルには至っていないものの、明らかに数字として遅い。CPUに関する性能は十分満たされるが、ディスクのI/O部分がネックになりやすい。



1．1 クラウド・コンピューティング （2）活用事例②

リクルート
～ 投資対効果を重視した基盤システムのクラウド化 ～

システム概要:
・2011年6月までに自社Webサイト基盤システムをプライベートクラウドに移行。
・ストレージとネットワーク機器を複数のWebサイトで共有。負荷に応じて自動的にリソースを割当。（ストレージ容量が使われない、運用ノウハウが蓄積されない等の課題が存在）
・データセンターを4箇所から1箇所に集約。

導入目的:
・サーバ等の集中購買によるコスト抑制
・採用する製品の標準化・統一化による運用負荷の軽減
・仮想化技術の採用によるリソース使用率の向上

導入効果:
・従来、Webサイト毎に構築・運用していたシステムを統合することで、投資対効果を5倍に向上。（IT投資額/サイト閲覧数＝ページビュー単価を0.23円→0.046円に削減）
・Webサイトの収入源が広告掲載から口コミ等の新しい販促手法に移る中、収益あたりのページ単価は下がる傾向。同じ投資額でページ閲覧数が増えることは経営面でのメリットが大きい。

パナソニック
～ グローバルな業務標準化を目指した
基幹業務のパブリッククラウドの利用 ～

システム概要:
・2011年4月に間接材の調達システムを、2012年4月以降に基幹系である生産管理システムをOracleのSaaSに置き換え。
・パブリッククラウドを評価する全社統一のガイドラインを制定することで、基幹系を含めたシステムをクラウド化する道筋をつける。
・パブリッククラウド評価ガイドライン
ステップ1：データ特性とクラウド特性を評価
ステップ2：セキュリティとコンプライアンス等を評価
ステップ3：システム個別の要件（機能要件、性能、運用性、外部評価）に応じたSLAの締結
（費用対効果も判断）
・ガイドラインを満たすクラウドサービスは全社でリストを共有。リストは半年～1年おきにたな卸しを実施。

導入目的:
・世界中の拠点で同じサービスを利用可能にし、グローバルで業務を標準化。
・システム部門の負荷軽減。

導入効果:
ー
（OracleのSaaS利用時、ステップ3で「日本語による障害対応の初動が30分以内」というSLAを検討していたが、費用対効果が合わず締結を見送り）

1．1 クラウド・コンピューティング （2）活用事例③

ユーザー企業名	適用業務・システム	概要
野村不動産	Webサイトの システム基盤	キャンペーン用のWebサイト構築に、IDCフロンティアの「NOAHプラットフォームサービス」を採用した。キャンペーン時は通常の4倍のアクセスが見込まれるため、一時的なITリソースの強化が必要だったが、クラウドの活用でこの問題を解決した。（1月）
パナソニック	グループウェア	約30万人規模でIBMのコラボレーションサービス「IBM LotusLive」を採用した。グローバルのグループ全社、パートナーやサプライヤーなどで共同作業できる環境を構築。Web会議や人物検索、ファイル共有などを利用可能。（1月）
三菱重工業	化学物質管理	空調機器やカーエアコンなどの製品に含まれる化学物質情報を管理するシステムの構築に、NECのSaaS「ProChemist/CS」を採用。サプライチェーンにおける化学物質情報の管理、伝達作業の効率化を図る。（1月）
第一三共	企業間情報共有	新薬開発などの機密性の高い情報を企業間でやりとりする仕組みとして、米イントラリンク社が提供する「IntraLinks Exchanges」を導入。文書に応じて閲覧できる人を制限したり、ファイルの印刷やダウンロードを制限したりできるようにした。（1月）
アサヒビール	社内システムへの アクセス基盤	育児休職者とのコミュニケーションツール、出張者の業務支援ツールとして、社外から社内のネットワークにアクセスできる「SASTIKサービス」を導入した。USB型の認証キーを利用することで安全に社内のWebアプリケーションなどを利用できる。（2月）
全国銀行協会	Webサイトの システム基盤	新規のWebサイト立ち上げに際し、システム基盤としてソフトバンクテレコムのクラウドサービス「ホワイトクラウド」を採用。今後のコンテンツ拡充に備え、迅速にリソースを調達できる、運用コストを低減できるなどの理由から導入に踏み切った。（2月）
国立大学法人静岡大学	システム基盤	学生および教職員、約1万3000人が利用するシステムをクラウドに移行した。給与や会計などの基幹システムはプライベートクラウドを、ホームページやSNSなどはAmazon EC2などのパブリッククラウドを使い分けて運用する。（3月）
トップツアー	グループウェア	グーグルの「Google Apps」を導入し、営業支援システムを刷新した。渉外営業担当者の機動性や業務効率性が向上するように、携帯端末からシステムにアクセスできる点を考慮。社外から携帯端末を通じてメールやスケジュールを確認できるようにした。（3月）

1．1 クラウド・コンピューティング （2）活用事例④

中外製薬	コールセンター業務	セールスフォースの「Salesforce CRM」とNTTコミュニケーションズのコールセンター向けサービス「Customer Connect」を連携してシステムを構築した。これまで以上のコール件数に対応できるようになったほか、情報をフィードバックし、顧客対応力を強化した。（3月）
TOHOシネマズ	ギフトカード管理	映画館で利用可能なプリペイドカードの残高管理、履歴管理などに、富士通エフ・アイ・ビーのSaaSを利用。各映画館でカードの入出金処理や残高を管理する必要がなくなり、作業負荷を軽減する。カード情報を使ってプロモーションも可能。（3月）
協和発酵キリン	臨床試験データ管理	医療機関から新薬の臨床試験データを収集する機能をクラウド経由で利用する。新薬開発期間の短縮とコスト削減を図るのが狙い。サービスは、NTTデータの製薬業界向けとなる臨床試験データ管理システム「DATATRAK eClinical」を採用。（3月）
中央三井アセット信託銀行	確定拠出年金管理	確定拠出年金を管理する仕組みを、日本ユニシスのクラウドサービス「ICTホスティングサービス」より利用する。取り引き状況を照会したり、加入者の資産状況および運用利回り分布を表示したりできる。アプリケーション部分は日本ユニシスの「Benefit Keeper」を基に開発した。（4月）
損害保険ジャパン	CRM	損保ジャパンと代理店がリアルタイムでコミュニケーションを図ることを目的に「Salesforce Partner Portal」を導入した。顧客とのコンタクト履歴を共有し、保険金の支払い処理などで必要な各種情報を把握できるようにした。（4月）
ジヤトコ	CRM	自動車変換機などを扱う同社の国内営業部が、オラクル「Oracle CRM On Demand」を導入した。電気自動車の普及に向け、営業力を強化することが目的。情報の一元化により、営業担当者は商談に関連する情報を包括的に把握できる。（5月）
スターバックス コーヒー ジャパン	エネルギー消費量管理	約900店舗で使用する電気やガスの使用量を把握できるようにした。日立製作所の環境情報管理SaaS「EcoAssist-Enterprise-Light」を導入し、エネルギー使用量を計測する作業員の負荷を軽減。環境改善業務の効率化を支援する。（5月）
日本ケンタッキー・ フライド・チキン	商品の品質管理	食品の原材料情報の管理や流通履歴を把握するサービス「i-TRe」を導入。これまでは成分情報などを記した書類を仕入れ業者とやり取りしていたが、クラウド上で書類を管理。収集時間の短縮や情報をデータ化する手間をなくした。（7月）
ネットイヤーグループ	SNS	社内のナレッジ共有、コミュニケーションの活性化などを目的に社内SNS「SKIP」を導入。180人の社員間で利用する。社員同士が声をかけやすい環境を作り上げることで、顧客への提案の質向上を目指す。（8月）
カシオ計算機	間接材購買	グループ企業19社の間接材の購買、調達業務を支援するシステムとして、富士通の購買・調達SaaS「ProcureMART間接材調達業務支援サービス」を採用した。取引先への見積もり、注文、検収などの業務を効率化するのが狙い。（8月）
千趣会	Webサイトの システム基盤など	ショッピングサイト「ベルメゾンネット」の基盤にIBMのクラウドサービスを導入した。キャンペーンなどによる一時的なアクセス集中に備え、システムの拡張性を考慮した。Webサーバーのほか、社内業務向けサーバーも含めて135台のサーバーを118個の仮想マシンに集約した。（8月）

1．1 クラウド・コンピューティング （2）活用事例⑤

Chatter（セールスフォース・ドットコム）

＜概要＞
・2011年1月、セールスフォース・ドットコムは、登録すれば誰でも無料で使える企業向けマイクロブログサービス「Chatter.com」を公開。
・公開時点で日本語対応も完了。
・従来まで、Chatterは、Saleseforce CRMユーザか、Salesforce CRMユーザが招待した同一企業内ユーザだけが利用可能。
・無料版でフォローできるのは、人とグループのみ。（ERPやデータベース、CRM等のアプリケーションや顧客名簿等のドキュメントファイルはフォロー不可）
・Chatterの専用クライアントはiOS版とWindows用デスクトップ版が用意。Andorid版も準備中。

＜機能＞
・ある資料に対するコメント、資料のアップロードや更新、等自身が関係する資料の更新等をいち早く知ることが可能。
・例えば、自身の営業先について、自身が知らなかった、その営業先と懇意な人間からアドバイスを受けながら商談が可能に。
・特定のプロジェクトに関係する人物がフォローをし合ってチャットで情報交換、プロジェクトに関係するデータやアプリケーションから、プッシュ形式で情報が提供、特定の顧客名をクリックして質問をつぶやくと、その顧客に詳しい社員からの回答を受け取ることができる等。

＜効果＞
・セールスフォース・ドットコムでは、2ヶ月間でトップのメールの量が25%削減。
・ネクスウェイ（BtoB間のFAX・メール配信システムやSEMサービス等を提供）。2011年4月からはChatterの全面利用を開始し、「面識がない営業マン同士がChatter上でノウハウ共有を始めた」「MVP賞を取った営業マンの表彰状をマネージャがChatter上にUPしたことで、全社的に評価されモチベーションが上がった」「営業マンが商談中に、他部署の過去営業担当者がChatter上でアドバイスした」等の効果があった。
・損保ジャパンでは、代理店も含め37万5000人で利用開始。保険契約手続きや保険金の支払処理がスムーズになり、より代理店との連携が密になった。

・IBM：企業向けTwitter「Project Vulcan」開発中
・マイクロソフト：Office Talkを開発中、社内で試験導入中
・Yammer：企業向けSNS。世界100万人超の利用者、8万の企業ユーザ
・SAP：コラボレーションツール「StreamWork」リリース

http://www.atmarkit.co.jp/news/201004/15/sf.html http://pc.watch.impress.co.jp/docs/column/mobile/20110210_426109.html
http://www.publickey1.jp/blog/10/chatter.html

1．1 クラウド・コンピューティング （2）活用事例⑥

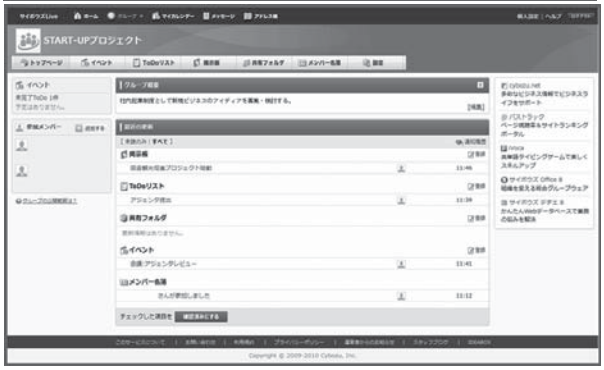
サイボウズLive（サイボウズ）

＜概要＞
・2010年10月一般公開
・グループウェア
・スケジュール管理、タスク管理
・無料版20人まで

＜機能＞
・サイボウズ社製品の補完用途を想定（アドホックな情報共有）
・利用者は自由にグループを設定し、自由にメンバーを招待。情報を投稿、共有する仕組みとして、スケジュール管理、タスク管理、掲示板などを提供。設定したグループ内のメンバー全員に自動的に公開される。投稿したデータは、掲示板などに蓄積。
・企業だけでなく、地域コミュニティ活動等にも利用できるよう、同一利用者がプロフィールを複数登録可能。

＜導入状況＞
・利用者数4万2,000人。2011年中に100万人を目指す。

※ なお、サイボウズは10月提供予定のPaaS「kintone」でもソーシャル機能を取り込む予定。

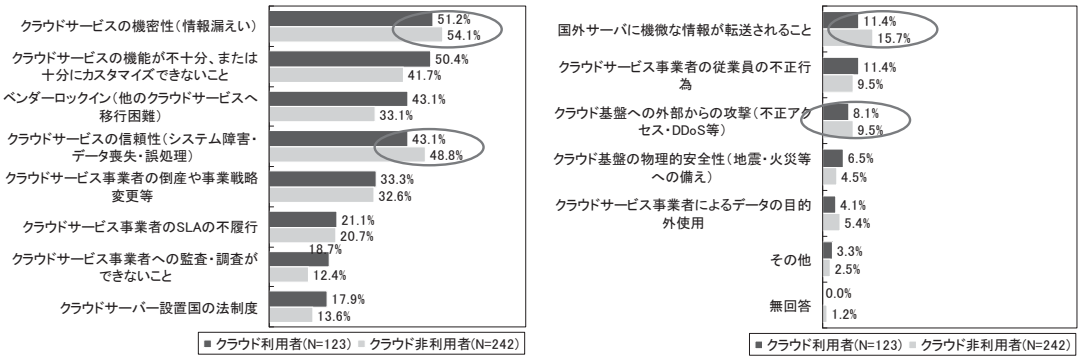


日経コンピュータ（2011年2月3日、5月26日）
http://technolog.jp/solution/cloud/3307

1．1 クラウド・コンピューティング （3）ユーザニーズ

■ 「クラウドコンピューティングに関するリスクマネジメント実態調査」（2010年12月）によると、主要な企業及び地方自治体365組織において、クラウド利用の是非を判断する上で懸念するリスクは、「クラウドサービスの機密性（情報漏えい）」が最も多い。次いで「クラウドサービスの信頼性」「クラウドサービスの機能が不十分、または十分にカスタマイズできないこと」となっている。
■ 機密性や信頼性等、セキュリティに関わる項目が上位2項目となっているが、外部からの攻撃や事業者の不正行為等、犯罪に関わる項目の懸念は少ない。
■ 非利用者のほうが懸念と感じる率がやや高く、実際の利用によってセキュリティに関わる懸念は下がると考えられる。

クラウド利用の是非を判断する上で懸念するリスク（3つまで）
利用者／非利用者別



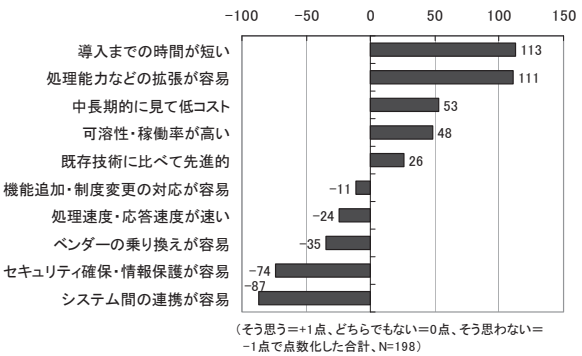
資料：「クラウド対応型セキュリティ対策技術の研究開発」（総務省、2010年度）

1．1 クラウド・コンピューティング （4）セキュリティ課題①

クラウド利用時のセキュリティ課題

・大企業におけるセキュリティ確保については懸念も未だ存在している。
・中小企業においては、クラウド非利用者の方がセキュリティ課題を感じている。
・新しい課題として以下の点が指摘されている。
- クラウド移行期における物理サーバ、仮想サーバ、クラウドサービス混在環境のセキュリティ確保
（管理できない仮想化サーバ、仮想マシン間での攻撃、セキュリティ境界線の消失　等）
- リアルタイム、高速、大容量のデータの安全な処理
- スーパーバイザのなりすまし防止

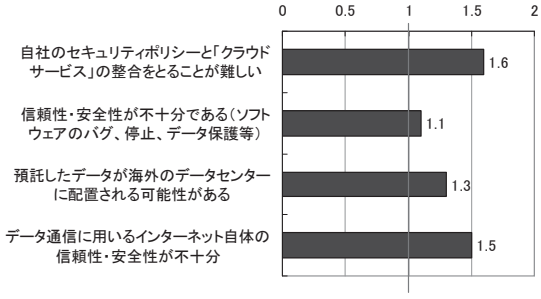
クラウドコンピューティングに対してCIOが持つイメージ



（そう思う＝+1点、どちらでもない＝0点、そう思わない＝−1点で点数化した合計、N=198）

「2011年版CIO調査」 日経情報ストラテジー（2011年6月号）

中小企業におけるクラウド非利用者における
セキュリティ課題の深刻度
（利用者の深刻度を1とした場合の比）



「中小企業等におけるクラウドの利用に関する実態調査」
情報処理推進機構（2011年3月）

1．1 クラウド・コンピューティング （3）セキュリティ課題②

セキュリティ課題

■ クラウドのリスクについて、専門家・利用者ともに重要と判断されているのは、クラウドの機能に関する懸念と、ベンダーロックインである。次いで、SLAや法制度に関するリスクである。しかし、専門家には重視されていないものの、ユーザ側の重要性が高いのは、機密性、信頼性、事業者の業務継続など、セキュリティに関わるリスクである。
■ セキュリティに関わるリスクの低減によって、クラウドの普及が進展するものと考えられる。

	専門的見地から 比較的重要性が高いリスク	専門的見地から 比較的重要性が低いリスク
ユーザにとって 重要性が高い リスク	■不十分な機能・カスタマイズ性[R1.15⑥, R2.6⑥] ■ベンダーロックイン[R1.11⑥] ■SLAに関するリスク[R1.4⑥, R1.9⑦, R1.13⑥]	■機密性に関するリスク[R2.10④, R2.2④, R2.13④] ■信頼性に関するリスク[R1.16④, R2.1④, R4.2④, R4.4④] ■事業者戦略[R1.5④]
ユーザにとって 重要性が低い リスク	■法制度に関するリスク[R3.1⑦] ■監査に関するリスク [R1.8⑦, R1.13⑥]	■その他のリスク

■[R1.3⑦, R1.6⑧, R1.7⑥, R1.10⑥, R1.12⑥, R2.7⑥, R2.18⑥]

丸数字はリスク評価結果（点数）

16 資料：「クラウド対応型セキュリティ対策技術の研究開発」（総務省、2010年度）

1．1 クラウド・コンピューティング （3）セキュリティ課題③

■ クラウド・コンピューティングにおけるセキュリティ課題を法的視点から見ると、データの所在が把握できない問題、トラブル発生時の責任分解点が曖昧である点、サービスの多様化、複雑化に伴う責任の所在の曖昧化等の問題が挙げられる。

テーマ	法的論点	セキュリティ課題
クラウドコンピューティングのビジネス利用（現在）	データがどこにあるか把握できない	・真の事故原因はIaaSの事業者しか知らないことになるので、SaaSの事業者すら鵜呑みにせざるを得ない。また、免責規定が多い。日本の裁判所は免責規定を厳しく解釈して適応範囲を狭めているが、外国はそうではない。
	トラブル発生時の責任分解点が曖昧	・データの所在がその時々で変化し、スケーラビリティが一つの特徴であることから、責任分解点の前にどこの強行法規が適用されるかすらわからない。 ・法的には、債務者側／債権者側で切り分けるが、下請けを使っていた場合は、親がいったん責任を持ち、後は下請けと中で調整するのが日本の発想である。 ・落ち度は、PL法（ソフトウェアに対して責任は認めないが、組込みは機器の一部なので認める）もしくは過失責任で問われる。
クラウドコンピューティングのビジネス利用（今後）	サービスの多様化、複雑化に伴う責任の所在のあいまい化	・ユーザに自己責任を取らせるためには、ある程度情報公開と選択性があり、ユーザが選択した製品をインストールした責任があると言わざるを得ないのではないか。

1．1 クラウド・コンピューティング （3）セキュリティ課題④

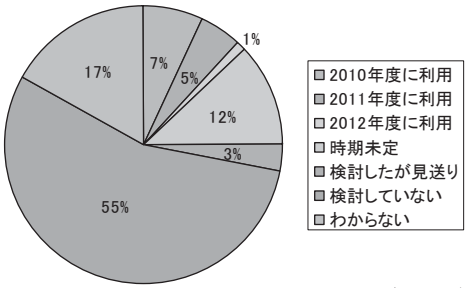
・ニーズと提供側のギャップに新しいセキュリティニーズがあるのではないか。
・セキュリティには、何を守るべきかのコミュニティにおけるコンセンサスが重要である。守るべきものをきちんと定義すべきである。
・守るべきものの定義、それに合わせたセキュリティレベル、破られることを前提としたセキュリティ対策をセットで考えるべきである。

テーマ	ITユーザの利用動向	セキュリティ課題
新しいビジネスモデルへの対応	・韓国のテレビメーカーは、端末を無料で配り、録画した番組を宿泊先や自宅のどこでも観られるなど、新しいビジネスモデルを作ろうとしている。	（新しいビジネスモデルに応じて、コンテンツ管理等の課題が発生する）
セキュリティ・エージェントの必要性	・米国では、セキュリティインシデントも含め、事業の全てのリスクに対して包括的に保険をかける。セキュリティインシデントで記者会見等行う際には、責任をかぶって説明するエージェント（保険会社）が存在する。	・日本では、セキュリティ事象の発生時、セキュリティコンサルではなくユーザ本体の責任となる。 （→ セキュリティエージェント、第三者のお墨付きのニーズがあるのでは）
守れないことが前提のセキュリティ	・クラウドにもメリット・デメリットがあるが、自身のセキュリティの状況や必要な対策をわからないまま、心配と言う声が多い。	・盗られることが前提のセキュリティ対策が必要である。 （→ 被害範囲が限定されるGoogleの分散ファイルシステム等）
	・ベンダに囲い込まれているため、システム間連携が容易ではない。ブラックボックスが存在する。	・全てを知っている技術で対応しようとすると、パッチが出ても迅速にあてられない。
ログ解析	・キーワードやキャッシュログを用いて、ユーザの位置や嗜好を特定し、それに応じたサービス提供が可能となっている。これは、個人名を特定するものではなく、またログの解析であるため、通信の秘密侵害にもあたらない。	・個人情報と引き換えにパーソナライズされた情報が得られることをメリットと見るか、デメリットと見るかは個人化された情報に依存する。ユーザに対して、説明を行うことが必要となる。

1．2 スマートフォン （1）市場動向①

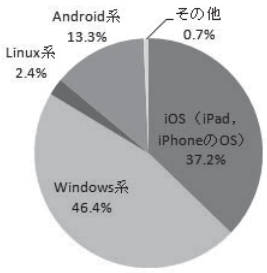
■ スマートフォンは企業の1/4が利用（2010年11月）。費用対効果の明確化と通信費用のマネジメントが解決課題。
■ 今後スマートフォンの新規・追加導入予定のある企業の利用予定のOSは、「Windows系」が46.4%でトップ、iPhoneの「iOS」が37.2%で続く。「Android」は13.3%で3位。中小企業では「iOS」の比率が高い傾向にあり、大企業では「Windows系」に対する意向が強い。
■ 端末の選択肢が増加し（iPhone4、Android搭載スマートフォンのラインナップ充実、iPad/iPad2、Galaxy TAB）、業務アプリケーションの増加（Salesforce、SAP等）や自社開発環境の整備等が進展してきたことから、2011年は企業でのスマートフォン/タブレット端末の利用がさらに進展すると予測。

スマートフォン利用状況



（N=1,643）

利用予定の端末



2010年(n=422)

利用予定のOS

モバイルコンピューティング推進コンソーシアム（MCPC）
「スマートフォン・タブレットPC最新市場予測」（2010/11）

1．2 スマートフォン （1）市場動向②

調査名：「業務用スマートフォンの導入状況」に関するアンケート
実施主体：キーマンズネット（IT担当者のための情報サイト）
実施期間：2011年3月2日～ 2011年3月9日
有効回答数：895件

業務用スマートフォンの導入状況
・導入済みは7.7%、導入検討中は36.9%で全体の44.6%、「導入を検討していない」のは55.3%となる。導入を検討するのは、大企業より中堅／中小企業の方が高い割合。

業務用スマートフォンの導入のきっかけ
・「導入済み」の1位は「業界での業務用スマートフォンの導入が進んでいるので、自社でも積極的に取り入れた」が50.7%。
・「導入予定」では、個人利用のスマートフォンが急増していることを受けて、会社としても導入を決めるケースが増えてきている。

業務用スマートフォンの導入単位
・「導入済み」の1位は「一部の個人（役員など、限られた役職者のみ）」で55.9%、2位は「部門導入（営業部門のみなど、一部の部署）」で26.5%、3位は「全社導入」で13.2%、4位は「支店導入（本社、一部の支社での導入など）」で1.5%と続いた。・「導入予定」の1位は「部門導入（営業部門のみなど、一部の部署）」で53.6%、2位は「一部の個人（役員など、限られた役職者のみ）」で30.3%、3位は「全社導入」で5.5%、4位は「支店導入（本社、一部の支社での導入など）」で3.0%と続いた。

図1-1 導入状況 n=895

		業務用スマートフォンを既に導入済みである	業務用スマートフォンの導入を検討している	業務用スマートフォンに興味があり、いずれは検討する	興味があるが検討はしない	今のところ関心がない
全体	n=895	7.7%	9.9%	27.0%	35.0%	20.3%
従業員規模 100名以下	n=251	8.8%	5.2%	29.9%	37.5%	18.7%
従業員規模 101～1000名以下	n=360	6.7%	10.3%	31.9%	31.4%	19.7%
従業員規模 1001名以上	n=284	8.1%	13.7%	18.3%	37.3%	22.5%
業種 IT製品関連業	n=221	9.0%	9.5%	21.3%	37.1%	23.1%
業種 (IT関連外)製造業	n=331	5.7%	13.9%	23.3%	38.1%	19.0%
業種 流通・サービス業全般	n=240	9.6%	7.9%	35.8%	30.8%	15.8%
業種 その他業種	n=103	6.8%	2.9%	31.1%	30.1%	29.1%

図1-2 導入のきっかけ

導入済み n=69

	業界での業務用スマートフォン導入が進んでいるので自社でも積極的に取り入れた	社員からの業務用スマートフォン利用の要望が高まったため会社として導入を決めた	個人利用のスマートフォンを業務利用することでセキュリティリスクが高まるため会社として導入を決めた	その他
全体 n=69	50.7%	31.9%	2.9%	23.2%

導入予定 n=320

	業界での業務用スマートフォン導入が進んでいるので自社でも積極的に取り入れた	社員からの業務用スマートフォン利用の要望が高まったため会社として導入を決めた	個人利用のスマートフォンを業務利用することでセキュリティリスクが高まるため会社として導入を決めた	その他
全体 n=320	35.9%	24.1%	23.7%	29.7%

1．2 スマートフォン （1）市場動向③

業務用スマートフォンの端末
・「導入済み」「導入予定」ともにiPhoneの割合が高い。
・導入予定では、GALAXY Sの人気が高まっている。

業務用スマートフォンの利用目的
・「導入済み」の1位は「社内コミュニケーションの円滑化」で69.6%、2位は「営業・渉外の効率化」で46.4%、3位は「業務時間の短縮」で31.9%、4位は「ファイル・データの共有」で14.5%、5位は「全体としてのコスト削減」で11.6%と続いた。
・「導入予定」では1位と2位が入れ替わって「営業・渉外の効率化」が1位となっており、単なるコミュニケーションツールから、営業活動での活用が進んでいくと考えられる。

図1-3 業務用スマートフォンの端末

導入済み n=69

	iPhoneシリーズの端末（アップルジャパン）	BlackBerryシリーズの端末（リサーチ・イン・モーション・ジャパン）	その他の端末（東芝、シャープなど）	GALAXY Sシリーズの端末（サムスン電子）	Xperiaシリーズの端末（ソニー・エリクソン・モバイルコミュニケーションズ）	Desireシリーズの端末（HTC Nippon）
全体 n=69	62.3%	26.1%	17.4%	13.0%	8.7%	2.9%

導入予定 n=326

	iPhoneシリーズの端末（アップルジャパン）	GALAXY Sシリーズの端末（サムスン電子）	Xperiaシリーズの端末（ソニー・エリクソン・モバイルコミュニケーションズ）	その他の端末（東芝、シャープなど）	Desireシリーズの端末（HTC Nippon）	BlackBerryシリーズの端末（リサーチ・イン・モーション・ジャパン）
全体 n=326	59.5%	41.4%	40.2%	32.8%	14.1%	9.2%

図2-1 利用目的

導入済み n=69

	社内コミュニケーションの円滑化	営業・渉外の効率化	業務時間の短縮	ファイル・データの共有	全体としてのコスト削減	セキュリティ向上	調査・検品・検針業務の効率化	建設・工事業務の効率化	店舗管理・在庫管理業務の効率化	運送・配送業務の効率化	その他
全体 n=69	69.6%	46.4%	31.9%	14.5%	11.6%	5.8%	4.3%	1.4%	1.4%	1.4%	13.0%

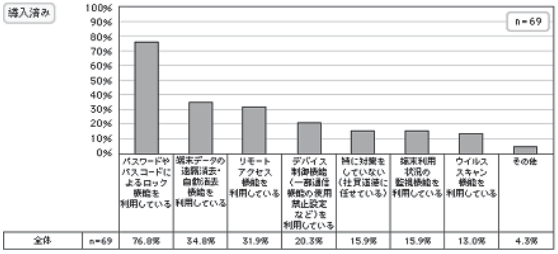
導入予定 n=330

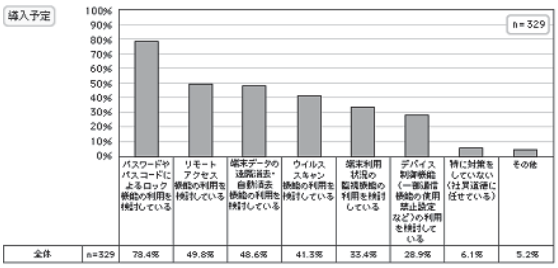
	営業・渉外の効率化	社内コミュニケーションの円滑化	業務時間の短縮	ファイル・データの共有	全体としてのコスト削減	セキュリティ向上	店舗管理・在庫管理業務の効率化	調査・検品・検針業務の効率化	建設・工事業務の効率化	運送・配送業務の効率化	その他
全体 n=330	65.8%	59.7%	33.6%	32.4%	20.3%	12.4%	7.3%	6.1%	5.5%	5.5%	5.8%

1．2 スマートフォン （1）市場動向④

業務用スマートフォンのセキュリティ対策状況
・「導入済み」の1位は「パスワードやパスコードによるロック機能を利用している」で76.8%。
・「導入予定」では「特に対策をしていない（社員道徳に任せている）」と回答した割合が減少しており、企業としてスマートフォンのセキュリティ意識が高まってきているようだ。

図3 セキュリティ対策状況





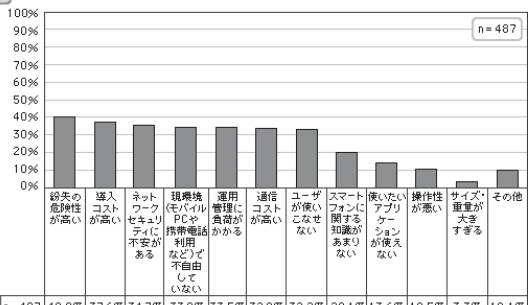
個人スマートフォンの業務利用
・業務用スマートフォンの「導入済み」では「業務での個人利用を認めていない」が58.0%、「セキュリティ対策を施した上で、個人利用を認めている」が37.7%、「その他」が4.3%であった。一方、「導入予定」では「業務での個人利用を認めていない」が67.5%、「セキュリティ対策を施した上で、個人利用を認めている」が20.4%、「その他」が12.2%であった。「導入済み」「導入予定」ともに、個人用スマートフォンの業務利用を認めていない企業が過半数を超えている。また、「その他」の中には「社内規定が取り決められていない」といった回答が含まれており、個人でスマートフォンを持つユーザが増加している一方で、企業でのスマートフォン利用に対する規定整備が遅れているケースもあるようだ。

業務用スマートフォンの満足度
・、「とても満足している」が17.6%、「まあ満足している」が45.6%、「やや不満がある」が26.5%、「とても不満がある」が10.3%。
・満足の理由は、「Eメール、スケジュールをリアルタイムで確認できる」等、ユーザ利便性の向上や業務の効率化、そしてビジネスの機会損失防止にも役立っているという意見が多かった。
・不満の理由は、「既存のWindows環境との不適合（ウイルス対策ソフトやその他の社内標準ソフト、機器）がある」や「セキュリティ上の理由で機能をかなり制限せざるを得ない。多機能なスマートフォンの本来の利点を十分にいかせない。」といった声が挙がった。

1．2 スマートフォン （1）市場動向⑤

業務用スマートフォンを導入しない理由
・1位は「紛失の危険性が高い」で40.0%、2位は「導入コストが高い」で37.6%、3位は「ネットワークセキュリティに不安がある」で34.7%、4位は「現環境（モバイルPCや携帯電話利用など）で不自由していない」で33.9%、5位は「運用管理に負荷がかかる」で33.5%、6位は「通信コストが高い」で32.9%、7位は「ユーザが使いこなせない」で32.2%と続いた。
・紛失リスクやセキュリティの解決、導入コストの問題が解決できれば、業務用スマートフォンの利用がさらに進展する可能性はある。

図4 導入しない理由

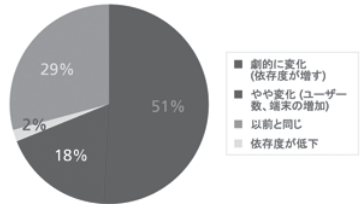


			紛失の危険性が高い	導入コストが高い	ネットワークセキュリティに不安がある	現環境（モバイルPCや携帯電話利用など）で不自由していない	運用管理に負荷がかかる	通信コストが高い	ユーザが使いこなせない	スマートフォンに関する知識があまりない	使いたいアプリケーションが使えない	操作性が悪い	サイズ・重量が大きすぎる	その他
全体		n=487	40.0%	37.6%	34.7%	33.9%	33.5%	32.9%	32.2%	20.1%	13.6%	10.5%	3.3%	10.1%
従業員規模	100名以下	n=137	31.4%	43.1%	21.2%	38.0%	29.9%	42.3%	35.0%	20.4%	10.9%	9.5%	5.1%	9.5%
	101～1000名以下	n=183	42.6%	38.3%	39.3%	37.2%	35.5%	30.6%	35.5%	25.1%	14.2%	12.0%	4.4%	10.9%
	1001名以上	n=167	44.3%	32.3%	40.7%	26.9%	34.1%	27.5%	26.3%	14.4%	15.0%	9.6%	0.6%	9.6%
業種	IT製品関連業	n=130	48.5%	31.5%	43.8%	36.9%	34.6%	28.5%	17.7%	16.9%	16.9%	10.8%	3.8%	9.2%
	（IT関連外）製造業	n=188	31.9%	39.9%	34.0%	31.9%	34.6%	32.4%	33.0%	22.3%	13.3%	10.1%	1.6%	9.6%
	流通・サービス業全般	n=109	41.3%	37.6%	32.1%	38.5%	28.4%	35.8%	48.6%	18.3%	10.1%	9.2%	6.4%	10.1%
	その他業種	n=60	45.0%	43.3%	21.7%	25.0%	36.7%	38.3%	31.7%	23.3%	13.3%	13.3%	1.7%	13.3%

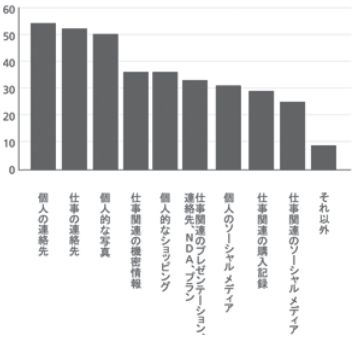
1．2 スマートフォン （1）市場動向⑥

■ マカフィーによる調査（2011年5月発表）によると、対象企業の7割が携帯端末に対する依存度が1年前よりも高くなっており、半数以上は携帯端末の紛失・盗難による情報漏えいを課題と捉えている。紛失または盗難に遭った携帯端末上のデータは、顧客データ（4割）、企業の知的所有権に係る情報（3割）など、重要な情報は多い。
■ また、携帯端末を企業で利用する場合のセキュリティ課題として、約半数が携帯端末の導入によるポリシーの不正利用や実装の不備など、セキュリティポリシーの問題を指摘している。

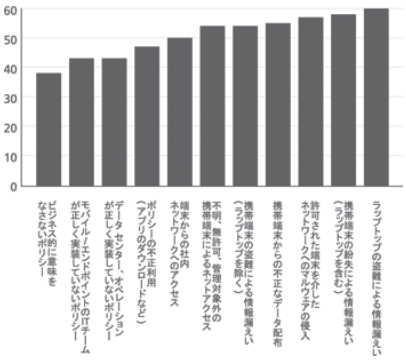
携帯端末の依存度（ラップトップを除く）



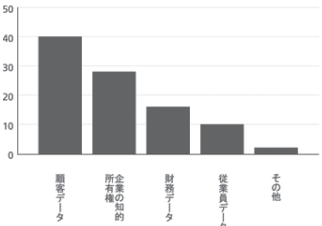
携帯端末で使用する情報の種類とアプリケーション



携帯端末で最も重大なセキュリティ問題



紛失または盗難に遭った携帯端末上のデータの種類



McAfee「スマートフォンおよびタブレットの企業導入における課題と対策：前編」（201
http://www.mcafee.com/japan/security/mcafee_labs/blog/content.asp?id=1292

1．2 スマートフォン （2）導入事例①

ガリバーインターナショナル

システム概要：
・出張訪問を担当する営業員約300人のノートPCをiPadに変更。
・同社が運営する中古車オークションサイト「ドルフィネット」の約4,000台の最新の車両在庫データを保存。
・1台につき平均10枚の画像が含まれているが、容量の関係から1枚目の写真だけをiPad内に保存し、2枚目以降は3G回線やWi-Fi経由で取得するという方式を採用。通信環境が悪い場合でも、端末内のデータだけでスムーズな車両閲覧が可能。
・自宅訪問時の車両査定を紙からiPadへ変更。
・最新のパンフレット、動画の提示
・顧客の個人情報の登録、アンケート入力

導入目的：
・営業員の利便性
・画像表示の美しさ、グラフィカルなインターフェース等、ノートPCでは難しい表現の実現

導入効果：
・ お客様への訴求効果
・ 買取業務の効率化、入力ミスの軽減
・ ノートPCより安く、業務も効率化
・ 今後もiPhone端末の配布等、脱PC化を図る予定

コクヨ

システム概要：
・iPadの直感的な操作性を動画や3Dイメージなどを用いたプレゼンテーションに活用し、顧客への説明をより充実させるほか、クラウドとの親和性を活かしてシンクライアント環境を構築してセキュリティの向上を図る。また、クライアントとのスムーズなコミュニケーションや経営会議等の主要な会議をペーパーレス化し、運営の効率化とコスト削減、および新たなワークスタイルの確立を目指している。
・イベントで活用できる営業ツールのプロトタイプを開発。
・総合カタログ2011アプリも新たにリリース。

導入目的：
・多機能情報端末を活用した新たな働き方を追求するとともに、それを踏まえた新規サービスを開発、顧客への提供を目的に、グループ会社に「iPad」を導入。
現在、グループ全体で251台のiPadを導入

導入効果：
・開発された営業ツールの活用により、営業はiPadですべての商品データ、提案書、映像等を持ち歩くことが可能になり、想定していなかったソリューションや商品の問合せを受けた場合でも、会社に資料を取りに戻ることなくその場で説明することができるようになった。
・将来的には、仕入先、販売店、さらには顧客との間で、それぞれにとっての利便性を考えたツールとして活用することも検討されている。

1．2 スマートフォン （2）導入事例②

フォーラムエンジニアリング

システム概要:
・新技術の積極的導入の一環としてiPad発売直後に5台を試験導入後、約200台を一括導入。
・営業用の情報を付け加えて閲覧できるiPad用アプリ「エンジニアピット for iPad」を独自開発（エンジニアの求人情報サイト「エンジニアピット」用）。
・全国の各拠点へ出張、導入支援。
・利用中に出てくる小さな疑問への回答、Tipsについては毎朝行われる全体会議で提供。
・全オフィスをテレビ会議システムで接続。

導入目的:
・試験導入し、担当者から人材教育や営業支援に関するさまざまな活用方法を提案してもらう。

導入効果:
・会議資料をペーパーレス化、iPadで閲覧、社員同士の情報交換でスキルアップ 。
・派遣先に営業資料を大きく美しい画面でより動的に見せることが可能になり、訴求力も格段にアップした。
・グラフィカルでわかりやすい資料を使った営業活動が現場の社員からも非常に好評。
・今後は、シンクライアント端末としての活用や、キーボードを接続してPC代わりに利用、また社員教育への利用など、さらに幅広く活用予定。

フィリップ・モリス・ジャパン

システム概要:
・新製品紹介キャンペーンスタッフ用にiPad250台を一括導入
・キャンペーンごとにツールとしての動画やアプリケー ションを用意。さらにアンケート回答者のプロフィールデータを入力・蓄積するアプリケーションを開発。
・3G対応のため、逐次送信も可能だが、電波状況が悪い場合も 多く、日次でまとめて送信が基本。
・iPad自体のトレーニングは、キャンペーンごとに実施されるトレーニングの中で実施。
・キャンペーン時の情報収集・アンケート入力

導入目的:
・タバコの新製品紹介活動として大画面の表現力とタッチによる成人喫煙者とのインタラクティブなコミュニケーションを期待。

導入効果:
・データ入力が簡略化され、情報が見やすくなっ
・現場でさりげなく情報入力できる.
・ iPadで映像を見せ、情報をスマートに伝えた後、会話で製品に興味を持ってもらえる。アナログとデジタルを組み合わせたコミュニケーションツールとなる。
・毎回ツールを作るよりコストも抑えられる。

左： http://journal.mycom.co.jp/series/iphoneipadkatsuyo/001/index.html
右： http://journal.mycom.co.jp/series/iphoneipadkatsuyo/002/index.html

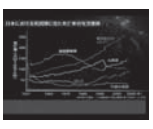
1．2 スマートフォン （2）導入事例③

明治製菓

システム概要:
・医薬営業に使用する動画ツールとしてiPad50台を試験導入。
・オフラインでも利用できるコンテンツ作成・配信・閲覧サービス「Handbook」（インフォテリア）を採用。
・利用場所が病院であるため、オンラインが前提のシステムは導入できない。導入した端末は3G対応のものだが、基本的には情報を提示する時などオフラインで使用する。
・セキュリティはID・パスワードによるログオン認証、データを遠隔地で消去するリモートワイプで運用。
端末保持は動画のみ。
・ウェブ会議システムを使用してユーザーにレクチャー。
・現在はアプリのインストール等にも強い制限は設けず、効果的な運用方法を模索。

導入目的:
・MRの営業活動に用いる動画活用ツールとして導入。

導入効果:
・バッテリ駆動時間の延長、起動時間の短縮、軽快な動作といった当初の目的は十分に達成。
営業からは「仕事が楽しくなった」という声も。
・今後、全国76営業所にiPadの導入を行い、本格導入を目指して徐々に運用を拡大していく予定。



内田洋行

システム概要:
・ Notesからの移行先としてMicrosoft Online ServicesのBPOS(Business Productivity Online Standard Suite)を選択し、シンクライアント端末としてiPadを活用。
・Citrix Receiver（シトリックス）を使用し、外部から社内情報にアクセスできるようにした。
・本人認証の強化に「PhoneFactor」を採用。

導入目的:
・ 顧客にワークスタイルを提案する立場にあり、話題のデバイスを活用した新しいワークスタイルを自ら体験すべく33台のiPadを導入。
・Notesからの移行でシンクライアント端末としても活用できることに期待。

導入効果:
・ワークフローの承認が必要な管理職にiPadが配布されたことで、重いノートPCを持ち歩いて上長の承認を得る必要がなくなった。
・携帯性と起動速度の面で優れており、作業が快適と好評。
・ GIGAPODをベースに自社開発によるセキュアなiPad業務活用ソリューション提案を準備中。
・すでにバックオフィスでの導入効果は十分出ている。ペーパーレスでの会議、1つの画面を見ながらの商談、Safariのファイルビュー機能によるファイル閲覧等、業務利用でもかなり便利な端末であり活用の幅は広い。

左： http://journal.mycom.co.jp/series/iphoneipadkatsuyo/007/index.html
右： http://journal.mycom.co.jp/series/iphoneipadkatsuyo/005/index.html

1．2 スマートフォン （2）導入事例④

モトックス

システム概要:
・ 年間1,500アイテム以上、700万本以上のワインの情報データベースを整え、ワインの情報を二次元コードではなくオリジナルのブドウ型にした独自のAR技術を開発。iPhoneアプリ「Wine-Link」(無料)として配布。
・ブドウ型のARコードを指定枠に収める形でカメラに認識させる。シャッターを切る必要はなく、自動認識されれば、短い言葉を添えたマークが表示される。これをタップすると、専用のサイトへ接続される。
・サイトではワインの風味や生産地、背景といった情報に加えて、生産者のコメントや動画も配信される。
・Android等への対応も準備
・クーポンサービスとの連携、リアル店舗からの誘導

導入目的:
・生産者と消費者の距離を限りなくゼロにできるツール開発。
・iPhoneユーザーのコアとなる30代～40代 の都会に住む男性というユーザー像が、ワインに興味を持つ層と近い。

導入効果:
・ボージョレ・ヌーヴォ解禁のイベントでiPhoneユーザーが、ブドウマークを読み取り、情報を楽しんだ。
・最終的には、自社で取り扱いのないワインの情報も見られるようにしたい。

ユナイテッドアローズグループ

システム概要:
・在庫検索端末としてiPhoneを30台弱導入。1店舗あたりの端末数は5～7台。
・従来システムにある在庫管理システムを検索するインタフェー スをiPhone用に開発。シンプルな操作とクイックな挙動にこだわった。
・システムは、品番を基準に自店だけでなく、他店在庫も確認できる。商品によっては、商品画像の確認も可能。検索データベースは、既存の商品データベースをそのまま利用する。

導入目的:
・在庫確認の効率化のため、実用に耐える機能とお客様の前でスマートに使える端末としてiPhoneを採用。

導入効果:
・お客様をお待たせずに済むようになった。
・導入当初は在庫検索機能に特化していたが、バージョンアップにより、当日の売上データを参照する機能も追加された。当日のデータを店頭で確認できることには大きな需要がある。
・導入店舗をどこまで拡大するのか、店舗あたりの配備台数をどうするのかが今後の課題。同社では、最終的に全店・全スタッフへの配布は考えていない。
・品番のバーコード読み取り機能の導入を検討。

左： http://journal.mycom.co.jp/series/iphoneipadkatsuyo/004/index.html
右： http://journal.mycom.co.jp/series/iphoneipadkatsuyo/009/index.html

1．2 スマートフォン （2）導入事例⑤

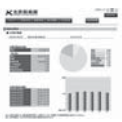
光世証券の営業支援システム

システム概要:
・営業担当者、幹部社員向けにiPhoneを導入。
・使い方は自由（機能制限無し）。
  ー 資産状況や取引履歴を確認できる顧客向けのWebサイト閲覧
  ー その他、ニュースや株価情報（BloombergやSimplex FX等）の閲覧が多い。
・特定の金融グループに属せず、業務システムは自前開発だったことから、早期に意思決定可能だった。（2009年春～）

導入目的:
・社員の意識改革
  対面を重視した効率の悪い営業スタイル（営業のノウハウ共有や横の連携不足）の変革。

導入効果:
・自由な発想でiPhoneを使うことで、ノウハウを社員間で共有。
・外部メール閲覧可能によって休日等でも伝達可能。

セキュリティ:
・一定時間で自動的にパスワードロックされ、設定した回数を超えてパスワードを間違えると全データが消去。
・iTuneで各自がバックアップ、システム部でバックアップイメージを保存。



ユナイテッドアローズの在庫確認システム

システム概要:
・4店舗で在庫確認のためにiPhoneを利用。
・専用アプリケーションを開発。
・サイズ別、色別の在庫数がその場で確認可能。
・操作は商品コードの入力のみ。今後バーコード読取を検討中。
売上のリアルタイム確認や売れ筋商品の確認機能を追加予定。
・30秒もかからずに在庫数確認が可能。
・販売員の携帯性を重視。
・開発期間は約3ヶ月。既存の在庫監理システムはそのまま。

導入目的:
・接客の質の向上

大塚製薬の情報提供システム

システム概要:
・iPadを1,300台を全MR（医薬情報担当者）に配布。
・対面での医療関係者向けの製品説明用資料。
・MRの自己学習用の教材。
・アジア諸国、北米、欧州に展開する社員のネットワーク化
・2010年7月導入。

導入目的:
・MRの情報提供活動の質とスピード向上
  - 視覚化された対話型コミュニケーションの実現
  - 最新情報の共有

左：http://www.itmedia.co.jp/news/articles/0912/16/news049_2.html
右：日経コンピュータ（201年12月8日号）、 http://www.otsuka.co.jp/company/release/2010/0607_02.html

1．2 スマートフォン （3）セキュリティ課題①

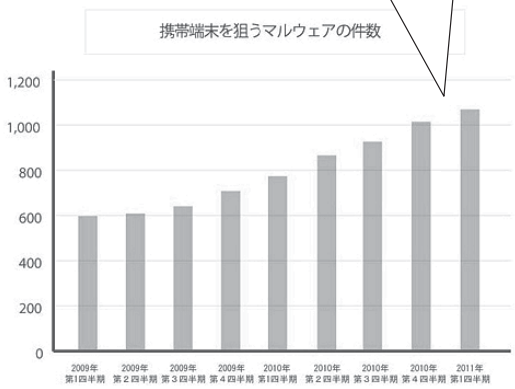
携帯端末の企業利用時のセキュリティ課題

・紛失や盗難
　- 端末データの漏洩　　- 攻撃者にとって企業への侵入口となる
・マルウェア等からの情報の盗難
・意図しない重要な情報の流出
　- SNS等への重要な企業情報の書き込み　- GPSや写真から位置情報を特定
・私物携帯端末の企業ネットワークへの接続
・端末毎の多様な機能の管理（おサイフケータイ、SIMフリー）

Android向け初のボット型ウイルス「Geinimi」は、端末内に潜伏し、悪意のある第三者（クラッカ）からの指令に従ってユーザーの端末を乗っ取ったり外部への攻撃を実行する。2011年1月にIPAが注意喚起。

携帯端末OS別脅威

iPhone	・基本的に安全。Jailbreak（脱獄、サードパーティアプリをインストール可能とし、ファームウェアを書き換える）を実行させるサイトに注意が必要。
Android	・McAfeeの四半期レポート（2011年第一四半期）によると、マルウェアの標的となった携帯端末プラットフォームは、Symbian OSが1位、Androidが2位。ユーザーの操作によって感染するだけでなく、近く自動的にインストールするエクスプロイトが出現すると指摘。
Blackberry	・Research In Motion（RIM）による一貫した生産体制のため、基本的に安全。 ・出所の不明なアプリケーションはインストールしない、BIS（Blackberry Internet Service）の利用等が必要。
Windows Mobile	・Windows OSと同様の脅威が存在。 ・対策にもノウハウがあり、セキュリティ対策ソフトも充実。



http://dt.business.nifty.com/articles/4307.html

1．2 スマートフォン （3）セキュリティ課題②

■ iOSアプリでは、マーケットプレースの審査により不審なアプリケーションのブロックが可能である。また、OSのバージョンアップにより脆弱性対策が可能である。
■ Android端末では、ウイルス対策が機能しない場合があり、業務での利用時には注意が必要である。
■ Windows Phone向けアプリケーションはWindows Phone Market Placeがウイルスや不審な動作などを審査し、一元的に配信することが可能である。

Android端末のセキュリティ課題

・マーケットプレースの審査
　→ Androidマーケットではウイルスチェックは行われない。

・ウイルス対策ソフト
　→ システム領域のウイルスや不正を調べることができない

・OSのバージョンアップ
　→ バージョンアップのタイミングが遅く、ばらつきがある

・OSのパーミッション管理機能によるデータ保護
　→ パーミッションの記述を改ざんされる恐れがある

新たな対策製品

○MDM
・ウイルス対策ソフトや業務アプリケーションが端末管理機能の一部を搭載
・携帯電話事業者がMDMサービスを提供

○スマートフォン向けブラウザ
・キャッシュをメモリ上に残さない、URLフィルタリング等の機能を搭載

1．2 スマートフォン （3）セキュリティ課題③

■ スマートフォンの企業利用におけるセキュリティ面での課題を法的な視点から見ると、スマホにはモバイルPCにはない機能があり、同じ対策では不足が生じる。スマホ自体には、知らないうちに情報を抜かれている懸念があり、会社から観ると、端末の中が見られないことや情報のやり取りのコントロールが聞かないことが問題となる。

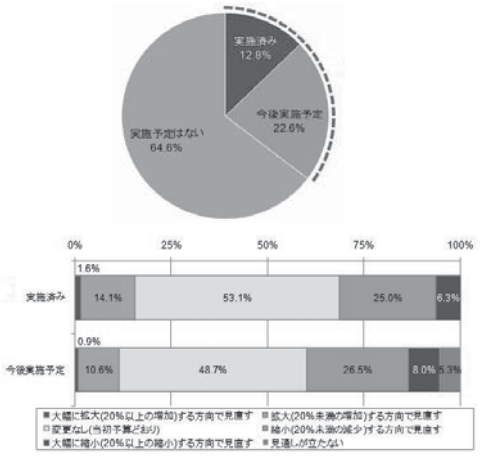
テーマ	法的論点	セキュリティ課題
スマートフォン等の私物利用の流れ	企業側・従業員側の双方にとって適切な出口はあるか	・利便性だけを追求するのではなく、不便であっても守るべきものがあることを認識することが必要である。 ・企業としてコントロールするには、内部規定と抱き合わせで行うことが必要。
	職場への私物PC持込と同じ考え方か	・スマホには、3GとWi-Fiの二段階の常時接続機能があり、GPS、通話機能がある。ユーザのアプリケーションのインストールが容易に可能であり、GPSも含めて個人情報が抜かれやすいが、プレイヤーのビジネスモデルが完全に分業化であり、コントロールが不能となっている。（→ 入口より出口対策が重要） ・録音、カメラ、動画など、情報を簡単に記録可能である。
	会社責任と自己責任の仕切り直し	・会社側からみると、プライバシー所有権で端末の中身が見られない、インストール制御、アプリによる情報のやり取りのコントロールが利かないことが問題。（→ 短時間でチェック可能な担保策は困難）
	私物利用が進むトリガーは	・「スマホセキュリティの紛失、マルウェア等の感染防止」より、意図しない情報流出防止の方が、より大きな問題（テロの対象など）に結びつきかねないという点で重要。
	セキュリティサービスが後押しできるか	・「可用性や利便性に配慮したセキュリティ」という点で、自分のデータがあるのかわからない、多端末からアクセス可能ということは、どこからでも破られる可能性があるということが問題。

第2章 企業における脅威の顕在化

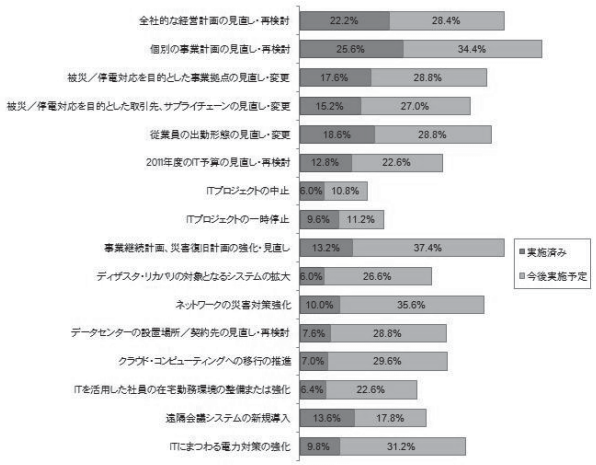
2．1 東日本大震災による影響 （1）市場動向①

■ 2011年度のIT予算の見直し状況について、「実施済み」とした企業は13%、「今後実施予定」とした企業は23%。見直しの方向性は減額を予定する企業が増額を上回り、投資意欲はやや下降・（JIPDEC/ITR、2011年6月）
■ 震災発生後の各社の施策は、「全社的な経営計画の見直し・再検討」「個別の事業計画の見直し・再検討」が多く20%を超える。被災や停電対応を目的とした「事業拠点の見直し・変更」「取引先、サプライチェーンの見直し・変更」は15%以上の企業が実施済み。一方、ITに関連する施策は今後実施予定とする企業が多い。

2011年度IT予算の見直し状況（N=500）



震災発生後の各社の施策（N=500）



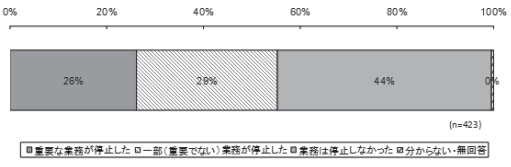
実施期間： 2011年5月20日～25日
調査方法： Web調査（モニタ対象）
調査対象：
国内企業の経営者や情報システム系および経営企画系部門の役職者

「企業IT利活用動向調査2011」JIPDEC／ITR
http://www.itr.co.jp/company_outline/press_release/110627PR/

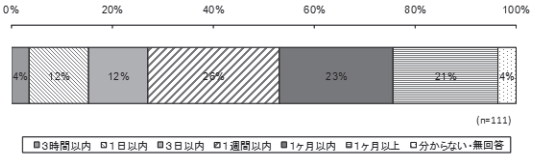
2．1 東日本大震災による影響 （1）市場動向②

■ 回答企業の26%が「重要な業務が停止した」と回答。「一部（重要でない）業務が停止した」（29%）を含めると、55%の企業で何らかの業務が停止。重要な業務が停止した企業のうち21%の停止期間が「1カ月以上」に及ぶ。
■ 重要な業務が停止した理由は、「停電のため」（62%）が最も多く、「業務に必要な生産拠点が利用できなかったため」（45%）、「取引先の業務停止などにより、必要な調達・供給が行えなかったため」（44%）が続く。

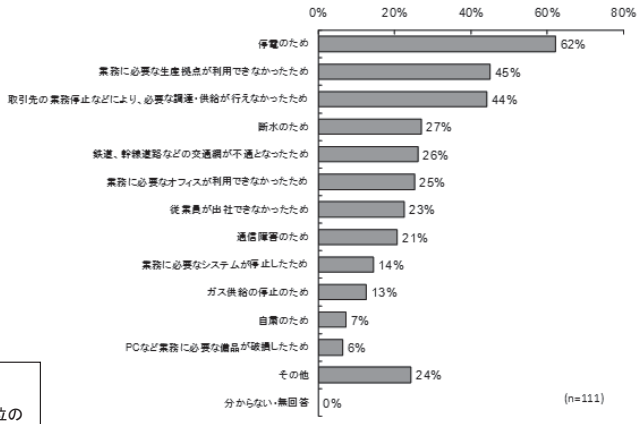
重要業務の停止状況



重要業務の停止期間
（重要な業務が停止した企業で集計）



重要業務が停止した理由
（重要な業務が停止した企業で集計）（複数回答）



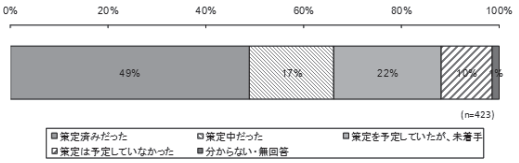
実施期間： 2011年6月
調査方法： 郵送調査
調査対象： 全国の証券取引所一部・二部に上場する企業および資本金額が上位の未上場企業3,000社。（岩手、宮城、福島、茨城に本社を置く会社を除く）3,000社

東日本大震災の影響とBCP（事業継続計画）に関するアンケート調査結果（NRI,2011/06/30）
http://www.nri.co.jp/news/2011/110630_1.html

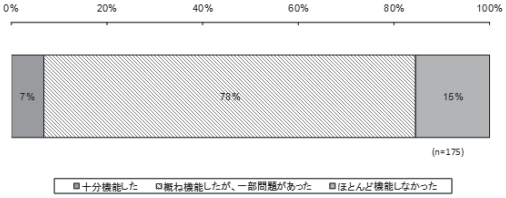
2．1 東日本大震災による影響 （1）市場動向③

■ 東日本大震災発生時点のBCP策定状況は、「策定済みだった」（49%、2007年調査では29%）、「策定中だった」（17%、同36%）であり、3分の2は準備を終えつつあった。しかし、震災時BCPが機能したかどうかについては、「十分機能した」と答えた企業は7%に留まる。
■ BCPの品質を決める重要な3要素である「重要な業務・サービスの絞り込み」「重要な業務・サービスの目標復旧時間の設定」「国・自治体等の想定被害を踏まえた、事業停止時間の想定」の検討を実施状況において、その評価が大きく変わることが判明。
■ その他、「発災直後の安否確認のルール」「重要拠点が被災した際のバックアップの確保」「バックアップのデータセンターの確保」「取引先が被災した場合の代替調達先の確保」「継続的なBCPの更新」等、多くの項目で「見直しが必要」または「項目の追加を検討したい」という回答。

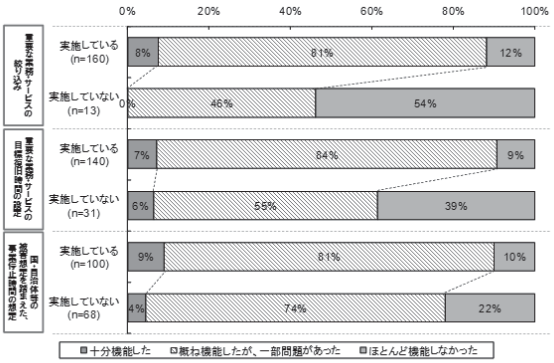
東日本大震災発生時点でのBCPの策定状況



自社のBCPに対する評価



自社のBCPに対する検討項目別の評価
（BCPの対象となる被害のあった企業で集計）

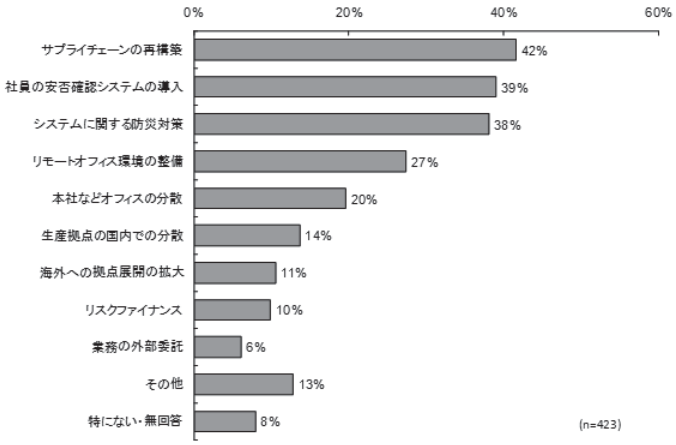


（注）無回答の企業を除いているため、検討項目毎の合計は 175 社（図 6 の集計対象社数）とはなっていない。

2．1 東日本大震災による影響 （1）市場動向④

■ 震災を踏まえた事業継続のための今後の取り組み課題については、「サプライチェーンの再構築」（42%）、「社員の安否確認システムの導入」（39%）、「システムに関する防災対策」（38%）の3つが特に多く挙げられた。

事業継続に関する今後の取り組み課題（複数回答）



2．1 東日本大震災による影響 （2）事例

■ 震災時、従来には無かったITを用いた新しいサービスが登場した。

・テレビを受信できない被災地や海外在住者への災害情報提供を目的に、Ustreamやニコニコ動画は、各テレビ局の地震関連報道番組をインターネット上で同時に放送。

・NHKは、Youtube上に、子ども向け番組やドキュメンタリー番組などを無料で公開。震災発生後、震災報道続きであったが、通常の番組が視聴可能となることで、被災者の精神的なケアにつながった。

・紙媒体での発行が困難となった週刊少年ジャンプなど一部の週刊誌はインターネット上でコンテンツを無料公開

・ヤフー、楽天やAmazonなどECサイトを運営する事業者は、自治体とも連携しながら、被災地の支援物資のニーズとユーザーの支援申し出とのマッチングを実施

・Googleは、ホンダが保有しているプローブデータを活用し、被災地の道路の状況の情報を一覧できるサービスを開始

・アプリ開発事業者は、消費者にわかりやすい形で「安否情報確認アプリ」「医薬品検索アプリ」「停電検索アプリ」などを開発し、無償提供

・東京電力の公表情報を用いて、ポータルサイト事業者が計画停電や電力使用状況に関する情報をユーザが利用しやすいよう整理して提供

・東京電力の公表情報を用いて、電力需給情報等をユーザーが閲覧するためのアプリ（多くが無償アプリ）を開発。

・電力会社やサイネージ事業者と連携し、東京メトロ駅構内デジタルサイネージにて、電力使用状況の掲載を開始。

・内閣官房により「助け合いジャパン」が創設。全国のボランティア情報をデータベース化し、無料で利用できるWEBサービスとして広く提供。

有事におけるIT活用策について（経済産業省、2011年6月）
http://www.jtec.or.jp/6.14kouenkai_meti_sekine.2.pdf

2．1 東日本大震災による影響 （3）セキュリティ課題

有事において発生したセキュリティ課題の例

①【CIA】被災者、死亡者の認証の問題（有事：身分証を持たない状況での認証問題）
・現在議論されている国民IDは物理カードによるもので、有事での問題を解決できるかは要検討である。被災の混乱に乗じて被災者になりすましなども考えられる。

②【CIA】ガセネタ、風評被害などの情報の信ぴょう性を問う問題（情報自体の完全性？）
・平時でも同様の問題が存在するが、パニック心理にある場合情報操作が容易化

③【CIA】設備の容量を超えるアクセスの問題（電話の輻輳など）
・有事で従来より想定される問題だが、通信手段の工夫（スカイプなど）で回避可

④【CIA】システム復帰時の電源再投入問題（有事：複数同時起動での突入電流など）
・復帰時の過電流によってルータ機器などが故障することがある。水に濡れた機器の電源再投入、UPSの活用など物理インフラの災害復旧の課題がある。

⑤【CIA】被災便乗攻撃の問題（有事のDoS問題）

⑥【CIA】有事でのデータ通信の問題（広告の転送時期）
・有事には不要な広告などが被災で狭い帯域をより狭くする問題

⑦有事での個人パソコン利用の問題（許すべきかどうか？）
・有事では個人PCでの社用データ利用を許可している会社がある

⑧有事での医療情報、個人情報の公開問題
・生死にかかわる場合、柔軟であるべきとの議論があったが、その境界線が難しい

⑨ATMでの個人認証の問題（有事に身分証を提示できない場合の対処問題）

⑩有事でのデータサルベージの問題（被災したデータの復帰）
・有事を想定してUPSを起動すべき（安全なシャットダウン）、通電の危険など

⑪HDDのリカバリの問題（RAID5で複数のHDD×TBオーダーになると回復が困難）
・将来、人力での復帰がままならない状況にならないか？

JNSA「有事に於けるインフラ・セキュリティの課題に関する勉強会」（2011/6/29）

2．2 サイバー攻撃の状況 （1）市場動向

■ 2011年は大規模な情報漏えいや防衛産業等をターゲットとしたサイバー攻撃が頻発した。
■ 特に、特定の組織や個人を狙った標的型攻撃が目立った。標的型攻撃の手法自体は従来からあるものだが、国内でも重要機関に対する本格的な攻撃事例が見られたことで、今後、対策の重要性が増していくと考えられる。

2011年に発生した主なサイバー攻撃事例

企業名	時期	サイバー攻撃の内容
ソニー・コンピュータ・エンタテインメント・アメリカ	4月	「PlayStation Network（PSN）」が不正アクセスを受けて停止。約2460万件のSOEアカウントと約1万2700件のクレジットカード/デビットカードの番号と有効期限情報、オーストリアとドイツ、オランダ、スペインユーザーの約1万700件のダイレクトデビットカードの購入履歴情報が流出。
スクウェア・エニックス（欧州子会社）	5月	「Eidosmontreal.com」など複数のWebサイトに不正アクセス。採用選考応募者の履歴書350人分、新商品に関する情報サービスに登録したユーザーのメールアドレス2万5000人分が漏えい。
米シティグループ	5月	ネットバンキングシステムにハッカーが侵入。北米地域36万0083人分のカード口座が影響。
米ロッキードマーチン、ノースロップグラマン	5月	外部から社内につなぐシステムを破られシステムに侵入。
米グーグル	6月	電子メールサービス「gmail」利用者数百人がメールの内容を盗み見られる。
米CIA	6月	公式サイトがハッカーに攻撃され利用不能に。
韓国SKテレコム	7月	子会社が運営するSNSなどが攻撃され、3500万人分の個人情報が流出。
衆議院	7月	議員パソコンや衆院内サーバがウイルスに感染し、議員ら利用者のIDとパスワードが盗難。
参議院	8月	議員パソコンや参院内サーバがウイルスに感染し、全議員・秘書と管理者用の計700件強のパスワードが流出。
オランダ・デジノター	8月	電子証明書発行システムにハッカーが侵入、500越の偽証明書を発行。グーグル利用者等に被害。
三菱重工業	9月	本社や工場、研究所など11拠点にあるサーバーと従業員のパソコン約80台がウイルスに感染
韓国ネクソン・コリア	11月	オンラインゲーム「メープルストーリー」へハッキング、1,320万人分の会員の個人情報が流出。

2．2 サイバー攻撃の状況 （2）セキュリティ課題

■ 標的型攻撃は攻撃を見分けることが困難であり、初期侵入の後、長期に渡って情報探索活動を行い、目的の情報を搾取するという特徴がある。
■ そのため、ネットワークシステム全体のトータルなセキュリティ確保が重要となる。守るべきもの、実現したいことに応じてリスクが異なるため、各組織に見合った対策が必要である。各組織では、必要な対策と可能な対策とを検討し、選択して採用する必要があるが、特に巧妙な攻撃においては、上流での検出・防御が難しいため、出口対策が重要となってくる。

攻撃手法

【攻撃準備】
・攻撃対象組織や、狙うべき弱い部分の事前調査

【事前攻撃活動】
①信頼できる組織や個人を騙った巧妙な標的型攻撃メールの送付
②特定の情報窃取を目的とした業種や組織への執拗な攻撃

【本攻撃】
③メールの添付ファイルの開封やURLのクリックによるウイルスの一次感染。ウイルス
は普段使っているアプリケーションソフトウェアの脆弱性（ゼロデイを含む）を悪用
しているケースが多い。
④感染ウイルスによる外部の攻撃指令サーバーとの通信
⑤ウイルスの増強、変身や、新たな攻撃プログラムのダウンロード
⑥組織システム内での潜伏、拡散、侵攻、探索
⑦機密情報や個人情報等の窃取
⑧外部の攻撃者への窃取情報の送出

脅威の特徴

・実メールの悪用や信頼できる実組織を騙るなど、攻撃を見分けることが困難である。
・一般ユーザ環境の脆弱性をついて、初期侵入をしかけてくる
・侵入（一時感染）後、組織に潜伏し、外部サーバーと連携し、隠密裏に時間をかけて目標となる情報を探索し、情報を窃取する。

技術的対策

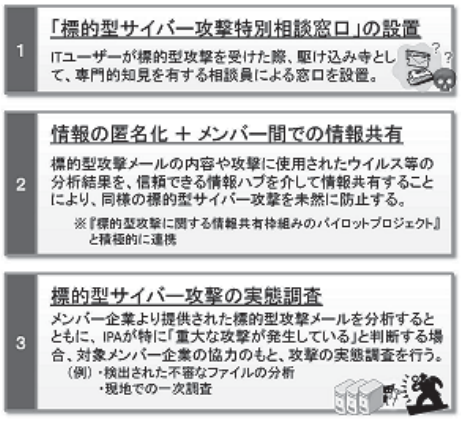
●トータルセキュリティ
・入口防御
・脆弱性対策
・標的型攻撃ルート対策
・ウイルス活動の阻害及び抑止（出口対策）
- 端末間、他部署間のネットワーク通信の制限（ウイルスの組織内蔓延抑止）
- 組織の端末からの外部通信はプロキシを経由させる等の経路制御
- 組織内ネットワーク量の監視（異常さを早期に検知しウイルスの蔓延を早期に発見）
- 知財等のある重要なサーバーはインターネットから隔離

・アクセス制御
・情報の暗号化
・システム監視、ログ分析
・管理統制、コンテンジェンシープラン

2．2　サイバー攻撃の状況　(2)セキュリティ課題

■　標的型攻撃に対しては、経済産業省と内閣官房情報セキュリティセンターが連携し、IPAが中心となった情報共有の仕組みとして、サイバー情報共有イニシアティブ(J-CSIP)が構築された。個別企業の利害関係を超え、NDAの締結を前提にメンバー企業間の情報共有を推進する。
■　防衛省では、装備品の調達の際の企業との契約時に、情報セキュリティの確保に関する特約条項を改正し、ウイルスなどの感染や不正アクセスがあった場合の防衛省への報告するを義務付けた。特約条項の改正の骨子は、防衛省への迅速な報告、セキュリティ対策の強化、企業における教育・訓練の強化の3点である。

J-CSIPの仕組み



資料：業界団体等向け情報セキュリティ対策説明会資料(IPA, 2011年11月)　| 42
http://www.ipa.go.jp/security/J-CSIP/documents/presentation2.pdf

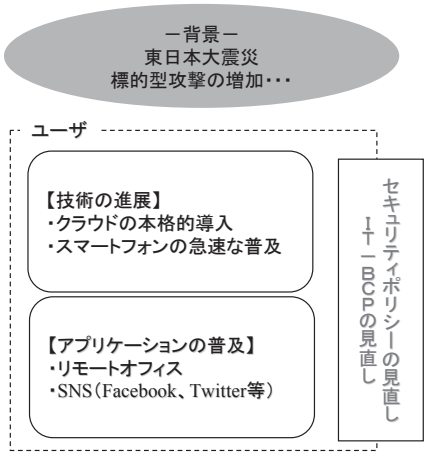
第3章　今後のIT活用と想定されるセキュリティ

3．1　今後のIT活用の方向性と想定されるセキュリティ

	IT活用動向	セキュリティ課題
クラウド・コンピューティング	・新しいクラウドの利用形態 - プライベート/パブリック混在、クラウド移行を背景としたクラウドブローカーの存在 - 複数サービス・ビッグデータの活用 - ソーシャルクラウド ・セキュリティ確保については企業の懸念も未だ存在	・物理サーバ、仮想サーバ、クラウドサービス混在環境のセキュリティ確保 （管理できない仮想化サーバ、仮想マシン間での攻撃、セキュリティ境界線の消失　等） ・リアルタイム、高速、大容量のデータの安全な処理 ・スーパーバイザのなりすまし防止 ・プライバシー確保
スマートフォン	・企業における本格的導入が進展 - Android携帯の普及 - 私物利用携帯端末の増加 - 高度なアプリケーション、社内システムとの連携 ・法的な問題の解決	・紛失や盗難 - 端末データの漏洩 - 攻撃者にとって企業への侵入口となる ・マルウェア等からの情報の盗難 ・意図しない重要な情報の流出 - SNS等への重要な企業情報の書き込み　- GPSや写真から位置情報を特定 ・私物携帯端末の企業ネットワークへの接続 ・端末毎の多様な機能の管理（おサイフケータイ、SIMフリー）
震災による影響	・企業のIT利用における新たなニーズ - サプライチェーン見直し - リモートオフィス - 停電対策 ・有事におけるセキュリティ課題	・可用性の確保（バックアップ） ・情報漏洩、不正アクセス ・有事におけるセキュリティのあり方（機密性と可用性のバランス）
サイバー攻撃の増加	・巧みな手法による、従来安全といわれた組織においても防御の必要性	・出口対策 ・守るべきもの、実現したいことに応じたセキュリティ対策

3．2　重要となるセキュリティ課題

- 昨年までは、国民ID問題でC（Confidentiality）が重要視されていたが、震災によりA（Availability）がフォーカスされるようになった。しかし、昨今、官公庁や防衛産業への標的型攻撃などが増加し、AからCに強引に引き戻されたのが現状。
- クラウドやスマートフォンなど、新しい技術の普及も背景に、企業においても、従来のセキュリティポリシーやIT-BCPの見直しが求められている。
- バランスの取れた情報管理のあり方を技術的に実現することで、IT産業の活性化を目指したビジネスをJEITAが推進する必要がある。



●複数クラウド利用時のセキュリティ確保
- 複数のクラウドを様々な形態で利用するユーザにとってのセキュリティ確保が課題となる。（クラウドブローカー）

●プライバシーに配慮した個人情報の利用
- ビッグデータや、クラウド、スマートフォンによる様々な箇所から大量の情報が集約、ビジネス活用される中、プライバシーの確保が重要な課題となる。

●スマートフォン等端末の企業利用
- スマートフォンの企業利用が進展し、紛失や盗難・マルウェア対策や意図しない情報の流出防止が求められる。

●機密性と可用性のバランス配慮したセキュリティ
- 東日本大震災により、可用性の確保に向けた取り組みや、冗長化の取り組みが進展したが、標的型攻撃の増加によって、機密性の確保も強く求められてきた。各社の状況に応じた適切なバランスに配慮した対策が求められる。

参考資料

参考1）委員会における講演等

（1） 第4回委員会　株式会社三菱総合研究所　クラウドセキュリティグループ （発表）
「クラウド環境等に関する意識調査」
※ 総務省から日立製作所が受託した「クラウド対応型セキュリティ対策技術の研究開発」（2010年度）の成果の一部に加筆・修正

（2） 第5回委員会　情報セキュリティ大学院大学　原田要之助　教授 （講演）
「大震災から見えてきた、今後のITの課題」

（3） 第7回委員会　株式会社ラック　最高技術責任者　西本逸郎氏 （講演）
「企業におけるスマートフォン活用の方向性と情報セキュリティについて」

（4） 第8回委員会　倉敷芸術科学大学　小林和真　教授 （意見交換）

（5） 第8回委員会　英知法律事務所　岡村久道　弁護士 （意見交換）

（6） 第8回委員会　関電システムソリューションズ株式会社 （事例紹介）
「グループワイドネットワーク Finderの紹介」
「関電グループシェアードシステムについて」

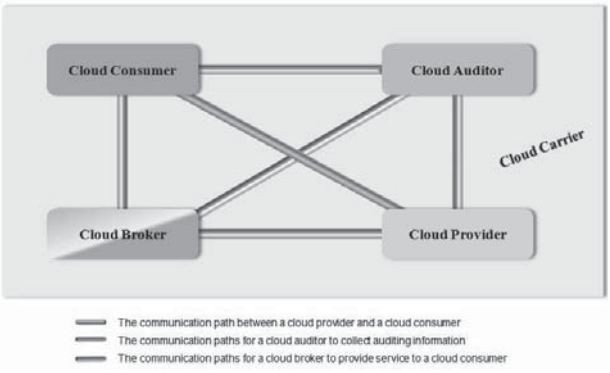
参考2）NIST-SP 500-291 “NIST Cloud Computing Standards Roadmap”

仮訳

NISTのクラウドコンピューティング・リファレンスアーキテクチャ

■ クラウドコンシューマ、クラウドプロバイダ、クラウドオーディタ、クラウドブローカ、クラウドキャリアーNIST「クラウドコンピューティングのリファレンスアーキテクチャ」は、5つの主要なアクターを定義している。各アクターは、トランザクションやプロセスに関与するエンティティ（個人または団体）であり、および/またはクラウドコンピューティングのタスクを実行する。クラウドコンシューマは、直接またはクラウドブローカを介してクラウドプロバイダにクラウドサービスを要求できる。クラウドオーディタは、独立した監査を実施し、必要な情報を収集するために他に連絡することができる。

アクター	定義
クラウドコンシューマ	クラウドプロバイダとビジネス関係を維持し、サービスを得る個人または組織
クラウドプロバイダ	クラウドコンシューマが利用可能なサービスを構築する責任を負う個人、組織または主体
クラウドオーディタ	クラウドサービス、情報システム運用、パフォーマンス、クラウド実装のセキュリティの独立した評価を行うパーティ
クラウドブローカ	クラウドプロバイダとクラウドコンシューマの間で関係の調整を行い、クラウドの利用、パフォーマンス、クラウドサービスの提供を管理する主体
クラウドキャリア	クラウドプロバイダからクラウドコンシューマまでの接続と通信を供給する仲介者



参考2）NIST-SP 500-291 “NIST Cloud Computing Standards Roadmap”

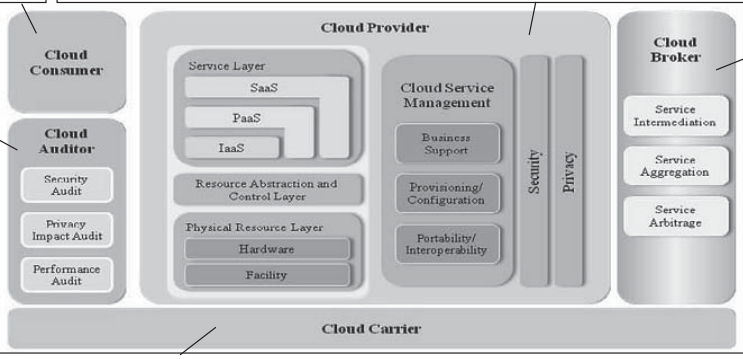
仮訳

NISTのクラウド複合概念リファレンスダイヤグラム

クラウドコンシューマ
クラウドコンピューティングサービスの究極のステークホルダー。ビジネス行う、またはクラウドプロバイダからのサービスを使用する人または組織。クラウドプロバイダからのサービスカタログを見て、適切なサービスを要求し、クラウドプロバイダとサービス契約をして、サービスを利用する。利用サービスに応じた支払いを行うが、要求サービスに応じて、利用形態やシナリオはコンシューマ間で異なる（SaaS、PaaS、IaaS等）。

クラウドプロバイダ
クラウドコンシューマに利用可能なサービスを提供する責任を持つ人または組織、実体。要求されたソフトウェア/プラットフォーム/インフラサービスを構築し、必要な技術インフラの管理、合意したレベルでのサービス提供。サービスのセキュリティとプライバシーを保護する。様々なサービスモデルを提供するためのタスクを行う。
Cloud Software as a Serviceでは、コンシューマの要求レベルで、クラウドインフラストラクチャ上で、アプリケーションの展開、コンフィグ、メンテナンス、運用がなされる。SaaSプロバイダーは、アプリケーションとインフラストラクチャの管理・制御に多くの責任を持つ。
Cloud Platform as a Serviceでは、プラットフォームのためのクラウドインフラストラクチャを管理し、コンシューマが開発、テスト、展開するためのツールと、実行リソース、管理者用アプリケーションを提供する。コンシューマは、アプリケーションとホスティングされる設定環境を制御可能だが、ネットワーク、サーバ、OS、ストレージを含むプラットフォームの下層のインフラストラクチャにはアクセスできない。
Cloud Infrastructure as a Serviceでは、物理的処理、ストレージ、ネットワーク、および他の基本的なコンピューティングリソースだけでなく、IaaSコンシューマのためのホスティング環境とクラウドインフラストラクチャを提供する。クラウドコンシューマは、ホスティング環境やオペレーティングシステムをより詳細に制御できるが、基盤となるクラウドインフラストラクチャ（例えば、物理サーバ、ネットワーク、ストレージ、ハイパーバイザ等）の管理・制御はできない。

クラウドオーディタ
クラウドサービス、情報システムの運用、パフォーマンス、およびクラウド実装時のセキュリティの評価を行うグループ。セキュリティコントロール、プライバシーへの影響、性能等の観点から、クラウドプロバイダの提供サービスを評価する。
監査は、政府機関にとって、「クラウドプロバイダーのセキュリティ統制を第三者が評価することを可能にする契約条項を含める必要がある」（by Vivek Kundra, Federal Cloud Computing Strategy, Feb 2011）の点で重要である。



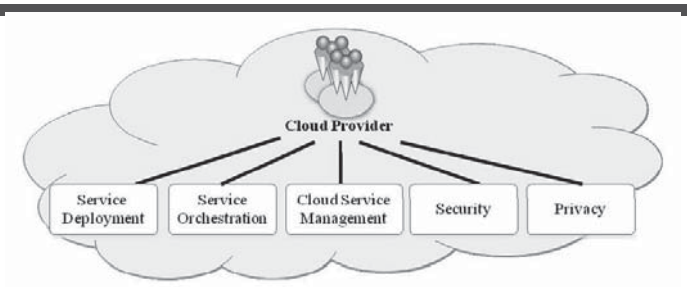
クラウドブローカ
クラウドコンピューティングの進化に伴い、クラウドサービスの統合は、クラウドコンシューマにとって管理が余りに複雑になる。クラウドコンシューマは、クラウドブローカーからクラウドサービスを要求することができる。クラウドブローカーは、使いやすさ、パフォーマンス、およびクラウドサービスの配信を管理し、クラウド間の関係を調整する存在である。
一般的に、「サービス仲介」「サービスアグリゲーション」「サービス裁定取引」の3通りでサービス提供が可能である。

クラウドキャリア
クラウドコンシューマとクラウドプロバイダの間でクラウドサービスの接続性と輸送を提供する仲介者として機能する。ネットワーク、テレコミュニケーション、およびその他のアクセスデバイスを介して消費者へのアクセスを提供する。クラウドコンシューマは、コンピュータ、ラップトップ、携帯電話、モバイルIInternetデバイス（MID）等のネットワークアクセスデバイス等を通じてクラウドサービスを利用する　通常、ネットワークや通信事業者またはトランスポートエージェントによって提供される。クラウドプロバイダーは、クラウドコンシューマと同等のSLAをクラウドキャリアと設定したり、クラウドコンシューマとクラウドプロバイダ間の専用線と暗号化接続を提供することが必要な場合がある。。

参考2）NIST-SP 500-291 “NIST Cloud Computing Standards Roadmap”

仮訳

クラウドプロバイダの主な活動



サービス展開	サービス組織化	クラウドサービス管理	セキュリティ	プライバシー
パブリッククラウドは、インフラストラクチャとリソースは、パブリックネットワークを介して一般公衆に利用可能にされたものである。クラウドサービスを販売する組織が所有。 プライベートクラウドは、インフラストラクチャは、単一の組織のために独占的に運営。顧客のオンサイトのプライベートクラウドまたはホスティング会社（外部委託プライベートクラウド）にアウトソーシングで実装。 コミュニティクラウドは、組織または第三者によって管理。 ハイブリッドクラウドでは、データとアプリケーションのポータビリティを可能にする標準化や独自の技術によって互いに結合された2つ以上のクラウド。	ITとビジネス要件を満たし、様々なクラウドサービスを提供するための配置、調整、クラウドインフラストラクチャの管理。 三層のフレームワークの最上層は、クラウドプロバイダの3つのサービスモデルのそれぞれを定義する。 中間層は、リソースの抽象化と制御層。ソフトウェアの抽象化を介して物理的なコンピューティングリソースへのアクセスを提供および管理するシステムのコンポーネントが含まれる。 フレームワークの最下層は、全ての物理的コンピューティングリソースを含むリソース層。 この枠組みでは、層の水平方向の位置決めは、上位層が下位層への依存性を有するスタックを意味することに注意。	必要とするクラウドコンシューマに要求されたサービスの管理と操作に必要なサービス関連の機能がすべて含まれる。 ビジネスサポート、プロビジョニング/コンフィギュレーション、移植性/相互運用性要件の観点から説明することができる。	リファレンスモデルの全てのレイヤに跨って、物理的なセキュリティからアプリケーションセキュリティまで、セキュリティが横断的であることの認識が重要である。一般的に、クラウドプロバイダと連邦政府のクラウドコンシューマの間では責任を共有している。 クラウドプロバイダは、クラウドサービスをホストしている施設が安全であること、スタッフが適切なチェックを持っていることの確認が必要。データやアプリケーションをクラウドに移行する際は、クラウドサービスは、セキュリティ要件の遵守コンプライアンスルールの適用を確認することが重要である。独立監査は、規制やセキュリティポリシー遵守の確認に行われるべきである。	クラウドプロバイダは、個人情報（PI）とクラウドで個人を特定できる情報（PII）の、確実に適切な、そして一貫性のある収集、処理、コミュニケーション、使用、廃棄を保護する必要がある。 CIO評議会によると、連邦政府の主要なビジネス上の緊急課題の一つは、収集した個人情報のプライバシーを確保することである。PIIは、社会保障番号、バイオメトリクスの記録等、単独で、またはリンク可能なその他の個人を特定できる情報と組み合わせて個人の身元を識別または追跡するために使用できる情報である。クラウドコンピューティングは柔軟なソリューションを提供しているが、消費者の新たなプライバシー課題となっている。

参考2）NIST-SP 500-291 “NIST Cloud Computing Standards Roadmap”

仮訳

クラウドブローカの主な活動

サービス仲介

クラウドブローカーは、いくつかの特定の能力を向上させ、クラウドコンシューマに付加価値サービスを提供することにより、特定のサービスを向上させる。クラウドサービス、アイデンティティ管理、パフォーマンスのレポーティング、セキュリティの強化、アクセス管理等ができる。

サービスアグリゲーション

クラウドブローカーは、1つまたは複数の新しいサービスを組み合わせて統合する。ブローカーは、データ統合を提供し、クラウドコンシューマと複数のクラウドプロバイダー間の安全なデータ移動を保証する。

サービス裁定取引（アービトラージ）

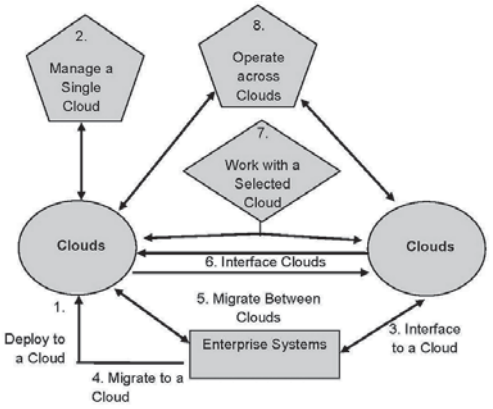
サービスの裁定は、集約されているサービスが固定されていないことを除き、サービスアグリゲーションと類似している。サービスの裁定取引は、ブローカーが複数の機関からサービスを選択できる柔軟性を持っていることを意味する。クラウドブローカーは、例えば、最高のスコアを持つエージェントを測定・選択するためにクレジットスコアリングサービスを使用することができる。

参考2）NIST-SP 500-291 “NIST Cloud Computing Standards Roadmap”

仮訳

クラウドコンピューティングの展開シナリオ

■ “クラウド最初の“ ビジネスユースケースは、米国政府機関のクラウドコンシューマとクラウドプロバイダの間の複雑な相互作用が要求される。「相互作用」は主に3つのグループから構成される。



シングルクラウド
シナリオ1：シングルクラウドの構築
シナリオ2：シングルクラウド上のリソース管理
シナリオ3：シングルクラウドへのインターフェースの
エンタープライズシステム
シナリオ4：シングルクラウド上に移行、または
置き換えられたエンタープライズシステム

マルチプルクラウド（順次、一度に1つずつ）
シナリオ5：複数クラウドへの移行
シナリオ6：複数クラウド間のインタフェース
シナリオ7：選択されたクラウドとの協調

マルチプルクラウド（同時、一度に複数）
シナリオ8：複数のクラウドを跨る動作

これらの技術的なユースケースは、クラウドの展開モデルと、クラウド関係者の総合作用の文脈で分析する必要がある。
これらの考慮事項は、クラウドコンピューティングのユースケースの領域に2つの根本的な次元を特定する。
・中央集中型 vs 分散
・内部 vs 信頼境界の横断
これら展開ケースは、クラウド標準への要求を加速する。

参考2）NIST-SP 500-291 “NIST Cloud Computing Standards Roadmap”

仮訳

クラウドの展開モデル

	信頼境界内型	信頼境界横断型
集中型 単一のクラウドプロバイダーが存在。各クラウドプロバイダーは、複数のクラウドコンシューマにサービスを提供することがある。各クラウドコンシューマは、プロバイダとの単純な相互作用を持つ。	通常、単一の内プライベートクラウド。非技術的な手段により、ポリシーやガバナンスが機能している。基本的な要件： ・シンプルなコンシューマープロバイダ間の認証 ・VM管理　・ストレージ管理 ・SLAおよびパフォーマンス/消費電力のモニタリング ・サービスの発見　・ワークフロー管理 ・監査 ・コミュニティクラウドのユースケースをサポートする仮想組織	単一の管理ドメインが信頼境界の外側。クライアントは、インフラストラクチャに「焼き付け」られる技術的手段を通じて、クラウドプロバイダーのポリシーやガバナンスに依存。基本的な要件： ・ガバナンス要件をサポートするSLA（国または地域の規制、コンプライアンス等） ・より強力な認証メカニズム（PKI、証明書、等） ・ハイパーバイザのサポートやハードウェアを通じたVM認証の分離 ・ハードウェアのサポートを介したストレージ認証の分離 ・データの暗号化
分散型 単一のクラウドコンシューマが持っている複数のクラウドプロバイダに分散して管理。クラウドコンシューマは単純なプロバイダを持つが、アプリケーションとプロバイダとの相互作用はより複雑なP2P相互作用が必要になる。	2つ以上のフェデレートされたクラウド。クラウドプロバイダーが境界外に存在。共通の信頼境界によって、ポリシーとガバナンスを実現。基本的な要件： ・P2Pサービスの発見 ・P2P SLAおよびパフォーマンスの監視 ・P2Pワークフロー管理 ・P2P監査 ・P2Pセキュリティ、認証、認可のためのメカニズム ・P2P仮想組織の管理	アプリケーションが交差するハイブリッドクラウド。パブリック-プライベート、もしくは複数のパブリッククラウドの信頼境界において、コンシューマは、インフラストラクチャに「焼き付け」られる技術的手段を通じて、クラウドプロバイダーのポリシーやガバナンスに依存。 アプリやサービスが配布され、P2P方式で動作する可能性がある。基本的な要件： ・ガバナンス要件をサポートするSLA（国または地域の規制、コンプライアンス等）

【共通の要件】
1.作成、アクセス、更新、雲内のデータオブジェクトを削除
2.仮想マシンと雲の間に仮想アプライアンスを移動
3.プライベート外部にホストされているクラウドに最適なIaaSのベンダーを選択
4.複数の雲を監視および管理するためのツール
5.クラウド間でデータを移行
6.複数のクラウドへのアクセス、シングルサインオン
7.雲全体のオーケストレーションのプロセス
8.クラウドリソースの検出
9. SLAおよび罰則の評価
10.監査クラウド

参考2）NIST-SP 500-291 “NIST Cloud Computing Standards Roadmap”

セキュリティのためのクラウドコンピューティング標準①

仮訳

クラウドコンピューティングサービスに対する攻撃タイプ

・クラウドプロバイダーからの転送中のデータの機密性と完全性

・急速にスケールを拡大し攻撃力を強めるクラウドコンピューティングへの攻撃

・コンシューマからの認可されていない、使用中のソフトウェア、データ、リソースへのアクセス（不正な認証または認可、あるいはメンテナンス中に導入された脆弱性を介して）

・以前はプライベートネットワークを介してアクセスされたリソースのインターネット脅威や脆弱性を念頭に置いて設計されていないソフトウェアを利用するDoS攻撃などのネットワークベースの攻撃

・マルチテナント環境におけるデータ暗号化能力の限界

・クラウドコンシューマが新しいクラウドサービスプロバイダに変更するために作る非標準のアプリケーションプログラミングインターフェイス（API）から生じる移植性の制約

・クラウドリソースが物理的に抽象である点を活用した、監査手続や記録内の透明性の欠如を悪用する攻撃

・最近パッチが適用されていない仮想マシンを利用した攻撃

・グローバルプライバシーポリシーおよび規制の不整合を悪用する攻撃

参考2）NIST-SP 500-291 “NIST Cloud Computing Standards Roadmap”

セキュリティのためのクラウドコンピューティング標準②

仮訳

クラウドコンピューティングの実装のための主要なセキュリティ目標

・不正アクセス、開示、改ざんまたは監視から顧客データを保護すること。これは、顧客がクラウドサービスにアクセスする権限のあるユーザのIDおよびアクセス制御ポリシーを実施する能力を持っていること等をサポートするID管理が含まれる。また、他のユーザにそのデータへのアクセスを選択的に利用できるようにする顧客の機能が含まれる。

・サプライチェーンの脅威から保護すること。これにより、信頼性を確保し、使用するハードウェアとソフトウェアの信頼性だけでなく、サービスプロバイダの信頼性の保証が含まれる。

・クラウドコンピューティングインフラストラクチャのリソースへの不正アクセスの防御。これは、コンピューティングリソースと使用中のsecure-by-defaultな設定の間の論理的な分離を持った安全なドメインの実装を含む。

・ソフトウェア開発プロセスにおけるインターネット脅威モデルと組み込みセキュリティを展開したWebアプリケーションのデザイン

・エンドユーザーのセキュリティの脆弱性を軽減するためのインターネットブラウザの保護。これは、セキュリティソフト、パーソナルファイアウォール、およびパッチのメンテナンスを適用した個人のコンピューティングデバイスのインターネット接続時の保護も含まれる。

・クラウドプロバイダーのアクセス制御や侵入検知技術を配備し、それらがきちんと整っていることを確認するために、独立した評価を実施すること。セキュリティパッチの展開を通じて、搾取から個々のコンポーネントを保護する－従来の境界セキュリティは、ネットワークやデバイスへの物理アクセスを制限したい場合など、デフォルトで最も安全な設定などの設定、使用されていないすべてのポートとサービスを無効にする、ロールベースのアクセス制御の使用、モニタリング監査証跡、特権の使用を最小限に抑制、ウイルス対策ソフトウェアの使用、通信の暗号化など。

・セキュリティを提供する責任が明確であることを保証するための、サービスプロバイダ（複数可）とコンシューマ間の信頼境界の定義。

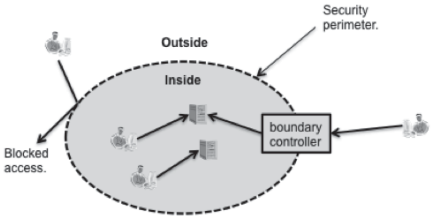
・コンシューマが、クラウドサービスプロバイダを変更するとき、可用性、機密性、および整合性の要件を満たすための移行性のサポート。これは、特定の日時でアカウントを閉鎖する、別のサービスプロバイダからデータをコピーする機能を含む。

参考3）NIST-SP 800-146 “DRAFT Cloud Computing Synopsis and Recommendations”

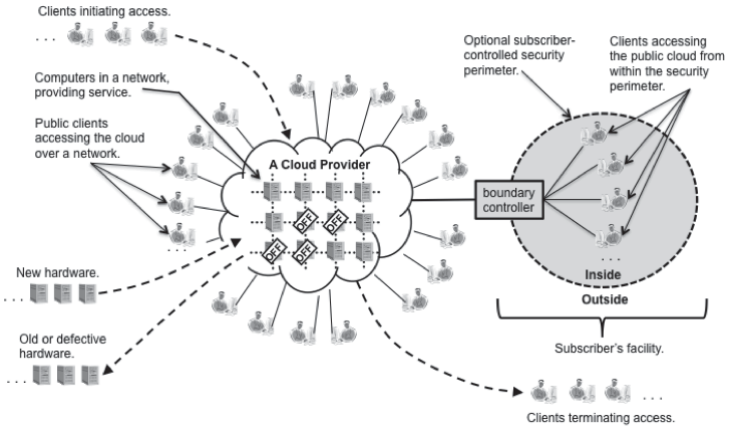
仮訳

クラウドコンピューティングのリソースコントロール①

スコープ	適用性
一般	すべてのクラウド展開モデルに適用
オンサイト・プライベート	顧客の構内で実装されるプライベートクラウドに適用
アウトソース・プライベート	サーバ側はホスティング会社に委託されるプライベートクラウドに適用
オンサイト・コミュニティ	コミュニティクラウドを構成する顧客の構内に実装されるコミュニティクラウドに適用
アウトソース・コミュニティ	サーバ側はホスティング会社に委託されるコミュニティクラウドに適用
パブリック	パブリッククラウドに適用



一般



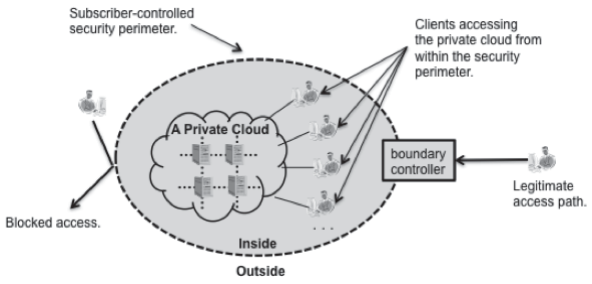
パブリック

資料：NIST-SP 800-146 “DRAFT Cloud Computing Synopsis and Recommendations”（May,2011）を基にMRI作成

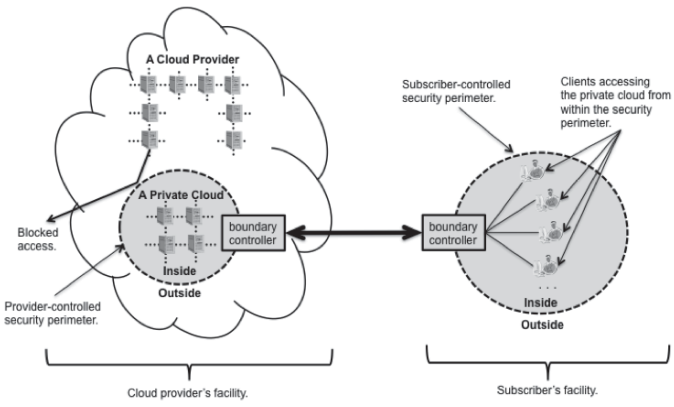
参考3）NIST-SP 800-146 “DRAFT Cloud Computing Synopsis and Recommendations”

仮訳

クラウドコンピューティングのリソースコントロール②



オンサイト・プライベート



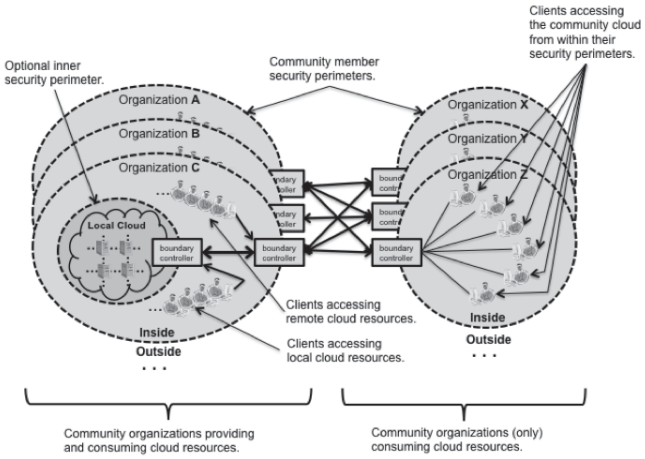
アウトソース・プライベート

資料：NIST-SP 800-146 “DRAFT Cloud Computing Synopsis and Recommendations”（May,2011）を基にMRI作成

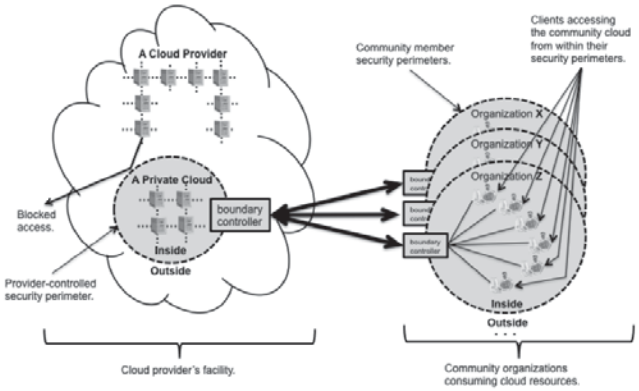
参考3）NIST-SP 800-146 “DRAFT Cloud Computing Synopsis and Recommendations”

仮訳

クラウドコンピューティングのリソースコントロール③



オンサイト・コミュニティ



アウトソース・コミュニティ

セキュリティ市場・技術調査報告書

発　行　日　　平成24年３月
編集・発行　　一般社団法人　電子情報技術産業協会
　　インダストリ・システム部
　　情報システムグループ
　　〒100-0004　東京都千代田区大手町1-1-3
　　大手センタービル
　　TEL　(03)5218-1057
印　　刷　　三 協 印 刷 株 式 会 社