EC における情報セキュリティに関する
活動報告書 2007

－ ECOM 情報セキュリティガイド2007 －

平成 20 年 3 月

次世代電子商取引推進協議会

はじめに

現在大きな「セキュリティ」の課題は、「何をしていたら違法状態にはならないのか？」です。当然情報政策を担う管轄官庁に問い合わせても「これをしていたら良い」などと回答は出ません。何故なら、セキュリティに対する悪の手段は日々想像を絶する手法を用いて進化しているという事実がある反面、企業におけるセキュリティ活動は、「何をしたから、もう大丈夫」などというものは無く、地道で継続的な活動が必要となるからです。その具体的なものが、ISMS（ISO27001）やプライバシーマークといった認証制度の存在理由の背景です。もっと分かりやすい活動で言えば、「安全衛生活動」や「品質改善活動」といった企業活動として真っ当と認識されている活動と同様な企業の取り組みが、「企業情報セキュリティ活動」なのです。

建設現場の監督者が最初に覚えさせられる事項に以下のことがあります。複数の業者が出入りする現場の安全対策の基本で、例えば新築のビルの現場がある。その際、現場監督が安全衛生上最初に注意するのは、例えば、天井の工事をする業者が入る日程には、足元にペンキの空き缶や建具といった部材を床に置かせないことです。一見、置いてあっても問題無い様に感じるかもしれませんが、違います。なぜならば、天井の工事をする業者は、天井に集中して工事をしているので、足元には注意を払わない。そんな際に足元に「労災」を呼ぶような物を「そもそも置いてはいけない」のです。

建設現場で行う、始業前のラジオ体操、安全点検、監督者、作業員、一体となった工事現場全体の安全意識向上、作り上げる建設物の品質向上に貢献しているのは言うまでもありません。場合によっては、地域住民との話し合いも行いながら、建設現場は作業を進めていくのです。一度労災が発生すれば、現場はストップし、怪我をした作業員自身も不幸ですし、現場全体、そして元受け、顧客も不幸になります。

IT が浸透し、情報漏洩が企業活動の根幹を脅かす社会になってきた昨今、上記の工事現場に相当する企業は多く存在すると思われます。つまり、皆さんのオフィスを、価値を創出している工事現場だと考えれば、皆さんの職場も工事現場と同じだと感じられるのではないでしょうか。労働安全衛生上、「危険な労働環境」になっていませんか？情報漏洩事故は、労使ともに回避すべき「労災」の要素も非常に大きいと考えています。

セキュリティを構成する重要な要素は、コンプライアンスやガバナンスを意識した地道で日常的な企業活動の基盤と、その組織が採用判断して導入・運用しているセキュリティシステム（ハード・ソフト）であり、それらが、両輪となって継続的に運用・向上されているという組織としての不断の努力が大事だということです。コンプライアンス意識の無い組織であれば、どんなに高額なセキュリティソフトウエアを入れても漏洩事故は容易に発生するでしょう。そのような魂の入っていないシステムの評価の仕組みだけが存在しても、全く意味が無いのは、皆さんも直感的に理解できると思います。

平成２０年３月

次世代電子商取引推進協議会

目　次

1. 情報セキュリティ WG 活動

次世代電子商取引推進協議会は平成１７年に設立され、情報セキュリティに関する意見交換の場として、情報セキュリティ懇話会を開催し、技術者、経営者、法律家、消費者の視点で事件や出来事に関して、意見交換をしてきた。平成 19 年度はこれらの活動を踏まえ、情報セキュリティ WG を組織した。

以下、情報セキュリティ WG の活動を報告するとともに、今後の我が国の情報セキュリティの向上に向けて、参加したメンバー（技術者、経営者、法律家、消費者関係、管轄行政担当者）で共通認識として得られた事項をガイドとしてまとめた。

1.1. 概要

平成 18 年度までの情報セキュリティ懇話会における情報交換の中から浮上してきた具体的なセキュリティ課題として、積極的、戦略的に情報セキュリティの脆弱性を会話するサイトや専門的な知識がなくて利用できるハッキングツールなどへの対策、顕在化してきている情報端末、特に組み込み型装置のセキュリティトラブルについて検討するとともに、企業間（BtoB）EC や企業消費者間（BtoC）EC における情報セキュリティ対策の標準的な利用ガイドブックを作成し、技術者と経営者、法律家、消費者での情報セキュリティに関する共通認識の醸成し、現在の安全・安心 EC（情報セキュリティ対策）の底上げに資する成果報告書を作成する。

技術者、経営者、法律家、消費者の共通認識となるガイドを作成することによって、情報セキュリティ対策の透明性を高め、企業、個人の情報セキュリティ対策の底上げに資する。特に、IT セキュリティ製品の開発・コンサルテーション・販売等に携わっている人たちが、具体的にセキュリティ対策を行う主体の責任者である、企業経営者に参考としてもらえるよう心がける。その際、法律家、消費者、担当行政組織の側からの声も反映させるべく本 WG 参加者や招聘する有識者等には留意する。特に、中小零細企業の経営者にこの情報セキュリティガイドを紹介し、その上で自らの情報セキュリティ向上に対する取り組みやセキュリティ製品の特徴や長所等を提案できるものとする。

具体的には、IT を構築している１、ハード、２、ソフト（下位・上位ソフト）、３、ネットワーク、４、実社会判断・経営判断（法的解釈）との連携を意識しながらガイドを作成し、且つ、現場ヒアリングを行い、本当の現場の声も反映させ、管轄の行政側も納得できるガイドとし、我が国の IT セキュリティの底上げと、全体レベルの向上に資する成果報告を行う。

1.2. 経緯

次世代電子商取引推進協議会での情報セキュリティに関する活動の根底にあったのは、インターネットは、誰にも何も保証しない、という業界関係者の常識を一般利用者は知らない可能性の高いということである。さらに、そのような誰にも何も保証しない環境をベースに、あまりにも社会基盤として、無責任なことを言えないビジネスインフラ、電子商取引環境になり始めている

という危機感であった。しかしながら、「セキュリティ」という意味を追求していくと、単にネットワークだけの問題には止まらず、ハード、ソフト、更には、企業経営者の意識、法環境、一般市民との常識のズレの補正といったことにも及ぶことが見えてきた。本 WG では、この事実（常識とのズレの補正）を、一般の方々や、特に社会的責任からセキュリティ対策を実施しなければならない企業経営者に、いかにして理解してもらうかということを中心に活動を行った。

■平成17年度（情報セキュリティ懇話会）

法律における自己情報コントロール権（特に個人情報に関する裁判が二箇所の地方裁判所でほぼ同時期に行われ、その判決が全く逆の内容だったことを踏まえ、司法判断が同一訴訟内容で異なるとしたら、個人情報保護に携わる者は、何をよりどころとして、どのような具体的な対策を行えばよいのかが疑問となったため）、クレジットカード情報の大量流出など、事件や法律、情報セキュリティに係るガイドラインや、分散セキュリティや生体認証などの最新技術、公的個人認証などの展開、ＩＳＭＳ、セキュリティ基準の国際標準化動向について有識者を招き、メンバーと情報交換した[1.2-1]。

■平成18年度（情報セキュリティ懇話会）

セキュアジャパン２００６などの政策や、関係団体から情報セキュリティに関する取り組みについて、ネット上での詐欺、フィッシング、スパイウエア、米国での取り組みについて情報を交換するとともに、現在のインターネット環境が安全安心なＥＣのインフラとしてうまく機能しているかについて、情報交換し、議論した[1.2-2]。

1.3. 活動体制

平成１９年度は３つのＳＷＧを構成した。情報セキュリティリスク研究ＳＷＧでは、安全安心なＥＣのインフラを脅かしている要素とそれに対する関係機関を含めた様々な取り組みに対し、消極的・受身的ではなく、積極的・戦略的に対策していかなければ、今日の情報セキュリティを脅かすリスクに対しては対応できないことを提言する。情報端末セキュリティ検討ＳＷＧでは、情報端末やネットワークが多様化するＥＣ環境において、組み込み型ソフトの脆弱性とその影響の大きさから、端末、ネットワーク、サーバにおける提供者の責任分解点を検討し、それぞれの開発者が意識すべきことだけでなく、それらの異なる業種間での情報連携や事故時の対応検討の連携組織の必要性を提言する。情報セキュリティガイド作成ＳＷＧでは、企業（大企業・中小企業）、政策部門の意識調査を行い、情報セキュリティ対策に対する意識が消極的・形式的になっていないか、積極的・戦略的にするには、どういう点を改善することをガイドとしてまとめていくべきかを検討し、この３年間の活動のエッセンスをまとめた。

■サブワーキング(SWG)構成

サブワーキングの活動と関係を図 1.3.1 に示す。

－情報セキュリティリスク研究 SWG（SWG１）
－情報端末セキュリティ検討 SWG（SWG２）
－情報セキュリティガイド作成 SWG（SWG３）

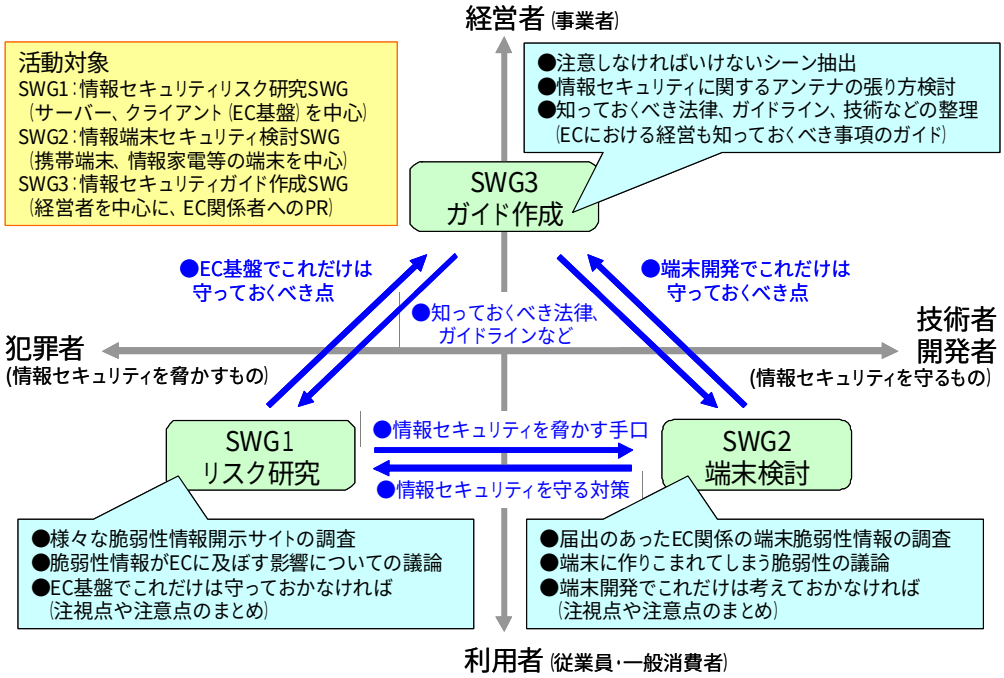


図 1.3.1　サブワーキング活動とサブワーキング間の関係

1.4. 活動経過

活動経過を以下に示す。

表 1.4-1　情報セキュリティ WG の活動経過

期日	活動内容
平成 19 年 6 月 29 日	第 1 回情報セキュリティ WG
	・メンバー紹介 ・経済産業省 情報セキュリティ政策について（METI） ・WG の活動概要、スケジュール、SWG 活動について
11 月 15 日	第 2 回情報セキュリティ WG
	・各 SWG の提言内容と報告内容(目次、纏め方)について
2 月 27 日	第 3 回情報セキュリティ WG
	・SWG 活動報告と提言、 ・WG 成果報告(ECOM ﾌｫｰﾗﾑ 2008)について

参考文献･資料

[1.2-1] 平成 17 年 ECOM 活動報告「情報セキュリティ懇話会」, ECOM Journal2006
[1.2-2] 平成 18 年 ECOM 活動報告「情報セキュリティ懇話会」, ECOM Journal2007

2. 情報セキュリティリスク研究 SWG 活動報告

2.1. 活動概要

（1） 目的

情報セキュリティにおいて、システムの脆弱性情報は、様々な形で公表されているものがあるが、それについて EC 内企業関係者が見聞きする機会は少ない。この SWG１では、そのような脆弱性情報の発生源について調査を行ない、関係するサイトなどの情報交換を行ない、実務的な情報セキュリティのリスクを研究した。

その公的なものとしては、JVN（Japan Vulnerability Notes : http://jvn.jp/index.html)[2.1-1]があり、その有識者から意見を聞くと共に、以下の活動を行った。

（2） 活動方針

活動は以下の方針で行った。

Step1 ： 発生元情報を見る（どのように脅威、危機と感じるかを議論する)。

Step2 ： EC に及ぼす影響を検証、評価する。

Step3 ： こうならないために、経営者や技術者がこれだけは進めるべき応対を纏める。

（3）活動経過

活動経過は表 2.1-1 の通りである。

表 2.1-1 情報セキュリティリスク研究 SWG の活動経過

期日	活動内容
平成 19 年 7 月 25 日	第１回情報セキュリティリスク研究ＳＷＧ
	・JVN(Japan Vulnerability Notes)について（JPCERT/CC) ・脆弱性情報の発生元「2003 年 8 月 MS/BLASTER ワーム発生」
8 月 27 日	第２回情報セキュリティリスク研究ＳＷＧ
	・脆弱性情報の発生元『脆弱性フレームワーク』
10 月 16 日	第３回情報セキュリティリスク研究ＳＷＧ
	・脆弱性発生元の情報に関する課題設定と討論
10 月 25 日‐26 日	BLACK HAT Japan 2007 参加（情報セキュリティリスク研究ＳWG）
11 月 15 日	第２回情報セキュリティＷＧ
	・各 SWG の提言内容と報告内容（目次、纏め方）について
12 月 12 日	第４回情報セキュリティリスク研究ＳＷＧ
	・インターネットトラブルについて(EC ネットワーク) ・報告内容と提言内容について
	第４回情報端末セキュリティ検討ＳＷＧ
	・提言内容（情報端末での責任分解点とあるべき姿）について

（４） 活動内容

下記の観点で参加メンバーとの議論を行った。

■ 発生元情報を見る（どのように脅威、危機と感じたか）

＞インターネットは安心して使えるものなのか

■EC に及ぼす影響（どう考えるか）

＞この２－３年に様々な社会問題を起した。

■こうならないために、経営者や技術者がこれだけは進めるべき応対

＞「形式」から「戦略」への転換

以下では、本ＳＷＧの活動を通して得られたメンバー間での共通認識を纏めて示す。

2.2. セキュリティインシデント

2.2.1. ＥＣ環境の変化と事件･事故の状況

経済産業省、ＥＣＯＭが共同で発表した「平成１８年度電子商取引に関する市場調査」（平成 19 年 5 月 11 日発表）によれば、インターネットを利用した日本の電子商取引は、企業間（BtoB）規模が 147.9 兆円、ＥＣ化率（国民総生産に対する割合）が 12.6%、消費者向け（BtoC）の市場規模が 4.4 兆円、ＥＣ化率が 2.0%である。日米比較で、日本の電子商取引は、企業間（BtoB）の EC 化率は米国（5.7%）の２倍、一方、消費者向け（BtoC）のＥＣ化率は米国（2.4%）に半分である[2.2-1]。

総務省が毎年発表している「通信利用動向調査」[2.2-2]によれば、世帯、企業及び事業所(5 人以上)へのインターネット普及率は平成 15 年から 80%を越え、平成１７年度末には 90%近くになっている。また、平成 18 年度のインターネット利用者人口は推定で 8754 万人(68.5%)となっている。

近年に起きた大規模な情報漏えい事件としては、平成 17 年 6 月の「米国におけるカード情報流出が挙げられる。国民生活審議会個人情報保護部会（平成 17 年 7 月 14 日）での報告によれば、米国で起きた情報漏えいの日本の利用者への影響は、流失の可能性がある会員数が 76,864 名、不正使用件数が 822 件、被害額が約 12,900 万円である。一方、国内でもいろいろな情報漏えい事件は起きている。「個人情報の保護に関する法律の施行状況の概要」(平成 18 年 6 月 30 日公表)によれば、１７年度に事業者が公表した個人情報の漏えい事案が 1,556 件にも及んでいる。こうした個人情報の情報漏えいは、民間(事業者)のサーバなどから起きているだけでない。公共機関関係者の自宅 PC などからも PtoP ソフト(ファイル交換ソフト、例えば Winny)やスパイウェアなどによって発生しており、色々な情報が様々な所から漏えいしている。

ＥＣでの取引金額(特に企業間)は飛躍的に増えてきたが、国を超えた営利目的の組織的・分業的な犯罪も出現し、情報セキュリティ対策の弱いところから情報が流出し、その被害は突然色々

な形で襲ってくる。インターネットが国民全体に拡がりを見せたものの、利用者全体が安心してＥＣを利用できる環境であるとはいいがたい状況である。

（1）セキュリティインシデント

最初に、セキュリティインシデントという用語について、説明する。ここでは、情報セキュリティインシデントと同義と考えてよいので、JISQ27002(ISO/IEC17799 から 2007 年７月に ISO/IEC27002 に番号変更)の定義から引用する。

“望まない単独若しくは一連の情報セキュリティ事象（event）、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率の高いもの”、即ち、実際に起こってしまった事件や事故だけでなく、発生の予測される事象も含むことになっている。しかし、ここでは、既に発生した事件・事故を主に扱うことにする。

まず、その情報セキュリティに関しては、話題に上るようになった、１９９０年代以降の動向から説明を始める。

（2）全般的な動向

2000 年以降、インターネットを利用する中で、多くの情報セキュリティの事件・事故が発生してきているが、当初の単純なウィルスや侵入からもっと複雑なやり方でのインシデントへ移ってきている。その変遷について、IPA の資料では、４つの段階に分けて考えられる。

第１期（～1990 年代）のパソコンが一般に普及し始めて、フロッピーなどで感染する被害が限定的な時代で、その目的も愉快犯の能力誇示が中心だった。

第２期（2000 年～2003 年）としては、インターネットの普及で、被害の規模も拡大し、攻撃側もウェッブ上で情報共有が進んで来た時代である。この時期には電子メール添付型のウィルスが発生してきて、ネット上で攻撃ツールが容易に入手できるようになってきた。このころには、政治的な意図をもってホームページの書き換えや DoS（Denial of Service）(バーファーオーバーフロー攻撃）も行われるようになり、防御側も、ウェッブやネットワークの設定を適切に行うことが必要になってきた。

第３期（2003 年～2004 年）では、ソフトウェアの脆弱性の問題が顕在化し、その脆弱性を悪用したウィルス・ワームが作られるようになり、その機能も高度化してきた。このころには、インターネットの普及で、システムが会社などの組織の情報基盤として使われることが一般的になり、その被害の拡がりが急速で、大規模な感染で、被害が深刻化してきた時期である。

第４期（2004 年～）では、経済的な動機（なりすまし・詐欺）や攻撃側が組織化。分業化が行われるようになり、手口も高度化・複合化してきた。その方法も、スパイウェア、フィッシング、ボットといった一層高度化した手口がとられるようになった。

それを表にまとめると、以下のようになる。

表 2.2-1. ITにおける脅威の変遷

背景	手段	脅威
1990 年代 第１期：パソコンの普及	記録媒体感染型ウィルス	愉快犯、限定的被害
2000 年～ 第２期：インターネットの普及	電子メール添付型ウィルス ネットでの攻撃ツール入手	被害の大規模化 攻撃側の情報共有の進展
2003 年～ 第３期：脆弱性問題の顕在化	脆弱性を悪用したウィルス・ワーム	ウィルス・ワームの高機能化
2004 年～ 第４期：経済的動機	スパイウェア、フィッシング、ボット	攻撃側の組織化 手口の高度化・複合化

また、ＩＰＡは、2006 年度から、情報セキュリティ白書を発行しており、２００７年度版において、2006 年度の 10 大脅威をまとめている[2.2-3]。それらの脅威をそのままここにあげると、以下のとおりである。

表 2.2-2. 10大脅威

第１位	漏えい情報の Winny による止まらない流通
第２位	表面化しづらい標的型（スピア型）攻撃
第３位	悪質化・潜在化するボット
第４位	深刻化するゼロディ攻撃
第５位	ますます多様化するフィッシュイング詐欺
第６位	増え続けるスパムメール
第７位	減らない情報漏えい
第８位	狙われ続ける安易なパスワード
第９位	攻撃が急増する SQL インジェクション
第１０位	不適切な設定の DNS サーバを狙う攻撃に発生

IPA:情報セキュリティ白書 2007 年度版より

2006 年度と比べると、SQL インジェクションが第１位から第９位に下がっているものの、その他の脅威は変わっていない。

これらは、2007 年 10 月に行った NRI での過去１年間の情報セキュリティインシデントの結果を見た場合、そのインシデントが発生した企業が、58.6%から 69.6%とかなり上昇している。

更に、海外では、FBI-CSI が毎年出している報告書“ CSI Survey 2007(12th Annual Compute crime and Security Survey)"があり、報告者の７０%以上が何らかのインシデントを受けており、その詳細をみると以下のような要因が挙げられている。

表 2.2.2. 情報セキュリティインシデントの要因

Insider abuse of Net access	59%
Virus	52%
Laptop/Mobile device theft	52%
Phishing where your organization was fraudulently represented as senders	26%
Instant messaging misuse	25%
Denial of service	25%
Unauthorized access to information	25%
Bots within the organization	21%
Theft of customer/employee data	17%
Abuse of wireless network	17%

FBI-CSI：“ CSI Survey 2007(12th Annual Compute crime and Security

2.2.2. ECOM 情報セキュリティ WG で取り上げた事件･事故

ここまでは、様々な組織が、色々な形で、情報セキュリティの発生状況について調査しているこのような状況の中で、今回の ECOM・情報セキュリティＷＧの中で紹介されたセキュリティインシデントの幾つかの事例を紹介していく。

7月25日 第1回 SWG2

組込機器における事例がその後の対策と共に報告された。

（事例１） DVD レコーダがスパムメールの踏み台にされた事例

（事例２） 携帯電話のウィルス
（2005 年 9 月に Symbian OS を搭載した携帯電話で猛威をふるった。）

（事例３） ATM,POS 端末ウィルスの感染（2003 年 8 月の「MS Blaster」等のウィルスが、金融機関の ATM や POS 端末などの専用システムまで感染が広がった。）

8 月 27 日 第2回 SWG2

追加の事例として

（事例４）Apple 社のビデオ iPod に WINDOWS ウィルス（RavMonE.exe）が混入との報告があった。

10 月 16 日 第3回 SWG3

発表「個人情報漏えいインシデントの調査と分析」の中で「情報セキュリティインシデント被害額算出モデル」を使って、「Yahoo!BB」及び「TBC」を事例として被害額を算出した。これは、NPO 日本ネットワークセキュリティ協会が 2007 年 10 月に発表した 2006 年の情報セキュリテ

ィインシデントに関する調査報告書[2.2-4]にまとめたものの抜粋である。この報告には、個人情報漏えいのインシデントの一覧表が掲載されており、2004 年から 2006 年の想定損害賠償額は全て 4,000 億円以上になっており、個人情報が漏えいした場合、企業としてかなりの負担になる可能性を予見するものである。

11 月 15 日 第2回情報セキュリティ WG

有限責任中間法人 EC ネットワークより ECOM ニュース[2.2-5]に掲載された「インターネットトラブルの解決に向けて」という題目で講演があった。このなかで、インターネット詐欺対策集としてよくあるトラブル事例[2.2-5]が紹介されている。

ここで、更に、電子商取引におけるトラブルの実例を紹介していく。

（事例 5） ワンクリック詐欺

国内においてワンクリック詐欺が確認されている。これは、ワンクリックウェアといわれるスパイウェアを利用して行われるものである。ワンクリック詐欺は、アダルトサイトといった年齢制限を設けているウェッブサイトでよく見られる詐欺手法で、その手順は次の通りである。

1) 年齢制限を設けている Web ページを表示させる際にダイアログでこっそりと有料である旨を記載し、ユーザに同意させる
2) ユーザが同意すると、アニメーション GIF、Flash を表示し、あたかも個人情報を取得されたかのように錯覚させる
3) IP アドレス、プロバイダといった情報を表示させ、登録が完了したとし、ユーザに登録料を入金させる

ワンクリックウェアは、手順の(1)の段階で簡単にインストールされ、アイコンが動画ファイルを想起させるようなものに偽装され､実行しやすいような工夫がされている｡インストール後は、定期的にポップアップで入金を促すようなメッセージを表示させる。

また、インストールさせるまでの動作や挙動は、海外のスパイウェアと類似しているが、スパイウェアのようにコンピュータ上の情報を外部に転送するのではない点が異なる。
このようなマルウェアは今後も増加傾向あることが推測される。

（事例６）Winny による情報漏えい

情報漏えい事件で盛んに取り上げられていた Winny や Share などの P2P ソフトウェアは、決して新しい技術ではないが、ファイル共用化によって無料で電子データがダウンロードできるという利便性から利用者が急速に増大した。更に大量の個人情報の漏えいに興味をもち、悪意のある人間によりその悪用も行われるようになった。

2006 年１月から６月において、Winny 及び Share からの情報漏えい事件は相次いで報告された。2006 年に入り、Winny を取り巻く環境は大きく変化し、各セキュリティ製品ベンダーから次々と対策ツールが公開された。しかし、いずれの対策案も製品単体では完全に防ぎきることができず、また、対策を施していないユーザが多く存在するために、この原因によって情報漏えいを発生させるユーザが後をたたない。

（事例７）巧妙化するフィッシィング詐欺

フィッシング対策協議会より ECOM ニュース[2.2-6]に掲載された「巧妙化するフィッシィング詐欺」という題目で講演があった。

2005 年くらいからフィッシング(Phishing)という言葉がメディアで報道されるようになった。2004 年 11 月に大手クレジットカード会社を装った日本語のフィッシィングサイトが出現し、日本で初の実被害が発生し、昨年後半よりインターネットバンキング、オークションサイトなどのフィッシィングサイトが日本国内での顕在化するようになってきているものである。

従来は、偽装されたメールやサイトの日本語の文言が片言で稚拙であったが、最近はかなり巧妙になった。

フィッシィングテクニックとしては、スパム、なりすまし、ハッキングなどがありますが、スパムメールに大手のサイトのロゴの一部分をメールアドレスに使う、アドレスバーやステイタスバーなどを詐称して、不正に情報をえるなど巧妙な手口が使われている。また、「あなたのアカウントは切れてしまいます。至急、更新をしてください」などと言葉でだます手口、メールのタイトルや本文に工夫を凝らし、相手を焦られて、偽サイトに誘導する手口なども行われている。最近では、スパイウェアを利用し、無作為に情報を盗み出すのではなく、銀行や大手モールのサイト名やターゲットとなる URL が入力されると効率よく情報を盗み出すことも行われている。

現在、このような状況を受けて、なりすましの対象となる金融機関などの企業とフィッシィング対策などのソリューションを提供する企業が集まって、フィッシィング対策協議会[が設立され、協議会メンバーや個人から送られてくる情報（フィッシングメール）を収集、分析して、あたらしい手口などの情報を提供している。

（事例８）　偽装セキュリティソフト

偽装セキュリティソフトについては、EC ネットワークやフィッシング対策協議会などから紹介された、2006 年 8 月頃になって多発した事例である。サイトを見ていると、突然、「あなたのパソコンはウィルスに感染しました。これを除去するためにはこのソフトを買ってください。」というメッセージが表示され、偽装セキュリティソフトを買わせるという詐欺である。ダウンロード（クレジット決済）後、偽装セキュリティソフトであることに気づき、ソフト自身をアンインストールし、スパイウェア対策ソフト等で関連ファイルを除去したが、「今後も更に請求等が来るのではないか」という不安がつきものである。このソフトを売っているのは海外の事業者で、対処が難しい。そのソフト自体は、は役に立たないもので、ソフト代金は、クレジットカード会社にチャージバック請求しても、クレジットカード会社に対応の差があるために救済されるケースされない場合がある。

2.2.3. 営利的な犯罪の進化と連携

（１）犯罪の巧妙化

JNSA からの報告[2.2-5]でも、上記の偽装セキュリティソフトは、2006 年 2 月頃になって、日本語バージョンのウインアンチウィルスプロ２００６というソフトまででている。さらに、その年の 8 月から 9 月にはシステムドクター２００６、つい最近ではドライブクリーナー２００６と

いう日本語版ソフトがでている。これらのソフトは、サイトの広告などをクリックすると、いきなりスキャンが始まり、スキャンが終わると「あなたのコンピュータは問題があるので！これをインストールしてください」という警告メッセージが出る。5 千円位なのでついお金を払ってしまっている人が多いとのことであった。詐欺的な行為で、年間使用料を自動更新する場合もあり、クレジットカード（番号)を切り替えるなどの自衛措置を取ることも必要である。

（２）犯罪組織の連携

これまでの活動での話を纏めてみると、犯罪組織の連携は、図 2.2-1 となる。例えば、北米のソフトウエアー会社がスキャンはするが何もしないソフトを出す。ソフトウエア会社はペーパーインストール料を支払うことをインターネットでアフィリエイトを公募する。欧州にいるソフトを宣伝する人（アフィリエイタ）はアドウエアなどを、いろいろなサイトに仕掛けたり、メールに忍ばせたりすることによって、そのソフトをインストールするように一般消費者を誘導する。ソフト会社に登録料が入ると、アフィリエーターにパーパーインストール料が支払われる。

始めは、英語で普及拡大していたが、2006 年 2 月頃からは、日本語化が始まり、日本の一般消費者からの問合せが増えだしたと言う次第である。犯罪者側は、国境を超え、連携し、巧妙な手段と先進的なツールを利用して、日本の一般消費者に役に立たないセキュリティソフトをインストールさせているのである。

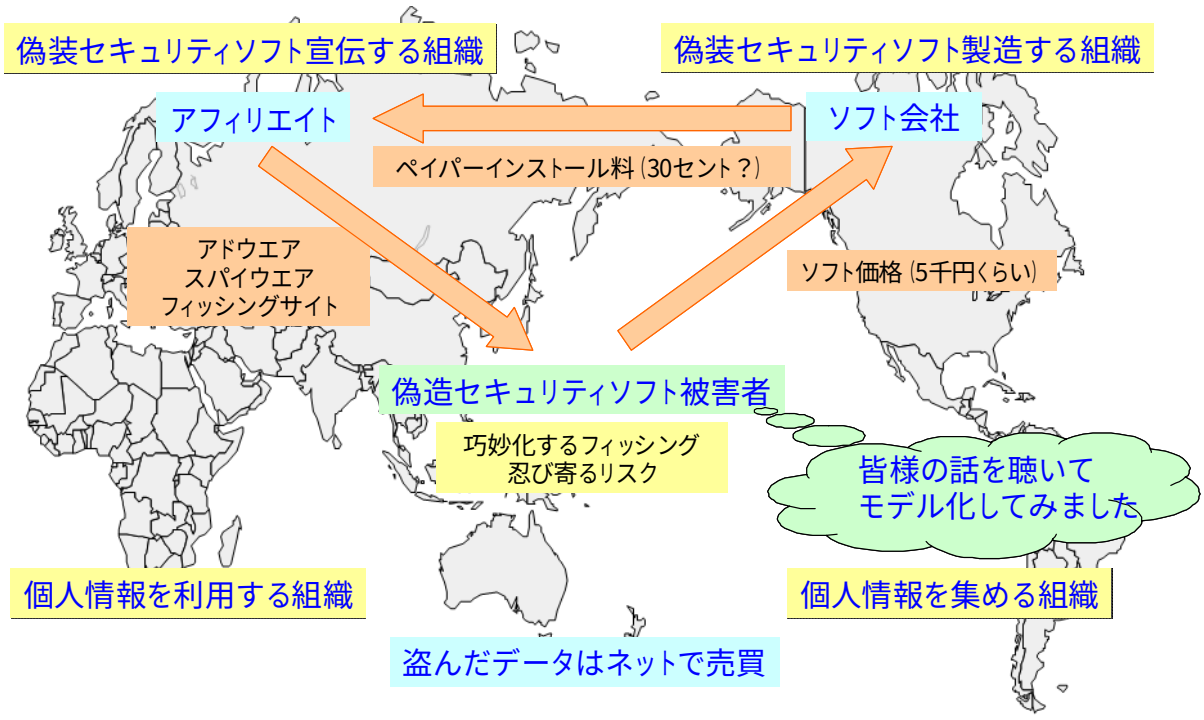


図 2.2-1　偽装セキュリティソフト問題

2.3. EC に及ぼす影響を検証、評価

ブロードバンド化が進み、携帯電話によるネットアクセスも広く行われるようになり、”ザ・インターネット ” が EC のプラットフォームとして定着し始めている。さまざまなビジネスがインターネットを使っておこなわれるようになり、金品すべてが電子情報という事例も多くなってきている。

しかし、インターネットでよく使われているメールや WEB などのツールがもつ特性を、そのリスクとともに理解されて使われているのであろうか。EC・ビジネスの道具として、どこまで信頼し頼りにしていいものなのか、万が一のときに意図する行動が取れるのであろうか。

技術的側面からインターネット関連の事件事故を鑑みるに、非常に危うい取引をしているのではないかとの懸念から、懇話会、セキュリティワーキングにおいて検証、評価をおこなった。

インターネットを使っている利用者は、必ずしもインターネットを正しく認識していないのではないのか。 安心、安全に対する幻想を抱いてはいないか。「電子メール」、「WEB サーバとの通信」を取り上げ、技術的にどのように情報交換が行われているのかを明らかにした上で、一般消費者の視点、サービス提供者の視点から、EC としておこなわれている行為の安心、安全を議論した。

2.3.1. EC に及ぼす影響を検証、評価

（1）電子メールの危うさ

2006 年初頭に起きた「ライブドア 堀江メール」の事件は、国会運営も左右する大きな事件となったが、その争点となったのは一通の電子メールの真偽であった。事件そのものは『本物と断定できない』ということで、情報は偽物として扱われ収束していったのであるが、たった一通の電子メールの真偽を判定する社会的共通規範がないこと、その規範が形成されることなく事件、話題は収束し、今もって電子メールの真偽判定はできないという状態が残されたのである。

ニュース報道を通じて伝えられる一般の意識、価値感覚においては、

- 一通の電子メール真偽を判断する共通認識が存在しない
- どう真偽判断すれば良いのか、方法論、分析手法が明確になっていない

ということがうかがい知れた。郵便物では議論できる、消印や筆跡など真偽や証拠の裏づけの取り方に値するものが存在していないのである。

情報セキュリティ懇話会において、「電子メール」の仕組み【RFC821】の検証とともに、簡単なツールをつかって「偽メール」を出す実験をおこなった。検証に参加した委員からは、ライブドア事件で争議されていた電子メールの差出人、メールツール名などでは真偽の分析ができないことが理解できたとき、電子メールの実体に対する自己の理解と現実の乖離に驚き、EC で電子メールを利用する危うさを認識した。

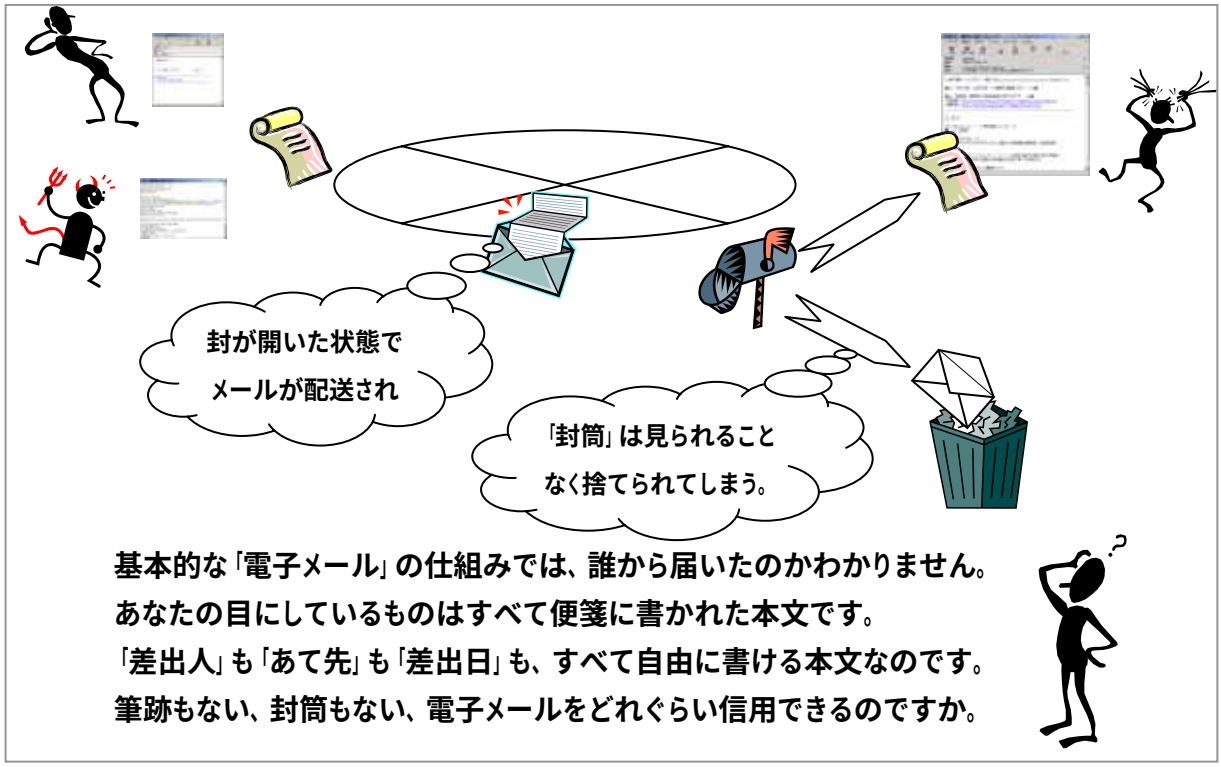


図 2.3-1　メールの真偽を見分けるのは困難

検証結果：

・「電子メール」は、便箋に書かれた本文をやり取りしている。
　差出人、差出日時、使っているソフトウエア... など、利用者が手に出来る情報の全ては、
　偽りの可能性が否めない状態。
・現実世界の封筒にあたる情報は手にすることができない。
　配送情報(どこから届いたのか、誰がサーバにアクセスしたのかなど)は残らない。

この電子メールの特性は、「送受信された電子メールそれ自体では、本物、偽物 は判別できない。 受信後に書き換えられていたとしても、書き換えられた事を認識できない。」ということを示しており、EC における確認や証拠として使うには、そのままでは非常に危ういと認識される。

（2）インターネット通信の特徴

インターネットで使われている情報伝達の技術のほとんどは、「ハガキ」とおなじ状態で電文を取り扱うことになっている。誰と誰がどんな情報伝達をしているのかを含め、覗き見ようとする行為に対して弱い物となっている。さらに、伝達の途中で書き換えられてしまったり、差し替えられてしまっても検知することもできない。（電文が壊れてしまった場合の検知はある。）

WEB サイトで品物を選び、電子カートに載せ、レジでクレジット決済という流れ出の WEB ショッピングが一般的になってきているが、こんな状態で本当に「安心」「安全」なのだろうか。安心、安全を謳う SSL の暗号化がなされている WEB サイトを想定し、その技術を検証した。

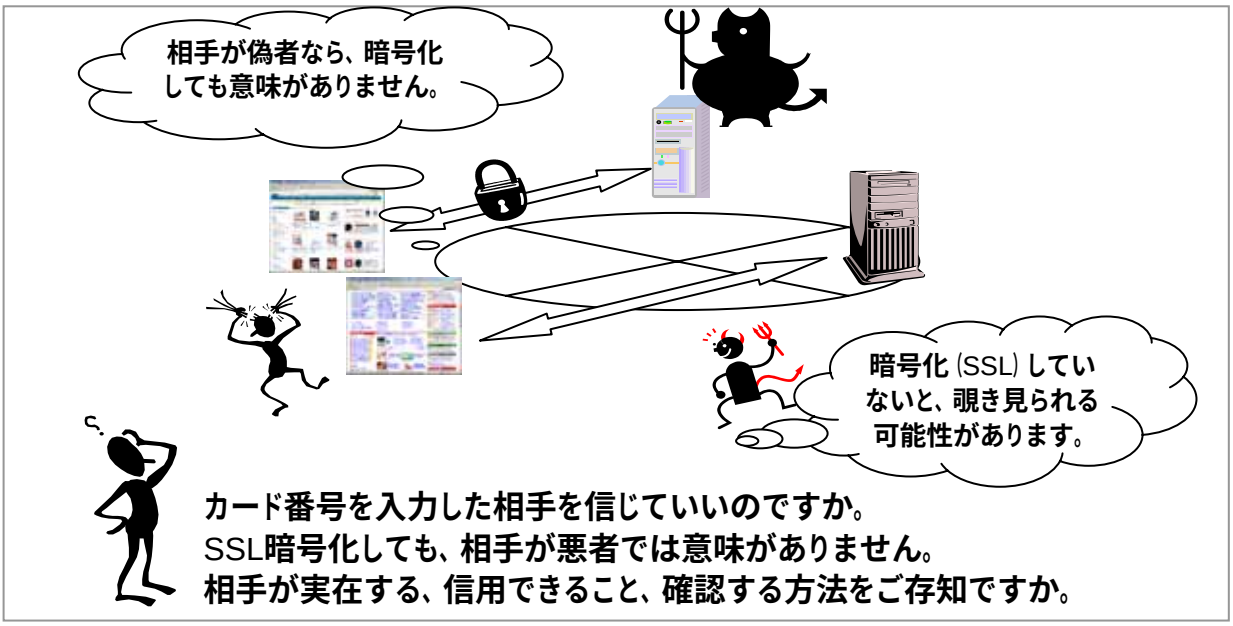


図 2.3-2 インターネット通信の特徴

検証では、本物を騙る偽物のサイトを用意し、本物なのか、偽物なのかどうすれば見分けられるのかを委員とともに評価した。「暗号化」については、ほぼ統一的な見解があり、SSL による暗号化（https://..となること）への理解には問題がなかった。しかし、相手が本物であるかを見分ける方法についての理解にはばらつきがあり、WEB ブラウザを使ってのサーバ証明書の確認を始めて聞いたというものもいたほどであった。また、第三者機関の認証を得ていない通称「オレオレ証明書」に対するブラウザからの警告に対する注意が薄く、せっかく偽物である可能性が通知されても、気がつかずに重要情報の入力へと進んでしまうことが多々ありえることが明らかとなった。

検証結果

・通信のほとんどは平文で行われている。
・「SSL」等の暗号化が出来ていないと、通信は簡単に傍受されてしまうとの理解は十分。
・「SSL」が通信相手の認証機能を持ち合わせている事実への関心は薄く、広く普及しているも、サーバ証明書をどう検証するのかの理解は進んでいない。

情報セキュリティ懇話会・WG において、電子メール、WEB 技術の簡単な確認を行い、

- 「偽」電子メールが簡単に作れること。
- 受信メールだけでは真偽がつかず、発信日、受信日、発信元すら信用できないこと。
- SSL で暗号化通信が出来ても、必ずしも正しいサイトとは限らない事
- 「オレオレ証明書」なるもので簡単に暗号化ができること。

がインターネットの「特徴」であることは、これを知らずして過信することは EC において大きな問題であると認識した。

また、これらの検証、実証が、簡易なオープンソースソフトウエア(フリーの UNIX とこれに附属の TELNET、OPENSSL)によって、低コストで実現できたことが開示されると、驚きとも

に EC に対する脅威はどこからでも発生するとの認識が芽生えた。

（3）インターネット上には、誰でも使える「悪い」サイト、ツールが存在する

簡易な道具・ツールで出来る事は、通常の利用方法下とは異なるいくつかの前提条件が必要な事は確かである。実験で明らかとなった特徴に気を付け、適切なツールを使う事で、「事故」や「悪事」を回避する事が出来ると考えられる。

実生活でも、「ハガキ」をもらって、そこに開いてある事だけを信じて行動することは少なく、電話で確認したり身の回りの人に相談したりなど、他の情報もつかって裏付け行動を行うものであり、同じようにインターネットでも複数の手段で真偽を確かめていく必要がある。

しかし、このような防衛策も乗り越えてしまうような、道具・ツールを配布するコミュニティが、同じインターネットに存在している。巧妙な「偽物」の作り方や、なりすまし方の議論、防御を破る直接的な攻撃方法を伝授する情報源も存在している。これらはインターネットをつかった EC の安心、安全に影響を及ぼしているといえる。

適切に設定できていたとしてもこれを破るものがあるということを検証するため、無線 LAN を題材に取り上げ、使用許可が与えられていない PC が、勝手にアクセスポイントに接続出来るとするインターネット上の情報を検証した。

ツールのほとんどは、開発者向けの動作確認用メンテナンス用ソフトウエアが基本となっていたが、そのツールを組み合わせ、のっとりの肝となる暗号解読のプログラムが付け足された構成で無線 LAN 攻略のサイトで配布されていた。おなじサイトに、これらのツールの組み合わせ方とアクセスポイントをが記録された「ビデオ」があることを発見した。その内容は実践的で少しの知識があれば、誰でも無線 LAN のセキュリティを突破できるレベルのものになっており、誰でも簡単にセキュリティを破る可能性があるということを実感したのである。

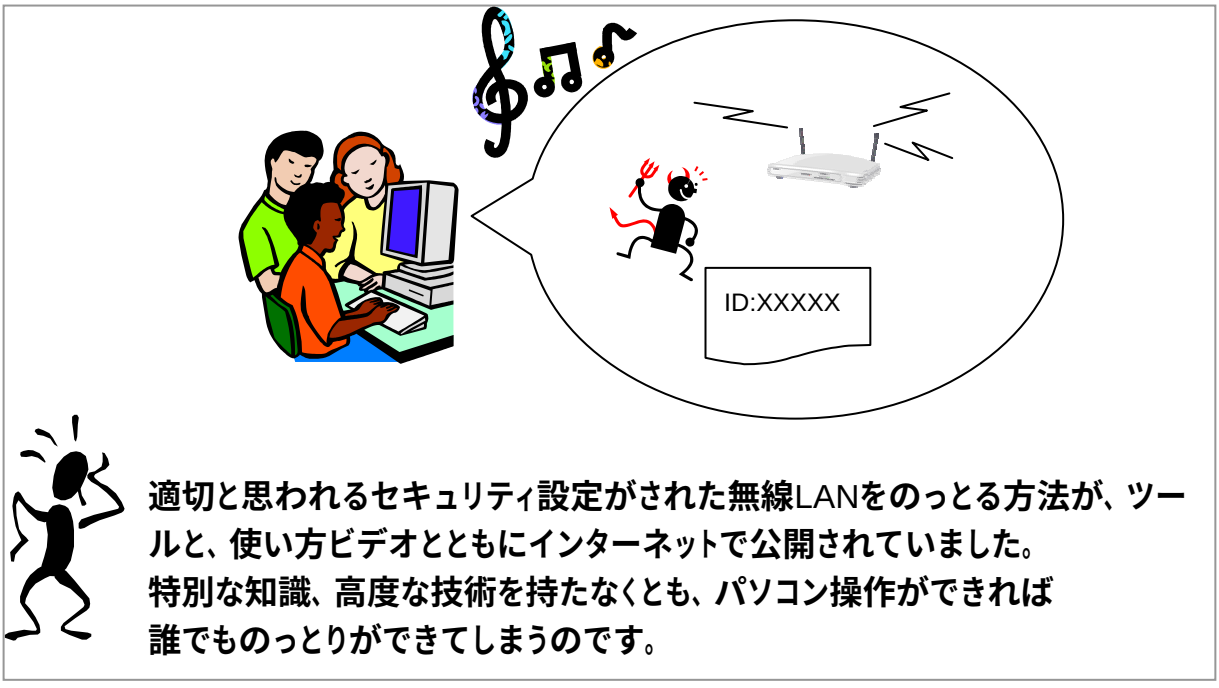


図 2.3-3 誰でも使える「悪い」ツールのサイト

検証結果：

- 無線 LAN アクセスポイントに付されたセキュリティ設定を迂回する方法が開示されたツールが存在し、使い方ビデオも存在していた。
- 利用者を限定する為に暗号化設定を付していても、その暗号が簡単に解けてしまった。

ビデオの中で使用されている道具・ツールは、CD 一枚にまとめられ、ノート PC 一つあれば、簡単にビデオの内容を再現可能である事が確認された。さらにこのビデオは複数の言語版があり、日本語で解説されているものもあった。専門家でなくても、他言語に弱い若年層においても、PC の操作ができれば無線への攻撃操作ができる事に気が付き、簡易なツールはさらに EC への脅威となることが容易に想像された。

2.3.2. 利便性とリスクの混在

EC を支えるインターネットには、EC を脅かす情報も同居していることを意識しなくてはならない。技術はあくまでも道具であり、どう使うかによって便利にもなり脅威にもなりうるということである。

（1）ソフトウエアの脆弱性が問題なのか

これらの事実を目の当たりにしたとき、「メールやブラウザがもっとしっかりしていれば…」、「インターネットをもっと安全にすることで…」という論調になっていく向きも少なくはなが、使う人についても考える必要がある。

前述の情報の真偽判定、取引相手の存在確認、潜在的な危険性は、インターネット特有のものではなく、実社会に取引においても課題であり、常に注意深く真偽を意識し、内容を確認し、危険を回避するための行動は各人がとっているものである。商売の道具立てが、物理的、直接的な方法から、仮想的、間接的なインターネットに変わったとしても、取引を成立させるために必要な基本的な事項は変わることはなく、最終的には取引をする個人の判断により成立していく事を忘れてはならない。どんなに便利なインターネットの技術、ソフトウエアであっても、使う人の意識が欠如していれば EC の「安心」「安全」は実現不可能である。

インターネットはひとつの手段であり、ソフトウエアも一つの構成要素でしかない。たとえそこに脆弱性や機能的に至らないものがあったとしても、逆に使う人の工夫と道具の組み合わせにより、相応の安心と安全を手にすることは可能である。

（2）「情報セキュリティ」としての問題と捉える。

「情報セキュリティ」として、個人データ、売買、決済、プライバシー... などの情報を、事件、事故から守り、安心して EC・電子的な取引をおこなうためには、商売する売り買い双方で 実世界と同様に用心深く行う必要がある。インターネットは便利であるが、期待通り、予想通りに結果だけをもたらしてくれる物ではない。目に見えない分、不正が行われたり、不利益をこうむるような落とし穴があるかもしれない。便利さに目を奪われ、せっかくの警告を盲目的に無視したり、面倒であるということから読み飛ばしたり、言われるがままに「OK」のボタンを押しては

いけない。「警告を無視せよ」という言葉を疑っていくことが必要なのである。

クレジットカードの番号を入力や会員登録をおこなうサイトで、SSL という暗号化手法がよく採用されている。PKI の技術をもちいており、サイトが第三者により確認されていることを、理論的に証明することが可能となっているため、サイトの存在確認、さらにはサイト運営者の認証としても使われている。認証局と呼ばれる第三者機関が、サイトの運営者とサイトの存在確認をおこない、電子証明書を付与することで利用者はサイトを確認できるのである。

技術的には証明書を作ることは難しいことではなく、前述の検証・評価で用いた OPENSSL というフリーソフトを使っても、自由に証明書を作ることが出来る。この場合、第三者機関を自らかねることで証明書を作るため、自分が自分を証明する、「オレオレ証明書」と呼ばれる証明書ができあがる。第三者の証明が必要のない場面、研究室や開発途中で用いられたりしている。

オレオレ証明書は、一般的に使われるブラウザでアクセスすると、正しく証明されていないという警告が表示され、利用者に証明書が間違っている・サイトは信頼が置けないとして接続継続の確認が求められるようになっており、詐称に対する防御機構が組み込まれている。この警告を無視することもできるようになっており、信じるか否かは利用者の選択に任されている。判断は利用者がするのである。

「警告を無視せよ」というサイトの案内に従い、そのまま続けてしまえば確かに暗号化通信が始まり、覗き見される危険は回避される。しかし、サイトが第三者に認められた本物であるかの保証はそこでなくなる。警告が出たり不安を覚える動きをした、いつもと違う画面が出た場合には、そのまま続けるのではなく、信頼してよいのか、継続してよいものなのか、確認、判断を行っていかなければならないはずである。

2.4.「脆弱性」の一般化

パソコンのセキュリティといって、具体的に実行する操作として広く認識されている内容は「アップデート」ではないだろうか。また、アップデートを促す動機付けとして、「脆弱性」という言葉もよく聞くようになってきている[2.4-1]。

身近なセキュリティ対策として、やらなければいけないことはと問えば、

- 使っているパソコンにはパッチ適用をしなければならない。
- ウイルス対策ソフトもウイルスデータの最新化をしていかなければいけない。

というところであろう。

情報セキュリティとしてとるべき対策はなにかと問われたときも、「パッチ適用」「ウイルス対策」が基本的な事項として挙げられるのであるが、このような対策が一般化したのは、2003 年に発生した「MS/BLASTER ワーム」による大きな騒動がきっかけだったのではないだろうか。

2003 年の騒動の原因となったワームはどこからきたのかを検証・追跡し、この事実から情報セキュリティとしてとるべき行動を議論した。

（1）「舞台裏」での出来事

ワームもウイルスも自然発生的に生まれてくるものではなく、人為的に生み出されているソフトウエアである。騒動の原因となった「MS/BLASTER」ワームが出現した下地を、ソフトウエアのバグ情報を扱うメーリングリスト、Bugtraq[2.4-2]の当時の記録からうかがい知ることができる。

Bugtraq は、SecurityFocus にて管理されるメーリングリスト。

> **SecurityFocus** is the most comprehensive and trusted source of security information on the Internet. **SecurityFocus** is a vendor-neutral site that provides objective, timely and comprehensive security information to all members of the security community, from end users, security hobbyists and network administrators to security consultants, IT Managers, CIOs and CSOs.
>
> 出典：seurityfocus[2.4-3]

このメーリングリストでは、さまざまなソフトウエアの欠陥、「バグ」の情報を、ベンダーの影響を受けない中立的な姿勢で取り扱う議論の場として存在している。こんな製品にこんなバグがあるという、善意的な姿勢での情報投稿、共有、対策検討がなされる場となっており、ベンダーの有償ソフトウエアからオープンソースのソフトウエアまで、ジャンルを問わずいろいろなソフトウエア製品について議論されていた。

2003 年 7 月、この Bugtraq で、マイクロソフトからの提供されたパッチ、MS03-026 の有効性に関する小さな議論が起きていた。概ねの議論は「任意のプログラムがリモートから起動される可能性がある。」ので、すぐにパッチを適用すべきという意見と、そのパッチは不完全であり無意味である、よってパッチを適用するのではなく根本的な解決を要求せよという意見の対立で、メーリングリストの性格上技術的な意見の積み重ねで議論は進んでいた。

最初の議論はパッチにより修正される範囲に関するおとなしいものであったが、対応できていない部分があれば修正していないことと同じであるという、パッチの意義を否定する強行な対抗意見が現れ、パッチを適用してもワームやウイルスに感染する恐れがあることを実証して見せるプログラム（PoC – Proof of Concept、実証コード）が、最終的に投稿されるに至った。

技術的な意見交換が多く、議論を証明するためとして PoC プログラムが投稿されることは良くある出来事であったが、この「欠陥」についてはプログラムが投稿された後も更に議論が白熱、Full-Disclosure というより過激なメーリングリストへと意見交換の場が移されていった。欠陥の証明であったはずのプログラムはどんどん洗練され、さまざまな言語、いろいろなバージョンの Windows で欠陥を証明、攻略できる能力を獲得してゆき、ほとんどの Windows を攻略できるプログラムが投稿されたところで、「これにワームプログラムを組み込むと大変な混乱を生み出せるのではないか？」という意見が出され、欠陥をつくことが及ぼす影響の大きさに気が付くという状況に至った。これが 7 月下旬のメーリングリストでの状況であった。

この数日後、8 月に入って早々、まさしくこの PoC に BLASTER ワームが組み込まれたと考えられる MS/BLASTER が、世界中のパソコンとインターネットを大混乱に陥れることになった。

この「MS/Blaster」は、ブロードバンドが普及し始めていた日本においては大変大きな反響があった。インターネットに繋ぐだけで感染する事から、対策パッチを入手しようとするとパソコンが使えない状態になるという大変困った事態を引き起こした。このため、対策パッチが入った CD が作られ無償で家電量販店、パソコンショップなどで配られる事態となり、新聞、T メディアでも大きく報じられ、「脆弱性」「パッチ適用」「ウイルス対策」が多くの人の知るところとなったのである。　どこから MS/BLASTER がやってきたのか？ 確定することは不可能であるが、当時のメーリングリストの記録と時間的な合致から、多くのコンピューターの専門家、ハッカーのコミュニティでの議論から生まれてきたのではないだろうか。

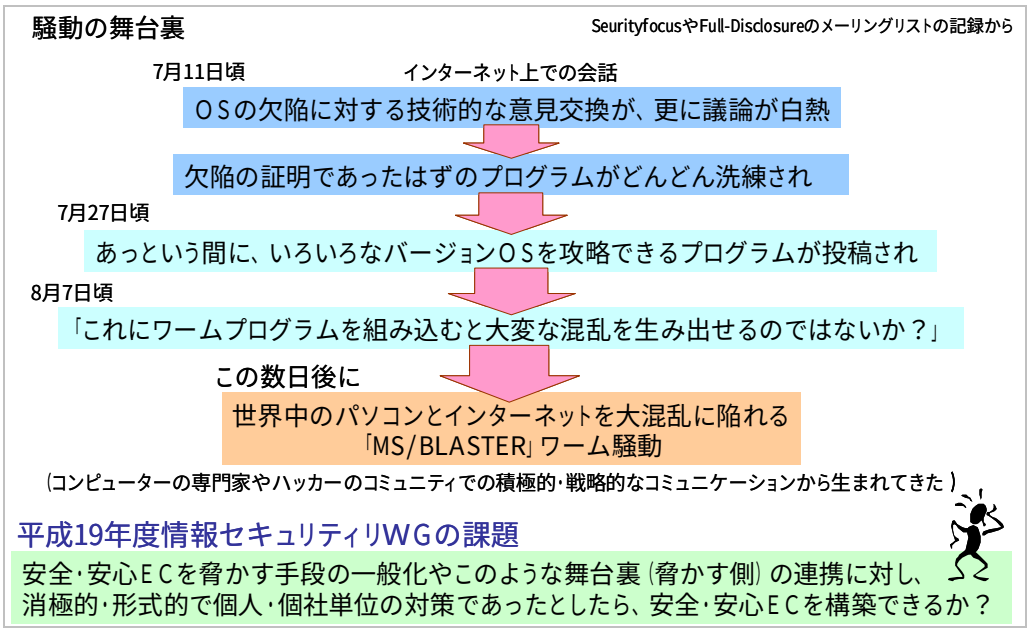


図 2.4-1　2003 年「MS/BLASTER」ワーム騒動の検証

ー「MS/BLASTER」ワーム騒動：2003年に世界中のパソコンとインターネットを大混乱に！ー

2.4.1. 「脆弱性」を利用する情報の展開

MS/BLASTER 騒動以降、セキュリティという言葉がメディアに現れると、ほぼ一緒に脆弱性、パッチ適用という言葉も目にするようになり、いままで積極的にはアップデートを行っていなかった人たちも、意識してアップデート、パッチ適用を行うようになった。「脆弱性」を放置することで、ウイルスやワームによる混乱が収束せず、自分のみならず皆に影響を与えるという意識も同時に認識された結果だと考えられる。

しかしながら、これほどまでの大きな社会的混乱はほとんど発生していないにもかかわらず、MS/BLASTER 騒動以降、たくさんの「脆弱性」が発見され、たくさんのパッチ、アップデートが発表され、同じようにたくさんのウイルス、ワームが生み出されつづけている。
この状況下「アップデート」をしていれば十分なのか、より意識的に能動的に対策を考えることが必要ではないだろうか。

（1）その後の「舞台裏」

バグ情報のメーリングリスト BugTraq も Full-Disclosure も、騒動とは関係なく同じように情

報交換が行われ、たくさんのバグ、脆弱性が報告され実証されつづけている。インターネット上のサービスの増加に伴い、議論の対象となるソフトウエア、サービスの数も拡大しており、活動はより活発になっていると考えるのが妥当である。

メーリングリストの活況からは、MS/BLASTER 騒動の再現が発生する下地は依然として存在しており、いつまた再演が行われるのかとの危惧もある。しかし、これらのメーリングリストは、セキュリティベンダや JVN のような脆弱性対応状況公開サイトの情報元ともなっており、大きな騒動になる前に注意喚起、対策実施が行われるようになってきている[2.1-1][2.4-4]。

また、脆弱性を利用した攻撃や悪事が、社会全体に対する愉快犯的なものから、特定の企業や団体を相手にした犯罪に利用されているとする傾向分析もだされており、大きな愉快犯事件の起きる可能性は少なくなるが、実害のある事件につながる可能性が増大しているとも考えられる。

バグ発見、脆弱性情報の議論は続けられており、いつまた… の可能性はなくなってはいない。

（2）より広く、より高度に

メーリングリストで行われていた議論は、ある程度の技術力がなければ読み解くことは難しく、誰もが実証コードを試してみることが出来るような状態ではなかった。しかし、前項で検証したように、脆弱性を探すツールやその使い方を解説するビデオがサイトにて配布されるなど、脆弱性を利用するためのハードルが下がってきているという実状が存在する。

近年では、サイトやツールの情報に解説を加え、インターネットに散らばるツールやテストコードを DVD に収めた本が出版されるなどしており、ネットに接続せずとも簡単に、解説を読みながら試すことが出来る状況になっている。当活動にて検証した無線 LAN の攻略についての情報も、インターネットに散在していた情報がまとめられ、無線を搭載したゲーム機に対する解説も加筆された上で出版されており、セキュリティを脅かす素地はより広く一般化している[2.4-5]。

「脆弱性が存在するか。パッチ適用により改善されたか」を検証するための「スキャナ」が無償で配布されており、脆弱性対策の効果測定を行うための有益なソフトウエアとして活用されている[2.4-6]。しかしこれは使い方によっては、攻撃可能なコンピューター、サイトを探し出すためのツールとなりうるものであり、サイトに対するスキャンは頻発している。

脆弱性を利用するプログラム断片と、断片を組み合わせてプログラムを生成するツールを配布するサイトも出てきている。このツールにより造られるのは、脆弱性の実証プログラム以上の効果をもつプログラムで、見方を変えればウイルスやワームを作り出すツールになる。ウイルスやワーム作成には、かなり高度なコンピュータに対する知識と技術が必要とされるが、このツールを使うと非常に簡単に新種のウイルスやワームを作り出すことが出来る。

2008 年 1 月、Winny を介してウイルスを流布したとして逮捕された（直接の逮捕容疑はウイルス作成、流布ではない）容疑者の手元からは、ウイルスを作り出すためのツールが発見されており、これを使って数百種類のウイルスを作ったとの自供もあり、実際にウイルス作成ツールが用いられ、数多くのウイルスが放たれている事実が垣間見えている。

2.4.2. 日本でも開催される BlackHat

コミュニティはネットだけではなく、情報技術に深い知識をもつ「ハッカー」の祭典とも称される BlackHat[2.4-7]や DefCon[2.4-8]など、互いの情報を発表しあう国際会議が開かれている。

メーリングリストやサイトでの議論とはちがい、顔を突き合わせての発表と討議となり、単なるソフトウエアのバグ情報披露会、実証討議ということではない。
セキュリティベンダ、ソフトウエアベンダの技術者が講師を務めることもあり、造る側、利用する側、双方の視点で、ソフトウエア、システムの「セキュリティ」の検討を行う場となっている。

特に BlackHat は、発表のみならず技術解説、講習も行っており、セキュリティに関する技術的な情報蓄積、収集の場ともなっている。DC、Europe、USA、Asia 各国で開催されており、2004 年から Asia は 日本で開催されている。今年度(2007 年)も日本・新宿にて開催された[2.4-9]。

BlackHat はセキュリティに関する技術的な学習をおこなう「トレーニング」と、研究成果を発表する「ブリーフィングス」の 2 部構成から成り、4 日間の日程となっていた。

（1） ハッカーの集いから、セキュリティの国際会議へ

「ハッカーの祭典」というフレーズからは、悪いことを企む集いのような印象を受けがちであるが、情報セキュリティ、インターネットセキュリティへの感心の高まりとともに、「セキュリティ」を考える上で重要な情報元であるという認識がなされるようになってきていると感じられた。開催前のインターネット関連メディア(パッチ情報等を取り上げている)での取り上げられ方、セキュリティを推進する団体からの支持を受けている事などが裏付けである。ブリーフィング開催初日に NHK の取材を受け、その当日に「セキュリティの国際会議」ということで TV 報道された事は、特に印象的であった。

（2）「技術」ではなく「影響」を考える

「ブリーフィングス」は基調講演と、2 トラック全 10 コマの発表から構成されていた。発表の全てが新規とは限らず、Asia のまえの USA、Europe にて既に発表されたものの再発表のものもあり、内容そのものの新鮮さを目玉にするのではなく、内容そのものを検討課題としているのではないかという意図も感じられた。基調講演を含めた、内容全体の傾向として、単にハッキング技法や脆弱性に関する情報交換ということではなく、技術が及ぼす社会的な影響や、インターネット社会、国際的な取り組みに対しての効果も考慮していこうという気概が感じられた。

参考文献･資料

[2.1-1] JVN（Japan Vulnerability Notes)：http://jvn.jp/index.html

[2.2-1] 経済産業省：平成 18 年度 電子取引に関する市場調査報告書(平成 19 年 3 月）
http://www.meti.go.jp/policy/it_policy/statistics/outlook/ie_outlook.htm

[2.2-2] 総務省：平成 18 年度 通信利用動向調査報告書(平成 19 年 3 月）
http://www.johotsusintokei.soumu.go.jp/statistics/statistics05.html

[2.2-3] IPA：情報セキュリティ白書　２００７年度版（2007 年 3 月 9 日）

[2.2-4] JNSA：【改訂版】2006 年度 情報セキュリティインシデントに関する調査報告書 ver2.0 (2007 年 10 月 11 日）

[2.2-5] ECOM：「電子商取引における利用者の声と忍び寄るリスクについて」, ECOM News No. 18(2006.9.29)

[2.2-6] EC ネットワーク：詐欺対策集、http://www.ecnetwork.jp/sagi/

[2.2-7] ECOM：「利用者に忍び寄るリスクと開発者が感じるリスクについて」, ECOM News No. 18(2006.12.26)

[2.4-1]IPA セキュリティセンター：http://www.ipa.go.jp/security/index.html

[2.4-2]seurityfocus：http://www.securityfocus.com/

[2.4-3]Bugtraq：http://www.securityfocus.com/archive/1

[2.4-4]トレンドマイクロ：Internet Security Knowledge.　http://www.is702.jp/

[2.4-5] HarkerJapan：http://www.byakuya-shobo.co.jp/hj/

[2.4-6] Tenable Network Security：　http://www.nessus.org/nessus/

[2.4-7] BlackHat：http://www.blackhat.com/

[2.4-8] DefCon：https://defcon.org/

[2.4-9] Black Hat Japan 2007：
http://www.blackhat.com/html/bh-japan-07/bh-jp-07-main.html

3. 情報端末セキュリティ検討 SWG 活動報告

3．1． 活動概要

⑴ 目的

今後、インターネット接続の各種端末機器が普及するに伴い、より一層顕在化すると予測されている EC(電子商取引)関連の組込みシステムの脅威に対する情報セキュリティ対策の浸透、向上を目指し、各端末分野個別に保護すべき情報資産とその脅威や対策を洗い出し検討した。

構成要素

・携帯電話、情報家電、ｶｰﾅﾋﾞ・ETC、金融端末、必要に応じて IC ﾀｸﾞ、IC ｶｰﾄﾞ等

対象情報

・ID、PW、個人情報、企業情報、取引情報、決済情報、電子ﾏﾈｰ

⑵ 活動方針

Step1 ： 届出のあった EC 関係の端末脆弱性情報の事例ピックアップ・調査

Step2 ： 端末に作りこまれてしまう脆弱性の議論

Step3 ： 端末開発でこれだけは守っておくべき注視点や注意点のまとめ

※検討ポイント

・既存端末に関する事故事案

・将来の EC 端末（情報家電など）

・組込みソフトに対する脅威と対策

・SWG１の調査結果

⑶ 活動経過

活動経過を表 3.1-1 に示す。

表 3.1-1 情報端末セキュリティ検討 SWG の活動経過

期日	活動内容
平成 19 年 7 月 25 日	第１回情報端末セキュリティ検討ＳＷＧ
	・組込みソフトウェアの脆弱性と情報セキュリティについて（MRI） ・ネット接続機器の脆弱性悪用例（ボット化の脅威）
8 月 27 日	第２回情報端末セキュリティ検討ＳＷＧ
	・情報家電機器認証技術（日立） ・情報端末での対象範囲と課題について
10 月 16 日	第３回情報端末セキュリティ検討ＳＷＧ
	・情報端末での脅威の見えるかと責任分解点について
12 月 12 日	第４回情報端末セキュリティ検討ＳＷＧ
	・提言内容（情報端末での責任分解点とあるべき姿）について

⑷ 活動内容

■ 届出のあった EC 関係の端末脆弱性情報の事例ピックアップ・調査

- 組込みソフトウェアの脆弱性と情報セキュリティについて
- ネット接続機器の脆弱性悪用例

■ 端末に作りこまれてしまう脆弱性の議論

- 組込み機器のあり方（家電かコンピュータか？）
- 組込み機器のセキュリティの確保
- 機器としての家電、サービスとの連携
- ネットワークインフラとの関連

■ 端末開発でこれだけは守っておくべき注視点や注意点のまとめ

－EC のための組込み機器
－機器認証の重要性
－セキュアなネットワーク環境の必要性

3.2. 情報端末を用いた EC 環境の現状

（1）情報端末での EC の拡大

EC で利用される情報端末としては、PC や携帯電話だけでなく、Suica に代表されるように生活のいたるところで利用されるような機器へと拡がってきている。2011 年には、アナログ放送が停波すると言われており、デジタル放送による TV などが情報端末として一般的に利用されることが予想される。

近年まで BtoB 及び一部の PC ユーザ(パワーユーザ)による BtoC が主体であった EC であるが、JR 東日本の Suica による小額決済等の普及等もあり、その利便性が一般消費者に幅広く認識されだしている。例えば、電子マネー(IC カード)には、Suica、Pasmo、Edy、nanaco、waon などがあり、オサイフ携帯としては、Suica、Edy、iD、QuickPay などの電子マネー機能が携帯電話で利用できる環境が広く普及している。

さらに、TV や HDD レコーダ、ゲーム機等が、インターネット接続用の I/F を実装するなど、情報家電が現実のものとして普及し始めている。一方で、ネットバンキングや株式取引、オークション、通信販売等、インターネットを通じた EC についてメニューが増加してきており、インターネット商取引への一般消費者の関心は強い。

これらの事象(メニュー）は、決して IT リテラシーが高いとは言えない一般消費者を対象とした企業消費者間（BtoC）の EC を意識しなければならない時代となったことを意味している。現状、PC を対象とした様々なセキュリティ事故が発生しているが、今までよりさらに安全・安心な EC 環境が必要とされる。

（２）家電等の情報端末の脅威

家電等の情報家電端末のトラブル事例として、携帯端末がウィルスに感染し起動しなくなったケース（図 3.2.1.）などが報告されいている[3.3-1]。また、ルータや家電のセキュリティトラブルも報告されており、これらがボットネットの温床になる脅威もある（図 3.2.2）。

図 3.2-1　「Symbian OS」に感染するウイルスの特徴
（携帯端末の感染例）
－独立行政法人 情報処理推進機構(IPA) ：組込みソフトウエアを用いた機器におけるセキュリティ(2006 年 4 月),P8 より-

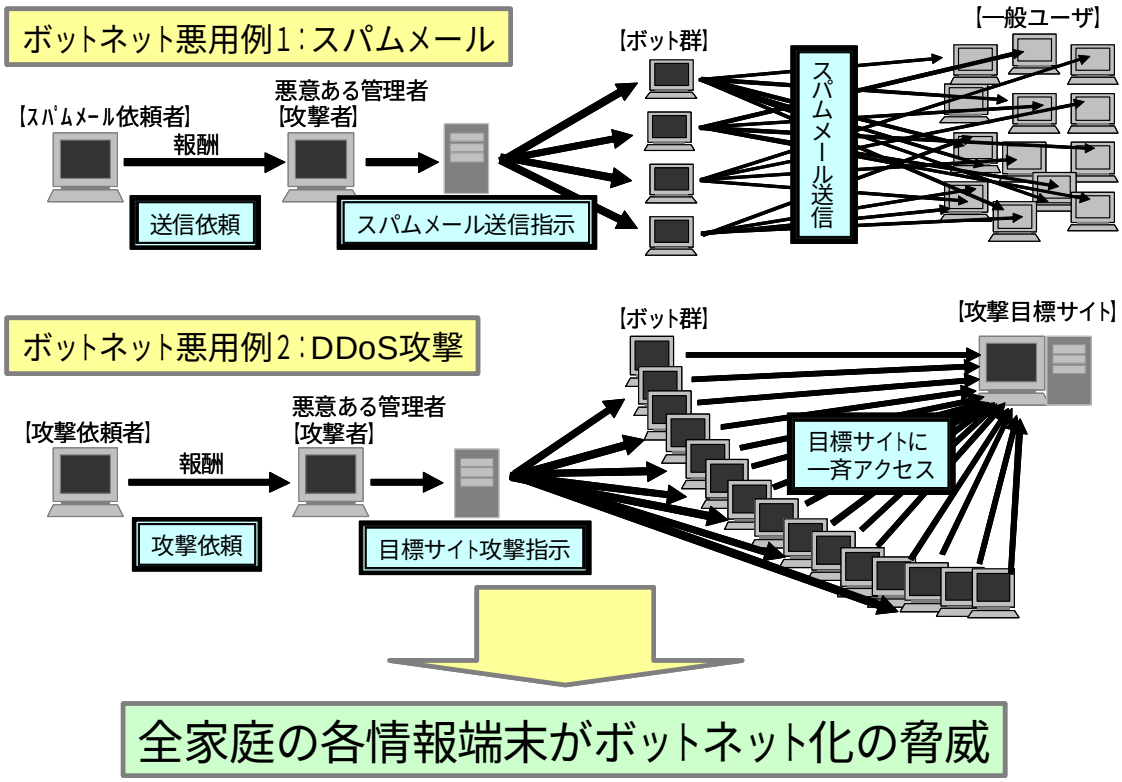


図 3.2-2 ボットネットの攻撃例

（３）家電等の情報端末の脅威に対応するための要件(特徴)

家電等の情報端末は、PC 利用者に比べ低リテラシーであっても利用できる必要がある。スイッチを入れるだけで使用できるような利用方法が想定されている。そのような情報端末は、手厚いユーザサポートが必要であり、またユーザもそれを期待している商品である。他の情報端末と比較した要件をまとめると表 3.2-１のようになる。

表 3.2-1 家電の要件

端末	リテラシー	ネットワーク	窓口	サポート
PC	高	インターネット	ASP (インターネット上)	低
携帯	中	ドコモ網など	キャリア	中
家電 (現状)	低	インターネットなど	各社 (インターネット上)	低
家電 (今後)	低	業界網 (各社ホスト)	業界	高

（ａ）組込み機器の特性

情報家電は PC とは異なり、以下のような特徴がある。

・CPU が遅く、複雑で実行に大量のリソースを必要とするようなセキュリティ機能の実現は難しい。
・セキュリティを意識させない必要がある(例：高齢者や幼年者のような IT リテラシーが低い層も対象とするため、簡単な UI で操作できなければならない)。
・販売価格を抑える必要があり、汎用 OS やミドルウェア、セキュリティチップ等、高価なハード/ソフトを用いることは難しい。
・電源を入れたらいつでも使える。
・電源を切ったら、コンテキストが残さずいわゆるリセットすることで初期状態にできる。

上記から、端末で対応可能なセキュリティ機能は限られており、ネットワーク側での対処も望まれる。

3.3. 情報家電等の情報端末を使った電子商取引のあるべき姿

情報家電等の情報端末を使った電子商取引のあるべき姿として、利用環境を含めた解決策の必要性と情報家電等の情報端末を安全に製造するためのポイントについて纏める。

（１）利用環境を含めた解決策の必要性

第２章で述べた脆弱性への対処やツール類の活用は、3.5.1.(3)で述べたように組み込み機器の特性や、制約がある。そのため情報家電では単体で、電子商取引を行う上でセキュアな情報端末を提供することは難しい。

その実現には、サービス側やネットワーク側での対処が必要である。言い換えると、情報家電等の情報端末を使用する際に前提となる環境の整備が必要ということなる。

例えば、小額決済を取り扱う Suica は、閉域網を用いた安全なネットワークを構築した。

最近の携帯電話端末は、EC サイトをすべて携帯電話会社が管理している。このように、安心安全なサービスは、前提となる利用環境の整備を行っている。

一方で、インターネット等のオープンネットワークに直接接続されている情報端末は日々進歩する無数の脅威に晒されることになり、限られたリソースの組込み機器では防御する仕組みを内包させることが難しい。

このように、家電等の情報端末では、ネットワーク環境を含めたサービス提供者による環境をユーザに対してサポートしないと、安全・安心な EC は実現できないと考える。

（2）情報家電等の情報端末を安全に製造するためのポイント

情報家電等の情報端末を安全に製造するためには、セキュアな環境の作り込みの重要性と機器認証の必要性があげられる。

■セキュアな環境の作り込みの重要性

情報家電等の情報端末では、脆弱性などの問題が発覚した場合に次のような特徴がある。

・大量生産される情報家電は、回収コストも膨大である。
・ユーザ登録されるとは限らない。
・告知してもユーザが自分のことであると気づかない。
・回収は進まずに費用が嵩む。

ユーザのリテラシーがある程度期待できる PC などであればパッチを配布するということも考えられるが、情報家電等の情報端末では、パッチの配布方法やアップデート処理なども難しい点が多い。

そのため最初から脆弱性を作りこまないように、可能な限り製造の段階でセキュアな作りこみを心がけることが重要となる。

技術者のスキルの向上や教育も重要であるが、プロジェクトのライフサイクルにセキュリティ対策を組み込む等の対策は、組織的に確実な効果を出すためには重要である。図 3.3.-1 にあるように、プロジェクトのライフサイクルの各局面にセキュリティ対策を取り入れることが IPA のガイド[3.3-2]などでも推奨されている。

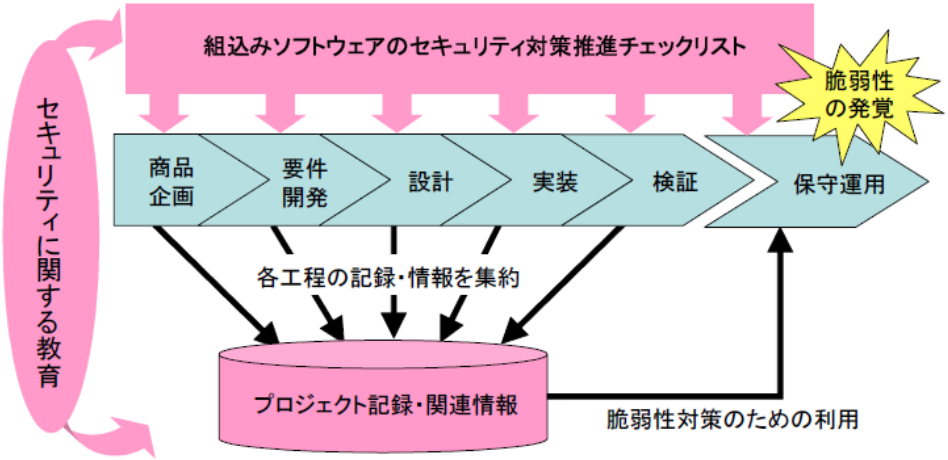


図 3.3.-1 組込み機器の開発等におけるセキュリティ確保

独立行政法人 情報処理推進機構(IPA) ：組込みソフトウェアのセキュリティ 機器開発等における セキュリティ確保のための４０のポイント,P.11（2006 年 4 月）より

■ 機器認証の必要性

次に、機器認証の必要性について述べる。例えば、設定画面等でユーザ ID や、パスワードをユーザに識別させたい場合の例で考えてみる。

家電としては、電源を入れたらすぐ動く必要がある。ユーザ名やパスワードを入力しないと使用できない家電はユーザのリテラシーやその性質上そぐわない側面がある。しかし、ユーザ名やパスワードを設定せず、全ての商品に同じデフォルト設定の状態で出荷した例がある。このことは、家電の利用場面を考えるといたしかたない側面がある。しかし、ネットワーク端末としてみた場合には、明らかにセキュリティホールとなる。

つまり、ユーザ名やパスワードなどユーザが意識しなくても良いような、その機器を識別したり認証できたりするソリューションが必要となる。ここで、有効な技術が、テレビに内蔵されている B-CAS カード、携帯電話に内蔵されている SIM のような IC チップによる機器認証である。IC チップを利用した機器認証を行うことで、ユーザにパスワードなどを意識させることなく、IC チップに埋め込まれた、機体固有番号などを確認でき、機器認証や相互認証を確実に行うことで、正しい相手との新しいサービスが可能となる。

3.4. 責任分解点について

現状のネットワーク環境を考えると、家庭内、通信事業者、ISP やインターネット、インターネットに接続している企業や個人がある。これらの概念図を図 3.4-1 に示す。

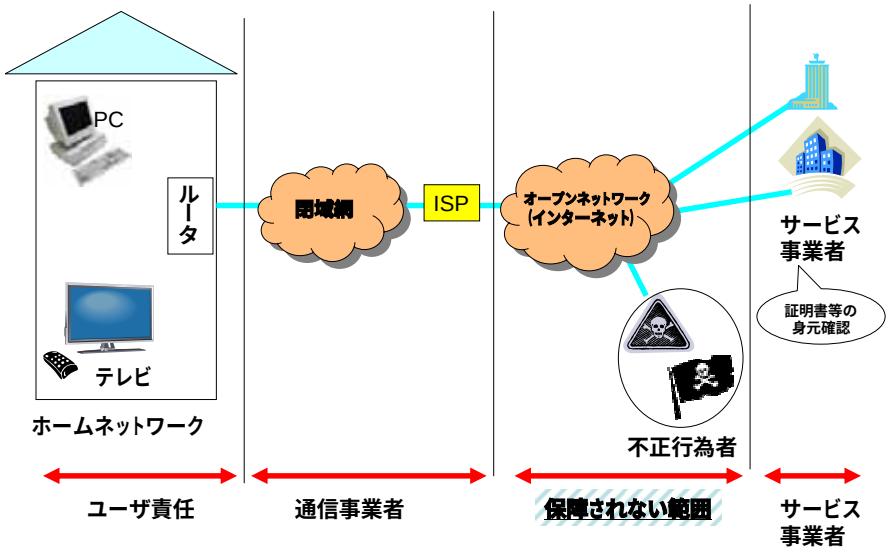


図 3.4-1 現状のネットワークの概念図

現状の PC によるインターネット接続では、通信事業者とサービス事業者の間（責任の所在が不明な地点＝インターネット）で発生する様々な攻撃について、パーソナルファイアウォールやウィルス対策ソフト等で対処している。しかし、これはユーザの責任の範疇であって、誰かの保障が受けられるわけではない。

高齢者や幼年者のような IT リテラシーが低い層にこれらの対策を求めることは難しい。さらに情報家電である場合には、これらの対策をとることはハード的にも困難である。

よって、通信事業者とサービス事業者の間の責任を、誰がになうのか明確にする必要がある。

責任を明確にしないと安全・安心な EC の普及を望むことはできない。そのため、図 3.4-2 にあるようにユーザのサービスを責任範囲内で行えるような環境が望ましいと考える。

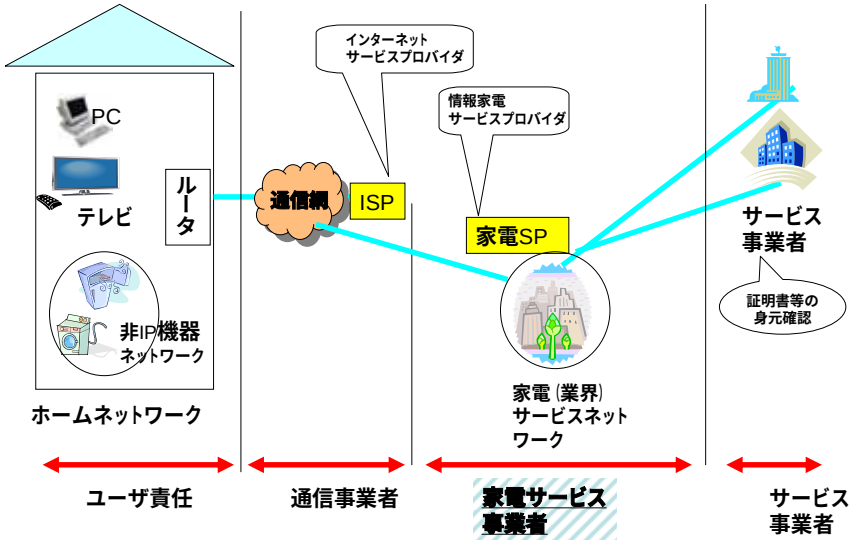


図 3.4-2 インターネットにおけるサービス提供の責任範囲

3.5. ネットワーク環境の実現方法

現在の技術では、通信事業者以降の網をクローズ化する案が良いと考えられる。クローズ化の方法としては、物理的に網を分離する方法と VPN を用いて網を分離する２通りが考えられる。１つ目は、網を独立にネットワークをハード的に分離する方法（図 3.5-1）で、２つ目は、VPN を用いて論理的にネットワークを分離する方法（図 3.5-2）である。

このように２つの実装方法があるが、通信事業者以降の網をクローズ化することにより、ネットワーク上の各ポイントでの運用責任が明確になることや、サービスプロバイダへのなりすまし行為等がなくなる（認定された事業者しか接続できない）等があり、サービス事業者も安心して参入できる。これらの実現方法の以下の利点と弱点がある。

（１）物理的ネットワーク分離

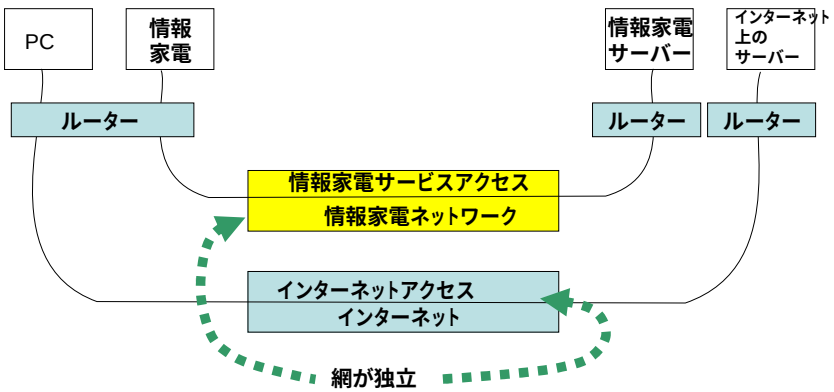


図 3.5-1 物理的に分離したネットワーク概念図

利点

・サービスプロバイダの管理が可能となるため、不法、不適切な内容等が入り込まない（入り込んだ場合でも排除が簡単に行える）。

・インターネットに接続されないので、インターネットのトランザクション量の影響を受けない。また、契約端末やサービス事業者数から、比較的簡単にトランザクションを予測できると考えられる。

・許可されたサービス事業者のみがサービスするため、他からの攻撃等が発生しない。

・ホームネットワーク上でインターネットアクセス機器と共存可能

弱点

・物理的に網を分離するため、構築コスト・運用コストが高い。

・サービス事業者のサーバロケーションが家電サービスプロバイダのロケーションに影響される場合がある。

・現状の家庭内通信機器では比較的高機能（２ISP 以上に接続可能）なものしか適用できない。

（２）論理的にネットワークを分離する方法

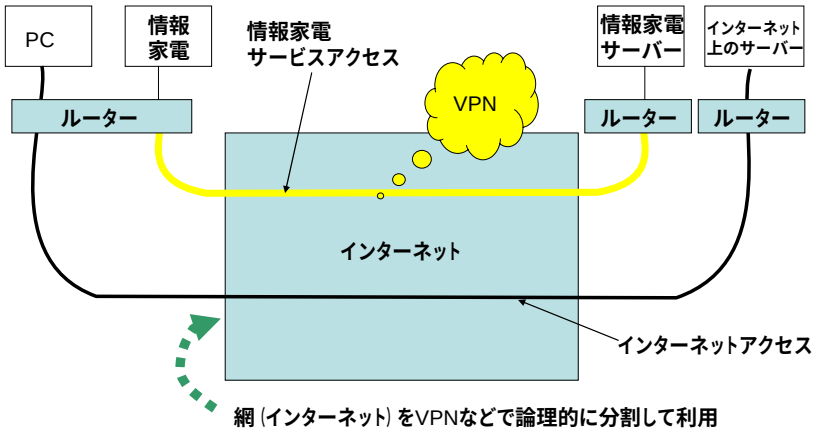


図 3.5-2 論理的に分離したネットワーク概念図

利点

・現状のインターネット上に構築できるので構築コスト・運用コストが安い。

・サービス事業者のサーバロケーションに制約がない。

・現行の家庭内通信機器（具体的にはルータ（ISP 接続機能、ルータ、HUB の一体製品））がそのまま使える。

・ホームネットワーク上でのインターネットアクセス機器と共存可能。

弱点

・インターネット上に構築するため、他からの攻撃等に対して完全とは言えない。

・インターネットのトランザクション量の影響を受けやすく、予測も難しい。

（３）ECOM の考える BtoC の未来像

さらに、ECOM 情報セキュリティＷＧで考える BtoC の未来像は図 3.5-3 となる。このような

ネットワークになることで、各種コンテンツプロバイダに安心安全にも接続できるだけでなく、必要に応じてサービスプロバイダ経由で安心安全なインターネットアクセスも可能とすることができる。

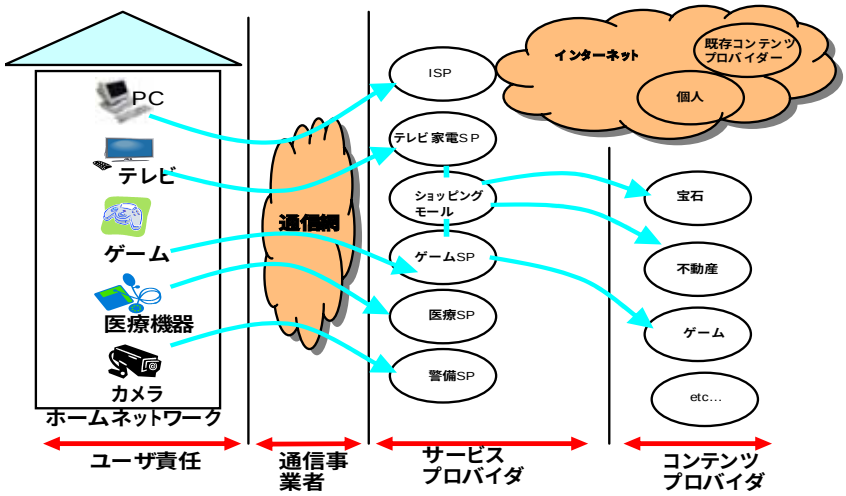


図 3.5-3 情報端末を使った安全安心な EC の将来像

参考文献･資料

[3.3-1] IPA：組込みソフトウエアを用いた機器におけるセキュリティ,P8(2006 年 4 月)
http://www.ipa.go.jp/security/fy17/reports/vuln_handling/documents/booklet_manager.pdf

[3.3-2] IPA ：組込みソフトウェアのセキュリティ 機器開発等における セキュリティ確保のための４０のポイント,P.11（2006 年 4 月）
http://www.ipa.go.jp/security/fy17/reports/vuln_handling/documents/booklet_manager.pdf

4. 情報セキュリティガイド作成 SWG 活動報告

4.1. 活動概要

⑴ 目的

情報セキュリティ懇話会での意見交換を踏まえ、安全・安心な EC を普及させることを目的とし、情報セキュリティをビジネスとして捉えている者達が、下記の事項を調査、研究、まとめ、共通の認識に立ち、EC に関連する企業の情報セキュリティの底上げに向け、「経営者が知っておくべき点・守っておくべき点」をガイドとして纏めた。

⑵ 活動方針

Step1 ： 既存の知っておくべき法律、ガイドライン、技術などを集める

Step2 ： 関係者にヒヤリングを行う。

Step3 ： ガイドブックとして纏める。

⑶ 活動経過

活動経過を表 4.1-1 に示す。

期日	活動内容
平成 19 年 10 月 16 日	第１回情報セキュリティガイド作成ＳＷＧ
	・2006 年度 情報セキュリティインシデントに関する調査報告(JNSA)
	第２回情報セキュリティガイド作成ＳＷＧ
	・「脆弱性」と「バグ」について
11 月上旬	企業の取組みヒヤリング（情報セキュリティガイド作成ＳＷＧ）
	・情報セキュリティ向上に関する企業の取組みについて （組織的な取組み、環境整備、対策の矛盾、望むことなど）
12 月 13 日	第３回情報セキュリティガイド作成ＳＷＧ
	・報告内容と提言内容、・報告書の目次と執筆分担について
平成 20 年 1 月 30 日	第４回情報セキュリティガイド作成ＳＷＧ
	・ 報告内容と提言内容について（その 2)

⑷ 活動内容

（１）既存の法律、ガイドライン、技術の収集

－政策、－国際標準化、－法律、－ガイドライン、－技術

（２）関係者ヒヤリング

－企業コンプライアンスとしての情報セキュリティ対策の進め方

－様々な分野に対する情報セキュリティの対策の進め方

－中小企業における情報セキュリティの対策の進め方

（３）報告書とガイドのまとめ

4.2. 情報セキュリティに関する政策

4.2.1. 日本全体の情報セキュリティ対策の流れ

1998 年以降の 10 年間は情報セキュリティに関連した動きは、大きな進展を示しきた。その状況は、その政策の主な項目を挙げただけでも、重大さが見て取れる。まず、その状況の概要から示しておく。

（1）この 10 年の情報セキュリティ政策の動き

この 10 年間の情報セキュリティ政策の流れをまとめたものを　図 4.2-1 に示す。

図 4.2-1 をみるとわかるように、10 年前には当時の通商産業省の機械情報産業局の中に情報セキュリティ政策室は発足したばかりの時期であった。そして 2000 年 1 月 21 日に「ハッカー対策等基盤整備に係る行動計画」発表され、その直後に省庁のホームページの書き換えが続発した。それを受けて２月１日に内閣情報セキュリティ対策室が発足した。これが我が国の政府が情報セキュリティの重要性を意識した最初といえる。

2000 年以降の主な政策実施状況をまとめると以下のような内容が挙げられる。

- 2000 年　　2 月 13 日　不正アクセス禁止法施行
- 2000 年　　暗号技術評価委員会（CRYPTREC）の設置
- 2001 年 4 月　IT セキュリティ評価・認証制度の創設（NITE/IPA）
- 2001 年 4 月　電子署名及び認証業務に関する法律施行
- 2002 年 4 月　情報セキュリティマネジメントシステム適合性評価制度創設（METI/JIPDEC）
- 2003 年 2 月　「電子政府における調達のための推奨すべき暗号のリスト（電子政府推奨暗号リスト）」の決定、「各省庁の情報システム調達における暗号の利用方針（2003 年 2 月行政情報システム関係課長連絡会議了承）」（各省庁が情報システムの構築する際には、可能な限り電子政府推奨暗号をリストに推奨された暗号の利用を推奨する）を発表
- 2003 年　　情報セキュリティ管理基準・監査基準の官報公布
  情報セキュリティ監査制度の創設

このように、現在も情報セキュリティの保護に関する施策が前半の５年間で実施された。情報セキュリティ政策の経緯を図 4.2-1 に示す。

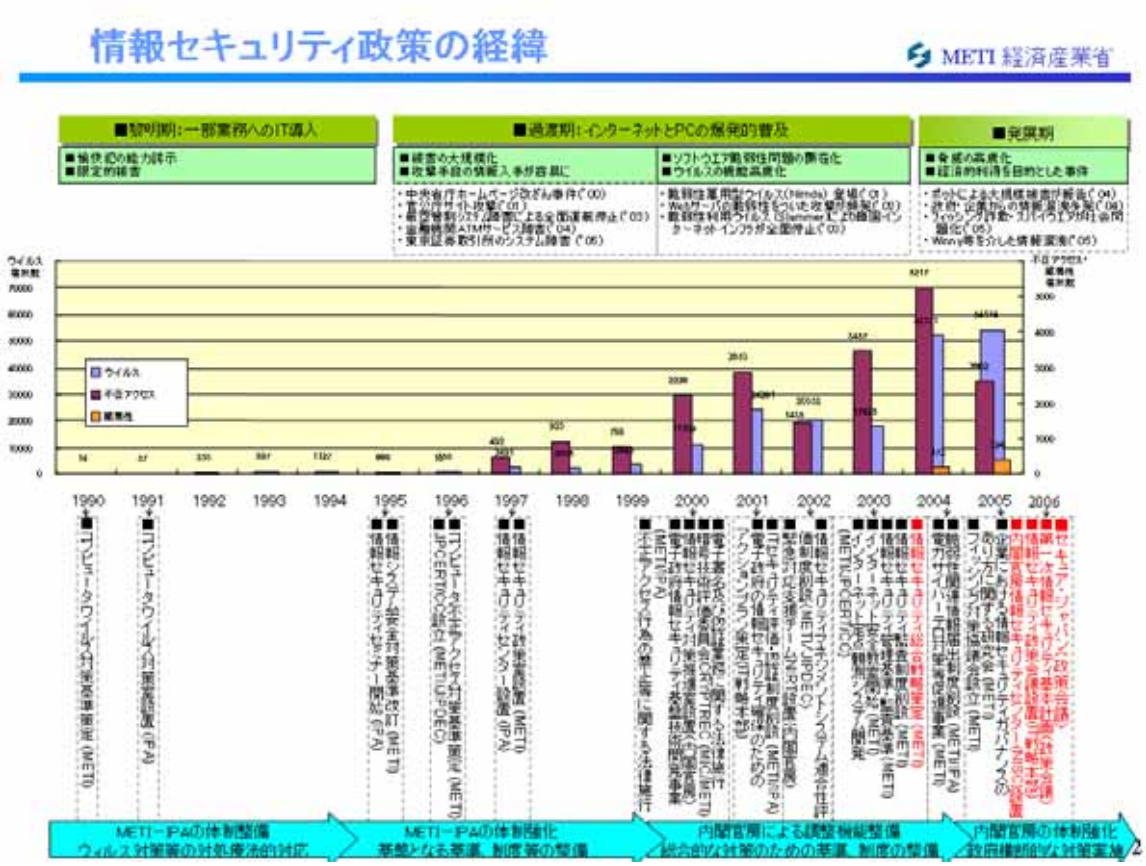


図 4.2-1 情報セキュリティ政策の経緯

（第30回 ECOM セミナー 経済産業省 講演資料 より）

（２）この３年間の動き

我が国のインターネット利用者について、平成 19 年度の情報通信白書によれば、平成 18 年のインターネットの人口普及率は 68.5%、利用人口は 8,754 万人と推定されている。その利用方法は、パソコン、携帯電話など多様化している。このことは、国の社会経済システムの重要な基盤となっていること、つまり、企業内、企業間の通信にも利用されていることを示している。このように社会基盤化した情報システムに対し、情報セキュリティを確保することは必須となっている。このような状況のなかで、経済産業省は、2003 年 10 月に情報セキュリティ総合戦略を作成した。その中で、基本目標を、経済・文化国家の強みを活かした「世界最高水準の『高信頼性社会』の構築とした。その要の「情報セキュリティ対策」について以下の３つの戦略（４２の施策項目）を提言した。

- 戦略１　しなやかな「事故前提社会システム」の構築
- 戦略２　「高信頼性」を強みとするための公的対応の強化
- 戦略３　内閣機能強化による統一的推進

その後、政府全体の取り組みに拡大し、官邸・ＩＴ戦略本部が２００４年１２月に「情報セキュリティ問題に取り組む政府の役割・機能の見直しに向けて」を決定し、

- 2005 年 4 月 25 日　内閣官房情報セキュリティセンター（NISC）を設置
- 2005 年 5 月 30 日　ＩＴ戦略本部の下に「情報セキュリティ政策会議」を設置

といった体制・機能整備を行った。

そして、その活動の中で、2006 年 2 月 2 日、第１次情報セキュリティ基本計画（2006 年～2008 年）を策定した。

その基本理念は以下の３つとなっている。

（１） 経済国家日本の基盤としての情報セキュリティ

（２） 安全・安心を求める、よりよい国民生活実現のための情報セキュリティ

（３） 新たな安全保障確保の観点からの情報セキュリティ

その内閣官房を中心とした統一的な取り組みを進め、2006 年度に、全体方針として「セキュアジャパン２００６」を策定した。個々には、事前予防策として、国・自治体向けの「政府機関統一基準」、及び重要インフラ向けの「セキュリティ確保に係る安全基準等策定のための指針」の策定を行い、また、事故対応策として NISC 緊急時連絡体制の構築をおこなった。企業向けには、早期警戒態勢、情報セキュリティ監査などの整備、BCP 策定ガイドラインの策定などを行っている。

また、ワーム、スパイウェア、ボット、ソフトウエアの脆弱性などの情報を早期に共有しておく必要性から JPCERT/CC 及び IPA などが協力して「情報セキュリティ早期警戒パートナーシップ」の体制を構築し、実績を上げている。

この同じ時期（2005 年４月）から、個人情報保護法の全面施行にともなって、経済産業省は「経済産業分野を対象としたガイドライン」を制定し個人情報保護の方向性を示した。

（３）この１年間の政策動向

この一年間の内閣情報セキュリティセンター（NISC）の動き及び経済産業省情報セキュリティ政策室の動きについて紹介する。活動としては双方が協力してその政策を実施しているが、個別に見ていくことにする。

内閣情報セキュリティセンター（NISC）

NISC では「第１次情報セキュリティ基本計画」の策定後、政府・民間がそれぞれの主体が適切な役割分担を果たす「新しい官民連携モデル」の構築に向けて、「セキュアジャパン２００７」及び「政府機関統一基準」の見直し（2006 年 6 月 14 日）を行った。

「セキュアジャパン２００７」では、主な取り組みとしては、「政府機関情報セキュリティ対策の拡充」、「広く国民を含めて対策が遅れがちな主体の対策の普及」、「情報セキュリティ基盤強化に向けた集中的な取り組み」を挙げている。その具体的施策として、重点４分野「政府機関・地方公共団体」、「重要インフラ」、「企業」、「個人」についてそれぞれ目標を設定し、その達成をめざすこととしている。この中では、「地方公共団体」、「中堅企業」「個人」のように、対策が遅れがちになる分野でのレベルアップを目指した対応を要求している。今回は、情報セキュリティ資格制度の体系化を行い、その中には情報処理技術者試験制度の見直しを行い、情報セキュリティ人材の育成なども含まれている。更に、サイバー犯罪の取り締まり強化のための技術水準向上なども急務である。

2008 年 1 月現在、2008 年度の対応に向けて、「政府統一基準・第 3 版」の見直しに向けた対応を行っている。また、情報セキュリティ政策会議の下で、「第 2 次セキュリティ基本計画」の策定に動いている。

4.2.2. 一般産業における情報セキュリティ対策の流れ

2007 年度には、2003 年末に策定した「情報セキュリティ総合戦略」について、技術の急速な進展に対応が必要との認識に立ち、産業構造審議会情報第 5 回セキュリティ部会の見直しの必要性が指摘された。新たな評価を行い、優先順位の明確化と重点分野の絞り込み、新たな課題の追加を行って、戦略の策定することになった。その課題の視点として、「企業価値への組込を進めると共に第三者評価などの信頼性向上策の仕組み導入」「情報セキュリティの 3 要素の中で機密性偏重から完全性、可用性等への対応」「情報漏洩等の深刻化への対応」、「情報家電などの新技術分野に対応した情報セキュリティ対策」を盛り込んだ。

2007 年 5 月に「グローバル情報セキュリティ戦略」を策定した(図 4.2-2)。
その 3 つの戦略は以下の通りである。

- 戦略 1　情報セキュリティ先進国の実現
- 戦略 2　情報セキュリティ政策のグローバル展開
- 戦略 3　国内外の変化に対応するメカニズムの確立

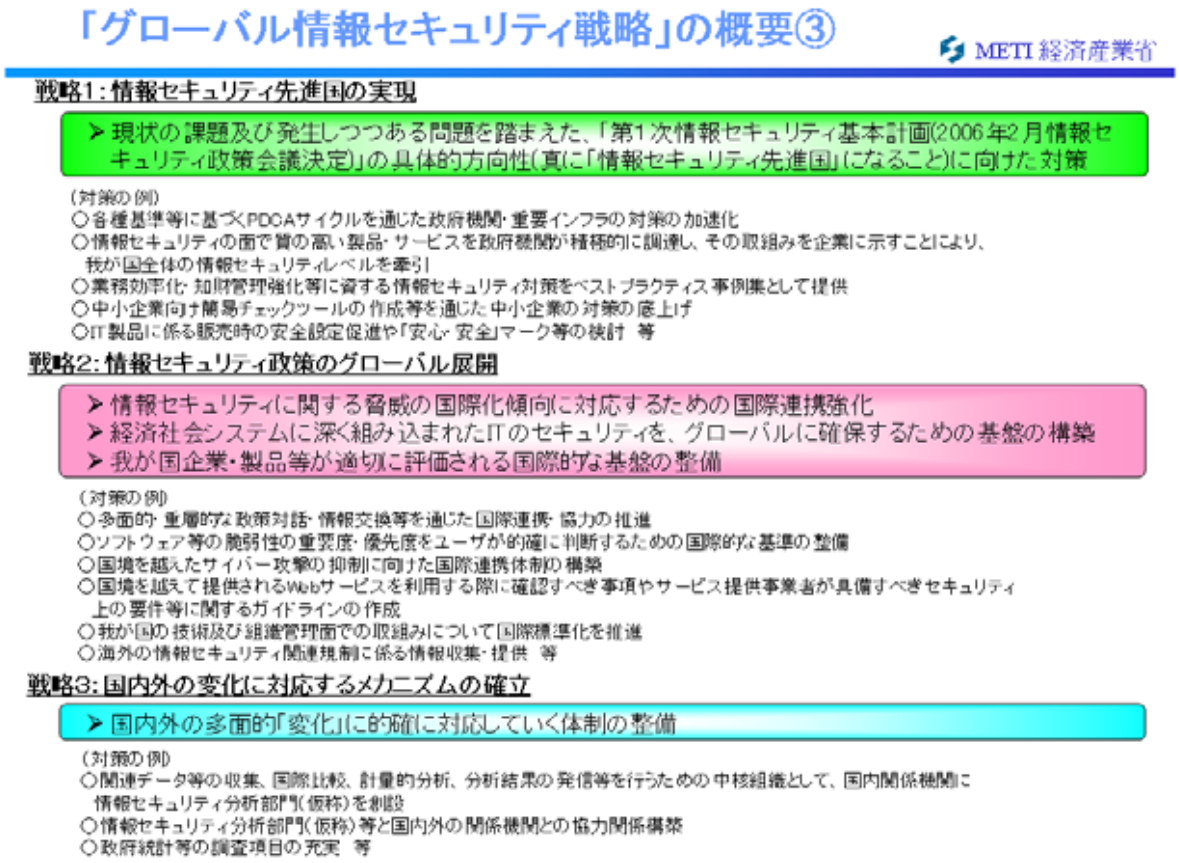


図 4.2-2 グローバルセキュリティ戦略の概要

(産業構造審議会情報ｾｷｭﾘﾃｨ基本問題委員会報告書「ｸﾞﾛｰﾊﾞﾙ情報ｾｷｭﾘﾃｨ戦略」(平成 19 年 5 月) より)

この中で新たにもうけられる組織は、情報セキュリティ関連のデータ等の収集、国際比較、計量的分析、分析結果の発信等を行うための中核組織として、2008 年４月 IPA 内に「（仮称）情報セキュリティ分析ラボラトリー」を立ち上げることになっている。このように、内閣、経済産業省などが中心となって、今後も適切な情報セキュリティ政策を実施されると考えられる。

また、経済産業省では、産業構造審議会情報経済分科会ルール整備小委員会において取りまとめられた提言を踏まえ、以前より電子商取引等に関する様々な法的問題点について、民法をはじめとする関係する法律がどのように適用されるのかを示す「電子商取引等に関する準則」を公表していた。2007 年 3 月 30 日には「電子商取引及び情報財取引等に関する準則」を公表した。それでは、以下の内容が追加・改訂された。

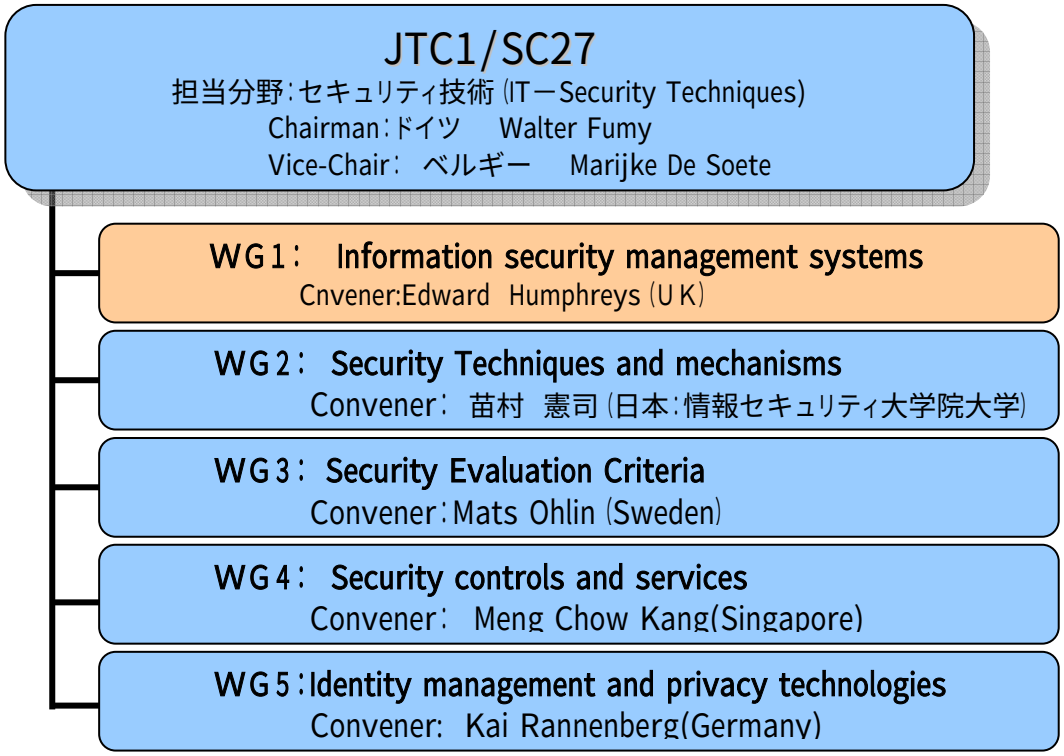
「電子商取引等に関する準則」からの改訂内容
・価格誤表示と表意者の法的責任 追加
・ワンクリック請求と契約の履行義務 追加
・なりすましによる意思表示のなりすまされた本人への効果帰属 修正※
・ホスティングを伴う電子商取引事業者の違法情報媒介責任 追加
・インターネットを通じた個人情報の取得 追加
・当事者による法選択がない場合の準拠法 追加
・越境取引における消費者保護法規 追加
・インターネット上の不法行為と準拠法 追加
・ソフトウェア特許権の行使と権利濫用 追加
・Ｐ２Ｐファイル交換ソフトウェアの提供者の責任 修正※
・ＩＤ・パスワード等のインターネット上での提供 追加
・肖像の写り込み 追加
・著作物の写り込み 追加
・サムネイル画像と著作権 追加
・ｅラーニングにおける他人の著作物の利用 修正※
※「修正」とあるのは、従来の「電子商取引等に関する準則」（平成１８年２月版）に盛り込まれている項目について、その内容を修正したものです。

4.3. 情報セキュリティの国際標準

情報セキュリティ関係の国際標準化は、JTC1／SC27 が中心になって行われている。その議長及び幹事国はドイツである。当初、その標準化中心は、暗号技術やその応用技術が中心であったが、2000 年の情報セキュリティマネジメントシステムの標準化以降、マネジメント関係の標準化がその活動の中心となり、参加国も次第にその数を増している。

2006 年以降、WG が５つに増えて、更にプライバシーやバイオメトリクスなどのセキュリティ領域に対象が広がってきた。

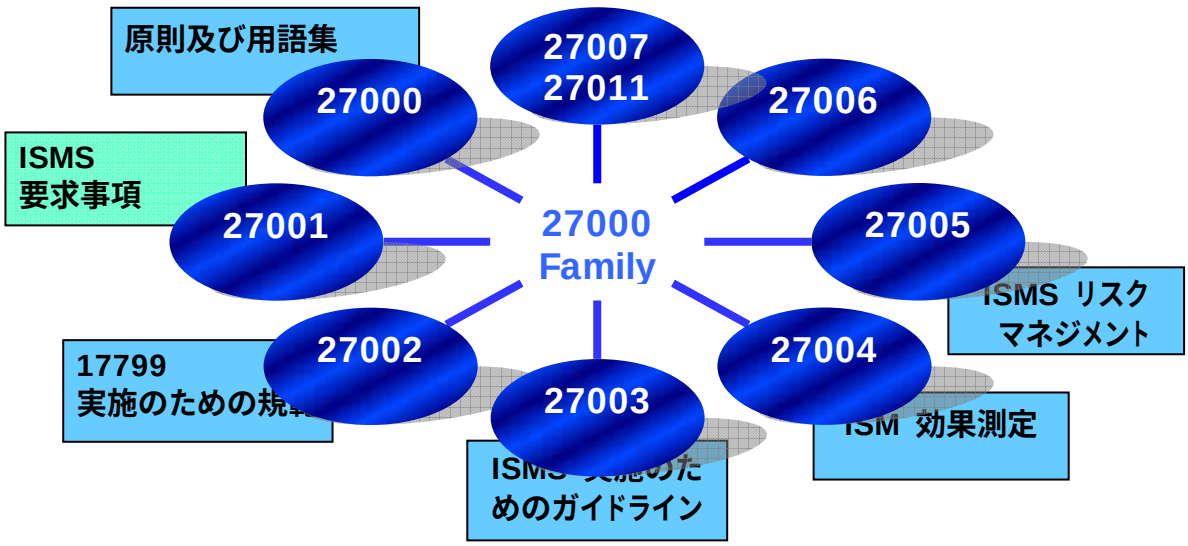
現在の組織を示すと以下の５つの WG の体制となっている。



現在、その５つの WG で審議されている項目の概要について紹介する。

（１） WG1　ISMS(情報セキュリティマネジメントシステム)

この規格は、ISMS 適合性評価制度の基本となる規格 ISO/IEC27001 を中心とした規格群である。既に、標準化が終わった 27001、27002（実践のための規範）、27006（審査登録機関のための要求事項）以外の標準について審議が行われている。



27001 をサポートする標準として、以下のものを扱っている。

- 27000（概要及び用語）
- 27003（ISMS の実践のための手引き）
- 27004（ISM―測定）
- 27005（情報セキュリティリスクマネジメント）
- 27007（監査人のためのガイド）
- 27011（情報通信事業者向けの ISMS ガイド）

今後は、ISMS の業界別の標準化について幾つか調査が行われているところである。
この ISMS の制度は、JIPDEC が認定機関としてかなり広まっていて、既に認証を受けた組織が 2400 以上になっている。詳細の制度は、JIPDEC のホームページ[4.3-1]を参照されたい。

（２） WG２　暗号技術およびその応用技術

ここは、暗号アルゴリズムおよびそれらの応用した認証技術、デジタル署名などのメカニズムの標準化を扱っている。

特に、暗号アルゴリズムの標準化が 2005 年に完了し、日本も作成には多くの貢献をした。その詳細は、ISO/IEC18033 の４つのパートで以下の通り構成されている。

18033-1：一般

暗号の種類と定義、附属書に選択基準などの一般的な説明。

18033-2：非対称暗号

カテゴリ	アルゴリズム名（提案国）
Ｅｌ Gamal方式に基づく KEM(鍵カプセル化機構)	ECIES-KEM（米国）
	PSEC-KEM（日本）
	ACE-KEM(ドイツ)
RSA 方式に基づく非対称暗号/KEM	RSAES（スウェーデン、米国）
	RSA=KEM(スウェーデン、米国）
モジューラー平方演算に基づく暗号	HIME（R)　（日本）

18033-3：ブロック暗号

カテゴリ	アルゴリズム名（提案国）
64 ビットブロック暗号	TDEA（米国）
	MISTY1（日本）
	CAST-128（カナダ）
128 ビットブロック暗号	AES（米国）
	Camellia（日本）
	SEED（韓国）

18033-4：ストリーム暗号

カテゴリ	アルゴリズム名（提案国）
鍵ストリーム生成専用アルゴリズム	MUGI（日本）
	SNOW2.0（スウェーデン）

日本では、各省庁の情報システム調達における暗号の利用方針（2003 年 2 月行政情報システム関係課長連絡会議了承）を決めたが、それは、CRYPTREC で独自に評価し安全性が確認されたものを使うこととした。そのため、リストの一部に違いがある。

（3） WG3：セキュリティ評価基準

この WG では、セキュリティ評価基準 ISO/IEC15408 に関連する標準を中心に作成している。現在は、CC（コモンクライテリア）の ver3.1 の標準化を進めている。最近は、暗号モジュール評価のセキュリティ要件ISO/IEC19790やバイオメトリクスのセキュリティ評価に関係するものも審議している。

ISO/IEC15446（PP&ST 作成ガイド）

ISO/IEC25459（暗号モジュール評価の試験要件）

ISO/IEC19792（バイオメトリクス評価技術）

特に、ISO/IEC15408 のセキュリティ評価・認証制度、ISO/IEC19790 の暗号モジュールの評価制度をアメリカに習って、IPA 中心に立ち上げ、活動している。

（4）WG4　セキュリティのガイドライン及び管理策

この WG は WG1 が ISMS のみを扱うため､ネットワークセキュリティ､ICT-Disaster recovery､TTP などを扱うことになった。ネットワークセキュリティは、ISO/IEC18028 の改訂のため、作業を開始したところである。また、ICT の Disaster Recovery　やサイバーセキュリティなどの議論も開始したところである。

（5）WG5：Identity and Privacy management

この WG では､他の WG に入らなかった IdM､プライバシー､バイオメトリクスなどを扱う。

ISO/IEC24760　認証の枠組み

ISO/IEC29100　プライバシーマネジメントの枠組み

ISO/IEC29101　プライバシーの参照モデル

プライバシーなどは、これまでなかった領域であり、2007 年末時点、その定義を含めて審議は長引いている。

4.4. 情報セキュリティに関わる法律

4.4.1. 情報セキュリティに関する法律の概観

情報セキュリティという言葉が、技術的にも、制度的にも幅広い意味を持つように、情報セキュリティに関する法律としてどのような範囲で捉えるかは難しい。現時点において、「情報セキュリティ」という用語を用い、また「情報セキュリティ」自体を保護法益として掲げて規定した法律は存在していない。いわゆるＩＴ基本法のもとで、政府は様々な情報セキュリティ関連施策を実施してきている。法整備の面では、生じてくる問題にその都度対処するため、役割を異にする個別の法律が種々主制定されてきている。情報セキュリティに関して発生する新たな問題も、民法その他の一般法によって律せられることもある。

法律の規定は、たとえば、「・・安全管理のために必要かつ適切な措置を講じなければならない」（個人情報保護法第２０条）というように、事業者の義務について抽象的な義務を課するのみで、その具体的内容については明らかにしていないものも多い。したがって、法令遵守体制を整備するにあたっては、法令を所轄する官庁のガイドラインを検討したり、法令の要請と必ずしもイコールではないが、各種規格を参考にすることになる。また、場合によっては、具体的事例を経て蓄積された判例の検討を要することもある。

大企業においては既に社内的に法務部門を擁し、法令遵守のための体制を整えることは比較的容易である。しかし、中小企業であっても、情報セキュリティを無視して事業を継続することはもはや困難な時代にあって、情報セキュリティに関連する法令を無視することはできない。自社の守るべき義務を認識し、事前に回避しうる法令違反リスクへの対策を立て、万が一自社の情報セキュリティが侵害された場合の対策についておよその知識を持っておくことは、現場レベルでの対応を検討する際のインセンティブとしても重要である。

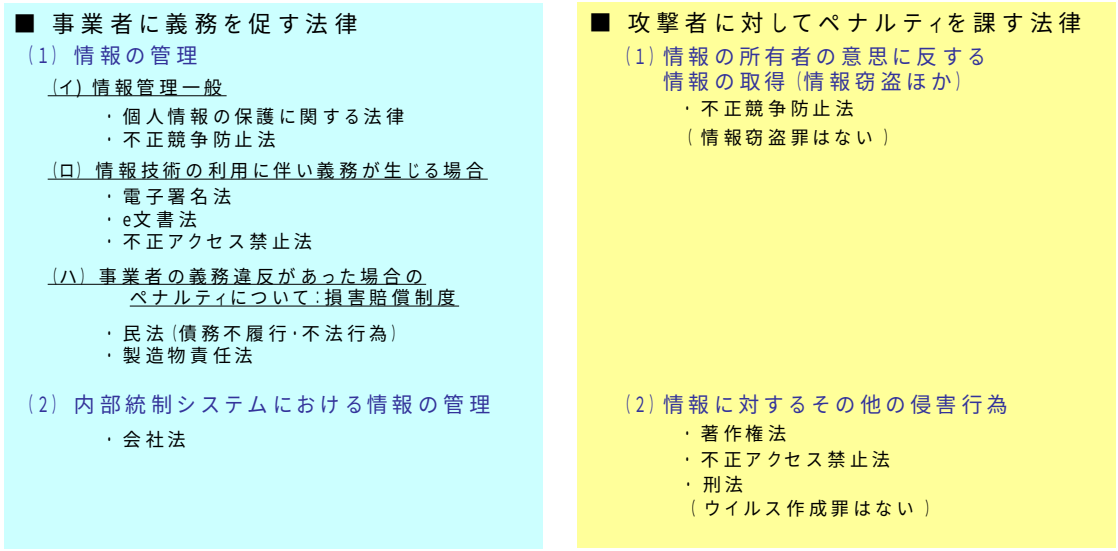


図 4.4-1 情報セキュリティに関わる法律

― 情報（電子データに限定されない）の取扱・情報技術の利用・セキュリティの確保等に関する法律 ―

なお、図中に紹介するものに限定されるものではない

情報セキュリティに関する法律という括りは前述のとおり難しいが、この項では事業者に、広い意味での情報セキュリティに関連して何らかの対応を促す法律と、情報セキュリティに対する攻撃者・不正行為者に対して何らかのペナルティを課す法律に大きく分け、その要点のみを紹介する。なお、情報（電子データに限定されない）の取扱・情報技術の利用・セキュリティの確保等に関する法律は、下記に紹介するものに限定されるものではないので、ご留意いただきたい。

4.4.2. 事業者に対応を促す法律

事業者に対応を促す法律に関するものとしては、情報の管理に関するもの、内部統制システムにおける情報の管理、情報に対するその他の侵害行為に関連した法律などがある。

4.4.2.1. 情報の管理

<u>情報管理一般</u>

・個人情報の保護に関する法律

（平成十五年五月三十日法律第五十七号、最終改正：平成十八年六月七日法律第五十五号）

対象事業者：

個人情報取扱事業者（法第２条３項で定義される）。同法上の個人情報５０００件を過去６ヶ月に亘って有していること等が要件となる。業種の制限などはなく、顧客情報のみならず従業員情報等もカウントされるため、相当数の事業者が本法の対象となりうる。

事業者の対応：

安全管理措置義務（法２０条）・従業者の監督義務（法２１条）・委託先の監督義務（法２２条）のほか、情報の取得・管理・第三者提供・情報開示など一連の過程において、事業者の留意すべき事項が定められている。

違反の効果等：

事業者に所定の義務違反があった場合には、主務大臣は、事業者に対し、違反行為の中止・是正措置を求める勧告・命令ができるとされている。また主務大臣は、事業者の義務の履行について、事業者に報告をさせ、事業者に対し助言をすることができる。行政命令に違反し、また、虚偽報告をした場合等について、懲役・罰金・過料の罰則もある。

本法の意義：

事業者の有する様々な情報のうち、「個人情報」に限定してその取扱上の留意点を定めている。そのほか、個別に情報の取扱につき規定を置いている法律もあるが、個人情報保護法は、対象となる事業者の範囲も広く、また事業者の有する多くの情報が「個人情報」のカテゴリーに属しうること、また顧客の関心も高いことから、現時点では、情報管理の一般法的な意味合いも有しているとも見うる。

・不正競争防止法（平成五年五月十九日法律第四十七号）

不正競争防止法は、不正競争として定義される各種行為を規制している法律であるが、営業秘密の侵害行為も、不正競争の一類型として規定されている。

事業者の対応：

不正競争防止法は、情報の管理について事業者に直接に義務を課す法律ではないが、事業者が保有しているノウハウなどの重要情報について、同法上の「営業秘密」として不正行為からの保護を受けるためには、その情報が「営業秘密」と認められるだけの情報管理体制を整備しておかなければならない。

「営業秘密」の保護：

営業秘密の不正取得行為、不正取得後の営業秘密の使用・開示行為等について、同行為の差止請求・損害が発生した場合の損害賠償請求・営業上の信用の侵害のあった場青の信用回復措置請求がなし得る。不正行為者に対しては、後述のとおり罰則もある。

不正競争防止法上の「営業秘密」とは：

秘密管理性（秘密として管理されていること）・有用性（生産方法、販売方法その他の事業活動に有用な技術上または営業上の情報）・非公知性（公然と知られていないもの）の３要件をいずれも充たさなければならない。各要件な内容については、複数の判例が蓄積されており、具体的な対策を行なう際の参考となる。

<u>情報技術の利用に伴い対応が必要となる場合</u>

・民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律

（平成十六年十二月一日法律第百四十九号）

一般にＥ文書法と略称されている法律である。法律により一定期間書類の保管義務が課されている事業者が、紙媒体での保管に代えて電磁的記録の形式で書類を保管する場合、電磁的記録の形式について同法所定の要件を備えなければならない（見読性、完全性、機密性）。

・電子署名及び認証業務に関する法律

（平成十二年五月三十一日法律第百二号、
最終改正：平成十八年三月三十一日法律第十号）

民事訴訟法上、本人の押印のある文書については、本人の意思に基づき真正に成立したものと推定される。これは、紙文書を対象にした規定なので、電子署名法では、電子文書に本人による電子署名が行なわれているときは真正に成立したものと推定することとした。ただし、ここでいう「電子署名」については、同法所定の要件を充たしているものであることが要請される。このような訴訟上の推定を受けるため、というよりは、官庁への電子入札などの場面で電子署名が要請される場合などにおいて、実務上意識される場面が多いと思われる。

・不正アクセス行為の禁止等に関する法律

（平成十一年八月十三日法律第百二十八号、
最終改正：平成十一年、十二月二十二日、法律第百六十号）

不正アクセス禁止法は、ネットワークに接続され、ＩＤ／ＰＷ等のアクセス制限がなされているコンピューターに対して権限なくアクセスすること等を禁止する法律であるが、アクセス管理者に対しても、不正アクセス行為を防御するための適切な対策を行うことが求められている。ただし、この法の要請は努力義務であって、違反に対する罰則はない。

不正アクセス行為を防御するための適切な対策（努力義務）：

アクセス管理者に対し、ＩＤ／パスワード等の適正な管理、アクセス制御機能の高度化、不正アクセス行為からの防御措置、を講じる努力義務が課せられている。

事業者に問題があった場合のペナルティについて：損害賠償制度

・民法

（明治二十九年四月二十七日法律第八十九号、
最終改正：平成十八年六月二十一日法律第七十八号）

民法の債務不履行・不法行為制度に基づく損害賠償制度（一般法）

情報セキュリティに焦点を当てたものではないが、情報セキュリティの整備に何らかの不備があり、第三者（取引先・顧客など）に損害が発生した場合には、事業者にこれら一般法に基づく損害賠償責任が発生する可能性がある。当事者間に契約関係があり契約上の義務の違反により損害が発生した場合には債務不履行責任が問題になり、契約関係がない場合であっても事業者の故意・過失による行為により第三者に損害が発生した場合には不法行為責任が問題になりうる。
情報セキュリティに不十分な点があり、判決により事業者に損害賠償が命じられた事例は数多く存在するが、特に、個人情報・プライバシー情報の漏洩が問題とされた事例が目立つ。この種の事例の場合は、個人情報・プライバシー情報の漏洩により具体的な財産的損害は発生しない場合の方が多いが、情報漏洩自体によって精神的な損害が生じているとして、慰謝料としての損害金の支払が命ぜられている。

・製造物責任法（平成六年七月一日法律第八十五号）

製造業者は、製造・加工・輸入等をした製造物について、製品の欠陥について他人の生命・身体・財産を侵害した場合には、それによって生じた損害を賠償しなければならない。同法上の製造物とは、「製造または加工された動産」とされているので、無体物であるソフトウエアに欠陥があったとしても同法の対象にはならないが、ソフトウエアがハードウエアに組み込まれて商品化されている場合には、その商品が製造物責任法の対象になる。

4.4.2.2. 内部統制システムにおける情報の管理

内部統制システムにおける情報の管理にかかわるものとしては、以下の法律などがあげられる。情報セキュリティシステムの整備は、事業者の内部統制システムの一環・一内容としても捉えられる。

・ 会社法（平成十七年七月二十六日法律第八十六号）

対象：

会社法上の大会社

（最終の貸借対照表において、資本金５億円以上または負債２００億円以上の会社）。

義務：

取締役会の義務として、内部統制システムの基本方針を決定しなければならない（大会社でない会社の場合は、内部統制システムの基本方針の決定は、取締役会の専決事項とされている

が、義務ではない)。決定内容については事業報告により開示する。

内部統制システムの内容:

内部統制システムの基本方針として決定すべき事項としては、「取締役(委員会設置会社においては執行役)の職務の執行が法令及び定款に適合することを確保するための体制」「その他株式会社の業務の適正を確保するために必要なものとして法務省令で定める体制」とされ、法務省令において更に詳細な規定がある。情報セキュリティを特に取り上げた項目はないが、規定された事項を実現するための手段として、情報管理の体制を整えることが重要な一手段になることが考えられる。

・金融商品取引法

(昭和二十三年四月十三日法律第二十五号、
最終改正:平成十九年六月二十七日法律百二号)

対象:

有価証券報告書の提出義務ある会社のうち一定の上場企業

義務:

対象会社は、内部統制報告書の作成・提出をし、内部統制に関する監査を受けなければならない。

内部統制システムの内容:

財務報告にかかる内部統制が要請されている。企業会計審議会「財務報告に係る内部統制の評価および監査の基準」において「ＩＴへの対応」の項目が挙げられている。

4.4.3. 攻撃者に対してペナルティを課す法律

以下では、情報の所有者の意思に反する情報の取得に係わるものと、情報に対するその他の侵害行為に係わる法律について紹介する。

4.4.3.1. 情報の所有者の意思に反する情報の取得(情報窃盗ほか)

現行法上、包括的な情報窃盗罪は存在しない。情報が記録された紙、CD-ROM、USB メモリ、PC などの媒体を盗んだ場合には、それらの媒体に対する窃盗罪が成立するが、データだけをメールで転送したり、または自分の所有する USB 等の媒体に移して取得した場合には、情報自体に対する窃盗罪を問題とすることはできない。

個人情報保護法でも、個人情報窃盗罪のような規定を設けるべきとの議論もあったが、現在はそのような規定はない。

不正競争防止法では、営業秘密の不正取得・開示・使用行為のうち、不正競争目的があるなど一定の要件を充たす行為について、処罰規定を置いている。ここでの「営業秘密」については、前述のような法の定める要件を充たしている必要があるが、この要件をクリアすれば、媒体の移転を伴わなくても、純粋なデータ自体が保護を受けることになる。目的・対象の限定をした情報窃盗罪とも言えなくもない。

4.4.3.2. 情報に対するその他の侵害行為

情報に対するその他の侵害行為に係わるものとしては、以下の法律などがあげられる。

・著作権法

（昭和四十五年五月六日法律第四十八号、
最終改正：平成十八年二月二十二日法律第百二十一号）

著作権法は、著作物（思想又は感情を創作的に表現したものであって、文芸、学術、美術または音楽の範囲に属するもの）について、著作権者の許可なく複製・公衆送信・送信可能化等の所定の行為をすることを禁じており、著作権侵害行為があった場合には処罰規定もある。

・不正アクセス行為の禁止等に関する法律

（平成十一年八月十三日法律代百二十八号、
最終改正：平成十一年十二月二十二日法律代百六十号）

不正アクセス禁止法では、ネットワークに接続され、ID・パスワード等を入力しないと利用できないようアクセス制御されているコンピューターに対し、他人の ID・パスワード等を無断で入力して不正にアクセスする行為、セキュリティホールを攻撃して不正にアクセスする行為、が処罰の対象とされている。

・刑法

（明治四十年四月二十四日法律第四十五号、
最終改正：平成十九年五月二十三日法律第五十四号）

ウィルス送信など情報セキュリティに対する何らかの侵害行為の結果、業務を妨害した場合は電子計算機損壊等業務妨害、電子データの破壊をもたらした場合には電磁的記録毀棄罪、不正なデータを作成した場合には電磁的記録不正作出・供用罪、システムをに不正な指令を与えて財産的利益を得た場合には電子計算機使用詐欺罪として処罰規定がある。

・ウィルス作成罪

ウィルスの作成を直接処罰の対象とする法令は現行法上存在しないが、ウィルスの作成を処罰対象とする「不正指令電磁的記録等作成等の罪」を刑法中に新たに創設する法案が継続審議中である。2008 年 1 月、「初のウィルス作成者の摘発事例」として、京都府警が大学院生を逮捕したことが報道されたが、これはウィルスの作用する際に著作権侵害行為が伴うことを問題にして著作権法違反で摘発されたものであり、ウィルス作成罪を欠く法の不備が議論となっている。

4.5. 個人情報保護ガイドラインについて

個人情報保護法が平成 17 年 4 月に全面施行されて、「個人情報保護に関する法律についての経済産業分野を対象とするガイドライン」が平成 16 年 10 月 22 日に経済産業省から出された。個人情報保護法（法第 20 条）で、「個人データの安全管理」のための適切な措置が求められており、経済産業分野を対象とするガイドラインが 2 年経って見直しされ、平成 19 年 3 月 30 日に改訂された。

4.5.1. 経済産業分野ガイドラインについて

経済産業分野ガイドライン本体は、経済産業省ホームページの「個人情報保護」のページ[4.5-1]で入手できる。

本ガイドラインは、経済産業大臣が法を執行する際の基準となる。本文中「しなければならない」と記載されている規定については、それに従わなかった場合は、経済産業大臣により、法の規定違反と判断され得る。

ガイドラインの内容は、

> １．目的及び適用範囲
> ２．法令解釈指針・事例（2-1 定義、２-2 個人情報取扱事業者の義務等、2-3 民間団体付属の研究機関等における個人情報の取扱いについて）
> ３．「勧告」、「命令」及び「緊急命令」についての考え方
> ４．ガイドラインの見直し
> ５．個人情報取扱事業者がその義務等を適切かつ有効に履行するために参考となる事項・規格
> 別添　クレジットカード情報を含む個人情報の取扱いについて

が示されている。

ガイドラインの見直しによる平成 19 年 3 月改正の主な内容は、「過剰反応」、「事業者の過剰な負担」、「クレジットカード情報を含む個人情報の取扱い」の 3 点が挙げられている。

> １．「過剰反応」に対する見直し
> ・ 法令に基づく個人データの提供
> ・ 人の生命、身体又は財産の保護に対する個人データの提供（2-2-1.項）
> ２．個人情報取扱事業者の過剰な負担の適正化に向けた見直し（2-2-3-2 項）
> ・ 安全措置の義務違反とはならない事例
> ・「事故又は違反への対処」を実践するために講じることが望まれる事例
> ３．クレジットカード情報を含む個人情報の取扱いに関する見直し
> ・クレジットカード情報等の安全管理措置として講じることが望ましい事例

しかし、もともとの「個人情報保護法」を十分に理解しないまま改正点だけで対策を講じると、

セキュリティが実用上機能しなくなる可能性がある。ガイドラインの改正点を踏まえて、セキュリティ面を中心に述べる。

「個人情報保護法第 2 条第 1 項」で、この法律において「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう、と定義している。

「改正前のガイドライン」では、「個人情報」とは、生存する個人に関する情報であって、特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。「個人に関する情報」は、氏名、性別、生年月日等個人を識別する情報に限られず、個人の身体、財産、職種、肩書等の属性に関して、事実、判断，評価を表すすべての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報もふくまれ、暗号化されているかどうかを問わない。」と解説してある。

「改正ガイドライン」では、「個人情報」とは、生存する個人に関する情報であって、特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。「個人に関する情報」は、氏名、性別、生年月日等個人を識別する情報に限られず、個人の身体、財産、職種、肩書等の属性に関して、事実、判断, 評価を表すすべての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報もふくまれ、暗号化されているかどうかを問わない。ただし、「2-2-3-2. 安全管理措置（法第 20 条関連）」の対策の 1 つとして、高度な暗号化等による秘匿化を講じることは望ましい。」とあるように最後の下線部の 2 行が追加された。

改正ガイドラインにおいても、「個人情報」は暗号化されているかどうかに拘らず「個人情報」の対象であることには変わりはない。改正ガイドラインでは、個人情報保護法第 20 条で規定されている「安全管理措置」についての 1 つの対策として、「高度な暗号化等による秘匿化」が具体的に例示された。

ガイドライン 2-2-3-2 項において、「組織的安全管理措置として挙げられた項目を実践するために講じることが望まれる手法の例示」の中で、「事故又は違反への対処」として挙げられている項目のうち、「影響を受ける可能性のある本人への連絡」及び「事実関係、再発防止策等の公表」は、「高度な暗号化等の秘匿化が施されている場合」は、上記の連絡や公表を省略しても構わないと考えられる、と示されている。

「高度な暗号化等による秘匿化」によっても個人情報保護法の対象となる情報であるが、「高度な暗号化等による秘匿化」の対策が講じられている場合は、「事故又は違反」があった場合に、本人への謝罪や連絡、及び事実関係や再発防止策等の公表を省略しても構わないとして、事業者の過剰な負担（対処の負担）は軽減されるが、その他の義務は同じである。

また、「高度な暗号化等による秘匿化が施されている場合」について、ガイドラインに関する Q&A で、『例えば、電子政府推奨暗号リスト又は ISO/IEC18033 に挙げられている暗号アルゴリ

ズムによって個人データを適切に暗号化し、かつ、復号（平文化）のためのかぎ（鍵）が適切に管理されていると認められる場合など、十分な秘匿性が確保されている場合は、「高度な暗号化等による秘匿化が施されている場合」に該当すると考えられます。（2007.3.30）』と説明されている。

以上のことは、事故等によって個人情報が漏洩するケースが多々あることに関し、「事業者の過剰な負担」を軽減するために、情報の管理をするのに暗号化等による秘匿手段が有効であると示されたと言える。しかし、この秘匿手段の管理のために新たな負担が生じては意味が無い。十分な秘匿性を確保するために、暗号化の他に新たな秘匿手段（例えば、秘密分散技術を用いた手段など）で、簡便な方法の実用化を待ちたい。

個人情報漏洩事案が発生する場として、事業者が委託先に委託する場合がある。個人情報保護法第 22 条で、「個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。」とある。

ガイドラインでは、委託先の監督 2-2-3-4（法第 22 条関連）で、

- 委託者及び受託者の責任の明確化
- 個人データの安全管理に関する事項（・個人データの漏洩防止、盗用禁止に関する事項、・委託契約範囲外の加工、利用の禁止、・委託契約範囲外の複写、複製の禁止、・委託契約期間、・委託契約終了後の個人データの変換・消去・廃棄に関する事項）
- 再委託に関する事項
- 個人データの取扱状況に関する委託者への報告の内容及び頻度
- 契約内容が遵守されなかった場合の措置
- セキュリティ事件・事故が発生した場合の報告・連絡に関する事項

等が記載されているが、委託元・委託先間のデータのやり取りで、秘匿化のための暗号化等の鍵管理などで煩わされることの少ない、秘匿化の手段が望まれる。

ガイドライン 4 章の「ガイドラインの見直し」に規定されているように、一回目の見直しが平成 19 年 3 月に行われた。しかし、経済産業省は、業務委託先から個人情報が漏洩した最近の例を挙げ、「委託先が大規模かつ重大な個人情報漏洩を起こした事実は少なくない。また、委託元が十分に監督を行っていなかったことに起因する事案も多い」と述べている。そのことから、今回、類似する個人情報漏洩事案の防止に向け、委託先に対する委託元の監督義務のあり方について、ガイドラインの見直しを行ったという。経済産業省は平成 19 年 12 月 18 日、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」の改正案に関するパブリックコメント募集を開始した（期間は 2008 年 1 月 17 日まで）。改正予定のガイドラインの概要を含め、個人情報保護法制について広く告知し、事業者の理解および意見を聴取し今後の見直しの参考とすることを目的として、「経済産業分野を対象とする個人情報保護ガイドラインに関する説明会」を大阪（2 月 28 日）、東京（3 月 4 日）で行う。改正ガイドラインは 2 月 29 日に発行された。「改正ガイドライン」及び「Q&A」は、経済産業省ホームページの「個人情報保護」のページ[4.5-1]で入手できる。

今回の改定は、個人情報の取り扱いを要する業務委託に関するものである。委託先に対する必要のない個人データの提供を禁止することや、委託元による委託先に対する「必要かつ適切な監督」の内容を明確化することが盛り込まれている。具体的には、委託する業務内容に対して、委託先に必要のない個人データを提供しないことを明記している。また、委託先に対する監督義務については、「委託先を適切に選定すること」「受託者との間で必要な契約を締結すること」「受託者における委託された個人データの取扱状況を把握すること」を明記している。

以上、経済産業省の「経済産業分野を対象とするガイドライン」について述べたが、他の省庁もそれぞれにガイドラインをだしているので、いくつかの主な項目について比較したものを表に示す。

4.5.2. 各省庁の個人情報保護ガイドライン（要約）

各省庁の個人情報保護ガイドラインの違いを以下に示す。

（1）個人情報

経済産業省	個人情報とは・・・ 暗号化等によって秘匿化されているかどうかを問わない（ただし安全管理措置の対策の一つとして、高度な暗号化等による秘匿化を講じることは望ましい）。
厚生労働省	個人情報とは・・・ 暗号化されているか否かを問わない。
金融庁	暗号化等の記述なし。
総務省	暗号化等の記述なし。

（2）保有個人データ

経済産業省	識別される特定の個人の数の合計が過去 6 ヶ月以内のいずれの日においても 5,000 人を超えない事業者は個人情報取扱事業者から除かれる。
厚生労働省	識別される特定の個人の数の合計が過去 6 ヶ月以内のいずれの日においても 5,000 を超えない事業者（小規模事業者）を除くものとされている。しかし、医療・介護関係事業者は、個人情報を提供して医療・介護関係事業者からサービスを受ける患者・利用者等から、その規模等によらず良質かつ適切な医療・介護サービスの提供が期待されていること、そのため、良質かつ適切な医療・介護サービスの提供のために最善の努力を行なう必要があること、また、患者・利用者の立場からは、どの医療・介護関係事業者が法令上の義務を負う個人情報取扱業者に該当するかが分かりにくいこと等から、本ガイドラインにおいては個人情報取扱業者としての法令上の義務等を負わない医療・介護関係事業者にも本ガイドラインを遵守する努力を求めるものである。
金融庁	―
総務省	―

（3）個人データの開示

経済産業省	個人情報取扱事業者は、本人から、自己が識別される保有個人データの開示を求められた時は、本人に対し、書面の交付による方法(開示の求めを行った者が同意した方法があるときはその方法)により、延滞なく、当該保有個人データを開示しなければならない。
厚生労働省	医療・介護関係事業者は、本人から、当該本人が識別される保有個人データの利用目的の通知を求められたときは.....遅滞なく通知しなければならない
金融庁	個人情報取扱事業者は、本人から、当該本人が識別される保有個人データの開示を求められたときは、本人に対し、遅滞なく、保有個人データを開示しなければならない。
総務省	電気通信事業者は、本人から、当該本人が識別される個人情報の開示を求められたときは、本人に対し、書面の交付による方法(開示の求めを行った者が同意した方法があるときは、当該方法)により、遅滞なく、当該個人情報を開示するものとする。

（4）漏えい等が発生した場合の対応

経済産業省	二次被害の防止、類似事案の発生回避等の観点から、個人データの漏えい等の事案が発生した場合は、可能な限り事実関係、再発防止等を公表することが重要である。ただし、二次被害の防止の観点から公表の必要性がない場合には、事実関係等の公表を省略しても構わないものと考えられる。
厚生労働省	個人情報の漏えい等の問題が発生した場合には、二次被害の防止、類似事案の発生回避の観点から、個人情報の保護に配慮しつつ、可能な限り事実関係を公表するとともに、都道府県の所管課等に速やかに報告する。
金融庁	1. 監督当局に直ちに報告すること。 2. 二次被害の防止、類似事案の発生回避等の観点から、漏えい事案等の事実関係及び再発防止策を早急に公表することとする。 3. 漏えい事案等の対象となった本人に速やかに漏えい事案等の事実関係等の通知を行なうこととする。
総務省	１．速やかに、当該漏えいに係る事実関係を本人に通知するものとする。 ２．二次被害の防止、類似事案の発生回避等の観点から、可能な限り、当該漏えい等に係る事実関係その他の二次被害の防止、類似事案の発生回避等に有用な情報を公表するものとする。(「可能な限り」とは、セキュリティの観点から公表するとかえって二時被害の拡大や類似事案の増大につながるようなものは公表することは要しないが・・・ 3. 当該漏えい当に係る事実関係を総務省に直ちに報告するものとする

（５）訂正・利用停止等　理由の説明

経済産業省	保有個人データの公表・開示・訂正・利用停止等において、その措置をとらない旨又はその措置と異なる措置をとる旨を本人に通知する場合は、併せて、本人に対して、その理由を説明するように努めなければならない。
厚生労働省	訂正等、利用停止等又は第三者への提供の停止が求められた保有個人データの全部又は一部について、これらの措置を行わない旨決定した場合、本人に対するその理由の説明に当たっては、文書により示すことを基本とする。その際は、苦情への対応を行う体制についても併せて説明することが望ましい。
金融庁	本人から求められた措置の全部又は一部について、その措置をとらない旨を通知する場合又はその措置と異なる措置をとる旨を通知する場合は、本人に対し、措置をとらない又は異なる措置をとることとした判断の根拠及び根拠となる事実を示し、その理由を説明することとする。
総務省	本人から求められた措置の全部又は一部について、その措置をとらない旨を通知する場合は又はその措置と異なる措置をとる旨を通知する場合は、本人に対し、その理由を説明するよう求めるものとすることを規定したものである。なお、本人の求めに応じた措置をとる場合は、本人の求めによることがその措置をとる理由であり、理由が自明であることから、理由を説明することとはしていない。

（６）開示等の求めに応じる手続き

経済産業省	開示等の求めにおいて、その求めを受付ける方法を定めることができる。また、その求めを受付ける方法を定めた場合には、本人の知り得る状態に置いておかなければならない。なお、個人取扱事業者が、開示等の求めを受付ける方法を合理的な範囲で定めたときで、求めを行った者がそれに従わなかった場合は、開示等を拒否することができる。
厚生労働省	医療・介護関係事業者は、保有個人データの開示の求めに関し、本人に過重な負担を課すものとならない範囲において、その求めを受付ける方法を定めることができる。
金融庁	法 29 条に従い、開示等の求めを受付ける方法を定めた場合には、第 23 条に定める「個人情報保護宣言」と一体としてインターネットのホームページでの常時掲載を行うこと、又は事務所の窓口等での掲示・備え付け等を行うこととする。
総務省	電気通信業者は必ずしも申請書の様式や窓口の特定等を定める必要があるものではなく、定めない場合には自由な申請を認めることとなる。一方、電気通信事業者が同項の規定に基づき申請書の様式等の求めを受付ける方法を定めたときは、本人は、当該方法に従って、開示等の求めを行う必要がある。

（7）プライバシーポリシー

経済産業省	個人情報取扱事業者は、「個人情報保護に関する考え方や方針に関する宣言（いわゆる、プライバシーポリシー、プライバシーステートメント等）」を策定し、ウェブ画面への掲載または店舗の見やすい場所への掲示。
厚生労働省	個人情報保護に関する考え方や方針に関する宣言（いわゆる、プライバシーポリシー、プライバシーステートメント等）及び個人情報の取扱いに関する明確かつ適正な規則を策定し、それらを対外的に公表することが求められる。
金融庁	個人情報に対する取組み方針を、あらかじめ分かりやすく説明することの重要性にかんがみ、事業者の個人情報保護に関する考え方及び方針に関する宣言（いわゆるプライバシーポリシー、プライバシーステートメント等。本ガイドラインにおいて、「個人情報保護宣言」という。）を策定し、例えば、次に揚げる内容をインターネットのホームページへの常時掲載、又は事務所の窓口等での掲示・備付け等により、公表することとする。
総務省	個人情報保護についての社会の信頼を確保するため、電気通信事業者は自らの個人情報の取扱いに関する方針についての宣言をプライバシーポリシーとして公表し、これを遵守するものとする。

また、「経済産業分野を対象とするガイドライン」は、経済産業省が所管する分野及び経済産業大臣が主務大臣に指定された特定分野における事業者等が取り扱う個人情報について定めているが、これらの事業者における従業員の個人情報に関する部分については、厚生労働省の指針（平成１６年厚生労働省告示第２５９号）で雇用管理に関する個人情報の適正な取扱いと整合している（従業員及び従業者の用語は、ガイドライン 2-2-3-3 項の「従業者の監督」の項を参照）。

4.6. 情報セキュリティ向上に関する企業の取組みについて

4.6.1. ヒヤリングの概要

情報セキュリティＷＧでは、電子商取引環境における情報セキュリティ向上に向け、企業間や経営・管理者層と技術・実務者層での情報セキュリティに対する共通理解を支援するため、業平成１９年１１月上旬から１２月上旬にかけて下記の４つの別の態様の企業(図 4.5.2‐1 参照)に対して、情報セキュリティ対策への取組みや考え方全般と開示可能な具体的な対策事例について、その対応を決定する際にトリガーとなった法令、通達、社内規約等との関係についてのヒアリングを行った。

（Ａ社）業界トップの企業（大企業）

（Ｂ社）複数業界にまたがる印刷業界のトップクラスの企業（大企業）

（Ｃ社）複数業界にまたがるコンベンション等の開催を支援する企業（中小企業）

（Ｄ社）数名で法務に関する業務を行う小規模事務所

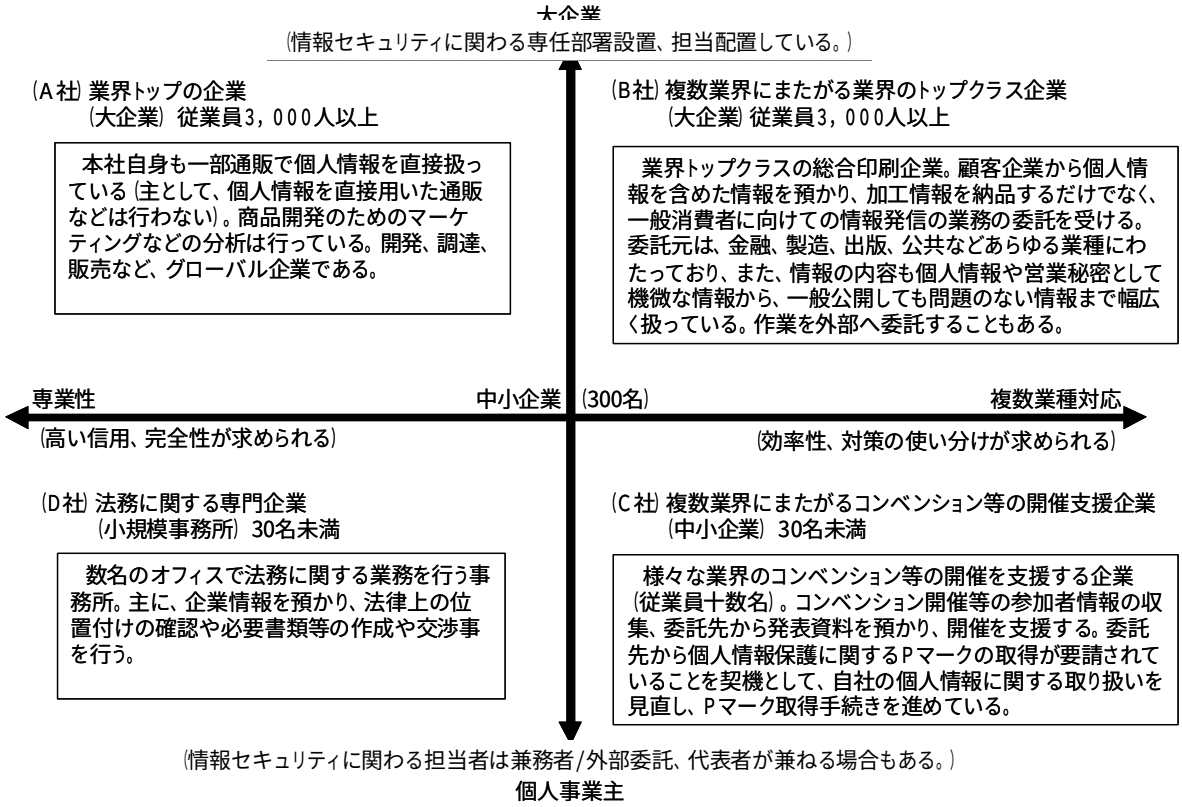


図4.5.2-1 ヒヤリング実施企業の特徴

ー 情報セキュリティ対策への取組みや考え方全般に関するヒヤリング ー

ヒアリング内容は

a）御社の情報セキュリティ対策全般について
b）開示可能な具体的対策について、その対策を講じる根拠となった法令等と、その対策との関連性について
c）個人情報保護に関する法律やガイドラインについて
d）個人情報保護や情報セキュリティ向上に関する組織的取組み、環境について
e）情報セキュリティに関する活動組織に望むこと

の５項目とし、経営者または管理者もしくは情報セキュリティ部門 実務担当者を対象とした。なお、ヒアリング結果の熟知度評価の判断基準は以下の通りに定めた。

◎大変よく知っている
　当該事項をよく調べ、それを知識として、応用して適用している。
○よく知っている
　当該事項をよく調べ、それを知識として、適用している。
◇知っている
　当該事項の意義までは理解しているが、詳細は知らない。
△よく知らない
　当該事項のキーワードは知っている。
×知らない
　当該事項のキーワードも知らない。

【各社からの回答内容】（詳細は参考資料 参照）

（１）個人情報保護法、不正アクセス行為の禁止等に関する法律他

４社とも知っているとの回答であり、社内周知徹底や保護推進のために役員を長とする委員会を設置している企業もあった。

（２）個人情報保護ガイドライン（経済産業省、ＥＣＯＭ、他）

自社の業界の監督官庁のガイドラインのほか、事業展開上、関連するものについては他業界の省庁のものも把握しておく必要がある。

（３）情報セキュリティ管理基準（経済産業省、他）

この管理規準をもとに現場に出向いて内部監査や外部委託先の監査を行ったり帰属業界のためのＱ＆Ａ集の策定に役立てている企業もある。

4.6.2. ヒヤリングの結果

（１）個人情報保護や情報セキュリティ向上に関する組織的取組みについて

(a) OECD 個人情報保護 8 原則、ISO27000 シリーズ（BS7799,etc）

４社とも認知していた。

(b) プライバシーマーク認定制度[4.6-1]、ISMS 適合性評価制度[4.6-2]

４社とも認知しており、認定されているだけでなく審査員補を担っている企業もあるが、認定を受ける、維持するには高額な費用がかかるのが難点である。

(c) 情報セキュリティ対策ベンチマーク(自己評価)[4.6-3]

企業規模によって実践した企業とそうでない企業とに分かれた。

(d) 情報セキュリティガバナンス、情報セキュリティ報告書

企業規模によって認知している企業とそうでないところに分かれるが、認知されていても現段階では策定に取り組んでいるところはなかった。

（２） 情報セキュリティ向上に関する環境整備について

(a) 早期警戒パートナーシップ(JVN[4.6.-4]等)

ＣＲＹＰＴＲＥＣ暗号技術評価報告[4.6.-5]

企業規模によって認知しており、契約活用している企業とそうでないところに分かれる。

(b) ISO／IEC 15408(Common Criteria)について

セキュリティ製品の事業部門がある企業は大変よく知っており、それを調達条件として意識しているが、それ以外は調達条件とはしていない。

(c) 管理が必要な情報と自社特有の情報セキュリティ環境整備について（設問 B）

特徴的な回答を以下に示す。

- 持ち出しデータの暗号化などを行っている。
- データの持ち出しは極力やめ、できればシンクライアントにしていく必要もあると考えている。
- 月間何千万件にもおよぶ個人情報を含む仕事を受託している企業では業務が発生するたびに、個人情報を含む業務であるか、識別番号を付け、システム上でも管理している。
- Ｐマークを取得しようとしている

・ 企業ではコンサルタントから、情報の秘匿性(機微度)によって情報のカテゴライズをするように指導され分類管理するようになっている。
・ その他、紙による現物主義が必要な企業では提出書類などは入力、印刷して提出先に持ち込む
・ 保存対象書類は少なくとも 3 年間は保存する必要があるため、事務所が書庫になっている。
・ 現物をイメージで取り込むことも必要であるが電子保存の目的が原本保証、偽造防止というよりも、経過、経緯説明などで再利用の必要性によるものとなっている。

(d) 情報システムの管理はどのようにされているか？

この設問は小規模事業者 2 社の企業に対して行った。その取り組みの例を示す。

・ 建屋、事務所への入退室はビル管理会社が管理している。
・ 休日は本人確認が取れないと入室できないようにしている。
・ Ｗｅｂサーバ、メールサーバはＡＳＰに（外部）委託し、会社の共有サーバは自社内に設置し、事務所内にある共通ＤＢ、プリンターサーバはアクセス履歴を取っている。
・ システム管理についてはＰＣに詳しい担当者が行う、または外部の専門家と相談しながらめる。
・ 外部のセキュリティソフト、Windows アップデートなどは随時行うなどの対応をとっている。

（3）情報セキュリティ対策でのギャップ（違いや矛盾）について

(a) 法律・ガイドラインと実務とのギャップ

様々な分野からの仕事を受託している場合、それぞれの自社事業部や顧客企業ごとに、関わる業界や主務官庁が異なる。また、それぞれの指針を理解し、ギャップを生じないようにする必要がる。実務においてはコンサルティング会社からオフィスで、トイレに行くにも、机の上に書類を残さないことも必要であるとの指摘もあるが、少人数の組織の場合、情報セキュリティの専任の担当者が監視しているわけではなく、監視を１００%達成させることは困難となる。情報セキュリティはどうやって徹底させるのかが明確でないという声もあるが、組織的に社内規程や対策マニュアルを策定し、ＰＤＣＡサイクルで運用を試みている企業もあった。

(b) 経営者と実務者の認識のギャップ

過去にワームの配信など事故を経験しているところは、役員も技術的な話も含め、実務面での課題も概括的には理解されている。企業規模の大きいところは情報セキュリティ管理推進部会設置するなど組織的に経営層を巻き込んでトップダウンで取り組んでいるが、認識については企業規模にかかわらず経営者と実務者のギャップはないという回答であった。

(c) 委託元と委託先の実施レベルのギャップ

委託先へ自社と同等の管理レベルを求めることは課題であり、特に物理的なセキュリティと人的なセキュリティに関しては監査基準を設けている企業がある。委託先は①信用調査、②契約事項、③監査基準（品質、どういうチェックをしているか）の３セットで監督し、監査基準項目としては５０項目位設けている企業もある。さらに、仕事が終了した後の管理、

例えば親展ＤＭ（ダイレクトメール）の不達の事後処理も重要であって、廃棄処分の徹底も必要となっている。不達のダイレクトメールは顧客企業への返却を原則としているが、委託先に不達となったＩＤ番号のみ（個人情報を含まない形で）情報を返す場合もある。

委託先の選定ならびに委託作業に実行において 150 項目程度の評価項目を設定しているところもあり、その評価項目は必須項目、実施までの改善項目、努力目標に分かれている。設定項目についての質問票を委託先より返答を回収し、その内容によっては実際に訪問、面接して確認（実地監査）する場合もある。委託先選定では業務委託内容によってどこにでも委託できるというものではないこともあるため、Ｐマーク取得は必須項目としていない。

IT セキュリティ関連の委託については、情報システムのインフラ監査も実施する場合もある。逆に、受託企業からの視点では、委託元から契約時の要請は概括的で、情報を漏らさないという条項だけが必須となることが多い。絶対漏らしてはならないことに関してはメモさえしない場合がある。

（4）情報セキュリティに関する活動組織に望むこと

特徴的な回答を以下に示す。

- 海外事業との関連でガイド、ルールの変更があった際、できれば 1 か月以内に英訳がほしい。プライバシーマークなどの認定では段階的に審査のレベルが上がってきているが、瑣末な現象のみに焦点をあてるばかりで本質的な問題から逸れ、形骸化してきていないか。
- 審査基準をあげていくと、何の目的でやっているか見えなくなっていくのではないかということが気になっている。
- プライバシーマークや ISMS 認定取得のためのコンサルテーション（指導）フィーは小さな会社としては、費用負担が大きい。
- 個人情報保護法施行以来、個人情報の照会が難しくなっている。
- 情報セキュリティ活動において何をすべきかの具体的な実施項目を提示すべきである。
- インターネットはなんとなく不安なところがあるのだけれど、どこが安全でどこが危険なのかが見えないため、どこを支援してほしいと言うのが難しい。

4. 6. 3. 情報セキュリティ WG での検討と提言

ヒアリングの結果を受け、現在の情報セキュリティに関する活動に対する課題を情報セキュリティ WG にて検討した。

（1）情報セキュリティ WG での自由討論

情報セキュリティの罰則が強化されると委託に逡巡する傾向が強まり、極端にいえば経済全体が円滑に動かなくなるのではとの懸念や、ユビキタス（情報社会）とその安全はトレードオフの関係にあるため、中小企業に大企業と同じ網（罰則強化の法律）がかかることになると、中小規模の委託先はかなり厳しくなると思われるといった声があった。

プライバシーマーク規格の改訂で、トップマネージメントが強く打ち出され、事故を起こせば社長が謝罪するなどの責任が明確になり、会社の規模に関わらず経営層が本気になってきていると認識しているという意見がある反面、それを取得している企業については外見的にはＯＫに思えるが、プライバシーマーク認定の委託先による紛失事故が起きたこともあって、新規委託先の

場合は現場確認をできるだけ行ない、プライバシーマークは委託先選定の１つの重要な判断要素ではあるものの、絶対条件ではないと考えているという声もある。協議会組織に期待することについてはデジタルフォレジングに関してログをどこまで取るのか、委託先にはどこまで取らせなければならないのか目安を提示する必要を唱え、自らはデータを残してどういう時に情報漏えいにつながる危険性があるかということを考え始めている企業もあった。

最低管理基準に関しては、ソフトハウス（セキュリティベンダー）の脆弱性チェックサービスの費用負担が重いため、情報セキュリティの仕組み（セキュリティスキャンなど）は限られた範囲で実施しているが、コスト面が改善され、標準になってくると、セキュリティベンダのパイが広がってくるのではないかという意見があった。

ヒアリングした各社の取り組みへの感想としては、業界トップ、企業コンプライアンス重視の会社においては、ＯＡ担当（システムの運営管理)、個人情報保護委員（個人情報漏えい防止）のほかに、職場から法令エキスパート委員を推薦に任命するなどの体制をとっているが、法令エキスパートが個人情報だけでなく、営業秘密や不正競争防止、ＳＯＸ法などを従業員に対し、どの程度意識つけていくかが情報経済社会を健全に発展させるかのカギのように感じられた。

委託先管理については数多くの評価項目を用意しながら、それらを必須項目、努力目標に分けてきちっと管理しつつ、委託先を教育していく姿勢も見受けられ、このヒアリング先の実務者は個人情報保護について前向きに取り組んでおり、また、その経営者にも理解がかなりあると思われた。

大企業の場合、情報提供者（消費者、モニタ、従業員）との合意（オプトイン／オプトアウト、契約事項、口頭／文書）や、資本関係のない委託先管理でどこまでの情報セキュリティを要求できるか、業界に関係なく、共通の基準と、企業レベル（大企業、中堅中小、個人事業主)、情報を取り扱う業態（インターネット、対面など）を含め、企業が情報を預かる先との基準、企業が情報を預ける先との基準と応用（事例）についてまとめていくことの必要性を感じた。

顧客が金融から公共、一般産業まで幅広い分野に亘っている業界では、業界としてのガイドラインを纏めている。情報セキュリティが会社の信用がビジネス受注のポイントであるため、かなり良く調査を行いながら、しっかり個人情報管理を進めている。特に、現場における個人情報保護のＱ＆Ａ集などは、データの受け渡し際の項目や、入社時やアルバイト採用時の誓約書の例など、具体的な定義もあり、他の業界でもかなり参考となる。従業員への徹底（社内教育）は、カードサイズの誓約書、小さな文庫本を用意し、携行させるようにしている。ケアレスミスの防止、悪意ある持ち出しを許さない管理強化など、企業として情報セキュリティに対する意気込みを感じる。

どういう時にどこにある情報が漏えいにつながる危険性があるかなど、危険性の発見の仕方についての検討を進めている企業もある。委託業務の場合は、企業間でのＩＤ連携などの仕方について議論していけると、企業の効率的な情報セキュリティ対策の実現に近づくと思われた。

（２）中小規模の企業においては情報セキュリティの取り組みについて

今回のヒアリングの内容から、中小規模の企業においては情報セキュリティの取り組みについて、人員、コスト、情報収集面でのハンデキャップがあり、その改善が最大のポイントであることを確認した。予定されている「個人情報の保護に関する法律についての経済産業分野を対象

とするガイドライン」の改正においては委託先の監督の強化が要請されているが、中小規模の企業のなかには当該ガイドラインに定める体制を整備する過渡期にある会社や、受託する業務の内容・個人データの性格によって、必ずしも当該ガイドラインに規定されている事項を遵守するまでもない場合もあり、当該ガイドライン上の委託先の選定基準・評価基準を厳格に適用しすぎると、委託先としてこれらの企業を排除することになりかねない。委託者による定期的な状況の把握を契約に明記し、また把握の実施状況を記録に残すこと等を条件とすることで委託を認める必要もあると思われる。

情報セキュリティについての技術革新と法令・規準での制限の高度化が進むほど、対応に要する人員や設備投資が困難な中小規模の企業が取り残されていく危険性が高まる。このことは委託元となる企業においても、業務委託先として優れた高度専門的技術を備えた中小企業であっても、情報セキュリティについて不備がある場合は委託対象からはずさねばならなくなり、委託先の選定に苦慮することになる。一例としてあげれば、少規模ながら優れた独自の印刷技術を保有している企業が委託元の従業員の写真付身分証明書の印刷を受託する場合、個人情報保護法で義務付けられている安全管理措置に不足があるため業務委託ができないという場合である。

こうした事態を回避するためにも大規模会社のように専任の推進部門や各部署での担当者の設置ができない中小企業対する容易で安価な対策パッケージソリューションの開発・提供と個人情報保護管理についての従業者教育など人的安全管理措置についての運用面での啓発が早急に必要である。

（3）情報セキュリティ向上に向けた組織間の連携について

大企業の場合、自社内で「法律･ガイドラインと実務のギャップ」や「経営者と実務者の認識のギャップ」を埋めるために、法律やガイドラインの解釈に対する教育や、かかわる業界や主務官庁、地域の指針を個々に理解し続ける活動を、委員会や代表者会議を設置すると言った組織的な運営により懸命に実施している姿が浮かびあがる。しかし、委託先等の関連企業に対しては、自社と同じ管理レベルを求めることは難しく、独自に評価項目を設定し、個々に評価しているのが実情である。

中小規模の企業の場合、「経営者と実務者の認識のギャップ」は、企業規模によらず「無い」との回答が寄せられた。当然のことながら、中小規模の企業の場合は、必然的に経営者と実務者が直接会話しており、認識を合わせる事が容易な反面、多くの意見を取り込むことは無いものと推察される。この穴を埋めるために中小規模の企業では、外部のコンサルタントやＰＣの専門家に指導を仰いだりしているが、この外部への委託費用が大きな負担となっているのが実情である。又、担当者個人のスキルを向上する等の方策を取っていると思われるが、専任者を置く事はできず、限界もあり得るものと推察される。

「委託元と委託先の実施レベルのギャップ」は、大企業が委託先に対し個々に評価基準を設け、評価している。一方、評価される側となり得る中小規模の企業側では、個々の契約毎に要請に応じて対応したり、暗黙の守秘義務の上で進められているのが実情である。また、「情報セキュリティに関する活動に望むこと」の解答からは、中小規模の企業が、自社を取り巻く他社が進める情報セキュリティの向上施策や、自社で進める情報セキュリティの向上施策により、業務効率の低下を招いているが、これを解消する具体的な術が分からないといった課題も見え隠れしている。

こうした検討の結果からは、以下の課題が浮かびあがる。

・大企業は、独自の解釈と運営で個々に実施しているが、委託先等の関連企業に同じ管理を求めることが難しい。

・中小企業は、外部のコンサルタント等への委託費用が大きな負担となっている。

・中小企業が、委託先として業務を行なう際には、個々の委託元毎に対応している。

・業務効率の低下を解消する具体的な術が分からない。

どれも難しい課題ではあるが、大企業も中小企業も共に情報セキュリティの質を向上させていくことは、この国で安全・安心なＥＣを普及していくためには必要不可欠な事と考える。このために、この情報セキュリティ対策でのギャップを埋めることも必要と考える。

更に、個々の企業が独自に進めている情報セキュリティに関する活動の共通認識を持ち、互いに評価し、責任分担することが出来れば、お互いの評価結果を相互に理解し、協力できる可能性がある。大企業での効率向上はもとより、特に、中小企業が個々の委託業務毎に実施している情報セキュリティの向上のための業務を削減できる可能性が考えられる。業務の削減により、費用の圧縮やより高度な業務の実施が可能となり、経済と産業全体の発展に繋がる可能性も秘めている。このため、例えば、企業間でのＩＤ連携等の枠組みや、このための法律・ガイドラインの解釈や評価手法の統一化が望まれる。

いずれも、業務効率の低下を招かずに情報セキュリティの向上を図るためのひとつの方策であると考える。今後、本ＷＧで案出した解消に向けた提言を、より具体化していく活動が継続することを切望される。

参考文献･資料

[4.3-1]JIPDEC：財団法人 日本情報処理開発協会 ホームページ http://www.jipdec.jp/

[4.5-1]経済産業省：情報政策ホームページ（個人情報保護）
http://www.meti.go.jp/policy/it_policy/privacy/index.html

[4.5-1]JIPDEC：プライバシーマーク認定制度 http://privacymark.jp/

[4.5-2]JIPDEC：ISMS 適合性評価制度 http://www.isms.jipdec.jp/

[4.5-3]IPA：情報セキュリティ対策ベンチマーク
http://www.ipa.go.jp/security/benchmark/index.html

[4.5-4]早期警戒パートナーシップ(JVN 等) http://jvn.jp/

[4.5-5]ＣＲＹＰＴＲＥＣ暗号技術評価報告
http://www.ipa.go.jp/security/enc/CRYPTREC/index.html

5.1. 情報セキュリティのリスクの今日的状況

2000 年代初頭は、単なるハッキングやウィルスによるサーバ停止など広範囲な一般ユーザを困らせる愉快犯的な情報セキュリティ事故が多かった。それらはファイヤ・ウォールの設置やセキュリティ・パッチの適用、ウィルス対策ソフトの導入が進んだことにより回避されるものとなる。

近年は標的を定め、情報悪用による金銭的利益を追求する情報セキュリティ・リスクが増大している。具体的には入手したユーザ ID やパスワードを具体的に使用し、ユーザに金銭的被害を与える事故が多く発生している。

2005 年 4 月施行したいわゆる「個人情報保護法」により、企業は情報漏えい事故を積極的に開示せざるを得なくなり、一般ユーザの情報セキュリティに対する意識は非常に厳しくなってきている。

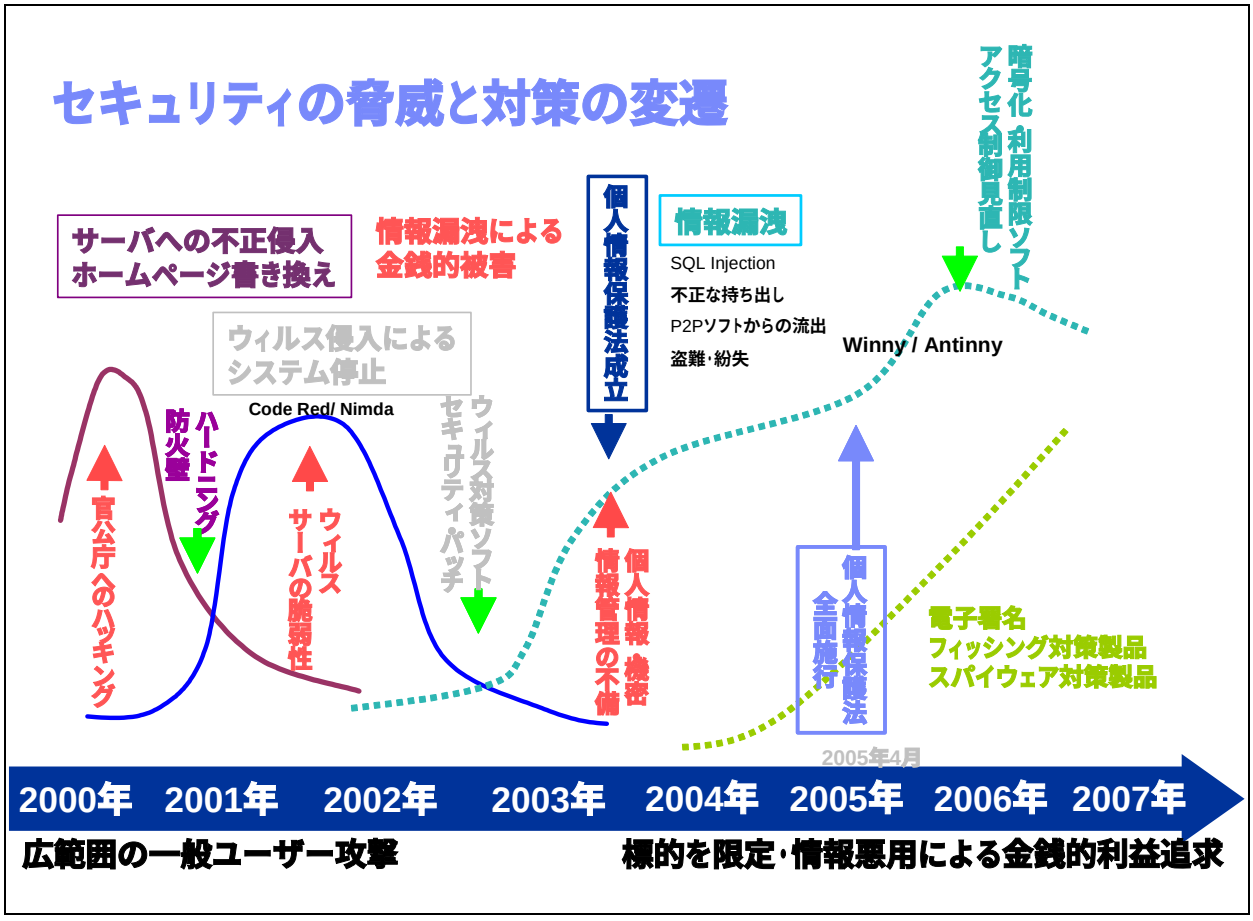


図 5.1-1 セキュリティの脅威と対策の変遷

（提供：日本アイ・ビー・エム株式会社）

独立行政法人 情報処理推進機構(IPA)の調査[5.1-1,2]によると、一般ユーザの情報セキュリティに対する意識は向上の傾向があるが、実際の事象の理解度は低いことが表されている。これは、一般ユーザが常に不安を抱えながらの利用を表したものとも言え、情報セキュリティが高い企業へ依存度が潜在的に高いということが推察できる。

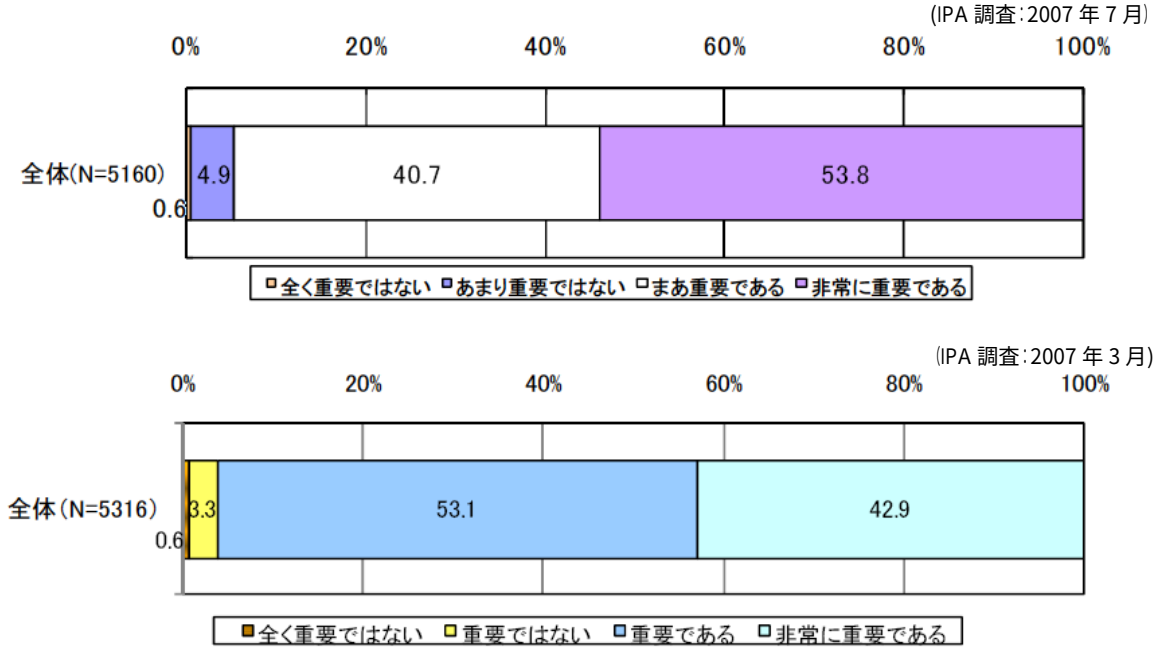


図 5.1-2 情報セキュリティに対する意識

ー独立行政法人 情報処理推進機構(IPA) 情報セキュリティに関する新たな脅威に対する意識調査[5.1-2, p34]よりー

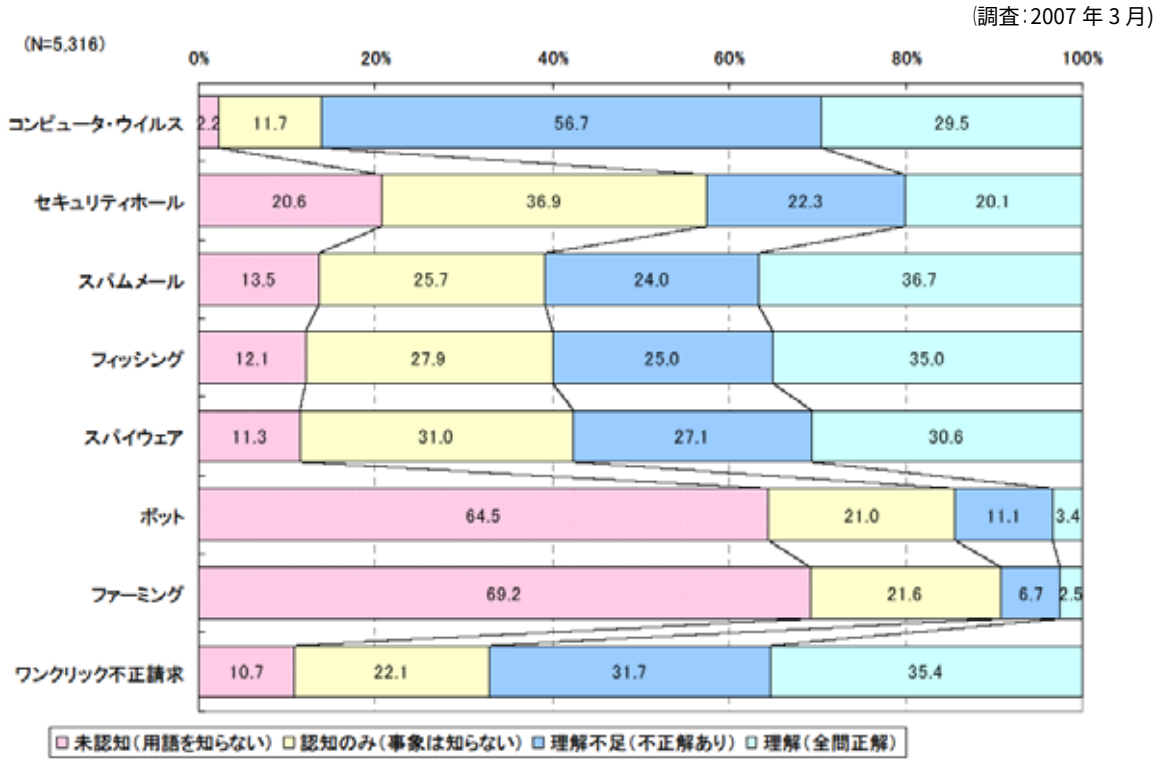


図 5.1-3 情報セキュリティに関する事象の理解度

ー独立行政法人 情報処理推進機構(IPA) 情報セキュリティに関する新たな脅威に対する意識調査[5.1-1, p15]よりー

一方、経済産業省　平成 18 年情報処理実態調査結果[5.1-3]によれば、企業においては何らかの情報セキュリティ対策[図 5.1-4]をとってはいるものの、その対策費用は減少傾向[図 5.1-5]にあり、また、情報セキュリティ向上以外の効果[図 5.1-6]については認められないとする企業が 50%を超えている。今後の企業における情報セキュリティのさらなる向上のためには経営者におけるその効果について可視化することが必要と考える。

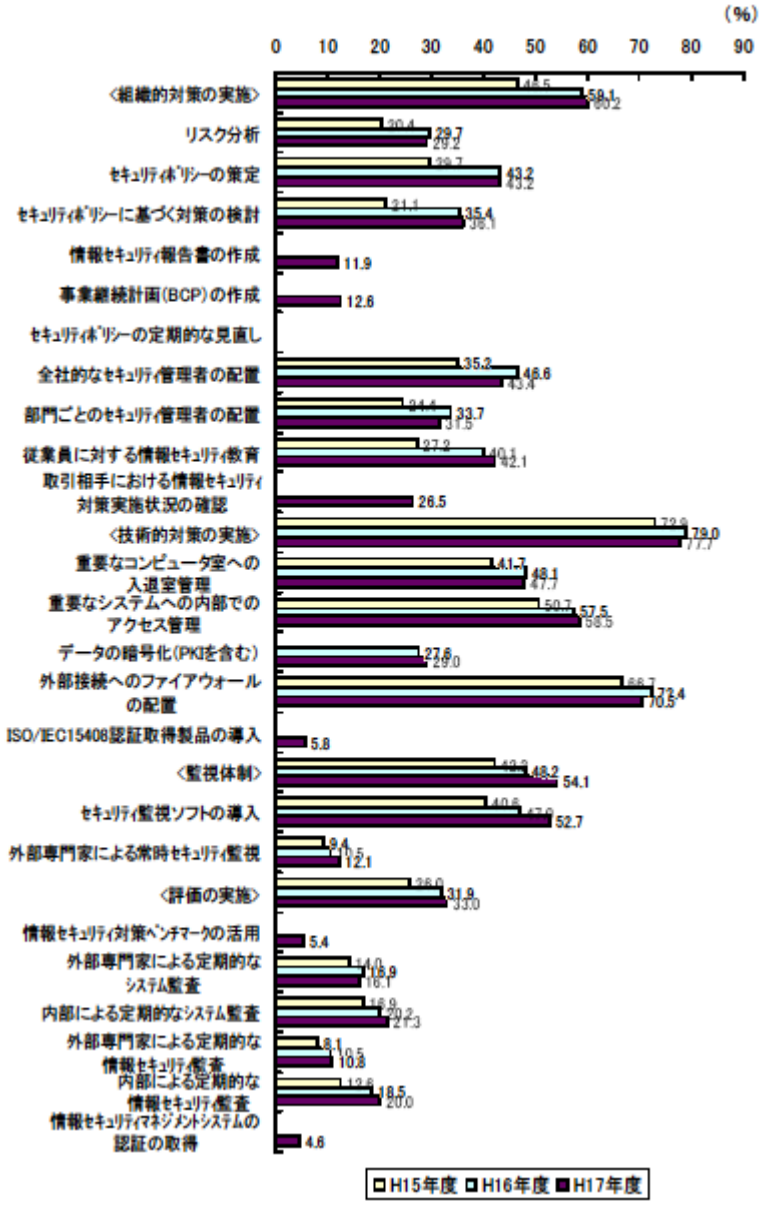


図5.1-4　各情報セキュリティ対策について実施している企業の割合の推移

－経済産業省　平成 18 年情報処理実態調査結果 (2007 年 11 月 13 日公表) [5.1-3, 図表 8-4]より－

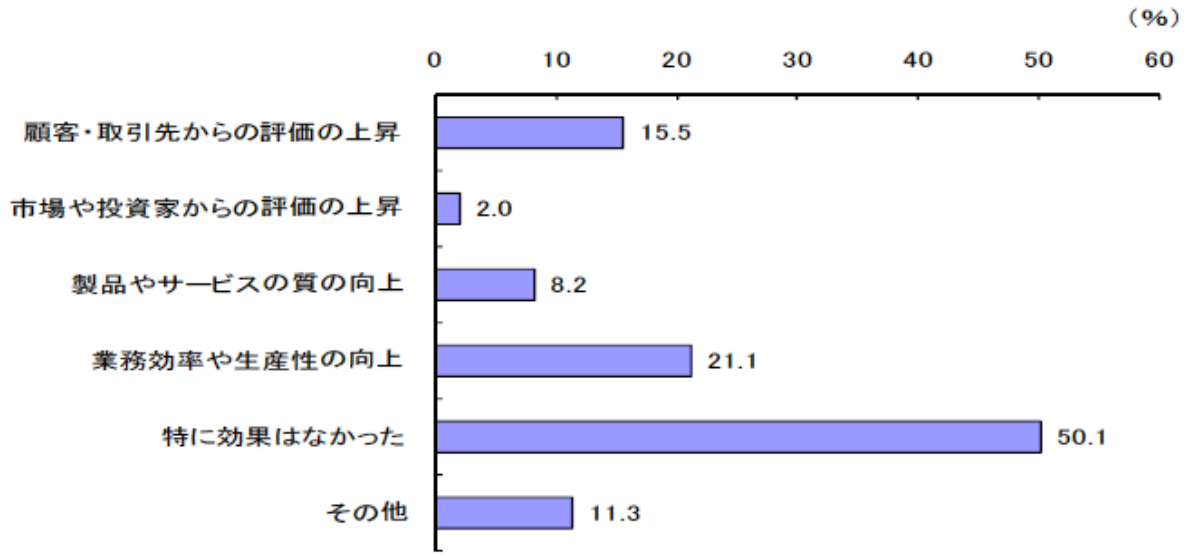


図 5.1-5 情報セキュリティ対策のセキュリティ向上以外の効果の状況（平成17年度）

－経済産業省　平成 18 年情報処理実態調査結果（2007 年 11 月 13 日公表）[5.1-3, 図表 8-7]より－

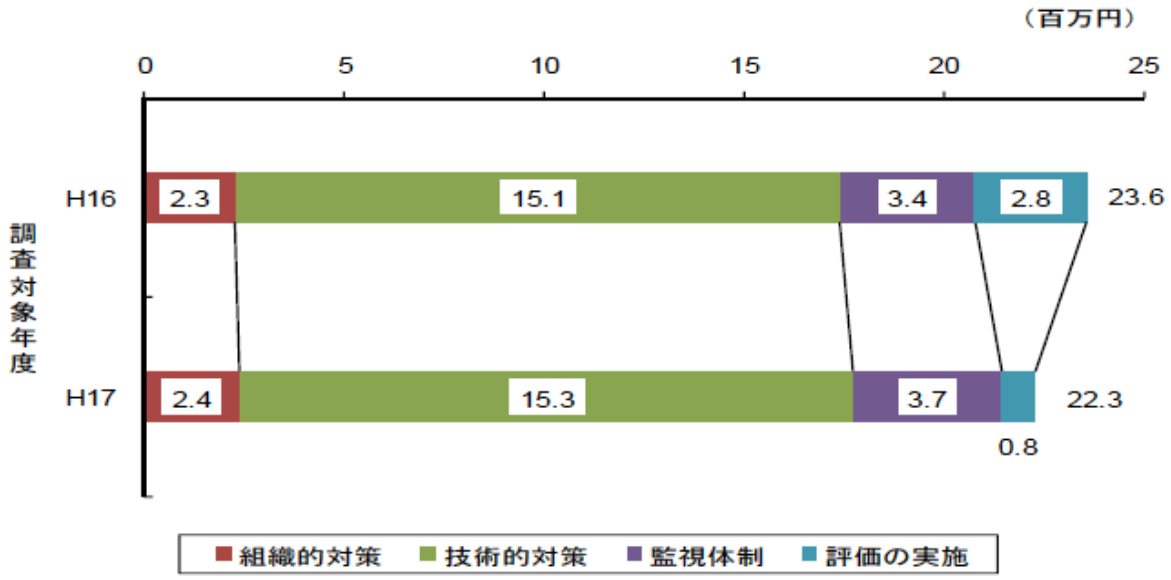


図 5.1-6 情報セキュリティ対策費用の推移

－経済産業省　平成 18 年情報処理実態調査結果（2007 年 11 月 13 日公表）[5.1-3, 図表 8-8]より－

5.2. 瑕疵と脆弱性の共通認識に向けて

瑕疵と脆弱性の共通認識に向けて、組込み機器等もセキュリティの確保（定義と予見性）について、システム環境と時間軸の共通認識として注意すべき事項を以下に示す。

（1）システム環境の共通認識

情報家電等の情報端末を使った電子商取引は，Ⅰ「プロバイダー」と「買主の自宅回線接続器」とを結ぶ接続領域，Ⅱ「買主の自宅接続器」から「情報家電等の情報端末」とを結ぶ接続領域，Ⅲ「情報家電等の情報端末自体」の３段階を経て行われる。そして，各段階をコントロールする企業は，それぞれ異なっている。すなわち，Ⅰはひかり通信等インターネット接続業者，Ⅱは室内回線接続業者，Ⅲはメーカーの作成にかかる情報端末を販売した会社（vendor）である。したがって，各段階におけるトラブルの責任主体はそれぞれ異なることになる。

（2）時間軸の共通認識

組込み機器等のセキュリティの確保にあたっては，特に，Ⅲの段階における「情報家電等の情報端末自体」の責任主体，責任の内容，製品販売会社（vendor）の対応とメンテナンス業者のサービスビジネスについての共通認識を形成させておく必要がある。

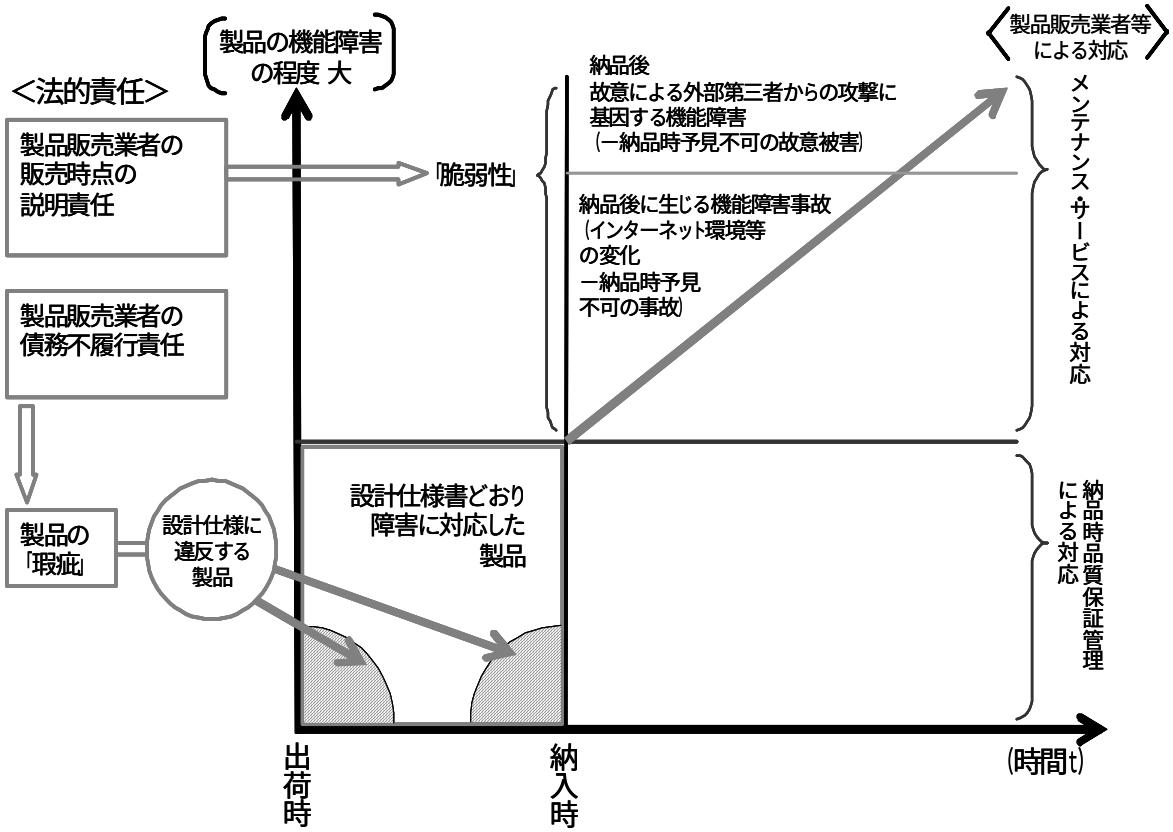


図 5.2-1　瑕疵と脆弱性について

①「瑕疵」の定義と売主の義務

まず，製品販売会社（vendor）の製品につき買主への納品時において不具合がある場合，この製品の不具合は，通常，当該製品の「瑕疵」と呼ばれる（なお，製品の出荷時に売買契約の目的物を特定する合意があれば，納品時ではなく，出荷時が基準となる。民法上は，持参債務なので買主への納品時に不特定物債務の特定が生じる（同法 401 条 2 項）。）。

売主である製品販売会社（vendor）は，買主との売買契約において，完全な製品を買主に納入する義務を負うから，納入した製品が仕様に従っていないなど不具合があれば，売主としての義務を果たしていることにはならず（民法上の債務不履行），製品販売会社は改めて売買契約内容に沿った不具合のない製品を製品市場から入手して納入しなければならない。逆に言えば，買主への納入時に不具合がなければ，売主である製品販売会社は，その納入をもって売主としての義務を免れるはずである。通常の製品の売買であれば，このように言うことができる（この「瑕疵」の問題は，本来，売主の製品の品質管理によって対応できる事柄である。）。

ところが，情報家電等の情報端末には，従来の典型的な売買の目的物とは異なる特殊性があり，そこから次に述べる「脆弱性」の問題が生じる。

②「脆弱性」の定義，売主の義務及び説明の必要

ここで述べる「脆弱性」とは，製品を買主へ納入した後に，インターネット環境等の変化に伴い生じる製品の安全性が欠如している状態をいう。

確かに，従来の典型的な市場に存在する製品の売買の目的物は，納入後に変化することはない。したがって，製品販売会社は，買主に対し，市場に存在する製品の中から，売買契約内容に沿った不具合のない製品を買主に納入すれば，売主の「完全な目的物を納入する義務」は履行したことになる。

しかし，情報家電等の情報端末は，納入時に，その後生ずるすべてのインターネット環境等の変化に対応するようには作られていないし，また，そのように作ることは不可能である。その意味で「納入後に変化が生じない製品」（コップなど）とは異なり，この情報端末は，「納入後に可変的要素を含んだ特殊性ある製品」である。したがって，製品販売会社は，買主に対し，市場に存在する製品の中から，納入時において売買契約内容に沿った不具合のない製品（納入時には完全な目的物）を買主に納入しても，その後，インターネット環境等の変化により，製品の安全性が欠如している状態が生じた場合，売主の「完全な目的物を納入する義務」は履行したことにはならないことになる。

他方，この論理を貫徹すると，納入後に生ずるインターネット環境等の変化は無限大のものであるから，売主の義務も無限大のものとなり，売主に不可能を強いることになる。

そこで，売主の義務は，買主への納入時に売主が予見可能であって，かつ，売主が対応可能なインターネット環境等の変化についてのみ，売主が対応する義務を負うと解すべきことになる（売主の義務の限定。医療過誤事件における医師の注意義務の有無について過誤時点での医療水準が基準となるのと同様である。）。このように解すると，納入時に予見不可能もしくは対応不可能なインターネット環境等の変化については，売主はさらに「完全な目的物を納入する義務」を負わないことになる。

もっとも，製品の買主は一般消費者であってインターネットの専門家ではないから，売主が納入後のインターネット環境等の変化に伴う製品の安全性の欠如状態につき義務を負わないことを十分に認識して製品を購入したとはいえないのが通常である。そのため，売主は自己の義務が限定されていることを買主に説明する必要がある。もしこれを怠ると，買主が納入後の売主のメンテナンス義務を当然の前提として売買の申込をした場合などにおいては，裁判所が売主の説明義務違反を認めて買主の売主に対する損害賠償請求を肯定したり，売主の不利益事実の不告知(消費者契約法 4 条 2 項)として契約の申込または承諾の意思表示の取消を肯定する可能性がある。

そこで，売主である製品販売会社（vendor）は，納入後のインターネット環境等の変化に伴う製品の安全性の欠如状態については買主が責任を負うこと，売主はこれについて責任を負わないことを買主に対して説明する必要がある（売主の説明義務。なお，この説明をした場合であっても，買主から，売主の免責規定は「消費者の利益を一方的に害するもの」（同法 10 条）である，との主張されることはあり得る。しかし，売主が買主に対し，納入時に予見不可能な「脆弱性」が存在する製品であること，そうした製品の性質から売主は納入後のインターネット環境等の変化に伴う製品の安全性の欠如状態について責任を負わないことを十分説明した場合であっても，売主の免責規定が信義則に反して「消費者の利益を一方的に害するもの」ということは通常は考えられないものと思われる）。

③インターネット環境等の変化

納入後のインターネット環境等の変化の原因とメンテナンスサービス納入後のインターネット環境等の変化には，２種類があり，一つは,「インターネット環境等の予期しない変化によってバグが生じたり，ウィルス感染したりするという予見不能の非故意の事態」があり，他の一つは,「ハッカー等による情報家電等の情報端末自体の攻撃を意図した予見不能の故意の事態」がある。前者は，事故の一種と見て発生確率を算定できるならば損害保険による対応が考えられないではないが，後者には保険による対応は困難である。

そこで，こうした納入後のインターネット環境等の変化に対応するためには，買主が製品販売会社（vendor）とは別のメンテナンス業者と，ウィルス対策，ファイアーウォール，バージョンアップ等のメンテナンスサービス契約を締結することによって対応することが重要であると考えられる（もっとも，新種のウィルスが日々量産・散布される今日においては，そのワクチン開発・接種は事後的にならざるを得ない。そのため，ウィルス発生・散布からワクチン開発・接種までのタイムラグが存在することは避けられず，その意味でメンテナンスで保護されない領域が存在する。）。

5.3. 「形式」から「戦略」への転換

悪意ある攻撃者を想定し、ソフトウエアの脆弱性・システムへの攻撃に対する対策という理由から、パッチ適用、ウィルス対策が行われている。実際に脆弱性を見つけ出すコミュニティや、攻撃するツールを提供するサイトが存在しており、パッチ適用、ウィルス対策の図式は成立している。

しかし、PC やインターネットの問題として片付けてはならない。使う道具が変わってはいるが、商取引の基本を忘れてはならない。道具だてが複雑になり、目に見えない電子データを扱うとしても、取引相手を確認する、取引内容を確認する、情報の真偽を判定する、商いを行うにあたり、企業間、対消費者どの取引においても、現実の取引同様しっかりと確認する姿勢が重要である。

取引相手の存在確認、取引情報の秘密を守る、交換した情報、商品の真偽、品質を見極める、EC においてそれぞれがどのように行われているのか、システム任せにするのではなく、納得できる程度のリテラシを身に付ける努力が必要である。

最新パッチを適用する、バージョンアップを行うといった、形式的、一般的なセキュリティ対策により、大部分の心配な出来事から身を守ることはできる。しかし、これだけでは決して安全、安心ではない。漫然とシステムを利用するのではなく、「正しく利用」「異常を無視しない」ということが重要である。

- JPCERT/CC フィッシングに関する FAQ
  （http://www.jpcert.or.jp/ir/faq.html）
- 内閣官房情報セキュリティセンター
  （http://www.nisc.go.jp/index.html）
- 「政府機関の情報セキュリティ対策のための統一基準（第３版）（案）」
  （http://www.nisc.go.jp/conference/seisaku/dai16/pdf/16siryou0102.pdf）

これをすべき、これだけやっていれば大丈夫ということはない。

「手順」や「すべき」ということは、最小限の対策である。攻撃側は情報システムに詳しく、メーリングリスト、コミュニティサイトを通じて日々の研鑽している。現在の対策を無に帰すような脆弱性が発見されるかもしれない、情報システムそのものではなく、人的なミスや勘違いを誘発させるメールが舞い込むかもしれない。

そのとき、単なる形式的な対策は用を成さない。企業、個人、すべての立場で、異常事態を察知、事故を防止する何らかの工夫、戦略が必要である。

5.3.1. 形式は基本

個人の対策以上に複雑で難しいのが、企業の対策である。事業を継続するために、IT 資産を正常に動作させることが重要になってきている企業は多い。机上の PC や業務システムの稼動しているサーバ類、インターネット環境など様々な IT 環境に、事業の業務オペレーションが大き

く依存してきている。これらの業務に使用している IT 資産も毎日のように脆弱性が発見され、その弱点を狙ったウィルスや攻撃が公的機関などに報告されている。業務を継続するためには、IT 資産を正常に保つことは非常に大切な事柄である。

形式的、一般的なセキュリティ対策をとることは、典型的な既知の攻撃から自らを守る際に基本となる。大部分の攻撃は、この基本的な防御によって防ぐことができる。インターネット上のサーバへの外部からの攻撃や、ユーザが利用しているパソコンに感染するウィルスの多くは、既知の典型的な脆弱性を悪用している。つまり、典型的かつ既知のよく知られているセキュリティ上の問題点や脆弱性に対する攻撃が、大部分を占める。このため、典型的な既知の脆弱性をターゲットにした攻撃やウィルスなどに対して対策を講じることは、攻撃やトラブルを避けるために、非常に有効な対策である。

例えば、PC やファイルサーバにウィルス対策ソフトを入れるなどの対策は、インターネット接続や USB メモリ、CD-R など外部メディアなどを媒介としたデータ交換を行う場合には大部分のトラブルや脅威から自らを守る手段として有効である。

公開している Web サーバに関しては、技術者の情報不足や動作テストが不十分であることが原因であることが多い。環境設定の不注意や、プログラム作成上の対処を怠ったケースである。IPA のガイドラインなどや JPCERT/CC などによるインシデント情報を活用し、開発ベンダーとの連携などによって、既知の対策を講じておくことにより大部分の脅威を遠ざけることができる。

5.3.2. 戦略への転換

このような形式的なウィルス対策ソフトや一般的な対策は非常で有効であるが、守りとしての受身の姿勢であることは否定できない。しかし、IT 資源はビジネスのプラットフォームとしてなくてはならないものとなりつつあり、不測の事態に陥り使えなくなった場合どのように事業を継続するのかという考えの下、より積極的な攻めの対策が求められる。

セキュリティリスクに対して積極的に向き合うため、最低限やっておかないといけないセキュリティ対策から、一歩前に出るための積極的なセキュリティ対策について述べる。

基本的、形式的なセキュリティ対策を打った上で、積極的なセキュリティ対策とは何か。
まず、何から何を守るのかを考えると。個人情報の漏洩やサーバで稼動する業務システムやネットワークのトラブルによる混乱などが事業にどのように影響するかを想定し、その影響のインパクトに応じた対策から始めるべきである。事業を行う上で必要なリソースとして捉えて考えるのである。

難しいものや見つけにくいものを対象にするのではなく、事業を行う上でインパクトのあるものから手をつけるという考え方が、組織の判断が利く。目に見えている事業の、一番インパクトの大きなものからはじめることが、積極的な対策の第一歩である。

要求開発アライアンスの萩本理事は、ビジネス価値を高めるためのビジネス戦略トリアージと要求において、ビジネス戦略が生ものであるという意識が重要であると語っている。この考えは、要求開発アライアンスのビジネスモデリング道場[5.3-1]でも掲載されており、経営リソースには優先順位があるが、IT も経営資源であるので優先順位の高いものには厚い対策を講じることになる（図 5.3-1）。さらに、通常の戦略と同様に PDCA によるサイクルで改善し続けることが、施策上重要であることは言うまでもないことである。

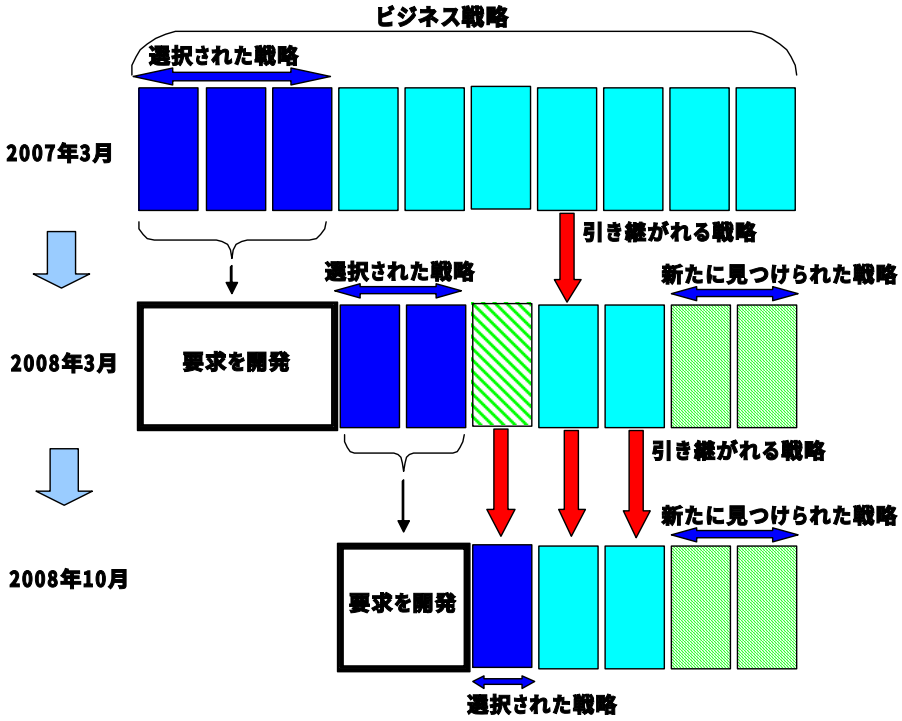


図　5.3-1. 戦略の優先順位

（参照：要求開発アライアンス）

（1）経営者の視点

セキュリティ対策を、事業を継続する目的で、経営資産を守ることとして捉えなおす必要性は述べる。事業の目的から、業務プロセスや製造プロセスが方法として考えられ、実施する上での要件が決まってくる。これらは、事業の目的から繋がっており、セキュリティ対策だけが単独で存在するわけではない。それを図示したのが図 5.3-2 である。

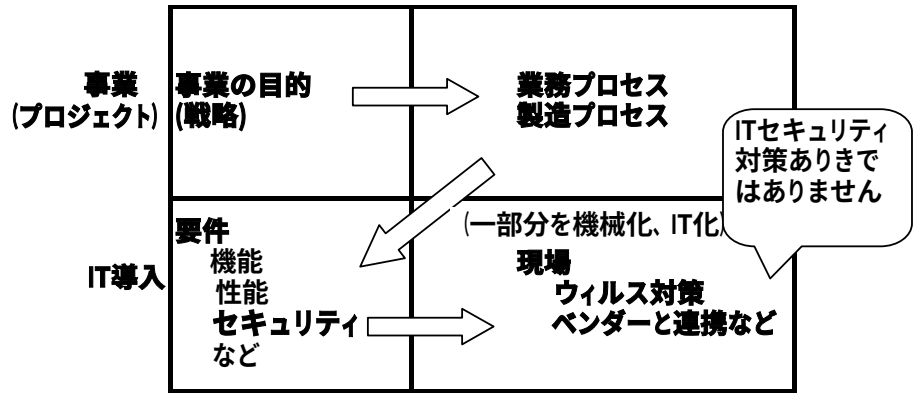


図 5.3-2 事業目的とセキュリティ対策のつながり

前出の図 5.3-2 で、注意したいのは事業に結びついていない IT 資産がセキュリティ対策から漏れやすいことである。戦略性のあるセキュリティ対策を行うためには、事業から見えていない IT 資産や撤退した事業で使用していたサーバなどが管理されずに稼動しているかを継続的にチェックすることも大切である。

具体的には、本来の目的とは異なる利用方法であるが、業務フローに組み込まれてしまっているシステムや PC の存在があげられる。事業の本来の目的とは異なる利用をされている PC やサーバ、各種システムは、管理者が不在であったり責任者が曖昧であったりすることが多いと考えられる。事業の予算と紐づかない隠れた資産であるため、事業活動からは見えにくい潜在的なリスクとなる。そのため、セキュリティ対策が漏れやすくボトムアップでしか情報が上がってこないが、責任者は予算を付けることが困難である。

このような潜在的リスクの洗い出しは、積極的なセキュリティ対策としては重要である。しかし、過度の管理はセキュリティの低下を招くことを忘れてはならない。管理のための管理になってしまえば、事業に対するモチベーションを低下させることになる。煩雑なセキュリティ運用規則は､本来の業務をとめてしまいかねない｡どこまで何を実施するか？出来ることを出来るだけ、効果のあることに集中し積極的に運用するのである。

（2）技術者の視点

JPCERT/CC や IPA のセキュリティインシデントなどの情報から､脆弱性に対する対策を適用することは、基本として施行すべきである。特に製品開発者においては、過去の事例を参考にして、よりセキュアな製品を作り出していくためにも、重要な行動、対策である。

しかし、どれもが技術的な内容であり、技術的な内容を鵜呑みにするだけでは、積極的な対策へとはつながらない。情報システムがどのように使われるのかという利用者視点での影響度合いを考慮の上、次の設計、構築、設定へと、活かす事ができて初めて積極的な対策になっていく。

技術的な観点からは、おなじ暗号化であっても、利用者が理解して暗号化された情報を取り扱っているかどうかによって、もたらす効果は大きく違ってくる。利用者を硬直させない、直感的な操作性と、常に正しいことを確認でき、やり直しの可能なやさしさを持った情報システムになれば、利用者自らの行動から、より強固なセキュリティの確保が望める。

例えば、PKI の技術を使った SSL による暗号化通信を、利用者に対して暗号化のみを意識させるシステムとしてしまうと、PKI の持つ本人確認の意味が利用場面で失われ、証明書の不備やフィッシングサイトでのサイト確認が見逃されることにつながりかねない。また、辞書攻撃や総当り攻撃に対する対策として、利用者に対して複雑かつ長いパスワードの設定を強制するシステムとすると、利用者離れが起きたり、パスワードをメモして張り出すなど、結果的にセキュリティ低下を招くことがある。

技術的な側面ばかりではなく、利用者を含めた運用場面での、総合的なセキュリティ対策を戦略的に考えていただきたい。

5.4 情報セキュリティの可視化と最低限の対策と対応

5.4.1. 情報セキュリティの可視化

高度にネットワーク化されたＩＴ社会における電子商取引は、電子商取引が情報システムの一応用形態であることから、電子商取引に使われる情報システムの情報セキュリティ対策と対応が重要となる。

情報セキュリティへの対策と対応を行うには、目に見えない漠然とした情報セキュリティを、「可視化」して、具体的に把握してから取り組むことが大切である。可視化しないで、闇雲に対策や対応を行うと、結果として無駄な投資に繋がったり、効果のない対策や対応を行ってしまうことになる。

電子商取引が企業間および企業消費間で行われることから、企業側における情報セキュリティの可視化は、次の３つの方法で行うことが考えられる。

（１）情報セキュリティの対応状況の「可視化」

企業は、自社の情報セキュリティ対策や対応の現状を把握し、具体的改善策を実施しながら、企業が社会から望まれる水準（企業が社会から望まれる水準であり、一様ではなく、企業の業態や保有する情報資産等の属性によって異なる）を維持・向上していくことが重要となる。
そのためには、まず初めに自社の現状の情報セキュリティ対応状況を把握するため、「情報セキュリティの対応状況の可視化」を行うことが必要である。

この可視化によって、自社の情報セキュリティ対策状況が、業界においてどの程度のレベルにあり、どこに弱点があり、どのように改善して行けばよいかが見えてくる。
この可視化の施策ツールの１つとして、ＩＰＡ（独立行政法人情報処理推進機構）が、Ｗｅｂサイトで公開している情報セキュリティ対策ベンチマークシステム[5.4-1]を利用して、自社の「可視化」を行ってみるのも１つの方法である。

（２）情報セキュリティリスクの「可視化」

企業において、情報セキュリティの対策や対応を行う場合には、（１）の『情報セキュリティの対応状況の「可視化」』によって、自らの弱点や改善点は見えてくるが、実際の対策を行う場合には、情報セキュリティのリスクを「可視化」し、企業の情報セキュリティへの投資とのバランスを考慮しながら、対策に優先順位を付けて、実施していくことが大切である。
情報セキュリティのリスクを「可視化」する手順は、概ね次の通りとなる。

（ａ）「可視化」方針の明確化
（ｂ）情報セキュリティを適用する範囲の明確化
　事業区分、物理的区分（拠点、事務所など）、ネットワーク接続などを考慮
（ｃ）適用範囲内の情報資産の洗い出し
（ｄ）情報資産価値、情報資産に対する脅威、各々の脅威に対する脆弱性の明確化
　効率化のため、情報資産をグルーピングして行うことを考慮

（ｅ）リスク分析を行いリスクの「可視化」を実施
　　リスクを定量的に扱うため、リスク値で表現

これらの手順で、「可視化」されたリスクに対して、対策を実施していくことになる。
また、上記の基本的な手順を実現するための枠組として、ＪＩＳ Ｑ 27001：「情報セキュリティマネジメントシステム－要求事項」（ＩＳＭＳ認証）に準拠した情報セキュリティマネジメントシステムの構築が考えられる。

（３）情報セキュリティ対策および対応の「可視化」
企業は、『（２）情報セキュリテイの「可視化」』によって、「可視化」されたリスクに対し、情報セキュリテイへの投資のバランスを考慮しつつ、有効な対策や対応の優先順位を付けて実施していくことになる。
この場合、情報セキュリティの対策と対応を有効性の確認などのため定期的に見直すことが必要であり、そのためには、どの対策や対応が実施されているのか、効果は出ているのか、などを一覧表によって対策および対応の「可視化」を行うことが大切である。
このことは、情報セキュリティのマネジメントを PDCA を回しながら、維持向上していく上で重要なことである。
以上のような、情報セキュリティの「可視化」は、電子商取引を実施する企業の情報セキュリティに対する投資の適性化を実現する上で、大きなメリットになる。

5.4.2 安全･安心な電子商取引を行う最低限の対策と対応

電子商取引は、情報システムの一応用形態であるが、その特性上から要求される最低限の対策と対応が必要である。この場合でも、前項の「可視化」を行った後に、最適な対策や対応を行うことは言うまでもない。
（１）インターネットの利用
　ネットワーク上での、盗聴･改ざん、不正侵入によるＷｅｂサーバの改ざんや DoＳ(Denial of Service)、XSS（Ｃross Site Scripting）などの各種の攻撃などの脅威

（２）情報の真正性の保証
　商取引の申込み、発注/受注確認、決済などの情報のコピーや改ざんなどの脅威

（３）相手確認（本人認証やユーザ認証）
　ユーザ ID やパスワードを盗んで、EC（Electric Commerce）サイトでショッピングをし、他人にその支払いを行わせる行為などの「なりすまし」脅威に対し、相手が正当な取引相手かどうかの確認

5.4.2.1. 企業側の対策と対応

そのため、企業は次のように、技術的、人的、物理的、自然災害に対する最低限の対策と対応を考慮しておくことが大切である。

（1）技術的セキュリテイ対策と対応

・暗号化（Web サイトの SSL-VPN でのアクセス化など）

・ファイヤウォール　・ウィルス対策　・SSL プロトコル

・デジタル署名（真正性）　・認証技術　・本人認証

など

（2）人的セキュリテイ対策と対応

・社員・派遣者などの採用時の情報セキュリティポリシー厳守の誓約書取得

・退職時のアクセス権の削除

・委託先企業との情報セキュリティに関する機密保持契約締結

（3）物理的セキュリティの対策と対応

・事務所や作業場所への入退室制御

（指紋認証，テンキーによるロック，施錠など）

・情報媒体（書類，ＣD/ＤＶＤなど）の保管キャビネットの施錠管理

（4）自然災害への対策と対応

・地震

・火災

尚、ＪＩＳ Ｑ 27001：「情報セキュリティマネジメントシステム－要求事項」（ＩＳＭＳ認証）の管理策を参考に自社に対する対策をすることも良い。

5.4.2.2 消費者側の対策と対応

消費者側の対策と対応としては、次を考慮しておくことが必要である。

（1）ＳＳＬ対応済などの安全なＷｅｂサイトへのアクセス

（2）他人に知られにくいＩＤ，パスワードの採用や定期的な変更

（3）ファイヤウォールやウィルス対策を行ったＰＣでのＷｅｂサイトへのアクセス

（4）ＯＳや関連Ｓ／Ｗの最新パッチの適用

5.5. 安全･安心な情報端末とサービスネットワーク環境の実現に向けて

電子商取引の将来のあるべき姿については、3.5.報告事項の節で示したとおりである。すなわち、安全・安心な電子商取引を行なう為のシステムとしては、サービス事業者もユーザも、共に安心して安全で確実な電子商取引を行える環境の構築が必要と考える。しかし、環境の構築には時間がかかるものであり、環境を待っていては、先に進めなくなるのも事実である。現在使われている、便利で利用価値のある仕組みとしての電子商取引を、サービス事業者とユーザ双方がうまく活用しながら安全・安心な仕組みに変えていく努力が重要と考える。

この観点から、本節では、現状のシステムを前提に、安全・安心な電子商取引を行なうために必要な機器やサービスネットワーク環境について考察する。

5.5.1.電子商取引システムの構成

利用者(ユーザ)が離れた場所から、物を注文したり、決済したりするためには、離れた２地点間で何らかの手段で情報のやり取りを行う必要がある。古くから、手紙を使ったメールオーダーや電話を使った注文をお店が受け、物を送付し、決済するといった仕組みの、いわゆる通信販売による取引が行なわれてきた。しかし、昨今は、各所へのインターネットの普及が進み、手紙や電話といった手段に変わって、この２地点間での情報やり取りをインターネットを使って行う事が一般的となってきている。

インターネットを使った電子商取引を行なうシステムといっても、対象となる商品・顧客・地域・環境・事業主などにより実にさまざまな様態を取っている。ここでは、この総てについて記すことは困難であるため、一般的な構成をモデルとして定義し、このモデルに立ち戻って記すこととする。接続して利用する。

図 5.3-1 に、前出の一般的なインターネットを使った電子商取引を行なうシステムのモデルを示す。利用者は、インターネットを利用するために、自宅でパーソナルコンピュータをルータに接続して利用する。

ルータはＩＳＰ事業者と閉域網であるアクセスネットワークを介して接続されている。アクセスネットワークは、ＩＳＰ事業者を介してオープンネットワークであるインターネットに接続されており、利用者とインターネットとの間の情報の橋渡しを行なう。利用者がインターネットを使った電子商取引を行なう相手として、インターネットの先には、電子商取引サービスを提供するサービス事業者が接続されている。

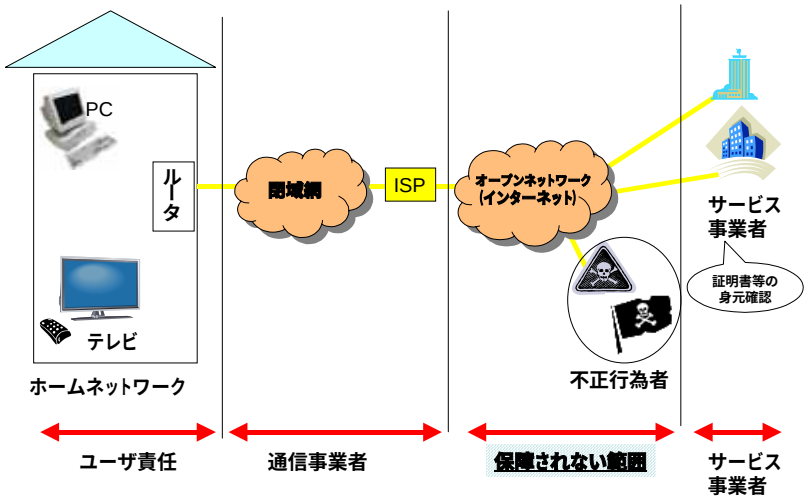


図 5.3-1　現状のネットワークの概念図

5.5.2.電子商取引システムに潜む脅威

利用者(ユーザ)がインターネットを使った電子商取引を実施する場合、どのような脅威があるかを整理した結果を図 5.5-2 に示す。

（1）電子商取引環境での責任分解点

インターネットを使った電子商取引の前提となるインターネット環境そのものに利用者は費用を支払っている為、その環境は安全なのではないかと思うかもししれない。しかし、実際に利用者が費用を支払っているのは、あくまでもＩＳＰ事業者に対してであり、ＩＳＰ事業者は、利用者とインターネット間のデータのやり取りを保証するに過ぎない。言い換えると、オープンな環境であるインターネットの先は、ＩＳＰ事業者は何も保証してくれないのである。

一方、電子商取引サービスを提供するサービス事業者は、商行為の延長として保証できる範囲は、あくまで自社のシステム、言い換えると自社のルーターから自社のサーバまでを保証できるに過ぎない。すなわち、自社の商取引のための収集した注文の情報と、これに付随する顧客情報等の関連情報を安全に守ることまでが電子商取引サービス事業者が責任を持って管理することが、最低限度、必要とされる範囲である。オープンで誰も保証しないインターネットでの作為は、誰も管理することが出来無い為、結果的に総て電子商取引に対する脅威となる。

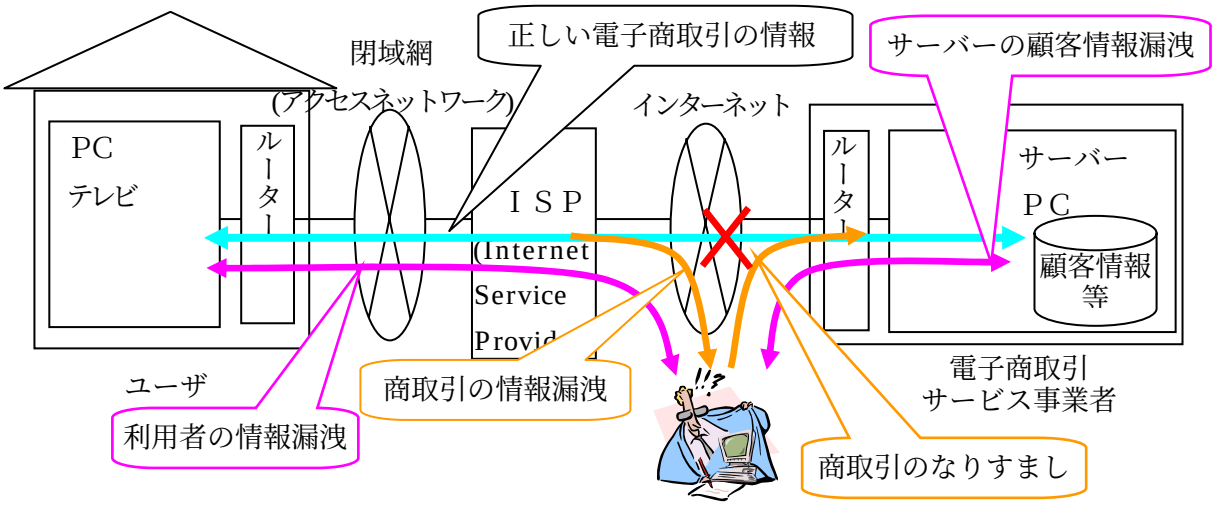


図 5.5-2　電子商取引システムの脅威

（２）電子商取引に潜む脅威

誰も管理しないインターネットからの電子商取引に対する脅威は、インターネットに存在する悪意の第三者から、利用者に対する詐欺等の不正行為か、電子商取引サービス事業者に対する詐欺等の不正行為の２つに大別される。

電子商取引で発生する不正行為としては、まず直接的不正として、商品/サービスに対する詐欺行為があげられる。例えば、他の人物に成りすましての商取引により、実際の支払い者では無い者に商品/サービスを提供したり、過多/過少請求や決済による不正な金額の徴収などが考えられる。付随するものとして、顧客情報や電子商取引自体の情報が漏洩することで、高度なプライバシー情報が悪意の第三者に渡り、電子商取引とは別の場所で不正に詐欺行為などで利用されることも考えられる。図 5.3.2 に現状のシステムで考えられる電子商取引システムの脅威を示す。

いずれも、利用者と電子商取引サービス事業者の間でやり取りされる電子商取引の情報や、利用者・電子商取引サービス事業者双方のパーソナルコンピュータの中の情報を悪意の第三者に伝えられることで生じる。

これらの脅威を排除できる情報端末やサービスネットワークがあれば、利用者も電子商取引サービス事業者も安心して電子商取引を行なうことが出来る事となる。

5.5.4. 安全･安心な情報端末

インターネットの脅威を排除し、安全･安心な電子商取引を行なうために、必要な情報端末は、以下となる。

・ 利用者(ユーザ)の情報を漏洩しない。
・ 正しい電子商取引サービス事業者のみとの間で情報をやり取りする。
・ 電子商取引の情報を漏洩しない。

これらが保証される端末であれば、利用者は安心して電子商取引を行なえる。端末の用途を電子商取引のみに限定すると、これらの解決手段は比較的容易である。利用者の端末が、正しい電子商取引サービス事業者との間の電子商取引のための情報やり取り機能を持ち、一切の個人情報を保存しない端末とすることで利用者の情報漏洩は強固に防ぐことが可能である。このとき、例えば、暗号技術を用いた認証を利用し、正しい電子商取引サービス事業者以外とは接続できないこととすれば、第三者との情報のやり取りも強固に排除可能である。又、利用者の端末で扱う情報は、総て正しい電子商取引サービス事業者のみが解読可能な暗号で暗号化することで、途中の経路上での情報漏洩は強固に防ぐことが可能である。商取引の情報等を利用者が入力する機構も、外部から読み取りが出来ない機構とすることで、商取引の情報を端末から読み取られる脅威を防ぐことが可能となる。しかし、電子商取引のみに限定することは、テレビのような用途を限定した端末であれば、比較的可能性は高いが、汎用のパーソナルコンピュータ(ＰＣ)を利用する場合は、容易なことではない。そこで、電子商取引のみに限定した機能を持ったアプリケーションソフトウエアをパーソナルコンピュータにインストールして利用することで、汎用のアプリケーションプログラム環境を利用する構成に比べ、強固な端末とすることが考えられる。当然、アプリケーションプログラムで考慮すべき事項は、電子商取引を安全に行なうことに十分考慮されたものである事が重要である。

5.5.5.安全･安心なサービスネットワーク

安全・安心な電子商取引を行なうために電子商取引サービス事業者が考慮すべき事項も以下となる。

・ 顧客情報等を漏洩しない。
・ 正当な利用者のみとの間で情報をやり取りする。
・ 電子商取引の情報を漏洩しない。

これらのうち、電子商取引サービス事業者側のサーバからの顧客情報等や電子商取引の情報を漏洩しないことは、電子商取引サービス事業者側の努力により可能と考える。確実に正当な利用者のみとの間で情報をやり取りすることの保証と、利用者側の端末側からの情報漏洩に関しては、完全にクローズドな回線ネットワークであれば、比較的容易に対策可能であるが、オープンなインターネットを介したシステムの上では、非常に難しい課題がある。

現在、一般的に利用者側で用いられている端末は、いわゆる市販のパーソナルコンピュータと汎用プログラムの構成であることが多い。この一般的な端末構成では、悪意の第三者による研究

も進んでおり、例えばパーソナルコンピュータに記録された認証用の鍵や暗号化の鍵を、何らかの手段を講じて入手することも技術的には可能である。このため、現実的には、パーソナルコンピュータの内部に悪意の第三者による悪意のソフトウエアが入り込まないようにする防御手段を講じたり、正しい電子商取引サービス事業者であることを確認するといった、利用者が個々に注意し必要な手段を講じているのが現状と思われる。しかし、利用者の意識は個人毎にまちまちであり、電子商取引サービス事業者の側が一元的に利用者側を扱うことは、難しいものがあると考える。この前提に立つと、サービス事業者がシステムとして安全・安心を守るといった考え方が望ましい。

ひとつの解決策として、利用者が電子商取引のシステムにログインする際に、正当な利用者であることを厳密に確認することで、不正なログインを排除するものがある。利用者がログイン時に利用するパスワードを IC カードや携帯型の端末で常に変化させて生成し、このパスワードをサービス事業者側のサーバーで認証を行ない、正当な利用者であることの確証を得るシステムである。正当な利用者以外は、毎回変化するパスワードを容易には類推不可能なので、成りすましの排除には高い効果があると考えられる。不正な利用者による電子商取引の利用を排除することが出来る為、情報の漏洩等があっても不正な電子商取引を排除することが出来る。しかし、電子商取引の情報の暗号化は既存のパーソナルコンピュータの機能を利用するといった考え方のシステムであるため、パーソナルコンピュータに悪意のソフトウエアが置かれた場合は、既存の電子商取引システムと同じとなる。

そこで、更に一歩踏み込んで、たとえばＩＣカードのように、悪意のソフトウエアを排除可能であり、内部に記録された暗号の鍵を読み出すことも出来ず、一切の個人情報を出力することが無い装置を、より積極的に利用することが考えられる。IC カードをパーソナルコンピュータと組み合わせ、パーソナルコンピュータを単なる通信路として利用することで、利用者のパーソナルコンピュータに悪意のソフトウエアが搭載されていた場合でも、正当な利用者の認証と重要な情報の暗号化をより確実に行なえるシステムが構築可能である。このようなシステム上で電子商取引を行ない、利用者の認証と暗号化に利用することで、より安全･安心な電子商取引が可能となると考えられる。

海外でも、既に IC カードそのものをパーソナルコンピュータとリーダライタで接続し、サービス事業者が、直接 IC カードを認証し、暗号化機能を利用することで、現在の実際の店舗で実施されているクレジット決済システムに匹敵する安全度を確保可能とするインターネット決済システムを提供している例もある。このようなシステムは、現在考えられる中では、安全・安心なシステムと呼べるひとつの例と考える。今後、電子商取引の更なる発展のために、これらのより安全なシステムが広く普及することが肝要である。

5.6. SOHO や中小企業でもできるセキュリティ向上対策について

セキュリティ対策に十分な予算確保や経費を捻出出来ないが故に、形式から戦略への転換で、自分達で自分の情報資産を守ることと法令遵守が求められる。

ISMS やプライバシーマークなどの第三者認証を取得することで、事業所内におけるセキュリティレベルを高めることができ、情報セキュリティに関する事件・事故が起こる確率が低いと解釈される。しかし、中小企業等で認証を得るための予算が確保できない場合が多い。また逆に、実際に、第三者認証が取得できても、事件や事故が起きないということは、絶対にありえない。一方で、第三者認証を取得していることを監査基準に含めている企業もあり、認証取得という形式的な対策だけに専念するとフォローが出来なくなる懸念が生じる。

対策として重要なことは、自分達の企業やオフィスにおいて情報セキュリティに対する認識ができており、且つセキュリティレベルを把握していることである。第三者認証を取得し、維持することは、自己評価及び客観的評価要素にはなるが、情報セキュリティを維持できていることの絶対条件ではないと考えられる。

セキュリティ向上対策として、情報の管理の仕方で戦略的な対策をとることが重要である。また、安全管理措置において実際に事故や違反が起きてしまった場合、事故後の早急な処理と早期の処置（報告、原因究明、再発防止、リカバリなど）で対応をすることである。事後処理の場合も、情報の管理の仕方で戦略的な対策が出来ていると容易となる。

情報の管理の形態（レベル）として、

	情報の保存形態	特徴
1	個人情報を保存しない	情報を出来るだけ必要最小限に限定し、業務の終えた情報は廃却（消去）する。保存する情報が少ないほど、情報管理が容易であり、漏洩等による被害も少ない。 情報を保持ならびに消去する管理ルールを明確にする。
2	情報価値を無くした形で保存する	盗難・紛失等でたとえ漏洩しても、例えば電子割符のような秘密分散のファイルで保存しておいて、漏洩したファイルが情報価値を持たないようにする。
3	情報を秘匿する	暗号化等で情報に鍵をかけて保存する。暗号化の鍵管理が十分でないと効果がない。また暗号が解読されると、情報は秘匿できない。

上記１～３は、適宜組み合わせることで、情報の秘匿効果は更に向上する。

情報の管理形態について、

1．個人情報を可能な限り必要最小量に限定し、業務の終えた個人情報は廃却（消去）又は返却する。保存する情報が少ないほど情報管理が容易である。さらに、経済産業省のガイドラインでは、個人情報の保有数が過去 6 ヶ月で 1 日も 5,000 人を超えていなければ個人情報取扱事業者の対象から除かれる。この場合、個人情報を保持する基準ならびに消去する管理ルールを明確にしておくことが重要である。さらに、毎日の業務で、この管理ルールに基づいて行われているかのチェックを行うことが必要である。

2．保存データの情報価値を無くした形で保存する。個人情報を保存するときに、例えば電子割符のような秘密分散ファイルで保存しておいて、保存データが、盗難・紛失等でたとえ漏洩しても、漏洩したファイル自体は情報価値を持たないようにする。この方法は、管理の負担とリスクの少ない対策であると言える。

3．暗号化で情報を秘匿する。暗号化でデータに鍵をかけて保存する場合、暗号の鍵管理が十分でないと効果がない。また暗号が解読されると、情報は秘匿できない。

事故後の処理については、

経済産業省のガイドライン 2-2-3-2 項⑤において、「組織的安全管理措置」で、「事故又は違反への対処」として、必要事項が示されている。これに従って対処する。主務大臣への報告が必要な場合もあり、不明な点は、所轄省庁に報告して、相談をする。

することが必要であると考える。

（1）情報セキュリティについての戦略的な考え方

ISMS やプライバシーマークなどのセキュリティに関する第三者認証の取得は、客観的な評価の手段として有効ではあるが、第三者認証の形式的な取得で情報セキュリティが確実に確保されるものではない。情報を管理・運用する者が、どのように情報セキュリティを確保するかの対策を戦略的に、またより効果的にするかにかかっている。

平成 20 年のガイドラインの改訂（案）では、委託先の事業者から個人情報やクレジットカード情報の漏洩事案が発生していることを踏まえて、ガイドラインの見直しを行った。
この中で、委託先の選定の水準として、保護法第 20 条で定める個人情報保護水準と同等の水準であることを推奨している。

この選定の水準は具体的に示されていないため、すでに ISMS やプライバシーマークなどのセキュリティに関する第三者認証の取得を客観的な水準評価手段としているケースも見受けられるが、認証を取得するため形式的に経営資源を投資してもセキュリティ意識が伴わないと十分な効果を発揮できない恐れがある。逆に、金銭的に余裕のない中小企業では、形式的な評価で水準が無いと判断されないとも限らない。しかし、ここは戦略的な対策でチャンスをつかめる可能性がある。形式的な投資を戦略的な投資に切り替えるチャンスでもある。

（2）情報セキュリティの PDCA サイクル

情報セキュリティ対策は、たとえある時点で最適な対策を講じても、攻撃手法の進化や新しい

脆弱性の発見といった要因により、時間とともにセキュリティレベルの低下は避けられない。強固なセキュリティの維持には、セキュリティの状態を常に把握し、問題点を改善し続ける必要がある。そのためには、セキュリティ PDCA サイクルを向上させることが重要である。この PDCA を上手く回すことが戦略的な対策と言える。

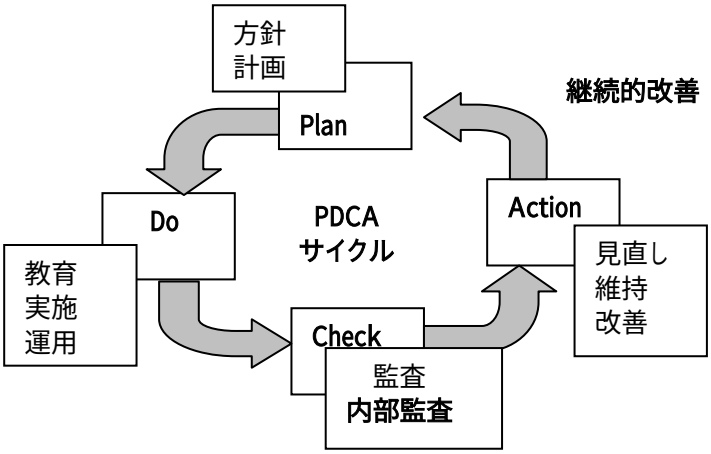


図 5.6-1 情報セキュリティの PDCA サイクル

このためには、組織的・人的・技術的・物理的な対策が不可欠とされている。しかし、中小企業の事業者には、「個人情報保護体制を作ろうにも社員数が少なく、専任者を置けない」、「プライバシーマークのコンサルティングを頼む経済的余裕がない」などの事情があるが、基本的には、情報セキュリティは自社の戦略で自分達が守ることを前提に、

① 中小企業に対して、経済産業省ならびに関連団体に、第 3 者機関認証を取得するための補助金支援を働きかける。

② 安価で便利なコンサルタント・パッケージを利用する。

③ 新たなセキュリティマーク（取得が経済的な）でセキュリティの底上げをする。

などが、考えられる。

①については、ECOM を含めた活動で行う。また、内閣官房情報セキュリティセンターは、ホームページで、2008 年 1 月に「第２次情報セキュリティ基本計画」（仮称）を発表し、その中で、「中小企業における情報セキュリティ対策について」の項目と挙げている[5.6-1]。課題として、初期投資の対策としてのベンチャー支援、大企業の過剰な対応なども挙げられている。なお、中小企業がアクションを起こす必要もある。

②については、最近手ごろな価格でのパッケージも出始めた。例として、安価に効率よくプライバシーマーク取得体制が整えられるように、通常のコンサルティング内容をコンパクトにしてまとめパッケージ化したものがある。 付属の DVD には、JIS Q 15001 要求事項 38 項目のコンサルタントによる解説を撮り下ろして収録し、CD には記入例付きで上書き可能なサンプル規程、様式集を収録。構築マニュアルは、規格概要から規程、様式集の説明、運用方法や審査対策などを詳しく掲載しており、要求事項で求められている、個人情報に関する従業員教育のための 教育

用テキストも付属している。必要な解説・ノウハウだけをまとめた内容なため、中小規模の事業者でも、効率よく自力で個人情報を保護するための体制整備と文書の作成が可能で、価格は 10 万円程度である。

また、PDCA サイクル（Plan-Do-Check-Action）の「Check」に効果を発揮する脆弱性診断サービスなども市場に提供されている。

③については、経済産業省所管の社団法人「ニューオフィス推進協議会」が、オフィスセキュリティマーク認証制度を、2006 年 4 月に発足させている。この認証制度は、情報（データ）よりも物（ハードウェア）に重点を置いたセキュリティである。取得までの費用と期間が少なく、情報を管理する PDCA をマスターするのに便利な手段と言える。

参考文献･資料

[5.1-1] IPA：2006 年度 第 2 回 情報セキュリティに関する新たな脅威に対する意識調査報告書(2007 年 7 月)
http://www.ipa.go.jp/security/fy18/reports/ishiki02/documents/200602_ishiki.pdf

[5.1-2] IPA：2007 年度 第 1 回 情報セキュリティに関する新たな脅威に対する意識調査報告書(2007 年 12 月)
http://www.ipa.go.jp/security/fy19/reports/ishiki01/documents/200701_ishiki.pdf

[5.1-3]経済産業省：平成１８年情報処理実態調査結果報告書（2007 年 11 月 13 日公表）
http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/pdf/3_H18report_rev071204.pdf

[5.3-1] IT Pro Watcher：ビジネス価値を高めるためのビジネス戦略トリアージと要求(1)（2007 年 02 月 15 日） http://itpro.nikkeibp.co.jp/article/Watcher/20070214/261949/

[5.4-1] IPA：情報セキュリティ対策ベンチマークシステム
http://www.ipa.go.jp/security/benchmark/index.html

[5.6-1] NISC：「第２次情報セキュリティ基本計画」（仮称）に係わる検討の視点（例）,情報セキュリティ政策会議、基本計画検討委員会、第１回会合、資料５（平成 20 年 1 月 16 日）
http://www.nisc.go.jp/conference/seisaku/kihon/dai1/pdf/1siryou05.pdf

[5.6-2] NOPA：オフィスセキュリティマーク認証制度、他 http://www.nopa.or.jp

6. おわりに

セキュリティへの取り組みレベルがどの程度なのかといったことの指標があれば、企業の地道で継続的な活動に加え、自社のセキュリティ対策のレベルが客観視でき便利であるが、そのような指標等明確に示したものは無い。あるのは、前述の組織の情報セキュリティ活動を評価するISO27001(ISMS）や P マークと、ソフトウエアやハードウエアの「でき」や「品質」を評価する ISO15408（CC）等である。今後、情報セキュリティに対する企業活動の評価と、導入しているセキュリティのハードソフトの品質等といった部分の双方を一体として評価する仕組み、指標が必要になってくるのかもしれない。

つまり、もっと機械やコンピュータソフトウエアに頼るのではない、本来の企業の実力を付ける必要があると感じるのです。

しかしながら「それ」を評価する仕組みや指標は、容易には作れないと考えています。なぜならば、企業情報セキュリティとは企業コンプライアンスを満たし、自主的な活動を阻害しない範囲で企業としての生産性や商品・サービスの品質をも向上させる企業ガバナンスを実現していく過程に存在する要素であり、決して機械的な話ではなく、極めて人間的な調和を、企業活動全体に及ぼすことが要求される事項だからです。

我々が対象とする「企業情報セキュリティ」に関しては、今後以下の事柄が更に明確に、多くの方々に受け入れられていくことになると思います。

1、冒頭で申し上げた、企業情報セキュリティは、企業活動が存続する限り維持される「安全衛生活動」や「品質改善活動」と同じく「企業情報セキュリティ活動」として継続、向上させていく性質の取り組みであり、完全は無い。
2、企業情報セキュリティは、フェールセーフから、一歩進んだフェールプルーフへとシフトしており、そもそも事故の発生しないような「積極的な工夫・努力」が必要となってきている。企業情報セキュリティ活動は、根底にコンプライアンスやガバナンスが存在するが、情報化社会における企業情報セキュリティの向上は、「企業価値向上の為の大事な取り組み」の一つである。
3、企業情報セキュリティも含めて、企業全体を付加価値の高い組織・存在へと導いていく企業全体の意識の醸成が必要。

当然ながら、社会的存在である企業・法人の経営を軽んじているような経営陣には、この報告書は無意味であり､そのような組織の経営陣の意識改革が何らかの形で促進されることを望みます。参考ながら、地道な企業組織の情報セキュリティ意識向上の活動と、投資したセキュリティハード・ソフトの相関関係を図示し、これに企業価値を適切に表現できる指数を掛け合わせて、新たな企業評価の手法ができると、面白いのではないかと感じております。これは、日常的な企業活動のレベルと、セキュリティ意識レベルが、その企業の経済的指数とどのように関係するかを見ることができるものになるのではないかと感じております。

以上

7. 平成 19 年度情報セキュリティWGメンバーリスト

メンバー名		団体名	（敬称略）
(ＥＣＯＭ会員)			
保倉　　豊	(主査）	グローバルフレンドシップ株式会社	
合原　英次郎	(主査)	松下電器産業株式会社	
山川　智彦		株式会社 NTT データ	
青山　　彰		花王株式会社	
川城　三治		グローバルフレンドシップ株式会社	
足立　和朗		電気事業連合会	
高橋　和博		株式会社テプコシステムズ	
小早川　直樹		日本アイ・ビー・エム株式会社	
垣内 伯之		財団法人日本情報処理開発協会	
平野　芳行		日本電気株式会社	
西岡　信佳		株式会社日立情報システムズ	
高見　　穣		株式会社日立製作所	
玉田　竜一		富士電機ホールディングス株式会社	
再起　和夫		松下電器産業株式会社	
吉田　久志		三菱電機インフォメーションテクノロジ株式会社	
井上　雄二		株式会社リコー	
(有識者)			
安田　　直		NPO 日本ネットワークセキュリティ協会	
大谷 尚通		NPO 日本ネットワークセキュリティ協会(ｾｷｭﾘﾃｨ被害調査 WG)	
原田 由里		有限責任中間法人　EC ネットワーク	
古田 洋久		有限責任中間法人　ＪＰＣＥＲＴ/ＣＣ	
山田 良史		フィッシング対策協議会	
服部 成太		弁護士	
稲益 みつこ		弁護士	
常盤 政幸		弁護士	
村瀬 一郎		株式会社 三菱総合研究所	
手塚 悟		株式会社 日立製作所	
(オブザーバー)			
金井 秀紀		経済産業省	
(事務局)			
川嶋 一宏		次世代電子商取引推進協議会（ECOM）	

参考資料

ヒヤリング依頼書

ＸＸＸＸＸＸ株式会社
部長以上　ＸＸＸＸ 殿

次世代電子商取引推進協議会
情報セキュリティＷＧ 事務局

情報セキュリティ向上への取り組みに関するヒアリングへのご協力へのお願い
－ 個人情報保護を中心として －

平素より、次世代電子商取引協議会（ＥＣＯＭ）の活動にご理解、ご支援を頂きありがとうございます。

情報セキュリティＷＧでは、電子商取引環境における情報セキュリティ向上に向け、企業間や経営・管理者層と技術・実務者層での情報セキュリティに対する共通理解を支援するための、電子商取引における「情報セキュリティガイドブック２００８」を作成していくことを目標として活動を進めております。

その際、代表的な企業様の、現実のセキュリティ対策の実情を踏まえたガイドブックにしたいと考えております。つきましては、御社の情報セキュリティ対策への取組みや考え方全般のお話と、開示可能な具体的な対策事例について、その対応を決定する際にトリガーとなった法令、通達、社内規約等との関係について、下記のヒアリングさせていただきたく、ご協力の程お願い申し上げます。

－ 記 －

１．ヒアリング希望時期　：　１０月上旬から１１月上旬
２．ヒアリング先　　：
（１）経営者もしくは管理者
（２）情報セキュリティ部門 実務担当者

３．ヒアリング時間　　：　各 1～２時間程度

４．ヒアリング項目（目的：別紙１.、ヒヤリング事項　別紙２）
（１） 御社の情報セキュリティ対策全般について
（２） 開示可能な具体的対策について、その対策を講じる根拠となった法令等と、その対策との関連性について
（３）個人情報保護に関する法律やガイドラインについて
（４）個人情報保護や情報セキュリティ向上に関する組織的取組み、環境について
（５）情報セキュリティに関する活動組織に望むこと

以上

ヒヤリング依頼書（目的、範囲）　　別紙１

情報セキュリティ向上への取り組みに関するヒアリング
－ 個人情報保護を中心として －

（１） 御社の情報セキュリティ対策全般について
- 御社のユニークな情報セキュリティに対する取り組み等ありましたら、お願いします。

（２） 開示可能な具体的対策について、その対策を講じる根拠となった法令等と、その対策との関連性について
- 詳細な対策そのものまでをお話いただく必要はありません。どのような要求（法令等）の下、どのような対策を講じることになったのか。を、可能な範囲でお話いただけますと幸いです。

（３） 個人情報保護に関する法律やガイドラインについて
- 個人情報保護法は、IT 関係法令の中でも比較的早期に実施されております。ヒアリング先の皆様の認知の度合いをお聞かせください。

（４） 個人情報保護や情報セキュリティ向上に関する組織的取組み、環境について
- 個人情報保護法施工後、実際にその法律や派生する各省庁の通達等を元に、何らかの対策を施している場合、可能な範囲でその内容をお聞かせ下さい。

（５） 情報セキュリティに関する活動組織に望むこと
- 私ども ECOM は、経済産業省管轄ですが、EC に関連した民間企業、法曹界、一般消費者を含めた幅広い意見を集約できる活動が特徴です。私どもや、その他中央官庁を含めた情報セキュリティに関する活動をしている組織に望まれる事柄がありましたら、お聞かせ下さい。

＊尚､本ヒアリング結果に関しましては､ご要望により名称等を匿名にすることも可能ですので、ご希望でしたらお知らせ下さい。ヒアリング内容は、ECOM 情報セキュリティ WG の成果報告に反映させ、今後の日本の情報セキュリティ政策に役立てます。

以上

ヒヤリング依頼書(具体的な設問項目)　　別紙２

個別設問項目

１．個人情報保護に関する法律やガイドラインについて（設問項目 A）

（１）個人情報保護法、不正アクセス行為の禁止等に関する法律、他

（２）個人情報保護ガイドライン（経済産業省、ＥＣＯＭ、他）

（３）情報セキュリティ管理基準（経済産業省、他）

http://www.meti.go.jp/policy/netsecurity/law_guidelines.htm

２．個人情報保護や情報セキュリティ向上に関する組織的取組みについて（設問 A）

（１）OECD 個人情報保護 8 原則、ISO27000 シリーズ（BS7799,etc）、

（２）プライバシーマーク認定制度、ISMS 適合性評価制度

（３）情報セキュリティ対策ベンチマーク(自己評価)

（４）情報セキュリティガバナンス、情報セキュリティ報告書

http://www.jipdec.jp/　http://www.ipa.go.jp/security/benchmark/index.html

３．情報セキュリティ向上に関する環境整備について（設問項目 A）

（１）早期警戒パートナーシップ(JVN 等)、ＣＲＹＰＴＲＥＣ暗号技術評価報告

（２）ISO／IEC 15408(Common Criteria)について

（３）管理が必要な情報と自社特有の情報セキュリティ環境整備について（設問 B）

４．情報セキュリティ対策でのギャップ（違いや矛盾）について（設問 B）

（１）法律・ガイドラインと実務とのギャップ

（２）経営者と実務者の認識のギャップ

（３）委託元と委託先の実施レベルのギャップ

５．情報セキュリティに関する活動組織に望むこと（設問 B）

（１）よく知っている情報セキュリティ活動組織や活動内容

（２）過剰、過不足していると思う情報セキュリティ活動内容

（３）情報セキュリティ向上に対し支援してほしい事項

以上

追記

設問 A

◎大変よく知っている ◎よく知っている ◇知っている △よく知らない ×知らない

（知っている場合：疑問・課題、知らない場合：知らなかった理由など）

設問 B

自由回答（普段思っていることなど）

ヒアリングコメント

A社：業界トップの企業

(1) 個人情報保護に関する法律やガイドラインについて

法律やガイドラインに関しては、専門部署がそれぞれ大変よく知っている。個人情報保護法は法務部門が、不正アクセスに関しては情報システム部門がフローしている。不正アクセス関係は専門的な知識（情報処理、暗号）が必要であって、情報システム部門が中心に内部規定を作っている。個人情報保護法などの専門法、法律関係の専門知識に関しては、職場ごとに１名の法令エキスパートを各部門からの推薦により、任命し、法務部門が法令エキスパートに対して、法令を教育し、各部門に展開してもらっている。

情報セキュリティ管理基準（経済産業省、他）については、監査フローを作って、委託先の管理などを行っている。

(2) 個人情報保護や情報セキュリティ向上に関する組織的取組みについて

OECD 個人情報保護 8 原則、ISO27000 シリーズも良く知っている。プライバシーマーク認定制度、ISMS 適合性評価制度もよく知っているが、自社として取得しているわけではなく、個人情報を取り扱う系列会社には取得するよう勧め、その系列会社では、プライバシーマークはとっている。自社としては、情報セキュリティ対策ベンチマークによる自己評価を行っている。情報セキュリティガバナンスなど、自社のコンプライアンスを向上させようとする取組みは、会社方針に掲げ、全社的な取組みを行っている。公式な情報セキュリティ報告書は公開していないが、全社的なＣＳＲ（Corporate Social Responsibility）報告書の中で、個人情報保護や情報セキュリティ向上に関する組織的取組みについて報告している。

(3) 情報セキュリティ向上に関する環境整備について

早期警戒パートナーシップにも参画している。暗号技術評価報告やＪＶＮは情報システム部門 担当者が見ている。ISO／IEC 15408 知っているがＩＴベンダー企業ではないので、それ自身を調達条件とはしていない。

管理が必要な情報と自社特有の情報セキュリティ環境整備については、情報・情報機器の持ち出し管理、メールの管理、持ち出しデータの暗号化などを行っている。データの持ち出しは極力やめたい。できれば、シンクライアント化にしていく必要もあると考えている。しかしながら、系列会社や関連会社などの中小企業に関しての設備投資は厳しいので、現時点では全てをシンクライアントにしていくというわけにはいかないように思う。

(4) 情報セキュリティ対策でのギャップについて

情報セキュリティ対策では、法律やガイドラインの解釈が対称に応じて多様であり、教育が必要であり、法令エキスパートなどを配置している。ガイドラインの違いに関しては、経

済産業省、厚生労働省、などで違う部分もあり、これらも、運用面で対象や内容が異なるので、法令エキスパートなどを通じて教育している。個人情報管理委員会を設置しており、ＰＤＣＡサイクルや保護状況を月１回確認している。法務関係のポータルサイトがあり、Ｑ＆Ａ集なども載せている。相談窓口も設置している。法務部門では、コンプライアンス関係のケーススタディー事例を 2 ヶ月に 1 回、ポータルサイトに流している。

（B 社） 複数業界にまたがる印刷業界のトップクラスの企業

(1) 個人情報保護に関する法律やガイドラインについて

総合印刷企業として、金融、製造、出版、公共などあらゆる業種にわたって、顧客企業から個人情報を含めた情報を預かり、加工情報を納品するだけでなく、一般消費者に向けての情報発信の業務の委託を受ける。また、情報の内容も個人情報や営業秘密として機微な情報から、一般公開しても問題のない情報まで幅広く扱っている。作業を外部へ委託することもある。このため、法律やガイドラインは大変良く知っている。主に、経済産業省のカイドライン（一般産業）をベースとし、金融庁、厚生労働省、総務省なども参照している。

情報セキュリティ管理基準は内部監査に活用している。本社指導による内部監査の管理基準の徹底は年に１回、事業部ごとに行っている。法令やガイドラインに関しては、印刷業界指針を作成（平成１６年１２月）し、社内へ事例集ともに配布している。平成１８年２月には、印刷業界における１２０項目からなるＱ＆Ａ集のまとめに尽力した。月に１度は、各事業所の情報セキュリティ管理責任者（幹部および関係者含む）に、実態調査要請や外部情報（ＪＩＰDEC／Ｎｅｗｓ／国内の情報漏えい事故など）の発信を行い、全社的に情報の共有化を図っている。

製造現場はいろいろな分野（金融、製造、出版、公共など）があり、現場での事故撲滅を図るため、トップダウン手法に偏ることなく、本社関係者が直接に実際の職場へ足を運ぶことにしている。足を運んだ製造現場では、ルールが適正か、また適正なルールであれば記録が残されているかを、製造現場（事業部）の責任者と本社の責任者とダブルチェックして確認している。高いセキュリティを必要とする職場に関しては、特別な管理策を導入し、頻繁に見に行く。

(2) 個人情報保護や情報セキュリティ向上に関する組織的取組みについて

OECD 個人情報保護 8 原則、ISO27000 シリーズは大変よく知っている。プライバシーマーク認定制度、ISMS 適合性評価制度に関しては、審査員補になっている。ＩＳＯ２７０００は個別部門では取得した。今後、全社で取り組んでいく。情報セキュリティ対策ベンチマーク(自己評価)はそれぞれの事業部でやったことがある。データの入力の仕方によっては、かなり良い点数がでる。より厳しい評価基準が必要と感じている。視点と範囲を定めないと何を評価していたのかわからなくなる。

公開を目的とした情報セキュリティ報告書の正式版は作っていない。情報セキュリティ報告書を公開することはしていないが、自社のＣＳＲ（Corporate Social Responsibility）のレポートを作って毎年報告している。その中で、特集記事として毎年情報セキュリティ管理の詳細を公開し、外部の評価機関からも「情報セキュリティ報告書としても十分」との評価

を得ている。

いろいろな対策を講じてきたが、委託された情報加工が大半であるため、顧客企業の指示や要望に沿った誤りのないサービス提供、すなわちケアレスミスによる完全性喪失の防止が最大の課題である。

(3) 情報セキュリティ向上に関する環境整備について

早期警戒パートナーシップは契約している。セキュリティ製品事業部としては、大変よく知っている。セキュリティ製品の事業部としては、それ自身を調達条件として意識している。月間約７０００万件にもおよぶ個人情報を含む仕事を受託している。仕事が発生するたびに、個人情報を含む仕事であるか、識別番号を付けてシステム上でも管理している。暗号ソフトも利用しているが、セキュリティの必要性によっては、パスワード保護の場合もある（個人情報を扱う委託業務の場合は１００%暗号化している事業所もある）。

(4) 情報セキュリティ対策でのギャップについて

法律・ガイドラインと実務とのギャップについては、いろいろな分野からの仕事を受けているが、それぞれの事業部や顧客企業ごとに、関わる業界や主務官庁が異なる。また地域の指針を理解し、ギャップを生じないようにしている。

経営者と実務者の認識のギャップはない。情報セキュリティ管理体制として、ＣＳＯの下に、事業部の責任者が集まる代表者会議（協議と認証）と、本社の情報セキュリティ管理推進部会（運用推進）とを設置し、代表者会議でトップダウンに意思決定、情報伝達するとともに、本社職員が事業部に足を運び、運用を推進している。

委託元と委託先の実施レベルのギャップについては、委託先へ自社と同等の管理レベルを求めることは課題であるが、特に物理的なセキュリティと人的なセキュリティに関しては監査基準を設けている。委託先監督には以下の３セット。監査基準項目としては５０項目位。

①信用調査

②契約事項

③監査基準（品質・管理面で、どういう項目をチェックをしているか）

仕事が終わった時の管理も重要で、親展ＤＭ（ダイレクトメール）の不達の事後処理も重要であって、廃棄処分の徹底も心がけている。また、不達のダイレクトメールは顧客企業への返却が原則。ただし、委託先に不達となったＩＤ番号のみ（個人情報を含まない形で）情報を返す場合もある。

（C 社）複数業界にまたがるコンベンション等の開催を支援する企業

(1) 個人情報保護に関する法律やガイドラインについて

最近、顧客からプライバシーマーク取得を期待されており、プライバシーマーク取得に取り、取得するためにコンサルテーションを受けているので、法律やガイドラインも知っている。情報セキュリティ管理基準も公共関係の入札に応札しているので、ある程度は知っている。

(2) 個人情報保護や情報セキュリティ向上に関する組織的取組みについて

OECD 個人情報保護 8 原則、ISO27000 シリーズも。セミナー等に参加したことがあるので、あることは知っている。プライバシーマーク認定制度、ISMS 適合性評価制度については、Ｐマーク取得のコンサルを受けている(前述)。情報セキュリティ対策ベンチマーク(自己評価)、ＩＳＭＳはよくは知らない。情報セキュリティガバナンス、情報セキュリティ報告書についても、あることはなんとなく聞いているが、よく知らない。

(3) 情報セキュリティ向上に関する環境整備について

早期警戒パートナーシップ、ISO／IEC 15408 はよくは知らない。ＰＣ関係のセキュリティに関しては、プログラミングも含めて、エキスパートと契約していて、その意見を聞いている。独自と言えるかわからないが、Ｐマークのコンサルタントから、情報のカテゴライズをするように指導されていて、個人の身体の情報や企業の名刺（参加者）の情報まで扱うので、情報の秘匿性(機微度)によって分類管理するようになってきた。

情報システムの管理については、Ｗｅｂサーバ、メールサーバはＡＳＰ（外部）委託し、会社の共有サーバは自社内にある。建屋、事務所への入出管理は、ビル管理会社がしっかりやっていて、休日は本人確認が取れないと入れない。共通ＤＢ、プリンターサーバは事務所内にある。アクセス履歴を取っている。それらの仕掛けに対しては、顧問契約をしているＰＣの専門家にアドバイスをもらっている。

(4) 情報セキュリティ対策でのギャップについて

プライバシーマーク取得で、事務所でトイレに行くにも、机の上に書類を残さないことも必要だと指導された。十数名の組織なので、情報セキュリティの専任の担当者が監視しているわけではない。監視を１００％達成させることは難しい。ノートＰＣの持ち出しに関しても、持ち出さないことが望ましいとの指導であったが、イベント開催では、ＰＣによるプレゼンテーションの準備が必要であり、ノートＰＣなどの持ち出しの際には、ＰＣのデータをクリアーにしてから、必要なデータをインストールして進めている。

出張先等でメールを受け取らないと、お客さまとのコミュニケーションが取れない。サービスの低下となる。単にノートＰＣを持ち出すなというのは、形式的になり、個人でＰＣを持ち出し、事故となる可能性がある。会社の持ち出しＰＣに関しては、アドミニストレータ権限に利用不可として、システムに不必要なソフトが勝手にインストールされることを禁止している。

経営者と実務者の認識のギャップについては、担当者からいろいろソフトを導入しては要望があるが、ＰＣの専門家と話して、導入すべきかを検討して進めている。特にギャップが大きくあるとは思っていない。

委託元と委託先の実施レベルのギャップについては、委託元から契約時の要請は、概括的なことが多く、情報を漏らさないという条項を一筆いれろということが多い。仔細な調査票を記入しろということを行ってくる組織は少ない。

トイレに行く時にも、書類（印刷物）を出しておくなと言われても、電子化されたデータの照合、確認等では、印刷物で確認していくことが多く、確認作業が終わるまで、トイレに

も行けないというのは不合理である。持ち出しＰＣはいけないというのも、それぞれに業務に合わせた対処方法がいるのだと思う。そうした運用管理において、うまくやっている事例などを教えてもらえる活動があると助かる。

Ｐマーク取得のため、コンサルテーション（指導）受けているが、かなりの投資で、小さな会社としては、負担が大きい。一括して払うために純利益の中から捻出するのはかなり厳しい。何か支援策があってもとも思う。大きな会社の様に、専任の教育担当やそれぞれの部署での委員を置くということはできない。トイレに行けない、ＰＣが持ち出せない、従業員の負荷やサービスの低下にならない､小さな事務所でも実現できる実務的な改善策がほしい。

（D 社） 数名で法務に関する業務を行う小規模事務所

(1) 個人情報保護に関する法律やガイドラインについて

法律関係の仕事なので､よく知っている｡法務省含め､経済産業省などのガイドラインは、大変よく理解している。法律やガイドラインはよく知っているが、事務所の実務としてはあまり使ったことがない。ガイドラインだけでは、具体的なことが見えないので、実際の問題では使い切れないし、良い、悪いの判断基準にしきれない。

(2) 個人情報保護や情報セキュリティ向上に関する組織的取組みについて

OECD 個人情報保護 8 原則、ISO27000 シリーズは、昔、関係したことがあるので、よく理解している。プライバシーマーク認定制度、ISMS 適合性評価制度に関しては、かなり前に、ＩＳＭＳを取得しようとしたが、初期コストと１００万円、維持コスト１００万円くらいかかるといわれ、取得をしなかった。情報セキュリティ対策ベンチマーク(自己評価)、セミナーなどで、聞いたことがある程度で知ってはいるが、実施したことはない。

情報セキュリティガバナンス、情報セキュリティ報告書があることはなんとなく聞いているが、士業として、守るべき責務としての守秘義務の方が重く、あえてそれを評価、公表、宣伝する必要はないと考える。

(3) 情報セキュリティ向上に関する環境整備について

早期警戒パートナーシップは知ってはいる。セミナーなどで、聞いたことがある程度である。ISO／IEC 15408 はよくは知らない。

事務所では、現物主義なので、業務上の重要な情報に関しては、紙ベースである。提出書類などは入力、印刷して、提出先に持ち込むことが多い。書類は１案件当たり、２－３センチの厚さにはなるので、数十件の案件でキャビネ１列分くらいにはなる。少なくとも 3 年間は保存する必要があるので、仕掛中の案件も含めると、かなりの量となり、事務所が書庫になってしまう。同業他社では、倉庫に預けるところもある。現物が多いので、イメージで取り込めることも必要である。電子保存の目的は原本保証、偽造というよりも、経過、経緯説明など再利用がしたくなることがある｡基本的には電子保存ではなく紙ベースでの保存です。当初から電子データにて作成しているデータは､不要になったものから CD-EOM に落とし､バックアップも作成の上保管しておりますが、保管メディアとして何が適切かは、検討の余地があるかもしれません。

事務所での情報共有は、申請書のフォーマットのような共通データは共有ディスクでファイルシェアを行っているが、業務上のデータ（個別案件データ）各自のＰＣにて作成、共用プリンターで印刷している。システム管理は、ＰＣに詳しい担当者が兼務している。外部の専門家と相談しながら進めていて、外部のセキュリティソフト、Windows アップデートなどは随時行っている。メールは外部のサービスプロバイダーの物を使っている。基本的にＰＣの持ち出しは行っていない。印刷して持って行く。出張時の連絡等については、事務所のＰＣではなく、個人所有ＰＣなどで、メールを受けている。

業務上の情報はすべて守秘義務事項であり、相手方の了解を得た場合以外はメールでのやりとりはしない。事務所の中で、秘匿性の高い情報は、担当と直接話す。スケジュール的な話や協議会などの公的なところとのやりとり、公的な情報のやり取りに関しては、メール（個人管理）のメールを使っている。

(4) 情報セキュリティ対策でのギャップについて

個人情報保護法施行以来、個人情報の照会が難しくなっている。個人情報保護法施行以来、個人情報の照会が難しくなっている。情報セキュリティ向上に対し支援してほしい事項として、具体的な何をすべきかを提示すべきかを示すべきと考えている。インターネットはなんとなく不安なところがあるのだけれど、どこが安全で、どこが危険なのかが見えないので、どこを優先的に対策していくべきかを言うのが難しい。

以上

ＥＣにおける情報セキュリティに関する活動報告書 2007

平成２０年３月　発行

発　行　　次世代電子商取引推進協議会

販　売　　財団法人　日本情報処理開発協会
電子商取引推進センター
東京都港区芝公園３丁目５番８号
機械振興会館３階
TEL:０３（３４３６）７５００

ISBN978-4-89078-663-3 C2055