最近の情報セキュリティ問題について

Current Status of Information Security

奥　山　　徹
Tohru　Okuyama

要　旨

情報セキュリティの問題は、加速する高度情報社会の進展にとって大きな脅威となると考えられている。そのため、日本政府は 2005 年から第一次セキュリティ基本計画を策定し、情報セキュリティの重要性を警告するともに、政府として取り組むべき情報セキュリティに関する基本的な問題点の洗い出しと、その対応策を示した。2008 年に第一次基本計画が終了すると、直ちに第二次セキュリティ基本計画を策定し、その中で、「事故前提社会」の概念を明確化した。すなわち、情報セキュリティ対策を施しても、全てのインシデントを防ぐことは出来ず、防御機構としての情報セキュリティ対策と同時に、いざインシデントが起きたときに、いかにすばやく復旧させるかが重要であることを示唆した。そして、2011 年に起きた東日本大震災は、重要インフラとしての情報ネットワークの災害時の重要性を高めたのと同時に、大災害時の弱点も露呈させた。そして、最近では、遠隔操作ウイルスに代表されるように、一般人がサイバー犯罪に巻き込まれることが日常的となり、さらには国家や大組織によるサイバーテロに対する対策まで、情報セキュリティを巡る状況は複雑さを増している。ここでは、このような状況を踏まえ、今後の情報セキュリティのあり方について考える。

1. IPA が示した 2013 年版情報セキュリティに対する 10 大脅威

日本の情報セキュリティに関する中心的機関での一つである独立行政法人情報処理推進機構（以下、「IPA」と記す。）は、2013 年 3 月に IPA セキュリティセンターより、「2013 年版 10 大脅威　～身近に忍び寄る脅威～」[1]を公表した。この中で、IPA は 2013 年度において特に重要となる情報セキュリティに対する脅威を有識者の意見をまとめる形で順位付けしている。このドキュメントの初めの部分には、変遷する情報セキュリティの問題についてのまとめが表 1 のようにまとめられている。なお、表 1 は、一部著者が加筆、編集した。図1に示すとおり、今世紀に入り、ネットワークウイルスが全盛となり、Nimda や Code Red など、旧来のウイルスとは一線を画すネットワークを介して伝播することを主な感染経路とするものが現れ、ネットワーク上で蔓延する事態となった。その後は、ウイルスの脅威は継続的に続いている中、いわゆる金銭窃取目的の新たな手口が多数出現し、それが全世界的に拡散し、今日に至っている。そのため、防衛戦略も個々のネットワークや PC を守るというレベルから、国家や企業が個人も交いた形ある

いは国際的な関係の中で組織的な防衛策をとらなければならなくなっている。

表 1. 情報セキュリティの変遷[2]

	2001 年～2003 年	2004 年～2008 年	2009 年～2012 年
時代背景	ネットワークウイルスの全盛	内部脅威・コンプライアンス対応	脅威のグローバル化
IT 環境	コミュニケーション手段の確立	e-コマースの加速	経済・生活基盤に成長
セキュリティの意味合い	サーバや PC の保護	企業・組織の社会的責任	危機管理・国家暗線保証
攻撃の意図	いたずら目的	＋金銭目的	＋抗議目的、諜報目的
攻撃の傾向	ネットワーク上の攻撃	人を騙す攻撃の登場	攻撃対象の拡大
攻撃対象	PC、サーバ	人、情報サービス	スマートデバイス、重要インフラ
対策の方向	セキュリティ製品中心	マネジメント体制の確立	官民・国際連携の強化 セキュリティ人材育成強化
主なセキュリティ事件	Nimda 流行（2001） Code Red 流行（2001） SOL Slammer 流行（2003）	P2P ソフトによる情報漏洩（2005～） 不正アクセスによる情報流出（2005～） スパイウェアによる不正送金（2005～）	米・韓に DDoS 攻撃（2009） Stuxnet による攻撃（2010） 政府機関を狙ったサイバー攻撃（2011） 金融機関を狙った攻撃（2012） 韓国に対する大規模攻撃（2013）

表 1 の「対策の方向」に示すとおり、これからの情報セキュリティ対策は、大規模な情報収集と人材の育成が急務な状況であり、そのための組織作り、法整備が急ピッチで進められている。このような中で公表された 10 大脅威とは以下のようなものである。

1. クライアントソフトの脆弱性を突いた攻撃
2. 標的型諜報攻撃の脅威
3. スマートデバイスを狙った悪意あるアプリの横行
4. ウイルスを使った遠隔操作

5. 金銭窃取を目的としたウイルスの横行
6. 予期せぬ業務停止
7. ウェブサイトを狙った攻撃
8. パスワード流出の脅威
9. 内部犯行
10. フィッシング詐欺

これらの中にはこれまでもよく知られたものから、最近流行のものまで含まれている。ここで、これらの詳細を示すことはしないが、我々の個人のネットワーク活動と深く関連するいくつかについて考える。なお、IPA は、この他に、これから注目すべき脅威として、

11. クラウド利用における課題
12. 重要インフラを狙った攻撃

をあげているが、この二つの問題は、これからではなく、今まさに緊急の課題として取り組まなければならないものである。例えば、12 に関連して、米国とイスラエルがイランの核関連施設を狙って開発されたとされる Stuxnet が、その制御を離れて流出し、その後多くの亜種を生みながら、未だに脅威となっていること[4、6 頁]は周知の事実である。また、11 に関してもクラウドの利用が加速する中、今後採用を考えている企業にとっては頭の痛い問題である。

さて、10 大脅威を個人の立場で見ていくと、1,3,4,5,8,10 当たりが特に重要と思われる。もちろん 10 個の脅威全てが、それぞれに重要であるが、個人のインターネット上での活動を考えた場合、この 6 つは特に重要である。そこで、これらの 6 つについて、最近の事例を交えて考えることにしたい。

2. 個人のインターネット活動における重要な脅威

1 については、これまではサーバに対する攻撃が主で、クライアントの場合でもその OS や Office ツールなどの主要アプリケーションの脆弱性を突く攻撃が一般的であった。しかし、今日では全てのクライアント上のアプリケーションが狙われている。文献[1]においても、Adobe の Reader や Flash Player のようなソフトウェアや Oracle の Java（JRE）の脆弱性を突く攻撃が横行しており、脆弱性の放置はウイルス感染リスクが高まると報告している。なお、現実に利用される脆弱性は 90％以上が既知のものであるが、中には未知のものもあり、いわゆるゼロディ攻撃の存在が IBM Tokyo SOC のレポート[5]でも報告されている。例えば Adobe Flash Player や Microsoft XML コア サービスの未知の脆弱性をついた攻撃などが 2012 年の上半期に登場している。今後も、このようなゼロディ攻撃の対象となる未知の脆弱性が使われる可能性があるが、現状でのそのほとんどが既知の脆弱性を利用した攻撃であることから、アプリケーションのアップデートを怠るべきではない。

3 のスマートデバイスを狙ったアプリの問題は深刻である。博報堂 DY グループ・スマートデバイス・ビジネスセンターの 2013 年 4 月の調査[6]によれば、全国のスマートフォン保有率は 45.6%であり（2012 年

11 月の時点では 39.1%と報告されている[7]。）、5 割を超えるのは時間の問題としている。このような中で、ポスト PC の代表としてのスマートデバイスを狙った新たな脅威が多数出現している。文献[4]に示したトレンドマイクロの調査によれば、スマートデバイスを狙ったマルウェアの検出数は、3 年間で 35 万件にも達している。この数値は、図 1 に示すように、PC 関係のマルウェアでは 14 年かけて到達した値であり、スマートデバイスに関連する情報セキュリティの重要性が浮き彫りとなっている。

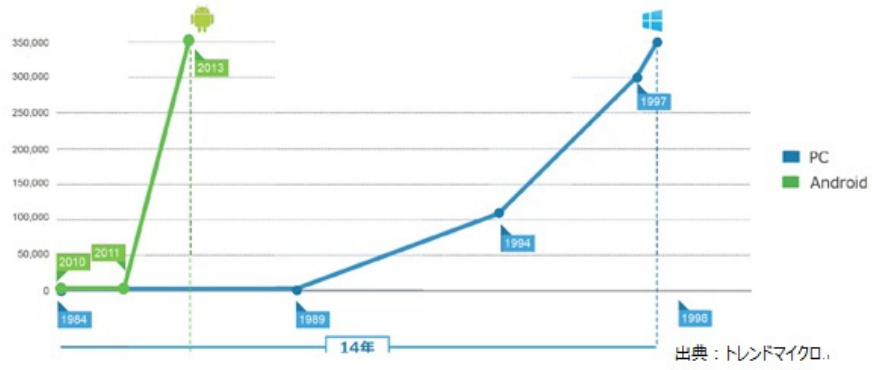

図 1. PC とアンドロイド端末における脅威の変遷（[4]の 3 頁参照）

4 の遠隔操作ウイルスの問題は、警察による誤認逮捕に発展し、大きな社会問題となった[8-11]。いずれの場合も、被疑者の IP アドレスの特定という単純な事実を元に誤認逮捕に発展してしまい、警察のハイテク犯罪に対する操作能力の低さを露呈する結果となった。詳細な分析は、誤認逮捕を犯してしまった警視庁[8]、神奈川県警察[9]、大阪府警察[10]、そして三重県警察[11]から出されている。いずれにしても、通常のネットワーク上での活動をしているだけで、このような事態に陥る可能性は誰にでもあり、今後、自分自身を守るための情報セキュリティ対策を強化しなければならない。

金銭窃取を目的としたウイルスとして、最近では ATS（Automatic Transfer System（自動送金システム））[12]や身代金要求型不正プログラム（ランサムウェイ）[13]が注目を集めている。金銭窃取目的としては、これまでキーロガーなどによるユーザ自身の入力を不正に入手するトロイの木馬型のウイルスが横行していたが、ATS はその後継というよりは進化型ととらえることができる。一方、ランサムウェイは PC などを使用不能にして、解除のための身代金を請求するものであり、日本国内では文献[13]に示すように 2012 年の 2 月に初めて確認された。このような手口により海外では既に多くの被害が出ている。いずれにしても、ネットバンキングが主流となりつつある現代において、金銭窃取を目的とした脅威は、今後猛威を振るうと思われる。

8 のパスワード流出については、これまでも大きな脅威として報告されており、「破られにくいパスワードを設定すること」、「パスワードはメモしないこと」など、多くの場面で様々な注意がなされている。しかし、最近の傾向を見ると、OpenID[14]のようなパスワードの一元管理が進んでいる。このような状態において、パスワードの流出は、個人が利用している全てのネットワークサービスを危険にさらすことになる。このような多様な技術の必要性と一元化による利便性の間の問題について著者らは既に警告を行っており

[15]、パスワードの管理は、今後も大きな情報セキュリティ上の問題となる。ところで、2013 年 4 月に eBookJapan から不正ログインに関する重大なお知らせ[16]が報告された。この報告では、2013 年 3 月までは、「複数の IP アドレスからログインページに対して機械的に総当たり攻撃等を行う大量アクセス行為（ブルートフォースアタック）」の発生が顕著に見られたというものから、4 月以降は「不正の疑われる複数の IP アドレスからログインページに対して、予め持っていたログイン ID とパスワードの適用可否を試行する大量アクセス行為」へと変わり、その査証として一つのログイン ID に対して発行するパスワードの数（ID を入れてログイン時にトライされたパスワードの数である。）がほとんどの場合、表 2 に示すように 1 回しか行われていないことをあげている。すなわち、あらかじめ流出した ID とパスワードが使われたことを示唆している。ここで問題はどのような経緯で ID とパスワードが流出したかであるが、残念ながらそれに対する調査は十分でなく、今後の調査の進展に期待した。いずれにしても、このように流出した ID とパスワードを使った不正アクセスは増加の傾向にあり、ID とパスワードの厳密な管理が必要である。

表2. eBookJapan への不正アクセスに使われた ID に対するパスワードの試行回数[16]

ログイン成立の場合		ログイン失敗の場合	
パスワード試行回数	該当 ID 数	パスワード試行回数	該当 ID 数
1	586	1	1327
2	347	2	72
3	37	3	20
4	4	4	7
5	5	5 回以上	5

最後、10 番目のフィッシング（Phishing）詐欺については、これまでたびたび警告されており、警視庁もフィッシング 110 番の Web ページを開設し、警告している。いずれにしても、フィッシング詐欺は人の弱みに付け込む悪質なソーシャルエンジニアリングアタックであり、今後も横行すると予測される。フィッシング詐欺にあわないためには、フィッシング対策協議会が公開している対策ガイドライン[17]などを参照し、各自が適切な対策を取ることが求められている。

以上、今回は個人向けと思われる問題を中心に解説したが、他の問題も重要である。そのため、文献[1]等を熟読し、必要な対策を講じるべきである。

3. 今後の情報セキュリティ対策について

最後に、今後の情報セキュリティ対策についてどのように考えるべきかを、総務省の情報セキュリティアドバイザリーボードが公表した総務省への提言[18]を元に考える。

この提言の中の基本的な考え方は、

① 情報の自由な流通の確保を基本原則とする
② 管理の規制を過度に行うことなく、信頼できるサイバー空間の構築
③ 完璧主義から脱却し、リスク認識に基づく対応の強化（事故前提社会）
④ 産学官がそれぞれの役割を果たす動的防御プロセス連携の確立
⑤ 国際連携によるサイバー空間政策の推進

の 5 項目である。①～③はこれまでの政府の施策の延長線上にあり、これまでも示唆されてきたことである。すなわち、これらは 3 項目は大原則であり、今後も継続されなければならない。一方、④と⑤もこれまで示唆されてきたことであるが、今回明確に④では産学官の連携、⑤では国際連携と関連機関の連携の重要性を説いている。ここでは、特にこの 2 項目に着目し、どのようなことが考えられているのか考察する。

3. 1. 動的防御プロセス連携

言葉だけとらえると何を意味するものか不明であるが、文献[18]を読み解くと次のような対策を想定していることがわかる。すなわち、

- モニタリングにおけるインシデント認知機能の向上
- モニタリングの高度化に資するサイバー攻撃の解析能力の向上
- 自律的な情勢判断の促進
- 情報共有の円滑化に向けた仕組みの検討

の 4 項目の重要性を説いている。これを図にすると、図 2 にようになる。すなわち、①モニタリング、②情勢判断、③意思決定、④行動というサイクルをまわすことになる。これは、従来、情報セキュリティの現場で考えられていた PDCA サイクル（Plan（計画）、Do（実施）、Check（点検・監査）、Act（見直し・改善））[19]とは似て非なるものである。情報セキュリティマネジメントにおいて考えられていた PDCA サイクルは経営現場のようなある程度時間的に余裕のある場合の手法を持ち込んだものであり、今日のような短期間に動的に事態が変動する場面を想定したものではない。したがって、現実の情報セキュリティマネジメントのように、より短時間に重大な決定をする場合にはもはや役に立たなくなっている。

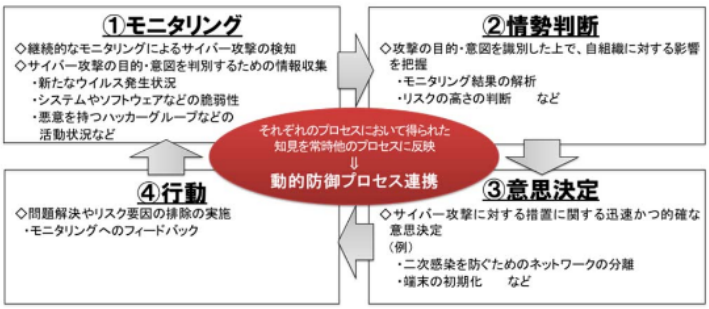

図2. 動的防御プロセス連携[18、4 頁]

図2に示されたサイクルは、一般には OODA ループ（Observe（モニタリング）、Orient（情勢判断）、Decide（意思決定）、Act（行動）を繰り返す。）と呼ばれるものである。OODAループは、米空軍のジョン・ボイド大佐の理論[20]に基づくものであり、本来は空戦を有利に導くための戦略・戦術レベルの意思決定のあり方を説いたものであった。それが今日では、マネジメントにおける有用性が着目され、経営場面に応用が図られるようになるとともに、情報セキュリティマネジメントでもその有用性が議論されるようになった。

ここで着目すべきは、モニタリングにおいて、現場における継続的なサイバー攻撃の検知（戦術的攻撃検知）を行うと同時にサイバー攻撃の目的・意図を判明するための情報収集（戦略的諜報活動）を行うことを示唆していることである。これまで、戦術的攻撃検知に関して、IDS/IPS の導入や Firewall の機能強化などと関連して議論されていたが、ある意図を持ったサイバーインテリジェンスの必要性について、明確な形で示されてはいなかった。この部分は、例えば CERT や IRT の情報活動について語られることが多かったが、今回の提言では明確な意図を持って、サイバーインテリジェンス機関が連携する必要性を説いている。今後は、産学官の総力を挙げた情報セキュリティに関する情報収集体制が整い、攻撃検知からその意図の把握、さらには反撃体制の構築までがスムーズに進むことが期待される。

そして、もう一つの問題点として「利用者に自律的な対応を促す仕組みづくり」を求めていることである。このような仕組みは 2011 年の東日本大震災後における個人の PC からの情報回復がほとんど行えなかったことを考えると、民間における個人の持つ情報を組織的に防衛する仕組みを整えることとも含めて考えるべきである。すなわち、大企業などはデータセンターを活用し、大災害に備えた事業継続性計画（BCP）を整備することで、自身のデータを守る術を計画できるが、個人や中小企業などのように大規模なデータセンターを頼れない情報弱者は、相互互助的な仕組みを立ち上げることが必要であり、その場合、個人の自律的な情報セキュリティへの取り組みは、その前提条件として重要な問題となる。

3. 2. 国際連携

文献[18]の提言の中でもう一つの連携の柱として、国際連携について示唆されている。今日のサイバー犯罪は国境を越えてやってくるため、どうしても国際的に連携した動きをとらなければならない。この点に関して提言では、以下の 3 つを主要な問題点として議論している。

（1）グローバルなインターネット環境の安全の確保
（2）日本企業のグローバル展開への貢献
（3）国際的なサイバー空間の規範形成への主導的な取組

（1）のインターネットの安全性確保に関してはこれまでも議論されてきたことであり、今後はより一層緊密な国際協力により安全性の向上が図られるべきである。一方、（2）に関しては、情報流通の安全性だけでなく、実際の企業の海外展開についての物理的な安全性を含めた広範な議論が必要である。最後に（3）に関して、全世界規模に広がったサイバー空間の秩序形成に対して、国際的な機関と連携した動きが重要となっている。（3）に関連して、政府のセキュリティ政策会議においても「世界を率先するサ

イバー空間の構築」として取り上げられており、第 34 回の会議資料[21]には、そのための施策として次のようなことがあげられている。

① 外交：基本的な価値観を共有する国等とのパートナーシップ関係の多角的構築・強化
▸ サイバー空間を利用した行為に対する国連憲章や国際人道法等の個別具体的な国際法の適用について引き続き検討。
▸ 米国等との間で、サイバー領域での具体的対処の在り方、国際的なルール作りといった分野における議論を深化。
② 国際展開：ASEAN等とともに成長できる関係を構築し、サイバー攻撃への対応能力構築の支援
▸ 諸外国と連携してサイバー攻撃に関する情報収集ネットワークを構築し、攻撃の発生予知、即応等に関する研究開発を実施。
▸ 官民連携によるボットウイルス対策など国内における成功事例の紹介や共同プロジェクト、机上演習等を実施。
③ 国際連携：国境を越えるサイバー攻撃に関するインシデントへの対応・連携の強化
▸ 外国捜査機関等とのサイバー犯罪に係る情報交換を継続的に行うとともに、連携強化等のため、職員を派遣。
▸ 相互不信による不測事態回避のため、我が国の基本的な立場等を共有するとともに、インシデント発生した場合の相互の連絡体制等を平時から構築し、国際共同研究や複数国間におけるサイバー攻撃対応演習等を実施。

これらは、これからの日本の情報セキュリティ対策に関する国際的施策として実施されることを求められており、今後の展開が期待される。

4. 終わりに

以上、情報セキュリティに関連した最近の動向を、主に IPA の示した 2013 年の 10 大脅威と総務省に対するセキュリティアドバイザリーボードの提言を中心として、最新事例を交えながら紹介した。ただし、今回紹介したものは、現在インターネットをはじめとするパブリックネットワークに関連する脅威のごく一部を示したものである。現実には、ここに示された以外にも多くの問題点があることを理解しておいて欲しい。

最後に、最近の気になる話題を示し、問題は根深く我々の生活に密着して広がりを見せていることを指摘して本稿を終える。セキュリティ関係者の最近の呟き（Twitter や Facebook などソーシャルメディアでの活動など。）を拾っていくと、そこに産業制御システムの高度化とそれに対するサイバー攻撃の懸念が散見される。例えば、産業ロボットによる組み立て工程におけるネットワーク化と高度制御の導入、インテリジェント医療ロボットによる高度な手術の実現、農業工場の制御・計測機器のネットワーク化と詳細制御、等などである。このような分野は、生産ラインの高度制御による生産性の向上や直面する疾患を

抑えるための緊急手術などが目的であり、そのため情報セキュリティ対策はどうしても後回しとされてしまう傾向がある。しかし、現実的にはこれらの制御システムは基幹産業や新世代農業を支える重大なコンポーネントであり、医療ロボットネットワークは人の生死に直結するものである。これらのシステムがランサムウェアのようなマルウェアに乗っ取られて、身代金を要求されるようなことは十分考えられることである。

情報システムの高度化が進み、人の生活により密着して発達し、人類の生活が良くなることは歓迎すべきことであるが、その裏で、このようなサイバー犯罪の危険性が高くなっていることは十分認識すべきである。

文献など

[1] 独立行政法人情報処理推進機構、「2013 年版 10 大脅威　～身近に忍び寄る脅威～」、2013 年 3 月。URL：http://www.ipa.go.jp/security/vuln/documents/10threats2013.pdf

[2] 独立行政法人情報処理推進機構、「2013 年版 10 大脅威 簡易説明資料」、2013 年 3 月。URL: http://www.ipa.go.jp/security/vuln/documents/10threats2013_slide.pdf

[3] Nate Anderson, “Confirmed: US and Israel created Stuxnet, lost control of it”, Art Technica, Law&Disorder, 2012/6. URL: http://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/

[4] トレンドマイクロ、「「ポスト PC」時代に進化する脅威」、Trend Labs 2012 年間セキュリティラウンドアップ、2013 年 2 月。URL: http://jp.trendmicro.com/imperia/md/content/jp/threat/report/qsr/2012asr.pdf?cm_sp=Corp-_-sr-_-2012asr

[5] IBM、「2012 年　上半期　Tokyo SOC 情報分析レポート」、2012 年 8 月。URL: http://www-935.ibm.com/services/jp/its/pdf/tokyo_soc_report2012_h1.pdf

[6] 博報堂 DY グループ・スマートデバイス・ビジネスセンター、「全国スマートフォンユーザー100 人定期調査　第 5 回分析結果」、2013 年 2 月。URL: http://www.hakuhodo.co.jp/archives/newsrelease/10469

[7] 博報堂 DY グループ・スマートデバイス・ビジネスセンター、「全国スマートフォンユーザー100 人定期調査　第 4 回分析結果」、2012 年 11 月。URL: http://www.hakuhodo.co.jp/uploads/2013/02/20130212_2.pdf

[8] 警視庁、「インターネットを利用した犯行予告事件における警察捜査の問題点について」、2012 年 12 月。URL: http://takagi-hiromitsu.jp/misc/misidentification2012/tokyo.pdf

[9] 神奈川県警察、「横浜市立小学校に対する威力業務妨害被疑事件における警察捜査の問題点等の検証結果」、2012 年 12 月。URL: http://takagi-hiromitsu.jp/misc/misidentification2012/kanagawa.pdf

[10] 大阪府警察、「インターネットを利用した犯行予告ウイルス共用事件の検証結果」、2012 年 12 月。URL: http://takagi-hiromitsu.jp/misc/misidentification2012/osaka.pdf

[11] 三重県警察、「インターネットを利用した犯行予告・ウイルス共用事件（伊勢神宮に対する威力業務妨害事件）の検証結果」、2012 年 12 月。URL: http://takagi-hiromitsu.jp/misc/misidentification2012/mie.pdf

[12] 勝村幸博、「サイバー金融詐欺の被害は 60 億円超　不正自動送金する手口も登場」、日本経済新聞、2012 年 12 月。URL: http://www.nikkei.com/article/DGXNASFK1803S_Y2A211C1000000/

[13] トレンドマイクロ、「PC を使用不能にして「身代金」を要求するランサムウェア、日本国内でも確認」、Scan NetSecurity、2012 年 2 月。URL: http://scan.netsecurity.ne.jp/article/2012/02/28/28510.html

[14] OpenID Foundation, "OpenID Authentication 2.0 - Final", 2007/12. URL: http://specs.openid.net/ auth/2.0.

[15] グエン スン カイン、奥山徹、「安全なデータ転送のための多様な暗号技術を結合するゲートウェイシステムの開発」、『朝日大学大学院経営学研究科紀要』、2013 年 3 月。印刷中。

[16] eBookJapan、「【重要なお知らせ】不正ログイン被害のご報告とパスワード再設定のお願い」、2013 年 4 月。URL: http://www.ebookjapan.jp/ebj/information/20130405_access.asp

[17] フィッシング対策協議会、「消費者向けフィッシング詐欺対策ガイドライン」、2012 年 12 月。URL: http://www.antiphishing.jp/report/pdf/consumer_antiphishing_guideline.pdf

[18] 情報セキュリティアドバイザリーボード、「総務省における情報セキュリティ政策の推進に関する提言」、2013 年 4 月。URL: http://www.soumu.go.jp/main_content/000217000.pdf

[19] 独立行政法人情報処理推進機構、「セキュリティマネジメントと PDCA サイクル」、2012 年 8 月。URL: http://www.ipa.go.jp/security/manager/protect/pdca/#pageHeader

[20] 例えば、中村好寿、『ビジネスに活かす！米軍式意思決定の技術』、東洋経済新報社、2006 年 6 月参照。

[21] 情報セキュリティ政策会議、「資料1－2　サイバーセキュリティ施策（案）概要」、2013 年 5 月。URL: http://www.nisc.go.jp/conference/seisaku/dai34/pdf/34shiryou0102.pdf

奥山　徹　（経営学部経営情報学科教授）