INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

情報システム等の脆弱性情報の取扱いにおける法律面の調査 報告書

2004 年 6 月

独立行政法人 情報処理推進機構

― 目次 ―

序 **1**

第 1 章 脆弱性情報と取扱いルールと法律とのかかわり **3**

第 1 序 3

（1）前提となる事実認識 *3*

（2）手法 *3*

（3）目的 *3*

第 2 脆弱性情報取扱い体制の法的意味 5

1　告示の法的性格 *5*

2　告示・ガイドラインと国民の権利との関わり *6*

3　慣習と国民の権利・義務との関わり *6*

4　告示・ガイドラインの適用範囲 *7*

第 3 脆弱性の意義と諸問題 9

1　序 *9*

2　脆弱性の意義 *9*

3　ソフトウエアの提供と「脆弱性」に対する修補の法的位置づけ *10*

第 4 脆弱性情報発見・通知と契約法の問題 17

1　リバース・エンジニアリング *17*

2　セキュリティ調査委託契約と脆弱性の公開 *18*

3　ライセンス契約、秘密保持契約と脆弱性の発見・公開 *19*

4　公益通報者保護法による契約関係からの保護 *20*

第 5 脆弱性発見と不正アクセス、そして、届出の受理について 22

1　脆弱性発見と不正アクセス *22*

2　先行行為の他の行為への影響 *24*

第 6 脆弱性発見・公開者と攻撃者によるセキュリティ侵害に対する不法行為 27

1　脆弱性の公開と表現の自由 *27*

2　脆弱性情報・開示の態様等と開示者の法的位置づけ *27*

3　攻撃コードとその作成を容易にする行為 *28*

4　ウェブサイトにおける脆弱性の指摘と名誉毀損との関係について *29*

第 7 脆弱性発見・公開者の行為による開発者に対する不法行為 30

1　名誉毀損との関係 *30*

2　信用毀損罪との関係 *31*

3　民事上の責任関係 *31*

第 8 取扱い基準関与者自身の法律問題 32

1　法執行の要請との関係 *32*

2　情報公開法との関係について *32*

3　責任問題 *33*

第 9 通信の秘密と脆弱性情報取扱い体制について 34
1　通信の秘密の概念 34
2　脆弱性の調査・発見行為と通信の秘密との関係 34
第 10 ベンダコミュニティの構成と競争市場 36

第 2 章 米国における脆弱性情報と法的論点 37

第 1 脆弱性報告について情報処理推進機構（IPA）のとるスキームについての報告（同スキームを米国に導入した場合の仮設的分析を含む） 37
第 2 米国における「責任ある公開スキーム」に関する報告 41
(A) 重要な社会基盤（critical infrastructure）を保護する目的での脆弱性報告 41
(B) 脆弱性報告についてのガイドライン策定に向けた業界のイニシアティブ 44
(C) 私企業による有料サービス 45
第 3 結語 48

第 3 章 報告書モデル案における法的関連記述の解説 50

第 1 「ソフトウエア等脆弱性関連情報取扱基準モデル案」の法的関連記述に関する解説 ... 50
Ⅰ．主旨 50
Ⅱ．用語の定義 53
Ⅲ．本基準における関係者の定義 57
Ⅳ．本基準の適用範囲 61
Ⅴ．対象がソフトウエア製品である場合の脆弱性関連情報取扱基準 62
Ⅵ．対象がウェブアプリケーションである場合の脆弱性関連情報取扱基準 63
Ⅶ．その他 64
第 2 「ソフトウエア等脆弱性関連情報取扱ガイドラインモデル案」の法的関連記述に関する解説 65
第 3 「発見者が心得ておくべき法的な問題」に関する解説 65
1．脆弱性関連情報の発見に際しての法的な問題 65
第 4 「製品開発者が心得ておくべき法的な問題」に関する解説 74
第 5 「ウェブサイト運営者の法的関連事項」に関する解説 79

付録 1 米国における脆弱性の取扱いに関する法律面の動向 82

1)　米国における情報セキュリティをめぐる最近の法律上の論点：サーベンス・オックスリー法、医療保険継続性及び責任法（HIPAA）、カリフォルニア州セキュリティ保護法等 82
2002 年サーベンス・オックスリー法（Sarbanes-Oxley Act of 2002） 82
健康保険継続責任法（HIPAA） 83
1999 年グラム・リーチ・ブライリー法（Gramm-Leach-Bliley Act）（「G-L-B 法」） 83
米国証券取引委員会（SEC）の「レギュレーション S-P：消費者の財務情報のプライバシー」 84
米国連邦取引委員会法（FTC Act） 85

コンピュータ詐欺及び不正利用防止法（Computer Fraud and Abuse Act）（「CFAA」）. 85
電子通信プライバシー保護法（Electronic Communications Privacy Act）（「ECPA」）.. 86
2001 年米国愛国者法（テロリズムを迎撃し阻止するために必要な適切な手段を提供することによりアメリカ合衆国を団結させ強化する法律）USA PATRIOT (Unifying and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act of 2001 86
情報自由法（Freedom of Information Act: FOIA)..... 87
2002 年国土安全保障法（Homeland Security Act of 2002） 87
内部告発者保護法（Whistleblower Protection Act） 88
セキュアなサイバースペースのための国家戦略（The National Strategy to Secure Cyberspace） 88
カリフォルニア州セキュリティ保護法（2002 年） 89
統一州法..... 89
その他の州法上の論点 90
2) 知的財産権法と情報セキュリティとの間の衝突に関する報告 91
特許権..... 91
著作権..... 92
商標 94
営業秘密..... 94
データベース..... 95
その他の形式の知的財産権 95

付録 2 韓国における脆弱性の取扱いに関する法律面の動向..... 97

付録２．１．SQL スラマー事件における訴訟..... 97
付録２．２．韓国における法律改正をめぐる議論資料..... 125
Ⅰ．改正の背景 129
Ⅱ.推進経過および主要な改正の内容..... 129
Ⅲ. 情報通信網保護関連の改正事項 130

序

平成１６年3月１８日
脆弱性情報取扱の法律問題研究会

脆弱性をめぐる取扱いルールに関連して「情報システム等の脆弱性情報の取扱いに関する研究会」内の「脆弱性情報取扱ガイドライン WG」は、現在、経済産業省において公的ルールである「ソフトウエア脆弱性情報取扱基準」および情報処理推進機構・JPCERT コーディネーションセンター・日本ネットワークセキュリティ協会の提唱する「脆弱性情報取扱ガイドライン」を準備し、情報システム等について一定の取扱い体制を構築しようとしている。この双方からなる一定の体制を便宜上、脆弱性情報取扱い体制と呼ぶことができる。この体制について（１）この体制についての法的論点の検討（２）この体制に関連する米国における法的論点の紹介・検討等をなそうとするのが、本報告書である。なお、（３）「ソフトウエア脆弱性情報取扱基準」「脆弱性情報取扱ガイドライン」における法的記述部分についての解説については、便宜上、別個の文書とした。この報告書においては、第１章「脆弱性情報と取扱いルールと法律とのかかわり」として、本体制において生じうる法律面の論点について解説し、第２章「米国における脆弱性情報と法的論点」として、脆弱性情報の流通において、同様に課題を認識し検討を進めている米国の体制と本体制を比較し解説している。また、第３章として、上記基準およびガイドラインについての法的な関連記述について逐条解説をなしている。これらの参考資料として、諸外国の中から米国と韓国を例に、脆弱性の取扱いに関する法律面の動向を調査し、付録として掲載した。

この報告書は、以下の研究会の構成メンバーの協同作業によるものであり、また、「脆弱性情報取扱ガイドライン WG」における委員の活発な議論にも非常に影響を受けているものである。脆弱性情報取扱い体制の確立・定着に本報告書がなんらかの貢献を果たすことができれば、研究会としても喜びである。

なお、研究会の構成員は以下のとおりである。なお、本報告書に先行するものとして、「ソフトウエア脆弱性情報取扱基準」「脆弱性情報取扱ガイドライン」の草案に対する検討および法的意見を当研究会において作成したが、その際には、夏井高人氏（明治大学教授・弁護士）にも研究会委員として参加いただいた。本報告書は、その際の研究成果にも負うところが多いため、本報告書においてもアドバイザーとして記した。

脆弱性情報取扱の法律問題研究会

代表	高橋 郁夫（弁護士・宇都宮大学講師）
委員	土井 悦生（弁護士）
委員	池村 聡（弁護士）
アドバイザー	夏井 高人（明治大学教授・弁護士）
大韓民国調査担当	近藤佐保子（明治大学政治経済学部）
米国調査担当	リチャード・L・フィールド（Richard L. Field）（米国弁護士）

第1章 脆弱性情報と取扱いルールと法律とのかかわり

第1 序

脆弱性情報取扱い体制についての基本的な事実認識、その取扱いに対する手法、この体制の目的は、以下のようなものと考えられる。

（1）前提となる事実認識

脆弱性情報については、その発見、報告、対策、公表の過程に関連して、その流通すべき適切なルートが明らかになっていないのではないかという懸念を脆弱性情報取扱ガイドライン WG の参加者が共有している。本来は、ソフトウエアの開発者、流通者、ウェブサイトの作成者およびその責任者、開発関係者などによってその脆弱性情報が適切に共有されて、早急にその脆弱性に対して対策がなされるべきであるにもかかわらず、そのルートが明らかではないことによって、脆弱性情報の共有が図られず、脆弱性に対する対応が遅れがちになったり、その脆弱性情報が悪意ある者の間でのみ共有されることになったりしてしまっていると考えられる。

（2）手法

脆弱性情報を適切に収集し、それを分析・評価し、それに対する対応を促し、これらの関係者を調整する機能が、現状において欠けているものと認識されている。これらの機能を実現するために、本基準は、そのような機能を担わせるものとして関係の機関を指定し、それに関連して、関係機関への届出の際の基準、それらの関係機関の機能および行動基準、内部関係者の行動基準を定め、関係者には、それに応じる一定の行動を推奨するものである。

（3）目的

このような事実認識のもと、WG としては、適切な脆弱性情報の流通ルールを提唱することにより、我が国における情報処理機能の機密性、完全性、可用性の確保・促進を図ろうとするのが妥当であるとの認識に到達した。脆弱性情報が、いわば、「闇に埋もれている」状態は、望ましいものではない。それを放置するよりも、適切なルートで「日のあたるところ」に拾い上げ、上記（2）の手法により適切な流通および共有を図ることにより、我が国のセキュリティが確保・強化・促進されるという認識に至ったということになる。

法的な観点からは、これらの脆弱性情報取扱い体制を定めた際には、どのような法律問題が発生し、その発生する論点に対してどのような対応方法をはかるのかという問題がある。

本考察は、以下の論点について、およその方向性を考えるものである。もっとも、以下の法的問題については、比較法的な実例があるわけでもなく、まだ我が国で関連する判決例があるというわけではないものが大半である。この意味で、法律の解釈としてはきわめて流動的なものとならざるをえず、きわめて、仮定的な判断となるものである点について、ご了承いただきたい。

第2 脆弱性情報取扱い体制の法的意味

今回、提案されている脆弱性情報取扱い体制は、「ソフトウエア脆弱性情報取扱基準」という公的ルールと「脆弱性情報取扱ガイドライン」という「ガイドライン」を併用して体制を準備しようというものである。そして、この公的ルールとしては、具体的には告示という形態が採用されるものと思われる。その場合に、この体制の有する法的意義について、（１）告示の法的性格（２）告示・ガイドラインと国民の権利との関わりという二つの論点を検討しておく必要がある。

１　告示の法的性格[1]

告示とは、行政措置の告示の形式をいう。国家行政組織法は、各大臣等は「その機関の所掌事務について、公示を必要とする場合においては、告示を発することができる」と定めている（同法１４条１項）。告示は、官報（国の場合）に掲載されて周知が図られる。告示は一般に、法規の性質を持たない行政規則の一種として説明されることが多い。しかし、個別の法令で、各種の事項について、告示の形式による公示を義務づけている。また、法律の明文では、公示が義務づけられていない場合であっても、法律の規定を実施するために、多くの事項について告示が発せられることに注意する必要がある。

これらの告示の法的性質は、それぞれの内容に即して検討されなければならないと言われている。告示の中には、法律の規定を補充し、法律の規定と一体となって国民を拘束するものもある（例、国民生活安定緊急措置法４条４項、９条４項に基づく灯油、トイレットペーパー等の価格についての価格の公示）。また、公正取引委員会の「不公正な取引方法」も、告示として独禁法の規定を補充し、実際上国民に対してかなりの拘束力を有しているものといえよう。行政行為の一種としての通知にあたると解されるものもある（例、土地収用法の定める事業の認定）。また、関係の法令の規定のみによっては、告示の法的性質が必ずしも明らかではないものとして、例えば、学習指導要領などがある。さらに、公害基本法９条に基づく環境基準は、直ちに国民に対して具体的な法的効果を及ぼすものではなく法的拘束力を持つ規範ではないが、政府はその基準の確保のために、公害対策を総合的かつ有効適切に講ずる責務を負うとされていることから、独自の意味を持つ法的措置とされており、そのような告示も存在する。

本件告示についていえば、国民の権利義務との関係は、直ちに国民に対して具体的な法的効果を及ぼすものではないということになる。しかし、行政組織法上の規定を補充し、情報の届出機関・調整機関を指定し、また、関係者に対する行政指導の運用基準等

[1] 外間　寛「告示・通達の法的性質」行政法の争点（新版）40 頁（有斐閣、1990）

となるという意味で、独自の意味を持つ法的措置の一部として考えられるものと思われる。

２　告示・ガイドラインと国民の権利との関わり

前項において「告示」の法的性格について検討したが、そこでも明らかなように、告示は、国民の権利義務について具体的に決めるものではない。また、ガイドラインも同様である。しかし、だからといって国民の権利義務と全く無関係というものではない点は留意が必要である。

かかる取扱基準は、それを遵守することが励行され、一般人の間でそれを遵守することが慣習として意識されていけば、法律の一般条項の解釈上斟酌されることになる社会通念などを通して、国民の権利義務に影響を与えることとなる。そして、これには、二つの側面がある。

その一つは違法性の阻却の側面である。具体的には、そのような基準において一定の行為をなすことが求められており、それに従った場合であるのにもかかわらず、刑事なり民事なりの責任を追求されるということがありうる。その場合に、かかる行為は、刑事的には、正当な業務行為（刑法３５条）として、違法性を阻却されるということがありうる。また、民事的には、かかる基準に従った行為は、社会通念上、違法性（民法７０９条の解釈論）を欠くものと評価される可能性がある。具体的にどのような形で影響が起こりうるかは、個別の論点ごとに見ていくことが妥当であろう。

逆にもう一つは、違法評価の側面である。いままでは、表現の自由としていわば放任されている行為であったものが、かかる基準が社会通念として定着すれば、かかる基準を無視してなされた行為については、例えば、犯罪を容易にする行為として認識されたり、不法行為を幇助するものとして認識されたり、行為そのものが不法行為として認識されたりすることも十分にありうるのである。このような場合には、本件で述べる体制が慣習として意識されることによって、構成要件の解釈に影響を及ぼす事例として理解することができるであろう。

３　慣習と国民の権利・義務との関わり

本件体制と国民の権利との関わりという点においては上の二つとも関連するが、本体制の行動基準の性質をどのようなものとして構築していくかという問題と、また、それが定着した場合にどのようなものといえるかという問題がある。

行動基準の性質については、関連当事者に対してこの基準に従って行動することを要請するといっても、その強制力についてどのように考えるかということがある。この基準に対し、①一定の強制したものと認識するか②ネットワークに関わるものの良き慣行

として推奨するものであると認識するかという二つの方向性があるように思われる。どちらにしても、この基準が関係者の行動基準として、いわば規範意識をともなって遵守されるようになった場合については、法例２条の「公ノ秩序又ハ善良ノ風俗ニ反セサル慣習」として「法令ニ規定ナキ事項ニ関スル」点からいって、「法律ト同一ノ効力ヲ有ス」ことになり、「慣習法」に該当することになる。もっとも、この点の慣習としての効力は、法律に定めがある場合はそれが優先するため、いわゆる「義務の衝突」がある場合には法令による義務が優先することになる。

４　告示・ガイドラインの適用範囲

告示・ガイドラインが、関係当事者にとって、一つの行動の参考規範となるべき性格を有するものと認識する場合には、その適用範囲がどのようなものであるかという観点が問題となる。理論的には、これが仮に法規の場合であったとすれば、法規の立法管轄権の問題として議論されることと同様の問題である[2]。

この告示・ガイドラインは、基本的に、脆弱性情報に関連して、その情報の流通により、一定の法律上保護された利益が侵害されることに留意して提案されているものである。この立法管轄権がどのような範囲におよぶかという視点で考えたときには、法例１１条１項の「事務管理、不当利得又ハ不法行為ニ因リテ生スル債権ノ成立及ヒ効力ハ其原因タル事実ノ発生シタル地ノ法律ニ依ル」という文言の解釈論として考慮される。もっともこの原因たる事実については結果発生地をも含むものであり、その意味で、脆弱性情報によりセキュリティが脅かされる場所が日本であれば、この告示・ガイドラインの適用があるとされるのも合理的であるように思われる。

「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」（以下、便宜上プロバイダ責任制限法という）において、適用範囲などが記載されていない点などから考えると、本告示・ガイドラインについても適用範囲を記載しないことにするということも考えられる。しかし、上記のような考え方から、行為（本件では、発見者の所在地）地を問題にすることなく、結果発生地に注目して本告示・ガイドラインの適用を論じるという点からいって、特別に記載しておく必要性は高いといえよう。また、各省庁において、このような国際的な視野を前提にした記述として、上記プロバイダ責任制限法以外に、郵政省放送行政局監修「国境を越えるテレビ」（［平成５年］23 頁）、公取委事務局編「独禁法渉外問題研究会報告書」［平成２年］97 頁以下）、通商産業省政策局「1995 年版不公正貿易報告書」［平成７年］279 頁以下）があるとされ

[2] 「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律－逐条解説－」（http://www.soumu.go.jp/joho_tsusin/chikujyokaisetu.pdf）の参照には、「１　渉外的法律関係における本法律の適用および裁判管轄」の記載がある。この記載自体、立法管轄の問題としての認識が弱い点があるが、それはさておき、ネットワーク関係の法律について、このような立法管轄が問題になるとの意識が明確に示されている点は、きわめて注目に値する。

ており、むしろ、このような国際的な視点と告示・ガイドラインの適用というのは、重要な視角であると考えられる。

　では、次に、適用範囲の記載を行うとした場合、具体的にどのような記載にするかである。まず、法理論的には、結果発生事実としてのセキュリティに対する脅威の発生・増加が我が国にあるということが、いわばこの告示・ガイドラインの適用の我が国との「連結点」になる。そして、この連結の程度が実質的であることが、この告示・ガイドラインの適用の有無を決めることになると思われる。問題は、これらの視点をどのような文言で表現するかということになる。刑法２条は、保護主義による刑法の適用として「第２条（すべての者の国外犯）　この法律は、日本国外において次に掲げる罪を犯したすべての者に適用する。」とし、例えば、「第七十七条から第七十九条まで（内乱、予備及び陰謀、内乱等幇助）の罪」などの罪をあげている。上述の考慮のもと、「基準に関する当事者が日本国外にいる場合であっても、脆弱性情報が日本国内のセキュリティに実質的に関連する限り、適用する」という方向性も一つの選択肢として考えることができる。

第3 脆弱性の意義と諸問題

１　序

脆弱性情報取扱い体制は、ソフトウエアやウェブアプリケーションの「脆弱性」について、対応の枠組みを定めようとするものである。従って、その「脆弱性」の意義がきわめて重要な意味をもつものとなる。

「欠点」や「脆弱性」が、セキュリティの問題の中で、きわめて重要な意義を有していることを明らかにした後に、ソフトウエアの提供の法的な意義がどのように位置づけられるかという点、そこでの「欠点」や「脆弱性」が法的にどのような意義をもつかという点、ウェブの利用によるサービスの提供の意義について、事前の問題として検討しておくことは有意義である。

２　脆弱性の意義

「脆弱性」という用語が法的にどのように位置づけられるかという点について、比較法的に見ても、我が国の法的な判決例などからしても、明らかにはなっていないことは、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の「『セキュリティホールに関する法律の諸外国調査』報告書」（以下、第１報告書[3]という）からも明らかである。また、この点に関して契約書中に定義規定を設ける例もあまりないのが現状である。

まず、我が国の法律との関係でいえば、判決文の中では、意図した結果をもたらさない状態を表現する用語として「欠陥」という用語が用いられている。また、研究の中では、「不具合」という表現を用いて、これを「プログラムが意図した（正しい）結果をもたらさない状態」と定義するものもある[4]。一方、ＪＩＳでは、「障害」という用語のもとに論じられており、「障害」は「要求された機能単位が遂行できなくなる偶発的条件」と定義されている。また、参考になる概念として、製造物責任法２条２項において、「『欠陥』とは、当該製造物の特性、その通常予見される使用形態、その製造業者等が当該製造物を引き渡した時期その他の当該製造物に係る事情を考慮して、当該製造物が通常有すべき安全性を欠いていることをいう。」と定義されているところでもある。

この点について、もし、「脆弱性」を定義するとすれば、以下のような要素から定義をすることが可能であろう。すなわち、（１）不具合であること－プログラム等が意図した（正しい）結果をもたらさない状態であること[5]（２）セキュリティに関すること

---

[3] http://www.meti.go.jp/policy/netsecurity/Security_Reports.htm

[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）３頁

[5] なお、（注 4）「ソフトウエアの不具合・バグ・瑕疵に関する調査研究」は、「不具合」の検討について現象、原因、対応、分析により整理することが有用であるとしている。

ー少なくとも、その「不具合」が、電子計算機の運用に関する機密性、保全性、可用性に関連するものであること、（３）（１）の不具合が、外部からの攻撃を誘引するものであること（４）（２）および（３）に関連する（１）を引き起こす要因または事項であることの４つ観点が必要となるものと思われる。

なお、ここで「プログラム等」として、「等」の文字を含んでいるが、これは、製品としてのソフトウエア、ウェブアプリケーションシステムなどに限らず、有体物たる製造物、プロトコルなどをも含む趣旨である。

なお、「欠陥」や「脆弱性」という用語については、マイクロソフト日本法人においては、「製品の適切な仕様による場合でも、攻撃者によるユーザシステムに対する特権の不正行使、操作の資源、システム上のデータの損傷、および許可されていない信頼の偽装を防止不能にする、製品に含まれる問題である」としている[6]。これは、設計と違った機能や性能を指す、いわゆる「欠陥」から「脆弱性」を峻別し、設計の時点でわからなかった弱点を、製品出荷後に悪意のある人が悪意のある方法で見つける[7]という意味で、脆弱性の特質を強調するものといえる。原因について考慮することは、脆弱性に対する修補義務の範囲という観点からは重要な意味を持ってくることになるし、また、「脆弱性」の特殊性を指摘するものとしては、きわめて重要である。しかしながら、セキュリティに欠ける状態についての情報の取扱いという観点からは、原因自体から峻別することに意味はない。本報告書では、現象面を示す「脆弱性」という用語について、原因面から考慮した用語法は、もちいないこととする。

３　ソフトウエアの提供と「脆弱性」に対する修補の法的位置づけ

3.1.　ソフトウエアの概念と開発の概念

ソフトウエアは、「データ処理システムの運用に関係する計算機プログラム、手順規則およびそれらに関する文書」と定義されている（JIS）。また、種類としては、ハードウエアの形態別から分ける場合、分野別に分ける場合などがある。

また、「ソフトウエアの開発」とは、ユーザの要求に応じソフトウエアを実現する過程をいうと定義される。これは、ユーザの要求を認識し、仕様を定め、プログラムを作成し、提供、検収、保守する過程として認識するものである。なお、参考になる概念として製造物責任法における「製造」や「加工」がある。「製造」とは、製品の設計、加工、検査、表示を含む一連の行為として位置づけられ、「原材料に手を加えて新たな物品を作り出すこと。生産よりは、狭い概念で、いわゆる第二次産業にかかる生産行為を

[6] http://www.microsoft.com/japan/technet/columns/security/essays/vulnrbl.asp?frame=true

[7] 「マイクロソフト、脆弱性報告の日本語受付窓口を開設」
http://enterprise.watch.impress.co.jp/cda/security/2004/02/25/1483.html におけるマイクロソフト日本支社チーフセキュリティアドバイザー東貴彦氏のインタビュー記事による

差し、一次産品の算出、サービスの提供には用いられない」とされている。また、「加工」については、「動産を材料としてこれに工作を加え、その本質は、保持させつつ新しい属性を付加し、価値を加えること」とされている。この「製造」や「加工」で念頭におかれている過程が、ソフトウエアに適用される場合に、「開発」と認識されると考えることができる。この結果、ソフトウエアの「開発者」といった場合は、「ユーザの要求に応じソフトウエアを実現すべくプログラム等の作成処理、既存のソフトウエアへの改良処理等をなす者」をいうと定義することが可能になる。

この過程の中で、法的な意義として注目すべきことは、プログラムの作成行為ということになる。「プログラム」については、著作権法２条１項１０号の２で「電子計算機を機能させて一の結果を得ることができるようにこれに対する指令を組み合わせたものとして表現したものをいう」と定義がなされている（なお、特許法２条４項では「電子計算機に対する指令であって、一の結果を得ることができるように組み合わされたものをいう」と定義されている）。誰が著作者かという問題については、多くのケースでは、法人の発意に基づいて従業員が作成することになるため、法人著作（著作権法１５条２項）とされ、会社が開発者と認識されることになる。一方、稀なケースではあるが、勤務規則等において法人著作の形をとっていない結果、個々のプログラムの著作者は個々の開発者（被用者）であるが、財産権としての著作権（特に複製権、公衆送信権、譲渡権、翻案権）は、雇用者が取得するという過程を経て、雇用者である会社からプログラムが販売供与される場合にも、やはり会社が開発者として認識されるということになるのであろう。

ここで、上記において「開発者」を「ユーザの要求に応じソフトウエアを実現すべくプログラム等の作成処理、既存のソフトウエアへの改良処理等をなす者」と定義することができたとしても、具体的に脆弱性の修補の関係で、どのような者を「開発者」もしくは、それと同視すべきかという問題がある。これについては、修補の意義付けについての考察をなした後で述べることとする。

3.2.　ソフトウエアの提供行為の意義

一般にソフトウエアの提供行為は、ユーザと開発者側とのライセンス契約の概念で捉えられる。すなわち、ソフトウエアは著作権法上の保護を受ける（特許権が成立している場合は特許法の保護も受ける）が、著作権法のみで規律されるものではなく、ソフトウエアの使用に関し、ライセンス契約が締結され、ライセンサー（ベンダ）がライセンシー（ユーザ）に対し、ライセンス契約の範囲内でソフトウエアの使用を許諾するのが通常である。ライセンス契約の具体的な内容（ライセンス条件）をどのようなものにするかは、私的自治の原則、契約自由の原則により、基本的には契約当事者間に委ねられているが、強行法規に反する内容に関しては、無効となる。

なお、製造物責任法２条１項は、製造物につき、「製造又は加工された動産をいう」と定義しており、ソフトウエアは無体物であるため、ソフトウエアのライセンス契約において、製造物責任法の問題は生じない。もっとも、この製造物責任法の解釈にあたっては、ソフトウエアがチップのファームウエア等に書き込まれて、一体化している場合には、この限りではない。「逐条解説　製造物責任法」[8]においては、「ソフトウェア自体については、無体物であり、製造物責任の対象とはしていない。ただし、ソフトウェアを組み込んだ製造物については、本法の対象と返される場合がありうる。ソフトウェアの不具合が原因でソフトウェアを組み込んだ製造物による事故が発生した場合、ソフトウェアの不具合が当該製造物自体の欠陥と解されることがあり、この場合、その欠陥と損害との間に因果関係が認められるときには、当該製造物の製造業者に本法に基づく損害賠償責任が生ずる」と記載されている[9]。また、これに関連して、ソフトウエアがプレインストールされたコンピュータ（ないし、コンピュータとソフトウエアがセット販売され、ユーザがこれをインストールする場合）において、ソフトウエアの不具合による事故が発生した場合の問題や、ソフトウエアが CD-ROM 等の記録媒体に記録されて販売されている場合の問題が論じられている。前者のケースでは、プレインストール（インストール）された時点で製造物の一部となり製造物責任法の対象となるとする説やソフトウエアとコンピュータのメーカが同一の場合に限って製造物責任法の対象となるとする説が存在するが、後者のケースでは、記録媒体は単なる容器に過ぎないという観点から、製造物責任法の対象とはならないと一般的に解されている。

3.3.　脆弱性についての修補の意義付け

では、上記のような脆弱性について、そのプログラム等の提供者は、それを「脆弱性」のない状態にまで修補すべき義務があるのか、また、あるとした場合に、それは法的にどのように位置づけられるのかという問題がある。

まず、この点については、「脆弱性」が、どのようなことに起因しているのかという観点から考えることができる。ここで、製造物責任法をめぐる議論が参考になる。製造物責任法における責任の要件としての「欠陥」には、製造上の欠陥、設計上の欠陥、指示・警告上の欠陥の３類型があるとされている。製造上の欠陥とは、製造物の製造過程で粗悪な材料が混入した、製造物の組み立てに誤りがあったなどの原因により、製造物が設計、仕様通りに作られず、安全性を欠く場合をいうとされている。設計上の欠陥とは、設計自体に十分に安全性に配慮しなかったために、製造物が安全性を欠く結果とな

[8] 経済企画庁　国民生活局消費者行政第一課「逐条解説　製造物責任法」（社団法人商事法務研究会、1994）59 頁

[9] なお、通商産業省産業政策局消費経済課 編・「製造物責任法の解説」（財団法人通商産業調査会、1994）67 頁においては、「なお、最近の電気製品や機械はソフトウェアによる制御を行うものが多いが、このようなソフトウェアを組み込んだ製造物については本法の対象と返され、ソフトウェアの不具合が、当該製造物自体の欠陥と解される場合がありうる。」と記載がなされている。

った場合をいうとされる。指示・警告上の欠陥とは、有用性ないし、効用との関係で除去しえない危険性が存在する製造物について、その危険性の発現による事故を消費者側で防止、回避するための適切な情報を製造業者が与えなかった場合のことをいうとされている。そして、これらの「欠陥」は、この製造業者の帰責根拠が「欠陥のある製造物を製造し、他人に引き渡したことにある」ため、判断基準となる時点は、製造業者が当該製造物を引き渡した時点であるとされている。

これらの具体的な原因から生じる「脆弱性」について、プログラム等の提供側の契約当事者がどのような修補等の義務を負うのかという点については、上述の製造物責任法の規定を参考にして、場合にわけて論じることができる。

「脆弱性」については、まず、上述の製造物責任法の「欠陥」概念の基準時をめぐる概念でも指摘されているが、その要因が、ソフトウエアの提供時において通常備えられている「セキュリティ」を欠いているかどうかということが一つのポイントとなる。この「セキュリティ」を欠いているかどうかは、設計上、開発上、指示・警告上の各観点から、当該ソフトウエアの特性、通常予見される使用形態、開発者等が当該ソフトウエアを提供した時期その他の当該ソフトウエアに係る事情を考慮して判断されることになる。ソフトウエアの提供時において通常備えられている「セキュリティ」の程度を備えていない場合には、開発者側とユーザ間の契約において、そのソフトウエアの提供行為は、債務の本旨に従った履行（民法４１５条）とはいえないのが一般である[10]と考えることができる。これに対して、提供時においては一定のセキュリティを備えていたにもかかわらず、後日欠点や脆弱性が判明した場合については別の考慮が要求されるものと考えられる。これらが、瑕疵担保責任（民法５７０条、５６６条、商法５２６条１項等）の対象となる瑕疵であるか否かという問題（瑕疵担保責任の対象となれば、瑕疵修補請求、代物請求、解除、損害賠償請求等の問題が生じることになる）に関しては、新たに判明する欠点や脆弱性のすべてを瑕疵担保責任の対象とするのは、開発者等にとって酷であり、妥当でないと思われる。これについては、後日のトラブルを未然に防止すべく、新たに判明する欠点や脆弱性に関しては瑕疵担保責任の対象外であることを契約上明記しておくべきであろう（勿論、以下に述べるとおり、本来瑕疵担保責任の対象となるべき欠点や脆弱性に関しても、「新たに判明した」という一点をもってすべて瑕疵担保責任の対象外とすることは消費者契約法上無効とされうる以上、契約上の表現には十分留意する必要がある）。

この点、実務上は、提供後の欠点や脆弱性に関しては、開発者等の保守義務の対象とし、これにより開発者等が対応していることが多い。これは、制定法上の義務（瑕疵担

[10] もっとも、セキュリティ上の問題についても保証しないとして開発すれば、その点について一定レベルを備えていなくても債務の本旨に従った利用ではある。

保責任に基づく瑕疵修補義務）というより、契約条項によって定められる保守義務の履行として行われているものとして認識されることになる。

3.4　修補に努めるべき者

上記では、契約関係にあるものを開発者側とユーザとして論じた。しかしながら、ソフトウエアの開発行為において、実際に契約の当事者でない場合にも、ソフトウエアの修補について努力すべき立場を認めて、それに関する脆弱性情報の取扱いについて、責任ある立場にあることを求めるべきではないかという論点がある。この点で参考になるのが製造物責任法２条３項の規定である。同項は、「この法律において「製造業者等」とは、次のいずれかに該当する者をいう。」として

「一　当該製造物を業として製造、加工又は輸入した者（以下単に「製造業者」という。）

二　自ら当該製造物の製造業者として当該製造物にその氏名、商号、商標その他の表示（以下「氏名等の表示」という。）をした者又は当該製造物にその製造業者と誤認させるような氏名等の表示をした者

三　前号に掲げる者のほか、当該製造物の製造、加工、輸入又は販売に係る形態その他の事情からみて、当該製造物にその実質的な製造業者と認めることができる氏名等の表示をした者」

と定義している。これは、これらに記載されている者が「危険責任」（危険を内在して製造物を製造又は加工したものが、その危険が実現した場合の賠償責任を負うべきである。）、「報奨責任」（製造者は利益追求行為を行っており、利益を上げる過程において、他人に損害を与えたことを根拠に賠償責任を負うべきである。）、「信頼責任」（自らの製品に対する消費者の信頼に反して、欠陥の製造物を製造し引き渡したことを根拠として賠償責任を負うべきである。）という観点から責任が認められるのが妥当であるという判断を内包するものである。

これらの観点をもとに考えるとき、「開発者等」という概念を準備し

「一　当該ソフトウエアを業として開発又は輸入した者（以下単に「開発業者」という。）

二　自ら当該ソフトウエアの開発業者として当該ソフトウエアにその氏名、商号、商標その他の表示（以下「氏名等の表示」という。）をした者又は当該ソフトウエアにその開発業者と誤認させるような氏名等の表示をした者

三　前号に掲げる者のほか、当該ソフトウエアの開発、輸入又は販売に係る形態その他の事情からみて、当該ソフトウエアにその実質的な開発業者と認めることができる氏名等の表示をした者」

と定義し、修補に努力すべき地位を認めるというのも一つの方向性である。

上述の考察をもとに、かつ、現代社会におけるセキュリティの重要性を考慮するとき、

（1）提供時において、設計上、開発上、指示・警告上の各観点から、「セキュリティ」を欠いている状態の場合（提供時における科学まだは技術に関する知見によって認識することができなかった場合を除く）、ソフトウエア提供契約の当事者は、それを修補するのが債務の本旨として求められているのが一般であること、また、開発者等においても、修補についての対策を取るのが望ましいと考えられること
（2）提供時において、設計上、開発上、指示・警告上の各観点から、「セキュリティ」を欠いているとは考えられない状態である場合、もしくは、提供時において、「セキュリティ」を欠いていたが、それが、提供時における科学まだは技術に関する知見によって認識することができなかった場合については、多くは開発者側の保守義務の履行として修補がなされること
がいえるものと思われる。

3.5. 修補の責任等についての特約の効力

ソフトウエアに関する何らかの不具合に関連して、「as　is」条項といわれる、欠点や脆弱性については責任を負わない旨の条項（具体的には、対象ソフトウエアに関し、一切の保証をしない旨の条項を指す）がライセンス契約において定められている場合があるが、そのような条項が法的に効力を有するのか、という問題がある。

上記問題点は、一般消費者とのライセンス契約の場合は、消費者契約法上の問題（同法８条は、事業者の債務不履行責任又は不法行為責任の全部免除条項、目的物の瑕疵に起因する損害賠償責任の全部免除条項は無効であると規定している）として検討する必要がある。その際、最初に、欠点や脆弱性を有するソフトウエアを提供したことが債務不履行や不法行為に該当するか否かが個々のケース毎に問題となってくることとなり、そこで過失がある場合に、その責任についての全部免除条項といえるかという問題になるのである。また、後日判明された欠点・脆弱性に関しても、ケースによっては、瑕疵担保責任の対象となる瑕疵と評価されることも想定でき、そのような場合においても、全部免除条項の問題は同様に生じることになる。その他、瑕疵担保責任の責任期間に関しても消費者契約法上の問題が生じる（民法上は瑕疵を知った時から１年間とされているため、これを短縮する契約は同法の問題が発生する）。

一方、債務不履行や不法行為の成否については、事業者同士のライセンス契約においても同様に問題となり、そこでは、欠点や脆弱性がどの程度のものなのか、提供ソフトウエアはライセンサーが保証しているソフトウエアの仕様に合致しているのか（欠点、脆弱性と仕様書との関係はどうなるのか）、完全なるソフトウエアの提供は不可能であり欠点や脆弱性が後日判明し得るということにつきライセンサーが十分な説明を行ったか等々の諸事情を総合的に判断し、故意過失の存否等につき検討することになる。

この他、実務上は、仕様書記載のとおりの動作をすることを保証する旨の条項を設ける例が多く、この場合、かかる条項をもっておよそすべての欠点、脆弱性についてライセンサーが免責されるのか、という問題もある。なお、事業者同士の契約においては、消費者契約法は適用されないため、全部免除条項に関する問題は生じないが、独禁法上の問題が生じうるところ[11]である。

[11] http://www.jisa.or.jp/activity/opnion/020131-j.html

第4 脆弱性情報発見・通知と契約法の問題

脆弱性の発見においては、リバース・エンジニアリングなどの手法が用いられることがありうる。この場合、この発見方法が、発見者とその対象となるソフトウエアの製造者との間の契約関係で、どのような評価を受けるかという問題がある。

１　リバース・エンジニアリング

まず、リバース・エンジニアリングについていえば、明確な定義は存在しないが、一般に、プログラムを解析し、オブジェクトコードをソースコードに変換することや、ソースコードからプログラムのアルゴリズムを抽出することをいう（得た情報を元に自社製品に利用することも含めて定義される場合もある）。

一般に、ライセンス契約においては、ソフトウエアの著作権を保護するために、このリバース・エンジニアリングを禁止する条項がおかれることがある。リバース・エンジニアリングに関しては、逆アセンブル、逆コンパイルといった解析の過程でプログラムの複製物が作成されることから、著作権侵害に該当するかという議論が従前よりなされており（なお、特許法６９条１項は、試験又は研究のための実施は特許権侵害とならない旨規定しており、特許法上は、リバース・エンジニアリングは許容される）、通説は、技術の研究・解析は技術の進歩に資するものであること等を理由に、著作権侵害性を否定する。そのため、ライセンサーはライセンス契約中にリバース・エンジニアリング禁止条項を設け、特約をもって対処しようとするが、当該条項の有効性に関しては、独占禁止法に抵触するのではないかとされている。この点、平成１４年３月２０日に公正取引委員会より公表された「ソフトウェアライセンス契約等に関する独占禁止法上の考え方－ソフトウェア独占禁止法に関する研究会中間報告書－」（以下、中間報告書という）においては、ソフトウエアの製品市場、技術市場におけるライセンシーの研究開発活動が阻害され、ハードウエアの製品市場等における公正な競争が阻害される場合には、不公正な取引方法（具体的には一般指定１３項拘束条件付取引）に該当し、リバース・エンジニアリングの禁止は違法になるとの見解が示されている。しかしながら、実務上リバース・エンジニアリングを禁止する条項を設ける例は多く、また、どのような禁止条項が違法で、どのような禁止条項が適法であるかという点については、未だ解釈が明確でない。

脆弱性発見の過程において、リバース・エンジニアリングが行われた場合に生じうる債務不履行責任の問題について考えるとき、大前提としての当該ライセンス契約上、リバース・エンジニアリングが禁止されているか否かが問題となる。禁止されていないのであれば、そもそも契約違反・債務不履行の問題は生じない。リバース・エンジニアリングが禁止されている契約の場合、当該条項の適法性が問題となるが、独禁法等の観点

から違法であると判断されるようなケースでは、リバース・エンジニアリング禁止条項は無効であるので、やはり契約違反・債務不履行の問題は生じないことになる。次に、リバース・エンジニアリング禁止条項が有効であると判断されるケースでは、契約違反・債務不履行の問題は生じうるが、単に受付窓口に脆弱性情報を報告したに過ぎない場合は、ライセンサーに何らの財産的損害は発生しておらず、損害賠償責任の問題も発生しないと思われる。

なお、ライセンス契約において違約金条項があるケースでは、損害の発生如何にかかわらず、違約金の支払義務が発生し、ライセンサーが違約金を請求する可能性もあり得るが、自己製品の脆弱性の報告を受けたような場合にまでライセンサーが違約金を請求するケースは稀であると考えられる。また、脆弱性の発見、検証という公益目的であることを考えると、脆弱性発見の過程においてリバース・エンジニアリングが行われた場合に生じうる債務不履行責任については、違法性がない、または、請求自体が権利濫用（民法１条３項）に該当する可能性があると解釈される余地がある。

脆弱性発見の過程とリバース・エンジニアリングの問題については、法的な解釈としては、種々の問題をはらむが、そのすべてにおいて未確定な状態であると判断せざるをえないであろう。

なお、これに関連して、脆弱性発見の過程において、単純なリバース・エンジニアリングではなく、技術的保護手段（コピーガードなど）を回避した上でリバース・エンジニアリングを行うことが想定できるが、この場合は著作権侵害（著作権法３０条１項２号）に該当することになるだろうし、ライセンス契約において技術的保護手段回避の禁止を定めている場合は、契約上の問題も生じることになる。

２　セキュリティ調査委託契約と脆弱性の公開

次に、ソフトウエアについて、ベンダが脆弱性情報の発表後に独立してセキュリティ調査会社にその脆弱性の調査を依頼したような場合に、調査会社がその脆弱性の情報を他に公開することは許されるかという問題がある。

このようなケースでは、ベンダと調査会社との間には、脆弱性調査に関する契約において、「調査の結果判明した脆弱性情報についてはベンダ以外の第三者には開示しない」ということが当然の前提事項となっているはずであり、調査会社がベンダの承諾を得ることなく脆弱性情報を公開等することは、契約の趣旨からそもそも許されないものと考えられる。この点、両者間の秘密保持契約の有無（ないし調査委託契約中における守秘義務条項の有無）といった事情は、ベンダが他社への開示・公開を積極的に許容する意思を有していたといったきわめて稀なケースを除いては、特段影響を与えないのではないと思われる。従って、原則として調査会社が脆弱性の情報を他に公開することは契約

違反、債務不履行の問題を生じさせる。

もっとも、その脆弱性の程度が重大で、人の生命身体に影響を及ぼし得る可能性や緊急性がある等の問題が発生し、かつベンダが漫然とこれを放置しているといった事情が認められるのであれば、上記とは別個の問題であると考えられる。この問題については、さらに検討を要する。

３　ライセンス契約、秘密保持契約と脆弱性の発見・公開

同種の問題として、ライセンスを受けているユーザが、ソフトウエアの脆弱性を発見し、ライセンサーの同意を得ないまま他社に通知したり、公開したりするとき、契約法などとの関係はどうなるかという問題がある。

事業者同士の契約の場合、ライセンス契約に先立って秘密保持契約を締結するケースが多いこと、ライセンス契約中に守秘義務条項が設けられていることも多いこと（これは個人ユーザとの契約でも同様に妥当する）から、脆弱性情報が秘密保持契約（ないしライセンス契約における守秘義務条項）上の「秘密情報」に該当するか否かを検討する必要がある。ただ、これについては、「秘密情報」の定義は一義的ではなく、個々の契約毎に異なるのが現状である。ごく大雑把にいうと、①契約に伴い知り、知り得る情報一切をいう、と秘密情報を広く定義するパターンと、②相手方が秘密と指定した情報に限る、と狭く定義するパターンに分かれ、秘密情報の媒体についても、紙や CD、フロッピーといった有形物に収められたものに限る場合と、口頭で伝えた情報など無形のものも含む場合とに分かれる。ここで、上記②のような定義を設けている秘密保持契約であれば、脆弱性情報は秘密情報には該当せず、秘密保持契約違反の問題はそもそも生じない。①の場合については、脆弱性情報が秘密情報に該当する可能性がある（①のパターンといえども、定義の仕方はさまざまである以上、該当しない場合も当然ありえる。なお、秘密保持義務の不当な拡張は独禁法上問題があると中間報告書に指摘されていることにも留意すべきである）ため、債務不履行責任が生ずる可能性がある（損害発生不発生の問題、違約金の問題等については上記記載事実がそのまま当てはまる）。

なお、秘密保持契約が締結されていなかったり、ライセンス契約上に守秘義務条項が設けられていなかったりするケースでは、脆弱性を発見するために種々の利用をすることがライセンス契約違反にあたる、ということは困難なように思われる。また、それによって得られた脆弱性情報の公開を禁止する趣旨を一般のライセンス契約に読み込むことは困難なように思われる。もっとも、後述のとおり、公開の態様によっては刑事上民事上の問題が発生する可能性もあることに留意すべきであろう。

次に、上記設例のように「権利主の同意を得ないままに他人に通知する」という事実と、特許権侵害、著作権侵害といった問題とは全く無関係であることに留意すべきであ

る。例えば、脆弱性発見過程において無許諾の複製物を作成しているような場合は（ただし、前述したように単純なリバース・エンジニアリングの過程で複製物が産出された場合は、著作権侵害の問題は生じない）、著作権侵害の問題が生じる（この場合、「他人への通知」の有無に関わらず著作権侵害の問題は生じる）が、そのような事実がないのであれば、基本的には特許権侵害、著作権侵害の問題は生じないと考えられる。

営業秘密の問題については、不正競争防止法が営業秘密開示等に関する諸類型を不正競争としており、脆弱性の開示が不正競争防止法上の不正競争に該当するか否かを検討する必要がある。不正競争防止法２条４項は、「営業秘密」について「秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないものをいう」と定義しており、当該定義により、①秘密管理性②非公知性③有用性、という営業秘密性の３要件が導かれる。ここで、脆弱性情報に関しては、ライセンサーは、ライセンシーなりその他の第三者なりから通知を受けて（ないし情報を公開されて）初めて当該脆弱性情報を認知するのが通常であって、そもそも脆弱性情報を秘密として管理しているわけではないため、①の要件を満たさず、不正競争防止法上の営業秘密には該当しないと思われる（従って、当然不正競争にも該当しない）。なお、ライセンサーが通知（公開・開示）前にすでに脆弱性情報を認知しており、これを秘密管理していたような場合は、①の要件を満たすことになるが、その場合は、当該脆弱性情報が③の有用性要件を満たすか否かが個別ケース毎に問題になる[12]。

４　公益通報者保護法による契約関係からの保護

この点については、従来から、内部告発による不利益を受けないような法手続きを整備し、いわば、内部告発者保護法を整備する必要があるとされていたが、公益通報者保護法が平成１６年３月９日第１５９回通常国会に提案されている[13]。この法案によれば、「公益通報」とは、「労働者が」「不正の目的でなく」「その労務提供先又はその役員、従業員等について」「通報対象事実が生じ、又は生じようとしている旨を」（１）勤務先などへの「内部通報」（２）「行政機関への通報」（３）マスコミや消費者団体などへの「外部通報」をする場合をいうとされている。通報対象事実は、刑法、独禁法、食品衛生法、証券取引法等の違反行為が予定されている。労働者がこれらを満たし告発をした場合に、告発を理由とした解雇や派遣契約の解除を無効とし、降格や減給などの不利益

[12] 田村善之「不正競争防止法概説［第２版］」336 頁は、「…新薬開発過程において効能、副作用等の点で結局医薬品たりえないことがわかった化合物に関する研究データなど、いわゆるネガティブ・インフォメーションも、このような情報を入手した者が労力、時間、費用を節約できることは明らかであるから、有用性の要件を満足すると解すべきである。」とするが、ソフトウエアに関する脆弱性情報がここでいうネガティブ・インフォメーションに該当するか否かは十分検討する必要がある。

[13] 法案については、http://www.consumer.go.jp/kankeihourei/koueki/kouekian.pdf なお、議事録等については、http://www.consumer.go.jp/info/shingikai/koueki-index.html

な扱いなども禁止するという趣旨のものである。この法案は、労働者（雇用者の指揮命令関係にある者をいう）に対してのみ適用されることを念頭においている。

脆弱性情報取扱い体制と関連する例として、製品が発表されたのちに、ベンダが、独立したセキュリティ調査会社に対して脆弱性調査を依頼した際に、調査の結果重大な脆弱性が発覚した場合を考えることができる。この場合、本件の脆弱性情報取扱い体制に基づき報告したとしても、それを理由とするベンダとセキュリティ調査会社との間の契約解除、損害賠償請求などに対しては、この法案では保護が及ばないことになる。また、ベンダが報告を受けたのにもかかわらず放置して対応しないために、ベンダの従業員がこれを公益のために通報するといったケースも想定できるが、この場合も「脆弱性を放置する」あるいは「自社の脆弱性を公開しない」ことは現状特に法令違反にならないため、当然公益通報者保護法上でも「別表」に掲げられておらず、法律の適用外になってしまうということになる。現在の法案では、脆弱性情報を公益目的から通報するという場合などについて適用されるというものではなく、その点からいって限界があるものといえる。

第5 脆弱性発見と不正アクセス、そして、届出の受理について

１　脆弱性発見と不正アクセス

（1）不正アクセス禁止法の一般的立場

特定のウェブアプリケーションの脆弱性が報告されている場合に、その情報を利用、または、応用して、他のウェブアプリケーションに同種の脆弱性が存在するかどうか確かめることが、不正アクセスに該当するのではないかという論点がある。

不正アクセスについての我が国における法的な対応としては、「不正アクセス禁止法」がある。同法により規制される「不正アクセス行為」の法的な意義としては、「他人の識別符号を入力して」または、「特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して」「アクセス制御機能により制限されている特定利用をし得る状態にさせる行為」（不正アクセス禁止法３条）である。我が国の法制度においては、電気通信回線を通じた無権限アクセスを禁止しようとするもので、スタンドアロンコンピュータに対するアクセスを禁止していない点[14]、また、特別の安全措置を要求しない点に特徴がある。脆弱性に対する問題との関係で意識しておくべきことは、故意犯であり、自己の行為が、「特定利用をし得る状態にさせる」という認識があれば、犯罪は成立するということである。その一方で、ファイルの改竄であるとか、情報の取得、漏洩などといった行為をなすとかの特定の目的などといったものは必要ではないこととなる。

この法律の適用に関し、いわゆる脆弱性を利用するタイプの不正アクセス行為については、アクセス制御機能の回避をしたといえるかどうかが、犯罪の成否を決める鍵になる。しかし、その回避といえるかどうかの判断については、脆弱性の種類および攻撃手法との関係でさらに困難な問題がある。この点については（２）の具体的な適用について検討する。

この点については、まず、そのような行為が、不正アクセスの「特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して」、「アクセス制御機能により制限されている特定利用をし得る状態にさせる行為」に該当するかどうかということがある。この定義に該当すれば、不正アクセス罪は成立すると解せられる。不正アクセス禁止法の規定によれば、その主観的なものとしては、特定利用をし得る状態にさせる行為をしているという認識があれば、犯罪は成立すると考えられる。その行為において、脆弱性の情報の検証をするためというような意図があったとしても、犯罪の成否には関係はない。また、この法律の制定の当時において、すでに、脆弱性の

[14] なお、サイバー犯罪条約においては、スタンドアロンコンピュータに対する犯罪についても処罰対象としている点に注意が必要である。

検証などが違法となるのではないかという議論があったにもかかわらず、そのような意図の有無を考慮せずに犯罪が成立することを当然としている[15]のであり、そのような立法の経緯からも、脆弱性の検証の意図が犯罪の成否に影響を与えるものとは思えない。また、同様な趣旨からして、正当業務行為などの見地から、違法性が阻却されると考えることは、困難であろう。

（2）具体的な適用について

脆弱性の種類および攻撃手法に関連して、不正アクセス禁止法の構成要件のうち、いわゆるセキュリティホール攻撃型についてみていくことにする。

同法３条２項３号が、主としてセキュリティホールを利用して攻撃する方法を想定した規定とされている[16]。この規定の趣旨については、「その立法趣旨は、誰が使っているかわからないようにすることがいけないという観点からの規制ですので、なりすまし型のみを、他人の ID・パスワードの盗用型のみを規制して、セキュリティホール攻撃型を規制しないというのは、規制のバランスを失するだろうということで２号と３号の規定をしたというのが第一の理由です。」と言われている[17]。そして、技術的に十分対処できるのであれば、わざわざ処罰する必要は無いのではないかという議論については、「実際いろんな方にお話を伺いましたが、セキュリティホールをゼロにしていくというのは技術的になかなか難しく、やはりいたちごっこになるだろうということでした。日々、新しいセキュリティホールが発見されている中、技術対策を講じ得るものは公表されますが、そうでないもの多数まだ闇に葬られているわけですので、そういうものをハッカーが探知しては攻撃してくる。解決策が見つからないままのものも結構放置されている現状からすると、やはり２号と３号を規定しないと、まだまだ不正アクセス対策としては十分ではないのではないかということから、これを規定したというのが立法の趣旨背景です。」と説明がなされている。

---

[15] 「現代刑事法その理論と実務」１９９９年１２月（第８号）（特集「ハイテク犯罪の現在」）の園田寿、牧野二郎、露木康浩、前田雅英の「ハイテク社会と刑事法」座談会における議論でもこの点はあきらかである。園田寿教授は、「やはり今回の特徴というのは単なるハッキングが処罰対象になったということですよね。ハッキングに対して脅威を感じるかどうかというのは、ハッキングの発展段階であるクラッキングですね、ファイルの改竄とか消去とか、そこまでいく可能性があるから脅威を感じるんだろうと思うんです。」と発言しているし、露木康浩氏は、「インターネットが犯罪の巣窟になったりしないようにしようという環境設定という観点から規定したものなんです。他方で、この電気通信の秩序の維持という概念の意味ですが、これは個人個人、それぞれハッキングを受けたときにどう感じるかということになるかもしれなせんけれども、基本的なみんなハッキングを受けたくないと思っている。ハッキングを受けるようなネットワークがそんな接続はやめようということになる。ネットワーク接続に対する抑止力が働くと、高度情報社会というものが発展しなくなりますから、そういう意味でみんなが嫌がる行為が行われないような秩序、ネットワークに繋げたくなくなる行為が行われないような秩序を維持するという意味でこの概念を用いています。保護法益という言葉がいいかどうかわからないですが、この二つの要素が、規制の趣旨だということです。」と発言している。

[16] 前出（注 10）露木発言 18 頁によれば、「もっとも、例えばクラッカー、ハッカーが、パスワードファイルに、勝手にバックドアのような架空の ID、パスワードを追加してそれを使ってしまうという場合がありますが、これも２号に該当します。」とされている。

[17] 以下、本項の発言については、前出（注 11）露木発言 18 頁および 19 頁

ここで、問題になってくるのが、１号の「アクセス制御機能を有する特定電子計算機」という概念が、どの程度のセキュリティシステムを意味するのか、あるいはどの程度の強さの管理をいうのかという問題である。この点については、「実際はセキュリティホールがあって、ID・パスワード以外の情報なり指令なりを入力すると使えてしまうということがあり得るわけで、ID・パスワードを入れないと絶対に使えないというところまでアクセス制御機能の点にとして要求すると、ほとんどのシステムが対象外になってしまいますから、そこはある程度緩和せざるを得ないんです。では、どの程度セキュリティホールが残っているものが救われるのかというのは、これはなかなか、実際のユースのレベルに応じて判断していかざるを得ないので、法律で具体的に書き切るのは、ちょっと無理があります。『特定利用の制限の全部または一部を解除する』の『制限』という言葉は、ID・パスワードを入れないと利用制限が解除されないという意味で使っているんですが、この『制限』とは普通は、そこは使えない、そこを使うことは社会通念上認められていないといえるという場合です。」と説明がなされている。結局、技術的な観点よりも社会通念という観点が入って来ざるを得ないということになる。

抽象論としては以上のようなことがいえるとして、問題は、社会通念上、アクセス制御がなされているというのはどういう場合かということになる。この点については、個別具体的なアクセス手法ごとに判断される要素が異なると考えられる。

２　先行行為の他の行為への影響

次に、そのような違法行為に密接に関連する脆弱性情報に対して、どのような取扱いをなすべきかという問題がでてくる。ただし、この点については、そのような脆弱性情報自体と、その発見過程での違法行為という要素とは、別個の問題といえるものと考えられる。いわば、先行行為の問題点が、どのように後行行為に影響するかという問題点である。この点についての法的な思考を補助するために、やや詳細ではあるが、いわゆる違法収集証拠の論点を参考にすることとする。

「脆弱性」や「安全性の欠如」に関する情報が一定の行為によって取得された場合に、その行為が違法であった場合には、届出機関は、その取得された情報について受け付けないとしなければならないのではないかという観点がある。

これについて、一つの思考の参考となるのが、いわゆる違法収集証拠の排除法則についての議論である。最高裁判所は、警察官が職務質問の際、被告人の上衣の内ポケットに手をいれて在中物を取り出したところ、覚醒剤だったので差し押さえたという事案について「違法に収集された証拠物の証拠能力については、憲法及び刑訴法になんらの規定もおかれていないので、この問題は、刑訴法の解釈に委ねられているものと解するのが相当であるところ、刑訴法は、「刑事事件につき、公共の福祉の維持と個人の基本的

人権の保障とを全うしつつ、事案の真相を明らかにし、刑罰法令を適正且つ迅速に適用実現することを目的とする。」（同法１条）ものであるから、違法に収集された証拠物の証拠能力に関しても、かかる見地からの検討を要するものと考えられる。ところで、刑罰法令を適正に適用実現し、公の秩序を維持することは、刑事訴訟の重要な任務であり、そのためには事案の真相をできる限り明らかにすることが必要であることはいうまでもないところ、証拠物は押収手続が違法であっても、物それ自体の性質・形状に変異をきたすことはなく、その存在・形状等に関する価値に変りのないことなど証拠物の証拠としての性格にかんがみると、その押収手続に違法があるとして直ちにその証拠能力を否定することは、事案の真相の究明に資するゆえんではなく、相当でないというべきである。しかし、他面において、事案の真相の究明も、個人の基本的人権の保障を全うしつつ、適正な手続のもとでされなければならないものであり、ことに憲法３５条が、憲法３３条の場合及び令状による場合を除き、住居の不可侵、捜索及び押収を受けることのない権利を保障し、これを受けて刑訴法が捜索及び押収等につき厳格な規定を設けていること、また、憲法３１条が法の適正な手続を保障していること等にかんがみると、証拠物の押収等の手続に、憲法３５条及びこれを受けた刑訴法２１８条１項等の所期する令状主義の精神を没却するような重大な違法があり、これを証拠として許容することが、将来における違法な捜査の抑制の見地からして相当でないと認められる場合においては、その証拠能力は否定されるものと解すべきである。」と判断している（最判昭和５３年９月７日）。

この判決を前提として、「違法の重大性」の要件と「排除相当性」の要件の二つの見地から排除の妥当性が検討されている。そして、特に「排除相当性」の要件は、「排除が必要であり、妥当（有効）だ」ということであるが、この具体的な内容をもとに個別の争いがあることになる。なお、私人による証拠の収集については、この理論の適用としては、排除の必要はないということになるが、捜査の一環と評価できる場合や違法の程度が著大で公正さを容認できない例外的な場合は、裁量的な排除の対象となるとされている。

これらをもとに脆弱性情報取扱体制を考えるとき、情報発見者が違法性を有する行為をしているに過ぎず、収集機関は直接違法性を有する行為をしていないという点で、情報収集機関が違法性をなしていた違法収集証拠の場合との違いを指摘することはできる。しかし、脆弱性情報取扱において、発見者が希望すればその発見者の名前をふして公開するという体制を考慮している以上、違法な発見による脆弱性情報等の取得に対しては、違法な行為の抑止という観点から、それが明らかである場合、やはり届出を受け付けないことがあるとすることが妥当である。

なおこの点については、WG の価値判断とは異なるが、研究会内部においては「このガイドラインが国際的にも注視されるであろうことは明白なため、日本国最高裁の判断

基準よりも若干厳しい基準に従ったほうがよい。その前提の上で、このスキームでは、違法に獲得された情報であっても受け付けて差し支えないのではないか。ただし、『提供された情報を受け付けたことによって、違法な取得行為に対する法的責任が免責されるものではない』旨を明記するのが良い。」という趣旨の意見もあった。

第6 脆弱性発見・公開者と攻撃者によるセキュリティ侵害に対する不法行為

ソフトウエアの脆弱性を発見したものが、自ら、セキュリティを侵害する行為をなさなかったとしても、しかるべき取扱い基準を満たさない方法でその情報を公開した場合、そのような行為は、どのような評価を受けるべきかという問題がある。

１　脆弱性の公開と表現の自由

憲法２１条の「集会・結社・表現の自由、検閲の禁止、通信の秘密」は、その第１項において、「集会、結社、および言論、出版その他一切の表現の自由は、これを保障する」としている。いうまでもなく、コンピュータネットワークにおける脆弱性の情報についても、その情報自体を発表することは、表現の自由として、憲法上、保護されるべき権利として尊重に値するということがいえるであろう。また、脆弱性情報についていえば、従来の、いわば完全開示の根拠として、（１）悪意ある攻撃者は脆弱性情報をすでに知っているため、攻撃者のテクニックをすべての人が知りうるのがベストである（２）ベンダは、脆弱性情報がひとたび公開されてしまえば、脆弱性についてのバグを隠すことはできない（３）脆弱性の情報を公開することは、将来におけるよりよいシステムをつくるために必要である（４）脆弱性情報は発見者の自身の財産である、という積極的な意味づけをもつ。これに対して、脆弱性情報について「責任ある開示」の体制を構築すべきという立場から反論がなされていくことは、第１報告書の別紙で詳細に述べたところである。

脆弱性情報の開示についてのルール制定においては、このような表現の自由との衝突という観点からも問題になりうる点について留意が必要である。

２　脆弱性情報・開示の態様等と開示者の法的位置づけ

脆弱性情報の開示について何らかのルールが必要とされるとして、その場合、そのような情報は、どのようなものとして位置づけられるのかという問題がある。表現の自由といえども、公共の福祉から制限されるということもあるし、また、内在的な制約に服するといわれることもあり、それ自体無制限ではない。加えて、脆弱性情報の公開については、いわゆるスクリプトキディを利するのみでなんらセキュリティに対して肯定的な影響を与えていないのではないかという指摘もある。このような観点から、表現の自

由との衝突が起こりうる場合として、攻撃コードの作成とその援助の観点、名誉毀損の表現、風評被害を与える場合[18]などを問題として検討する必要がある。

３　攻撃コードとその作成を容易にする行為

攻撃コードまたは脆弱性を「利用するコード」（exploit code）という概念が有るが、脆弱性の情報の取扱いを考えるときに、その情報を悪用して攻撃コードが考えられ、攻撃に使用されることになる。より、一般的に用いられている概念としては、コンピュータウイルスがあるが、「コンピュータウイルス対策基準」（通商産業省告示第９５２号）２（１）においては、コンピュータウイルス自体は「第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、 次の機能を一つ以上有するもの。(1)自己伝染機能 （略）(2)潜伏機能 （略） (3)発病機能（略）」と定義されている。この定義と比較した場合に、特に脆弱性を悪用したものを、ここで「攻撃コード」といっていることになる。しかしながら、攻撃コードにおいては、特に伝染機能を有せず情報を漏洩するのみであるという場合も十分考えられるため、上記三つの機能が必要だというわけではなく、「攻撃コード」という概念は、きわめて広いものということになる。

法的な観点から、「攻撃コード」の問題を考えるときには、サイバー犯罪条約の４条の「データの妨害」の規定（「権利なく、意図的に、コンピュータ・データの毀損、消去、劣化、改変又は排除」をなすプログラム等の一部）および６条「装置の濫用」（Misuse of devices）の規定（「第２条ないし第５条により設けられる犯罪のいずれかを実行することを目的として設計又は採用されたコンピュータ・プログラムを含むデバイス」）として位置づけられることになる。また、我が国においては、「人の電子計算機における実行の用に供する目的で、人の使用する電子計算機についてその意図に沿うべき動作をさせず、又はその意図に反する動作をさせる不正な指令に係る電磁的記録その他の記録を作成し、又は提供した者」を「不正指令電磁的記録等作成等の罪」（刑法１６８条の２第１項）として処罰するべく法律改正が準備されている。

なお、攻撃コードの実行については、上記の「不正指令電磁的記録等作成等の罪」の適用のみが問題となるものではない。適用の可能性としては、①偽計業務妨害罪（刑法２３３条）（または刑法２３４条の威力業務妨害罪）②電子計算機損壊等業務妨害罪（刑法２３４条の２）および③器物損壊罪（刑法２６１条）がある。①偽計業務妨害罪・威力業務妨害罪の構成要件は、(1)偽計を用いて（または威力を用いて）(2)「業務」を(3)妨害したことであり、②電子計算機損壊等業務妨害罪の構成要件は、 (1)電子計算機に

[18] 商品やサービス自体には何ら問題がないにも関わらず，それらが忌避されることにより，経済的に壊滅的な損害を与える場合をいう。また、この点については、最判平成 15 年 10 月 16 日のいわゆる所沢ダイオキシン報道事件をめぐる一連の判決例が参考になる。

向けられた加害行為、(2)電子計算機の動作阻害 (3)業務妨害 の３つである。この二つの犯罪の相違は、電子計算機損壊等業務妨害罪が、きわめて法定刑が重いということである。この二つの規定の適用関係については、争いがある。一つは、法は電子計算機に直接向けられた加害行為による業務妨害と人に対する業務妨害を峻別し、電子計算機に対する加害行為については、電子計算機損壊等業務妨害罪の成立のみを考えるという立場である。いま一つは、そのような峻別は、可能とは思えないので、電子計算機に対する加害行為についても一般の業務妨害罪は成立するが、一般の業務妨害のうち、特に「電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせて」（以下、動作阻害という）という中間結果を発生させる場合について、特に刑罰を重く定めた規定であるというものである。本報告書の立場は、後者の立場を前提に考えるものである。動作阻害とは、「使用目的に沿うべき動作をさせず」もしくは「使用目的に反する動作をさせる」ことをいうとされており、その例示として、加害行為によりシステムダウンを引き起こした場合や電子計算機に指令を与えて三角形を作ろうとしていたのに出てきた製品が四角形になった場合をいうと説明[19]されている。この「動作阻害」という中間結果がきわめて重大である点から、一般の業務妨害罪と比較して刑罰が重くなっているものと思われる。したがって、この電子計算機損壊等業務妨害罪は、ホームページ内の画像をわいせつな画像に置き換えたという事案に対して適用するのはともかくとして、現在よく流布されているコンピュータウイルスに対して適用するのは、困難であるように思える。また、業務妨害の立証の問題からか、通常の業務妨害罪についても、コンピュータウイルスの作成・投与に対して、これを適用するというのは容易ではないようである。また、③の器物損壊罪については、「記録媒体の効用というものはそこに記録されている特定の情報を保存することにあり、記録媒体に記録された特定の情報をほしいままに破壊、消去、改竄することは」その効用を害しているので、コンピュータウイルスの作成・投与は、「入力されているデータと一体として認められる記憶媒体の効用を害していると考え」る[20]とするものである。しかしながら、このような形で効用が害されたとされるかは、議論の余地がある。

４　ウェブサイトにおける脆弱性の指摘と名誉毀損との関係について

現時点においては、ソフトウエアやウェブサイトの脆弱性の発見とその公開は、表現の自由の観点から十分に尊重に値するものと考えられる。仮にその情報の公開によってその情報を目にし、いわば、攻撃ツールを作製し、または、利用したものがいたとしても、特段の事情のないかぎり発見・公開者が、かかる攻撃行為を教唆したとか、容易に

[19] 的場・河村著「コンピュータ犯罪 Q&A」126 頁
[20] 岡田好史「ハッキング・クラッキングに対する刑事規制」現代刑事法第６巻１号 37 頁（現代法律出版、2004）

したということは、困難なのではないかと思われる（容易にしたといえるのであれば、刑事的には、従犯[21]の可能性があり、民事的には、共同不法行為[22]などの可能性がある）。

しかしながら、取扱い基準の実際の運用とそれが社会にどれだけ定着するかということは、このような評価を変える可能性がある。つまり、脆弱性情報を発見したものは、このような取扱い基準に従って行動しない場合、そのような攻撃ツールを作製し、セキュリティ侵害を行なうものによるサイトに対する攻撃を（抽象的にせよ）認識し、それでもかまわないとして、脆弱性情報を公開したのだという認定がなされる状況になりうる。いわば、脆弱性情報の取扱い分野における「デファクト・スタンダード」である。そうなれば、そのような攻撃を認容するかのような公開活動は、刑事的に、不正アクセス禁止法の従犯、業務妨害罪の従犯などの評価を受け得るし、被害者からの攻撃者に対する損害賠償請求訴訟において、共同不法行為としての責任の追求対象となることも十分に考慮しうるのである（もっとも、具体的な成否については、攻撃の蓋然性の高さや公開の動機なども関連して認定されるであろうから、そのような方向性も考えられ得るというにすぎない点は、留意が必要である）。

第7 脆弱性発見・公開者の行為による開発者に対する不法行為

１　名誉毀損との関係

脆弱性を発見され、通知されたソフトウエア会社が、例えば、そのような評価がもとで製品の売上げが低下した（もしくは、営業上の地位が損なわれた）として、発見・公開者に対して損害賠償請求を提起してきた場合や刑事事件として告訴してきた場合、発見・公開者の立場はどうかという問題がある。刑事的なものとして、最初に名誉毀損罪との関係について検討する。名誉棄損罪について、刑法２３０条１項は、「公然と事実を摘示し、人の名誉を毀損した者は、その事実の有無にかかわらず、３年以内の懲役若しくは禁錮又は５０万円以下の罰金に処する。」と規定している（条文上は「人の名誉」となっているが、法人等の団体も含むと解釈するのが通説判例である）。まず、単に第三者が当該企業に対してのみ脆弱性を通知したようなケースでは、そもそも「公然性」の要件を欠き、名誉毀損罪が成立する余地はない（公然性については、摘示された事実を不特定又は多数人が認識しうる状態をいうとするのが通説判例である。）。これに対し、例えばインターネットのホームページで脆弱性を公開するような場合は、公然性の要件は満たすため、名誉毀損罪が成立する余地がある。この場合、民事上も不法行為が成立し、損害賠償義務が発生することになる。

---

[21] 刑法６２条は、正犯を幇助して犯罪を容易にする場合を従犯として処罰しうることを明らかにしている。
[22] 民法７１９条２項は、教唆者と幇助者については、共同行為者とみなすとしている。

ただし、刑法２３０条の２は、公共の利害に関する場合の特例として、事実の摘示行為が、①公共の利害に関する事実に係り、②目的が専ら公益を図ることにあったと認める場合には、③事実の真否を判断し、真実であることの証明があったときは、これを罰しないと定めているため、上記①ないし③の要件を満たす場合は、処罰はされないことになる。①に関しては、対象ソフトウエアの性質、ユーザ数、マーケットシェア、脆弱性の程度等、②に関しては、開示者の開示意図が個々のケース毎に判断されることになろう。

２　信用毀損罪との関係

次に、信用毀損罪の成否についても併せて検討する。刑法２３３条は、「虚偽の風説を流布し、又は、偽計を用いて、人の信用を毀損」することをもって信用毀損罪の構成要件としているため、脆弱性情報が真実のものであれば、虚偽の風説の流布にも該当せず（「虚偽の風説を流布し」とは、客観的真実に反する情報を不特定又は多数の人に伝播させることをいう）、偽計にも該当しない（「偽計」とは、人を欺罔し、又は人の不知、錯誤を利用することをいう）ことになり、信用毀損罪は成立しない。なお、同様の理由により業務妨害罪の成立も否定されることになろう。

３　民事上の責任関係

また、民事的な責任追求という観点から検討した場合も、この点については、相当な検証などを経た上で脆弱性があると判断し、その脆弱性を発表することは、一般に表現の自由として許容されるべきものと考えられる。これは、脆弱性情報取扱い基準が存在しなくても同様なことがいえるものと思われるが、基準が存在することによって、さらにその情報の発見および取扱い基準に従った手順による公開の重要性が強調されることとなるであろう。かかる点について特段の定めがあるわけではないが、名誉毀損における事実の証明の規定と同様な利益状況にあり、同様の判断基準が適用されて、不法行為の成立要件の一つである違法性の解釈の中で、バランスがとられることになる可能性が高い。

第8 取扱い基準関与者自身の法律問題

１　法執行の要請との関係

このような体制は、法執行の要請との関係も問題になる。刑事訴訟法１０３条〔押収と公務上の秘密〕は、「公務員又は公務員であつた者が保管し、又は所持する物について、本人又は当該公務所から職務上の秘密に関するものであることを申し立てたときは、当該監督官庁の承諾がなければ、押収をすることはできない。但し、当該監督官庁は、国の重大な利益を害する場合を除いては、承諾を拒むことができない。」と定めている。ここで、「職務上の秘密」というのは「単に形式的に秘扱とせられたというにとどまらず、実質的にも職務上知ることのできた秘密に当たる」ものをいうことになる（国家公務員法１００条１項にいう「秘密」の意義につき判断した最決昭和５２年１２月１９日が参考になろう）。この脆弱性情報取扱い体制で IPA に収集される情報は、公開される情報以外については、上記の実質秘として保護されるべき「職務上の秘密」に該当する情報が多いものと思われる。

ところで、IPA に関連しては、「情報処理の促進に関する法律」１９条により「機構の役員及び職員は、刑法（明治四十年法律第四十五号）その他の罰則の適用については、法令により公務に従事する職員とみなす。」とされている。刑事訴訟法１０３条に規定する「公務員」については、「罰則適用についてのいわゆる『みなす公務員』は、もちろん、法例により公務に従事する職員とみなされる公務員についても消極（略）に解すべきであろう」とされている[23]。この結果、IPA に対する捜索・押収がなされれば、それによって、脆弱性情報発見に関係する情報や対策情報が収集されることになる。この場合、脆弱性発見に関係する情報や対策情報、そして、それに関する発見者との連絡に関する情報一切を刑事訴訟法上、何らかの形で秘密として捜索・押収等から保護すべきではないかという論点が存在しうる。

なお、この点については、米国におけるセキュリティインシデントに関する情報の政府との共有について、産業界が懸念していることの一つにも入っている点は、注目に値するであろう（本報告書４３頁）。

２　情報公開法との関係について

届出機関が IPA になるということは、IPA が情報公開法の対象（「独立行政法人等の保有する情報の公開に関する法律」）となるため、かかる届出情報がすべて情報公開の対象になるのではないかという問題がある。この問題に対しては、独立行政法人情報公開法５条において、一定の情報についての非開示が定められている。この脆弱性情報取

[23] 新版注釈刑事訴訟法［第２巻］（立花書房、1997）167 頁

扱い体制でIPAに収集される情報は、同条の「四　国の機関、独立行政法人等又は地方公共団体が行う事務又は事業に関する情報であって、公にすることにより、次に掲げるおそれその他当該事務又は事業の性質上、当該事務又は事業の適正な遂行に支障を及ぼすおそれがあるもの　」のうち、「ロ　犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序の維持に支障を及ぼすおそれ 」「ホ　調査研究に係る事務に関し、その公正かつ能率的な遂行を不当に阻害するおそれ 」などに該当するものと考えられる。もっともこの点については、詳細な検討[24]が必要である。

３　責任問題

また、取扱い基準として、従前から提案のあったスキームを採用する場合には、むしろ、そのスキームに中心的に関与する届出機関、分析機関の法的な地位に着目しなければならない。これらの届出機関・分析機関が十分なリソースを持ち、十分な検討ができるのかという実際上の問題が米国有識者から指摘されているところであり、また、分析機関がどのような形態をとるにせよ、法的な責任から免れる仕組みを採用する必要があるという指摘がなされた点は、念頭に置く必要がある。

また、IPAが、第三者にこの分析業務を委託するということになれば、その第三者の行為に対しても責任を負うのではないか、特にその第三者の過失について使用者責任（民法７１５条）を負うのではないかという問題がある。ここで、参考になるのは、個人情報保護法の規定である。個人情報保護法は、委託先の監督について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。」と定めている。また、宇治市の個人情報漏洩の事件においても、大阪高判平成１３年１２月２５日は、「 (2)　指揮・監督関係の有無について、ア　民法７１５条は,「或ル事業ノ為メニ他人ヲ使用スル者」は被用者が事業の執行につき第三者に加えた損害について賠償の責任を負うとしているから, 控訴人がその事業のために不法行為者Ｔを使用する関係にあることが必要である。そして, 使用者と被用者の関係があるかどうかについては, 実質的な指揮・監督関係の有無によって決するのが相当と解される。」として、実質的な指揮・監督関係を認めており、民法７１５条の使用者責任を認めている。一方で、この取扱い体制で分析機関として指定されている IPA が、第三者に指揮・命令関係を有しない形態で、この分析をゆだねることができるかという問題があり、仮に第三者に分析業務を委託する場合には、（民法７１５条の適用を前提に）十分な監督が必要になる。

[24] なお、米国でも情報公開との関係が問題になっている（本報告書４３頁）

第9 通信の秘密と脆弱性情報取扱い体制について

１　通信の秘密の概念

通信において、その秘密が維持されることはきわめて重要な利益である。セキュリティにおいても、ネットワーク通信の秘密は、通信の「信頼性」の一環をなすものとしてきわめて重要な一つの要素をなす。法的なものとして、我が国においては、「通信の秘密」の問題として位置づけられる。以下、脆弱性取扱いの観点として、通信の秘密の位置づけについて簡単に触れることとする。

憲法２１条２項後段は、「通信の秘密は、これを侵してはならない」と定めている。そして、「通信の秘密」の内容として、一般には「通信」の「秘密」にかかる事実を「通信当事者以外の第３者が積極的意思をもって知得してはならず」「第３者にとどまっている秘密を、漏洩（他人が知りうる状態にしておくこと）することおよび窃用（本人の意思に反して自己または他人の利益のために用いること）してはならない」の二つの意味を包含するものととらえられている。これらを受けて、電気通信事業法４条は、「電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。」とし、有線電気通信法９条は「有線電気通信（電気通信事業法第四条第一項又は第九十条第二項の通信たるものを除く。）の秘密は、侵してはならない。」として、それぞれ通信の秘密の保護を定めている。また、電気通信事業者の取り扱うもの以外の無線通信については、電波法が、第５９条において、「特定の相手方に対して行われる無線通信…（中略）…を傍受してその存在もしくは内容を漏らし、又はこれ窃用」することを禁じている。

２　脆弱性の調査・発見行為と通信の秘密との関係

電気通信事業者の取扱いにかからない無線通信については、現在においては、通信の秘密との関係では電波法の規制のみが問題となる。したがって、これを受信することは可能であるが、「その存在もしくは内容を漏らし、又はこれ窃用」することは禁止されることになる。情報取扱い基準としては、無線 LAN サイトに脆弱性がある場合についても、この脆弱性もこの脆弱性情報取扱体制の適用対象ということになる。その際、特定のサイトにいわば「宅内」だけで通信し、そのサイトの情報を取得した場合に、その通信に関する事実を IPA に報告することは、その無線通信の「存在」を漏らすということになるのではないかという問題がある。文言の解釈から行くと、電波法の禁止する漏洩に該当するように思える。なおも検討を要する。

また、第１５９回通常国会において「暗号通信を傍受した者又は暗号通信を媒介する者であつて当該暗号通信を受信したものが、当該暗号通信の秘密を漏らし、又は窃用す

る目的で、その内容を復元したときは、一年以下の懲役又は五十万円以下の罰金に処する。」という改正案が提案されている（改正案１０９条の２）。

第10 ベンダコミュニティの構成と競争市場

脆弱性情報取扱ガイドライン WG の直接の担当範囲ではないが、脆弱性情報についてベンダコミュニティを構成して、脆弱性情報について、外部開示を禁止し、また、優先提供を求めないという相互の合意を形成させることは、競争法上問題を提起する可能性がある。独占禁止法上は、競争を制限する効果を有する合意を「不当な取引制限」として禁止している（同法３条）。競争市場においては、いかなる市場参加者も優れて脆弱性情報を取得し、これを利用する立場があり、それをもとに市場においてもっとも安全なシステムを消費者に提供する権利を有すると考えることができよう。そのような立場を合意により制限しようとするのであれば、「不当な取引制限」となる可能性がある。

また、ベンダコミュニティを構成した場合に、脆弱性情報等の開示者が、ベンダコミュニティ内での秘密保持をどのように維持するのかも課題である。ベンダコミュニティそれ自体は実組織ではないので、開示者は、ベンダコミュニティの構成員のそれぞれと秘密保持契約を個々に締結せざるを得ないのではないかと思われる。その際、当事者間それぞれの契約内容を統一できるのか、不統一の場合に問題はないのかといったことも検討する必要がある。仮にベンダコミュニティとしての組織を設けた場合には、開示者とその組織との間の秘密保持契約と、その組織と各構成員との間の秘密保持契約との関係についても同様の課題や２次的な開示を前提とする秘密保持の責任構成について検討する必要がある。

第2章 米国における脆弱性情報と法的論点

第1 脆弱性報告について情報処理推進機構（IPA）のとるスキームについての報告（同スキームを米国に導入した場合の仮設的分析を含む）

ソフトウエアの脆弱性は、国家の安全保障のみならず企業にとっても重要な問題であり続けている。基本的なポリシー上の問題は、そもそも、よりセキュアなソフトウエアを制作するよう奨励するにはどのようにすべきかである。ソフトウエアベンダが、契約で責任をすべて排除することができなくすべきだと主張する者もある。むしろ、ソフトウエアベンダは、欠陥製品を販売したときに適用される製造物責任を負担すべきだというのである。これに対して、ソフトウエアはすべての脆弱性を予め排除できないほどあまりに複雑であることから、ソフトウエアをともかく制作させ、後でエラーがあれば補正させる方が、完全を期して発売を遅らせるより得策であると論ずる者もある。

脆弱性報告について何が適切なアプローチであるかについては、多年にわたり、米国およびその他の国でも論争の対象となってきているが、本ガイドラインでとっているような制限的な脆弱性報告スキームが、総体的なネットワークセキュリティを維持するための最良の方法であることに、大方の人は同意している。米国で、実施できる脆弱性報告のスキームは多様であって、その中には、本ガイドラインで採用しているアプローチに似た情報の流れをとっているもので、最終案とされているスキームもある（第２・米国における「責任ある公開スキーム」に関する報告参照）。

多くの専門家が、セキュリティ脆弱性の開示を責任のある体制で行うというシステムが米国において歓迎されていると認めているものの、若干の懐疑は残っている。公開をいかに行うべきかについては、論争が続いている。昨年のラスベガスで開催された「Black Hat Briefings」でのセキュリティ会議では、脆弱性報告へのアプローチの仕方の問題が、「ホットな話題」となったと報道されている。一般に、ソフトウエアベンダの側では、脆弱性が公表される前に、問題に対処する時間を十分に与えられるべきだと論じた。ソフトウエアベンダは、公表すれば、ハッカーに攻撃の機会を教えるにすぎないと主張している。しかし、それらの主張においては、単に販売に支障が生ずることだ

けを理由として、ミスを公表することを避けたいと望んでいるように見えるものもあった。

他方で、セキュリティ問題の研究者の幾人かは、「完全な公開」を通じて脆弱性情報を自由に利用できるようにすることが最善のアプローチだと論じた。「曖昧ですますことでセキュリティを確保する」では、全くセキュリティがないことになると述べる者や、人気製品の脆弱性を発表することができた際に発見者が手に入れることのできる名声、尊敬、そして一躍の昇進の可能性を高く評価していると考えている者もいた。それに対し、ソフトウエアライセンスにおいては、ほとんどの保証および責任が徹底的に排除されている点に鑑みると、ベンダが商品のセキュリティを確保することに重点を置かなくてはならない十分なインセンティブはなく、「責任ある公開」に移行することにより、かえって状況が悪化することがあり得ると論じる者もいた。

目標とすべきは、これらの懸念される事項と改善の動機をかみ合わせて、強制的ではないもののしたがうことが可能であり、秘密保持のため当初の窓口では制限するが後にすべての必要な情報を広く配布できるような基準を策定することである。また、JPCERT/CC を信頼のおける仲介機関として利用することで、ベンダが報告に適切に対応しないのではないかという、発見者の疑念を減らせるようにも思われる。

本ガイドラインは、米国から見た場合、一般的にいって脆弱性報告の良いアプローチと評価されると思われるというのが、米国調査員の意見である。何れの側からもバイアスがかかっていないと思われるような、公表された、便利な、そして親しみのもてる場所を、脆弱性報告書を送付する場所とすることは良い選択である。

ただし、本ガイドラインが、すべての状況でうまく働くわけでないことは明らかである。脆弱性が、通常のシステムの外にいる人、つまり、ハッカー、テロリスト、敵対的な政府等により発見される場合もあり、この場合には、期待どおりには報告してくれることはないだろう。反対に、システム内の研究者がその発見を公表したがる可能性もある。一定の国家の安全保障やその他の要件の適用範囲内に留まる限り、言論および公開の自由が米国憲法で強く保護されている（もっとも、契約上の合意のある場合、その制限を受けるが）こと、また、研究者が、脆弱性の存在をつきとめ、それを分析するため、しばしば、その発見について同僚とまたはオンラインで議論したがることを考えると、報告するための適切なインセンティブを与えるシステムを構築することで、これを使用したいと思う人の数を最大限に増やすことができるであろう。

強制的な報告スキームは、法的および実際的な理由から、うまく機能しないと考えられる。いくつかの脆弱性については、世界中の人々に危険性を即座に知らせることによって、バグフィックスが開発されるまで、ユーザにその製品の使用を止めさせることが重要となるだろう。他には、民間の契約による取り決めにしたがい、セキュリティコンサルタントが脆弱性を発見することもあるし、または監査人もしくは規制官が発見することもある。契約によっては、第三者への一切の公開を禁止していたり、あるいは公開を一定の方法で行うよう義務づけていたりすることがある。このような様々な状況から、強制的ではなく選択可能なスキームの方が望ましい。また、本スキームが、何れかの態様によって、これを利用する発見者に対し、これを行っておけば責任を免れられると安心できる、ある種のセーフ・ハーバーを提供できるかを検討する余地がある。例えば、ベンダは、脆弱性を見つけた発見者が本ガイドラインにしたがう限りは、その人に対して一定の権利侵害やその他の契約上の責任追及を行わないことに同意するとすることもありうるのであろう。

本ガイドラインは、OIS ガイドライン（下記の第２で検討する）ほど包括的なものではない。OIS ガイドラインは、発見者とベンダとの間で継続的な協力関係が築けるように気配りしている点で、明らかにより完全なものである。最近の興味深い事例の一つに、フィンランドの研究者が、マイクロソフトの Outlook 2002 の脆弱性を報告した例がある。マイクロソフトは、これをマイクロソフトの尺度で「重要（important）」と位置づけ、2004 年 3 月 9 日にフィックスを公表したが、研究者は、公の場でこれに不満を表明し、翌日、マイクロソフトはそのフィックスを「緊急（critical）」に格上げしたというものである。

しかしながら、本ガイドラインのアプローチをとることにより、責任を負わされる潜在的な可能性がある。IPA と JPCERT/CC が、脆弱性情報を公表すると選択する前に、ユーザが損害を負った場合、損害を被った当事者は損害賠償を請求してくる可能性がある。もちろん、仮に、ユーザが、国家の安全保障または重要な社会基盤を保護する職責を自ら担っている機関であった場合には、ユーザに脆弱性を知らせないでおくことにより、政治的のみならず安全保障上の危機が発生する可能性がある。この点が、カリフォルニア州のセキュリティ保護法の場合に見られるような、政治的な巻き返しを導いた潜在的な原因である。

同時に、IPA あるいは JPCERT/CC が、脆弱性情報を取捨選択した（あるいは取捨選択するのに失敗した）場合の潜在的な責任について考察しておくべきである。原因となったベンダを見つけるのが遅れたり、誤ったりした場合に、その遅れから第三者に損害が生じ、あるいは誤って競争相手の企業の知るところとなった場合の損害賠償責任と

いう問題が生じる。仮に、ある脆弱性によって複数のプロダクションサプライヤーやシステム管理者が影響を被るときに、原因となった者すべてを発見できなかったり、知らされなかったりした場合に、えこひいきだという抗議や、逸失利益の喪失を含む損害賠償の請求という状況が発生する可能性がある。IPA と JPCERT/CC は、曖昧なかたちでしか報告されなかった脆弱性のもつ意味に常に注意すべきであるし、それに基づいて行動をとり、あるいはとらなかった場合にどうなるか、常に注意しておかなければならない。

その他に、企業の製品に関する脆弱性情報が、証券取引法における重要な内部者情報とみなされる可能性がある。この場合には、開示義務を負う端緒となったり、および/または内部者情報を保有したりする当事者は、当該企業の株式を売買するのを制限されることがある。

最後に、「脆弱性」として報告されたものに、製品供給者あるいはシステム管理者が対処するのを拒む場合がありうる。このような状況で、IPA や JPCERT/CC がどのように反応するのかは明確でない。

米国での問題を考察する際には、世論やマスコミの動向が、世論やマスコミの意向を反映する政治的対応に劣らず重要である。米国に対して影響を及ぼすような何らかのスキームを採用する場合には、世論の反感をかう可能性を考慮に入れておかなければならない。

第2 米国における「責任ある公開スキーム」に関する報告

米国での脆弱性報告の問題は、いくつかの経路をとっている。それは、(A) 重要な社会基盤を保護する目的での脆弱性報告、(B) 業界の主導のもとでの脆弱性報告に関するガイドラインの策定、および (C) 民間の業務サービスによるものである。

(A) 重要な社会基盤（critical infrastructure）を保護する目的での脆弱性報告

国土安全保障法にしたがい、2003 年 2 月、ホワイトハウスは、国家にとって死活的な、通信技術を保護するための持続的な、多面的アプローチの概略を説明した「セキュアなサイバースペースのための国家戦略（*The National Strategy to Secure Cyberspace*）」という、76 ページの冊子を発表した。優先課題 II では、国家的なサイバースペースセキュリティへの脅威と脆弱性の低減計画を確立することが取り上げられている。そこでは、以下のように述べられている。

> 「組織化された攻撃が、わが国のサイバーシステムの脆弱性に乗ずることにより、わが国の重要な社会基盤のセキュリティが脅かされることがある。サイバースペースにとって、もっとも脅威となる脆弱性は、重要な社会基盤を担っている企業自身の情報資産と、インターネットのメカニズムのような、その外部の支持構造で起こっている。ネットワークが互いに接続しているネットワークにおいて、安全性の低いサイトがあることが、また、サイバー攻撃の潜在的な重大な危険を生んでいる。脆弱性は、テクノロジに弱点がある結果として生ずるが、また、テクノロジ製品の実装と監視が不適切であることからも生ずる。」

「セキュアなサイバースペースのための国家戦略（*The National Strategy to Secure Cyberspace*）では、脅威と関連する脆弱性削減のための主要な措置とイニシアティブとして、以下の 8 点をあげている。

1. サイバースペース上の攻撃を防止し、犯罪者を訴追するための捜査機関の能力を高める。
2. 脅威および脆弱性の潜在的な影響をよりよく理解するために、国家的な脆弱性評価の手続を創設する。

3. プロトコルおよびルーティングの改善により、インターネットのメカニズムをセキュアにする。
4. 信頼できるデジタル制御システムおよび監視制御/データ取得システムの利用を促進する。
5. ソフトウエアの脆弱性を低減し、修正する。
6. 社会基盤の相互依存性を理解し、サイバーシステムおよび電気通信の物理的セキュリティを改善する。
7. 連邦のサイバーセキュリティ研究開発計画を優先的に取り上げる。
8. 新しく生まれるシステムを評価し、セキュアにする。

「セキュアなサイバースペースのための国家戦略」のその他の優先課題には、セキュリティ意識の啓発と訓練計画、サイバーセキュリティの認証制度を発展させること、および政府のサイバースペースをセキュアにすることが含まれている。

1988 年以来、ピッツバーグのカーネギーメロン大学の CERT Coordination Center (CERT/CC) <http://www.cert.org/meet_cert/meetcertcc.html> は、脆弱性情報の公開ソースを監視し、12,140 件を超える脆弱性報告書を受け取っている。報告を受け取り次第、CERT/CC の脆弱性問題の専門家が、潜在的な脆弱性を分析し、技術開発者と協力して、それらの製品のセキュリティの欠陥をこれら技術開発者に通知し、これらの問題へのそれら企業の対応を促進し、また対応を追跡する。CERT/CC は、600 社を超えるハードウエアとソフトウエアの開発者と交流があり、しばしば、これら開発者から、勧告に含めなければならないような情報が CERT/CC に提供されている。CERT/CC は、また、インシデント分析も行い、脆弱性の存在を示唆したり、ある同種の繰り返されるインシデントを探したりしている。CERT/CC は、ウェブベースのインシデント報告システム <https://irf.cc.cert.org/>、そして、電子メールベースの脆弱性報告システムを備え、「脆弱性解説データベース（Vulnerability Notes Database）」<http://www.kb.cert.org/vuls> を通じて、脆弱性情報を広い範囲の人々が入手できるようにしている。

脆弱性解説データベースは、「共通の脆弱性およびエクスポージャー（Common Vulnerabilities and Exposures：CVE）カタログ」とクロスレファレンスされている。CVE は、Mitre Corporation <http://www.cve.mitre.org> が開発した、脆弱性とその他の情報セキュリティエクスポージャーの標準化された名称を自由にダウンロードできるリストである。その目標は、広く一般に知られた脆弱性とセキュリティエクスポージャーの名称を標準化することにある。

「セキュアなサイバースペースのための国家戦略」の結果として、国土安全保障省のナショナル・サイバー・セキュリティ・ディビジョンは、2003 年 9 月に、インターネットのサイバー攻撃を防ぎ、これに対応するため、CERT/CC と連携する旨を公表した。パートナーシップである US-CERT <http://www.us-cert.gov/capabilities.html>は、ワシントン D.C.に本拠をおく、政府から資金の援助を受けた研究開発センターである。その目標は、システムへのウイルス、ワームの攻撃といった、サイバー攻撃の脅威への民間の対応と政府部門による対応を協調させることにあり、また、ソフトウエア脆弱性を報告するための新しい探知ツールと共通のプロトコルを開発するにあたり、全世界の CERT および民間のセキュリティ会社との間の調整を行うことである。US-CERT が公表した目標は、政府部門と民間部門の脆弱性と脅威への対応時間を、新たに 2004 年度末までに 30 分に縮めることにある。

米国連邦政府内のコンピュータの脆弱性は、国土安全保障省の一部門である連邦コンピュータインシデント対応センター（Federal Computer Incident Response Center：FedCIRC）が調整を行っている。FedCIRC は、CERT/CC、営利ソフトウエアベンダ、捜査機関、情報機関および米国連邦政府のインシデント対応チームと緊密な関係を保っている。FedCIRC の業務についての有益な議論は、<http://www.whitehouse.gov/omb/legislative/testimony/030910_lorentz.html>で入手できる。

コンピュータのセキュリティインシデントに関する情報を政府に報告し、政府と共有することを企業が躊躇する点について、産業界および業者団体と米国政府との間で、対話が続けられている。この対話のオブザーバーは、かかる情報を共有することを躊躇するのは、以下の 3 点をめぐり懸念があるからだと述べている。

i.　企業は、政府と共有した情報が、情報公開法（FOIA）の要請により公開されるかもしれないことをおそれている。

ii.　産業界は、この情報の保護が不十分であることから、秘密または固有の情報が公開されることとなり、提出した会社の評判を害し、市場占有率を失い、株価の下落を招くのを心配している。Yahoo!、Ebay および Amazon.com を含む企業の各々が、ウェブサイトでの営業に対して Dos 攻撃があった後数週間、会社の株価が大幅に下落したという証拠がある。

iii. 企業は、共有された情報が、犯罪捜査で利用されるのではないかと懸念しており、そうなった場合、企業は、捜査をコントロールすることはできないし、また、その犯罪捜査は、業務の実質的な妨げとなったり、その他の問題を引き起こしたりすることがありうる。

(B) 脆弱性報告についてのガイドライン策定に向けた業界のイニシアティブ

2001 年 11 月、マイクロソフトおよびその他のいくつかのセキュリティ関連会社（Foundstone、@Stake、Guardent、BindView および Internet Security Systems を含む）が、ソフトウエアのセキュリティ脆弱性を報告し公開するにあたっての、限定的な国際基準のドラフトを初めて公表した。これらの計画は、マイクロソフトの人間が「情報の無政府状態（information anarchy)」と呼ぶもの、つまり、ハッカーがどのように利用しようとおかいまなく、インターネット上で脆弱性情報を自由に入手できるようにしている慣行に対処するためのものであった。同グループは、「Organization for Internet Safety」（OIS）として知られることとなった。

最初の Request for Comment（RFC）が 2002 年 2 月に発行された。この RFC には、以下の主要な規定が含まれていた。

- 発見者は、アプリケーションのベンダに脆弱性を報告すべきであり、また、仮にベンダに連絡をとれない場合には、CERT/CC のような信頼のおける第三者であるコーディネータに報告すべきである。
- すべてのソフトウエアベンダは、セキュリティ警告と脆弱性報告を受け取るために、「secalert@companyname.com」のような電子メールアドレスを、特別に用意すべきである。
- ひとたび通知を受けた場合には、ソフトウエアベンダは 7 日（自動システムを利用している場合は 10 日）以内に回答しなければならない。
- ソフトウエアベンダは、その進捗状況について 7 日ごとに発見者に最新の情報を提供し、通知から 30 日以内に問題を解決することができるよう努めなければならない。問題を解決すべき確定した期日はないが、ソフトウエアベンダは、誠実に事を進めなければならない
- 問題が解決されるまで、報告は秘匿しておくべきである。

OIS <http://www.oisafety.org> は、2003 年 7 月 28 日に、「OIS セキュリティ脆弱性報告および回答に関するガイドライン」の第 1 版（*Guideline for Security Vulnerability Reporting and Response*）を発表した。2003 年 9 月 2 日には、「OIS セキュリティ脆弱性報告および回答に関するガイドライン実装のためのガイド － 1.0 版 」（*Guide to Implementing the Security Reporting and Response Guideline - Version 1.0*）が発行された <http://www.oisafety.org/reference/process.pdf>。この OIS ガイドラインでは、前記 RFC で提案されている基本的なアプローチと日程にしたがっている。注目すべき点は、CERT/CC への言及が省かれたことである。同団体は、ベンダおよび発見者に対して、脆弱性が是正された時点で、ベンダと発見者は、同時にセキュリティ勧告を公表すること、そして当該勧告から少なくともさらに 30 日間は、人々が脆弱性の機に乗ずることを直接に可能にすることができるような、補足データを公表することを避けるよう勧めている。このガイドラインには、脆弱性要約報告書の見本および発見者に提出するベンダの現状報告書の見本を含め、多くの書式見本がおさめられている。

OIS ガイドラインは、今日、セキュリティ脆弱性を報告し、調査するためにいくつかのモデルが利用されていることを認識しており、OIS ガイドラインを一つの有用なモデルとして提供している。強制的とする意図はなく、何らかの法的権利もしくは義務を創設することも、また各国各地の法律を変えようとする意図もない。OIS ガイドラインは、発見者とベンダとの間の協調と善意の関係を基礎としており、また、発見者が、調査に関与する望ましい水準を選択することを認めている。発見者とベンダとに相反があり、協調関係が壊れた場合に備えた手続も設けられている。

OIS ガイドラインを採用する企業は、それら企業のセキュリティポリシーにおいて、その手続がガイドラインと異なる部分を含め、それら企業がこのガイドラインにしたがっているものであることを注記しておくべきである。企業のセキュリティポリシー内にその旨を記載したならば、ガイドラインを真剣に順守することは義務となり、FTC その他の機関による調査の対象となる（本報告書・付録１・１）－FTC に関する記述参照）。

(C) 私企業による有料サービス

営利企業の何社かは、企業がソフトウエアの脆弱性を管理できるようにするためのサービスを提供している。これらの企業では、その公開しているウェブサイト上で、いく

つかの脆弱性警告を提供してはいるが、主に、秘密保持を条件として、代金を支払う用意のある会社に対して、早期の情報を提供することを業務としている。以下の会社が、脆弱性トラッキングまたはテストサービスを提供しているベンダの一例である。

- Security Tracker <http://securitytracker.com/startup/index.html> -- SecurityGlobal.net LLC の Security Tracker は、顧客に対してカスタマイズされた即時の脆弱性アラートを送り、また顧客に脆弱性通知サービスを提供している。SANS、CERT、CVE やベンダが用意する資料を「待つことができない」組織を相手としている。同社は、時間と労力が節約できること、情報過多を防ぐためのよりよい情報組織を提供し、またプロアクティブにセキュリティリソースを管理する能力を提供することを約束している。

Security Tracker は、脆弱性のトピックを以下のような大範疇に分類している。

- 第三者たる組織が発する勧告的警告
- 製品カテゴリ
- 脆弱性の原因
- 脆弱性の影響
- 報告者
- ターゲット（製品名）
- 影響を受ける基礎となるオペレーティングシステム
- ベンダ
- 時間順

- Secunia <http://secunia.com/> -- Secunia 社は、発表されたセキュリティ勧告を取り上げるサブスクリプションリストを毎週提供している。このサブスクリプションリストは、毎週、先週からのすべての脆弱性情報を要約している。同社のリストでは、勧告が製品別、またベンダ別に利用できるようになっている。Secunia 社は、CVE で採用している脆弱性の名称のような、一般的な基準にしたがっている。同社の勧告は、危険度にしたがい次のように格付けされている（深刻、高危険度、中危険度、低危険度、危険度無し）。同社の契約条件では、情報の精確性、質、完全性等々の保証がすべて排除されている。

- その他の企業は、システム管理者が、当該企業の既存の企業レベルでのセキュリティポリシーに、個々のワークステーションが準拠しているかをテストすることのできるツールやサービスを提供しているものもある。これら製品の中には、Configuresoft 社の Enterprise Configuration Manager、そして Harris Corporation の STAT Scanner がある。

第3 結語

「情報ネットワークの脆弱性については、共有されている情報が相対的に乏しいことから、ネットワーク化された情報を保護するためには、緊急の対応措置をとることが死活的に重要となる。」と米国連邦議会の技術評価局は、『ネットワーク環境における情報セキュリティとプライバシー』（57 頁）で述べている。U.S. Congress, Office of Technology Assessment, *Information Security and Privacy in Network Environment* (at page 57), OTA-TCT-606 (Washington, DC: U.S. Government Printing Office, September 1994).

最近の SANS Institute の報告書によると、オペレーティングシステムに対する攻撃で成功したものの過半数は、ソフトウエアのほんの少数の脆弱性を突いた攻撃である。攻撃者たちは、機会主義的行動をとり、最も容易でまた最も便利なルートをたどって、最も周知のソフトウエアの欠陥に乗ずるということに、これらの現象の原因を求めることができる。ほとんどすべての攻撃は、ベンダが既にパッチを提供している脆弱性に乗ずることによって起こされている。この点は、カリフォルニアに本拠をおくセキュリティ会社である Quays 社で行われた調査でも確認されているが、同社は 2002 年 1 月から 150 万件の脆弱性をスキャンした結果を分析して、脆弱性が存在するアナウンスメントが行われてから 60 日以内に、脆弱性に乗じた事例の 80%が起こっていることを見出している。

このことは、脆弱性報告に対して直ちに対応する効率的な方法があれば、それにこしたことはないことを示唆している。もっと重要なことは、かなり小規模な企業でも継続的に対応できるような、集中管理された態様で情報やパッチを迅速にユーザに提供することである。本ガイドラインと、本ガイドラインの手続に組み込まれるべき集中管理された公開の情報サービスは、情報セキュリティと社会基盤を保護するというゲームで、つねに一歩先を行っておこうと奮闘している全ての人が必要としているものであるとともに、それらの人々から歓迎されるツールである。

この点において低く評価すべきではないことは、情報を公表しておくことで、セキュリティが問題になったときに、ユーザが特定のベンダの警戒体制を評価できるようになることである。ヘルスケアと金融業界を除いては、オンラインの商取引におけるこれら多くの問題を取り扱う、米国における主たる法の執行者は、連邦取引委員会である。連

邦取引委員会の任務は、詐欺的で不公正な取引慣行を取り締まることにあるため、皮肉なことに、セキュリティポリシーを公表したばかりに、それにしたがって行動できなかった企業が不利を被る図になっている。セキュリティに関する規制を行う際のこのアプローチは、企業がセキュリティについてほんの僅かか、全く約束しなくなるような、意図せざる効果をもたらしており、それによって消費者は企業を評価する資料をまったくもち得ない事態になっている。望ましい方向は、脆弱性情報を公表して、最終的には、セキュリティにおいて優れていることが、市場競争に勝ち残るための条件となるような効果をもたせることであろう。

第3章 報告書モデル案における法的関連記述の解説

第1「ソフトウエア等脆弱性関連情報取扱基準モデル案」の法的関連記述に関する解説

ここでは、「情報システム等の脆弱性情報の取扱いに関する研究会 報告書」の資料１に示された「ソフトウエア等脆弱性関連情報取扱基準モデル案」における法的関連記述について逐条解説を示す。[25]

Ⅰ．主旨

Ⅰ．主旨 本基準は、ソフトウエア等に係る脆弱性関連情報等の取扱いにおいて関係者に推奨する行為を定めることにより、脆弱性関連情報の適切な流通及び対策の促進を図り、コンピュータウイルス、コンピュータ不正アクセス等によって不特定多数の者に対して引き起こされる被害を予防し、もって高度情報通信ネットワークの安全性の確保に資することを目的とする。

（解説）

本「ソフトウエア脆弱性情報取扱基準」は、上記主旨を果たすために政府が、公的ルールとして定めるのが望ましいものとして提案されている。経済産業省においては、通商産業省時代から、情報セキュリティに関する「告示」として、「不正アクセス対策基準」（通商産業省告示第 950 号）、「コンピュータウイルス対策基準」（通商産業省告示 第９５２号）を、システム自体の安全対策の実施に関する「告示」として、「情報システム安全対策基準」（通産省告示第 518 号）をそれぞれ発表している。これらの経緯などから、本件の公的ルールについても「告示」の形式で定められることになるものと考えられる。

一般に行政官庁が、その所掌する事務について公表する文書としては、告示、ガイドライン、運用基準がある。そのうち、国家行政組織法第 14 条は、「各省大臣、各委員会及び各庁の長官は、その機関の所掌事務について、公示を必要とする場合においては、告示を発することができる。」と定めており、上記各基準も、この「告示」の形式によって、定められているものである。この「告示」の性質は、行政機関の活動の指針とと

[25] 以下、本報告書において「情報システム等の脆弱性情報の取扱いに関する研究会 報告書」に示された「ソフトウエア等脆弱性関連情報取扱基準モデル案」および「ソフトウエア等脆弱性関連情報取扱ガイドラインモデル案」に関して逐条的な解説を記しているが、これらは本報告書執筆作成段階における法律家チームの見解・解説であり、経済産業省がこれらの見解・解説を承認するものではない。

もに関係者への指導の指針ということになるものと思われる。本件公的ルールを告示の形式で定めるとき、これにより一定の機関を届出機関および調整機関として指定しうることになる。

なお、不正アクセス対策基準においては、その「主旨」は、「本基準は、コンピュータ不正アクセスによる被害の予防、発見及び復旧並びに拡大及び再発防止について、企業等の組織及び個人が実行すべき対策をとりまとめたものである。」とされており、また、ウイルス対策基準においては、「本基準は、コンピュータウイルスに対する予防、発見、駆除、復旧等について実効性の高い対策をとりまとめたものである」とされているところである。

これらを前提に、上記主旨を解説する。なお、（１）前提となる事実認識（２）手法（３）目的については、研究会の報告書を参照されたい。

①「ソフトウエア等に係る脆弱性関連情報等の取扱いに関し」

「ソフトウエア等」の解説については、「Ⅱ．用語の定義」の「４．ソフトウエア製品」の定義を参照のこと。また、「脆弱性関連情報等」の定義については、「Ⅱ．用語の定義」の「２．脆弱性関連情報」の定義を参照のこと。

②「関係者に推奨する行為」

関係者というのは、「Ⅲ．本基準における関係者の定義」参照のこと。「推奨する行為」については、関係者の協調と善意をもとに、準拠するのが望ましいとして経済産業省が認識している行為を意味する。

この意味については、「コンピュータ不正アクセス対策基準」においては、「企業等の組織及び個人が実行すべき対策」とされており、また、「コンピュータウイルス対策基準」においては「実効性の高い対策」をとりまとめたものであるとされているところと対照して理解する必要がある。これら両告示は、名宛人に対する義務の基準としての意味をも直接に意図しうるものとして提示されている。これに対して、本公的ルールは、推奨する行為と記載されている点に意味がある。これは、脆弱性情報が、その脆弱性の重大性についても種々の態様があること、いわゆる完全開示の原則との相剋があることに基づき、直接的に名宛人の義務の基準として提案されているものではないと考えられることによるものである。まさに関係者の協調と善意をもとに準拠することが望ましいものということになる。また、本基準で定める関係者（例えば、「製品開発者」）が、「製品開発者」としての役割を果たせるような実効性をもつためには、調整機関との事前の契約（NDA 契約、社内での脆弱性関連情報ハンドリングポリシーの策定等の条件をクリアすること）が必要であり、これらの点からいって、たとえば、製品開発者の定義に合致するからと言って、直ちに本件公的ルールを遵守することが義務づけられ、記載された役割を果たさな

ければならないとされるものではないと考えられる（すなわち、本体制を利用するか、または、利用しないかは、あくまでも製品開発者自身の判断によるものである）。

もっとも、本公的ルールが、関係者により遵守され、その遵守意識によって支持され、法的な一般条項によって上記「コンピュータ不正アクセス対策基準」や「コンピュータウイルス対策基準」と同様の義務の基準としての効力を有するものと認識されるようになる場合もありえよう。

③「脆弱性関連情報の適切な流通及び対策の促進を図り」

「脆弱性関連情報」については、「Ⅱ．用語の定義」の「２．脆弱性関連情報」の定義を参照のこと。「適切な流通」とは、「脆弱性関連情報の早期の交換による迅速かつ適切な対応、検証による情報の正確性の担保などの長所を最大限にいかしつつ悪用の危険性を可及的に排除しうるような情報の交換」をいう。「対策の促進」については、「対策方法を適時に、かつ可及的速やかに採用すること」をいう。ここでいう「対策方法」については、「Ⅱ．用語の定義」の「３．対策方法」を参照のこと。

④「コンピュータウイルス、コンピュータ不正アクセス等によって多数の者に対して引き起こされる被害を予防し、」

「コンピュータウイルス、コンピュータ不正アクセス等」については、以下の「Ⅱ．用語の定義」の「１．脆弱性」の定義を参照のこと。

ここにおける「被害」とは、本項（５）で定義が示される「安全性」が、脅かされる状況をいう。被害が「不特定多数」の者に対して引き起こされる場合を念頭に置いて、以下の脆弱性関連情報取扱い体制が定められていることになる。また、この不特定多数の者に対する安全性上の脅威に対する対応であるという観点から、「Ⅱ．用語の定義」の「４．ソフトウエア製品」の定義がなされている。

⑤「高度情報通信ネットワーク社会における安全性の確保に資することを」

「高度情報通信ネットワーク社会」とは、「高度情報通信ネットワーク社会形成基本法」（いわゆるＩＴ基本法）の第２条において、「この法律において『高度情報通信ネットワーク社会』とは、インターネットその他の高度情報通信ネットワークを通じて自由かつ安全に多様な情報又は知識を世界的規模で入手し、共有し、又は発信することにより、あらゆる分野における創造的かつ活力ある発展が可能となる社会をいう。」と定義されている。

なお、「安全性」という用語が用いられているが、これは、情報システムの安全性に関連する場合には、「情報システム安全対策基準」（通産省告示第 518 号）において、「情報システムの機密性、保全性及び可用性」の３点から、把握できるとされている（情報システム対策基準一　主旨）ことに対応するものである。もっとも、通信プロトコルの脆弱性などが問題になる際には、本体制によって、ネットワーク

における通信の「信頼性」も保護されることになる。すなわち、情報システムに関連する（広義の）ネットワークセキュリティを意味するものと解されるであろう。製造物責任法における製品の不具合の中で（実際の世界における）安全性に関するものについて特段に「欠陥」として、特別の取扱いをなす（なお、製造物責任法２条２項は、「『欠陥』とは、（略）当該製造物が通常有すべき安全性を欠いていることをいう」としている）のと同様に、ソフトウエアが、「安全性」に関して不具合を有しているときに、「脆弱性」として、特別な取扱いを議論しようというのが本体制の趣旨になる。

なお、「コンピュータウイルス対策基準」においては、２定義の「（８）セキュリティ機能」において「プログラム、データ等の機密性、保全性及び可用性を確保するための機能」と定義されているところでもあり、また、情報処理振興事業協会（当時）は、セキュリティセンター「情報セキュリティの現状－2002 年版－」（2002 年 6 月 9 日）において、「情報セキュリティ」につき、「正当な権利を持つ個人や組織が、情報やシステムを意図通りに制御できる性質である」と定義している。そして、「上記の定義は、以下の性質を満足させることを条件とする。」として「可用性」「一貫性」「機密性」「道徳性」の各概念をあげている。（なお、「不正アクセス対策基準」においては、特に定義を設けることなくセキュリティ対策という用語が用いられている。）

Ⅱ．用語の定義

Ⅱ．用語の定義

本基準で用いられる用語の定義は、以下のとおりである。

１．脆弱性

ソフトウエア等において、コンピュータウイルス、コンピュータ不正アクセス等の攻撃によりその機能や性能を損なう原因となり得る安全性上の問題箇所。ウェブアプリケーションにあっては、ウェブサイト運営者がアクセス制御機能により保護すべき情報等に誰もがアクセスできるような、安全性が欠如している状態を含む。

（解説）

①「ソフトウエア等」

「ソフトウエア」については、以下の「４．ソフトウエア製品」の定義の解説を参照のこと。ここでは「ソフトウエア等」として、「等」の文字を含んでいる。こ

れは、製品としてのソフトウエア、ウェブアプリケーションシステムなどに限らず、有体物たる製造物、プロトコルなどをも含む趣旨である。

②「コンピュータウイルス、コンピュータ不正アクセス等の攻撃により」

「コンピュータウイルス」や「コンピュータ不正アクセス」の定義については、「６．コンピュータウイルス」と「７．コンピュータ不正アクセス」の定義を参照のこと。「攻撃により」における「攻撃」とは、安全性に対する意図的な脅威をいう。なお、コンピュータ不正アクセス「等」とされているのは、不正アクセスについて、アクセス制御機能を中核にして理解をする見解が一般化している点から、コンピュータウイルスや狭義の不正アクセスに限定されずに、逆にスパイウエア（spyware）、キーロガー（key logger）、フィッシング（phishing）などをも攻撃の種類として含める趣旨を盛り込んだものである。

③「安全性の問題個所」

「安全性」の定義については、上述「Ⅰ．趣旨」の解説⑤を参照。「問題箇所」とは、「通常有すべき程度を備えていない事項」をいう。

④「ウェブサイト運営者がアクセス制御機能により保護すべき情報等に」

「アクセス制御機能」については、不正アクセス禁止法２条３項参照。「情報等」については、ウェブサイト運営者が、アクセス制御機能により保護している情報のみならず、社会通念上、かかる機能により保護されるべき情報をも含む。すなわち、個人情報が、アクセス制御機能のかかっていない領域に保存されており、一般からアクセスしうる状態になっている場合においては、かかる個人情報は、機密ではない状態にあることになる。安全性が欠如している状態と評価されることになり、そのようなウェブアプリケーションの状態を含む趣旨である。

⑤「アクセスできる等の安全性が欠如している状態を含む」

「安全性」の定義については上述「Ⅰ．趣旨」の解説（５）参照。「欠如している状態」とは、「通常有すべき程度を備えていない状態」をいう。

２．脆弱性関連情報

（解説）

特に法的な観点から検証すべき用語は存在しない。

３．対策方法

（解説）

特に法的な観点から検証すべき用語は存在しない。

４．ソフトウエア製品

ソフトウエア又はそれを組み込んだハードウエアであって、汎用性を有する製品。

（解説）

①「ソフトウエア」

ソフトウエアとは、「データ処理システムの運用に関係する計算機プログラム、手順規則およびそれらに関する文書およびそれらに関する文書」をいう。

②「組み込んだハードウエア」

ソフトウエアと一体となった情報処理の用に供される有体物をいう。

③「汎用性を有する製品」

「製品」とは、ユーザの要求に応じた処理を実現すべく処理されたものをいう。汎用性を有するとは、他の製品とともに利用されること、もしくは、利用者が不特定多数存在することをいう。従って、ソフトウエアにおいても、ハードウエアにおいても、注文に応じてごく少数のユーザのために作成されるものについては、それが脆弱性を有したとしても、本ルールの対象ではないことになる。

５．ウェブアプリケーション

インターネット上のウェブサイトで稼働するシステム

（解説）

特に法的な観点から検証すべき用語は存在しない。

６．コンピュータウイルス

コンピュータウイルス対策基準（平成７年７月７日通商産業省告示第４２９号制定）における「コンピュータウイルス」をいう。

（解説）

①コンピュータウイルスの定義

「コンピュータウイルス対策基準」の ２用語の定義（１）において「第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、 次の機能を一つ以上有するもの。

(1)自己伝染機能

自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能

(2)潜伏機能

発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能

(3)発病機能

プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能」

と定義されている。

技術的な側面から考察すると、他のプログラムにみずからを複写し、プログラムの動作を狂わせてしまうコードをウイルスの定義とする方法もあるが、コンピュータ対策基準における定義は、それと比較するとより広いものになる。

②類似の定義との関連

法的な観点からすると、我が国においては、「人の電子計算機における実行の用に供する目的で、人の使用する電子計算機についてその意図に沿うべき動作をさせず、又はその意図に反する動作をさせる不正な指令に係る電磁的記録その他の記録を作成し、又は提供した者」を「不正指令電磁的記録等作成等の罪」(刑法 168 条の 2 第 1 項)として処罰するべく法律改正が準備されている。

上記のコンピュータウイルスの定義のみでは、スパイウエアなどについては、対応しきれないものと考えられるが、当該「不正指令電磁的記録等作成等の罪」においては、その射程範囲とすることができるように考えられる。その点で適用範囲に違いが存在することになる。なお、上記刑法改正において、上記の不正指令電磁的記録の記録の取得、または保管自体も処罰することが提案されている。

７．コンピュータ不正アクセス 不正アクセス行為の禁止等に関する法律（平成１１年８月１３日法律第１２８号）における「不正アクセス行為」をいう。

（解説）

①コンピュータ不正アクセスの定義

法律として「不正アクセス行為の禁止等に関する法律」（以下、不正アクセス禁止法という）がある。そこでは、「不正アクセス行為の禁止」として第３条で「何人も、不正アクセス行為をしてはならない」と定められており、「不正アクセス行為」の定義としては、

「アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為」（３条１号）

「アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為」（同２号）

「電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為」（同３号）

が列挙されている。

これらの行為の個別の定義の詳細については、不正アクセス禁止法の解説にゆだねる。また、具体的な解釈に関連して、行為が不正アクセス禁止法に触れるかどうかについては、「資料２　ソフトウエア等脆弱性関連情報取扱いガイドラインモデル案」付録１「発見者が心得ておくべき法的な問題」を参照のこと。

②関連する定義との関係

なお、「不正アクセス対策基準」においては、「不正アクセス」とは「システムを利用する者が、その者に与えられた権限によって許された行為以外の行為をネットワークを介して意図的に行うこと」をいうと定義がなされている。

この「不正アクセス対策基準」と不正アクセス禁止法の定義との相違であるが、「不正アクセス対策基準」の定義は、システムの利用者からの定義であり、一方、不正アクセス禁止法の定義は、システムへの許されないアクセスを意味するという定義である点で異なっている。「不正アクセス対策基準」の「不正アクセス」の定義は、論者によって、サービス妨害攻撃やポートスキャン行為などをも含むこともありうる。現時点においては、「不正アクセス」という用語について、アクセス制御機能を中心に把握する認識が一般化しているものと考え、不正アクセス禁止法の定義を利用するものとしたものである。

Ⅲ．本基準における関係者の定義

Ⅲ．本基準における関係者の定義

本基準における関係者の定義は、以下のとおりである

１．発見者

脆弱性関連情報を発見又は取得した者。

（解説）

発見とは、「初めて見出すこと」をいう。

「取得」とは「情報を自ら管理できるようになること」をいう。

２．受付機関

（解説）

特に検討すべき問題はない。

３．調整機関

（解説）

特に検討すべき問題はない。

４．製品開発者

ソフトウエア製品の開発等を行う者であって、以下のいずれかに該当する者。

(1) ソフトウエア製品を開発した者

(2) (1)に掲げる者のほか、ソフトウエア製品の開発、加工、輸入又は販売に関する形態その他の事情からみて、当該ソフトウエア製品の実質的な開発者と認められる者。

（解説）

①「ソフトウェア製品」

ソフトウエア製品の定義については、「Ⅱ．用語の定義」の「４．ソフトウエア製品」参照のこと。

②「開発した者」

「開発した者」というのは、「ユーザの要求に応じソフトウエアを実現する者」をいう。ソフトウエアの「開発」は、ユーザの要求に応じソフトウエアを実現する過程をいう。ユーザの要求を認識、仕様を定め、プログラムを作成し、提供、検収、保守の過程として認識されることになる。

③「開発、加工、輸入又は販売に関する形態」

「加工」とは、「既存のソフトウエアに改変等を加えること」をいう。特に、フリーなソフトウエアやオープンソースなどの形態により開発されているソフトウエアを念頭に置くとき、加工をなしたものも開発者等として、本体制の利用が推奨されることになる。

「輸入」に関して、いわゆる外資系ベンダについては

・自ら輸入し、販売する場合

・第三者に輸入させ、販売のみする場合（レアケース）
・第三者に輸入・販売させる場合（いわゆるマーケティング・サポート子会社）
・企業向けの輸入製品においては、輸入した荷姿のままで納入され、国内の輸入者または販売者がいちいち表示されるとは限らない場合

が考えられる。これらについても本体制の利用の推奨がなされることになる。

④「販売」

「販売者××」等の肩書で自己の氏名等を付している場合であって、当該ソフトウエアを一手販売している場合などが典型例にあたる。

⑤「実質的な開発者と認められる者」

実質的な開発者と認めることができるか否かの判断は、個別の事案における個々の脆弱性による被害者等の主観的な判断にゆだねられるものではなく、当該ソフトウエアの開発、加工、輸入または販売にかかる形態、ソフトウエアにかかる種々の表示等の事情とそれに対する一般の認識その他の諸般の事情を総合的に考慮して、社会通念に照らして客観的に判断されることになる。

⑥製品開発者とされることの意味

本件の定義にあてはまり製品開発者として認められるということは、本公的ルールが適用になり、各行為が推奨されるということになる。

これらの定義に該当する者の範囲が実際にソフトウエア製品を製造するものよりも広汎なのは、製品開発者において、スキームを活用したいという判断をした場合に、製品開発者が調整機関と交渉し、本スキームを活用するというスタイルでよい、と考えられることによるものである。

なお、この結果、製品開発者の定義に該当するものが複数存在することになるが、その場合は、脆弱性関連情報の厳格な管理体制、効率的な情報連絡体制の整備という観点から「調整機関」と「当該外国の製品開発者の製品を取り扱う複数の国内関係会社」との間で事前の協議を行い、調整機関から当該脆弱性関連情報を取り扱うコンタクトポイント（窓口）をひとつ決定し、情報の管理及び漏洩の防止を図る方向で運用されるべきことになる。

事前協議において、どのような体制が最適なのかを検討し、一律の対応ではなく、同じ製品開発者のソフトウエア製品を取り扱う各社の事情等、個々のケースに応じて脆弱性関連情報の流通体制を整備していくことが重要となる。

５．ウェブサイト運営者 ウェブサイトを運営する者。

（解説）

①「ウェブサイトを運営する者」

ウェブサイト運営者とは、ウェブアプリケーションシステムの動作を管理・運営する者をいう。本規定は、ウェブサイトが、一般の利用者に対してウェブのサービスを提供しており、その提供について誰がどのような責任を負うのかという観点から定められているものであり、ウェブアプリケーションシステムについて、その運営の責任を負うものは、当該運営主体ということになる。

なお、不正アクセス禁止法は、2 条 1 項において「アクセス管理者」を「電気通信回線に接続している電子計算機の利用につき当該特定電子計算機の動作を管理する者をいう。」と定義しており、「管理」とは、「財産、権利等についてその性質を変更しない範囲内での保存、利用、改良を目的とする行為」をいう。そして、特定電子計算機について、その「特定利用につき」動作の管理を行うことから、「管理」の主たる内容は、特定電子計算機をコンピュータネットワーク経由で他人に利用させるか否か、利用させる場合にはどの範囲の利用をさせるかということを決定することになる。この結果、ここでいう「アクセス管理者」は、後述するシステム管理者ではなく、あくまで当該法人自体ということになる。本件におけるウェブサイト運営者も、結果として上記の「アクセス管理者」と同義になる。

②システム管理者との違いについて

これに対して、別個の者として、「システム管理者」が、定義されているのが一般である。これは、「企業・学校等の法人の場合に、職員の中から任命され一般に、『管理者』、『ルート』、『スーパーユーザ』などと呼ばれて『管理』の業務を担当している者」とされる。本ルールにおいては、このようなシステム管理者が、ウェブサイト運営者と認識されるわけではない。

③具体例

なお、この具体例として、「資料２　ソフトウエア等脆弱性関連情報取扱いガイドラインモデル案」付録４「具体的な説明」の「７．ウェブサイト運営者」の説明を参照のこと。

Ⅳ．本基準の適用範囲

Ⅳ．本基準の適用範囲 本基準は、以下に掲げるものの脆弱性であって、その脆弱性に起因する被害が不特定多数の者に影響を及ぼし得るものに適用する。 １．日本国内で利用されているソフトウエア製品 （ソフトウエア製品において通信プロトコル等の仕様を実装した部分を含む） ２．主に日本国内からのアクセスが想定されているウェブサイトで稼働するウェブアプリケーション

（解説）

①「脆弱性に起因する被害」

「脆弱性」の定義については、「Ⅱ．用語の定義」の「１．脆弱性」参照のこと。「起因する被害」については、「因果関係を有する被害」をいい、「被害」については、「安全性が脅かされる状況」をいう。

②（本基準は）「適用する」

この公的ルール・ガイドラインは、基本的に、脆弱性情報に関連して、その情報の流通により、安全性が脅かされることに留意して、名宛人に対して「推奨する行為」の集合体を提案するものである。その意味で、本基準が「適用される」というのは、その名宛人に対して、そのような推奨が及ぶという意味である。

この名宛人に対する効力が、その名宛人の所在する場所によって左右されるのかという問題は、いわば、法律でいえば、立法管轄権の問題に該当する。この点、法例１１条１項の「事務管理、不当利得又ハ不法行為ニ因リテ生スル債権ノ成立及ヒ効力ハ其原因タル事実ノ発生シタル地ノ法律ニ依ル」という文言の解釈論において、原因たる事実については結果発生地をも含むとされている点が参考になる。この点に照らせば、脆弱性情報により安全性が脅かされる場所が、日本であれば、この公的ルール・ガイドラインの適用があるとされるとすることにも合理性があるということがいえる。上記記述は、上述のような観点から、日本における不特定多数の者に対して安全性上の影響を及ぼすときに、その名宛人に対して本基準の適用がなされることを明らかにしたものである。つまり、関係者の所在地という要素は、この基準の適用を免れる理由には、ならないと考えられるということである。

③「日本国内で利用されている」「日本国内からのアクセスが想定されている」

これらについては、「資料２　ソフトウエア等脆弱性関連情報取扱いガイドラインモデル案」の「Ⅲ．本ガイドラインの適用の範囲」を参照のこと。

Ｖ．対象がソフトウエア製品である場合の脆弱性関連情報取扱基準

Ｖ．対象がソフトウエア製品である場合の脆弱性関連情報取扱基準

（中略）

１．発見者基準

（中略）

(３)発見者は、違法な方法により脆弱性関連情報を発見又は取得しないこと。

（解説）

発見者基準の(１)および(２)については、特に法的関連する記述はないので省略する。

①「発見者」

「発見者」の定義については、「Ⅲ．本基準における関係者の定義」の「１．発見者」を参照のこと。

②「違法な方法」

「違法な方法」とは、「法令に違反する方法」をいう。代表的なものとして不正アクセス禁止法違反があげられる。本条の基準は、脆弱性関連情報の発見のために違法な手段を用いることが許されないことを意味している。

③「発見」および「取得」

これらの定義についても、上記「発見者」の定義における解説を参照のこと。

この点については、脆弱性情報取扱体制を考えるとき、発見者が希望すれば、その発見者の名前を付して公開するという体制を考慮している以上、違法な発見による脆弱性情報等の取得に対しては、違法な行為の抑止という観点からも、場合によっては、届出を受け付けないものとすることが妥当である場合があることになる。

(４)発見者は、当該対策方法が公表されるまでの間は、第三者に漏えいしないように当該脆弱性関連情報を適切に管理すること。ただし、当該脆弱性関連情報を正当な理由により第三者に提供する場合は、あらかじめ受付機関に問い合わせをすること。

（解説）

①「発見者」「対策方法」

「発見者」については、「Ⅲ．本基準における関係者の定義」の「１．発見者」の定義、対策方法については、「Ⅱ．用語の定義」の「３．対策方法」を参照のこと。

②「漏えい」

「漏えい」とは、「他人が知りうる状態にしておくこと」をいう。ここでは、積極的な行為をも含み、他人に知りうる状態にしておくことすべてを意味することになる。

脆弱性情報の性質に鑑み、修正方法の公表があるまでは、発見者に対して第三者に対する公表について慎重な配慮を求めるものであるとともに、管理のずさんささなどから、第三者に対して漏えいしないようにすることを求めるものである。

③「正当な理由」

「正当な理由」の有無については、届出等から十分な期間が経過したか、原理的に知られていないものを公表するものか、発表されたとしても即座に攻撃できるものかどうか、事前の対策が現実的でないかどうか、公表の目的・態様などの観点から攻撃を幇助する可能性が高いものかなどの要素から、総合的に考慮される。

④「受付機関に問い合わせをすること」

公表について慎重な配慮を求める点については、「資料２　ソフトウエア等脆弱性関連情報取扱いガイドラインモデル案」「付録２．脆弱性関連情報の管理に際しての法的な問題」を参照のこと。これは、受付機関に連絡の上、公表等の手段をとるように配慮願いたいという趣旨である。

２．受付機関基準

（解説）

特に法的関連記述は存在しない。

３．調整機関基準

（解説）

特に法的関連記述は存在しない。

４．製品開発者基準

（解説）

特に法的関連記述は存在しない。

Ⅵ．対象がウェブアプリケーションである場合の脆弱性関連情報取扱基準

Ⅵ．対象がウェブアプリケーションである場合の脆弱性関連情報取扱基準

（中略）

１．発見者基準

（解説）

特に法的関連記述は存在しない。

２．受付機関基準

（解説）

特に法的関連記述は存在しない。

３．ウェブサイト運営者基準 *（中略）* （４）当該ウェブサイト運営者は、当該脆弱性に起因する個人情報の漏えい等の事案が発生した場合は、二次被害の防止、類似事案の発生回避等の観点から、可能な限り事実関係等を公表するなど必要な対策をとること。

（解説）

①「ウェブサイト運営者」「脆弱性」

これらについては、「Ⅱ．用語の定義」のそれぞれの定義についての当該項目を参照のこと。

②「個人情報」

「個人情報」とは、個人情報保護法の第２条１項に従い、「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等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。

③「漏えい等」

「漏えい」については、「Ⅴ．対象がソフトウエア製品又はプロトコルである場合の脆弱性関連情報取扱基準」の「１．発見者基準」の（４）の記述中の解説を参照のこと。「漏えい等」における「等」には、個人情報の改竄、消去などが含まれる。

④「可能な限り」

これは、漏えい等をされた当該個人情報の保護の要素、かかる事案が刑事的な問題を含む場合には、適正な処罰等を求める法執行等の要素、開示する場合における正確な事実の把握の必要性などの観点を総合的に配慮した上で、最大限に（公表する）という意味である。

⑤「事実関係を公表する」

これは、事実関係を不特定多数の者に了知しうる状態にすることをいう。

Ⅶ．その他

Ⅶ．その他

（解説）

特に法的関連記述は存在しない。

第2「ソフトウエア等脆弱性関連情報取扱ガイドラインモデル案」の法的関連記述に関する解説

（解説）

「Ⅰ．本ガイドラインの位置づけ」から「Ⅵ．IPA および JPCERT/CC による対策方法の普及支援」までの本文にわたる部分については、公的ルールにおける解説と同旨である。本文における文言の意味については、公的ルールに関する記述の解説を適宜参照のこと。

第3「発見者が心得ておくべき法的な問題」に関する解説

１．脆弱性関連情報の発見に際しての法的な問題

１．脆弱性関連情報の発見に際しての法的な問題 （１）関係する行為と法令の関係 ａ）ネットワークを用いた不正 ・例えば、脆弱性関連情報を利用して、アクセス制御機能を回避し、インターネットなどを介してシステムにアクセスした場合には、不正アクセス禁止法に抵触します。

（解説）

①「脆弱性関連情報を利用しての」

「脆弱性関連情報」については、公的ルール編「Ⅱ．用語の定義」・「２．脆弱性関連情報」を参照のこと。

②「アクセス制御機能を回避し」

これは、厳密には、「アクセス制御機能により制限された特定利用を識別符号の入力によらないでし得る状態にすることができる情報または指令」を「入力」（電磁的方式により送り、伝えること）することをいう。一般には、脆弱性を利用して一定の動作をさせる指令を送信することを指すことになる。

③「インターネットなどを介して」

「不正アクセス禁止法」においては、「電気通信回線に接続している電子計算機」に対するアクセスが禁止されており、「インターネット」は、その代表的な例示ということになる。ここで、「電気通信回線」とは、「電気通信を行うために設定される回線」をいうとするのが一般である。

④「アクセスした場合」「不正アクセス禁止法に抵触します。」

「不正アクセス行為」の定義については、公的ルール編「Ⅱ．用語の定義」「７．コンピュータ不正アクセス」参照のこと。

・例えば、管理者の了解無く、他人のパスワードを取得し、それを用いて権限なしでシステムにアクセスした場合には、不正アクセス禁止法に抵触します。

（解説）

①「管理者の了解無く」

ここでは、法の定めるアクセス管理者（不正アクセス禁止法 2 条 1 項）から個別にまたは一時的に利用をすることを認められることなしに（なお、同法 3 条 2 項 2 号括弧書参照）という意味である。

②「他人のパスワードを取得し、それを用いて権限なしで」

これは、「他人の識別符号を無断入力」すること（同法 3 条 2 項 1 号）の例示になる。なお、厳密には、入力される識別符号についての利用権者から承諾を得てアクセスする場合については、犯罪が成立しないが、説明の都合上、上記記載では、かかる例外的な事情については、省略してある。

③「システムにアクセスした場合」

本報告書・第１章・「第 5 脆弱性発見と不正アクセス、そして、届出の受理について」の記述を参照のこと

・故意にサーバの機能や性能の異常を来たそうとして何らかの行為をなし、コンピュータの性能を低下させたりした場合、刑法上の偽計（もしくは威力）業務妨害罪に抵触する可能性があります。さらに、その妨害の程度によっては、刑法の電子計算機損壊等業務妨害罪にも抵触すると解される可能性があります。

（解説）

①「刑法上の偽計（もしくは威力）業務妨害罪に抵触する可能性があります」

刑法２３３条後段は、「虚偽の風説を流布し、又は偽計を用いて、人の信用を毀損し、又はその業務を妨害した者は、三年以下の懲役又は五十万円以下の罰金に処する。」として偽計業務妨害罪を定めている。また、同法 234 条は、威力業務妨害として「威力を用いて人の業務を妨害した者も、前条の例による。」としている。

ここで、「偽計」とは、人を欺もう、誘惑し、あるいは他人の錯誤または不知を利用する違法な行為をいう。また、「威力」とは、人の意思を制圧するに足りる勢力を用いることをいう。ここで、この両罪の限界は微妙になる。コンピュータウイ

ルス等の投与によって、ネットワークに対して機能・性能の異常を来たそうとして、実際に性能を低下させた場合、業務妨害罪が成立する。判例では「業務の『妨害』とは、現に業務妨害の結果の発生を必要とせず、業務を妨害するに足る行為あるをもって足る」とされている（最判昭和 28 年 1 月 30 日）ので、業務妨害の結果の発生じたいは、要件ではなく、「コンピュータの性能を低下させたりした場合」というのは、成立する場合の例示の一つということになる。なお、この解釈は、人に対する加害行為による業務妨害と電子計算機に直接向けられた加害行為による業務妨害を峻別するという立場をとらないものによる。また、「抵触する可能性があります」という記載については、コンピュータの性能の低下といっても千差万別であり、その点を考慮しての表現ということになる。

②「電子計算機損壊等業務妨害罪にも抵触する」

また、刑法 234 条の 2 は、電子計算機損壊等業務妨害罪として「人の業務に使用する電子計算機若しくはその用に供する電磁的記録を損壊し、若しくは人の業務に使用する電子計算機に虚偽の情報若しくは不正な指令を与え、又はその他の方法により、電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせて、人の業務を妨害した者は、五年以下の懲役又は百万円以下の罰金に処する。」と定めている。この規定は、法解釈論的には、上記の業務妨害罪との規定の適用関係等の解釈について問題のあるところである。

本報告の立場は、①法は電子計算機に直接向けられた加害行為による業務妨害と人に対する業務妨害を峻別するものではなく②刑が上記の業務妨害罪に対して重いのは「電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせて」という中間結果を発生させる場合について、特に刑罰を重く定めた規定であるという立場に立つものである。もっとも軽微なウイルス等による攻撃行為に対して、そのような中間結果を認定することは、困難をきたすであろうと考えられる。「解される可能性があります」という記述は、上述のように解釈上の問題点を含み異なる解釈が成立する可能性があるという点や現時点においてはウイルス等による攻撃による中間結果の認定についての権威ある解釈が存在しない点を考慮して、その解釈の可能性の一つを示したという立場からのものである。

b) 暗号化されている無線通信の復号化

・暗号化されている無線通信を傍受し復号する行為（無線 LAN の WEP キーの解読など）は、第 159 通常国会で改正の審議がなされている電波法に触れる可能性があります。

（解説）

①「暗号化されている無線通信を復号化し」

「暗号化」とは、「その内容を即時に復元することができなくするための方法により他人に了知できないようにすること」をいう。

「無線通信」とは、「電波（放射により空間を伝搬する電磁波）を利用する通信」をいう。

「傍受」とは、「現に行われている他人間の通信について、その内容を知るため、当該通信の当事者のいずれの同意も得ないで、これを受けること」をいう。暗号通信における暗号部分を解読し、その内容を了知することは、これに該当する。

「復号化」とは、「暗号化されたメッセージから平文をえること」をいう。

②「電波法に触れる」

159 回通常国会において「暗号通信を傍受した者又は暗号通信を媒介する者であつて当該暗号通信を受信したものが、当該暗号通信の秘密を漏らし、又は窃用する目的で、その内容を復元したときは、一年以下の懲役又は五十万円以下の罰金に処する。」と提案されており（電波法改正案第 109 条の 2)、法律が改正されると、上記条項に違反する行為となる。

（２）不正アクセス禁止法に抵触しないと推察される行為の例

脆弱性の発見に最も関係が深い不正アクセス禁止法に対しては慎重な扱いが求められます。といっても脆弱性を発見する際に、必ずしも不正アクセス禁止法に抵触するとは限りません。以下に、不正アクセス禁止法に抵触しないと推察される行為の例を挙げます。

（解説）

①「推察される行為」

これは、不正アクセス禁止法の構成要件に該当する違法・有責な行為と「考えられる」ということをいう。法の解釈を提示することになるが、これは、経済産業省が示している「電子商取引等に関する準則」（準則がひとつの法解釈の叩き台となることにより、新しいルール形成の一助になることを願って示されているもの）と同様に、ひとつの解釈を提案するものにすぎない。従って、これが解釈の「叩き台」にすぎないという意味を明らかにするために「推察される」という表現をなしたものである。

1) ウェブアプリケーションの利用権者が、正規の手順でログインするなどして通常のアクセスをした際に、ブラウザとサーバとの通信の内容を観察したところ、それだけで脆弱性の存在を推定できた場合。

（解説）

これについては、「正規の手順でログインするなどして通常のアクセスをした際に」と特定がなされているのであり、不正アクセス禁止法の構成要件該当性の問題はない。

2) ウェブページのデータ入力欄に HTML のタグを含む文字列を入力したところ、入力した文字列がそのまま表示された。この段階ではアクセス制御機能の制限を回避するに至らなかったが、悪意ある者に別の文字列を入力されれば、このサイトにセキュリティ上の問題が引き起こされかねないと予想できた場合。

（解説）

①「ウェブページのデータ入力欄に」

ウェブブラウザにおける http に関する指令を書き込める欄をいう。ウェブサイトにおいて、特定のデータが、特定の ID・パスワードの入力がなければ、認識しえない状態になっている場合、法的には、その「電子計算機」は、「特定利用の一部利用が制限されている」ものと考えられている。従って、そのような特定のデータの内容を認識する行為については、「特定利用の一部利用の制限」を解除するかどうかという構成要件の該当性の問題がでてくる。

②「入力した文字列がそのまま表示された」

これは、自己の入力した文字列がそのまま一定のメッセージとしてウェブページ上に表示された状態をいう。一部利用の制限によって保護されているデータが表示されたわけではないので、アクセス制御機能の制限を回避したわけではない。

③「悪意ある者に別の文字列を入力されれば、このサイトにセキュリティ上の問題が引き起こされかねないと予想できた場合。」

不正アクセス禁止法３条２項３号においては、コンピュータを「作動させ、その制限されている特定利用をし得る状態にさせる行為」が処罰されることになっている。従って、実際に、一部利用の制限によって保護されているデータを表示させるということがなければ、その制限を解除しアクセスしたということにならないので、本事案においては、不正アクセス禁止法の構成要件該当性はない。

しかしながら、脆弱性の内容により、別の文字列の入力がなされれば、その保護されているデータの表示がなされることが十分に予想されることがある。そのような場合には、不正アクセス禁止法の構成要件該当性があることが十分に考えられるのである。

3)アクセス制御による制限を免れる目的ではなく、通常の自由なページ閲覧を目的として、日付やページ番号等を表すと推察される URL 中の数

字列を、別の数字に差し替えてアクセスしてみたところ、社会通念上、本来は利用できてはならないはずと推定される結果が、偶発的に起きてしまった場合。（ただし、積極的に多数の数字列を変えて試す行為等は、制限を免れる目的とみなされる可能性があります。）

（解説）

①「社会通念上、本来は利用できてはならないはずと推定される結果」

ウェブサイトにおける特定利用の一部制限については、2）記載のとおりである。「特定のデータ」が、日付やページ番号等を表すと推察される数字列を含んだ「http」以下の指令のみによって表示されるというのは、社会通念的には、特定利用の一部が制限されているというのには、不十分なように思われる。その点で構成要件該当性が存在しないと思われる。

②「偶発的に起きてしまった場合。」

なお、「偶発的に起きてしまった場合」とされている点からも、故意がない場合（本事案では、特定利用の一部制限がなされていることを認識していないことが前提となっている）と考えられ、その場合、法的には、違法・有責とは考えられない。記載の関係で、不正アクセス行為について、「制限を免れる目的」というような特定の目的が必要なように記載されているが、これは、法的には、特定利用の一部制限についての認識がある場合の代表的な認識状態の例示にすぎない。本報告書もしくは研究会において、不正アクセス禁止法の解釈等において特別の要件を付そうとするものではない。

③「（ただし、積極的に多数の数字列を変えて試す行為等は、制限を免れる目的とみなされる可能性があります。）」

本報告書・第１章・「第 5 脆弱性発見と不正アクセス、そして、届出の受理について」において触れたように、特定利用の一部制限がなされているかどうかは、最終的には、社会通念による判断になることとなる。その意味で、特定の文字列をいれた場合に、通常、表示をなすことが不可能なデータが表示される場合には、そのデータに関して、特定利用の一部制限がなされていると評価される可能性が存在するものと考えられる。「制限を免れる目的とみなされる可能性がある」というのは、「特定利用の制限がなされている」として、構成要件に該当するとされ、また、それについての認識があり故意があったとされる可能性が十分に存在することを意味する。

（３）IPA の対応と発見者の法的責任

IPA は、脆弱性関連情報の入手方法に関して関知しません。ただし、違法

な手段で入手されたことが明白な脆弱性関連情報に関しては、受け付けないことがあります。

また、IPA が脆弱性関連情報を受け付けた場合でも、IPA は脆弱性関連情報の入手手段に関して合法であると判断したわけではありません。さらに、IPA が脆弱性関連情報を受け付けた場合、発見者の脆弱性関連情報の発見に係る法的責任が免責されるわけではありません。

（解説）

①「**不法な手段で入手されたことが明白な脆弱性関連情報に関しては、受け付けないことがあります**」

これは、「Ｖ．対象がソフトウエア製品又はプロトコルである場合の脆弱性関連情報取扱基準」の「１．発見者基準（３）」等と対応するものであって、届出として受理しないことがありうることを意味する。

②「**IPA が脆弱性関連情報を受け付けた場合、発見者の脆弱性関連情報の発見に係る法的責任が免責されるわけではありません**」

これは、この付録で考察されている種々の法的な責任から発見者が免責されるものではないこと、すなわち、この体制に基づいて届出をなしたことの一事をもって、法的に発見行為に関する違法性が阻却されるものと解されるべきではないことを意味している。

２．脆弱性関連情報の管理に際しての法的な問題

発見者の脆弱性関連情報の管理に際しては、以下の法的な問題への注意が必要です。

(1)脆弱性についての調査・報告は、その率直な交換により、ソフトウエアやウェブアプリケーションシステムのセキュリティが結果として強化され・向上するという側面があります

(2)しかしながら、その情報については、悪用というデメリットがあるので、その点についての十分な配慮がなされるべきであり、その一つの方向性を提唱するのが、このガイドラインといえます。

(3)また、情報自体そのような性格をもつので、発見者についても脆弱性関連情報の管理について真摯な態度が必要とされます。

(4)そのような真摯な態度を保つ限り脆弱性関連情報についての調査・報告は、社会的に有用なものと考えられます。

（解説）

①「**脆弱性についての調査・報告**」

「脆弱性」についての発見・検証・情報交換・批判・本体制に基づく報告などをさす。それらは、憲法における「表現の自由」の保護の趣旨から鑑みて、十分に尊重に値するものとされる。そして、「表現の自由市場」において、その脆弱性に関する情報が批判・検証されることは、その問題とされたソフトウエアやウェブアプリケーションシステムのセキュリティのレベルは、もちろんのこと、学問としてのセキュリティの向上にも貢献するものである。

②「その情報については悪用というデメリット」

これは、脆弱性関連情報を利用した攻撃コードの作成などによる安全性に対する攻撃をいう。これによって安全性に対する脅威が増すことは、「悪用」であり、脆弱性情報の自由な開示の「デメリット」として存在しているのである。

③「その一つの方向性を提唱する」

本脆弱性情報取扱い体制の方向性であり、脆弱性情報について、これを保持するものは、責任をもって、これを取り扱うものとすること、特に、製品開発者および届出機関に対して、これを報告することおよび正当な事由のないかぎり、不用意な開示を慎むことを推奨するものとするというのが、この方向性ということができよう。

④「真摯な態度を保つ限り」

開示にあたって、相対立する種々の要請を考慮しつつ、かつ情報の公開については自己の責任であることを認識しつつ、その情報の取扱い等に最大限の善処をすることをいう。

⑤「社会的に有用なものと考えられます」

脆弱性情報に関する開示等について、これは、（１）において「結果として強化され・向上する」と同趣旨の意味しかない。脆弱性関連情報を開示したことによって、何らかの問題が生じた場合に、それが、脆弱性情報の開示であるからといって特段の法的な効果が与えられるべきであると提唱しているものではない。

この体制は、この脆弱性関連情報の取扱いについて、この体制に準拠した場合に違法性を阻却する効果が与えられるべきであるとか、逆にこれに反した場合、違法と見なされるべきであるとかの内容について判断を下しているものではない。そもそも、脆弱性関連情報の安全性に対するかかわりの程度が異なる以上、一概にどうのといえるものではない。これらの点については、裁判所の判断にゆだねられるものとなる。

しかしながら、管理について真摯な態度を欠く場合については、上述の限りではありません。そのような真摯な態度を欠く場合の具体的な例として以下が

あります。

a) 脆弱性関連情報の公表は、その情報の内容が真実と異なることを知っていた場合、あるいは，真実である場合であっても、特定人の名誉を毀損する意図で公表がなされ、かつ、公共の利益と無関係である場合には、刑法の名誉毀損罪に触れる可能性があります。

b) 特定人の信用を毀損する意図で事実と異なる脆弱性関連情報を、事実と異なると認識して公表がなされる場合には、刑法の信用毀損罪に触れる可能性があります。

c) 通常人に求められる程度の相当の注意をもって調査・検証したりしたのではなしに脆弱性関連情報であるとして公表し、かつ、脆弱性関連情報の開示に起因して損害が発生した場合、損害賠償責任などの民事責任を追及される可能性があります。

（解説）

①「名誉棄損罪」

刑法 230 条 1 項は、名誉毀損の罪を定め、「公然と事実を摘示し、人の名誉を毀損した者は、その事実の有無にかかわらず、三年以下の懲役若しくは禁錮又は五十万円以下の罰金に処する。」と定めている。この場合、摘示した事実が真実であるか否かは、問わないとされている。

②「かつ、公共の利益と無関係である場合には」

刑法 230 条 2 項は「前条第一項の行為が公共の利害に関する事実に係り、かつ、その目的が専ら公益を図ることにあったと認める場合には、事実の真否を判断し、真実であることの証明があったときは、これを罰しない。」と定めている。従って、公共の利益と無関係の場合には、公益を図ることにあったと認められることはないことになり犯罪が成立することになる。

なお、解釈論としては、「相当な根拠に基づいた摘示であれば、真実と証明し得なくとも不可罰とする」という結論が認められている点は、注意が必要である。

③「事実と異なる脆弱性関連情報」

刑法 233 条は、「虚偽の風説を流布し、又は偽計を用いて、人の信用を毀損し、又はその業務を妨害した者は、三年以下の懲役又は五十万円以下の罰金に処する。」として、信用毀損罪を定めている。条分上「虚偽の風説」とは、「事実と異なった噂」をいう。従って、事実と異なる脆弱性関連情報は、「虚偽の風説」にあたることになる。

④「事実と異なると認識して」

「虚偽の風説」について、「虚偽」であると認識している場合を指す。

⑤「通常人に求められる程度の相当の注意をもって調査･検証したりしたのではなしに」

風評被害を与える場合について、相当な調査をなして事実を摘示した場合にその事実が真実ではなかった場合に民事的に違法と評価されるかという点については、議論があり、その違法性の問題は、明確な判断基準が明らかであるとはいえない。しかしながら、相当な調査もなしに発表した場合に、違法なものと評価されるのは、明らかであり、上記は、その明らかな場合について論じて注意を喚起しているものである。

⑥「脆弱性関連情報であるとして公表し、かつ、脆弱性関連情報の開示に起因して損害が発生した場合」

脆弱性関連情報ではないのにもかかわらず、脆弱性関連情報であるとして発表した場合をいう。これは、いわゆる「商品やサービス自体には何ら問題がないにも関わらず、それらが忌避されることにより、経済的に壊滅的な損害を与える場合」ということになり、風評被害を与える場合の問題として議論されている。

第4「製品開発者が心得ておくべき法的な問題」に関する解説

製品開発者における法的な位置付けは、以下の通りです。 (2)ソフトウエアの提供行為についていえば、セキュリティに問題が生じず、日頃の運用で安心して使えるというレベルのソフトウエアを提供することが、法律上、債務の本旨に従った履行（民法４１５条）として求められています。 (3)もし、提供したソフトウエアにおいて、設計上の問題、プログラミング上の問題、運用上の問題の如何を問わず、社会通念上、安心して使えるというレベルにいたらない箇所が生じている場合には、その点に対してサポートの約定の趣旨に従い対策をすべきことが求められます。 (4)もっともその対策方法の選択については、種々の考慮が必要になります。

（解説）

①「ソフトウエアの提供行為」

「ソフトウエアの提供行為」とは、ユーザと開発者側とのライセンス契約等によって、ユーザがソフトウエアの使用許諾を得て、使用し、保守を受ける行為をいう。そして、「提供」時とは、ソフトウエアの使用許諾時と考えられる。

②「安心して使えるというレベル」

「セキュリティに問題が生じず、日頃の運用で安心して使えるというレベルのソフトウエア」というのは、セキュリティを欠いた状態ではないことをいう。

かかる状態であるかどうかは、設計上の問題点、開発上の問題点、指示・警告上の問題点の各観点から、当該ソフトウエアの特性、その通常予見される使用形態、

その開発者等が当該ソフトウエアを提供した時期その他の当該ソフトウエアに係る事情を考慮して判断されることになる。

また、「日常生活で安心して使えるレベル」か、どうかの判断の基準は、提供時ということになる。

③「債務の本旨に従った履行」

法律上、「債務の本旨に従った履行」とは、「契約その他法律で定められた内容・態様の給付をしない場合」をいう。

「通常です」というのは、ソフトウエアの提供態様において、フリーソフト等において、セキュリティなどの機能については、何ら保証はしませんという限定のもとに提供されることがあり、その場合には、セキュリティとしての一定のレベルを欠いている場合であっても債務の本旨に従った履行として認められるということを念頭においたものである。

(3)もし、提供したソフトウエアにおいて、設計上の問題、プログラミング上の問題、運用上の問題の如何を問わず、社会通念上、安心して使えるというレベルにいたらない箇所が生じている場合には、その点に対してサポートの約定の趣旨に従い対策をすべきことが求められます。
(4)もっともその対策方法の選択については、種々の考慮が必要になります。

（解説）

①諸概念

「提供したソフトウエア」「設計の問題」「プログラミングの問題点」「運用上の問題点」については、前述（１）についての解説を参照のこと。

②「いたらない箇所」

「社会通念上、安心して使えるというレベルにいたらない箇所」は、脆弱性のある箇所を指す。

③「対策をすべきことが求められます」

「対策」については「公的ルール」の「Ⅱ．用語の定義」「３．対策方法」を参照。

ソフトウエアの提供に際して、提供時点において、当時の技術等に関する知見（客観的に社会に存在する知識の総体）をもって、安心して使えるレベルのソフトウエアを提供する義務が通常あることは（１）で触れた通りである。また、その後の状況の変化や提供当時の技術知識で対応しきれなかった事項に起因する脆弱性についても契約上、サポートについての定めがなされることが通常である。そのようなサポートの約定が契約によってなされている場合には、その契約の趣旨に従って、対策がとられることになる。

④「対策方法の選択」

「公的ルール」の「Ⅱ．用語の定義」「３．対策方法」を参照。

⑤「種々の考慮」

対策方法の採用にあたっては、そのなかで回避を採用するか、修正を採用するか、直ちになすか、しばらく対策を猶予するか、どのような公表をなすかなどの点で配慮すべき事項が多い。これは、脆弱性の要因によって、対策方法を取るべき法的な位置づけが異なってくること、サポート条項の合理的な解釈によって対策方法が求められることが多いことにもよる。

個々の対策方法の種類については、「公的ルール」の「Ⅱ．用語の定義」「３．対策方法」参照のこと。

これらの選択については、善良な実務慣行によって決まる部分が多いものと考えられ、その際には、どのような対策を、どの段階で、どのように採用するかという点で総合的な考慮がなされるということになる。

この対策方法の選択に際しては、以下の点を論点として意識する必要があります。

(a) 上記の対策方法の選択について、状況に応じて債務不履行責任（民法４１５条）、不法行為責任（民法７０９条）、瑕疵担保責任（同法５７０条、５６６条、商法５２６条１項等）の対象となる可能性があります。

(b) 提供の際の契約で、これを免除する場合については、消費者契約法の適用がある場合には、責任の全部免除が認められない場合がありえます。

(c) 製造物責任法上の問題として、現時点において、ソフトウエアそれ自体については製造物責任が問われないと一般に解釈されていますが、電気機器や電子部品その他の工業製品等に組み込まれたソフトウエアは動産である製造物ですので製造物責任法に定める責任規定の適用がなされることがありえます。

（解説）

①「対策方法の選択」

「対策方法」の種類については、参照のこと。

②「状況に応じて」

「対策方法」の選択については、上記「種々の考慮」でふれた事項を総合判断し、ソフトウエア開発者は、善良な取引慣行と契約の趣旨に従って上記対策方法を採用することになる。

契約によりソフトウエアを提供する者が、過失により債務の本旨に従わない履行をなした場合、または、サポート条項に違反する場合は、債務不履行責任（民法

415 条)、瑕疵担保責任（同法 570 条、566 条、商法 526 条 1 項等）を負う可能性がある。

また、ソフトウエア開発者として認められる当事者は、場合によっては、不法行為責任（民法 709 条）の「違法性」の判断において、責任を負う可能性が存在する。

(b) 提供の際の契約で、これを免除する場合については、消費者契約法の適用がある場合には、責任の全部免除が認められない場合がありえます。

（解説）

①「消費者契約法の適用がある場合には」

消費者契約法第 2 条 3 項は、「３　この法律において「消費者契約」とは、消費者と事業者との間で締結される契約をいう。」として、消費者（個人をいう、同条 1 項）と事業者（法人その他の団体及び事業として又は事業のために契約の当事者となる場合における個人、同条 2 項）との間の契約を「消費者契約」として定義し、この消費者契約に消費者契約法の適用があることを明らかにしている。

②「提供の際の契約で」

提供行為およびその際に契約が締結される点については、（１）参照のこと。

③「これを免除する場合」

(a) で発生しうる可能性が指摘されている責任を免除することをさす。なお、契約によりソフトウエアを提供する者について、かかる脆弱性から損害が惹起された場合であっても、それについて過失がない場合については、責任がそもそも発生しないので、消費者契約法の適用の範囲外となる。

④「責任の全部免除が認められない場合がありえます」

消費者契約法は、第８条で（事業者の損害賠償の責任を免除する条項の無効）として「第八条　次に掲げる消費者契約の条項は、無効とする。」として

「　一　事業者の債務不履行により消費者に生じた損害を賠償する責任の全部を免除する条項

二　事業者の債務不履行（当該事業者、その代表者又はその使用する者の故意又は重大な過失によるものに限る。）により消費者に生じた損害を賠償する責任の一部を免除する条項

三　消費者契約における事業者の債務の履行に際してされた当該事業者の不法行為により消費者に生じた損害を賠償する民法の規定による責任の全部を免除する条項

四　消費者契約における事業者の債務の履行に際してされた当該事業者の不法行為（当該事業者、その代表者又はその使用するメの故意又は重大な過失によ

るものに限る。）により消費者に生じた損害を賠償する民法の規定による責任の一部を免除する条項

五　消費者契約が有償契約である場合において、当該消費者契約の目的物に隠れた瑕疵があるとき（当該消費者契約が請負契約である場合には、当該消費者契約の仕事の目的物に瑕疵があるとき。次項において同じ。）に、当該瑕疵により消費者に生じた損害を賠償する事業者の責任の全部を免除する条項 」

としている。

(a) で発生しうる可能性が指摘されている責任について、それが消費者契約である場合には、上記の免責条項が適用されることなる。従って、全部免責の条項については、消費者契約法 8 条 1 項 1 号、同 3 号、5 号の適用により無効になる。しかしながら、同条 2 項により修補が義務として定められている場合は、この限りではない。

(c) 製造物責任法上の問題として、現時点において、ソフトウエアそれ自体については製造物責任が問われないと一般に解釈されていますが、電気機器や電子部品その他の工業製品等に組み込まれたソフトウエアは動産である製造物ですので製造物責任法に定める責任規定の適用がなされることがありえます。

（解説）

①「ソフトウエアそれ自体については製造物責任が問われないと一般に解釈されています」

ソフトウエアは無体物であるため、ソフトウエアのライセンス契約において、製造物責任法の問題は生じないという趣旨である。これは、製造物責任法 2 条 1 項は、製造物につき、「製造又は加工された動産をいう」と定義していることにもよる。

②「工業製品等に組み込まれたソフトウエアは動産である製造物ですので」

例えば、「ただし、ソフトウェアを組み込んだ製造物については、本法の対象と解される場合がありうる。ソフトウェアの不具合が原因でソフトウェアを組み込んだ製造物による事故が発生した場合、ソフトウェアの不具合が当該製造物自体の欠陥と解されることがあり、この場合、その欠陥と損害との間に因果関係が認められるときには、当該製造物の製造業者に本法に基づく損害賠償責任が生ずる」とされている。

③「製造物責任法に定める責任規定の適用がなされること」

製造物責任法は、製造業者等が負う責任について、行為または過失を責任要件とする不法行為（民法 709 条）の特則として欠陥を責任要件とする損害賠償責任を規定している。具体的には、当該製造業者等が、製造物を自ら引き渡したこと、欠陥

の存在、他人の生命身体または財産の損害、損害の発生、欠陥と損害との間の因果関係を明らかにすることにより責任が認められるのである。

この結果、訴訟における証明事項の拡散を防ぎ、争点を単純化・明確化することができるといわれている。

第5「ウェブサイト運営者の法的関連事項」に関する解説

ウェブアプリケーションの脆弱性に関する法的な位置づけ、論点は、以下の通りです。 1) ウェブサイト運営者と、ユーザとの間においては、そのウェブアプリケーションの利用に際して、一定の契約関係にはいると考えられます。そして、ユーザが、そのサイトに一定の個人情報などをゆだねる場合には、ウェブサイト運営者は、そのサイトの利用契約に付随した義務として一定レベルのセキュリティ維持を果たすべき義務を負担していると考えることができます。

（解説）

①「ユーザが、そのサイトに一定の個人情報などをゆだねる場合」

ウェブアプリケーションの利用についても個々の利用については、契約関係と認識される場合が少なくない。

また、利用者（個人情報との関係では、個人情報によって識別される特定の個人、「本人」個人情報保護法 2 条 6 項）は、例えば、通信販売のサイトにおいては、その購入した商品の送付のためにそのウェブサイト運営者に対して、個人情報を明らかにしなければならない。その際に、その個人情報は、いわば、そのウェブサイトにゆだねられると考えられる。

なお、その運営者は、（法による個人情報取扱い事業者の要件を満たす限り）個人情報保護法の「利用目的の特定、利用目的による制限」（同法 15 条、16 条）「適正な取得、取得に際しての利用目的の通知」（17 条、18 条）「データ内容の正確性の確保」（19 条）、「安全管理措置、従業者・委託先の監督」（20 条～22 条）、「第三者提供の制限」（23 条）などの義務を負うことになる。

②「ウェブサイト運営者は、そのサイトの利用契約に付随した義務として一定レベルのセキュリティ維持を果たすべき義務を負担」

ウェブサイト運営者が、上述の義務を負い、利用者との関係では、その義務を実現するプロイバシーポリシー等の遵守を内容とする契約を締結するものと考えら

れることから、ウェブサイト運営者は、利用者に対しても種々の義務を負うものと考えられる。

そして、個人情報保護法は、第 20 条において「安全管理措置」として、「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防　止その他の個人データの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。」と定めており、これを果たすことがウェブサイト利用に関して契約の内容になっているものと考えられるから、ウェブサイト運営者は、サイトの利用に際して、利用者の個人情報に関してセキュリティに対して配慮すべき義務を負うことになると考えられる。

なお、個人情報保護法の各条項の定めから直接に利用者が一定の権利を有するかという点については、争いがある。

2) 各サイトに「プライバシポリシー」などが記載されている場合には、その内容をも前提にユーザとウェブサイト運営者は、契約関係にはいると考えられます。

（解説）

①「『プライバシポリシー』などが記載されている場合 」

1)で詳述したとおりである。

②「その内容をも前提にユーザとウェブサイト運営者は、契約関係にはいる」

この点については、現時点において明確に議論されてはいないものといえるであろう。上記記載は、契約関係の詳細な事項については、かかるプライバシポリシーなどにより補充されるという立場を前提に記述している。なお、検討を要すべき事項である。

米国においては、連邦取引委員会（FTC）が、その遵守を強制する一定の権限を有しており、その点については、本報告書・付録１「米国における情報セキュリティをめぐる最近の法律上の論点：サーベンス・オックスリー法、医療保険継続性及び責任法（HIPAA)、カリフォルニア州セキュリティ保護法等」を参照願いたい。

3) この場合、ウェブサイト運営者において、上記のセキュリティ維持等について過失が有る場合、その過失による損害賠償の責めを免れるような規定は、消費者契約法上、全部免責の規定については無効となることがあります。

（解説）

①「ウェブサイト運営者において、上記のセキュリティ維持等について過失が有る場合、その過失による損害賠償の責め」

上述のようにウェブサイト運営者にセキュリティ配慮義務があると考えられる点からいって、かかる義務違反は、債務不履行（民報 415 条）または不法行為（709 条）を構成するものと考えられ、責任を生じさせるものと考えられる。

②「免れるような規定」

上記の義務違反により、上述のような責任を免除するという定めをさす。

③「消費者契約法上、全部免責の規定については無効となることがあります。」

消費者契約法８条と責任免除の規定の解釈については、「製品開発者が心得ておくべき法的な問題」の(３)（b）に関する本報告書の解説を参照のこと。ウェブサイト運営者におけるセキュリティ維持等について過失のある場合についてもそこでの議論と同様の議論があてはまる。

付録 1 米国における脆弱性の取扱いに関する法律面の動向

1) 米国における情報セキュリティをめぐる最近の法律上の論点：サーベンス・オックスリー法、医療保険継続性及び責任法（HIPAA）、カリフォルニア州セキュリティ保護法等[26]

2002 年サーベンス・オックスリー法（Sarbanes-Oxley Act of 2002）

17 U.S.C. § 7241(a)

サーベンス・オックスリー法（Sarbanes-Oxley Act）は、会計および監査人による監視、コーポレート・ガバナンスそして役員の責任に関する、広範囲な改革を打ち立てた。同法は、Enron Corporation、WorldCom Inc.、その他企業で会計詐欺事件が続発した後、2002 年に連邦議会で制定された。同法は、企業の経営陣に厳格な内部統制を実施することを求めるとともに、その有効性を評価するよう求めている。同法は、特に、公開会社の最高経営責任者と財務責任者は、米国証券取引委員会（SEC）に年次報告書または四半期報告書を提出する際に、当該署名を行った役員が同報告書を検討したこと、また同報告書には重要な事実についての真実でない記載はなく、また当該財務情報は当該会社の財務状態を公正に表示していることを証明するよう義務づけている。署名した役員は、重要な情報が当該役員に知らされるように確保するため内部統制を確立し、維持する責任を負っており、またこれら内部統制の有効性について当該役員が得た結論についても報告しなければならない。役員は、また、監査人に対して内部統制の欠陥および当該会社の内部統制において重要な地位を占める経営陣または従業員が犯した詐欺的行為についても開示しなければならない。同法の違反行為には、内部統制の破綻または財務情報をおさめるコンピュータシステムに関わる是正措置について報告を怠ったことが含まれ、また、仮に当該情報がそれら報告書に記載されていなかった場合には、情報セキュリティに対する攻撃に起因する財務情報の改変または改竄が生じた場合には、これをもって違反に問われる可能性がある。

[26] なお、本報告は、報告書第２章と一体をなすものである。報告を求める都合上、研究会から種々の限定を付しているうえでの報告であることを了承いただきたい。

サーベンス・オックスリー法には、また、広範囲な内部告発者（whistleblower）の保護にむけた規定が設けられている。公開会社の従業員は、政府機関、連邦議会の構成員、または監督機関が、証券関係法、米国証券取引委員会（SEC）の規制または証券詐欺に関係した従業員を調査する際に、情報を提供しまたはその他の方法でこの調査に協力したことを理由に懲罰的に解雇されたり、その他不当な雇用上の取扱いをこうむらないよう保護が講じられている。

健康保険継続責任法（HIPAA）

45 U.S.C. § 1320

1966 年健康保険継続責任法（The Health Insurance Portability and Accountability Act of 1996：HIPAA）は、本報告書に関連する二つの目的を有している。同法は、従業員のために健康保険の適用を保証するとともに、ヘルスケアに関連する詐欺的行為や濫用を削減するというその立法目的を有しているが、それに加えて、個人の医療情報を不正なアクセスから保護すること、および、米国のヘルスケア制度内部の管理機構の簡素化のために制定されている。同法は、個人の医療情報を不正に開示することを禁止している。同法の対象となる機関は情報の不可侵性を確保するための保護措置を講じておかなければならず、また予期せざる危険要因から情報を保護しておかなければならない。

同法が制定された結果、多くの規格や規制が新たに作成され、この中には電子署名規格、プライバシー・レギュレーションおよびセキュリティ・レギュレーションが含まれている（45 C.F.R. Part 164)。同法のもとで作成された最終的なセキュリティ・レギュレーション（「セキュリティ・ルール」）は、2003 年 2 月 20 日に連邦官報（Federal Register）に公表されており、2005 年 4 月 21 日に発効し、実施される予定となっている。「セキュリティ・ルール」は、機密性を保護するため、一定の、管理上、物理的および技術的な保護措置を講ずるよう求めている。これらの基準は、広範囲にわたる「対象機関」がすべて実施しなければならないが、これらの中には、セキュリティ実務の欠陥点をなくすことが含まれている。

1999 年グラム・リーチ・ブライリー法（Gramm-Leach-Bliley Act）（「G-L-B 法」）

15 U.S.C. § 6805(b)

グラム・リーチ・ブライリー法は、米国において、ここ 60 年間で最も包括的な金融サービス規制分野での改革法であると考えられている。第一に、同法は、強力な機能的規制システムのもとで、銀行、証券会社そして保険会社の間で提携を行う際の障壁を取り除いた。同法は、また、米国で初めて、財務上のプライバシー保護に関して、順守すべき最低の基準を連邦法のかたちで設けた。広く定義された「金融機関」は、書面化されたプライバシー保護方針を設けておく義務を負い、またこれを顧客に対して開示しておかなければならない。同法は、(1) 顧客記録および情報のセキュリティと機密性を確保し、(2) それら記録のセキュリティや不可侵性に対する予期される侵害のおそれや危険要因から保護し、また (3) それら記録への不正アクセスや不正利用から保護するための管理上、技術上および物理的な保護措置に関する、金融機関向けの適切な基準を設けるよう、連邦準備銀行および米国証券取引委員会を含む規制当局に対し求めている。金融機関は、非公開の個人情報の機密性とセキュリティを保護するため、当該機関で採用している方針を開示する義務を負っている。

金融機関の規制当局（連邦準備制度理事会、通貨監督庁、連邦貯蓄金融機関監督局、連邦預金保険公社）は、この求めに応じて、『顧客情報の保護に関する完備性基準（*Interagency Standards for Safeguarding Customer Information*)』（「セキュリティガイドライン」）を採用した。「セキュリティガイドライン」は、12 C.F.R. Part 30、付録 B を含む多くの規則集で公表されている。それら金融機関の規制当局は、パブリックコメントを求めて、『顧客情報および顧客通知への不正アクセス対応プログラムに関する完備性基準（*Interagency Guidance on Response Programs for Unauthorized Access to Customer information and Customer Notice*)』案を公表しており、これは 2003 年 8 月 12 日の連邦官報（Federal Register）（47954 頁）に掲載されている。

G-L-B 法は、また、セキュリティ保護の適切性や、それが金融機関にもたらす潜在的な便益を含め、金融機関およびその関連会社の間での情報共有の実態について調査するよう求めている。

米国証券取引委員会（SEC）の「レギュレーション S-P：消費者の財務情報のプライバシー」

17 C.F.R. Part 248

レギュレーションS-Pは、米国証券取引委員会（SEC）の管轄に服する機関に対して、消費者情報を守るための管理上、技術的および物理的な保護措置についての方針および手続を採用するよう義務づけている。

米国連邦取引委員会法（FTC Act）

15 U.S.C. § 1

米国連邦取引委員会（FTC）は、米国連邦取引委員会法（FTC Act）に基づき、企業が提示しているプライバシーおよびセキュリティ保護方針を順守していない場合に、その企業を制裁する権限を与えられており、この分野で積極的に活動している。連邦取引委員会は、かかる違反行為は、不公正なまたは欺瞞的な取引慣行となり、連邦取引委員会法違反にあたると考えている。連邦取引委員会は、それら企業が実施すると約束した高水準のセキュリティを維持することを怠った数々の企業を提訴し、和解に持ち込んで解決している。これには、Eli Lilly & Co. <http://www.ftc.gov/os/2002/01/lillyagree.pdf> や Microsoft <http://www.ftc.gov/os/2002/08/microsoftagree.pdf> の例がある。各州の法務長官も、連邦取引委員会とは別に、ときとして同様な理由からこれらの事件について提訴することがあることに注意されたい（例えば、*In re Ziff-Davis Media Inc.* <http://www.oag. state.ny.us/press/2002/aug/aug28a_02_attach.pdf>、参照)。

さらに、16 C.F.R. Part 314 は、連邦取引委員会の管轄に服する金融機関（一般には、何らかの種類の金融業務を営むノンバンクがこれにあたり、旅行代理店、法律事務所等がこれに含まれる）に対して、その事業の規模及び複雑性、事業の内容及び範囲、並びにその保有する顧客情報の重要性に応じて適切な、包括的なセキュリティプログラムを策定し、実施するよう義務づけている。連邦取引委員会のセーフガード・ルールについての詳細と、リンクについては、<http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm>を参照されたい。

コンピュータ詐欺及び不正利用防止法（Computer Fraud and Abuse Act）（「CFAA」）

18 U.S. C. § 1030

CFAA は、政府部門と企業部門のコンピュータシステムのセキュリティを侵害する、広い範囲のさまざまな行為に対して、民事および刑事責任を課している。とりわけ、この連邦法は、保護対象のコンピュータに損害を生じさせると脅迫する旨を伝えることにより、金員を喝取することを禁じている。同法は、また、「意図的にプログラム、情報、コード又はコマンドを送信せしめて、その結果、保護対象のコンピュータに、権限なく、意図的に損害を生ぜしめる」人に賠償責任を負わせている。

電子通信プライバシー保護法（Electronic Communications Privacy Act）（「ECPA」）

18 U.S.C. § 2511

ECPA は、通信を違法に傍受することに関係するさまざまな問題を取り上げている。同法は、通信サービス施設に違法アクセスすることのみならず、通信を傍受するためのデバイスを送付することを犯罪行為として規定している。

2001 年米国愛国者法（テロリズムを迎撃し阻止するために必要な適切な手段を提供することによりアメリカ合衆国を団結させ強化する法律）USA PATRIOT (Unifying and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act of 2001

31 U.S.C. § 5311

http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011025_hr3162_usa_patriot_bill.html

米国愛国者法は、2001 年 9 月 11 日の世界貿易センターとペンタゴンへの攻撃の後、テロリズムを追跡、防止し、テロリズムと戦うための追加的手段を連邦政府に与えるため制定された。同法は、CPAA 及び ECPA を含む既存のいくつかの法律を改正している。同法第 III 編、その表題が「2001 年マネーロンダリング（資金洗浄）取り締まり及びテロ資金供与防止法(International Money Laundering Abatement and Antiterrorist Financing Act of 2001)」となっているものであるが、銀行秘密保護法（Bank Secrecy Act）にいくつかの新規定を加えるものである。これらの規定は、国際的な資金洗浄とテロリストへの資金提供の防止、探知および訴追を容易にすることを意図するものであ

る。同法は、また、重要な社会基盤（critical infrastructure）の保護に関連して、情報を共有することを規定している。

情報自由法（Freedom of Information Act: FOIA)

5 U.S.C. § 552(b)
http://www4.law.cornell.edu/uscode/5/552.html

FOIA は、多くの例外があるものの、政府が保管している文書の写しの交付を個人が請求することを認めるものである。例外としては、(1) 営業秘密、および秘匿特権が認められ第三者から得られたまたは秘密に属する営業上または財務上の情報、および(2) 捜査目的で収集された記録または情報が含まれているが、ただし、かかる情報を提出した場合、(i) 捜査手続の妨げになると合理的に予想される場合、(ii) 公平な裁判または偏りのない審尋を受ける権利を奪うこととなる場合、(iii) 秘密を守る約束の下に情報を提供した、州、地方または外国の機関もしくは当局または民間機関を含め、秘密の情報源が誰かが明らかとなると合理的に予想される場合、(iv) 捜査機関の捜査もしくは訴追のための技巧および手続が明らかとなってしまう場合、あるいは (v) 何れかの個人の生命または身体の安全を危険にさらすことが合理的に予想されうる場合にもっぱら限られる。

2002 年国土安全保障法（Homeland Security Act of 2002）

6 U.S.C. § 133

本法により、情報の分析および社会基盤を保護する職責を担う国土安全保障省（The Department of Homeland Security）が創設された。国土安全保障省の職責は、(1) 捜査機関情報および諜報活動の結果を受け取って分析し、(2) 主要なリソースと重要な社会基盤（critical infrastructure）の脆弱性を評価し、そして (3) 保護措置を見つけ、それに優先順位を付けるため諜報活動による分析と脆弱性評価を統合し、(4) 主要なリソースと重要な社会基盤の安全を確保するための総合的な国家的計画を策定し、(5) これらの主要なリソースと重要な社会基盤を保護するため必要な措置を講じ、(6) 適切な防護措置と対抗措置について勧告するのみならず、州および地方政府そして私企業に対して、セキュリティ上および公共に対する脅威について勧告し、そして (7) 連邦、州そして地方政府の間で、またそれらとともに、国内的なセキュリティ関連の諜報活動の成果を検

討して、勧告することにある。国土安全保障法は、「重要な社会基盤および保護対象のシステムのセキュリティに関連して、また分析、警告、依存性調査、回復、復旧およびその他の情報関連の目的で国家機関に利用させるために、秘密の連邦職員に任意で提出された重要な社会基盤に関する情報（提供者または提供団体が誰かに関する情報を含む）...」に関して、情報自由法（FOIA）の例外に新たな例外を追加している。同法は、また、一定の捜査目的を除き、当該情報を提供した人の書面による同意なくして、いかなる連邦、州または地方政府の役職員または従業員も、かかるすべての情報を開示してはならないと定めている。保護を受けるためには、当該情報には、「この情報は、2002年重要な社会基盤情報法の規定にしたがい、開示の対象とならない例外として、任意に米国連邦政府に提出されるものである。」との記載を添付しておかなければならない。仮に、報告が政府機関に対してなされ、それが重要な社会基盤情報にかかわるものである場合には、これらの規定が脆弱性情報の報告に影響を及ぼす場合がありうる。

内部告発者保護法（Whistleblower Protection Act）

1989 年に連邦議会で初めて制定された本法は、連邦政府公務員が、職場で目撃した浪費、詐欺的行為、権限の濫用、法令違反行為と同人が信ずるものを発見した場合に、これらの連邦政府公務員を保護することを目的とするものである。本法は裁判所の解釈により弱められたため、現在では効果が不十分であると多くの者は考えている。改正により本法を強化する努力がなされている。多くの州は、自らの内部告発者保護法を制定している。

セキュアなサイバースペースのための国家戦略（The National Strategy to Secure Cyberspace）

http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf

*「セキュアなサイバースペースのための国家戦略」*は、2003 年 2 月 14 日、ホワイトハウスより発表された。これには、特に、以下の 5 つの国家的な優先事項が明記されている。

(I) 国家的なサイバーセキュリティ対応システム
(II) 国家的なサイバースペースの脅威と脆弱性の低減計画

(III) 国家的なサイバースペースセキュリティの啓発と訓練計画
(IV) 政府サイバースペースのセキュリティ確保、そして
(V) 国家安全保障と国際的なサイバースペースセキュリティの協力

カリフォルニア州セキュリティ保護法（2002 年）

California Civil Code §§ 1798.29、1798.82

2003 年 7 月 1 日に施行された同法は、州の機関またはカリフォルニア州で事業を営むすべての企業であって、個人情報をおさめるコンピュータ化されたデータを所有するか、使用許諾しているものに対して、データのセキュリティの事故一切を開示するよう義務づけている。暗号化されていない個人情報を権限のない人が取得した（または合理的に取得したと信ずる）場合には、当該個人にこれを通知しなければならないとしている。同法は、脆弱性報告には直接的な影響を持たない。しかしながら、カリフォルニア州の顧客データに事故が生じた結果、脆弱性が明らかとなった場合には、一定の役割を果たすのは明らかである。発見者がカリフォルニア州の顧客情報にアクセスした場合にも、一定の役割を果たす可能性がある。

統一州法

統一コンピュータ情報取引法 (The Uniform Computer Information Transaction Act: UCITA)は、コンピュータのソフトウエア使用許諾についての州法を統一しようと試みたものであるが、今日、一般的には成功しなかったと評価されているものである。しかし、メリーランド州とバージニア州は、これを採択している <http://www.law.upenn.edu/bll/ulc/ucita/cita10st.htm>。承認された一つの UCITA は、情報の使用の制限を強制し、ライセンス終了後のソフトウエアの使用を防止することを目的としたプログラムやコードを使用することを認めている。かかる「自動的制限」（第 605 条）や「自力救済」（第 815 条、816 条）による救済方法は、法的には承認されているものの、多くのインターネットセキュリティ専門家は、使用されているシステムのセキュリティに対する脆弱性となると見ている。

統一商法典（UCC）第 2 章（売買）の最近の改正案が、その起草団体である、統一州法委員会全国会議（National Conference of Commissioners on Uniform State Law：

NCCUSL）とアメリカ法律協会（American Law Institute：ALI）により最終案としてかためられ、米国法曹協会（American Bar Association）から承認を受けた。州レベルでは、数年のうちに、州法としてこの改正案が採用されることになるものと期待されている。この第 2 章の改正は、ソフトウエアの使用許諾に対処しようとするものではないが、専門家は、保証を含めた売買法の規定を、ソフトウエア契約に適用する機会を裁判官に提供することができるものと予想している。具体的な場合には、この度の改正は、ソフトウエア契約の責任制限の強制実現可能性に、特に、消費者契約または物品と組込みソフトウエアを混合している取引に影響を与える可能性がある。

その他の州法上の論点

脆弱性報告は、連邦法において一般的に禁止されていないことから、脆弱性報告についての問題の多くは、ソフトウエアを受け取り、またウェブアクセスを行う根拠となる契約の条件から影響を受けることになるであろう。契約条件の解釈と強制実現可能性は、これに優先する連邦法や憲法上の論点がない限り、通常は州法上の問題となる。

2)　知的財産権法と情報セキュリティとの間の衝突に関する報告

特許権

特許権と知的財産の間の衝突は、先ず、セキュアなシステムを設計しようとする際に現れる。システムデザイナーが、ソフトウエア製品やウェブサービスのための最善のセキュリティアーキテクチャを構築しようとする際、既存の特許が障害物として道をふさいでいるのを発見することがある。既存の特許は、また、脆弱性を補修するため最善のパッチを作成する可能性に影響を与えることがある。

米国では、ソフトウエアとビジネスモデルがともに、特許権の保護の適切な対象として潜在的には承認されている。但し、それは、次のような、特許要件としての一般的な基準を満たすことが条件となる。特許要件の伝統的な基準は、(1) 新規性、(2) 有用性、および (3) 非自明性である。*State Street Bank & Trust* 事件（1998）において、特許性は、当該テクノロジの実用的な業務上の有用性の水準の関数であるとされた。同事件で、裁判所は、管理者が、財務情報（日々の資産配分、収益、費用および関連情報を含む）の流れを監視し、記録することができるようにし、いくつかのミューチュアルファンドをそのリソースにプールできるようにするデータ処理システムは、ビジネスモデルとして特許権取得可能であると判示した。かなりの数の電子取引関連の特許が、過去 10 年の間に認められてきた。電子取引のビジネスモデル特許の全般的な有用性については論争がくりひろげられてきたが、近い将来、このルールが根本的に変えられる兆しはない。むしろ、特許審査の方で、ビジネスモデル特許の発行数を制限するため、先行技術の調査をより厳しくし始めている。多くの、初期の電子取引関連のビジネスモデルについての争いは、依然として続いている。

米国連邦政府が開発した、または公的資金を使用して開発された技術には特許権を取得する資格はなく、その他一切の法的規制にしたがうことを条件に、すべての者がこれを自由に使用することができる。

特許権は、規格設定団体において、継続的な議論の対象となってきた。多くの規格団体が確固とした方針をまだもっていない一方で、議論は一般的に二つの方向に進んでいる。即ち、(1) 特許権者がある技術を規格に組み入れるべきように提案した場合には、特許権を放棄し、規格を採用するすべての人が自由にかかる技術を使用できるようにし

なければならない、あるいは (2) 特許権者がある技術を規格に組み入れるべきように提案した場合には、事前にその特許権を開示し、合理的な料金で、その技術を差別することなく使用に供さなければならない。

本件ガイドラインに関係する特許があることは定かでない。しかしながら、事業モデル（第２章・第２参照）のもとで、脆弱性報告データベースを立ち上げている私企業が数社ある。いくつかの企業が、ビジネスモデルの特許保護を取得しようとしたことがあることも考えられる。

特許の実施権者は、リバース・エンジニアリングまたは第三者と脆弱性情報を共有することについて、ライセンス契約の条件に基づき制限されることがある。

著作権

ソフトウエア脆弱性報告に関しては、著作権法上の問題が、もっとも大きな役割を果たすように思われる。著作権による保護を受けるための要件として、(1) 創作的な著作物であって、(2) 有形的な表現媒体に固定されたことが求められているに過ぎない。1980 年に、連邦議会は、著作権法を改正して、明示的にソフトウエア著作権を認めた。

著作権は、以下のとおり行いまた以下のとおり行うことを他人に認める独占的な権利を、著作権者に与えている。

(1) 著作権で保護されている著作物を複製すること
(2) 著作権で保護されている著作物に基づいて二次的著作物を作成すること。
(3) 著作権で保護されている著作物を公衆一般に頒布すること。
(4) 著作物で保護されている著作物を公演し、展示すること。

著作権は、権利の束であると考えられており、分割することができ、全部または一部を許諾することができる。したがって、著作権のライセンスは、ユーザによる使用権を制限するためには、販売するよりもっとずっと強力で、柔軟な方法であると考えられる。しかしながら、著作権は、ファースト・セール・ドクトリン（first sale doctrine）に服し、原本は、著作権ライセンスの制限を受けずにさらに頒布することができるものとされている、また著作権は、いくつかのフェア・ユースという適用除外に服する。新

しい技術手段に鑑みると、複製物のみならず原本の頒布を防ぐような新しい技術的手段が登場してきていることから、これら二つの適用除外規定の実際的な将来像について、現在も討論が続けられている。

1998年デジタルミレニアム著作権法第1201条（Digital Millennium Copyright Act of 1998、17 U.S.C.§1201）は、「いかなる者も、本編［著作権法］に基づき保護される作品へのアクセスを効果的に制限するための技術的措置を回避してはならない」と規定し、アクセスを制限する技術的措置を回避するために設計されたいかなる技術も製造、輸入してはならず、広く一般にむけて提供を申し出たり、提供したりしてはならず、またその他の方法で取引を行ってはならないとしている。「技術的手段を回避(circumvent)」するという用語は、著作権所有者の承認を得ることなく、スクランブルのかかった作品のスクランブルを解除し、暗号化された作品の暗号を解除し、またはその他の方法で技術的措置を避け、バイパスし、取り除き、作動できなくし、害したりすることを意味する。デジタルミレニアム著作権法（DMCA）は、作品の使用が著作権侵害にあたることまたは著作権法に基づき認められるであろうことを問わず、技術的装置を取り外した場合に責任を課すものである。本規定は、合法的なアクセス権を取得している人にアクセスを制限するにあたって、デジタル化された著作物のライセンサーを支援している。著作権法上の損害賠償額は、1回の回避行為につき最大$2500とされている。刑事責任が問われることもある。

著作権においては、譲渡される権利が潜在的に複雑であることから、ソフトウエア製品のライセンス契約は、しばしば、権利の制限について定義するところでは細々とした規定が設けられている。ライセンス契約の契約上の問題点には、第三者の固有の情報の共有の禁止や、営業秘密の承認、リバース・エンジニアリングの禁止、製品を公開の場で批評することの禁止を含む、詳細な秘密保持規定が含まれ、エラーや脆弱性を一定の方法でライセンサーに報告すべき義務、固有の情報の不正使用の場合に損害賠償額の予定額を請求することおよび/または差止命令による救済を認める規定、並びにエラー、脆弱性等による損害賠償責任を追及する権利を放棄する規定が含まれることがある。州によっては、一定の消費者契約上での保証等を排除することを禁止しているが、他の州では、裁判官が、所定の状況のもとで過度に不公正および非良心的であると判示しない限り、強制実現することが可能である。これらの種類の規定は、市販のソフトウエア契約およびソフトウエア開発契約の双方に見られる。同様な規定がサイトサービス契約にも見られる。ソフトウエアまたはウェブサービスにかかる契約が適用される場合には、かかる契約は、本ガイドラインで提示されているとおり、脆弱性を報告する発見者の能力を制限することがありうる。

それらが免責されていない限り、ライセンスやウェブサービスにもまた、機能および性能についての黙示の保証が含まれていると解釈することができる一方、明示の保証が含まれていることもある。これらの場合、脆弱性の存在は、契約違反の根拠となることがある。ほとんどの市販のソフトウエアのライセンス契約書および標準的なウェブサイトアクセス契約書には、機能および責任、並びにその結果生ずる責任についての完全なまたは広範囲な免責規定が設けられている。契約条件の解釈および強制実現は、優先する連邦法または憲法上の論点がない限り、通常は州法上の問題となる。裁判官には、非良心的契約であると認定するかまたは契約がそもそも締結されたことはなかったと認定することを含めて、特別な状況においては、免責規定を無効とするための手段が与えられている。しかしながら、米国法では、私的契約の有効性が尊重されることから、したがって、ほとんどの裁判官は契約の規定を支持するものであるが、これは特に企業間の取引についてそうである。

脆弱性報告書それ自体が、著作権による保護の対象となる著作物であると考えられるため、著作者は、本ガイドラインにしたがった再頒布を認める意向であるか、また報告書の使用を認める意向であるか明確にしておくべきである。発見者の脆弱性報告書について権利を取得するのが誰であるのかの問題は、発見者が特許権の取得可能性があったり、営業秘密またはその他販売可能なフィックスを提供することを望むことがありうるので、他の状況でも起こる可能性がある。

商標

本論点の文脈では、商標法と情報セキュリティとの間に明白な、直接的衝突は見受けられない。

営業秘密

営業秘密の保護は州法により与えられているものであり、よって法域ごとに異なることがある。通常、営業秘密とは、事業の運営に当たって使用できる何らかの情報であって、十分に価値があり、これを知らないまたは使用していない競合者に比して、実際のまたは潜在的な経済的な優位を与える秘密である。営業秘密の不正使用を主張するため

には、営業秘密の保有者は、(1) ソフトウエアまたは情報が営業秘密であること、(2) 保有者は、その機密を守るために合理的な措置をとったこと、および (3) 営業秘密を取得するため受領者が不正な手段をとったこと、またはこれを濫用もしくは開示したことにより秘密保持関係に違反したことを証明しなければならない。

営業秘密は、他の人または一定のグループの人に開示することができるが、これは、適切な秘密保持契約を締結することを条件に、なおも営業秘密たる性格を保つことができる。ひとたび、営業秘密が、広範なグループの人に開示された場合には、営業秘密たる地位を失うことがある。この点については、州によって異なり、営業秘密を含むところの脆弱性報告書について懸念となるであろう。脆弱性の発見者が、営業秘密の有効な受領者である場合には、第三者に営業秘密を開示しない旨の契約上の義務に服する可能性がある。

データベース

目下のところ、米国では、データベースは、独立した別個の知的財産として、特に保護されていない。

その他の形式の知的財産権

パブリシティ権のような、その他の形式の知的財産権が、情報セキュリティに直接に衝突することはないと思われる。

付録２ 韓国における脆弱性の取扱いに関する法律面の動向

韓国においては、具体的な立法の流れが急であること、そして、現在もきわめて活発に立法作業がなされていることは、第１報告書で報告したとおりである。そこで、今回は、韓国における脆弱性をめぐる法的問題についての議論の現状報告という趣旨で、ＳＱＬスラマー事件に関連して提起された訴訟の現状および平成１５年６月１１日に情報通信部主催、韓国情報保護振興院主管で、韓国電算院大会議室で開かれた「インターネット侵害事故対応及び個人情報保護強化のための情報通信網利用促進ならびに情報保護等に関する法律 改正（案）討論会」の会議の模様を報告する。

前者のＳＱＬスラマー事件に関連して提起された訴訟の訴状は、本報告書付録２．１に記載のとおりである。

後者の討論会の議題は、「改正の背景」「推進経過および主要な改正の内容」「情報通信網保護関連の改正事項」「個人情報保護関連の改正事項」などからなっている。ここで、特に「情報通信網保護関連の改正事項」については、「情報通信網の安全性の確保」「集積情報通信施設事業者の緊急対応」「情報保護の安全診断」「インターネット侵害事故対応支援センターの設置」「情報通信網侵害事故の申告及び対応」「情報通信網侵害事故の原因分析および資料保全命令」などが注目される。具体的な内容については、本報告書付録２．２に記載のとおりである。

付録２.１．SQL スラマー事件における訴訟

訴訟１

訴　　状

原告　　参加連帯　他　1,586

訴訟代理人　法務法人　ハンギョル

担当弁護士　ハク・スンフン、チョン・ヨンスン、ユン・ボクナム、ヨ・ヨンハク、キム・テヒ

被告　　株式会社　ケイ・ティー　他　7

損害賠償（キ）請求の訴

ソウル地方法院（裁判所）　御中

訴　　状

原告　　別紙１、２目録に記載の通り
　　訴訟代理人　法務法人　ハンギョル
ソウル　江南区　駅三洞　825-33　テヘランビルディング５、６、８階
（電話　02-3487-3000、ＦＡＸ　02-3787-3811）
　　担当　弁護士　ハク・スンフン、チョン・ヨンスン、ユン・ボクナム、ヨ・ヨンハク、キム・テヒ

被告　　１．株式会社　ケイ・ティー
　　城南市　盆唐区　亭子洞　206
　　代表理事　イ・ヨンギョン

２．ハナロ通信　株式会社
　　ソウル　瑞草区　瑞草洞　1445 の　3
　　代表理事　シン・ユンシク、イ・インヘン

３．株式会社　ドウルネット
　　ソウル　瑞草区　瑞草洞　1338 の　5
　　代表理事　イ・ホンソン

４．株式会社　デイコム
　　ソウル　江南区　駅三洞　706 の　1
　　代表理事　パク・ウンソ

５．ドリームライン　株式会社
　　ソウル　松坡区　新川洞　7 の　17
　　代表理事　イ・スンイル

６．株式会社　オンセ通信

城南市　盆唐区　亀尾洞　192 の　2

代表理事　ファン・キヨン

７．大韓民国

法律上　代表者　カン・クムシル

所管　情報通信部　長官

８．マイクロソフト　コーポレーション(Microsoft　Corporation)

アメリカ合衆国　ワシントン州　レッドモンド　マイクロソフト　ウェイ１番地

(One　Microsoft　Way、　Redmond、　WA　98052)

送達場所：株式会社　韓国マイクロソフト

ソウル　江南区　大峙４洞　892　ポスコセンター　西館６階

代表理事　コ・ヒョンジン

損害賠償（キ）　請求の訴

請求の趣旨

１．被告は各自

ア．別紙１目録の原告に各　金　50、000 ウォン

イ．別紙２目録の原告 11 ないし 700 に各　金　300、000 ウォン

ウ．原告株式会社　コサン・アイアンドシーに　金　20、000、0000 ウォン

及び上の各金額（金ウォン）に対して 2003 年 1 月 25 日からこの事件訴状の控えの送達日まで、年 5%、その翌日から完済日まで、年 25%の各利率による金額（金ウォン）を支給せよ。

２．訴訟費用は被告の負担とする。

３．第１項は仮執行することができる。

という判決を求める。

請求原因

１．当事者の地位

ア．原告の地位

原告は皆、インターネット通信網に加入して、インターネット通信網サービスを利用している者たちである。具体的には、
別紙１目録の原告 12 ないし 522 は、被告、株式会社　ケイ・ティー　インターネット通信サービスの加入者、
原告 523 ないし 943 は、被告、ハナロ通信　株式会社　インターネット　通信サービスの加入者、
原告 944 ないし 1,099 は、被告、株式会社　ドウルネット　インターネット　通信サービスの加入者、
原告　1,100　1,121 は、被告、株式会社　デイコム　インターネット　通信サービスの加入者、
原告　1,122 ないし 1,139 は、被告　ドリームライン　株式会社　インターネット　通信サービスの加入者、
原告、参加連帯及び 1,140 ないし 1,189 は、被告、株式会社　オンセ通信　インターネット　通信サービスの加入者である。
一方、別紙１目録の原告　1,190 ないし 1,516 は、被告１ないし６以外の他のインターネット通信網サービス提供業者に加入するなどの方法でインターネットを使用している一般のインターネット利用者である。

別紙２目録の原告 11 ないし 700 は、インターネット通信サービスを利用して営業をしている、いわゆる「PC 喫茶店」事業者であり、原告、株式会社　コサン・アイアンドシーは、被告、株式会社　ケイ・ティーの大容量インターネット通信網サービスの提供を受けて、これを「PC 喫茶店」事業者に再販売している事業者である。

イ．被告の地位

被告 1 ないし 6 は、それぞれ、インターネット通信網サービスを提供している企業等であり、被告大韓民国は、被告 1 ないし 6 に対して、インターネット通信網サービス提供を監督している情報通信部を傘下の機関に置いており、被告マイクロソフト　コーポレーション（以下。「マイクロソフト社」という）は、米国に本社を置き、韓国の上記送達場所に支社をおいて、ソフトウエア製造、販売業を営む法人である。

２．事件の概要　－損害賠償責任の発生との関連

2003年1月25日に前後して発生したインターネット通信網の全面的な麻痺事件（以下「インターネット麻痺事件」という）の経緯を、現在までに明らかになった範囲で順序だてて注意深くみれば、次の通りである。（甲第1号証）。

2003年1月25日14時10分頃、被告、株式会社ドリームラインで、インターネット通信網に対する異常徴候が発見され、報告された。
同日 14 時 35 分頃から、インターネット通信網サービス提供事業者（Internet Service Provider）である被告、株式会社　ケイ・ティー（以下「ケイ・ティー」という）、被告、ハナロ通信株式会社、被告、株式会社オンセ通信などのインターネット通信網に障害が本格的に発生し始め、エスケイ（SK）テレコム、ケイティーエフ（KTF）、エルジー（LG）テレコムなど、無線インターネットサービス提供業者のインターネット使用が不可能になった。
以後、21時30分頃、コンピュータワクチン提供業者である、訴外株式会社　アン・チョルス研究所と、訴外株式会社　ハウリ等は、被告、マイクロソフト社が製造、販売したコンピュータプログラムである、エムエス・エスキューエル・サーバ（MS SQL Server）2000（以下、「MS SQL サーバ」という）の脆弱点を利用した、スラマーワーム（Slammer Worm）の拡散によって、2003年1月25日インターネット麻痺事件が触発されたと明らかにした。

上記のようなインターネット麻痺事件の発生によって、インターネット通信網加入者及び利用者は、麻痺事件が発生した以後、正常化するまで相当な時間、インターネット通信を利用できなかっただけでなく、インターネット通信網を利用して事業をしているショッピングモールなどのインターネット事業者と、「PC喫茶店」などは、インターネット麻痺事件が発生した当日、及びその後、何日かの間、客等の利用が減少して、営業上、相当な損害を被った。

しかし、このような原告の被害が発生したにもかかわらず、インターネット麻痺事件の発生後、相当な時間が経過したにもかかわらず、責任当事者である各被告は、その具体的な原因糾明、及びそれに基づく損害の保全に対しては、まだ明確な解決策を提示しないままである。

これに対し原告は、このような事態を正し、原告が被った損害の賠償を受けるために、本件、インターネット麻痺事件に対して、責任がある被告を相手どり、本件損害賠償訴訟を提起するに至った。

以下に、各被告別に責任の根拠について、詳細に見ることにする。

３．被告１ないし６の損害賠償責任

被告 1 ないし 6 は、インターネット通信網サービス提供者として、安定したインターネット通信網を構成、運用して、今回のような麻痺事件が発生しないように、未然に防止し、万一、障害が発生した場合には、迅速に措置をして通信網を復旧する、契約上、法律[27]上の義務を持った者である。

それにもかかわらず、被告 1 ないし 6 は、このような義務を正しく履行しないという故意または過失により、前述のようなインターネット麻痺事件の発生を防止できなかったり、拡散させたりして、損害発生に対して責任があるとするものである。

被告 1 ないし 6 の責任の有無を分けるためには、先に詳述したインターネット麻痺事件がどのような原因により発生したのかを検証しなければならず、該当原因を検証するために、まず、インターネット通信網の構造と安定的な運用の要件を簡単に検証しておく。以下、順に記述する。

ア．インターネット通信網及びドメインネームシステムの構造

インターネット通信網は、パケット（Packet）交換の方式で運用されている。パケットは、情報を一定の大きさに分割して、各々に送受信のアドレスを付加して作ったデータブロックである。すなわちパケットは、データが含まれた小包と考えることができ、このような小包には、受信及び発信アドレス、その他オプションが書かれている。

ところで、インターネット通信網を通してこのようなパケットが転送されるためには、基本的サービスがさらに追加されなければならない。ドメインネームシステム（Domain Name System；DNS と略称）[28]がまさにそれである。

---

[27]「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 項によると、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われる情報通信網の安全性及び情報の信頼性を　確保するための保護措置を整備しなければならない。

[28]人が容易に理解できるように作られた、英文字、数字などからなるウェブサイトアドレス（ドメインネーム）を、コンピュータが理解できる 4 単位の数字のインターネットプロトコル（IP）アドレスに変える装置である。DNS は、電話システムの場合の交換機に該当するもので、IP アドレスを知らない場合、DNS を通してウェブサイトに接続できる。

DNS システムは、各コンピュータのインターネットプロトコル（Internet　Protocol；IP と略称)）アドレスを探し、これを連結するサービスとして、以下の順序で作業を進行する。例えばインターネットを通して大法院（最高裁判所）ウェブサイトに接続するためには、「203.240.67.150」という形態の IP アドレスを持った大法院（最高裁判所）ウェブサイトのサーバーコンピュータに接続しなければならないとする。しかし、通常のインターネット利用者らは、このようなアドレスを記憶できずにいるために、www.scourt.go.kr　という形態のドメイン名をウェブブラウザのアドレス窓に入力する。すると、コンピュータは該当使用者のインターネット通信環境に設定された該当ドメインネームサーバ（例えば、使用者のコンピュータ環境が、被告、ケイ・ティー（KT）の DNS サーバに連結するように設定されているならば、被告、ケイ・ティー（KT）の DNS サーバ）に、上記のドメイン名に該当する問い合わせを送る。

該当 DNS サーバは、問い合わせを受けた上記のドメイン名前に該当する IP アドレスを明らかにするために、段階的に IP アドレスを探していく。
すなわち、一番はじめに、ルートサーバ(Root　Server)に、一番終わり一の「kr」について問い合わせる。すると、ルートサーバは、該当情報を持っている「kr」ドメインサーバを知らせてくれる。その後、段階的に、「go.kr」情報を持った特定ドメインサーバを探した後、該当ドメインサーバに、「scourt.go.kr」について問い合わせをすれば、そのサーバが、該当 IP アドレス(「203.240.67.150」)を知らせてくれて、はじめて大法院（最高裁判所）ウェブサイトや該当Ｅメールアドレスを探して、使用できるようになる。

イ．インターネット麻痺事件に関連した、被告 1 ないし 6 の過失ならびに損害賠償責任

技術的に、インターネット麻痺事件が発生した当時の現況を要約しようとするならば、ドメインネームシステムが作動しなかったし、インターネット通信網の中の、もう少し根本的であるパケット伝送の一部が作動しなかったと理解される。

そうであれば、上記のようなドメインネームシステムがうまく動かない原因とは何であるかが事態把握の核心と考えられる。

上述において整理した通り、今回のインターネット麻痺事件の初めは、問題のスラマーワームが、急速に MS SQL サーバプログラムが装着されたコンピュータに広がって、ネットワークトラフィック(Traffic；着発信信号の数)を急増させたことによるものである。

ところで、当該MS-SQLサーバがインターネットデータセンターのような集積施設にあって、DNSサーバがインターネットデータセンターに共に設置されるように設計され、運用されている場合、上記のようなトラフィックの増加は、上記の感染サーバに連結したあらゆる装備、及び DNS サーバの通信も円滑にいかなくなるという影響を及ぼすようになる。したがって、DNSサーバを運営する者は、他の障害要因から分離して、危険要素が最小化されるよう、安定的運用をする義務があるとされるはずである。

また、上記被告は、DNSサーバについて、平常時よりトラフィックがはるかに急激に増加しうる種類のウィルス感染やワームの拡散に備えて適切な予備容量を確保し、これを管理することにより、ユーザが今回のようなインターネット麻痺事件を経験することのないよう注意する義務があり、さらにこうしたインターネット麻痺事件が発生したときには、即刻に分析、対応して、正しい措置を取ることによって、その被害が拡散するのを防いだり最小化したりする義務があると考えられる。

また、上記被告はインターネット通信網事業者として、安定したインターネット通信の運用のために、上記で指摘した安定した DNS サーバの運用以外に、ますます広がって行くウィルス、ワームの活動を持続的にモニタリングし、それにしたがって対応体制を整えるべき義務があるとされるはずである。

それにも拘わらず、被告1ないし6は、DNSサーバの分離、独立した構築、適切な予備容量の維持、事故発生時の適切な対応策の用意、ネットワークに対する事故発生前のモニタリング活動や、DNSサーバの点検等などの義務を疎かにし、また事件発生後に被害の拡散を防止するための措置を正しく取らなかった結果、インターネット麻痺事件が発生し、広がったものであり、原告はそれによる精神的、経済的な被害を被った。

一方、前述の不法行為責任と別個に、被告1ないし6は、原告1ないし1,189に対しては、上記で詳述したように、インターネット通信サービス契約関係を結んでいる。したがって被告 1 ないし 6 は各加入者(原告)らに対して、契約上の債務不履行責任によっても損害を賠償する理由があると考えることができる。

結局、被告 1 ないし 6 は、インターネット通信網事業者として、自己の故意または過失による不法行為によって原告らに損害を及ぼし、さらに、自己のインターネット通信網に加入した原告に対しては債務不履行によって損害を及ぼしたと考えられる。

４．被告大韓民国の損害賠償責任

ア．インターネット通信網サービスに対する管理などの義務の存在

被告大韓民国は、下記のような法律上の義務を負っている。

情報通信網利用促進ならびに情報保護に関する法律
第 4 条　第１項　情報通信部長官は情報通信網の利用促進ならびに安定した管理・運営と利用者の個人情報の保護などを通して、情報社会の基盤を造成するための施策を整備しなければならない。
第２項　第１項の規定による施策には、次の各号の事項が含まれなければならない。
第８号　情報通信網の安全性及び信頼性の向上

第 15 条　第１項　情報通信部長官は、インターネットサービス利用者の権益の保護と、インターネットサービスの品質の向上及び安定した提供を保障するための施策を整備しなければならない。

これ以外にも、情報通信部を含み、被告大韓民国は、情報通信基盤保護法に基づいて上記の法律第 2 条第 1 号の「情報通信基盤施設」の中のひとつであるインターネット通信網に対する侵害事故に対して、次の条項に基づいて事前に脆弱点を分析し、侵害事故発生時には、これに対する充分の対策を樹立するべき義務を負っている。

情報通信基盤保護法
第 5 条　第１項　主要情報通信基盤施設を管理する機関（以下「管理機関」という）の長は、第 9 条第 1 項の規定による脆弱点の分析・評価の結果に従い、所管主要情報通信基盤施設を安全に保護するための物理的・技術的対策を含んだ管理対策（以下「主要情報通信基盤施設保護対策」という）を樹立・施行しなければならない。

第 9 条　第１項　管理機関の長は、大統領が定めるところに従い、定期的に所管主要情報通信基盤施設の脆弱点を分析・評価しなければならない。

第 14 条　第１項　管理機関の長は所管主要情報通信基盤施設に対する侵害事故が発生したときには、当該情報通信基盤施設の復旧及び保護に必要な措置を迅速に取らなければならない。

イ．被告大韓民国の過失及び損害賠償責任

被告大韓民国は上記のような法律上の義務があるにもかかわらず、これに違反して充分なインターネット通信網事業者に対する管理・監督及びインターネット通信網の安定した運用計画の樹立、侵害事故への対応についての準備（脆弱点の分析、対策作り等）を怠ることによって、前述のインターネット通信網事業者が不法行為をするよう放置し、さらに以後の復旧対策の樹立過程でも、充分な注意義務を傾けることなく、損害に対して責任があると考えられるものである。

５．被告マイクロソフト社の損害賠償責任

ア．製造物責任

製造物の欠陥によって財産上の損害が発生した場合には、製造業者等は損害を被った者に、その損害を賠償しなければならない（製造物責任法第３条第１項）。

製造物とは、他の動産や不動産の一部を構成する場合を含んだ、製造または加工された動産をいう（同法第２条第１号）。
インターネット麻痺事件を触発させた契機になった、被告マイクロソフト社製作の MS　SQL サーバ（及び MSDE　2000；Microsoft　SQL　Server　2000　Desktop　Engine，以下「MS SQL サーバ」に通称する）は、大容量のデータを体系的に管理できるようにするプログラムであり、シーディーロム（CD-Rom）という動産の形態に製造されて販売される。したがって、製造物に該当する。

一方、被告マイクロソフト社が製造した MS　SQL サーバは、脆弱性が除去出来ないまま、市場に出され、スラマーワームと共に今回のインターネット麻痺事件を起こしたワームの出現によって、あっという間に感染して被害を産んだものである。
したがって被告マイクロソフト社が、このような脆弱性を除去できないまま、市場に出した過程で、充分な試験（extensive　testing）を経ないなどの、設計上の欠陥があるされるはずである。

さらに、一定の脆弱点が発見された場合、上記被告としては最善の対策を講じて、保安パッチファイルを開発、配布せねばならない。しかし、上記被告は充分な危険性を告知することもなく、さらに、保安パッチの必要性に対しても、自社に登録されたＥメールに一度だけ知らせたのと、ウェブサイトに掲載したにとどまり、より積極的な措置を取らなかった表示上の欠陥があるとすることができる。より積極的な措置とは、電話、訪問などの手

段や、これ以外にも、自動化サービスまたは自動防御装置（automatic defense system）を利用して、必須不可欠な保安パッチが設定され得るようにすることを意味する。

イ．不法行為責任

一方、被告マイクロソフト社は、上述した製造物責任の他にも、前述の「欠陥」を除去する義務があるにもかかわらず履行しなかった過失があり、これは民法第 750 条が定める不法行為責任にも該当すると考えられる。

６．原告等の損害発生とその損害額の範囲

ア．　別紙 1 目録の原告の損害

別紙 1 目録の原告は、被告 1 ないし 6 が運営するインターネット通信網サービスの加入者及びその他インターネット利用者である。
彼らは、2003 年 1 月 25 日 14 時 10 分頃から発生したインターネット麻痺事件によって、当日インターネットサービスを利用することができなかった。したがってインターネット麻痺事件によって、通常インターネットを利用する価値の損害が発生した。

さらに、原告によっては、当日、重要なメールの確認や、インターネットバンキングなどができずに、途方もなく大きい被害を被った場合もある。既にインターネットが生活必需品になった現在において、このような損害は、インターネット通信網サービス業者（被告 1 ないし 6）及び被告大韓民国、被告マイクロソフト社としては、当然、予見可能なことであって、特別な損害であるといっても、これもまた、賠償すべき損害の範囲に属するはずである（該当原告が被った損害については、以後、訴訟過程で、また特定し、立証する。）

また、このような財産上の損害以外にも、原告は、普段利用していたインターネットサービスを利用できないことによって、相当な精神的苦痛まで経験した。

イ．　別紙 2 目録の原告等の損害

別紙 2 目録中、番号 1 から 70 番の原告までは、いわゆる「PC 喫茶店」を運営する個人事業者であり、被告 1 ないし 6 からインターネットサービスの提供を受けて、これを一般利用者に、直接、提供する事業をしているものである。

また別紙 2 目録の番号 71 番の原告、株式会社コサン・アイアンドシー（以下「コサン・アイアンドシー」とする）の場合、被告ケイ・ティーの大容量インターネット通信網サービスの提供を受けて、これを「PC 喫茶店」事業者らに再販売する事業をしている。

上記別紙 2 目録の原告は、このように、インターネットの使用者であり、同時にインターネットサービス事業者であるがゆえに、今回のインターネット麻痺事件によってインターネットが全面的に中断された当日はもちろん、それ以後 2 日以上、思うように営業できないという財産上の損害を被った。

またさらに、上記のような財産上の損害以外にも、PC 喫茶店利用者（及び原告コサン・アイアンドシーの場合、顧客である PC 喫茶店事業者）に対し、インターネット利用についての信用を喪失して、今後の事業にかなり否定的な影響を及ぼすという、信用上の損害を被り、上記原告の今後の事業の展望に関連して、精神的苦痛を味わうことにもなった。

ウ.　　損害額の範囲

詳細な損害額の算出は、以後の訴訟過程で明らかにすることとし、まず別紙 1 目録の原告においては、財産上の損害及び慰謝料を合計して、各、金 50000 ウォンを、別紙 2 目録の原告の中、PC 喫茶店を運営する番号 1 ないし 70 番の原告においては営業損失に基づく財産上の損害及び慰謝料として、合計、金 300000 ウォンを、原告、コサン・アイアンドシーにおいては、その被害規模などに照らして、財産上の損害及び慰謝料として、合計、金 20000000 ウォンを一応請求するものである。

一方、上記損害は、被告の共同不法行為に因るものであるので、被告は上記損害賠償に関して、不真性連帯債務を負担しているといえる。したがって、被告は各自、原告にその損害を賠償するべきである。

７．結論

結論的に、被告は各自、財産上の損害及び慰謝料の合計額として、インターネット加入者及び利用者である別紙 1 目録の原告に各、金 50000 ウォン、PC 喫茶店事業者である別紙 2 目録 1 ないし 70 番の原告に各、金 300000 ウォン、インターネットサービス再販売業者である原告、株式会社コサン・アイアンドシーには金 200000000 ウォンを、及び上記各金額（金ウォン）に対して、不法行為発生日である 2003 年 1 月 25 日から、この事件訴状副本送

達日までは、民法所定の年 5%、その翌日から完済日までは、訴訟促進等に関する法律に所定する、年 25%の各利率に従い、遅延損害金を支給する義務があるとするものである。

立証方法

１．甲第１号証　　情報通信網侵害事故調査結果
その他の立証資料は、訴訟進行時に随時提出する。

添付書類

１．上記立証方法　　１通
１．訴状副本　　８部
１．納付書
１．法人登記簿謄本　９通
１．委任状
１．担当弁護士指定書

2003 年 4 月
原告の訴訟代理人
法務法人　ハンギョル
担当弁護士　　ハク・スンホン
担当弁護士　　チョン・ヨンスン
担当弁護士　　ユン・ボクナム
担当弁護士　　ヨ・ヨンハク
担当弁護士　　キム・テヒ

ソウル地方法院（裁判所）　　御中
別紙１目録
原告名簿
各個人名簿
（各加入ネットワーク別　　－上記被告１ないし６の順序に変更要望）

別紙２目録
原告名簿

PC 喫茶店事業主名簿
（委任状の順序に同じ）

訴訟 2

訴　　状

原告　　株式会社　インターパーク
訴訟代理人　法務法人　ハンギョル
担当　弁護士　ハク・スンフン、チョン・ヨンスン、ユン・ボクナム、ヨ・ヨンハク、キム・テヒ

被告　　マイクロソフト　コーポレーション

損害賠償（キ）請求の訴

ソウル地方法院（裁判所）　御中

訴　　状

原告　　株式会社　インターパーク
ソウル中区乙支路 2 街 185
代表理事　イ・キヒョン
訴訟代理人　法務法人　ハンギョル
ソウル　江南区　駅三洞　825-33　テヘランビルディング５、６、８階
（電話　02-3487-3000、ＦＡＸ　02-3787-3811）
担当　弁護士　ハク・スンフン、チョン・ヨンスン、ユン・ボクナム、ヨ・ヨンハク、キム・テヒ

被告　　マイクロソフト　コーポレーション(Microsoft　Corporation)
アメリカ合衆国　ワシントン州　レッドモンド　マイクロソフト　ウェイ　１番地
(One　Microsoft　Way、　Redmond、　WA　98052)
送達場所：株式会社　韓国マイクロソフト
ソウル　江南区　大峙 4 洞　892　ポスコセンター　西館６階

代表理事　コ・ヒョンジン

損害賠償（キ）　請求の訴

請求の趣旨

１．被告は原告に金 50000000 ウォン、及び上の各金額（金ウォン）に対して 2003 年 1 月 25 日からこの事件訴状の控えの送達日まで、年 5%、その翌日から完済日まで、年 25%の各利率による金額（金ウォン）を支給せよ。
２．訴訟費用は被告の負担とする。
３．第 1 項は仮執行することができる。
という判決を求める。

請求原因

１．当事者の地位
ア.　　原告の地位

原告は、www.interpark.com というドメイン名のウェブサイトを利用して、インターネットショッピングモールを運営するなど、電子上の取引による卸、小売業などを営業している法人である。

イ.　　被告の地位

被告は、米国に本社を置き、韓国の上記送達場所に支社をおいて、ソフトウエア製造、販売業を営んでいる会社である。

２．事件の概要　－損害賠償責任の発生との関連

2003 年 1 月 25 日に前後して発生したインターネット通信網の全面的な麻痺事件（以下「インターネット麻痺事件」という）の経緯を、現在までに明らかになった範囲で順序だてて注意深くみれば、次の通りである。（甲第 1 号証）。

2003 年 1 月 25 日 14 時 10 分ごろ、被告、株式会社ドリームラインで、インターネット通信網に対する異常徴候が発見され、報告された。

同日 14 時 35 分ごろから、インターネット通信網サービス提供事業者（Internet　Service Provider）である訴外、株式会社　ケイ・ティー、訴外、ハナロ通信株式会社、訴外、株式会社オンセ通信などのインターネット通信網に障害が本格的に発生し始め、エスケイ（SK）テレコム、ケイティーエフ（KTF)、エルジー（LG）テレコムなど、無線インターネットサービス提供業者のインターネット使用が不可能になった。
以後、21 時 30 分ごろ、コンピュータワクチン提供業者である、訴外、株式会社アン・チョルス研究所と、訴外、株式会社ハウリ等は、被告が製造、販売したコンピュータプログラムである、エムエス・エスキューエル・サーバ（MS　SQL　Server）2000（以下、「MS　SQL サーバ」という）の　脆弱点を利用した、スラマーワーム（Slammer　Worm）の拡散によって、2003 年 1 月 25 日インターネット麻痺事件が触発されたと明らかにした。

上記のようなインターネット麻痺事件の発生によって、インターネット通信網加入者及び利用者は、麻痺事件が発生した以後、正常化するまで相当な時間、インターネット通信を利用できず、インターネット通信網を利用してインターネットショッピングモールを運営する原告の場合、売上げ損失はもちろん、インターネットに対する顧客の信頼低下に基づく信用下落など、相当な損害を被ることになった。

これに対し、原告が被った損害の賠償を受けるために、本件、インターネット麻痺事件に対して責任のある被告を相手取り、本件、損害賠償訴訟を提起するに至ったものである。

３．被告の損害賠償責任

ア.　　製造物責任

製造物の欠陥によって財産上の損害が発生した場合には、製造業者等は損害を被った者に、その損害を賠償しなければならない（製造物責任法第 3 条第 1 項)。

製造物とは、他の動産や不動産の一部を構成する場合を含んだ、製造または加工された動産をいう（同法第 2 条第 1 号)。
インターネット麻痺事件を触発させた、被告製作の MS　SQL サーバ 2000（及び MSDE　2000；Microsoft　SQL　Server　2000　Desktop　Engine，以下「MS　SQL サーバ」に通称する）は、大容量のデータを体系的に管理できるようにするプログラムであり、シーディーロム（CD-Rom）という動産の形態に製造されて販売される。したがって製造物に該当する。

一方、被告が製造した MS　SQL サーバは、脆弱性が除去出来ないまま、市場に出され、スラマーワームと共に今回のインターネット麻痺事件を起こしたウォームの出現によって、あっという間に感染して被害を産んだものである。
したがって被告が、このような脆弱性を除去できないまま、市場に出した過程で、充分な試験（extensive　testing）を経ないなどの、設計上の欠陥があるとされるはずである。

さらに、一定の脆弱点が発見された場合、上記被告としては最善の対策を講して、危険性を告知し、保安パッチファイルを開発、配布せねばならない。しかし、上記被告は充分な危険性を十分に告知することもなく、保安パッチの必要性に対しても、自社に登録されたＥメールに一度だけ知らせたのと、ウェブサイトに掲載したにとどまり、より積極的な措置を取らなかった表示上の欠陥があるとすることができる。より積極的な措置とは、電話、訪問などの手段や、これ以外にも、自動化サービスまたは自動防御装置（automatic defense　system）を利用して、必須不可欠な保安パッチが設定され得るようにすることを意味する。

一方、このような被告の製造物の欠陥を利用したスラマーワームが開発されることによって、本件、インターネット麻痺事件が引き起こされたので、被告は、原告に被告の製造物の欠陥による損害を賠償する責任があるはずである。

イ．　　不法行為責任

一方、被告は、上述した製造物責任の他にも、前述の「欠陥」を除去する義務があるにもかかわらず、履行しなかった過失があり、これは民法第 750 条が定める不法行為責任にも該当すると考えられる。

４．原告の損害発生とその損害額の範囲

原告は、上記のようなインターネット麻痺事件が発生した当日、及び翌日まで、営業売上げが思うように発生しなかったことに基づく損害などの財産上の損害と、一般インターネット利用者について、ショッピングモール媒体としてインターネットに対する全般的信用下落などによる精神的損害を被った。

詳細な損害額の算出は、以後、訴訟過程で明らかにするが、上記、財産上の損害及び慰謝料をあわせて、金、50000000 ウォンを一応、請求するものである。

５．結論

結論的に、被告は、財産上の損害及び慰謝料の合計額として、原告に金、50000000 ウォンを、及び上記金額（金ウォン）に対して、不法行為発生日である 2003 年 1 月 25 日から、この事件訴状副本送達日までは、民法所定の年 5%、その翌日から完済日までは、訴訟促進等に関する法律に所定する、年 25%の各利率に従い、遅延損害金を支給する義務があるとするものである。

立証方法

１．甲第１号証　　情報通信網侵害事故調査結果
その他の立証資料は、訴訟進行時に随時提出する。

添付書類

１．上記立証方法　　1 通
１．訴状副本　　8 部
１．納付書
１．法人登記簿謄本　2 通
１．委任状
１．担当弁護士指定書

2003 年 4 月
原告の訴訟代理人
法務法人　ハンギョル
担当弁護士　　ハク・スンホン
担当弁護士　　チョン・ヨンスン
担当弁護士　　ユン・ボクナム
担当弁護士　　ヨ・ヨンハク
担当弁護士　　キム・テヒ

ソウル地方法院（裁判所）　　御中

訴訟 3

訴　　状

原告　　株式会社　オーマイニュース
訴訟代理人　法務法人　ハンギョル
担当　弁護士　ハク・スンフン、チョン・ヨンスン、ユン・ボクナム、ヨ・ヨンハク、キム・テヒ

被告　　株式会社　ケイ・ティー　他　7

損害賠償（キ）請求の訴

ソウル地方法院（裁判所）　御中

訴　　状

原告　　株式会社　オーマイニュース
　　ソウル　鍾路区　内需洞　167　大宇複合ビルディング　505 号
　　代表理事　オ・ヨンホ
訴訟代理人　法務法人　ハンギョル
ソウル　江南区　駅三洞　825-33　テヘランビルディング５、６、８階
　　（電話　02-3487-3000、ＦＡＸ　02-3787-3811）
担当　弁護士　ハク・スンフン、チョン・ヨンスン、ユン・ボクナム、ヨ・ヨンハク、キム・テヒ

被告　　１．株式会社　ケイ・ティー
　　城南市　盆唐区　亭子洞　206
　　代表理事　イ・ヨンギョン

　　２．ハナロ通信　株式会社
　　ソウル　瑞草区　瑞草洞　1445 の　3
　　代表理事　シン・ユンシク、イ・インヘン

３．株式会社　ドウルネット
ソウル　瑞草区　瑞草洞　1338 の　5
代表理事　イ・ホンソン

４．株式会社　デイコム
ソウル　江南区　駅三洞　706 の　1
代表理事　パク・ウンソ

５．ドリームライン　株式会社
ソウル　松坡区　新川洞　7 の　17
代表理事　イ・スンイル

６．株式会社　オンセ通信
城南市　盆唐区　亀尾洞　192 の　2
代表理事　ファン・キヨン

７．大韓民国
法律上　代表者　カン・クムシル
所管　情報通信部　長官

８．マイクロソフト　コーポレーション(Microsoft　Corporation)
アメリカ合衆国　ワシントン州　レッドモンド　マイクロソフト　ウェイ　１番地
(One　Microsoft　Way、　Redmond、　WA　98052)
送達場所：株式会社　韓国マイクロソフト
ソウル　江南区　大峙４洞　892　ポスコセンター　西館６階
代表理事　コ・ヒョンジン

損害賠償（キ）　請求の訴

請求の趣旨

１．被告は各自、原告に金 30000000 ウォン、及び上の各金額（金ウォン）に対して 2003 年 1 月 25 日からこの事件訴状の控えの送達日まで、年 5%、その翌日から完済日まで、年 25%の各利率による金額（金ウォン）を支給せよ。

２．訴訟費用は被告の負担とする。
３．第１項は仮執行することができる。
という判決を求める。

請求原因

１．当事者の地位
ア．　原告の地位

原告は、www.ohmynews.com というドメイン名のウェブサイトを利用して、インターネットニュース、通信、新聞発行業などを営業している法人である。

イ．　被告の地位

被告 1 ないし 6 は、それぞれ、インターネット通信網サービスを提供している企業等であり、被告大韓民国は、被告 1 ないし 6 に対して、インターネット通信網サービス提供を監督している情報通信部を傘下の機関に置いており、被告マイクロソフト　コーポレーション（以下。「マイクロソフト社」という）は、米国に本社を置き、韓国の上記送達場所に支社をおいて、ソフトウエア製造、販売業を営む法人である。

２．事件の概要　－損害賠償責任の発生との関連

2003 年 1 月 25 日に前後して発生したインターネット通信網の全面的な麻痺事件（以下「インターネット麻痺事件」という）の経緯を、現在までに明らかになった範囲で順序だてて注意深くみれば、次の通りである。（甲第 1 号証）。

2003 年 1 月 25 日 14 時 10 分頃、被告、株式会社ドリームラインで、インターネット通信網に対する異常徴候が発見され、報告された。
同日 14 時 35 分頃から、インターネット通信網サービス提供事業者（Internet　Service Provider）である被告、株式会社　ケイ・ティー（以下「ケイ・ティー」という）、被告、ハナロ通信株式会社、被告、株式会社オンセ通信などのインターネット通信網に障害が本格的に発生し始め、エスケイ（SK）テレコム、ケイティーエフ（KTF）、エルジー（LG）テレコムなど、無線インターネットサービス提供業者のインターネット使用が不可能になった。

以後、21時30分頃、コンピュータワクチン提供業者である、訴外、株式会社アン・チョルス研究所と、訴外、株式会社ハウリ等は、被告、マイクロソフト社が製造、販売したコンピュータプログラムである、エムエス・エスキューエル・サーバ（MS　SQL　Server）2000（以下、「MS　SQL　サーバ」という）の脆弱点を利用した、スラマーワーム（Slammer　Worm）の拡散によって、2003年１月２５日インターネット麻痺事件が触発されたと明らかにした。

上記のようなインターネット麻痺事件の発生によって、インターネット通信網加入者及び利用者は、麻痺事件が発生した以後、正常化するまで相当な時間、インターネット通信を利用できず、インターネット通信網を利用してインターネット新聞を発行する事業をしている原告の場合、広告損失と、インターネットに対する顧客の信頼低下に基づく信用下落など、相当な損害を被ることになった。

しかし、このような被害が発生したにもかかわらず、インターネット麻痺事件の発生後、相当な時間が経過したにもかかわらず、責任当事者である各被告は、その具体的な原因糾明、及びそれに基づく損害の保全に対しては、まだ明確な解決策を提示しないままである。

これに対し、原告が被った損害の賠償を受けるために、本件、インターネット麻痺事件に対して、責任がある被告を相手どり、本件損害賠償訴訟を提起するに至った。

以下に、各被告別に責任の根拠について、詳細に見ることにする。

３．被告１ないし６の損害賠償責任

被告１ないし６は、インターネット通信網サービス提供者として、安定したインターネット通信網を構成、運用して、今回のような麻痺事件が発生しないように、未然に防止し、万一、障害が発生した場合には、迅速に措置をして通信網を復旧する、法律上の義務を持った者である。

それにもかかわらず、被告１ないし６は、このような義務を正しく履行しないという故意または過失により、前述のようなインターネット麻痺事件の発生を防止できなかったり、拡散させたりして、損害発生に対して責任があるとするものである。

被告１ないし６の責任の有無を分けるためには、先に詳述したインターネット麻痺事件がどのような原因により発生したのかを検証しなければならず、該当原因を検証するために、

まず、インターネット通信網の構造と安定的な運用の要件を簡単に検証しておく。以下、順に記述する。

ア．インターネット通信網及びドメインネームシステムの構造

インターネット通信網は、パケット（Packet）交換の方式で運用されている。パケットは、情報を一定の大きさに分割して、各々に送受信のアドレスを付加して作ったデータブロックである。すなわちパケットは、データが含まれた手紙封筒と考えることができ、このような手紙封筒には、受信及び発信アドレス、その他オプションが書かれている。

ところで、インターネット通信網を通してこのようなパケットが転送されるためには、基本的サービスがさらに追加されなければならない。ドメインネームシステム（Domain Name System；DNS と略称）がまさにそれである。

DNS システムは、各コンピュータのインターネットプロトコル（Internet Protocol；IP と 略称））アドレスを探し、これを連結するサービスとして、以下の順序で作業を進行する。
例えばインターネットを通して大法院（最高裁判所）ウェブサイトに接続するためには、「203.240.67.150」という形態の IP アドレスを持った大法院（最高裁判所）ウェブサイトのサーバーコンピュータに接続しなければならないとする。しかし、通常のインターネット利用者らは、このようなアドレスを記憶できずにいるために、www.scourt.go.kr という形態のドメイン名をウェブブラウザのアドレス窓に入力する。すると、コンピュータは該当使用者のインターネット通信環境に設定された該当ドメインネームサーバ（例えば、使用者のコンピュータ環境が、被告、ケイ・ティー（KT）の DNS サーバに連結するように設定されているならば、被告、ケイ・ティー（KT）の DNS サーバ）に、上記のドメイン名に該当する問い合わせを送る。

該当 DNS サーバは、問い合わせを受けた上記のドメイン名前に該当する IP アドレスを明らかにするために、段階的に IP アドレスを探していく。
すなわち、一番はじめに、ルートサーバ(Root Server)に、一番終わり一の「kr」について問い合わせる。すると、ルートサーバは、該当情報を持っている「kr」ドメインサーバを知らせてくれる。その後、段階的に、「go.kr」情報を持った特定ドメインサーバを探した後、該当ドメインサーバに、「scourt.go.kr」について問い合わせをすれば、そのサーバが、該当 IP アドレス(「203.240.67.150」)を知らせてくれて、はじめて大法院（最高裁判所）ウェブサイトや該当Ｅメールアドレスを探して、使用できるようになる。

イ．インターネット麻痺事件に関連した、被告１ないし６の過失ならびに損害賠償責任

技術的に、インターネット麻痺事件が発生した当時の現況を要約しようとするならば、ドメインネームシステムが作動しなかったし、インターネット通信網の中の、もう少し根本的であるパケット伝送の一部が作動しなかったと理解される。

そうであれば、上記のようなドメインネームシステムがうまく動かない原因とは何であるかが事態把握の核心と考えられる。

上述において整理した通り、今回のインターネット麻痺事件の初めは、問題のスラマーワームが、急速にMS SQLサーバプログラムが装着されたコンピュータに広がって、ネットワークトラフィック(Traffic；着発信信号の数)を急増させたことによるものである。

ところで、当該MS SQLサーバがインターネットデータセンターのような集積施設にあって、DNSサーバがインターネットデータセンターに共に設置されるように設計され、運用されている場合、上記のようなトラフィックの増加は、上記の感染サーバに連結したあらゆる装備、及び DNS サーバの通信も円滑にいかなくなるという影響を及ぼすようになる。したがって、DNSサーバを運営する者は、他の障害要因から分離して、危険要素が最小化されるよう、安定的運用をする義務があるとされるはずである。

また、上記被告は、DNSサーバについて、平常時よりトラフィックがはるかに急激に増加しうる種類のウイルス感染やワームの拡散に備えて適切な予備容量を確保し、これを管理することにより、ユーザが今回のようなインターネット麻痺事件を経験することのないよう注意する義務があり、さらにこうしたインターネット麻痺事件が発生したときには、即刻に分析、対応して、正しい措置を取ることによって、その被害が拡散するのを防いだり最小化したりする義務があると考えられる。

また、上記被告はインターネット通信網事業者として、安定したインターネット通信の運用のために、上記で指摘した安定した DNS サーバの運用以外に、ますます広がって行くウィルス、ワームの活動を持続的にモニタリングし、それにしたがって対応体制を整えるべき義務があるとされるはずである。

それにも拘わらず、被告１ないし６は、DNSサーバの分離、独立した構築、適切な予備容量の維持、事故発生時の適切な対応策の用意、ネットワークに対して事故発生前のモニタリ

ング活動や、DNS サーバの点検等などの義務を疎かにし、また事件発生後に被害の拡散を防止のため措置を正しく取らなかった結果、インターネット麻痺事件が発生、広がったものであり、原告はそれによる精神的、経済的な被害を被った。

結局、被告 1 ないし 6 は、インターネット通信網事業者として、自己の故意または過失による不法行為によって原告に損害を及ぼしたと考えられる。

４．被告大韓民国の損害賠償責任

ア．　　インターネット通信網サービスに対する管理などの義務の存在

被告大韓民国は、下記のような法律上の義務を負っている。

情報通信網利用促進ならびに情報保護に関する法律
第 4 条　第１項　情報通信部長官は情報通信網の利用促進ならびに安定した管理・運営と利用者の個人情報の保護などを通して、情報社会の基盤を造成するための施策を整備しなければならない。
第２項　第１項の規定による施策には、次の各号の事項が含まれなければならない。
第１号ないし第７号　省略
第８号　情報通信網の安全性及び信頼性の向上

第 15 条　第１項　情報通信部長官は、インターネットサービス利用者の権益の保護と、インターネットサービスの品質の向上及び安定した提供を保障するための施策を整備しなければならない。

これ以外にも、情報通信部を含み、被告大韓民国は、情報通信基盤保護法に基づいて上記の法律第 2 条第 1 号の「情報通信基盤施設」の中のひとつであるインターネット通信網に対する侵害事故に対して、次の条項に基づいて事前に脆弱点を分析し、侵害事故発生時には、これに対する充分の対策を樹立するべき義務を負っている。

情報通信基盤保護法
第 5 条　第１項　主要情報通信基盤施設を管理する機関（以下「管理機関」という）の長は、第 9 条第 1 項の規定による脆弱点の分析・評価の結果に従い、所管主要情報通信基盤施設を安全に保護するための物理的・技術的対策を含んだ管理対策（以下「主要情報通信基盤施設保護対策」という）を樹立・施行しなければならない。

第 9 条　第１項　管理機関の長は、大統領が定めるところに従い、定期的に所管主要情報通信基盤施設の脆弱点を分析・評価しなければならない。

第 14 条　第１項　管理機関の長は所管主要情報通信基盤施設に対する侵害事故が発生したときには、当該情報通信基盤施設の復旧及び保護に必要な措置を迅速に取らなければならない。

イ.　　被告大韓民国の過失及び損害賠償責任

被告大韓民国は上記のような法律上の義務があるにもかかわらず、これに違反して充分なインターネット通信網事業者に対する管理・監督及びインターネット通信網の安定した運用計画の樹立、侵害事故への対応についての準備（脆弱点の分析、対策作り等）を怠ることによって、前述のインターネット通信網事業者が上記のような不法行為をするよう放置し、さらに以後の復旧対策の樹立過程でも、充分な注意義務を傾けることなく、損害に対して責任があると考えられるものである。

５．被告マイクロソフト社の損害賠償責任

ア.　　製造物責任

製造物の欠陥によって財産上の損害が発生した場合には、製造業者等は損害を被った者に、その損害を賠償しなければならない（製造物責任法第 3 条第 1 項)。

製造物とは、他の動産や不動産の一部を構成する場合を含んだ、製造または加工された動産をいう（同法第 2 条第 1 号)。
インターネット麻痺事件を触発させた契機になった、被告マイクロソフト社製作の MS　SQL サーバ 2000（及び MSDE　2000；Microsoft　SQL　Server　2000　Desktop　Engine，以下「MS　SQL サーバ」に通称する）は、大容量のデータを体系的に管理できるようにするプログラムであり、シーディーロム（CD-Rom）という動産の形態に製造されて販売される。したがって製造物に該当する。

一方、被告マイクロソフト社が製造した MS　SQL サーバは、脆弱性が除去出来ないまま、市場に出され、スラマーワームと共に今回のインターネット麻痺事件を起こしたワームの出現によって、あっという間に感染して被害を産んだものである。

したがって被告マイクロソフト社が、このような脆弱性を除去できないまま、市場に出した過程で、充分な試験（extensive　testing）を経ないなどの、設計上の欠陥があるとされるはずである。

さらに、一定の脆弱点が発見された場合、上記被告としては最善の対策を講じて、危険性を告知し、保安パッチファイルを開発、配布せねばならない。しかし、上記被告は充分な危険性を十分に告知することもなく、保安パッチの必要性に対しても、自社に登録されたＥメールに一度だけ知らせたのと、ウェブサイトに掲載したにとどまり、より積極的な措置を取らなかった表示上の欠陥があるとすることができる。より積極的な措置とは、電話、訪問などの手段や、これ以外にも、自動化サービスまたは自動防御装置（automatic defense　system）を利用して、必須不可欠な保安パッチが設定され得るようにすることを意味する。

イ．　　不法行為責任

一方、被告マイクロソフト社は、上述した製造物責任の他にも、前述の「欠陥」を除去する義務があるにもかかわらず履行しなかった過失があり、これは民法第 750 条が定める不法行為責任にも該当すると考えられる。

６．原告等の損害発生とその損害額の範囲

原告は、上記のようなインターネット麻痺事件が発生した当日、企業広告及び生活広告の営業売上げが直接、発生しなかったことに基づく損害、自発的有料化による後援支援金の未受納による損害などの財産上損害と、さらには、当日、記事を挙げられなかった 20,000 余人の記者の不便さ、広告業主からの信用下落、一般インターネット新聞購読者へのニュース媒体としてのインターネットに対する全般的信用下落などによる精神的損害を被った。

詳細な損害額の算出は、以後、訴訟過程で明らかにするが、上記、財産上の損害及び慰謝料をあわせて、金、30000000 ウォンを一応、請求するものである。

一方、上記損害は、被告の共同不法行為に因ったものであるので、被告は上記損害賠償に関して、不真性連帯債務を負担しているといえる。したがって、被告は各自、原告にその損害を賠償するべきである。

７．結論

結論的に、被告は各自、財産上の損害及び慰謝料の合計額として、原告に金、30000000 ウォンを、及び上記金額（金ウォン）に対して、不法行為発生日である 2003 年 1 月 25 日から、この事件訴状副本送達日までは、民法所定の年 5%、その翌日から完済日までは、訴訟促進等に関する法律に所定する、年 25%の各利率に従い、遅延損害金を支給する義務があるとするものである。

立証方法

１．甲第１号証　　情報通信網侵害事故調査結果
その他の立証資料は、訴訟進行時に随時提出する。

添付書類

１．上記立証方法　　１通
１．訴状副本　　8 部
１．納付書
１．法人登記簿謄本　8 通
１．委任状
１．担当弁護士指定書

2003 年 4 月

原告の訴訟代理人
法務法人　ハンギョル
担当弁護士　　ハク・スンホン
担当弁護士　　チョン・ヨンスン
担当弁護士　　ユン・ボクナム
担当弁護士　　ヨ・ヨンハク
担当弁護士　　キム・テヒ

ソウル地方法院（裁判所）　　御中

付録２.２. 韓国における法律改正をめぐる議論資料

インターネット侵害事故対応及び個人情報保護強化のための
情報通信網利用促進ならびに情報保護等に関する法律 改正（案）討論会

■ 一時： 2003 年 6 月 11 日(水) 10:00 ～ 15:00
■ 場所：韓国電算院　大会議室
■ 主催：情報通信部
■ 主管：韓国情報保護振興院

□討論会　プログラム□

時　間	主題	発表者／討論者
10:00-10:10	開会の辞	情報通信部次官
	第１主題：情報通信網情報保護分野（司会：カン　キョングン　崇実大教授）	
10:10-10:40	主題発表	
	－法律の改正方向 　国家・社会部門別の情報保護の水準向上　方案 －インターネット侵害事故対応方案	ファン　チョルスン 　情報保護企画課長 パク　ヨンウ 　韓国情報保護振興院チーム長 クォン　ホンヨン 　韓国電算院 先任研究員
10:40-11:20	指定討論	マ　フンニョル　教授 （スンチォンヒャン大） イム　チョンニン　教授 （高麗大） ムン　ヨンソン　教授 （崇実大、経実連情報通信委） チョン　ユンチョン　チーム長 （アン　チョルス研究所）
11:20-11:30	休息	
11:30-12:10	指定討論	アン　ヒョンシル　論説委員 （韓国経済） シン　ヨンチュン　事務局長 （韓国 ISP 協会） ユ　チャンハ　チーム長 （次のコミュニケーション）
12:10-12:20	質疑応答	
12:20-14:00	昼食時間	
	第２主題：個人情報保護分野（司会：カン　キョングン　崇実大教授）	
14:00-14:20	主題発表	
	－個人情報保護強化　方案	カン　ダルチョン 　韓国情報保護振興院　先任研究員

14:20-14:50	指定討論	チョン　ジュンヒョン　教授 （ソンムン大法学部） キム　ユンホン　情報人権局長 （ともに行う市民行動） キム　ホンジェ （情報通信部事務官）
14:50-15:00	質疑応答、閉会	

< 目　次 >

Ⅰ.　改正の背景

Ⅱ.　推進経過および主要な正の内容

Ⅲ.　情報通信網保護関連の改正事項

１．定義規定の新設

２．情報通信網の安全性の確保

３．集積情報通信施設事業者の緊急対応

４．情報保護の安全診断

５．情報保護管理体系の認証対象の拡大

６．情報保護の事前評価

７．利用者の情報の保護措置

８．インターネット侵害事故対応支援センターの設置

９．情報通信網侵害事故の申告及び対応

１０．情報通信網侵害事故の原因分析および資料保全命令

１１．韓国情報保護振興院の情報保護の役割強化

１２．韓国情報保護産業協会の設立

１３．罰則条項

Ⅳ.　個人情報保護関連の改正事項

１．個人情報の保護措置義務の強化

２．個人情報の処理の委託を受けた者に対する義務の強化

３．個人情報侵害および不法スパム関連の苦情処理に関する根拠の整備

４．個人情報の国外移転時の保護措置の強化

５．個人情報紛争調停委員会の小委員会制度の導入

６．クッキーなどを通した個人情報の収集・利用の規制

Ⅰ．改正の背景

○　情報化の進展により各社会部門がネットワークに相互に連結され、政府、企業その他の団体ならびに個人の活動は、情報システムとネットワークに絶対的に依存している。

－　しかし、情報システムとネットワークによって保存、伝達される情報は、非人（悪人）のアクセス、使用、誤用、変造、悪性コード伝送、サービス拒否またはシステム破壊のような多様な危険にさらされている。

○　特に、去る１月２５日のインターネット侵害事故は、従来のサイバー攻撃と違い、ネットワーク自体を攻撃して急速にインターネット網全体に障害を発生させる、新しい形態に変化している。

－　いまや、情報保護は特定の部門の問題でなく、情報システムとネットワークを利用する政府、企業、利用者全体の問題へと拡大され、すべての人が総体的に協調してこそはじめて効果的な対応が可能となる。

○　また、最近、個人情報管理上のセキュリティホールによって流出する事例が発生する等、個人情報保護に対する不安感が大きくなっており、個人情報保護に対する管理的措置の強化が必要である。

○　したがって、インターネットの公共性を勘案し、インターネットの安全性、信頼性を確保して、インターネットを利用する各利用者の責任と役割を向上するために、関連法律の改正を推進する。

Ⅱ.推進経過および主要な改正の内容

１．推進経過

○　2003 年 3 月 13 日　　：情報通信網保護対策政策討論会を開催

－　主要政策方案の発表ならびに関係専門家などの意見を収斂

○　2003 年 3 月 28 日　　：大統領年頭業務報告

－インターネット侵害事故対応支援センターの設置、情報保護事前評価制導入などを報告

○　2003 年 4 月　　：情報通信網保護対策細部計画を樹立

○　2003 年 5 月　　：法律改正専門担当作業班を構成、また改正案草案を準備

○　2003 年 5 月 27 日　　：主要内容を情報通信基盤保護実務委員会に報告

２．主要な改正の内容

□　インターネット侵害事故関連の主要な改正の内容

○　インターネット侵害事故発生時の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および役割

－　ISP、IDC、ワクチン業者などに対して侵害事故を迅速に報告させるようにし、侵害事故原因分析などのため、ログ記録保全命令制、現場調査権、資料提出要求権等を規定

○　個人、企業、政府など、各部門別の情報保護を強化

－　現在 IDC にだけ保護措置を義務化しているが、ISP、IDC、多重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することを規定

※情報保護コンサルティング専門業者などを通じて周期的な安全診断を実施し、KISA の安全診断基準ならびに技術開発、遠隔診断サービスの提供などの業務を規定

－　情報通信施設が集中している IDC の場合、重大な侵害事故の発生時に、IDC が入居している業者のサーバーに対して、異常トラフィックの遮断などの緊急措置をできる権限を附与

－　ISP を通した利用者の情報保護措置の強化

－　ソフトウエア業者は、保安パッチ情報を購買者に２回以上、告知

○　情報保護の投資拡大を促進

－政府、地方自治体などが、一定規模以上の情報化事業推進する時には、企画段階から情報保護要素を反映するように、「情報保護事前評価制」を導入

○　ハッキング、ウイルス流布などのサイバー犯罪の処罰を強化

○　その他、情報保護産業、情報保護産業協会の根拠規定の整備など

□　個人情報保護関連主要改正内容

○　個人情報保護のための技術的、管理的基準を整備して、情報通信サービス提供者にこの遵守を義務化

○　個人情報収集、処理などを委託する場合、受託者に対する委託者の管理、監督を明示して、受託者にも個人情報の不正乱用禁止などの義務を附与

○　紛争調整業務の効率的な遂行と、迅速で簡易な被害救済のために、５人以内の委員で小委員会を構成し、運営

Ⅲ．情報通信網保護関連の改正事項

「１　定義規定の新設」「２．情報通信網の安全性の確保」については省略

3．集積情報通信施設事業者の緊急対応

ア．新旧条文対比表

現行	改正案
<新設>	第 46 条の 2(集積情報通信施設事業者の緊急対応) ①集積情報通信施設事業者は次の各号のひとつに当該する場合は利用約款が定めるところにしたがって当該利用者または集積情報通信施設全体のサービ

	スの全部または一部を中断することができる。 1. 利用者の情報通信システムで発生した異常現象により他の利用者または集積情報通信施設のネットワークに障害を発生させる憂慮があると判断した場合。 2. 外部で発生した侵害事故によって深刻な障害が発生する憂慮があると判断した場合。 3. 侵害事故に関連して情報通信部または韓国情報保護振興院など関係機関の緊急処置要請がある場合。 ②集積情報通信施設事業者は第 1 項の規定によりサービスを中断した時には中断事由、発生日時、期間、内容などを明示して直ちに通報しなければならない。 ③集積情報通信施設事業者はサービスの中断事由が解消された場合、直ちに中断処置を撤回してサービスを再開しなければならない。

イ. 背景

o 集積情報通信施設事業者(IDC)に緊急な侵害事故が発生した場合、サービスを中断できる権利が事業者に付与されておらず、インターネット侵害事故の初期対応及び拡散防止が困難であった。

※ IDC : Interent Data Center

- 情報通信施設が集積されている IDC 侵害事故に関する迅速な対応及び拡大の防止のためには、サービス中断など緊急対応手段が必要である。

ウ. 現況及び問題点

o 集積情報通信施設の場合、情報通信網法及び下位法令で保護指針を規定しているが、サービスの性格上、物理的、管理的側面に重点を置いてあり、非常時に緊急対応の権限が付与されていない。

o 1.25 インターネット侵害事故時には、全国的に普及している超高速通信網を通してワームウィルスが急速に拡散し、感染サーバがある IDC 内でトラフィックが増加してインターネット接続が困難になった。

- IDC 内の少数のサーバが Slammer　Worm に感染し、IDC 内部ネットワーク構造及び Slammer　Worm の特徴上、IDC 内部ネットワークにトラフィックが暴走した。

エ. 国内・外の事例

(1) 国内事例

o 国内 IDC の現況

- サーバ及びネットワーク装備を一箇所に集めて、インターネット接続サービス及びサーバなどの保管、維持サービスを提供する事業者

- 2003 年 2 月基準、物理的な施設を保有する IDC は、15 個の事業者が IDC を運営中

※ 15 個の事業者と 33 個の事業所(KT、ドールネット、ドリームライン、オンセ通信、ハナロ通信、韓国インターネットデータセンター、エリームネットなど)

(2) 他の立法例、他の部門の事例

- 消防法

第 72 条(関係者などの消火義務) ①火災が発生した消防対象物の関係者は消防隊(消防機具を装備した消防公務員また義勇消防員で構成された組織体を言う。以下同様)が火災現場に到着するまで人を救出して火を消したり、火が広がらないようにするため、必要な処置をしなければならない。

- 検疫法

第 37 条(一般感染病の検疫処置) ①外国において検疫伝染病以外の伝染病が発生し、その病原体が国内に持ち込まれる憂慮がある場合には、保健福祉府令として、伝染病の種類を指定し、1 年以内の期間、本法の全部または一部を準用できる。

②第 1 項の場合において、監視または隔離期間は、当該伝染病の潜伏期を考慮して保健福祉府令でこれを定める。

第 38 条(非難港の入港時の処置) 船舶また航空機が緊急な危難を避けるために仕方なく検疫港に入港また着陸した際には、当該区域を管轄する保健当局に検疫伝染病患者または死亡者の有無その他を保健福祉府令の定めるところにしたがって報告した後、その指示を待たなければならない。

オ. 重要内容

(1) IDC 緊急対応権限付与

o 情報通信施設が集中している IDC の場合、侵害事故の発生時に IDC が入居している企業サーバに対して異常トラフィックを遮断し、緊急対応できるような権限を付与した。

(2) 重要内容

o 脆弱点及びウィルスに関連して注意を要するポートに対してモニタリングを強化し、必要時に一時的に遮断、運営

o 侵害事故時に顧客サーバで遮断処理を実施できる環境を助成

- 顧客サーバのネットワーク設備中、非常時にアクセス制御機能を設定できる設備を把握し、非常処置のためのアクセス権限を確保する。

o 緊急処置権の行使要件と内容

- IDC は利用約款に従い、利用者の同意を求めて緊急処置権を行使する。

- IDC は次の場合、顧客の利用約款による同意を得て、当該顧客または IDC 全体のサービスの一部または全部を中断する。

1. 利用者の情報通信システムに発生した異常現象により、他の利用者または集積情報通信施設のネットワークに障害を発生させる憂慮があると判断した場合

2. 外部で発生した侵害事故により、深刻な障害が発生する憂慮があると判断した場合

3. 侵害事故に関連して情報通信部または韓国情報保護振興院など関係機関の緊急対応の要請がある場合

（省略）

8. インターネット侵害事故対応支援センターの設置

ア. 新旧条文対比表

現行	改正案
<新設>	第 48 条の 2(インターネット侵害事故対応支援センターの設置などど) ①情報通信網侵害事故情報の収集、伝播、侵害事故の予報、警報及び迅速な対応のため、保護振興院にインターネット侵害事故対応支援センター(以下、「支援センター」という)をおく。 ②重要情報通信網接続サービス提供者は保護振興院と協約を締結して、第 1 項の規定による支援センターに侵害事故への対応支援に必要な攻撃類型別統計など、情報通信部令が定める統計を提供しなければならない。 ③第 2 項の規定によって締結した協約は、情報通信部長官の認可を貰わなければならず、情報通信部長官は相当な期間を定め、協約締結当事者に補完を命じることができる。 ④重要情報通信網接続サービス提供者は、正当な理由なしに第 2 項の規定による協約締結を拒否したり、その履行の遅滞または不履行をしてはならない。協約の変更の要請を受けた場合も同じである。 ⑤支援センターは第 2 項の規定による統計情報を、情報通信網侵害事故の対応のために必要な範囲に限って使用しなければならず、他の用途で不正に使用してはならない。

イ. 背景

o 1.25 インターネット侵害事故は従来のサイバー攻撃と異なり、ネットワークそれ自体を攻撃して急速に全インターネット網に障害を発生させる新たな形態に変化している。

- これに効果的に対応するため、ネットワークの異常トラフィックのモニタリングを通して、早期の予報、警報体制の構築が急務である。

ウ. 現況及び問題点

o 1月25日に国内に入ってきたSlammer　Wormは、毎秒1～5万個の攻撃パケットを大量に生成してネットワークを攻撃する悪性プログラムで、国内8千8百あまりのシステムが急速に感染した。

- Slammer　Worm はウィンドウズサーバ(MS-SQL2000)の脆弱点を利用して不特定多数のコンピュータを攻撃し、被害にあったコンピュータがまた他のコンピュータを攻撃してインターネットトラフィックを爆発的に増加させる。

※ 1.25 インターネット侵害事故の特徴

- 攻撃類型 : 個別システムの攻撃 → ネットワーク攻撃
- 被害範囲 : 局地的、個別的 → 全国的、広域的

o 現行インターネット侵害事故対応体系は、個別情報システム保護を主として構築されている。

- 侵害事故発生時に通報を受け付けて対応する体系として、事後復旧技術支援を主としており、早い時間内で全世界に拡散するウィルス拡散に効果的に対応するのが困難である。

o 1.25 インターネット侵害事故時に、ISP、管制企業などとの常時的な情報共有、及び緊急連絡体系の不備により、緊急対応及び原因分析に苦労した。

エ. 国内・外の事例

o アメリカの場合、本土安全部(Department of Homeland Security)傘下でサイバー攻撃対応業務を遂行する。

- 傘下の国家通信システム(NCS)で通信情報共有分析センター(ISAC)を運営中であり、通信 ISAC 主導でインターネットの健全性を監視する為の EWIS(Global Early Warning Information System)を構築し進行中である。

- NIPCは重要基盤施設の脆弱点の評価、サイバー攻撃警報の発令、サイバー攻撃関連の重要情報の提供を行う。

※ NIPC : National Infrastructure Protection Center

o 日本は経済産業省内にある情報処理振興協会(IPA)が情報保護関連情報の収集、動向の分析、ウィルス予報、警報の発令などを担当している。

※ IPA : Information technology Promotion Agency

- 最近、官民合同の「情報保安センター」を設立して、インターネットトラフィックの常時モニタリングを推進している。

o ヨーロッパの場合、ヨーロッパネットワーク情報保護機構(European Network and Information Security Agency)を設立し推進している。

o 大部分の国家において、コンピュータ侵害事故に対し、常時、対応できるような専門組織を設置している。

オ. 重要内容

□ 概要

o サイバー攻撃に迅速かつ効率的に対応するため、韓国情報保護振興院内に「インターネット侵害事故対応センター」を設置する。

- 各 ISP のネットワークトラフィックの異常徴候をモニタリングするシステムを設置して、年中 24 時間のモニタリング及び早期予報、警報体系を構築する。

- 侵害事故発生時、迅速に侵害事故原因を分析し、適切な対応処置を伝播し支援する。

□ 重要機能

o インターネット侵害事故情報を早期に総合的に収集、伝播する。

- 侵害事故の探知及び対応のために必要な攻撃類型の統計に関する情報を通信事業者から収集、分析する。

- インターネット侵害事故により、インターネット網それ自体が麻痺する場合でも、安全かつ持続的に通信できるよう、別途通信網を構築する。

o 侵害事故の分析、対応

- 侵害事故発生時における事故原因の分析による緊急対応

- ハッキング、ウィルスなどのサイバー攻撃情報の収集、分析

- ネットワーク脆弱点の通報の受付、関連情報の収集、技術支援

o 国内・外の情報共有及び共助

- ISP、アンチウィルスベンダ、情報保護企業、ソフトウエア製造者、国内・外の CERT、ISAC、メディアなどと連係体系を構築

- 国家安全保障会議(NSC)など国家非常対応体制と有機的な連係

同センターと個別ネットワーク間にはホットラインを構築して、サイバーテロに関する情報共有、異常徴候の早期発見及び一次的な対処を支援を行う。

同センターは個別ネットワークが公衆ネットワークを通してのハッキングやウィルス侵害事故の憂慮がある場合、個別ネットワーク所管部署にハッキングやウィルス関連の情報などの侵害事故関連の情報提供を行う。

□ 構成(案)

区分	重要内容
モニタリングチーム(15 名)	- 24 時間、ネットワークトラフィック、管制情報に関するモニタリング（5 名 3 交代） - ハッキング、ウイルス関連の重要サイトモニタリング - 予報・警報システムの運営 - NSC、災難管理庁と緊急連絡体系を維持
事故受付チーム(9 名)	- Cyber118、掲示板、メールなどを通して侵害事故を受付、処理
分析対応チーム(8 名)	- ハッキング、ウイルス技法及び対応方案の研究

	- 侵害事故への緊急対応及び復旧の支援 - 侵害事故分析のため現場調査及び重要ウイルスのサンプリング - 支援センターのシステム及びネットワークの維持、補修
対外協力チーム(8 名)	- ISP、管制企業などとの協助体系の構築及び情報協約の締結 - FIRST、APCERT、VB、AVAR などとのインターネット侵害事故情報

9. 情報通信網侵害事故の通報及び対応

ア. 新旧条文対比表

現行	改正案
<新設>	第 48 条の 3(侵害事故の通報など) ①情報通信サービス提供者、集積情報通信施設事業者、情報通信システム管理者などは、侵害事故の発生や侵害事故が発生する徴候を発見した時には、直ちにその事実を第 48 条の 2 の規定にしたがって支援センターに通報しなければならない。 ②第 1 項の規定により侵害事故の進行を受けた支援センターは、侵害事故予報、警報などの必要な処置を行わなければならない。

イ. 背景

o サイバー攻撃に迅速かつ効果的に対応する為、情報通信サービス提供者、IDC、情報通信システム管理者などに侵害事故を通報させるようにする。

- 急速に拡散する侵害事故の情報を早期に総合して対応する必要がある。

※ 1.25 インターネット侵害事故の場合、ISP、IDC が事故発生の通報をしておらず、状況の把握及び対応が困難であった。

ウ. 国内・外の事例

(1) 国外事例

o 日本の場合、情報通信網侵害事故に関連して、経済産業省公示を根拠にして、被害通報を勧告している。

※ コンピュータ不正アクセス対策基準及びコンピュータウイルス対策基準

- システム管理者、ネットワークサービス事業者、ハードウエア・ソフトウエア供給者は、不正アクセス及びウイルスによる被害の拡大と再発防止の為、必要な情報を経済産業省大臣が指定する者(情報処理振興事業協会)に通報する。

o アメリカはサイバー空間保護の為、国家戦略(2003 年 2 月)において、分析、徴候、警告のための能力開発の為、自発的な公共及び民間の間の情報共有の必要性を強調している。

(2) 他の立法例、他の部門の事例

□ 侵害事故の通報に関する他の立法例

- 消防法

第 71 条(火災の通報) ①火災を発見した人は直ちに消防署、警察署、市、郡または関係者に知らせなければならない。

- 災難管理法

第 17 条(災難の通報) ①誰でも災難の発生や災難が発生する徴候を発見した時には、直ちにその事実を市、郡、区また消防機関、その他関係機関に通報しなければならない。

②第 1 項の規定による通報を受けた市、郡、区また消防機関、その他行政機関の長は、直ちにこれを第 25 条の規定にしたがって地域緊急救助本部に通報しなければならない。

- 伝染病予防法

第 4 条(医者などの通報) ①医者また漢方医が伝染病患者など、または予防接種後の異常反応者を診断したり、医者がその死体を検案した時には、伝染病患者などや予防接種後の異常反応者またその同居人に消毒方法と伝染防止の方法を指示して、第 1 群、第 2 群、第 4 群の伝染病及び第 3 群の炭疽病と予防接種後の異常反応者の場合は直ちに、炭疽病を除く第 3 群及び指定伝染病の場合は 7 日以内に、伝染病患者などや予防接種後の異常反応者またはその死体の所在地を管轄する保健所長にその姓名、年齢、性別、その他事項を通報しなければならない。

②第 1 項の規定による診断基準、医者また漢方医が通報しなければならない伝染病患者などと予防接種後の異常反応者の範囲、通報手続きなどに関して必要な事項は保健福祉府令でこれを定める。

□ 侵害事故緊急処置に関する他の立法例

- 消防法

第 78 条(緊急処分) ①消防本部長、消防署長また消防隊長は、人を救出したり火を消すか拡大しないようにするために必要な時は、火災が発生した消防対象物及びその土地を一時的に使用したりまたその使用を制限したりその他の消防上必要な処分をすることができる。

②消防本部長、消防署長また消防隊長は、火または気象の状況やその他の周囲の事情を合理的に判断して、火が広がる事を防ぐ為に必要な場合には、広がる憂慮がある消防対象物またその消防対象物がある土地に対して第 1 項の規定にしたがって処分をすることができる。

③消防本部長、消防署長また消防隊長は、人を救出したりまた火を消すか拡大しないようにするために緊急であると判断した場合には、第 1 項及び第 2 項に規定した消防対象物及びその土地以外の消防対象物または土地に対しても第 1 項の規定にしたがって処分をすることができる。

④市、道は、第 3 項の規定による処分で損失を受けた者がいる場合には、これを補償しなければならない。

- 伝染病予防法

第 39 条(第 1 群伝染病予防処置) ①市、道知事は第 1 群伝染病の予防上、必要がある時には、次の各号の全部また一部を施行しなければならない。

1. 市町村の全部また一部の交通を遮断する事
2. イベント、集会、祭礼その他大勢の人の集合を制限または禁止する事
3. 健康診断また死体検案を実施する事
4. 伝染病の伝播の危険性がある飲食物の販売、受付を禁止し、またその廃棄やその他必要な処分を命じる事
5. ～ 13. 省略

エ. 重要内容

(1) 侵害事故の通報

o サイバー攻撃の発生時に、ISP、IDC、管制企業、アンチウイルスベンダ、電子商取引企業などに侵害事実を直ちに支援センターへ通報させるようにする。

(2) 通報者の範囲、通報対象となる侵害事故の種類及び範囲

o 通報者の範囲

- 情報通信サービス提供者、集積情報通信施設事業者、情報保護事業者、システム管理者など

o 通報対象 : インターネット侵害事故

o 通報方法

- Cyber118(地域番号なし：118 番)、インターネット侵害事故対応支援センターホームページの掲示板、メール、ファクスなどを通して侵害事故を通報

(3) 緊急処置の重要内容

o ハッキング、ウイルスの総合通報及び緊急の情報伝達

o 侵害事故の分析及び技術支援

o 緊急対応処置など

10. 情報通信網侵害事故の原因分析及び資料保存命令

ア. 新旧条文対比表

現行	改正案
<新設>	第 48 条の 4(侵害事故の原因分析など) ①情報通信網を保有した者は、侵害事故が発生した時には、侵害事故の原因を分析して被害拡散を防止しなければならない。 ②情報通信部長官は、情報通信網に重大な侵害事故が発生した時には、事故対応及び復旧と再発防止の為、当該事故の原因分析をすることができる。

	③重要情報通信網接続サービス提供者は、情報通信網に接続した重要設備への接続情報、提供サービス及び保安に関連した誤謬発生記録(以下「通信網接続記録など」という)を定期的に収集、分析するシステムを構築、運営しなければならない。 ④情報通信府長官は第 1 項の規定による原因分析のため、必要だと判断した際には情報通信サービス提供者に通信網 接続記録など侵害事故関連資料の保存を命じる事ができる。 ⑤情報通信部長官は侵害事故の原因分析のために必要な場合には、情報通信サービス提供者に侵害事故関連資料の提出を要求することができ、所属公務員または情報通信部長官が指定する者に関係者の事業所へ出入して侵害事故の原因を調査させる事ができる。 ⑥第 5 項の規定にしたがって提出した資料及び調査を通して明らかになった情報は、侵害事故の原因分析及び対策準備以外にはこれを使う事はできず、原因分析が終了した後はこれを破棄しなければならない。 ⑦第 2 項の規定による侵害事故関連資料の保存対象、保存期間及び提出資料を保護するための管理対策、第 3 項の規定による調査を遂行する者の資格、指定手続き、調査手続き等に必要な事項は大統領令でこれを定める。

イ. 背景

o 侵害事故に対する被害拡散の防止、侵害事故の再発防止などのためには詳細な原因分析が必要である。

- 侵害事故の原因分析のための資料保存、調査などができる法的根拠の整備が必要である。

ウ. 現況及び問題点

o 侵害事故が発生した場合、迅速な原因分析のため、関連資料を関係専門家が分析して対応しなければならないが、

- 関連資料が喪失して調査できない場合が多く、
- 関連資料が存在する場合であっても、これを調査する法的な根拠が不備なため、原因分析業務の遂行が困難である。

o 通信網接続記録などの保存は、業界の自律に任せてあるが、大部分の保存期間が短く、侵害事故発生後、原因分析の時点では、当該記録が存在しない可能性もある。

エ. 国内・外の事例

(1) 国外の事例

□ ログ記録の保存命令

o 「EU サイバー犯罪協約」では、通信記録保存命令、技術的手段を使った実時間収集、記録、関連事実に対するサービス事業者の秘密遵守義務を規定している。

※ サイバー犯罪協約は、ヨーロッパ会議(Council of Europe)が中心となって、サイバー空間上で発生する各種犯罪を処罰できるよう各国の国内法を整備するようにし、多様な国際共助手続に従うようにすることで、国際社会のサイバー犯罪に効率的に対処するために作られた国際協約である。(2001 年 11 月 23 日制定)

※ APEC 及び OECD 会議では、各国のサイバー犯罪関連法をサイバー犯罪協約の水準に訂正するよう勧告した。(2003 年 10 月までに法律の整備を合意)

o アメリカの場合は、“ Electronic Communications Privacy Act of 1986 ” Sec2703 を根拠として、

- 政府機関はインターネットサービス提供者に対し、電子的な記憶装置内にある特定資料の保存を要請することができる。(最大 180 日)

(2) 他の立法例

- 消防法

第 81 条(火災原因と被害の調査) ①消防本部長また消防署長は、火災が発生した時には、その火災原因と火災また消火により生じた損害を調査しなければならない。

②第 1 項の調査は消火活動と同時に始めなければならない。

第 82(強制調査権) ①消防本部長また消防署長は、第 81 条第 1 項の規定による調査を行うために必要な場合には、関係者に対して必要な報告また資料の提出を命じたり、関係公務員に関係場所に出入させて、その火災原因と被害状況を調査させたり、関係者に質問することができる。

②第 5 条第 1 項但書、第 4 項及び第 5 項の規定は第 1 項の場合にこれを準用する。

- 家畜伝染病予防法

第 16 条(家畜取引記録の作成、保存など) ①農林府長官は家畜伝染病が広がる事を防止するために必要と判断した場合には、家畜の所有者などに家畜取引の記録を作成、保存させることができる

②農林府長官は第 1 項の規定によって家畜取引の記録を作成、保存させる時には、対象地域、対象家畜の種類、記録の書式及び保存期間などを定めて告示しなければならない。

オ. 重要内容

o インターネットに相当な影響を与える侵害事故が発生した場合、再発防止などのために、情報通信部長官は、ISP などにログ記録の保存を命令できる(情報通信網法 改正)。

o ISP 等の過度な負担を防止するため、保存対象のログ記録の範囲を必要最小限に限定する。

- 対象設備と記録内容、期間を特定(例:oo 所在、oo 設備が記録した 02:00 から 04:00 までの記録)

o ネットワーク全般にわたって重大な侵害事故が発生した時、情報通信部長官は侵害事故の原因分析と対策の樹立のために必要な場合には、

- 関係職員及び専門家に現場調査をさせ、

- ISP などに関連侵害事故の関連資料を提出するように命令することができる。

（省略）

以上