（平成１５・０４・０１財情第２５号）

『セキュリティホールに関する法律の諸外国調査』
報告書

平成 15 年 8 月 29 日

経済産業省
セキュリティホールに関する法令等の国内外調査委員会

改訂履歴：

平成 15 年 8 月 29 日 初版
平成 15 年 10 月 31 日 改訂

目次

（余白）

第１章　はじめに

２００３年１月末に、ＳＱＬスラマーの大量な感染被害が報道をにぎわせた。このＳＱＬスラマーは、SQL Server 2000 と MSDE 2000 のセキュリティホールを悪用した新種のワームであって、これが、多大な損害を引き起し、とくに韓国において、深刻な障害を引き起こしたのは、いわゆるバグ・フィックス（不具合の修正）をあてていなかったことが被害拡大につながったということであった。このような事件を契機として、韓国においては、報道によれば、マイクロソフト社自体が、そのソフトウエアの瑕疵について責任を追求される訴訟を提起されたり、また、脆弱性を放置していたシステム管理者に対して、刑事罰をも考慮に入れた対応策を考えられたりしている。また、米国では、2003 年 2 月に発表された”National Strategy to Sec ure　Cyberspace”[1]の” Priority II: A National Cyberspace Security Threat and Vulnerability Reduction Program　“の“3. Reduce and Remediate Software Vulnerabilities”において政府が、 脆弱性公開にむけての最適のアプローチとメカニズムについて共同で発展させる義務があることが触れられている。世界的に見て、ソフトウエアの脆弱性に対して、何らかの対応を義務づけることにより、その脆弱性を塞いでいこうという流れが議論されはじめたところであるということができよう。

このような状況のもと、本調査の目的は、日本の経済産業省に対してコンピュータやネットワークの脆弱性から惹起される問題に関して主要各国の制定法、規則、ガイドラインの情報を提供することにあり、情報セキュリティの問題に関して各国の実際の規則、標準及び法律の概観をなすことにある。本調査が対象とする範囲は、民事・刑事及び行政法すべてにわたる。

本調査の手法は、我が国において調査委員会を構成し、その委員会で、各現地における法律専門家（法律事務所、大学教授等）に依頼する調査内容の調整および分析を行った。また、各現地における法律専門家においては、セキュリティと法律問題に対してのその国における第１人者を選任することができた。以下の質問の趣旨とそれに対する回答は、各国の生きた法を伝えてくれることになった。回答は、ソフトウエアの脆弱性をめぐる問題が、まさに、今議論が始まったばかりであること、もしくは、現時点では、未解決の問題であることを示すものとなったが、基礎的な資料として、重要な意味をもつものと考えられるであろう。

[1] “ http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

調査委員会

委員名簿

委員長　高橋郁夫（弁護士・高橋郁夫法律事務所）（英国担当）
委員　土井悦生（弁護士・オリック東京法律事務所 *）（米国担当）
委員　吉田一雄（清和大学法学部）（カナダ担当）
委員　町村泰貴（南山大学法学部）（フランス担当）
委員　石井徹哉（奈良産業大学法学部）（ドイツ担当）
委員　近藤佐保子（明治大学政治経済学部）（大韓民国担当）
委員　佐藤慶浩（日本ヒューレット・パッカード株式会社）
オブザーバ　山崎琢矢（経済産業省）
オブザーバ　川口修司（経済産業省）
オブザーバ　赤松寛明（経済産業省）

＊ オリック東京法律事務所：特定共同事業　オリック・ヘリントン・アンド・サトクリフ外国法事務弁護士事務所

調査協力　現地法律事務所等

米国
Professor Amelia H. Boss, Charles Klein Professor of Law, Temple University
Jon Stanley, Attorney at Law, Jon Stanley, P.A.
Joel B. Rothman, Vice President, Legal & Government Affairs, Cylant, Inc.
Stephen S. Wu, President and CEO, InfoSec Law Group, PC
英国（連合王国）
Graham JH Smith 、バード&バード法律事務所（ソリシターズ）、ロンドン
カナダ
John D. Gregory, General Counsel, Policy Branch, Ministry of the Attorney General (Ontario)
フランス
Valerie SEDALLIAN Avocat a la Cour de Paris（パリ控訴院付き弁護士）
ドイツ
Prof. Dr. Thomas Hoeren, Institut fuer Informations-, Telekommunikations- und Medienrecht, Zivilrechtliche Abteilung, Wesfalische Wilhelms-Universitat Munseter
大韓民国
㈱ローアンドビー　代表取締役／弁護士　李　海完

第２章　質問事項の法的背景

ソフトウエアの脆弱性をめぐる議論を法的な観点から検討すべきことが、委員会の課題となる。委員会としては、第３章の質問事項を作成した。詳細については、個々の質問と回答を検討する際に触れるが、これらの質問事項は、二つの焦点において、法的な議論が起こり得ることに注目して作成されている。二つの焦点というのは、脆弱性をめぐる責任の議論と脆弱性をめぐる開示の議論の問題であり、それらは、それぞれ、脆弱性に関し、それに関連する人々の対応についての評価規範と行為規範として位置づけられるものである。

2.1. 責任　(Liabilities)

そもそもソフトウエアの脆弱性が、どのようなものとして定義されているか、そして、各国の制定法、判例において、どのようなものとして認識されているかということが問題になろう。通常のソフトウエアに比較して、ハードウエアのファームウエアのようなソフトウエアが、法的にどのような位置づけがなされているか、また、既製品として市販されているソフトウエアと個別の依頼で開発させたソフトウエアとで法的にどのような位置づけがなされているかが検討されなければならないであろう。

次に脆弱性に関する欠点は、ソフトウエアの利用に際して法的にどのように評価されるかという問題がある。この問題は、修補義務は、どのような根拠から、どのような場合に発生するかという問題や、ベンダーは、その脆弱性をどの程度まで修補すべきかという問題を有している。

そして、脆弱性の情報を利用する行為は、法的にどのように位置づけられるのかという問題になる。脆弱性情報の利用やツールが、法的にどのようなものとして位置づけられるのかということが関心事項となる。これについては、民事的な位置づけと刑事的な位置づけについて各国の位置づけについて興味があるところである。特にサイバー犯罪条約の批准を目指した動きがあれば、貴重な情報となる。

次に脆弱性を有するシステムの法的問題に移る。この場合、かかる脆弱性を有するシステムをめぐる法的責任問題が注目される。この法的問題には、そのシステム自体に生じる損害の問題と脆弱性をもとに第三者に損害を与えた場合の問題とが存在するものと思われる。そして、それぞれに脆弱性を有するソフトウエアの作成者の責任、システムの納入業者の責任、システム管理者の責任の問題がある。そして、実際に不正に侵入したものの責任、その侵入を援助したものの責任、被害のさらなる拡大を防ぐべき義務について、法的にどのような位置づけがなされるかという問題がある。そして、当然、セキュリティの観点からは、一定の監査がなされ、それを基にシステムの脆弱性についての評価・招請が施されることになろう。そのような手法は、かかる責任問題に影響を与えるかという点も議論されなければならない。

上述の論点において、脆弱性の修正において、さらに法的に検討すべき事項がある場合は、その点についての調査が必要になる。特にＳＱＬスラマー事件においては、いわゆるバグ・フィックスをあてていなかったことが被害拡大につながったとの報道がなされており、かかる観点から何らかの動きがある場合には、報告がなされる必要がある。

2.2 責任ある開示の問題

次に、脆弱性をめぐっては、それに関する情報を具体的にはどのような形で開示することが適切であるのかという、「責任ある開示」に関する論点がある。この点については、従来は、ソフトウエアの脆弱性の問題については、議論はあったものの、万人に公開されるべきであるとするいわゆる完全開示原則というものが適用されていた。これは、（１）不正アクセスをする者は、脆弱性に関する情報をすでに知っており、彼らがなしうる手法をすべての人が知りうるのが最善である（２）ベンダー

は、ひとたび脆弱性情報を公開されれば自らのバグを隠すことはできない（３）脆弱性情報は、将来におけるよりよいシステムをつくるために公開することが必要である、などを根拠とする。しかしながら、（１）脆弱性の大多数は、それによって脆弱性を解消するという目的のためよりは、自己の力量の顕示などの公開すること自体が目的であるという動機によって導かれて調査され、公開されるのである（２）欠点を公開する効果的な他の方法がある（３）より良いシステムを作るためといっても脆弱性情報の詳細を教えたりテストしたりする必要はないのではないか、という観点から、脆弱性の発見者が、一定の責任ある開示のシステムに従うべき枠組みを準備する必要があるのではないかという点が議論されつつあるのである。この論点は、「責任ある開示の問題」ということができるであろう。一定の責任ある開示システムについてどのような枠組みが提案され、実行に移されているかということが調査されなければならない。

なお、この具体的な議論については、別紙「ソフトウエアの脆弱性をめぐる法律問題」として報告する。

第３章　質問と回答

回答の詳細については、「付録Ｂ　各国報告書日本語訳」の各国回答全文を参照されたい。

3.1　定義(Definition)
3.1.1.　脆弱性を議論するにあたって、「ソフトウエア」の定義が法にありますか。
3.1.2.　「セキュリティホール」「脆弱性」「不具合」について法令等で定義をしていますか。
3.1.3　「セキュリティホール」という用語が法令等で使用されていませんか。

［質問の位置づけ］
3.1.1 について
ソフトウエアに起因するネットワークの脆弱性についてその法律問題を検討する際に、まず、最初にソフトウエアの定義について法的にどのように取り扱われているかを検討する必要がある。
ちなみにこの点についての日本法を参照する際には、製造物責任法をめぐる議論[2]が参考になる。この点について、製造物責任法において、「製造物」とは、製造または加工された動産に限られる（２条１項）から、不動産、サービス、ソフトウエア、無形エネルギー等は、製造物責任法の対象にならない。但し、欠陥あるソフトウエアが機械に組み込まれて製造販売された場合には、当該機械自体の欠陥としてソフトウエアが適用になりうる[3]と解されている。したがって、この見解からすれば、ファームウエア自体も、脆弱性に関する責任の議論対象となることとなり本調査でいうソフトウエアの範囲に含まれることになろう。
各国において、ソフトウエアの定義がなされているか、またなされている場合に、どの程度の広がりがあるか、ハードウエアと一体になったソフトウエアについてどう考えられているかなどについての報告をなすことが求められ、この点の比較は、議論の契機として興味深いものとなるだろう。
また、ソフトウエアの提供形態が、有体物として一体化した提供とライセンスによる提供があるであろうし、後者においても売買や請負による成果物という形での提供が考えられる。それらの形態によって、どのように法的な位置づけがなされているかという点も、その脆弱性についての考察を開始するのにあたって事前に調査しておく必要がある。

3.1.2 および 3.1.3 について

3.1.2 は法令等での定義とかかる用語が実際に使用されているかどうかの両面からの質問ということになる。
日本法のもとにおいては、「セキュリティホール」「脆弱性」「不具合」などの用語が、法令で用いられているということはない。判決例からいくと、コンピュータソフトウエアの欠陥についての判断をなしたものがいくつか報告されている[4]ところである。これらの判決例は、開発委託契約等による

[2] 製造物責任法に関する一般的な解説書の他に、　財団法人比較法研究センター「情報産業と製造物責任に関する調査研究」（財団法人産業研究所、1992）15 頁、同「コンピュータ・ソフトウエアをめぐるリスクと民事責任に関する調査研究」（財団法人産業研究所、1994）51 頁など。
[3] 前出「コンピュータ・ソフトウエアをめぐるリスクと民事責任に関する調査研究」6 頁
[4] 財団法人比較法研究センター「ソフトウエアの不具合・バグ・瑕疵に関する調査研究」（財団法人産業研究所、1995）84 頁に松本恒雄「ソフトの瑕疵についての日本の裁判例の分析」がある。そこにあげられている判決以降のものとして、那覇地判平成 12 年 5 月 10 日（コンピュータソフトウエアの開発委託契約において、作成されたソフトウエアに欠陥があるとは認められないとして、同契約

問題を取り扱ったものが多いが、判決文のなかで、「欠陥」という用語が用いられているのが一般である。

［各国の回答］３．１．１

ソフトウエアの定義については、脆弱性と関連した文脈で定めているものは見受けられなかった。その文脈以外では、法律に定義を定めているもの（知的財産権の文脈での定義を除く）としては、アメリカ合衆国、大韓民国（以下、韓国という）から具体例が報告されている。

アメリカ合衆国は、コンピュータソフトウエアレンタル修正法１０１条（17 U.S.C. § 101）で、「コンピュータにおいて特定の結果をもたらす直接的または間接的な記述または指令のセット」と定め、また、連邦高裁判決（U.S. v. Seidlitz, 589 F.2d 152 (4 th Cir1978)）では、「指令により一定のことをなすマシーンにロードされた論理および指令をいう」と判示している。なお、統一コンピュータ情報取引法は、ソフトウエアという用語を意図的に避け、代わりにコンピュータ情報という用語を用いている。

韓国は、ソフトウエア産業振興法第２条第1号において「『ソフトウエア』というのはコンピュータ・通信・自動化などの装備とその周辺装置に対して、命令・制御・入力・処理・保存・出力・相互作用が可能になるようにする指示・命令（音声または映像情報などを含む）の集合と、これを作成するために使用された技術書その他関連資料をいう。」と定めている。

また、ドイツにおいては、「DIN/ISO規格9000、第3部の定義（ソフトウエアの開発、提供および保守に対するISO9001の適用のための便覧（1992年））」において、「ソフトウエア：情報処理プログラムによる作業に属する、プログラム、プロセスならびにそれに属するすべての仕様書から構成される精神的製品[5]（No. 3.109）ソフトウエア製品：ユーザに提供するよう決められているコンピュータプログラム、プロセスならびにこれに属する仕様書およびデータ一式全て」と定められている。

一方、これ対して、連合王国（以下、便宜上、英国という）においては、消費者保護法1987の解釈との関係で、物理的媒体によって提供されるソフトウエアに「製品（goods）」という規定の適用があるかについては、現在でも、議論があるとされている。

なお、コンピュータプログラムについては、著作権との関係で規定している国が多い。

［各国の回答］３．１．２および３．１．３

セキュリティホールの定義については、法律によって定義なされている国は、報告されていない。

「セキュリティホール」「脆弱性」の用語の使用という点については、韓国は、「脆弱点」（即ち、韓国法で使用している脆弱点という用語は、「security hole」と同じ意味と判断されている）という用語を「情報通信基盤保護法」（２００２年１２月１８日一部改正）とその施行令で使用し、また、「情報通信サービス情報保護指針」第８条（「情報通信網利用促進ならびに情報保護に関する法律」に基づく）において「保安脆弱点」という用語を使用されている。それ以外の国では、かかる用語が法令等で使用されているという報告はなかった。

なお、消費者保護の文脈において製造物責任法などの文脈で、「欠陥」という用語が用いられている国は多い。英国では、「製品の安全性が、人が、一般に備えていると期待するものでない場合をいう」と定めている。ドイツでは、不具合の中に瑕疵と欠陥があるといえる。製造物責任法第３条で、「欠陥(Fehler)」の定義を有しているが、定義された欠陥以外の不具合についても、瑕疵担保責任に

の解除が認められなかった)、広島地判平成 11 年 10 月 27 日（基幹業務システムコンピュータのソフト製作の欠陥を原因とする損害賠償請求訴訟において、ソフトの製作請負もしくは製造販売契約に基づいた債務不履行責任が認められた）など。

[5] 精神的製品: ドイツ語の geistige produkt を直訳した。意味としては、精神的産物あるいは精神活動の所産ということになる。

おける「瑕疵」の概念を場合により適用できると考えられている。さらにドイツでは、DIN6627 がソフトウエアの不具合についての判断を扱っている。

3.2.1 一般的フレームワーク (General frame work)

情報セキュリティ脆弱性もしくは不具合からの責任について、定義や責任が定められていますか。
もし、必要であれば、請求原因を不法行為、制定法、契約法に分けることもかまいません。民事上の責任について詳細に記述してください。ただし、脆弱性の濫用に対しての刑事的責任および行政的手法についても概観をしてください。

［質問の位置づけ］

本調査の基本的なテーマはソフトウエアの脆弱性に関して、ネットワークに関連する当事者の責任をめぐる規範及び行動規範を明らかにしようとするものである。この目的のために、その責任の基本的な枠組みについて明らかになすことを求めることとなる。

この位置づけとしては民事上の位置づけおよび刑事上の位置づけが考えられる。民事上の位置づけとしては損害賠償における評価の基準の有無程度であろうと推測されるが、各国においてどのような位置づけがなされているか興味深いところである。一方、刑事的な位置づけとしては、本稿の目的から直接的には離れてしまうので、サイバー犯罪条約の批准に向けた各国の動き（なおサイバー犯罪条約は第 1 章においてコンピュータのセキュリティに対する侵害についての実定法の整備を各締結国に求めている）についての基礎的な情報収集することを目的とする。

我が国の法律に関して本調査の主題についての分析の基本的な枠組みを指摘したものは存在しないものと考えられるが、バグについて、（1）ハードウエア・ソフトウエア・システムの瑕疵（2）サービスの瑕疵（3）客観的瑕疵（4）主観的瑕疵（5）ソフトウエアの不完全履行（6）事業者の附随義務違反(7)製造物責任法における欠陥などの論点から検討されるという指摘がある(脚注４、「ソフトウエアの不具合・バグ・瑕疵に関する調査研究」２頁)。法的には、契約責任、製造物責任、不法行為の判断枠組で判断がなされるものと思われる。

［各国の回答］３．２．１

情報セキュリティに関する脆弱性や不具合からの責任についての一般的な枠組みという点については、刑事的責任、民事的責任という観点から回答を得た。

刑事的責任については、すべての国において脆弱性を利用する行為について一定の刑事的責任を認める立法例 がある。個別の分野について、例えばデータ保護、製品の安全、ヘルスケア等に関する分野などにおいては一定の行為の形態について刑事責任を問うものがあることが指摘されている(英国)。また、この点については、いわゆる重要インフラに対する防衛という観点からそれらに対する攻撃について特に重く処罰するとかセキュリティの維持について過失があったものについて過料を課すといった規定（韓国）が注目される。また、データ保護の観点からは、直接に刑事的な処理を規定している例（フランス）も注目されるところである。

民事的責任については、契約責任と不法行為、そして契約責任の第三者に対する拡張、製造物責任法の議論などの下で論じられているのが一般である。もっとも、このような一般的な分析をもとに、安全性の問題が関係するとする立法例（英国）もあるし。個別の分野について重い責任を負担させるという立法例（特に医療関係などについては、多数）もある。

以下の責任についての論点を考慮にいれて報告ください。

(a) ソフトウエアまたはハードウエアに欠陥があった製造者、開発者の責任
(b) 「下流責任」(情報セキュリティ侵害攻撃を停止するのに失敗した最初の被害者の責任、すなわち、そのシステムが他者のシステムを攻撃するのに利用された責任-公開されたパッチを宛てるのを怠った責任や公知の脆弱性に対応するのを怠った責任)
(c) システムにおける脆弱性を発見するために効果的な監査を怠った際の責任

［質問の位置づけ］

（a）について

そもそもソフトウエアの提供形態が、法的にどのように位置づけられるかという点が問題である。

わが国においては、前述したように、有体物と一体化している場合においては、その有体物についての売買と考えられるであろうし、それ以外には、ライセンス契約で提供がなされている場合においては、売買、請負の成果物として位置づけられるものと考えられる。その際には、契約当事者間の問題であるが、売買、請負の契約問題としては、その不具合等については、その契約関係の問題として取り扱われる。本検討においては、第三者との関係が問題となるので、一般の不法行為としての取扱になるのが一般であるように思えた。製造物責任法の適用が有るのは、以下のような限定された場合ということになる。製造物責任法は、「製造業者等」が、３条規定の「製造、加工、輸入、氏名等の表示」をして引き渡した同法２条１項規定の「製造物」に存在した『欠陥』により、他人の生命、身体または財産を侵害したとき（但し、当該製造物について損害が生じただけで、拡大損害が生じなかったときを除く）に適用される（同法３条)。ここで、『欠陥』とは、講学上、製造物の欠陥は、製造上の欠陥、設計上の欠陥、および表示（指示・警告）上の欠陥に分類される。そのうち、製造上の欠陥については、標準逸脱基準（設計書・仕様書による標準からの逸脱の有無で欠陥の有無を判断する）によるべきとされ、設計上の欠陥、および表示上の欠陥については、消費者期待基準（通常の消費者が期待する安全性を有するか否かで、欠陥を判断する)、あるいは、危険効用基準（製品のもつ効用が危険を上回るか否かで、欠陥の有無を判断する）によるとされている。

本文は、このような製造物責任法の射程について、各国の法制度や対応を比較しようという趣旨である。

（b）について

脆弱性を用いた攻撃のなかで最も一般的な方法としては、あるサイトに侵入し、その管理者権限を取得してしまい､その管理者権限を用いて､さらに新たな攻撃を行うという方法があげられる｡そこで、問題になるのは、侵入されるサイトが、一般に必要とされる注意義務を怠っているような場合に、第三者に対して責任を負うかという問題である。

我が国においては、第三者に対する責任の有無という問題になるので、不法行為の問題となるものと思われる。

（c）について

セキュリティを保ったシステムのためには、セキュリティポリシーの立案・実装・監査のサイクルが、有効なものであることは、一般的な理解を得ているが、果たして、そのような監査を怠ったのに義務懈怠があるような場合に、何らかの責任が発生し得るのであるかという点が問題になる。

我が国においては、いわゆる「情報提供者の責任」についての議論がある[6]ので、そこでの議論が参考になろう。法的な議論としては、相当因果関係の範囲と注意義務の範囲の問題と思われる。

［各国の回答］

これらの点については、以下の回答で詳述されることとなる。むしろ、各国の回答のなかで、（a）

[6] 岡　孝「情報提供者の責任」現代契約法体系第７巻（有斐閣、昭和 59 年）306 頁以下

については、契約関係について、第三者への効果の拡大や契約の連鎖という概念から、英国、米国において、契約関係の果たす役割が大きいことが特筆されよう。また、韓国においてＳＱＬスラマー事件が引き起こした損害についてマイクロソフト社が訴訟に巻き込まれていることが判明した。この資料の分析は、今後の課題となるが非常に参考となる事案ということが言えるであろう。

3.2.2：セキュリティ－法的責任の要素 (Elements of security legal liability)

情報セキュリティ、機密性、正確性、可用性と法的責任には、どのような関係がありますか。

［質問の位置づけ］

一般に法的には、損害(damage)として、考慮されるが、一方で、セキュリティの用語においては、データを漏えい取得されたことなどによる機密性（confidentiality）に対する脅威、データの破損されたことなどによる正確性(integrity)に対する脅威、一定の侵害に対して防衛のために停止したことなどによる可用性(availability)に対する脅威などの観点から考察されることになる。そうだとすると、セキュリティに対する侵害があったとしても損害としては評価されない場合もあるであろう。また、逆に従来の損害や権利侵害という概念で包含しきれないセキュリティ自体に対する侵害をあらたな法益侵害と認識していることがあるかもしれない。この点について回答を求めるものである。

我が国においては、セキュリティ侵害と法的な評価が直接に関連するものではないと認識されている。これに関連して、例えば、機密性の侵害（情報が漏洩されてしまうこと）に関して、宇治市住民基本台帳データ不正漏洩事件の判決例（大阪高判・平成 13 年 12 月 25 日）が注目される。データの経済的価値という問題[7]については、フロッピーディスク紛失事件（神戸地判・平成 2 年 7 月２４日判例時報 1381 号 81 頁）がある。また、個人情報の漏洩がなされていても、それが情報主体に通知されなかったという事件[8]もあり、これらに対する各国の対応は、興味深いところである。

［各国の回答］３．２．２

この点については、出題者の意図がうまく伝わらなかったものといえよう。もっとも、セキュリティ自体が一定の保護されるべき法益として認識されていること、そのうちで、重要インフラや特定の分野についてのセキュリティは、さらに一定の対応が図られていることについては注目に値する。また、米国において、具体的な立法例として、健康保険分野（Health Insurance Portability and Accountably Act (HIPAA)）、金融機関分野（Financial Modernization Act of 1999, also known as the “Gramm-Leach-Bliley Act ”）などにおいて特定の規制があることは注目に値する。

また、情報の漏洩を純粋に問題として捕える立場としては、カリフォルニアの上院法案 1386 とカリフォルニア民法典第 1798.85 条がある。前者の法案は、2003 年７月１日から発効しているが、顧客の情報が、危険にさらされた場合に、顧客に対して、通知をしなければならないというものである[9]。その理としては、顧客に「アイデンティティ窃盗（identity theft）」の可能性を知らせ、対応する機会を与えるべきであるという判断である。また、さらにかかる法案に対応するものが、連邦において、提案されている。後者は、カリフォルニアにおいて、社会保障番号自体を、「安全」な方法で「暗号化」しないで送信することを禁じるものである。この効果としては、刑事的な処罰とは、関連しないが、「それ自体ネグリジェンス」と認識されることになる。

---

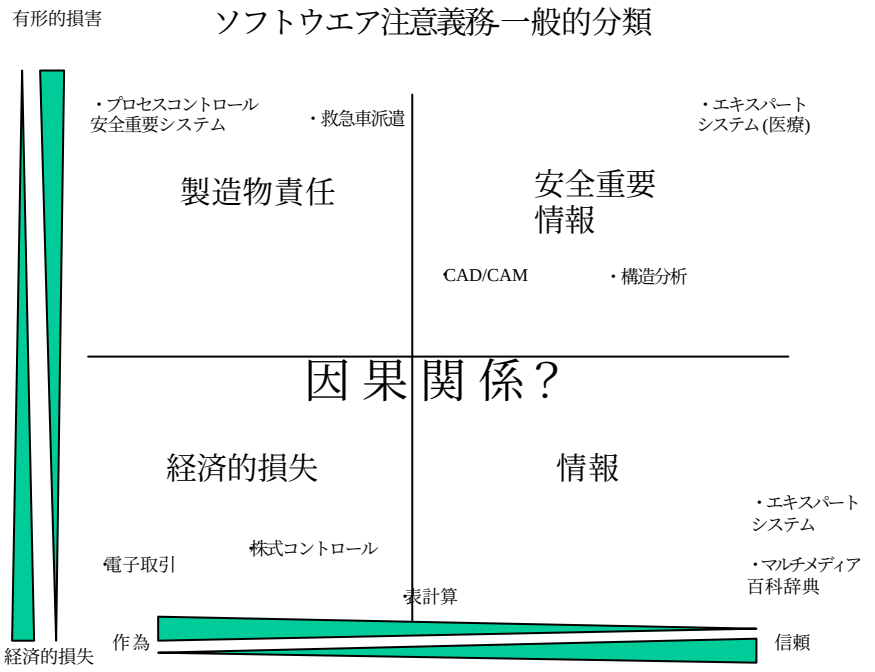
[7] 前出「コンピュータ・ソフトウエアをめぐるリスクと民事責任に関する調査研究」86 頁

[8] 百貨店の危ない無線 POS，クレジットカード情報が見えた」――対策は 2003 年 1 月末に完了――（http://itpro.nikkeibp.co.jp/free/NBY/NEWS/20030221/1/）

[9] 但し、法執行機関が、刑事捜査に影響があるとする場合には、通知を延期させることができるとする。

その上、英国においては、「有形的損害」と「経済的損失（エコノミック・ロス）[10]」の縦軸に、「作為」と「信頼性」を横軸にして、情報に関する損害が「製造物責任」「安全重要情報」「経済的損失」「情報」の四つに分類できること（図１）が示唆されている。この分類に法的な注意義務の範囲と程度がリンクされており、示唆に富むものといえるであろう。（いわゆる純粋な経済的損失が、損害賠償として、賠償の対象にならないのは、米国においても同様である）

図１



Encyclopedia of Information Technology Law（Sweet & Maxwell）７０１２より

[10] 「うべかりし利益」に該当する

3.2.3 主体的側面 (Subjective aspect)

情報セキュリティに対する侵害があった場合に、被害者から責任を追求され得る当事者についてあげて下さい。
具体的に以下の例について記述して下さい。

- 脆弱性に対して攻撃するソフトウエアを開発し、意識的に配布する者
- 脆弱性の存在するハードウエアまたはソフトウエアの製造業者または開発者
- コンサルタント、システムインテグレーター、配布者、販売業者、その他脆弱性有る技術を推奨したベンダー
- セキュリティの評価やセキュリティ脆弱性の回避を委任されたコンサルタント
- 脆弱性を発見する監査人
- 攻撃を抑止するように依頼していたセキュリティ・プロバイダー
- アプリケーションを最新に、パッチを宛ててもらうことにしているアプリケーション・サービスプロバイダー
- システムをアウトソースしている場合のホスティング会社
- 攻撃を許容し、または、停止し得なかったISP
- 脆弱性を発見していながら、それを被害者、ベンダーまたは公に報告しなかった者

［質問の位置づけ］

この点については、基本的フレームワークでの報告をさらに敷衍し、個別の事案について解説を求めようとするものである。

我が国においては、いまだ具体的な検討は、なされていない論点ということができるものと思われる。

［各国の回答］３．２．３

刑事責任であるが、脆弱性に対して攻撃するソフトウエアを開発し、意識的に配布する者に対しては、対象物が重要インフラに属する場合、そのような犯罪として重罰化されている立法例がある（米国、韓国）ことには注意がなされるべきである。具体的に韓国では、「それが重要情報通信基盤施設を撹乱、麻痺または破壊する結果をもたらす場合には情報通信基盤保護法上の処罰規定に抵触し、それに従った重い処罰を受けることになる。」と報告されている。

脆弱性の存在するハードウエアの問題については、それが仮にそのハードウエア内のソフトウエアの問題であるとしても、製造物責任の問題として、議論されるのが一般である。記録媒体の保存されたソフトウエアについては、製造物責任の適用について、各国で議論がある状況である。また、上述した韓国のＳＱＬスラマー事件のほかに、フランスにおいて雑誌の付録でコンピューターウイルスをディスクの形で配布した場合、このディスク配布者に民事責任が課せられ、この例においては過失相殺の適用がないという判決が報告されており、注目される。

コンサルタント、システムインテグレーター、配布者、販売業者、その他ベンダー等については、契約関係によって基本的に規制されることは、各国同様である。もっとも、その契約の解釈の問題としては、手段債務であるなどの理由をもって責任を認められるということはほとんどないだろうということが報告されている。なお、各国の法制により、製造業者、販売業者などの定義が異なることが指摘されている。ドイツにおいては、製造物責任法 4 条 3 項により、供給者を製造物責任法による製造業者とみなすという規定や OEM 販売業者自体が、責任を負担するという規定も存在している。

また、第三者に発生した結果については、さらに注意義務の問題となるが、責任が肯定される可能性はあまり積極的には報告されていない。

セキュリティの評価やセキュリティ脆弱性の回避を委任されたコンサルタントについても同様である。ドイツにおいては、2001 年 7 月 18 日のハンブルクラント裁判所の判決において、データメディアをウィルス発生について検査することを契約によって引受けた会社は、検査の際に、最新ではない検査プログラムを使用することによってウィルスを見逃した場合、発生した損害について責任を負うという判決がある。また、韓国におけるＳＱＬスラマーに関連して提起された訴訟では、韓国（情報通信部）が共同被告のひとりになっており、これは、重要情報基盤施設を管理する機関の長（この事件では情報通信部長官）が、この基盤施設の脆弱性を分析し、回避するための措置をとる法令上の包括的義務を負担しているという点を前提としている。この事件では、原告が勝訴するためには、情報通信部が実際の法令上の注意義務に違反していたということと、それが被害者たちの損害との間に相当因果関係があるということを主張、立証しなければならないが、成り行きが注目される。

監査人、セキュリティ・プロバイダー、アプリケーション・プロバイダー等については、契約責任についての追及の可能性は存在するであろう、ただし第三者に対する契約責任という観点は認められないだろうという報告が一般になされている。具体的な規定がなされているのは、ドイツで、サービス・プロバイダが具体的な法侵害を理由とする指摘、あるいは、警告を受け取った場合は、積極的な認識をもったこの時点から、テレサービス法 11 条により、プロバイダは、認識がある場合、遅滞なく活動しなければならないとされている一方で、契約の相手方が適法に行動することを前提にすることが許されなければならないとされている。また、米国においては、マネッジド・セキュリティ・プロバイダー（Managed Security Providers、以後単に MSP と記す）という業務を担う企業が発生している点、そして、かれらは、依頼者との間で、契約によってリスクを負担し、移転していることが報告されている。また、韓国では第三者への責任も負うのではないかという議論がなされている。

システムをアウトソースしている場合のホスティング会社については、そもそも、ＥＵにおけるデータ保護指令の規定との関係で、そのホスティング契約自体が、
「(a) 処理は、
(i) 書面により、作成されるか、または、証拠化される、
(ii) そして、その契約においてデータ処理者がデータ管理者からの指示だけに従って行動することになっており、
そして、
(b) 英国データ保護法 1998 における第７原則によってデータ管理者に対して課せられるのと同等の義務に応ずることを、データ処理者に対して要求する契約であること」
と定められている点に注意が必要である。また、フランスの立法例において、個人情報保護についてのホスティング会社は民事・刑事ともに責任を負うという点が注目される。

攻撃を停止しえなかったＩＳＰについては、韓国の法制においてサーバの賃貸を業としているＩＤＣセンターに対して保護措置の義務というのが明示されているという点が注目に値する。具体的には、「情報通信網利用促進ならびに情報保護に関する法律」第４６条により「①他人に情報通信サービスを提供するために集積された情報通信施設を運営、管理する事業者は、情報通信施設の安全な運営のために、情報通信部令が定めるところにより、保護措置をとらなければならない。②第１項の規定による事業者は、集積された情報通信施設の滅失、毀損、その他運営の傷害によって発生した被害を補償するために、情報通信部令が定めたところに従い、保険に加入しなければならない。③情報通信部長官は、第１項の規定による保護措置をとらない事業者に対し、相当な期間を定め、是正措置を命ずることができる。」とされ、保護措置の不履行による損害について責任を負うことが明らかになっている。

また、英国では、各プロバイダの防御における協力の合理的要請について、電気通信規則 1999 第２８条において「電気通信サービス・プロバイダは、関連した電気通信ネットワークのプロバイダに対して合理的要請をなし、そのプロバイダは、その要請に対して応じなければならないとともに、必要な措置をとる」と定めている点は、興味深い。

脆弱性を発見していながら、それを被害者、ベンダーまたは公に報告しなかった者の責任については、一般論としては、特に報告がされていない。韓国においては、「契約上、明示的にあるいは黙示的に、報告義務を負っている場合には、契約上、法令または条理上の報告義務が認定される場合には債務不履行責任を負うことになる場合がある。」と報告されている。

電気通信分野においては、EU 指令の第４条において、「2. ネットワークのセキュリティが破られる特定のリスクがある場合には、公的に利用可能な電気通信・サービスのプロバイダは、そのリスクについて、加入者に知らせなければならず、そのリスクが、サービス・プロバイダによってとられた措置の範囲の外にある場合には、可能な救済策について、かかりそうな経費をも示して加入者に知らせなければならない。」とされている点について注目が必要である（フランス、英国からの報告）。同じく電気通信分野であるが、韓国では、「情報通信基盤保護法では、情報保護コンサルティング専門企業に対して、一定の保護義務ならびに記録保存などの義務を賦課している（同法、第２２条、第２３条など参照）。情報保護コンサルティング専門企業がこうした法令上の義務に違反したことが侵害事故の原因である場合には、不法行為などの責任を負う場合があり得る。」とされている。

また、通知という観点からするとき、米国においては、前述のようにカリフォルニアの上院法案 1386 において、顧客の情報が、危険にさらされた場合に、顧客に対して、通知をしなければならないということを定めているのは興味深い。

3.2.4 脆弱性の提供方法 （ manner of providing software ）

以下のような脆弱性の発生個所によって、責任を問われる人が異なりますか？
- クライアント側
- サーバ側
- ネットワーク機器部分
- など

以下のようなソフトウエアの提供形態によって、責任の違いを区別しているかを解説してください。
- パッケージ品ソフトウエア（市販品）
- 個別開発品ソフトウエア
  - 外注（成果物検収 Deliverable）
  - 委託（工数検収 Labor hour）
- サービス提供に利用しているソフトウエア
- など

［質問の位置づけ］

英国においては、消費者保護法の適用に際して、ソフトウエアの提供方法によって法律の適用関係が異なってくることが知られている。また、我が国においても、製造物責任法の適用において、製品にソフトウエアが用いられていれば、その瑕疵は、製造物責任法の射程で議論されることは、明らかになっているとおりである。

本質問は、そのような観点から、各国の法制において、ソフトウエアの提供方法が責任論に与える影響を質問しようとするものである。

［各国の回答］３．２．４

この点については、むしろ、このような議論がなされているのが、英国程度しか見当たらないという回答であった。ちなみに、その英国の法的な構造は、マス・マーケットでのソフトウエアであるの

か、量の少ない、もしくは、注文制の製品であるのかで、異なる可能性があるというものである。英国においては、情報に対する信頼については、特別の技能を信頼したなどという特段の事情がない限り、損害賠償を負うことはないとされているので、マス・マーケットの製品については、損害賠償が極めて困難になってくるのである。

3.2.5 注意義務-標準 (Duty of care-standard)

3.2.5.1 一般(general)

法によって情報セキュリティの基準が定義されていますか。
脆弱性の改善義務についての基準を法令等で設けているか？
法令等以外の情報も知っていれば教えてください。

［質問の位置づけ］

法的な注意義務として、情報セキュリティの遵守のために、一定の基準の遵守が求められることになると思われるが、本質問においては、各国において、かかる基準の存否を法的なもの、実務的なものあわせて質問しようという趣旨である。とくに、業界ごとの基準は、有意義な情報となるであろう。

［各国の回答］３．２．５

各国において、法律によって基準が定義・制定されているというのは、報告されなかった。ただ、フランスにおいて、個人情報がセキュリティの欠陥の修復なしにアクセス可能とされている場合、おそらく刑法２２６－１７上の定義するセキュリティ義務違反となるとされている。

法律と、セキュリティの維持という観点からすると、韓国においては、一般的な規定がおかれているとの報告があった。この内容は、情報通信網利用促進ならびに情報保護に関する法律第５２条第１項において、「政府は情報の安全な流通のため、情報保護に必要な施策を効率的に推進するために、韓国情報保護振興院（KISA）を設立する。」と規定し、同条第３項において、KISA の業務を規定し、その中の一つに、＜情報保護システムの性能と信頼度に関する基準制定ならびに標準化支援＞を揚げる（同項第５号）ものである。また、上記、法第４７条第１項は、「情報通信サービス提供者および情報通信サービスを提供するために物理的施設を提供する者は、情報通信網の安定性および情報の信頼性を確保するために樹立運営している技術的・物理的保護処置を含む総合的管理体系（以下、「情報保護管理体系」と呼ぶ）が、当該サービスに適合するか否かに関して、第５２条の規定による韓国情報保護振興院から認証を受けることができる。」と規定し、情報保護管理体系認証制度を設けている（２００１．７．１．施行）ものである。これらの規定により、韓国では、KISA の主導で情報保護に関する標準の制定ならびに認証業務を遂行しており、具体的に、基準自体を制定するものではないが、その基準制定の根拠規定を置くものであって注目に値する。

また、各国ともに、同様の制度は、準備されており、ドイツでは、政府機関である BSI の「情報技術のシステムのセキュリティ監査に関する基準」があり、また、連邦データ保護法(BDSG)9 条が個人情報について規定している。契約上の義務については判例があるという。

特定の分野におけるセキュリティ基準の法定という観点では、アメリカの動向がきわめて注目される。ここで、注目されるのは、医療関係の分野および金融情報の分野である。医療関係については、Health Insurance Portability and Accountability Act (HIPAA)がある。これは、健康保険会社、ヘルスケアプロバイダ、ヘルスケアクリアリングハウスを対象企業として、対象企業は、（A） 情報の正確性、機密性を確保する（B）情報のセキュリティ、正確性に対する脅威・危険、および無権限の利用・開示から、保護する（C）経営者と従業員とで遵守するために経営的、技術的、物理的な安全策を採用しなければならないと定められている（42 U.S.C. § 1320d-2(d)(2)）。この法律のもと Department of Health and Human Services (DHHS)が、標準を採用している。そして、この規定に対する遵守がなされない場合について、DHHS は、民事上のペナルティを課すことができ、また、政府は、HIPAA 違反をしりながら、犯すものに対しては、刑事上の手続をなすことがでる。金融情報の

分野における法律は、The Financial Modernization Act of 1999, または、“Gramm-Leach-Bliley Act”（以下、GLBA ともいう）として知られる法律である。GLBA は、「金融機関」が「その顧客のプライバシーを尊重し、非公開の個人情報のセキュリティと機密性を保護するように継続的な義務を課す」というものである。この法律を実装するために、種々の規制がなされているが、それらの規制は、要するに合理的に予測できる脅威から、記録のセキュリティを保護するということである。また、アメリカでは、一連の公開会社による会計の不祥事を受けて、公開会社における監査の分野において、Sarbanes-Oxley Act37 が制定されたことは、注目される。この法律は、複雑で、多岐にわたるが、現地の調査によれば、以下の３点で、情報セキュリティとの関連性があると考えられる。第１は、１０３条において、公開会社会計監視委員会が、監査人に対して、関連する資料とともにすべての書類を７年間保管することを義務づけていること、第２には、ＳＥＣ規則において、金融顧客については、データを保存することを義務づけており、政府機関に対しては、「変更不可のメディア」で電子メールを７年間保存することを義務づけていること、第３には、４０４条において、正確な「会計報告」をなすために、執行役員と経営陣は、「内部コントロール」および「手順」を実装することを要求していることである。この第３の条文について、学者は、情報セキュリティの体制が、構築されることが含意されていると解釈しており、公開会社の執行役員は、そうでない場合に、責任を負うと解されている。
また、英国では、電気通信（データ保護とプライバシー）規則がある。特にその第２８条は、
第１項において「電気通信サービス・プロバイダは、提供するサービスのセキュリティを確保するために適切な技術的かつ組織的な措置を第２項に従ってとらなければならない。」とし、
第２項において「電気通信サービス・プロバイダは、関連した電気通信ネットワークのプロバイダに対して合理的要請をなし、そのプロバイダは、その要請に対して応じなければならないとともに、第１項によって必要な措置をとる。」
と定めている。

各国において、BS7799 の適用をはじめとして、種々の標準が提唱されている。詳細については、各国の報告書を参照されたい。

3.2.5.2. 管理者の義務 (Duties of administrators)

システム管理者が、不具合を修正するためになすパッチやソフトウエアを使用することを怠った場合、責任があるか。
システム管理者がセキュリティ情報を収集するのを怠ったとき、責任があるか。

3.2.5.3 インシデントにおけるシステム管理者の義務（Duties of system administrators in case of incidents）

インシデントに対応する際、システム管理者は、不十分な対応しかできなかった場合、または、対応がおくれた場合、責任を負うか。

損害を回避する責任を負う当事者が他にいますか。

［質問の位置づけ］
これは、とくにＳＱＬスラマー事件において、その被害の拡大に際して、管理者が、不具合を修正するために、パッチやソフトウエアを使用することを怠ったのが、原因のおおきな一つではないかといわれているのに着目して、管理者の法的義務という観点から質問するものである。

［各国の回答］３．２．５．２

基本的には、システム管理者の注意義務が、誰に対して、どの程度負うかという問題である。この点については、契約上の責任が存在する場合、責任を負うという報告（ドイツ）、職責を適切に果た

していない場合、有責であるという報告（アメリカ）と第三者に対しては、責任を負う注意義務というのは、基本的には考えられないという報告（英国）があった。
特に情報通信分野に限ると、ＥＵ諸国においては、電気通信の指令第４条において、「公的に利用可能な電気通信サービスのプロバイダは、必要であるならば公的電気通信ネットワークのプロバイダとともにネットワークセキュリティに関して、そのサービスのセキュリティを保護するための適当な技術的かつ組織的な措置をとらなければならない。」という定めがなされている点は、かかる分野における義務を前提としているとも考えられる。また、韓国においては、「情報通信網利用促進ならびに情報保護に関する法律」第４５条第１項において、「情報通信サービス提供者は、情報通信サービスの提供に使用される情報通信網の安定性および情報の信頼性を確保するため保護処置を準備しなければならない。」と規定し、同条第２項は、「情報通信部長官は、第１項の規定による保護処置の具体的な内容を定めた情報通信サービスの情報保護に関する指針を定め、公示して、情報通信サービス提供者にその遵守を勧告することができる。」と規定している。この規定による情報通信サービスの情報保護指針が情報通信部により公示されていることが報告されている。その意味で、世界的には、電気通信サービスに携わる主体に対して、抽象的には、注意義務を課していると評価することも可能であるといえそうである。

［各国の回答］３．２．５．３

この点については、責任を負うことが考えられるという報告（ドイツ）、事案により MSP などの第三者に対してもインシデント・レスポンスにおいて協力すると契約で定められる場合には、責任を認められる余地があるという報告（アメリカ）と第三者に対しては、責任を負う注意義務というのは、基本的には考えられないという報告（英国）があった。ＥＵ諸国においては、電気通信の指令第４条（前述）において、他の電気通信プロバイダとの協力が前提とされており、かかる回避義務が念頭におかれているということもできよう。
また、韓国においては、情報通信サービス情報保護指針第８条第５項で「サービス提供会社により指定された情報保護責任者は、周期的にアクセス記録を分析して侵害事故を予防し、侵害事故を発見した場合には直ちに必要な処置を取らなければならない」と規定されている。これらの規定が第三者に対する損害賠償の根拠規定となることが報告されている。

3.2.5.4. セキュリティポリシー (Security policies)

1 注意義務の標準として、セキュリティポリシーを必要としていますか。
2 保険会社や産業界の事業者協会で、ガイドラインを標準としていることはないですか。
3 セキュリティポリシーの実際の運用が責任に対する抗弁になりますか。
セキュリティポリシーの実際の運用が連邦ガイドラインのようにコンプライアンスの観点から考えられていますか。
4　セキュリティ上の脆弱性が、セキュリティの監査および評価をしていながら、それを探知できなかった場合、その監査および評価をしていた事実は、抗弁となりえますか。

［質問の位置づけ］
セキュリティの確立のために人的システムを含むセキュリティポリシーの立案・実装・監査が、どのように責任論に影響するかを調査する趣旨である。

［各国の回答］３．２．５．４
３．２．５．４．１について

各国において、セキュリティポリシーが一般的に必要とされる。

法律上、一般的にセキュリティポリシーが位置づけられている国がある（ドイツ、韓国、フランス）。韓国では、注意義務の基準となる情報保護基準は必要なものと認識されており、「情報通信サービス情報保護指針」が制定されている。

また、アメリカでは、医療関係（HIPAA による）や金融機関（GLBA による）において、セキュリティポリシーを文書化することが義務づけられている点が、報告されている。

３．２．５．４．２について

保険会社や産業界の事業者協会で、ガイドラインを標準としているか、という点については、種々のガイドラインの存在が報告されている。ドイツにおいては、 BSI が、IT 安全性基準 http://www.bsi.de/zertifiz/itkrit/itkrit.htm や IT 基本保護ハンドブック http://www.bsi.de/gshb/deutsch/menue.htm その他、http://www.bsi.de/fachtem/sinet/index.htm が明らかにされているとしている。また、ヨーロッパのレベルでは「情報技術セキュリティ評価基準 ?ITSEC」がある。

米国では、NACHA（ National Automated Clearing House Association）やクレジットカード協会や会社の運営基準が、セキュリティの記述を定めている点が報告されている。

３．２．５．４．３について

各国において、セキュリティポリシーの運用自体が、それだけで責任を否定する事由になるという報告はなかった。しかしながら、注意義務を果たしたか否かという観点から、一定の評価がなされるというのも、同様であった。

３．２．５．４．４について

上の回答と同趣旨であるが、韓国においては、「情報通信サービス情報保護指針」第８条第４項において、「情報保護責任者は、周期的に情報システムの保安脆弱点を点検、分析して、その結果を情報通信サービス提供者に報告しなければならない。」と規定されているので、情報保護責任者が情報システムの保安脆弱点を周期的に点検、分析しているのであれば、これ自体が上記指針上の（注意）義務を遵守している部分であり、損害賠償請求訴訟において有力な抗弁事由の一つとなり得る」との指摘がなされている。

3.2.6 その他（Miscellaneous）

1　セキュリティ・インシデントの実体を明らかにするのに有効だと考えられる法的システムはありますか

2　「内部告発者保護」や「司法取引」の法制度を有していますか。

3 「内部告発者保護」や「司法取引」の法制度が、セキュリティ・インシデントの実体を明らかにするのに有効と考えられるのではないかという議論はありませんか。

［質問の位置づけ］

委員会において、いわゆる Trusted OS において提案が採用されている「デュアル・ロック認証」と法的制度の背景についての議論がでた。この「デュアル・ロック認証」とは、管理者は、管理権限のみを有するというものであって、これは、情報のいろいろな側面をシステム管理者の権限と ISSO（情報セキュリティシステムオフィサー）とにわけて保有させようとするものである。従って、情報は、その保有当事者、システム管理者、ISSO にわけて有されることになり、もし，その情報の濫用を図ろうとすれば、その３当事者のうち２名が謀議をはからないとなしえないという構造になっているものである。もし、このような「デュアル・ロック認証」がシステムにおいて採用されれば、犯罪の嫌疑がある際に、司法取引や公益通報制度が採用されている司法システムのもとでは、犯罪等の全貌を

明らかにすることができ、それはシステムのセキュリティ防衛のために重要な要素になりうるものと考えたのである。

そこで委員会としては、基礎的な情報として、かかる司法取引制度や公益通報者保護制度の採用の有無を各国に質問するものとして、さらに、かかる制度とセキュリティとの関連についての議論の進行状況について聞くことにしたものである。

［各国の回答］３．２．６

３．２．６．１について

セキュリティ・インシデントの実体を明らかにするのに有効だと考えられる法的システムという質問について、具体的な指摘での回答は、困難であった。なお、韓国においては、SQL-Slummer 事件が発生した後、情報通信部など政府機関の立場からは、事故の実態を素早く把握するため、ISP が持っているログ資料などの提出を要求する権利を認める方向の立法を推進すると話しがもちあがり、これに対してプライバシー侵害を警戒する市民団体の強い反対意見が提起されたことがあるとのことである。

［各国の回答］３．２．６．２

内部告発者保護の制度についていえば、これに該当する制度を有しているのは、米国、英国（公共の関心公表法 1998 による）である。韓国においては、内部告発者保護については、韓国の政府（財政経済部）や法務部において、一定の内部告発者保護制度の導入を検討中とのことである。
司法取引については、これに直接該当する制度を有しているのは、米国のみである。一方、ドイツにおいては、関連するものがあるとの報告であった。

［各国の回答］３．２．６．３
この点については、具体的な議論は、報告されなかったが、調査委員会としては、Trusted OS の構築に際して、かかる議論が関与していることを把握しており、各国において、比較法的な検討と情報セキュリティについての制度設計が、なかなか意識して議論されにくいことを示しているということもできよう。

3.3 責任有る開示の問題（Responsible disclosure issue）

1. 脆弱性に気がついたとき、気がついた人間は、会社や公的機関に報告すべき義務がありますか
2. 報告された会社などは、これに対して対応すべき義務はありますか。また、対応をなしうる体制をとっておく義務があると解されていますか。
3. 産業界や政府の機関が、脆弱性がわかった際に、それに対して責任有る開示となるようなガイドラインを準備していますか。もし、準備しているならば、その内容をお教えください。
4. 脆弱性の報告について、その内容を分析する専門的な委員などの制度が提案されていませんか。もし、議論されているのであれば、その内容をお教えください。

［質問の位置づけ］
これは、本質問事項の責任論に対応した、いま一つの柱である脆弱性情報を公開するために用いる、一定のガイドラインの問題である。これについての議論の進行状況を各国に質問する趣旨である。

［各国の回答］３．３

この点については、各国の回答以前に、すでにネットワークコミュニティで一定の対応が議論されており、その対応を紹介することが妥当になろう。その点について、詳述すると、

このソフトウエア脆弱性の問題は、第２章　2.2.で紹介した議論の後、セキュリティコミュニティや各ベンダーにおいて、積極的に、重要な問題として認識されるようになっていった。２００１年８月には、Russ　Cooper 氏は、完全開示原則が、悪意有るコードの拡散をたすけたのではないかという問題提起をなしており、１１月には、NT BugTrack 上で責任ある開示フォーラムを作るという提案[11]をなしている。また、Microsoft のセキュリティ対策センターの Scott Culp は、その２００１年 10 月に発表した「It’s time to end Information Anarchy」[12]という論文において、脆弱性情報を慎重にかつ責任をもって取り扱うことが重要であり、他の人々をリスクにさらすことを超えるものは何かという線引きをすべきだと提案している。また、Microsoft は、カリフォルニア州マウンテンビューにセキュリティの専門家やプライバシー擁護派，政治家などを集め，「Trusted Computing Conference」と銘打ったカンファレンスを開き（２００１年１１月６日から８日まで）、そこで、「システムの脆弱性の情報開示」という基本原則を改めようとする動き[13]をさらに強化するように考え[14]、さらに、そのメンバーと団体を設立する動きを見せた。

そして、具体的な脆弱性の報告のプラクティスをめぐっては、上記の議論をめぐっていろいろな提案がなされている。なお、この点については、この議論が一般化する前から、CERT/CC において、「脆弱性公開ポリシー」として明らかにされていた[15]が、これらの 議論のうちもっとも注目すべきものは、IETF における「バグ報告ガイドライン」である。このガイドラインは、責任ある開示プロセスのための最善の手法を提示することを目的とし、セキュリティ研究者は，ソフトの脆弱性を発見したら、それを開発元に報告するか、開発元と連絡が取れない場合は、 CERT/CC など，信頼できる第三者セキュリティ機関に報告すること、開発元は報告を受けたら、早急に具体的な回答をいつ返せるかを明記して連絡すること、ソフトメーカーは 7 日ごとに、研究者に対して当該問題に関する最新情報を提供し、報告から 30 日以内に問題を解決できるよう努めること、また、すべてのソフトメーカーに対して、「secalert@companyname.com」のように、セキュリティ専門家からソフトの脆弱性に関する警告／通知を受け付けるためのメールアドレスを別途用意することなどを提案している。結局、このガイドラインは、3 月 18 日に、IETF の管轄外として取り下げられた。

その後も、この点をめぐる議論は続き、2002 年 10 月には、前述の Microsoft が設立の動きを見せていた団体である Organization for Internet Safety という団体が設立された[16]。しかしながら、具体的な活動については、そのホームページなどを見る限り、未知数である。

そして、各国の回答をみていくと

３．３．１について

各国において、一般的な義務というのは、報告されていない。しかしながら、韓国においては、「情報通信サービス情報保護指針」第８条第４項は、「情報保護責任者は、周期的に情報システムの保安脆弱点を点検、分析して、その結果を情報通信サービス提供者に報告しなければならない。」と規定されている。そして、この報告を公的な機関になすべきものとして拡張すべきか否かという点が、現在、議論されている。

---

11 http://www.ntbugtraq.com/default.asp?sid=1&pid=47&aid=66

12 http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/essays/noarch.asp

13 http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/news/standard.asp

14 http://www.zdnet.co.jp/news/0111/07/e_relief.html

15 http://www.kb.cert.org/vuls/html/disclosure

16 http://www.oisafety.org/

３．３．２について

法的な位置づけとの関係でいえば、この点については、英国、フランス、ドイツについては、そのような義務があるものとは認識されていないようである。これに対して、韓国では、「情報通信網利用促進ならびに情報保護に関する法律」および、それに基づく、「情報通信サービス情報保護指針」によると、このような対応義務および管理体制構築義務があるとして、電気通信プロバイダにおいて、しかるべき対応義務を認めていることが報告されている。

３．３．３について

米国においては、2003 年 2 月に発表された”National Strategy to Secure Cyberspace” の“Priority II: A National Cyberspace Security Threat and Vulnerability Reduction Program”（http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf） の“3. Reduce and Remediate Software Vulnerabilities”で触れられており、政府が、 脆弱性公開にむけての最適のアプローチとメカニズムについて共同で発展させることが触れられている。具体的な内容については、米国の報告においても、あまり詳細は、はっきりしないが、資金援助について、国土安全省にその管轄が移管になったこと（2003 年３月１日の執行命令による）、また、国土安全省において、FedCirc という部局が存在し、さらにそのサブ部局であるＰＡＤＣ（ Patch Authentication and Dissemination Center）において、「侵入の脅威および脆弱性についても適時的な周知」「認証済みパッチの安全なダウンロード」「テクニカルサポート」をウエブで提供している。

３．３．４について
脆弱性の報告について、その内容を分析する専門的な委員などの制度については、米国では、上述のように PADC などの動きが参考になる。
また、韓国では、大きな動きがあるが、この点については、以下、3･4 の回答参照のこと。

3.4　SQL Slammer の事件をきっかけに何か動きなどがありましたか？

［各国の回答］３．４

具体的な動きが指摘される国は、多くは、なかった。

ドイツでは、BSI は、今年、インターネットにおけるセキュリティを実行に移す場合にとくに市民を支援することになるイニシアティブ[17]をスタートさせたことが報告されている。

また、韓国では、韓国情報通信部においては、最近、いわゆる「インターネット大乱」（SQL-Slummer 事件）を契機に情報保護関連規定を大幅に強化することを重要内容として含んだ、情報通信網利用促進および情報保護に関する法律改正案を出し、公聴会などを通して世論を収斂している。その内容は、「いまや情報保護は特定な部門の問題ではなく、情報システムとネットワークを利用する政府、企業、利用者全体の問題に拡大し、皆が総体的に協調してこそ、効果的な対応が可能である。」ということを基本的な認識の一つとするものである。そして、具体的な対応策としては（１）インターネット侵害事故発生時における迅速な対応と原因分析（インターネット侵害事故対応支援センターの設置とその役割、ISP、IDC、アンチウィルス業者などに対して、ログ記録保存命令制、現場調査権、資料提出要求権などを規定）（２）個人、企業、政府など各部門別に情報保護を強化。（現在、IDC だけに保護処置を義務化しているが、ISP、IDC、大衆利用施設などに対して細分して、情報保護安全基準を賦課し、これを遵守するように義務化を規定、IDC が、入居している業者のサーバに対し、異常トラフィックの遮断などの緊急処置を行う権限などを付与、ISP を通じた利用者情報保護処置の強化、

[17] http://www.bsi-fuer-buerger.de

S/W 業者の購買者に対する２回の保安パッチ情報の告知義務）（３）「情報保護投資拡大の推進」（「情報保護事前評価制」の導入）（４）ハッキング、ウィルス流布などの「サイバー犯罪の処罰強化」（５）その他情報保護産業や情報保護産業協会による根拠規定の準備などの導入などが提案されており、極めて注目に値するものといえるであろう。

第４章　まとめと提言

４．１　報告内容の各論点に対するまとめ

調査委員会としては、ソフトウエアの脆弱性をめぐる問題について、その行為規範としての側面において問題となる点（2.2）と評価規範としての側面（2.1）において問題となる点との二つの観点から分析を試みた。
まず、評価規範としての観点からの分析の観点から、脆弱性をめぐる責任論について各国の報告を求めた。基本的には、かかる（民事的）責任論については、各国において、似たような基本的なフレームワークでもって分析がなされている（報告 3.2.1）。そして、細かく見ていく際には、重要インフラに関する情報セキュリティに対して一定の対応を図ったり、健康保険、金融機関などにおいて特定の情報セキュリティについての要請を求めたりしている措置が注目されるであろう（報告 3.2.2.）。また、個人情報保護に関する情報セキュリティの原則が具体的なものとして解釈されて適用されるものであることも注目される。各情報セキュリティのプレーヤーに関する責任論については、契約関係が重視されることが指摘され、また、一定の場合に責任を第三者に対しても負うことが報告されている（報告 3.2.3）。また、特に情報セキュリティをめぐる新たなサービス形態として、各依頼者の具体的な情報システム運用に応じてセキュリティを提供する形（いわゆる MSP である）が事業として存在感を増し、法的な考察の対象になりつつある点も注目されるであろう。評価の基準となる注意義務については、法律によって、注意義務を定めるということはないが、特定の分野に対して注意義務を定めることを要求する米国のアプローチ、その基準制定および標準化支援をあげるための韓国情報保護振興院を設立した韓国のアプローチなどが注目される（報告 3.2.5）。
　行為規範として提案されているものについていえば、いわゆる「責任ある開示の問題」以外についても、米国におけるカリフォルニアの上院法案 1386 とカリフォルニア民法典第 1798.85 条は、興味深いものといえよう（報告 3.2.2）。その趣旨は、我が国においても十分に合理性をもつものとおもわれるものである。「責任ある開示」の問題については、2003 年 2 月に発表された”National Strategy to Secure　Cyberspace”　において触れられており、政府が、 脆弱性公開にむけての最適のアプローチとメカニズムについて共同で発展させるべく行動していることが明らかにされている。具体的な内容については、その詳細は、はっきりしないが、資金援助について、国土安全省が現時点では、担当しており、また、FedCirc という部局が存在し、さらにそのサブ部局である ＰＡＤＣ（Patch Authentication and Dissemination Center）において、「侵入の脅威および脆弱性についても適時的な周知」「認証済みパッチの安全なダウンロード」「テクニカルサポート」をウエブで提供しているというのは、具体的な米国における動きとして注目すべき事項であるといえよう。

４．２　各国報告の特徴

なお、各論点毎のまとめについては、1 の通りであるが、各国ごとに特徴のある制度等を特筆すれば、以下のとおりになる。

4.2.1.アメリカ合衆国

　米国は英米法系の国であり、判例法の集積により大きな比重のある法制度といえるが、ネットワークセキュリティの脆弱性に起因する法律問題に関する判例法は、本報告書作成時点では極めて限られている。ネットワークセキュリティの脆弱性に起因する法律問題は、基本的には、不法行為責任、契約責任、行政規制、特別法等の適用により判断される。しかし、例えば不法行為責任における過失責任の法理の適用あるいは法律上の過失法理の適用にあたってどのような場合に注意義務違反が認定されるか、どのような場合に法律上の過失となるかなど、判例法の集積がないと責任の成立範囲に関

し判断が難しい状況である。特にプライバシー保護に関連するネットワークセキュリティ問題に関しては、金融機関や児童の個人情報など特別法で規制されており、注目に値する。判例法、特別法等の発展の余地が大きいといえる。

4.2.2.カナダ

大陸法系に属するケベック州法と、英米法系に属するその他の州で、法理論上の理由付けは若干異なる。しかし、大まかに共通した特徴としては、ソフトウエアの脆弱性をめぐる議論につき、必ずしも新たな立法を必要とせず、刑事責任、契約責任、不法行為責任、および規制それぞれの側面で、それぞれ現行法上の解釈方法による解決方法があるという認識である。したがって、また、なんらかの注意標準が設定されたとしても、その遵守が必ずしもそのまま責任に関する抗弁になると解されていない。情報セキュリティ、機密性、正確性、または可用性に関して、サービス・プロバイダの責任を規定するものとして、ケベック州の「情報技術への法的枠組みを確立するための法律」が目新しい。

4.2.3.フランス

フランスでは、特別立法がなされておらず、民法の不法行為責任又は契約責任に関する一般論の応用として責任の有無が考えられている。従って脆弱性についての過失責任は容易には認められず、いわゆる手段債務となることもあって、セキュリティの脆弱性について民事責任が問われるのはごく例外的ということになる。ただし、個人情報保護については、ＥＵ指令がいくつかの領域で、より厳しいセキュリティ確保義務を課していることもあり、刑事・民事両面で情報セキュリティを確保すべき義務があり、判例も存在する。

4.2.4.英国

英国におけるソフトウエアの脆弱性をめぐる問題について、特段の対応がなされているわけではなく、判例法、制定法、産業界の基準などにより対応がなされている点である。民事上の問題については、契約、過失、厳格責任などの項目で議論がなされている。情報については、有形的損害か、経済的損失か、作為によるか、信頼の要素があるかについて、４つの分析がなされ、経済的損失については、契約による以外には、損害賠償は、困難であるという点に特徴があるものといえよう。また、注意義務については、どの種類の人たちに対して、どの程度負うかという判断枠組みで判断がなされるためにシステムの管理等に携わる者についても第三者に対しての責任という観点からは、責任を負うということはほとんどないとされている。また、注意義務の基準に関連するものとして業界標準があり、それについては、一般のものと部門別のものがある。特に、保険医療関係・電気通信分野については、注目がなされる。

4.2.5.ドイツ

ドイツでは、特別の法規制をすることがなくても、現行の民法および刑法の諸規定により、責任を問うことが可能である。とりわけ、ソフトウエアの脆弱性により生じた損害については、瑕疵担保責任もしくは不法行為による損害賠償責任を追求することが可能である。これに関して、わが国や米国でみられるいわゆる Shrink wrap 契約における免責条項は、ドイツ民法の規定（307、３０９条）によりきわめて制限され、軽微な過失以外では許容されないため、実際上、そのような免責条項をもつ契約自体がほとんど存在しないことに留意すべきである。

また、情報セキュリティにおける脆弱性については、政府機関としての BSI が重要な役割を果たしている。とりわけ、BSI が情報セキュリティの領域では他の政府機関・公的部門に対する情報提供・指導により公的なシステムのセキュリティの確保を図ると同時に、民間領域におけるシステムのセキュリティの維持にも寄与していることは、注目すべきである。BSI の活動に対する信頼性は、それが連邦政府の機関であるということにとどまらず、技術水準ならびに活動内容に関する徹底した情報公開により、得られているということも、併せて注目すべきである。

4.2.6.大韓民国

韓国では近年、情報通信部が主体となってＩＴ関連の法整備を強力に推進してきた。本調査に密接にかかわる分野では、「情報通信基盤保護法」と「情報通信網利用促進ならびに情報保護などに関する法律」などの整備が挙げられ、特に国家の重要通信基盤施設を保護した前者は、こうした施設に対する電子的侵害行為に対して重い刑事処分を科している。民事上は、一般的に契約責任と不法行為責任を論ずることになり、契約の有無と注意義務の有無が問題となる。この際、上記法律の他、「情報通信サービス情報保護指針」などの規定中に関係者の注意義務が明文で詳細に定められる傾向があり、このため注意義務とその違反に基づく過失責任は比較的広範囲に認定される可能性がある。いずれにせよ他国に比較すると行政主導型の規定主義的色彩が強いように思われる。製造物責任については、情報の「物」への化体が問題となるが、この点でも SQL スラマー事件の今後の行方が注目される。本事件をきっかけに、現在、上記「網法」改正など、法制度のおおがかりな改正の動きがあり、今後の法整備に注目したい。

４．３　提言

4.3.1.我が国における情報セキュリティと法律との関わり

我が国における脆弱性の問題と情報セキュリティに対する法律の関わり方が、今回報告の対象となった各国と比較して、特に対応が不十分であるというような見方というのは、できないであろう。情報セキュリティの問題については、むしろ、法的な対応になじみにくい点もあるものと思われる。この点について、報告書においては、『セキュリティの詳細な基準を法定することは、情報技術の進展にとって有害である』(ドイツ)とするものもあるくらいである。しかしながら、調査委員会の意見としては、各国の法的対応を調査すると、我が国においては、あまりに全範囲について、法的対応が、後手にまわっているのでなはいかという意見が多数を占めた。各国を比較すると、韓国のように、問題点として考えうるものに対して、積極的に法律を定め、それで、解決を図ろうとしている国の実際の運用と課題は、きわめて我が国の立法の方向性を考える上で参考になるであろうし、他の国においても、重要インフラに対する保護の法的位置づけや、部門別立法における情報セキュリティの法的位置づけについては、参考にすべきであるという点で意見の一致をみたところである。かかる基本的な立場を基に我が国の法的制度を考える上で参考になる提案としては、以下の点をあげることができるであろう。

4.3.2　具体的提案

提案１　分野を特定せずに、画一的な法規制を行なうことは現実的ではないと考える。むしろ、特に重要な情報を取り扱う分野においては、他と比べてより重点的な情報セキュリティの維持・向上の重要性を認識し、かかる分野に対する特別の法規制の是非について、各国の比較法制をもとに議論が深められるべきである。

提案理由

重要な情報を取り扱う分野として、諸外国では、電気通信分野、医療情報取扱分野、金融機関分野をあげている。それらの分野については、米国やＥＵ指令によって、特に情報セキュリティの保持・向上がきわめて重要な意義をもつと認識される分野である。かかる分野において、例えば、セキュリティポリシーの書面化の義務付け、セキュリティへの脅威が存在した場合の対応義務の法定などが、比較法的には、実際になされており、我が国においてもかかる定めをなすべきではないかという点は、十分に議論に値するものと思われる。

提案２　情報セキュリティに対する脅威があり、情報の取得がなされたものと思慮される、または、その疑いがあると確実に考えられる場合に、情報主体にたいして、かかる事件の存在を通知することの義務づけおよび、その手順の定めをなすべきである。
一定の情報については、安全な通信方法（暗号化など）について考慮していない送信に対して、法的には、注意義務違反とされることを明示すべきである。

提案理由

米国において、カリフォルニアの上院法案1386（2003年７月１日から発効）が、顧客の情報が、危険にさらされた場合に、顧客に対して、通知をしなければならないと定められている。これは、顧客に「アイデンティティ窃盗（identity theft）」の可能性を知らせ、対応する機会を与えるべきであるという判断である。我が国において、前述3.2.2において述べたように情報漏洩の事件の際に、情報主体に通知がなされなかったという新聞報道がなされたことから、情報主体への影響を取扱事業者が独自に判断することが、認められるべきかという論点が存在するものと思われ、米国のかかる対応は、一つの方向性を示すものと考えられる。

また、カリフォルニア民法典第 1798.85 条は、カリフォルニアにおいて、社会保障番号自体を、「安全」な方法で「暗号化」しないで送信することを禁じるものである。我が国においてもかかる認識は当然に妥当するものであろう。我が国において、当然過失を構成するという法理が、成り立つかどうかについては、議論の余地があるものと考えられるが、社会通念として、かかる送信が、注意義務違反となることが共通の認識とされることが重要であると思われる。

提案３　ソフトウエアの脆弱性をめぐっては、脆弱性の発見から、製造業者への報告ソフトウエア脆弱性の評価、修正ソフトの認証、脆弱情報の公表などについて、善良な実務慣行が構築されなければならない。
また、特に提案１で触れられた分野において、修正ソフトの検証、導入がスムーズに行われるための公的サービスの導入などについて、さらなる検討がなされなければならない。

提案理由

ソフトウエアの脆弱性情報については、従来の完全開示原則の妥当性について、疑問が投げかけられており、一定の責任ある開示原則というものの採用を考慮すべきではないかというのが議論されている段階である。そのような責任ある開示原則に移行すべきとしても、そこでの論点としては、開発元に対する連絡の方法、開発元での対応義務の有無および対応に要する時間、脆弱性情報の審議・重要性の判断方法、修正ソフトの作成・配布の問題、開示の可能になるべき時期などの諸問題がある。これらの論点について、米国では、重要な問題として認識されつつ有り、我が国においても、議論を掘り下げるべき問題であると認識すべきである。

また、修正ソフトの検証・導入についても、一定の資金援助のもとに、公的サービスが提供されており、かかる制度の運営状況などを参考にし、かかるサービスの導入等について前向きに検討されるべき問題であると考えられる。

（余白）

（別紙）

ソフトウェアの脆弱性をめぐる法律問題

弁護士　高橋郁夫

1.　議論の契機

従来のソフトウェアの脆弱性の問題については、議論はあったものの、これは、万人に公開されるべきであるとするいわゆる完全開示原則とでもいうべきものが適用されていた。しかし、これが今現在、正面から議論されるべき問題として認識されている。

この議論が正面から、議論されるようになったのは、おそらく２０００年7月２６日のラスベガスにおける“Black hat Security Conference”における Marcus Ranum 氏の”Script Kiddies Suck“ [1]という講演からだと思われる。Ranum 氏は、その講演の中で①セキュリティに対する認識を変更すべきこと②問題を開示する方法を変更すべきこと③アカウンタビリティーを変更すべきことを説いている。

①セキュリティに対する認識を変更すべきことというのは、「スクリプトキディ」が多数おり、一般大衆は、彼らにうんざりしていること、そして、彼らの数を減らさなくてはならない、そのようにセキュリティの考え方を変更しなければならないということを説いている。そして、ハッキングは、アマチュア・テロリズムだといい、容赦なく対応しなければならないとしている。そして現在は、ホワイトハットとブラックハットとの間に非常に大きなグレーのエリアがありこのグレーのエリアを減らさなくてはならない、元ハッカー[2]をセキュリティーコンサルタントとして雇うのを止めなければならないといっている。

②完全開示の変更について、彼は、完全開示の方法は、スクリプトキディの大軍を作り、ソフトウェアの品質に何らのポジティブな影響を与えず、バグを訂正するためのポジティブなインパクトを与えるものではないという点で自己欺瞞だったという。脆弱性の情報の進化の過程は、欠点（情報以前のもの）があり、脆弱性があり、それが現実化し、公開されず、ツールが生まれ、スクリプトキディがこれを利用する。その一方で脆弱性の公開により発見・評価の論理がなされ、パッチが作られ、ユーザがこのパッチをインストールするという過程を経る。そして、彼は、スクリプトキディは必要悪でありうるかという疑問を呈し、ソフトウェアには自動アップデートのシステムを設定しうるし、公表するにはよりよい方法があるので、スクリプトキディがユーザにアップデートをなすよう強制しているとかベンダーがミスを隠すのを不可能にしているということは言えないとしているのである。そして、完全開示の神話として４つのことがあるという。（１）ハッカーはこれらの記述をすでに知っており、彼らがなしうる手法をすべての人が知りうるのがベストである。（２）ベンダーは、ひとたび公開されれば彼らのバグを隠すことはできない。（３）情報は将来におけるよりよいシステムをつくるために公開することが必要である。（４）そしてそれは発見者の財産である。これらの神話に対して彼は、（１）確かにハッカーはそうであるがスクリプトキディはそうではない。脆弱性の大

---

[1] http://www.blackhat.com/presentations/bh-usa-00/MJR/MJR-blackhat-2000-keynote.ppt

[2] ここでいう「ハッカー」は、善意の研究者を含む広義のハッカーではなく、不正アクセスを目的とする者のみを指す。本別紙については以下同じ。

多数は、それによって脆弱性を解消するという目的のためよりは、自己の力量の顕示などの公開すること自体が目的であるという動機によって導かれて調査され、公開されるのである。（２）欠点を公開する効果的な他の方法がある（３）詳細を教えたりテストしたりする必要はない。（４）自分の財産だといっても、自分の宣伝、財産的利益、エゴのメッセージなどである。

③セキュリティに関連する問題のアカウンタビリティーのレベルを増加すべきであるという主張もなされた。ツールなどをリリースする人間は、彼らの行動の結果に対して責任を取るべきであり、また、セキュリティのバグを持った製品を生産するベンダーは、修正を提供する標準を守らなければならない。

これらの考察をもとに、彼は、自分が正しいかどうかは明らかではないとしながら、以下のような点などを予言として指摘するのである。（１）グッドガイは、敵に対して反撃なすであろう。（２）攻撃ツールの作者と頒布者は、民事損害賠償訴訟において高い判決額を受けるであろう（３）従来、法執行機関がハッキングに対応しようと試みてきたが、その役割は、民事裁判によって、とって代わられるであろう。

そして、結論として、私たちは、インターネットセキュリティ時代の始まりの終わりにいると思うとしている。フン族は、ローマのなし方をしらずに、その吸いつくし方を知っていたにすぎないということを覚えておくべきであるとしている。

2. 議論に対するリアクション

この議論は、大きな反響を巻き起こしたようである。Weld Pond、 ZDNet/USAの記事[3]によれば、「Ranum氏は、聴衆の神経を逆なでしたに違いない。あらゆる人が、カンファレンスの基調を定めるものとして同氏のスピーチを話題にしていたが、私が話をした一部の人たちが示した「基調」は、ある種の怒りだったからだ。」とされているのである。Ranum氏は、この問題提起に一定の理解をしめしつつも、「情報公開を排除すれば、問題はさらに悪化するだけだ。」として、「セキュリティ研究情報の自由な交換を抑えつけようとするのではなく、ベンダーにモチベーションを与え、より安全な製品が開発されるよう協力して取り組む必要がある。出荷される製品に、過去の問題が潜在的な脆弱性として再び含まれることがないようにする必要がある。ユーザがセキュリティホールをすばやく簡単に修復できるようにするという課題にも、協力して取り組む必要がある。攻撃者がセキュリティ問題を発見してそれを悪用できるのなら、善良な人々の側が、先に問題を見つけて修復できるような、より良い方法がきっとあるはずだ。」としている。

3. 脆弱性の論点をめぐる提案

その後、このソフトウェア脆弱性の問題は、セキュリティコミュニティや各ベンダーにおいて、積極的に、重要な問題として認識されるようになっていった。２００１年８月には、Russ Cooper氏は、完全開示原則が、悪意有るコードの拡散をたすけたのではないかという問題提起をなしており、１１月には、NT BugTrack上で責任ある開示フォーラムを作るという提案[4]をなしている。

また、Microsoftのセキュリティ対策センターの Scott Culpは、その２００１年 10

[3] 「セキュリティ情報の公開は是か非か」（http://www.zdnet.co.jp/news/0008/22/pond.html）
[4] http://www.ntbugtraq.com/default.asp?sid=1&pid=47&aid=66

月に発表した「It's time to end Information Anarchy」[5]という論文において、「セキュリティコミュニティは、これらの兵器を構築する青写真を提供するのをやめる時期に来た。コンピューターユーザーは、セキュリティコミュニティに対してユーザを保護すべき義務があると主張すべき時期に来ている。私たちは、セキュリティ脆弱性を議論することができ、そして、すべきであるが、私たちは、賢明で、スマートで、責任ある方法でなすべきである。」といっているのである。彼は、まず、すべてのセキュリティの脆弱性を排除できないのであれば、脆弱性情報を慎重にかつ責任をもって取り扱うことが重要になるという。ところが実際にセキュリティコミュニティが、取り扱っているやり方は、良くいって情報アナーキーというべき方法である。そしてこの点の実務とワームの近ごろの動きは関係しており、脆弱性情報の詳細の公表は、兵器として利用することに貢献しているのである。

情報アナーキーは、近ごろにおけるベンダーがセキュリティ脆弱性を公に明らかにする点についての進歩のほとんどを無駄にしてしまう危険性を有しているのである。もし、脆弱性を公に明らかにすることが、不可避的に脆弱性の利用につながるのであれば、ベンダーは、顧客を守るために他の方法を探すしかなくなるのである。これは、脆弱性を議論することを止めることを求めているではなく、他の人々をリスクにさらすことを超えるものは何かという線引きをしようとしているのである。表現の自由をあきらめさせるといっているのではなく、混雑した映画館で火事だと叫ぶのをやめさせようとしているだけなのである。この問題は、セキュリティコミュニティ自体よりも問題が大きく、すべてのコンピューターユーザーは、利害関係を有しているのであり、私たちは、みんな、脆弱性情報が、適切に取り扱われることを確かにするのを助けることができるのである」といっているのである。

このような論考の立場と呼応するかのように Microsoft は、カリフォルニア州マウンテンビューにセキュリティの専門家やプライバシー擁護派、政治家などを集め、「Trusted Computing Conference」と銘打ったカンファレンスを開き（２００１年１１月６日から８日まで)、そこで、「システムの脆弱性の情報開示」という基本原則を改めようとする動き[6]をさらに強化するように考え[7]、さらに、そのメンバーと団体を設立する動きを見せた。

4. 議論の発展と混迷

具体的な脆弱性の報告のプラクティスをめぐっては､上記の議論をめぐっていろいろな提案がなされている。なお、この点については、この議論が一般化する前から、CERT/CC において、「脆弱性公開ポリシー」として明らかにされていた[8]。

これらの 議論のうちもっとも注目すべきものは、IETF における「バグ報告ガイドライン」であろう。このガイドラインの内容は、IETF のホームページからは、既に削除さ

[5] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/essays/noarch.asp

[6] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/news/standard.asp

[7] http://www.zdnet.co.jp/news/0111/07/e_relief.html

[8] http://www.kb.cert.org/vuls/html/disclosure

れていて[9]、詳細は、不明である。なお、報道記事などを前提にすると、責任ある開示プロセスのための最善の手法を提示することを目的とするものである。そのプロセスは、具体的には、以下のようになる。セキュリティ研究者は、ソフトの脆弱性を発見したら、それを開発元に報告するか、開発元と連絡が取れない場合は、 CERT/CC など、信頼できる第三者セキュリティ機関に報告する。開発元は報告を受けたら、7 日以内に回答する。あるいは、報告に対する返信を自動化している場合は、より具体的な回答をいつ返せるかを明記する必要がある。またこの場合、具体的な回答は 10 日以内に行うこと。ソフトメーカーは 7 日ごとに、研究者に対して当該問題に関する最新情報を提供し、報告から 30 日以内に問題を解決できるよう努めなければならない。また、すべてのソフトメーカーに対して、「secalert@companyname.com」のように、セキュリティ専門家からソフトの脆弱性に関する警告／通知を受け付けるためのメールアドレスを別途用意することを提案している。

そして、この特徴は、報告者に対しても一定の責任を要請するものとしての傾向が顕著なところにある。具体的には、「ベンダーが 30 日以内に脆弱性を解決するのが困難な場合もある」という点をバグ報告者が理解すべきだと指摘し、具体的には、次の 3 つのケースが挙げられるという。1 つは、バグがセキュアではない設計に起因するものの場合。2 つめは、バグが影響するハードウェアや OS、サポートすべき製品のバージョンが多数に及ぶ場合。3 つめは、ベンダーがセキュリティ技術に熟達していない場合である。これらの場合には、「上記のケースに当てはまる場合には、ベンダーが誠意を持って脆弱性の解決に当たっている限り、報告者はベンダーに時間的猶予を与えるべきだ」とこの草案には記されている。

もっともこの提案に対しては、批判も強い。「こうした方針を採用すれば、ベンダーがこの草案の条件を盾に、自社のバグウェアを棚に上げて報告者に『無責任（な言いがかり）』のレッテルを貼ることになりかねないという。」のである。

そして、このガイドラインは、3 月 18 日に、IETF の管轄外として取り下げられた。

その後も、この点をめぐる議論は続き、2002 年 10 月には、前述の Microsoft が設立の動きを見せていた団体である Organization for Internet Safety」という団体が設立された[10]。しかしながら、具体的な活動については、そのホームページなどを見る限り、未知数である。

現時点におけるこの論点の議論は、いまだ混迷を続けていると評価することができそうである。ここで、一つの事件を紹介することができる[11]。この事件は、ソフトウェアの著作権と第三者のセキュリティホールの公開についての法的問題という形式をとったものである。AutoProf.Com 社は、ScriptLogic 社のツール（Windows のクライアントを中央から環境構築する）に無権限で管理者アクセスを可能にする脆弱性があることをホワイトペーパーで明らかにした。 ScriptLogic 社は、2002 年 8 月に、AutoProf 社を、リバースエンジニアリングおよび、悪意有る宣伝を企てることにより、著作権法およびライセンス契約違反で訴訟を提起した。この訴訟については、原告と被告が、競争相手ということもあり、開示の適切性を直接に争点とするものではないが、しかし、開示の

9 http://www.ietf.org/internet-drafts/draft-christey-wysopal-vuln-disclosure-01.txt
10 http://www.oisafety.org/
11 http://www.gcn.com/21_34/security/20634-1.html

ルール自体の必要性を強調するものだという評価があり、そのような指摘は、的外れとはいえないであろう。

5.最後に

再度、Marcus Ranum 氏の問題提起に戻ることとする。そこでは、刑事的手法による規制よりも民事的な判決例の積み重ねによる脆弱性をめぐる利害関係の調整が期待されているように思われる。そして、特に脆弱性の侵害に対して、高額の損害賠償による一定の判断が、提唱されていた。

しかしながら、このような問題提起について見れば、現時点では、あまりあたっているとはいえないようである。セキュリティをめぐる然るべき技術的措置を取るべき法的義務という観念は、いまだ、一般化していないようにも思え、また、米国においても、なかなかそのような義務が問題になった法的事案の報告を見かけないのである。

Ranum 氏の民事的な判決例の積み重ねによる脆弱性をめぐる利害関係の調整という問題意識が、はたして、現実化してくるのか、成り行きが注目されるものと言うことができるであろう。

（余白）