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　報告書改訂版

2019 年 3 月

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

序

「情報セキュリティ早期警戒パートナーシップ」（以下、「早期警戒パートナーシップ」という）は、基本的な枠組みが構築された後、2004 年 7 月 8 日より運用が開始された。当該運用は、世界的にみて先駆的なこころみとなり、世界的な脆弱性対応の動きをリードするものとなっている。

脆弱性情報取扱の法律問題研究会が 2004 年に公表した「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」（以下、「法律面の調査報告書（2004 年版）」という）は、脆弱性をめぐる法律問題を広く論じるとともに、脆弱性情報の取扱いルールの必要性とその意義を考察するものであった。そのような考察の対象が広範であったこともあり、その後の早期警戒パートナーシップの運営の際に、生じる問題について法的な観点からの考察を与えるものとして、一定程度、安定した運営の助力となったものである。

しかしながら、その後、早期警戒パートナーシップの基礎となる告示の改正もあり、また、早期警戒パートナーシップ自体も、公表判定委員会制度の創設、重要度の高い脆弱性についての優先的取扱いなどのような制度の改正があったこともあり、法律面の調査報告書（2004 年版）のいくつかの点について、修正・追加をなすとともに、記述を現在の制度に合わせて理解しやすいように整える必要があると判断するにいたった。また、法律面の調査報告書（2004 年版）においては、脆弱性をめぐる問題を広く捉えようという観点から捉えるあまりに冗長となった記述も散見された。そこで、法律面の調査報告書の第一章については、若干の記述を追加して、全体の構成を整え、また、記述を整理して簡潔なものとするとともに、従前の第三章の記述も参考に、「情報セキュリティ早期警戒パートナーシップガイドライン」（以下、「P ガイドライン」という）における法的な意味をもつ関連記述に対する解説を作成した。また、従前の第二章(第 2 章 米国における脆弱性情報と法的論点)および付録を削除し、現在における我が国の早期警戒パートナーシップの運営に参考になる記述に集約するものとした。

本報告書が、早期警戒パートナーシップの今後の発展にいくらかでも貢献することがあれば、望外の喜びである。

株式会社 IT リサーチ・アートの高橋郁夫が、今回の改訂を担当したが、本報告書の記述には、2004 年版の記述の相当部分を維持している。今回の改訂に際して、2004 年版の記述を担当いただいた土井弁護士、池村弁護士には、改訂を快諾いただいた。両氏には、重ねて感謝の意を記したい。

目 次

1. 脆弱性情報の取扱いルールと法律とのかかわり

脆弱性情報の取扱い体制である、情報セキュリティ早期警戒パートナーシップについて、その背景や法律との関係等について解説する。

1.1 総論

本節では、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等について述べる。

1.1.1 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、結社及び言論、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。

脆弱性情報については、自由な流通が望ましいという考え方（完全開示の考え方といわれる）がある。この考え方は、その根拠として、（1）悪意ある攻撃者は、脆弱性情報をすでに知っており、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）そして、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っている。

これに対して、責任ある流通の仕組みが必要であるといういわば「責任ある開示」の考え方がある。これは、（1）脆弱性の大多数は、脆弱性を解消するという目的よりも、自己の力量の顕示などの公開すること自体が目的であるという動機によって導かれて調査され、公開される（2）脆弱性を公開するにも効果的な他の方法が有り得る（3）より良いシステムを作るためといっても脆弱性情報の詳細を教えたりテストしたりする必要はない、などという考え方にもとづくものである。また、この考え方は、近時においては、「協調された開示（coordinated vulnerability disclosure）」ともいう例が増えている。[1]

どちらにしても、この脆弱性情報の開示についてのルール制定というのは、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は留意が必要である。

[1] 具体例として“Coordinated Vulnerability Disclosure”（https://www.microsoft.com/en-us/msrc/cvd?rtc=1）、National Telecommunications and Information Administration (NTIA)“”Early Stage” Coordinated Vulnerability Disclosure Template Version 1.1”
（https://www.ntia.doc.gov/files/ntia/publications/ntia_vuln_disclosure_early_stage_template.pdf）などがある。

1.1.2 取扱いルールの必要性

上述の問題に関して、2003 年度に独立行政法人情報処理推進機構において脆弱性情報取扱いガイドライン WG が設置された。当該 WG においては、脆弱性情報に関して、脆弱性関連情報の流通に関するルールが明らかではないことによって、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、共有がはかられず、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、それに対して望ましいルールが提唱されるべきであると提言された。このような認識のもと、2004 年に経済産業省の「ソフトウエア等脆弱性関連情報取扱基準」告示（平成 16 年経済産業省告示第 235 号、なお、以下、「平成 16 年告示」という）とそれに基づく「情報セキュリティ早期警戒パートナーシップガイドライン」が定められて、早期警戒パートナーシップの運営が開始された。「早期警戒パートナーシップ」とは、告示及びガイドラインに基づいた、関係者間における脆弱性関連情報の取扱いに係る有機的なプロセスをいう。IPA 及び JPCERT/CC が、一般社団法人電子情報技術産業協会、一般社団法人コンピュータソフトウェア協会、一般社団法人情報サービス産業協会、特定非営利活動法人 日本ネットワークセキュリティ協会と連名で策定している「情報セキュリティ早期警戒パートナーシップガイドライン」に従い、発見者・製品開発者・ウェブサイト運営者らが、脆弱性関連情報を取り扱っていくことを中核としている。

1.1.3 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、2004 年当時において欠けていたものと認識されていた。これらの機能を実現するために、上記平成 16 年告示（その後、平成 26 年に改正された）は、関係の機関を、そのような機能を担わせるものとして整理し、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ことによって、実現しようとしたものである。

1.1.4 その後の発展

情報ネットワーク社会の発展に伴って、脆弱性を巡る社会的な状況は、種々の面で、変化を遂げている。具体的には、社会的にきわめて重要な意味を有するようになってきていること、製品開発者においてもソフトウエア製品等における脆弱性の対応が重要であるとの認識が高まってきていること、国際的にも、脆弱性情報に対する対応に関する標準的なルールづくりの努力が開始され、標準が認識されるようになったこと、また、それとともに、脆弱性に関して法的な枠組のもとに置こうとする動きが生じてきたことがあげられる。このような状況のもとで、早期警戒パートナーシップも社会的に広く認知されるに至ったが、その一方で、届出件数の増大、事務処理の停滞といった現実的な問題も生じるようになった。

脆弱性の社会における重要性の増大というのは、脅威の変質・攻撃手法の変質・被害の変

質などに応じるものである。サイバーセキュリティに対する脅威は、攻撃者が自らの興味や自己顕示欲の赴くままに個別的に攻撃をなすという従来のものから、金銭的な欲求を背景にした組織的なもの、国家関与の窺われる執拗なものなどに変わってきている。また、攻撃手法も、攻撃を自動化するツールを悪用すること等によって、大規模、組織的な手法を用いることが一般化・容易化してきている。これらの攻撃の端緒として、特に脆弱性対策情報が公表される前の、いわゆるゼロディの脆弱性が悪用されることが多い。また、被害の変質というのは、多大な金銭的な損害を引き起こしたり、場合によっては、大規模な国家経済的なマヒを引き起こしたり、制御機器をコントロールしたりすることよって人身被害／財産被害を惹起するものになってきたということである。その意味では、従来は、単なるネットワーク内における情報の機密性・完全性・可用性の問題であったものが、国家の独立性をおびやかす一因となりうるとまで認識されるにいたってきたということになる。

開発者が脆弱性情報に対応する役割を見直しつつあるという動きというのは、当初の告示・P ガイドラインが制定された 2004 年時点においては、脆弱性という用語それ自体になじみがなかったし、それとソフトウエアの欠陥との違いというのも意識して議論されていることがなかった。また、開発者において、脆弱性をできるかぎり解消した製品を社会に提供するのが望ましいものであるという認識も非常に乏しかった。発見者から、脆弱性の報告を受けたからといって、むしろ、製品に対して何かクレームをつけられているかのような対応をとる開発者もいたといわれたところである。しかしながら、現在においては、脆弱性のもたらすセキュリティ上の脅威が社会においても許容しうるものではないという認識が一般化しつつある。開発者が、積極的に、脆弱性の届出受け付けの窓口をもうけるようになってきている [2]。制度が構築された時期と比較して、セキュリティの重要性の認識／脆弱性解消の努力の正当な評価という観点からすると、非常に良い方向に進展していると評価することができる。そもそも、開発者の提供するソフトウエアが脆弱性なく安心して使えることは、現代社会においては、本来であれば、他の性能などと総合的に正当に評価されるべきひとつの要素である。ソフトウエアの利用者が、その開発者のセキュリティに対する積極的な対応姿勢などをも踏まえた総合的な判断をベースにソフトウエアを選択し、すぐれたものが社会に受け入れられるようになり、その一方で、脆弱性対応などに劣ったソフトウエアは、利用者の評価で劣ったものとして支持をうしなうものとなって、社会で利用されなくなり淘汰されるというのが望ましい姿である。このようなあるべき姿にむけて、社会においてプログラムの脆弱性を減らしていこうという意識が高まっているというのは、きわめて重要な動きであるということができる。

国際的な脆弱性情報に対する標準的なルールづくりについては、脆弱性取扱い手順に関しては、「情報セキュリティーセキュリティ技術　脆弱性取扱過程（ISO/IEC 30111:2013 Information technology -- Security techniques -- Vulnerability handling processes）」、脆弱性開示に関しては、「情報セキュリティーセキュリティ技術　脆弱性開示（ISO/IEC 29147:2018 Information technology -- Security techniques -- Vulnerability disclosure）」が制定、公表されている。

脆弱性と法的な関係に関しては、我が国におけるサイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律（平成 28 年法律第 31 号）をあげることが

[2] 脆弱性を発見したものに報奨金を出す制度（バグ・バウンティ制度ともいわれる）を採用している会社もある。

できる。情報処理の促進に関する法律（昭和 45 年法律第 90 号。以下「情促法」という。）の改正において、情促法 43 条 3 項に、IPA が必要があると認めるときには、サイバーセキュリティの確保のために電子計算機を利用する者が講ずべき措置の内容を公表することができるとの規定を設け、脆弱性情報に係る公表について法律上の根拠が与えられることとなった。これらの改正に対応して、2017 年 2 月 8 日には、平成 26 年告示を廃止し、新たに法律に根拠を置く「ソフトウエア製品等の脆弱性関連情報に関する取扱規程（平成 29 年経済産業省告示第 19 号。以下「取扱規程」という。）」が定められた。

国際的には、脆弱性情報や当該脆弱性を悪用するエクスプロイトのソースコードなどについて、国境を越える場合に対して輸出規制等をはじめとして、法的な規制が準備されている。ワッセナー・アレンジメント[3] において「侵入ソフトウエア」「IP ネットワーク監視」が管理品目に追加された（2013 年 12 月）のに対応して、外国為替及び外国貿易法における輸出管理の対象となっていた。その後、外国為替令及び輸出貿易管理令の改正およびそれに関する省令の改正によって、セキュリティの脆弱性の開示等にかかる技術の除外規定が追加される（貨物等省令 20 条第 1 項及び 2 項）とともに、侵入ソフトウエアに係る技術の除外規定の追加がなされている（同 2 項 6 号）。

1.1.5 運用の実態と早期警戒パートナーシップの現在

早期警戒パートナーシップは、2004 年 7 月に平成 16 年告示に基づく届出受付を開始して以来、届出の件数は、ソフトウエア製品に関するものが 4,266 件、ウェブアプリケーションに関するものが 9,866 件になり、修正が完了した件数は、ソフトウエア製品に関するものが約 1,936 件、ウェブアプリケーションに関するものが約 7,346 件になっている（2018 年 12 月末時点）。こうした実績を踏まえれば、関係者による協力の下で脆弱性関連情報の取扱いがなされており、早期警戒パートナーシップの果たしている役割は大きいと思われる。

また、早期警戒パートナーシップの運用上の問題点については、IPA で開催されている「情報システム等の脆弱性情報の取扱いに関する研究会」（以下、脆弱性研究会という）において議論・検討され、「情報セキュリティ早期警戒パートナーシップガイドライン」も度重なる改訂を重ねている。かかる改訂によって、公表判定委員会制度、影響度の大きい届出に関する優先取扱い制度などの制度が追加されている。

このような制度の発展の一方で、届出件数の増大、事務処理の停滞といった現実的な問題も生じている。

1.2 脆弱性情報取扱い体制の法的意味

現在の早期警戒パートナーシップは、「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」という経済産業省告示をもとにした「情報セキュリティ早期警戒パートナーシップガイドライン」という「ガイドライン」でもって、脆弱性関連情報についての一定のルールを整備しようというものである。従って、最初に、この体制の有する法的意義については（1）告示の法的性格（2）告示・P 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

[3] 正式には、「通常兵器及び関連汎用品・技術の輸出管理に関するワッセナー・アレンジメント（The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies）」

討しておく必要がある。

1.2.1 告示の法的性格[4]

告示とは、行政措置の公示の形式をいう。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おり、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相当な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、環境基本法 16 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ある規範ではないが、しかし、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。

取扱規程についていえば、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。

1.2.2 告示・P ガイドラインと国民の権利との関わり

「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、P ガイドラインも同様である。しかしながら、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。取扱規程は、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。具体的には、違法性の阻却の側面と違法評価の側面とがあるものと考えられる。つまり、脆弱性関連情報に関する行為の社会的な相当性が判断されるにあたって、早期警戒パートナーシップに則った行為をなしていることが、そのひとつの要素として考慮されるということである。本件体制が、そのような影響を与える事例として理解することができるであろう。

---

[4] 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）

1.2.3 告示・P ガイドラインの適用範囲

告示・P 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。

この告示・P 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、法の適用に関する通則法（平成 18 年 6 月 21 日法律第 78 号）17 条の「不法行為によって生ずる債権の成立及び効力は、加害行為の結果が発生した地の法による。ただし、その地における結果の発生が通常予見することのできないものであったときは、加害行為が行われた地の法による。」という文言によることになる。その意味で、脆弱性関連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、取扱規程・P ガイドラインの適用があるとされるのも合理的である。このような観点から、従前から、P ガイドラインにおいて適用範囲がさだめられていたが、取扱規程は、第 1　総則 4　において「本規程の適用範囲」として「本規程は、日本国内で利用されているソフトウエア製品又は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に係る脆弱性であって、その脆弱性に起因する影響が不特定又は多数の者に及ぶおそれのあるものに適用する。」と明らかにしている。

2018 年度脆弱性研究会での検討を経て改訂した P ガイドラインにおいて、ウェブサイトに関する適用に関して、「日本国内からのアクセスが実質的にな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」とされているのは、かかる趣旨によるものである。ここで、実質的な関連があること、もしくはアクセスが実質的になされていること、は、脆弱性情報取扱い体制を利用して調整すべき程のものであるか、という観点から判断される。

1.2.4 他の安全規制との関係

脆弱性情報取扱い体制については、有体物をソフトウエアでコントロールする場合について、そのコントロールしているソフトウエアの脆弱性についても、当然に適用の対象となる。ソフトウエアでコントロールされている有体物については、種々の法的観点から、いわゆる安全規制が準備されている。例えば、電気事業法 39 条 1 項は、「事業用電気工作物を設置する者は、事業用電気工作物を主務省令で定める技術基準に適合するように維持しなければならない。」と定めており、電気設備に関する技術基準を定める省令　（平成 9 年 3 月 27 日通商産業省令第 52 号）が、この技術基準を明らかにしている。ところで、例えば、電気工作物（一般送配電事業、送電事業、特定送配電事業及び発電事業の用に供するものに限る。）の運転を管理する電子計算機のソフトウエアに脆弱性があった場合には、事業用電気工作物が上記技術基準に適合している状況が脅かされる可能性があるかもれしれない。その一方で、当該脆弱性は、早期警戒パートナーシップによる調整の対象となることになる。この場合に、脆弱性への対応が十分になされることがなく、当該電気工作物のサイバーセキュリティの確保に問題が生じており、それとして、技術基準違反の状態が生じうる可能性があり、電気事業法の安全確保のための規定の適用がなされるとしても、そのことと、本脆弱

性情報取扱い体制についての規定が適用されることとは、また、別の問題であり、それぞれ別個のものとして適用されるものと考えられる。

1.3 脆弱性の意義と諸問題

1.3.1 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。

「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は明らかになった。ところで、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「脆弱性」が、法的にどのような意義をもつかという点について、事前の問題として検討しておくことは有意義である。

1.3.2 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は、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。[5]また、契約書中もこの点に関して定義規定を設ける例は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。[6]一方、JIS X 0014-1999 では、「障害」という用語のもとに論じられており、「障害」は「要求された機能を遂行する機能単位の能力の、縮退又は喪失を引き起こす、異常な状態」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。

ISO/IEC29147（2018）においては、「脆弱性」は、「セキュリティポリシに明示もしくは黙示に違反する製品またはサービスの機能的振る舞い」と定義されている（3.1）。そして、概念（5 Concepts）において、脆弱性は、「一般的に、セキュリティポリシの違反を明示的に／黙示的に引き起こす挙動もしくは条件のセット」であるとされている（5.4.5）。

これらの点をもとに「脆弱性」については、以下のような要素から定義をすることが可能である。すなわち、（1）不具合であること－プログラム等が意図した結果をもたらさない状態であること（2）セキュリティに関すること－少なくても、その「不具合」が、電子計算機の運用に関する機密性、完全性、可用性に関連するものであること、（3）（1）の不具

[5] 早期警戒パートナーシップの開始にあたって、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」がこの点を明らかにした。

[6] 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

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つ観点が必要である。このような考察のもと、取扱規程は、「第１　総則　3 定義（3）脆弱性」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、アクセス制御機能により保護すべき情報等に不特定又は多数の者がアクセスできる状態を含む。）をいう。」としている。

1.3.3 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

(1) ソフトウエアの概念と開発の概念

ソフトウエアは、「情報処理システムのプログラム，手続き，規則及び関連文書の全体又は一部分」と定義されている（JIS X 0001-1994）。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、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するものである。[7]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ろう。この過程の中で、法的な意義として注目すべきは、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）。

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、むしろ、修補の意義付けについての考察をなした後で述べるのが妥当であろう。

(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

---

[7] 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」という概念がある。「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指し、一次産品の産出、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られよう。

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、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（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）。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、「ソフトウエア自体については、無体物であり、製造物責任の対象とはしていない。ただし、ソフトウエ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。ソフトウエアの不具合が原因でソフトウエアを組み込んだ製造物による事故が発生した場合、ソフトウエ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おり、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し、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) 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、あるとして、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ことになる。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り、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った場合をいうとされる。指示・警告上の欠陥とは、

[8] 経済企画庁　国民生活局消費者行政第一課 編「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エアによる制御を行うものが多いが、このようなソフトウエアを組み込んだ製造物については本法の対象と解され、ソフトウエアの不具合が、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。

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、回避するに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ところでもある。

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、場合にわけて論じられるものと思われる。

「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、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、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ろう。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であろう。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、後日判明した欠点や脆弱性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、瑕疵修補請求、代物請求、解除、損害賠償請求等の問題を生じさせるのかという問題に関しては、新たに判明する欠点､脆弱性について､これらすべてを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・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・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、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と思われる。これは、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いうことになる。

(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。）

[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履行ではある。

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、欠陥ある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、修補に努力すべき地位をもつものを「開発者」と定義するというのもひとつの考え方である。

取扱規程は、「製品開発者」として、次のいずれかに該当するものをいうと定義している。

① ソフトウエア製品を開発した者

② ソフトウエア製品の加工、輸入、販売又は頒布する者であって、当該者の性質及び態様その他の事情に照らして、当該ソフトウエア製品を実質的に開発した者と認められる者

とするが、これは、このような考え方を背景にするものと思われる。

1.4 脆弱性情報発見・通知と契約法の問題

脆弱性が、リバース・エンジニアリングなどの手法でもって発見さ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。

1.4.1 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問題が存在した。この問題については、IPA から「情報セキュリティに関連するソフトウエアの取扱いに係る法律上の位置付けに関する調査」が 2008 年 5 月に公開[11]され、そのあと、コンピュータ・プログラムのリバース・エンジニアリングについては、相互運用性の確保や障害の発見等の一定の目的のための調

[11] https://www.ipa.go.jp/security/fy19/reports/legal/index.html

査・解析について権利制限を早期に措置する必要がある旨の提案が相次いだ[12]が、具体的な法律改正までは、いたらなかった。しかしながら、文化審議会著作権分科会報告書（平成 29 年 4 月）[13]を経て、2018 年著作権法改正において、著作物は、技術の開発等のための試験の用に供する場合その他の当該著作物に表現された思想又は感情を自ら享受し又は他人に享受させることを目的としない場合には、その必要と認められる限度において、利用することができることとすることとされて、同法 30 条の 4 が定められた。これは、著作物に表現された思想または感情の享受を目的としない行為については、著作物に表現された思想または感情を享受しようとする者からの対価回収の機会を損なうものではなく、著作権法が保護しようとしている著作権者の利益を通常害するものではないと評価できると考えられたことによる。同条は、「著作物は、次に掲げる場合その他の当該著作物に表現された思想又は感情を自ら享受し又は他人に享受させることを目的としない場合には、その必要と認められる限度において、いずれの方法によるかを問わず、利用することができる。」とし、その 3 号において「著作物の表現についての人の知覚による認識を伴うことなく当該著作物を電子計算機による情報処理の過程における利用その他の利用（略）に供する場合」が、利用できる例外の例としてあげられている。そして、この権利者の利益を通常害さないと評価できる行為類型の代表例として、「セキュリティ確保のためのソフトウエアの調査解析等」があげられている。[14]これにより、脆弱性調査のためのリバース・エンジニアリング行為が著作権法上禁止されているのではないかという問題については、決着をみたものと考えられる。もっとも、ライセンス契約におけるリバース・エンジニアリング禁止の効力が、脆弱性情報調査に対しても有効なのか、という問題は、依然として存在している。

1.4.2 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。

思うに、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かと思われる。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がある

---

[12]知的財産戦略本部「知的財産推進計画 2008－世界を睨んだ知財戦略の強化－」2008 年 5 月 29 日経過報告（http://www.kantei.go.jp/jp/singi/titeki2/tyousakai/digital/dai4/pdf/sankou.pdf）
文化審議会著作権分科会「文化審議会著作権分科会報告書 平成 21 年」　など

[13] http://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/pdf/h2904_shingi_hokokusho.pdf

[14]文化庁長官官房著作権課「著作権法の一部を改正する法律案概要説明資料」
（https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho_hyoka_kikaku/2018/contents/dai4/siryou6.pdf）

とか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、また、上記とは別個の問題であるように思われる。さらに検討を要するであろう。

1.4.3 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。

この点、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。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り、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よう。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公正取引委員会の「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ーソフトウェア独占禁止法に関する研究会中間報告書ー」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存するところである（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、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というの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、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。

1.5 脆弱性発見と不正アクセス、そして、届出の受理について

1.5.1 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

特定のウェブサイトの脆弱性が報告されている場合に、その情報を利用し、または、応用して、他のウェブサイト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してしまうことにな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は、我が国において、法的な対応としては、「不正アクセス禁止法」があり、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 2 条 4 項）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、[15]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、システムを対応しうる状態におくという認識が必要であ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「犯意」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。しかしながら、その回避といえるかどうか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。セキュリティホール攻撃型については「（2）具体的な適用について」で、検討することになる。

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、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、そのような意図を考慮せずに犯罪が成立することを当然としている [16]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

---

[15] 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なすことができる点に注意が必要である。

[16] 「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ませんけれども、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（同 16 頁）。

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 2 条 4 項 2 号と 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。[17]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。[18]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、後述の (4) 不正アクセス禁止法の成否が問題になった事案を参照されたい。

(3) IoT 機器についての調査と不正アクセス

推測しやすい ID・パスワードによる入力が、「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」ということがいえるか、という問題がある。この問題に関しては、いわゆるデフォルトの設定として取扱い説明書等で広く公開されている ID・パスワードを入力するのはどうか、という問題も存在する。

この識別符号は、アクセス管理者において当該利用権者等を他の利用権者等と区別して識別することができるように付される符号であって、アクセス管理者によってその内容をみだりに第三者に知らせてはならないものとされているなどの性格を有するものである（2 条 2 項）。特定利用をさせることとした相手方に番号、記号等をつける場合には「通常、この番号、記号等として用いられているのが相手方ごとに付けられる ID とその相手方以外のものが知らないようにされているパスワードである」とされる。[19]

上記の定義の解釈から、①特定利用を認める相手方ごとに違うものであること、②その相手方以外に用いることができないようなものであることの 2 つの要件を備える必要があると考えられる。特定利用を認める相手方ごとに違うものであることを求めるので、「複数の利用権者等に同一の符号が付されないようにするとともに、どの利用権者等に付されたものであるかが分かるように付されていることが必要」と解されている。[20]もっとも、具体的

---

[17] 前出（注 16）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。

[18]前出（注 16）露木発言 18 頁および 19 頁

[19] 以上について不正アクセス対策法制研究会「逐条不正アクセス行為の禁止等に関する法律」（第 2 版）（立花書房、2012）39 頁

[20] 前注 19　41 頁

な事例となると明らかではない。「guest」、「anonymous」等の誰もが特定電子計算機を利用できるように広く公開されている ID・パスワードについては、識別符号に該当しないと解される一方で、特定電子計算機の特定利用の一部（例えばウエブサイトの閲覧）についてはすべてのネットワーク利用者に許諾し、その他の特定利用全体はアクセス管理者のみが ID・パスワードを入力して行うような場合には、利用権者等は複数存在し、符号によりアクセス管理者を他の利用権者と区別して識別することができるから、当該 ID・パスワードは識別符号に該当すると解されている。[21]

このような解釈を前提とする限り、実際に機器の設定をなす管理者までも「ID:admin パスワード:admin」によって機器を管理していた場合には、他の利用権者と区別して識別するという要件を満たさないものと考える立場もなりたつものといえる。もっとも、これに対して、そうはいっても、ID が、admin という者に対して、admin というパスワードを設定しているといえるという立場もある。明確な立場が明らかにされているという問題とはいえない。

また、デフォルトの設定として取扱い説明書等で広く公開されている ID・パスワードを入力することによりアクセスできる場合には、誰もが特定電子計算機を利用できるように広く公開されている ID・パスワードであると解することが素直であるように考えられる。なお、この点については、「たとえば「0000」や「guest」といったような、誰でも容易に推測できるような ID やパスワードを設定しているようなネットワーク、あるいは、そもそも ID・パスワードの管理がずさんなネットワークは、保護の対象とはされない可能性がある」というコメントがある。[22]明確な解釈が明らかにされているとはいえない状況である。

(4) 不正アクセス禁止法の成否が問題になった事案

不正アクセス禁止法が脆弱性調査との関係で、問題となった事案としては、東京地判・平成 17 年 3 月 25 日がある。この事案は、国立大学研究員の A が、2003 年 11 月 8 日、東京都内で開催されたコンピュータ・セキュリティの会議において、web サーバの脆弱性を指摘する発表をしたが、その際に、その web サーバの脆弱性を悪用して、同サーバ内にあった氏名・住所・電話番号・年齢・メールアドレス・相談内容等の個人情報が保存されたファイルの内容を閲覧するとともに、同会議において、その個人情報をスクリーンに投影したという事件である。東京地方裁判所は、「プログラムの瑕疵や設定上の不備があるため，識別符号を入力する以外の方法によってもこれを入力したときと同じ特定利用ができることをもって，直ちに識別符号の入力により特定利用の制限を解除する機能がアクセス制御機能に該当しなくなるわけではないと解すべきである」として、不正アクセス禁止法違反であるとして有罪判決を言い渡した。

1.5.2 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、その過程での違法行為という要素については、また、別個の問題といえるものと考えられる。

---

[21] 同上　41 頁

[22] 園田寿、野村隆昌、山川健「ハッカーvs.不正アクセス禁止法」（日本評論社、2000）194 頁

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。

一定の行為によって「脆弱性」や「安全性の欠如」に関する情報が、取得された場合に、その行為が違法であった場合には、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わ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い体制を考えるとき、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、脆弱性情報取扱いにおいて、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。もっとも、早期警戒パートナーシップにおいては、受付機関は、届出がなされた事実が、脆弱性を構成するのか、という形式的な審査を行うのみであるから、

基本的には、違法行為によって脆弱性が明らかになったということを知る手段はあまりない。しかしながら、届出の趣旨を明らかにすべき添付されたその証拠等によって違法行為であることが明らかになり、その様な届出を排除しない場合には、結果として、違法行為による届出を奨励するおそれがあると考えられる場合には、届出を受理しないことが許されると解される。

1.6 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

脆弱性情報の公開は、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ところである。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[23]などが問題として検討する必要がある。

1.6.1 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）という概念がある。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、この攻撃コードが作成され、攻撃に使用されたりする場合を想定する。コンピュータウイルスは、一般に「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「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、特に伝染機能を有しないで、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ので、上記三つの機能が必要だというわけではない。

法的な観点から、「攻撃コード」の問題を考えるときに、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」は「不正指令電磁的記録作成等の罪」（刑法 168 条の 2 第 1 項）として処罰される。

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）の適用の可能性がある。これらの詳細については、省略する。

1.6.2 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

[23] 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。

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、その情報を目にしたものが、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、容易にしたということは、困難であると思われる（容易にしたといえるのであれば、刑事的には、従犯[24]の可能性があり、民事的には、共同不法行為[25]などの可能性がある）。もっとも、早期警戒パートナーシップの運用が社会において広く認識されつつある現在においては、早期警戒パートナーシップを無視した脆弱性の公開は、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事情の一つ、もしくは、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されうる事情のひとつとして配慮される可能性もありうるといえる。

1.7 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

1.7.1 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。名誉毀損罪について、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につき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。

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な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。

1.7.2 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

[24] 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。

[25] 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。

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。

1.7.3 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としても、この点については、相当な検証等を経て、脆弱性があると判断して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、早期警戒パートナーシップに関するルールが存在しなくても同様なことがいえるが、早期警戒パートナーシップ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と考えられる。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ものと思われる。

1.8 公表判定委員会の概要と趣旨について

1.8.1 公表判定委員会の趣旨について

早期警戒パートナーシップは、脆弱性をめぐる関係者の利害関係の調整のための制度であり、そこでは、脆弱性情報を開発者に速やかに通知すること、脆弱性の有無および新規性の検証結果について製品開発者にたいして報告を求める一連の行為を調整行為と呼んでいる。調整においては、発見者、開発者、受付／調整機関が合意によって、脆弱性情報を公表することが一般に前提とされている。しかし、かならずしも合意によるものだけではなく、脆弱性情報についての公表を前提として、開発者に対する十分な手続保障によって関係間の認識の調整を図り、脆弱性情報を社会的に責任ある形で公表することが妥当であると考えられる場合もある。このような趣旨にもとづいて準備されたのが、公表判定委員会である。

1.8.2 合意のない公表の法的な位置づけについて

脆弱性情報について、開発者等の合意なく、これを公表することができるかという問題について、IPA が独立行政法人であり、JPCERT/CC が前記告示で指定された調整機関であることから、行政機関等が情報提供をなす場合に法的に違法行為等を構成する可能性がないのかどうかという法的問題について検討することが必要になる。

まず、IPA および JPCERT/CC が当事者の合意なく公表する場合に、公表行為について特別の法律の根拠を必要とするかということが問題となる（いわゆる法律の留保の問題）。この点について、日本においては、制裁等を目的としない公共の安全を守るための情報の公表であれば法律の根拠を要しないと一般に考えられている。これは、命令強制的行為について法律の根拠を要求する法律の留保に関する侵害留保原理からすると、直接私人の権利を制限しあるいはその私人に義務を課すものではない公表行為については法律の根拠を必要としないと考えるためである。従って、調整が不可能であった場合に IPA および JPCERT/CC

が当事者の合意なく脆弱性情報を公表することについても法律の根拠は必要としないと考えられる。

しかし、制裁や不遵守に対する実効性確保の手段としてなされる公表については、実質的に公表行為が法律の根拠を必要とする命令強制的行為としての性格をもつため、法律の根拠の要否について特に争いがあることに留意する必要がある。このことから、公表があくまで脆弱性情報の悪用から公共の安全を確保することを目的とするものであり、調整手続に従わないことへの制裁や、調整手続に従わせるための実効性確保の手段として用いられるものではないことは周知されるべき事項となる。行政機関が法律の根拠によらず公表を行うことができるとしても無制限に許されるわけではなく、「〈1〉公表目的の正当性、〈2〉公表の必要性、〈3〉公表内容の真実性ないし真実と信ずるについて相当な理由の存在、〈4〉公表態様ないし手段の相当性が肯定される場合には、当該公表行為は公務員の適切な職務行為の一環として評価され、違法性が阻却されると解するべきである。」（東京地判平成 18 年 6 月 6 日）。

この判例の見解をもとに考えるときに、早期警戒パートナーシップのもとに調整が不可能である場合でも、脆弱性情報を公開することは、慎重な公表手続を設け、公表目的の正当性、公表の必要性・合理性、公表内容の性質、公表内容の真実性、公表方法や公表の態様の相当性、公表の緊急性の諸点を十分に考慮し、製品開発者の利益を不当に害さないよう注意義務を尽くすことで可能であると考えられた。そして、議論の結果、脆弱性について、IPA および JPCERT/CC が、その手続きにしたがって、脆弱性の検証をなして、脆弱性情報の深刻さを評価し、適切な公表方法・公表態様により公表した場合には、そのような公表は、社会的に相当なものとして認識される。

1.8.3 制度設計時において考慮された事項

上述のように脆弱性に関する情報を、合意による場合でも合意に達し得ない場合であっても、公表することができるように過程を整備することが必要と考えられるところである。

処分、行政指導及び届出に関する手続などについては、公正の確保と透明性の向上を図る目的で、行政手続法が定められている。脆弱性情報公表制度との関係で考えれば、脆弱性情報の公表自体は、行政手続法による不利益処分というものではないが、脆弱性情報公表制度およびそこで論じられている概念や問題点などについては、行政手続法の制度の趣旨を十分に尊重し公正手続きの理念を生かして具体的な制度を論じることが重要になる。これらの検討の結果、脆弱性情報公表についての連絡、意見表明の機会の付与、異議申立の要否などについて留意が払われるべきとなる。

これらの点についての検討の結果、脆弱性公表について公表判定委員会制度が制定された。具体的な部分については、第 2 章の該当部分による。

1.9 受付機関・調整機関自身の法律問題

1.9.1 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」42 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、法令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。[26]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は、存在しうるものと考えられる。

1.9.2 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。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、地方公共団体又は地方独立行政法人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、詳細な検討が必要になろう。

1.9.3 責任問題

早期警戒パートナーシップの枠組みの中心として関与する受付機関、調整機関の法的な地位に着目しなければならない。この早期警戒パートナーシップの導入にあたって、これらの受付機関・調整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[27]されていたところであり、また、受付機関、調整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ていた。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

[26] 新版注釈刑事訴訟法［第 2 巻］（立花書房、1997）167 頁

[27] 法律面の調査報告書（2004 年版）：当時の指摘では「届出機関」「分析機関」に関するコメント

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起こりうる可能性がある。

2. 「情報セキュリティ早期警戒パートナーシップガイドライン」における法的関連記述の逐条解説

「情報セキュリティ早期警戒パートナーシップガイドライン」を読み進める上で、法的な見地から特に意識しておくべきと思われる事項について、以下に解説する。

Ⅰ. はじめに

脆弱性関連情報が発見された場合に、それらをどのように取り扱うべきかを示した、経済産業省告示「ソフトウエア等脆弱性関連情報取扱基準」が 2004 年に制定され、2014 年の改正を経て、2017 年に新たに経済産業省告示「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」になりました。

（解説）

① 脆弱性関連情報が発見された場合に

脆弱性関連情報については、本報告書「Ⅱ. 用語の定義と前提　2. 脆弱性関連情報の種類」を参照のこと。

② それらをどのように取り扱うべきかを示した、

「取り扱う」ことは、発見・届出・受理・通知・検証・報告・公表などの一連の行為を総称するものである。

③ 経済産業省告示「ソフトウエア等脆弱性関連情報取扱基準」

「ソフトウエア等脆弱性関連情報取扱基準」が、平成 16 年経済産業省告示第 235 号として平成 16 年（2004 年）に制定されている（旧告示という）。当該旧告示は、「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」旨としたもの（「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 条参照）である。

その後、2014 年の旧告示の改正のもと、IPA の脆弱性研究会における 2011 年度以降の論議を踏まえ、調整不能案件としてきた事案のうち連絡不能案件について、受付機関に設置される公表判定委員会における判定を経て脆弱性情報を公表できるよう運営がなされてきた。

さらに、サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律（平成 28 年法律第 31 号）により情報処理の促進に関する法律（昭和 45 年法律第 90 号。以下「情促法」という。）の改正において、情促法 43 条 3 項に、IPA が必要があると認めるときには、サイバーセキュリティの確保のために電子計算機を利用する者が講ずべき措置の内容を公表することができるとの規定が設けられたことにより脆弱性情報に係る公表について法律上の根拠が与えられることとなった。さらに、同条 4 項に、その公表の方法及び手続について経済産業省令に定める旨の規定を設け、同項の委任を受け、施行規則 42 条に、公表する方法に係る規定、同 43 条に、その他公表の方法及び手続について経済産業大臣の定めるところによるとする規定を設けた。これらを受けて、経済産業省告示として「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」（平成 29 年経済産業省告示第 19 号）、「受付機関及び調整機関を定める告示」（同 20 号）が定められている。

なお、告示の意義については、本報告書「1.2　脆弱性情報取扱い体制の法的意味」

を参照のこと。

「ソフトウエア等」の解説については、本報告書「Ⅱ．用語の定義と前提　5．ソフトウエア製品」および「Ⅱ．用語の定義と前提　7.ウェブアプリケーション」を参照のこと。

④ 経済産業省告示「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」になりました

取扱規程は、③で述べた経緯のもとに制定されたものである。経済産業省が、その定める「告示」[28]の形式で、発表するものである。

取扱規程においては、サイバーセキュリティ確保のためにソフトウエア製品等の脆弱性関連情報を取り扱う者に推奨する行為を定めることに鑑みて、サイバーセキュリティ基本法 1 条の目的を参考に、その目的は、「情報の適切な流通の促進を図り、経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現」と修正されている。

本ガイドラインは、上記告示を踏まえ、脆弱性関連情報の適切な流通により、コンピュータ不正アクセス、コンピュータウイルス等による被害発生を抑制するために、関係者に推奨する行為をとりまとめたものです。

（解説）

① 脆弱性関連情報の適切な流通により

「脆弱性関連情報」の解説ついては、本報告書「Ⅱ．用語の定義と前提　2．脆弱性関連情報の種類」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という長所、検証による情報の正確性の担保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情報の交換」をいう。

② 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）（以下、不正アクセス禁止法という）における「不正アクセス行為」（同法 2 条 4 項）をいう。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。

③ コンピュータウイルス等

「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

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

[28] 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」（通商産業省告示第 518 号）をそれぞれ発表している。

(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、他のプログラムに自らを複写し、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、対策基準における定義は、より広いものになる。

法的な観点からすると、「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」を対象とする「不正指令電磁的記録等作成等の罪」(刑法 168 条の 2 第 1 項)が定められている。俗に、同条は、コンピュータウイルス作成罪といわれることがあるが、コンピュータウイルス対策基準の定義に該当するプログラムのみではなく、より広い範囲を包含するものである。

④ 被害発生を抑制する

ここにおける「被害」とは、安全性が脅かされる状況をいう。これが「不特定または多数」の者に対して引き起こされる場合を念頭に置いて、パートナーシップ制度が定められていることになる。また、この不特定または多数の者に対するセキュリティ上の脅威に対する対応であるという観点から、ソフトウエア製品についての定義がなされている。

⑤ 関係者に推奨する行為

関係者というのは、発見者、受付機関、調整機関、製品開発者、ウェブサイト運営者をいう。これは、旧告示において「Ⅲ．本基準における関係者の定義」として上記の者らが関係者としてあげられていたのに対応するものである。

「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されている行為を具体的に論じたことを意味する。取扱規程「第 1　総則　1 目的」において「脆弱性関連情報を取り扱う者に推奨する行為」とされているのに対応する。

脆弱性関連情報が、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、一定の取扱いのルールを直接的に名宛人の義務として提案しうるものではないことから、推奨する行為とされている。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。

さらに、本ガイドラインに基づく取組みがより効果的に社会貢献できるように、影響の大きい届出（脆弱性の深刻度の大きさや影響範囲の広さで判断、詳細は付録 4 を参照）を優先して取り扱うことや、発見者と製品開発者または、ウェブサイト運営者との調整において自律的な進展が困難な場合の打開を促すことにも取り組みます。

（解説）

① 効果的に社会貢献できるよう

前述の取扱規程の目的において「情報の適切な流通の促進を図り、経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現に資する」と定められているところであり、当該記述に対応するものである。

② 影響の大きい届出を優先して取り扱う

影響とは、「脆弱性に起因する影響」であって、脆弱性を悪用したサイバー攻撃により生じたセキュリティ侵害をいう。脆弱性の影響は、P ガイドライン「付録 4　脆弱性の影響度に関する考え方について」において記述されているように脆弱性の深刻度と影響範囲で分析される。この場合には、受付の順序にかかわらず、優先的に取扱いを行うとともに、影響が小さい場合には、処理を取りやめることがある。

③ 発見者と製品開発者または、ウェブサイト運営者との調整において自律的な進展が困難な場合の打開を促すこと

製品や運営するウェブサイトにセキュリティ上の問題箇所がないように努めるのは、製品の開発者やウェブサイト運営者の責任であるということができる。しかしながら、発見者と開発者等において、開発者の連絡先が不明な場合については、開発者の連絡先を調査するなどして、調整の進展に努力するという趣旨である。

Ⅱ. 用語の定義と前提

本ガイドラインに用いられる用語の定義は以下の通りです。

1. 脆弱性

脆弱性とは、ソフトウエア製品やウェブアプリケーション等において、コンピュータ不正アクセスやコンピュータウイルス等の攻撃により、その機能や性能を損なう原因となりうるセキュリティ上の問題箇所です。 なお、製品開発者の不適切な実装やウェブサイト運営者の不適切な運用によって、個人情報等が適切なアクセス制御の下に管理されておらずセキュリティが維持できなくなっている状態も含みます。（ウェブサイトの不適切な運用に関しては付録 1 に例を示します。）

（解説）

① ソフトウエア製品及びウェブアプリケーション等

「ソフトウエア製品」については、以下の「4. ソフトウエア製品」の定義の解説を、「ウェブアプリケーション」については、「7. ウェブアプリケーション」の定義の解説を参照のこと。

ここでは、「ソフトウエア製品やウェブアプリケーション等」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、プロトコルが実装された部分などをも含む趣旨である。（なお、旧告示Ⅳ1 を参照）。

② コンピュータ不正アクセス又はコンピュータウイルス等の攻撃により

「攻撃により」における、「攻撃」とは、第三者による安全性に対する意図的な脅威をいう。なお、コンピュータウイルス「等」とされているのは、スパイウエア（spyware）、キーロガー（key　logger）、フィッシング（Phishing）などをも含める趣旨であって、不正アクセスやコンピュータウイルスの形態による攻撃に限定されな

いという趣旨を盛り込んだものである。

ここで、「攻撃」とは、セキュリティに対する意図的な攻撃をいう。したがって、プログラムが自らセキュリティの問題を引き起こすことがあったとしても、それは、攻撃によって問題が引き起こされたとは解されない。また、この「攻撃」は、直接に、その機能や性能を損なう原因となりうる性質を伴うものであることを要する。従って、被害者がスクリプトを実行させて初めてセキュリティ上の「機能や性能を損なう原因となりうる」場合においては、攻撃者がスクリプトを入力して送信して、攻撃者のウェブブラウザ上でスクリプトが実行されたとしても、その被害者にスクリプトを実行させる手法がない場合であるので、「攻撃」であるということはできない。

③ セキュリティ上の問題箇所

サイバーセキュリティは、サイバーセキュリティ基本法（平成 26 年法律第 104 号）において、「（略）情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（略）が講じられ、その状態が適切に維持管理されていること」をいうとされている。本報告書の「セキュリティ」は、上記定義と同義であり、具体的には、「機密性」「完全性」「可用性」が保たれている状態をいうと解される。なお、取扱規程は、「安全性上の問題箇所」というが、取扱規程と同義である。

「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。具体的には、上記のセキュリティ要素への脅威を明示的に／黙示的に引き起こす条件のセットということができる。

何が「通常有すべき程度の安全性」であるかを一律に規定することは困難である。

一般論としては、当該ソフトウエア製品等の利用者の人数や属性、利用目的あるいは利用環境および当該脆弱性が顕在化した際の影響等を総合的に考慮して、社会通念に従って判断すべきものと考えられる。

なお、ソフトウエア製品については、その製品のライフサイクルが示されて、サポート期間が明らかにされることが多い。このセキュリティの問題個所という概念は、そのようなサポート期間とは、別個に、「通常有すべき程度」を備えているか、という観点から判断される。サポート期間が終了している製品については、サポート期間経過によって脆弱性という概念に該当しなくなるということによるものではない。

④ 製品開発者の不適切な実装

これは、ソフトウエア製品の開発者が不用意に個人情報をプログラム内に記載したりすることをいう。

⑤ ウェブサイト運営者の不適切な運用

これは、社会通念上、アクセス制御機能により保護されるべき個人情報等の機密な情報が、保護されていない運用状況をいう。

⑥ 個人情報等が適切なアクセス制御の下に管理されておらず

「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も含む。個人情報は、社会的に機密とされるべきと考えられるが、そうでありながら、アクセス制御機能のかかっていない領域に保存され、一般からアクセスしうる状態になっているのは、適切なアクセス制御がなされていないことを意味している。このような場合の

個人情報をも含む趣旨である。

「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。

⑦　セキュリティが維持できなくなっている状態

「通常有すべき程度を備えていない状態」をいう。

2. 脆弱性関連情報の種類

脆弱性関連情報とは、脆弱性に関する情報であり、次のいずれかに該当するものです。 1）脆弱性情報 脆弱性の性質および特徴を示す情報のことです。 2）検証方法 脆弱性が存在することを調べるための方法のことです。例えば、特定の入力パターンにより脆弱性の有無を検証するツール等が該当します。 3）攻撃方法 脆弱性を悪用するプログラムやコマンド、データおよびそれらの使い方のことです。例えば、エクスプロイトコード（付録 1 を参照）や、コンピュータウイルス等が該当します。

（解説）

脆弱性関連情報は、取扱規程において、「① 脆弱性情報　② 脆弱性が存在することを検証する方法　③ 脆弱性を悪用するプログラム､指令又はデータ及びそれらの使用方法」とされているところ（取扱規程「第 1　総則　3 定義（5）」）、P ガイドラインにおいて、具体的な記述をしているものである。

① 脆弱性情報

脆弱性の性質及び特徴を示す情報をいい、脆弱性関連情報の中心をなすものといえる。具体的には、ソフトウエア製品の場合には、製品の名称及びバージョン、その脆弱性によりもたらされる具体的な脅威等からなる。ウェブアプリケーションの場合には、ウェブサイト URL やウェブサイト名等のウェブサイトを識別する情報や脆弱性の種類、現状から想定されるリスク等の情報からなる。

脆弱性情報の定義は、取扱規程「第 1 総則　3 定義（4）」と同一である。

② 脆弱性が存在することを調べるための方法

具体例として、特定の入力パターンにより脆弱性の有無を検証するツール等が挙げられる。なお、この検証方法だけでも、専門的な見地から脆弱性が存在することは分かってしまうおそれ恐れがあり、関係者に対しその取扱いに注意を促し、脆弱性が世に出回る事態を回避する面でも、脆弱性関連情報として取り扱うことに意味があると考えられる。

③ 脆弱性を悪用するプログラムやコマンド、データおよびそれらの使い方

脆弱性に対する具体的な攻撃方法のことであり、その意味では、脆弱性情報と対をなすものといえる。この方法の具体例としては、PoC（Proof of Concept: 概念実証）、エクスプロイトコード（脆弱性を悪用するソフトウエアのソースコード。攻撃コード。）やコンピュータウイルス等が挙げられる。

3.　対策方法

対策方法とは、脆弱性から生じる問題を回避するまたは解決を図る方法のことです。回

避方法と修正方法から成ります。

（解説）

「脆弱性から生じる問題を回避する方法」とは、脆弱性が原因となって生じる被害を回避するための方法（ワークアラウンド）であり、当該脆弱性を修正する以外の方法で脆弱性の影響を受けないようにする方法をいう。具体的には、脆弱性に関連するポートを閉じることや、当該ソフトウエア等の利用そのものを取りやめる等の対策が挙げられる。
また、「脆弱性から生じる問題を解決する方法」とは、脆弱性そのものを修正する方法であり、脆弱性を有するソフトウエアから脆弱性部分を解消するためのソフトウエア（パッチ）をあてる等が考えられる。

4. 対応状況

これについては、特段、法的観点からコメントするべきものはない。

5.ソフトウエア製品

ソフトウエア製品とは、ソフトウエア自体またはソフトウエアを組み込んだハードウエア等の汎用性を有する製品のことです。技術情報の統括や開発保守を行っている者をコミュニティとしてしか特定できない、オープンソースソフトウエアのようなものも含みます。具体例は、付録１を参照してください。

（解説）

① ソフトウエア製品

ソフトウエアとは、「情報処理システムのプログラム、手続き、規則及び関連文書の全部又は一部」をいう（JIS X 0001-1994）。

P ガイドラインは、ソフトウエア製品とウェブアプリケーションを別個のものとして取扱っている。もっとも、現在においては、情報処理のクラウド化・サービス化にともなって、ソフトウエア製品とウェブアプリケーションの判断が困難になりつつある。P ガイドラインの取扱いに関してソフトウエア製品に該当するのか、ウェブアプリケーションに該当するのかは、修正作業および対応について利用者の行為を要するかどうかがその判断基準となる。すなわち、ソフトウエア製品は、プログラムを実行しているものが修正／対応作業を行うことが必要であるのに対して、ウェブアプリケーションは、そのウェブアプリケーションの提供されているウェブサイト運営者によって修正／対応作業を行うことでたりることになる（P ガイドライン「Ⅲ．本ガイドラインの適用の範囲」を参照）。

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。

一般的なプロトコルは、あくまでも手順や規約という約束事であって、それ自体は実体を持たない。そのため、プロトコルは、具体的な製品に実装されない限り、具体的なセキュリティ上の被害をもたらすものではない。この理由から、一般的なプロトコルは、P ガイドラインの対象外である。

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、利用者が不特定または多数存在することをいう（取扱規程「第１　総則　３定義　（1）」を参照）。したが

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、P ガイドラインの対象ではないことになる。この点については、P ガイドライン「Ⅲ　本ガイドラインの適用の範囲」において、確認されている。

6. オープンソースソフトウエア（OSS）

これについては、特段、法的観点からコメントするべきものはない。

7. 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等で稼動する固有のシステムのことです。

（解説）

ウェブサイト等で稼動するデータ処理システムの運用に関するプログラム等であってウェブサイト管理者によって、設定・運営をなしうるものをいう。「固有のシステム」とは、インターネットのウェブサイトなどで、公衆に向けて提供するサービスを構成するシステムで、そのソフトウエアがサイトごとに個別に設計・構築され、一般には配布されていないものであることを意味する。動作しているウェブサイト固有の環境のもとで情報処理がなされることが、一般のプログラムとの違いとなる（本報告書「Ⅱ．用語の定義と前提　5. ソフトウエア製品」の①の解説を参照）。

なお、ISO/IEC29147（2018）においては、サービス（Services）について、ウェブサイトの利用者が、サービスを利用するのみで、ソフトウエアの保有、操作、メンテナンスをしないという点に特徴があることがふれられている（5.4.4）。

8. 発見者

発見者とは、脆弱性関連情報を発見または取得した者のことです。例えば、ソフトウエアの脆弱性を発見した人や、インターネット上で脆弱性関連情報を入手した人等が当てはまります。ソフトウエアの脆弱性を発見した人のみを対象としているわけではありません。

（解説）

脆弱性関連情報を発見又は取得した者をいう（取扱規程「第 1　総則　3　定義　(8)」）。

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。脆弱性関連情報を知得しているとしても、管理をなしていない場合は、含まれない。

なお、発見者という概念には、自らソフトウエア製品の開発等を行った製品について脆弱性を発見した場合も含まれる。この理は、取扱規程「第 2　ソフトウエア製品に係る脆弱性関連情報に関する取扱い　1　手続きの概要　①」において、発見者のうちから、手続の概要の適用の対象者として影響が自社製品にとどまる場合の開発者を除外していることからも明らかである。

9. 製品開発者

製品開発者とは、次のいずれかに該当する者のことです。

1) ソフトウエア製品（0SS を含む）を開発した官庁、法人、個人、またはコミュニティ
2) ソフトウエア製品（0SS を含む）の加工、輸入、販売または頒布する官庁、法人、個人、またはコミュニティ

（解説）

①ソフトウエア製品

ソフトウエア製品の定義については、本報告書「Ⅱ．用語の定義と前提　5. ソフトウエア製品」を参照のこと。

② 開発した

「開発した」というのは、「ユーザの要求を満たす機能をソフトウエアにより具体的に実現すること」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、保守する過程として認識されることになる。

③ 加工

「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、フリーソフト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。

④ 輸入

「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。

これらの記述が、広汎なのは、その定義として捉えられる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１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。

10. 脆弱性検証

これについては、特段、法的観点からコメントするべきものはない。

11. ウェブサイト運営者

ウェブサイト運営者とは、ウェブアプリケーションを運営する主体のことです。当該ウェブアプリケーションが官庁、法人等の組織によって運営されているのであれば、その組織が該当します。個人によって運営されているのであれば、その個人が該当します。ウェブサイト運営者の例は、付録 1 を参照してください。

（解説）

① ウェブアプリケーションを運営する主体

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の決定ということになる。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」と同義で、例えば運営者が法人である場合、当該法人のような運営の責任を負う主体をさすことになる。

システム管理者との違いに関しては、「システム管理者」が、別個の者として、定義されている。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。パートナーシップ制度においては、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。

12. 製品利用者

製品利用者とは、ソフトウエア製品のライセンス許諾（明示的でないケースを含む）を受けてソフトウエア製品を導入・管理する官庁、法人または個人のことです。一般に、ソフトウエア製品の脆弱性対策を適用する立場にあります。

（解説）

製品利用者は、ライセンス許諾を受けて、ソフトウエア製品を利用するものをいう。これに対して、その製品利用者の提供するサービスを利用するものは、サービス利用者となる。サービス利用者は、早期警戒パートナーシップの運用上、関係者としては、認識されないが、影響が不特定または多数の者に及ぶかという判断の際には、考慮されることになる。

13. システム構築事業者

これについては、特段、法的観点からコメントするべきものはない。

Ⅲ.本ガイドラインの適用の範囲

本ガイドラインは、次のものに係る脆弱性であって、その脆弱性に起因する影響が不特定または多数の人々におよぶおそれのあるものに適用します。

○日本国内で利用されているソフトウエア製品

・「暗号アルゴリズム」や「プロトコル」を実装しているものも含みますが、一般的な「暗号アルゴリズム」や「プロトコル」等の仕様そのものの脆弱性は含みません。（プロトコルの実装に係る脆弱性については付録 1 を参照。）

・ソフトウエア製品に係る脆弱性関連情報の取扱いは、IV.で記述します。

○日本国内からのアクセスが実質的になされているウェブサイトで稼動するウェブアプリケーション

・例えば、主なコンテンツが日本語である、あるいは URL のホスト名の最上位ドメインが「jp」であるウェブサイト等のことです。

・ウェブアプリケーションに係る脆弱性関連情報の取扱いは、V.で記述します。

なお上記の分類が難しい場合には、修正作業が事業者側のみで済む場合をウェブアプリケーション、製品利用者側の対応が必要な場合をソフトウエア製品として判断することを基本とします。

（解説）

①　脆弱性に起因する影響

「脆弱性」の定義については、本報告書「Ⅱ．用語の定義と前提　1．脆弱性」を参照のこと。

「起因する影響」については、「因果関係を有する影響」であり、「影響」については、「セキュリティが脅かされる状況」をいう。なお、旧告示においては「影響」ではなく「被害」と規定していたが、取扱規程においては、対象が狭くなることが懸念されたために「影響」が適当であるとされている。

② 不特定または多数の人々におよぶ

ソフトウエア製品に関していえば、影響を受けるものは、製品利用者（本報告書「Ⅱ．用語の定義と前提　12．製品利用者」を参照）に限らず、その製品を利用したサービスの利用者などまで含めて考えることになる。また、不特定または多数であるので、少数であっても、不特定である場合、また、特定されていても多数である場合については、P ガイドラインが適用されることになる。

もっとも、影響が小さい脆弱性の場合、製品開発者に通知することで取扱終了とすることができるので、少数である事情、もしくは、特定されているという事情は、この脆弱性の影響を判断する際に参照されることになる。

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実質的になされている

本報告書「1.2.3 告示・ガイドラインの適用範囲」を参照のこと。

なお、これについては、現在におけるウェブアプリケーションの作成に関して、豊富なプラグイン等が提供されるようになったことから、ウェブサイトを日本語への機械翻訳のサービスを利用した上で、日本語で、表示するページを多々みることができるようになった。

早期警戒パートナーシップおける調整の労力をかけて解決すべき脆弱性であるかどうかという観点から運用が見直されており、かかるアクセスが実質的に我が国の利用者にとって重要であるかどうかということが、P ガイドラインが適用されるために重要な指標になっており、かかる観点から、「実質的に」アクセスがなされることを適用の要件としたものである。

④ 適用します

早期警戒パートナーシップは、脆弱性関連情報に関連して、その情報の流通により、セキュリティ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」として提案されているものである。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。

この定めは、取扱規程「第 1　総則　4　本規定の適用範囲」に対応する。

日本における不特定または多数の者に対して、セキュリティ上の影響が実質的に及ぶときにその名宛人に対して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。

Ⅳ.ソフトウエア製品に係る脆弱性関連情報取扱

1　概要

具体的な点については、個別の記載において対応する。

2　発見者の対応

1) 発見者の範囲

IVにおける発見者とは、製品開発者以外の者（研究者等）のみを指しているわけではありません。製品開発者自身であっても、自身のソフトウエア製品についての脆弱性関連情報であって、脆弱性が外部のソフトウエア製品に含まれることが推定されるものを発見・取得した場合、発見者としての対応が推奨されます。

（解説）

発見者の定義については、本報告書「Ⅱ. 用語の定義と前提　8. 発見者」を参照のこと。

自身が開発したソフトウエア製品において脆弱性を発見した場合において、当該脆弱性関連情報に起因する影響が自社のソフトウエア製品に限られると認められる場合には、早期警戒パートナーシップの枠組みを利用せずに製品開発者が自発的に脆弱性に対処することが期待される。受付機関への届出等の手続を省略することによって、より迅速かつ適切な処理が可能となることも期待される。そのために、取扱規程においては、「自ら開発等を行ったソフトウエア製品に係る脆弱性関連情報（脆弱性に起因する影響が自ら開発等を行ったソフトウエア製品にとどまるものに限る。）を発見又は取得した製品開発者」が、除かれるとされている（取扱規程「第 2　ソフトウエア製品に係る脆弱性関連情報に関する取扱い 1　手続の概要　①」を参照）。

その一方で､影響が自ら開発等を行ったソフトウエア製品にとどまらない場合､もしくは､外部のソフトウエア製品に類似の脆弱性があると推定される場合には、発見者としての対応が推奨されている。

2) 脆弱性関連情報の発見・取得

脆脆弱性関連情報の発見・取得に際しては、関連法令に触れることがないように留意してください。詳細は、付録 3 を参照してください。

(解説)

「発見」の定義については本報告書「Ⅱ．用語の定義と前提　8. 発見者」を参照のこと。

この点については、早期警戒パートナーシップを考えるとき、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。

「関連法令に触れることがないように留意してください。」は、取扱規程において「ウ 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。」とされている（取扱規程「第 2　ソフトウエア製品に係る脆弱性関連情報に関する取扱い　2　具体的な手続及び行動指針　(1) 発見者　ウ」を参照）のに対応している。

関連法令の代表的なものとして不正アクセス禁止法があげられる。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。具体的な内容については、P ガイドライン付録 3 を参照のこと。

3) 脆弱性関連情報の届出

これについては、特段、法的観点からコメントするべきものはない。

4) 脆弱性関連情報の管理および開示

発見者は､脆弱性関連情報を正当な理由がない限り第三者に開示しないでください（発見者に対する情報非開示依頼、以下「情報非開示依頼」という）。ただし、正当な理由があって脆弱性関連情報を開示する必要がある場合には､事前に IPA に相談してください。脆弱性関連情報の管理および開示に係る法的な問題に関しては、付録 3 を参照してください。 なお、起算日から 1 年以上経過した届出については、発見者は IPA に対し、情報非開示依頼の取り下げを求めることができます。

(解説)

① 発見者

「発見者」については、本報告書「Ⅱ．用語の定義と前提　8. 発見者」、「脆弱性情報」「脆弱性関連情報」については、本報告書「Ⅱ．用語の定義と前提　2. 脆弱性関連情報の種類」を参照のこと。

② 脆弱性関連情報を正当な理由がない限り第三者に開示しないでください

これは、脆弱性関連情報について、発見者は、自ら開示しないように IPA が発見者に対して依頼をなす趣旨である。これを情報非開示依頼といっている。責任ある開示（もしくは、協調された開示）の枠組みからは、発見者がこの依頼に応じて、調整の間においては、第三者が脆弱性関連情報を悪用できないという枠組みを想定している。

これは、取扱規程　「オ　発見者は、正当な理由がない限り、第三者に脆弱性関連情報を開示しないこと。」（取扱規程「第 2　ソフトウエア製品に係る脆弱性関連情報に関する取扱い　2　具体的な手続及び行動指針　（1）発見者　オ」を参照）に対応している。

「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、脆弱性が原理的に新奇なものかどうか、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。

③ 事前に IPA に相談してください

これは、IPA においても脆弱性関連情報の流通状況について的確に把握し、関係者間での足並みを揃えるため、また、開示による影響について事前に想定しておくため、重要インフラなどへの影響が無いこと等を確認するために、事前に相談することがもとめられているものである。前述の取扱規程オの後半である「正当な理由により開示するときは、あらかじめ受付機関に問い合わせること。」に対応している。

④ 情報非開示依頼の取り下げ

実際の調整においては、相当期間を要することも少なくない、そのような場合においては、大原則（本報告書「1.1.1 脆弱性の公開と表現の自由」を参照）に戻って、発見者が、脆弱性関連情報を公表することを認めるべきであると考えられる。そのために、発見者は、情報非開示依頼の取り下げを求めることができるようにしている。

5) 届け出る情報の内容

発見者は、届け出る情報の中で以下の点を明示してください（詳細は、https://www.ipa.go.jp/security/vuln/ を参照）。

（ア）氏名等の発見者を識別するための情報
（イ）電子メールアドレス等の発見者の連絡先
（ウ）（ア）および（イ）の製品開発者への通知の可否
（エ）製品開発者から直接連絡を受けることの可否
（オ）（ア）の公表の可否
（カ）脆弱性関連情報に係るソフトウエア製品の名称
（キ）脆弱性関連情報の内容（脆弱性関連情報を確認する環境、手順および結果）
　　可能であれば、脆弱性が存在する証拠を一緒に提出してください。ただし、証拠の取得に際しては、関連法令に触れることがないように留意してください（付録 3 を参照）。
（ク）個人情報の取扱方法（製品開発者への通知および直接の情報交換の可否、一般への公表の可否）

•発見者が望まない場合、IPA は、JPCERT/CC および製品開発者に対して、発見者を特定しうる情報を通知することはありません。

•発見者が望む場合、IPA および JPCERT/CC は、脆弱性情報と製品開発者ごとの脆弱性検証の結果、対策方法および対応状況を公表する際に発見者名を付記するとともに、製品開発者に対しても、対策方法の公表時に発見者名を付記することを推奨します。

（ケ）他組織（製品開発者、他のセキュリティ関係機関等）への届出の状況　等

（解説）

これらは、取扱規程において定められている届出事項（取扱規程「第 2　ソフトウエア製品に係る脆弱性関連情報に関する取扱い　2　具体的な手続及び行動指針　(1) 発見者　イ」の①ないし⑦に定める事項）および取扱いにおいて受付機関・調整機関が、参照すべき事項が含まれている。

特段のコメントすべき事項としては、以下がある。

(ア) 氏名等の発見者を識別するための情報

調整の手続等をなすにあたって、IPA としては、具体的に発見者と連絡をとりあうことが必要になる。そのために、氏名等によって発見者を識別することが必要であり、そのための情報が届出事項としてもとめられている。「等」とあるのは、仮名による届出も許容されるという趣旨である。ここでいう仮名とは、発見者を一意に識別する名称であって、一般には固定した名称が利用される。もっとも、他人の著作物の名称、商標等を権限なく利用したりすることは、認められるものではない。

6) 製品開発者との直接の情報交換ないし 7) 届出後の対応について

これについては、特段、法的観点からコメントするべきものはない。

3. IPA（受付機関）の対応

（1）脆弱性関連情報の届出受付と取扱いについて

以下、特に法的な観点からコメントをなすべき事項については、以下のとおりである。

2) 届出の受理

IPA は、届出の記載が以下の条件をすべて満たしていると判断した時、その時点で届出を受理し、発見者に連絡します。

(ア) 上記 2. 5)の項目がすべて記載されていること

(イ) 届出内容に矛盾等が無いこと

(ウ) 届出の対象が本ガイドラインの適用範囲に該当すること（III章を参照）

(エ) 記載されている内容が脆弱性であること

(オ) 既知の脆弱性とは異なる脆弱性の関連情報であること（JPCERT/CC、製品開発者等により公表された脆弱性の関連情報ではないこと）

なお、IPA は、これらの条件により、届出の受理または不受理を判断し、その理由とともに発見者に連絡します。なお、発見者に届出の受理を連絡した日が IPA および JPCERT/CC が脆弱性関連情報の取扱いを開始した日（受理日）となります。

（解説）

①IPA は、届出の記載が以下の条件をすべて満たしていると判断した時、その時点で届出を受理し、発見者に連絡します。

受付機関である IPA における発見者からの届出の受理に係る規定である。

従来のガイドラインは、「IPA は、以下のいずれかに該当することを確認します。・IPA が精査した結果､脆弱性が存在する可能性があると判断できる」という表現をなしていた。当該表現においては、IPA が届け出られた報告を実際に再現して、脆弱性の存否を確認しなければならないと解釈されかねない。

しかしながら、取扱規程「第 2 ソフトウエア製品に係る脆弱性関連情報に関する取扱い　2　具体的な手続及び行動指針　(2) 受付機関　ア　届出の取扱い及び脆弱性情報の公表に係る手続及び行動指針」は、

「(ア) 受付機関は、発見者による届出が次に掲げる事項のいずれにも該当するときは、これを受理し、発見者に届出を受理した旨を通知すること。また、届出を不受理としたときは、発見者にその旨及びその理由を通知すること。

① 届出事項を全て記載していること。

② 本規程の適用範囲内であること。

③ 既に公表されている脆弱性情報に関する脆弱性関連情報でないこと。」

としており、IPA が届出に際して審査しうる事項は、その形式的な事項にのみ及び、実質的な脆弱性の有無に及ばないとしている。また、この仕組みは、受理という用語が用いられていることにも対応する。ここで、受理とは、「他人の行為を有効な行為として受領する行為」をいう。まさに形式的な審査を前提とする用語である。実質的な脆弱性の判断に及ばないことを明らかにすることが必要であるために、脆弱性が存在する可能性があると判断できるという表現を避け、届出した事実が、存在すれば、脆弱性であること、が受理の実質的な要件とされているのは、そのためである。

3) 違法な手段で入手された脆弱性関連情報への対応

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脆弱性関連情報であることが明白な場合、処理を取りやめることがあります。

（解説）

この点については、本報告書「1.5.1 脆弱性発見と不正アクセス」及び、届出の受理について「1.5.2 先行行為の他の行為への影響」を参照されたい。

4) JPCERT/CC への連絡

IPA は、上記 2)、3)における対応の是非の判断の結果、対応することが妥当との判断を下した脆弱性関連情報について、速やかに JPCERT/CC に通知します。なお、届け出された脆弱性による影響が大きい場合、受付の順序に関わらず、優先的に取扱いを行います（付録 4 を参照）。

（解説）

①　上記 2)、3)における対応の是非の判断の結果

これは、受理された届出について、3)における取りやめに該当する事情が伺えた場合以外については、対応しなければならず、通知するという趣旨である。

② 脆弱性による影響が大きい場合

2016 年度脆弱性研究会において、早期警戒パートナーシップの運営上の問題として、製品の脆弱性情報の届出が急増したことにより、届出件数が膨大なため、受理前の状態で大量に溜まっている状況、本制度の存在意義を疑問視されかねない深刻な事態にいたっているという認識が示された。これに応じて「脆弱性情報の取扱い判断基準と取扱ルールに関する検討 WG」が開催され、その意見をもとに、従来は、届出順による一律の取扱いであったが、これを脆弱性の影響度に応じた取扱いに変更するべきであるとされて、取扱いルールについて見直しを図り影響度の高い案件を優先的に取り扱えるようにした。また、その際に、IPA・JPCERT/CC の作業効率を高めるため、影響度の低い脆弱性については、開発者やウェブサイト運営者に参考情報として通知するとともに、簡易な手続きで取扱いを終了することとされた。

このような考え方にもとづいて、P ガイドライン付録 4 で、脆弱性の深刻度と脆弱性の影響範囲の双方の観点から、脆弱性の影響度を判断する考え方が明らかにされている。影響度の考え方の詳細については、P ガイドライン付録 4 を参照されたい。

③ 受付の順序に関わらず、優先的に取扱いを行います

②で触れたように、従前は、届出順による取扱いであったところ、影響度において、深刻度が高い、もしくは、影響範囲が広いとされた場合において、優先的に取扱いがなされる。

5) 脆弱性関連情報の取扱い

IPA は、脆弱性関連情報に関して、正当な理由がない限り発見者・JPCERT/CC・当該製品開発者以外の第三者に開示しません。ただし、以下のような正当な理由がある場合、IPA は第三者に情報を開示することがあります。なお、技術的分析を依頼する場合、IPA は秘密保持契約を結びます

(ア) 脆弱性を有するソフトウエア製品が、他のソフトウエアやウェブサイトで利用されている場合に、それらの製品開発者やウェブサイト運営者に連絡する場合

(イ) 脆弱性が再現する状況を特定できない等の場合に、国立研究開発法人産業技術総合研究所や技術研究組合制御システムセキュリティセンター等の外部機関に脆弱性関連情報に関する技術的分析を依頼する場合

この場合、関係者の許諾を得た上で、JPCERT/CC と連携し、脆弱性の再現に必要な情報を製品開発者に開示することがあります。

また、IPA は、脆弱性関連情報に関して、それに関する脆弱性情報が一般に公表されるまでの間は、発見者・JPCERT/CC・当該製品開発者以外の第三者に漏えいしないように適切に管理します。

（解説）

当該規程の趣旨については、本報告書「Ⅳ．ソフトウエア製品に係る脆弱性関連情報取扱 2．発見者の対応　4)　脆弱性関連情報の管理および開示」を参照のこと。

① 脆弱性関連情報に関して、正当な理由がない限り発見者・JPCERT/CC・当該製品開発者以外の第三者に開示しません。

これは、脆弱性関連情報について、IPA が、意図的に発見者・JPCERT/CC・当該製品開発者以外の第三者が了知しうる状態にはしないという意味である。

ただし、正当な理由がある場合については、この限りではなく、下記で論じられる。

② 正当な理由がある場合、IPA は第三者に情報を開示することがあります

「正当な理由」とは、脆弱性関連情報を第三者に開示することにつき合理的な事情が存在することをいう。正当な理由の有無については、届出からの期間、当該脆弱性関連情報の内容、開示による即時の攻撃の可能性の有無・程度、対策の可能性、公表の目的・態様等の観点から総合的に判断される。

開示とは、自らの意思にもとづいて第三者が知りうる状態にすることをいう。

③ 第三者に漏えいしないように適切に管理します

「漏えい」とは、他人が知り得る状態にしておくことをいう。対策方法が示されないままに脆弱性関連情報が第三者に漏えいした場合、それが悪用されるおそれがあるので、適切に管理する旨を定めたものである。

6) 発見者に係わる情報の取扱い

これについては、特段、法的観点からコメントするべきものはない。

7) 脆弱性関連情報の受理後の対応

IPA は、JPCERT/CC に通知した脆弱性関連情報に関して、以下のいずれかに該当する場合、発見者に連絡するとともに、処理を取りやめることがあります。 (ア) 脆弱性関連情報に該当しない場合 (イ) 本ガイドラインの適用範囲外である場合 (ウ) 脆弱性による影響が小さい場合（付録４を参照） (エ) 脆弱性関連情報が既知であり、かつ公表されている場合 (オ) 製品開発者がすべての製品利用者に通知する場合（システム構築事業者を介して通知するケースを含む）

（解説）

① 処理を取りやめることがあります

取扱規程「第 2 ソフトウエア製品に係る脆弱性関連情報に関する取扱い 2 具体的な手続及び行動指針 (2) 受付機関 ア 届出の取扱い及び脆弱性情報の公表に係る手続及び行動指針 （ウ）」において「受付機関は、届出に係る脆弱性関連情報が次のいずれかに該当することが明らかになったときは、当該届出に係る処理を取りやめることができる。」としており、それに対応するものである。調整手続のなかで処理の取りやめということになる。

② (ア) 脆弱性関連情報に該当しない場合

取扱規程「第 2 ソフトウエア製品に係る脆弱性関連情報に関する取扱い 2 具体的な手続及び行動指針 (2) 受付機関 ア 届出の取扱い及び脆弱性情報の公表に係る手続及び行動指針 （ウ）」において「① 脆弱性関連情報に該当しないこと。」とされており、従前、脆弱性ではない場合としていたが、今回、取扱規程と用語を揃えた。脆弱性関連情報が検証された結果､セキュリティ上の問題箇所を示す事象が確認されない場合､または、再現された事象が、脆弱性の概念に該当しない場合などがこれに該当する。手続を進めた場合に、公表判定委員会において「脆弱性の存在が認められること」が必要であり、これは、公表判定委員会の主宰者である IPA が明らかにしなければならないものである。しかしながら、検証手続は、種々の労力・コストがかかる作業である。これらを総合的に配

慮して脆弱性が存在することを具体的に明らかにできる可能性が低い場合も、この概念に含まれるといえる（なお、具体的に例示可能であることが必要であることは後述）。従って、製品開発者からの応答がないような場合において、調整の過程において検証した結果、脆弱性が存在したとしても想定される影響度と比較して検証の労力をかけて、脆弱性が存在することを明らかにする意味があるとは考えられない場合もこれに含まれる。

③ (イ) 本ガイドラインの適用範囲外である場合

P ガイドライン「III. 本ガイドラインの適用の範囲」において適用範囲が示されており、脆弱性に起因する影響が特定かつ少数である場合や、日本国内で実質的な利用が考えられない場合などがこの場合に該当する。前記の取扱規程において「② 本規程の適用範囲外であること。」に該当する。

④ (ウ) 脆弱性による影響が小さい場合（付録 4 を参照）

4) JPCERT/CC への連絡でも論じたように、脆弱性による影響が少ない場合において、処理の取りやめをなすものとされたのに対応するものである。前記の取扱規程において「③ 脆弱性に起因する影響が生じるおそれが著しく低いこと。」に該当する。

⑤ (エ) 脆弱性関連情報が既知であり、かつ公表されている場合

そもそも、早期警戒パートナーシップにおいて調整されるべき脆弱性についての届出の要件として、「既に公表されている脆弱性情報に関する脆弱性関連情報でないこと。」が要求されているものであって、調整の過程において、当該要件をみたさないことが明らかになった場合には、処理を取りやめすることができるものとしたものである。前記の取扱規程において「④ 脆弱性関連情報が既知であり、かつ、脆弱性情報等が既に公表されていること。」に対応する。

⑥ (オ) 製品開発者がすべての製品利用者に通知する場合（システム構築事業者を介して通知するケースを含む）

ソフトウエア製品について多数の利用者がいる場合、その製品の脆弱性は、早期警戒パートナーシップの適用範囲内ということになるが、すべての製品利用者に通知する場合については、調整を進めて、公表をなすという手続をとる必要性に乏しいために、汎用性を欠く製品として、処理を取りやめることができるものとしたものである。

8) 発見者との情報交換ないし 11) 情報非開示依頼の取下げ

これについては、特段、法的観点からコメントするべきものはない。

12) 優先的な情報提供実施時の発見者への通知

IPA は、届出がなされた脆弱性関連情報に関して、JPCERT/CC から政府機関や国民の日常生活に必要不可欠なサービスを提供するための基盤となる設備を保有する事業者等に対して優先的に提供された場合、発見者に対して、その旨を通知します。当該基盤保有事業者は内閣サイバーセキュリティセンター（NISC）の最新の「重要インフラの情報セキュリティ対策に係る行動計画」 で定める重要インフラ事業者等とします。

（解説）

① 趣旨

重要インフラは国民の生活や経済を支える社会基盤であり、重要インフラを支えるシステムに深刻な脆弱性が見つかった場合には、重要インフラ事業者にその問題を伝え、リスク低減を促すことが望まれるという認識のもとに、JPCERT/CC が、脆弱性関連情報に

ついて当該事業者等に対して優先的に通知するものとした（後述）。詳細については、本報告書「IV.ソフトウエア製品に係る脆弱性関連情報取扱　4. JPCERT/CC（調整機関）の対応　8）優先的な情報提供」を参照のこと。

② 発見者に対して、その旨を通知

重要インフラ事業者に対して優先提供をなす場合においては、係る趣旨を発見者に伝えることが望ましいという判断にもとづくものである。取扱規程において「(ク) 受付機関は、調整機関から政府機関や事業者等に脆弱性情報等をあらかじめ通知する旨の連絡を受けたときは、発見者にその旨を通知すること。」（「第 2 ソフトウエア製品に係る脆弱性関連情報に関する取扱い　2　具体的な手続及び行動指針　（2）受付機関　ア 届出の取扱い及び脆弱性情報の公表に係る手続及び行動指針　（ク）」とされており、それに対応するものである。

(2)調整不能案件の公表判定について

1) 公表判定委員会の組織

IPA は、JPCERT/CC からIV.4. 10)の通知を受けて、JPCERT/CC と製品開発者との間で脆弱性情報の公表に係る調整が不可能であると判断した場合（以下「調整不能」という）、その案件が脆弱性情報を公表する条件を満たしているかを判定する「公表判定委員会」を組織します。

（解説）

① 設置の趣旨等

調整不能案件について、公表判定委員会が設置されるにいたった趣旨およびその枠組み等については、本報告書「1.8 公表判定委員会の概要と趣旨について」を参照のこと。

取扱規程においては、「第 2 ソフトウエア製品に係る脆弱性関連情報に関する取扱い　2　具体的な手続及び行動指針　（2）受付機関　イ 公表に係る調整が不可能な脆弱性情報の公表の可否の判定に係る手続及び行動指針」　が準備されている。

② 公表に係る調整が不可能であると判断した場合

公表にかかる調整とは、脆弱性関連情報の公表に関して製品開発者との間で合意にいたることをいう。合理的な期間内に、かかる合意に至ることが、社会通念上、期待できないと考えられる場合、「公表に係る調整が不可能であると判断した場合」に該当する。連絡がとれない場合、もしくは、意見の相違などにより、合意に至ることが困難であると判断される場合などがこれにあたる。

③ 公表判定委員会

脆弱性情報が公表する条件を満たしているかの判定する委員会をいう。取扱規程においては、「法律又はサイバーセキュリティに関する専門的な知識経験を有する者（判定を行う脆弱性情報に関し利害関係を有しない者に限る。）により構成される機関として、受付機関が設置するものをいう。」（取扱規程「第 1　総則　3　定義　（10）公表判定委員会」を参照）とされている。

会議の主宰者は、IPA である。詳細な点については、以下の解説を参照のこと。

2) 判定に必要な情報の収集・整理

これについては、特段、法的観点からコメントするべきものはない。

3) 調整不能案件に係る製品開発者への連絡

公表判定委員会は、調整不能案件の当事者である製品開発者に対し、当該脆弱性情報を公表すべきかどうか判定する旨を連絡します。

1) 連絡内容

公表判定委員会が製品開発者に伝える内容は、当該脆弱性情報とその存在を判断した根拠、経緯、公表予定の文案、意見書の提出先と提出期限です。

2) 連絡方法

公表判定委員会から製品開発者に対し、電子メール等の合理的手段をもって連絡を試みます。連絡は、プライバシーに十分に配慮します。

また、連絡不能案件の場合には、付録 5 の方法を実施したことをもって、通達努力を果たしたものとみなします。

なお、この製品開発者から、脆弱性検証の結果、対策方法および対応状況のいずれか一つ以上について新しい報告があった場合には、その内容に応じて、IPA は脆弱性関連情報に係る処理を JPCERT/CC に戻すことがあります。

（解説）

調整不能案件に係る脆弱性情報の公表は、長期滞留による弊害を避けてセキュリティ上の問題点から公共を守る、すなわち、脆弱性による問題を回避することを目的としたものであり、製品開発者が調整手続に従わないことに対する制裁ないし調整手続の実効性の確保を目的とする措置ではない。しかし、当該公表によって、製品開発者に対して一定の事実上の不利益が生じるおそれがあることは否定できない。そこで、①公表判定委員会という中立的な立場を有する機関から公表の可否の判定を受けること、②脆弱性が存在することや受付機関が広く一般に公表しない限り脆弱性を知り得ない製品利用者がいるおそれがあること等の一定の条件に該当する場合にのみ公表する旨の判定をすることができること、③判定に当たっては、製品開発者が意見を表明する機会を確保すること、④判定の結果、公表することとなった場合にも、公表する内容について製品開発者の見解を聴取し、当該見解を併記して公表すること等、調整不能案件の公表にあたり十分な手続規定を設けている。

このような製品開発者に対する手続保障の見地から、製品開発者に対して連絡する旨が定められているのが、この規定である。

4) 関係者からの意見聴取

公表判定委員会は、製品開発者をはじめとする関係者からの意見聴取を行います。意見聴取は、原則として書面による手続きで行います。また、公表判定委員会は、その裁量によって、関係者から口頭での意見を聴取することができます。

（解説）

上述したように製品開発者への十分な手続保障の一環としての規定である。取扱規程において「公表判定委員会は、判定をするときは、製品開発者（連絡を取ることができない者を除く。（略））が意見を表明する機会を確保すること」（取扱規程「第 2 ソフトウエア製品に係る脆弱性関連情報に関する取扱い　2　具体的な手続及び行動指針　（2）受付機関イ 公表に係る調整が不可能な脆弱性情報の公表の可否の判定に係る手続及び行動指針

（ウ）」を参照）に対応する。

5) 判定

公表判定委員会は、脆弱性検証結果や当該製品開発者をはじめとする関係者の意見書に基づき、脆弱性情報の公表に関する判定を行います。取り扱う案件が下記のすべての条件を満たす場合、IPA および JPCERT/CC で公表することが適当と判定します。それ以外は公表をしないことと判定します。

(ア) 調整機関と製品開発者との間の脆弱性情報の公表に係る調整が不可能であること（調整不能案件であること）

(イ) 脆弱性の存在が認められること

ソフトウエア製品の脆弱性とは、ソフトウエア製品等において、コンピュータ不正アクセスやコンピュータウイルス等の攻撃により、その機能や性能を損なう原因となりうるセキュリティ上の問題箇所です。ソフトウエア製品において、情報セキュリティの三大要素（機密性、完全性、可用性）の１つ以上が侵害される可能性があり、その原因となる問題挙動を IPA または JPCERT/CC が具体的に例示可能であり、製品開発者が反証できないとき、脆弱性の存在が認められると判断します。

なお、判断においては、一般的なソフトウエア製品の利用方法や、製品開発者があらかじめ提示している使用条件等を考慮します。

(ウ) IPA が公表しない限り、脆弱性情報を知り得ない製品利用者がいるおそれがあること

製品開発者が当該ソフトウエア製品の製品利用者全員に確実に通知することが困難な場合を対象とします。例えば、ソフトウエア製品が市販されている場合や、ウェブサイト等でダウンロード可能である場合はこれに該当します。

(エ) 製品開発者や製品利用者の状況等を総合的に勘案して、公表が適当でないと判断する理由・事情がないこと

製品開発者の取組みや製品利用者の状況を鑑みて、公表することが適当ではないと判断する明確な理由・事情がある場合には、公表を行いません。

（解説）

①公表判定委員会は、脆弱性検証結果や当該製品開発者をはじめとする関係者の意見書に基づき、脆弱性情報の公表に関する判定を行います。

取扱規程においては、「(ア) 受付機関は、調整機関から、製品開発者との公表に係る調整が不可能である旨の通知を受けたときは、公表判定委員会に対し、脆弱性情報の公表の可否の判定を求め、これを得ること。」（取扱規程「第 2 ソフトウエア製品に係る脆弱性関連情報に関する取扱い　2　具体的な手続及び行動指針　(2) 受付機関　イ 公表に係る調整が不可能な脆弱性情報の公表の可否の判定に係る手続及び行動指針　（ア）」を参照）とされているのに対応して、判定を行うことが定められている。

判定にあたって、十分な手続的保障がなされるべきことについては、本報告書「IV.ソフトウエア製品に係る脆弱性関連情報取扱　3. IPA（受付機関）の対応　(2) 調整不能

案件の公表判定について　3)　調整不能案件に係る製品開発者への連絡」を参照のこと。その一環として、脆弱性検証結果や当該製品開発者をはじめとする関係者の意見書に基づくものとされている。

②取り扱う案件が下記のすべての条件を満たす場合、IPA および JPCERT/CC で公表することが適当と判定します。

これは、取扱規程の「(イ) 公表判定委員会は、次に掲げる事項のいずれにも該当するときに限り、脆弱性情報を公表する旨の判定をすることができる（以下、略）」（取扱規程「第 2 ソフトウエア製品に係る脆弱性関連情報に関する取扱い　2　具体的な手続及び行動指針　(2) 受付機関　イ 公表に係る調整が不可能な脆弱性情報の公表の可否の判定に係る手続及び行動指針　（イ）」を参照）に対応するものである。

③調整機関と製品開発者との間の脆弱性情報の公表に係る調整が不可能であること（調整不能案件であること）

調整が可能であれば、通常の手続にしたがって処理すべきであるから、この要件は当然の前提を規定したものといえる。

④ 脆弱性の存在が認められること

脆弱性については、本報告書「Ⅱ.用語の定義と前提　1. 脆弱性」を参照のこと。「存在が認められること」については、IPA または、JPCERT/CC において、その問題挙動を具体的に明らかにする必要がある。そのために、問題挙動の明示に際しては、具体的な環境やコストの問題が生じる可能性があり、その場合には、脆弱性の存在が認められることとはいえない、ということになる。

⑤ IPA が公表しない限り、脆弱性情報を知り得ない製品利用者がいるおそれがあること

ソフトウエア製品に脆弱性が存在するとしても、製品利用者が不特定または多数に渡ることから、公表しない限り脆弱性情報を知り得ない製品利用者がいることである。その一方で、脆弱性情報について、製品開発者からの周知等、他の方法や手段ですべての製品利用者が知り得る場合には、受付機関が広く一般に公表する必要性はないと考えられる。

⑥製品開発者や製品利用者の状況等を総合的に勘案して、公表が適当でないと判断する理由・事情がないこと

（ア）ないし（ウ）の要件を満たした場合でも、脆弱性情報を公表することが不適当であると認められる特段の事情が存在する場合、公表を差し控えるべきと考えられることから、かかる要件が規定されている。具体的には、影響の軽微性、公表することによって生じる攻撃の危険性、公表に伴う法的な問題等を総合的に考慮して個別に判断される。

6) 結果の通知

これについては、特段、法的観点からコメントするべきものはない。

7) 判定後の対応

IPA は、判定結果によって、以下の処理を行います。

（ア）脆弱性情報を公表すると判定された場合の対応

脆弱性情報を公表するという判定になった場合、IPA は、その判定を踏まえ、脆弱性情報の公表を判断するとともに、以下の処理を行います。

・経済産業大臣に対して、公表に関する手続きが告示の定める手続きに適合していることについての確認を求めます。ただし、連絡不能案件

の場合、告示の定める手続きに適合していることについて確認はしません。

・公表日を決定します。

・公表する内容について製品開発者から併記を希望する見解を聴取します。ただし、連絡不能案件の場合、この確認はしません。

・JPCERT/CC に、公表日と製品開発者から得られた併記を希望する見解を通知します。

・公表日に、製品開発者名とともに脆弱性情報等を JVN で公表します。また、製品開発者から併記を希望する見解が提出された場合、その見解を併記して公表します。

・発見者に、公表したことを通知します。

（イ）脆弱性情報を公表しないと判定された場合の対応

脆弱性情報を公表しないという判定になった場合、IPA は、発見者にその結果と理由を通知します。

（ウ）脆弱性情報の公表に係る調整が可能であると判定された場合の対応

脆弱性情報の公表に係る調整が可能であると判定された場合、IPA は JPCERT/CC に製品開発者との調整を再度行うように通知します。

（解説）

① 脆弱性情報を公表すると判定された場合

これは、本報告書「IV.ソフトウエア製品に係る脆弱性関連情報取扱　3. IPA（受付機関）の対応　（2）調整不能案件の公表判定について　5 判定」において記載されている条件を満たす場合であり、公表判定委員会が公表するという判定にいたった場合をいう。

② IPA は、その判定を踏まえ、脆弱性情報の公表を判断する

IPA が、公表判定委員会の判定をふまえて公表を判断するということが明らかになっている。あくまでも公表の判断の主体は、IPA ということであり、この法的な根拠は、IPA が、必要があると認めるときには、サイバーセキュリティの確保のために電子計算機を利用する者が講ずべき措置の内容を公表することができるとの規定（情促法 43 条 3 項）である。

③ 経済産業大臣に対して、公表に関する手続きが告示の定める手続きに適合していることについての確認を求めます

情促法 43 条 4 項が、公表の方法及び手続については、経済産業省令で定めるとして、同法施行規則が定められ、同施行規則の規定に基づき、取扱規程が定められている。そこでは、公表の手続として経済産業大臣の確認が定められており（取扱規程「第 2 ソフトウエア製品に係る脆弱性関連情報に関する取扱い　2　具体的な手続及び行動指針　（2）受付機関　イ 公表に係る調整が不可能な脆弱性情報の公表の可否の判定に係る手続及び行動指針　（ク）」を参照））、手続の適合性を確認するという形を取りつつ、公表判定に係る手続が適当かを確認する過程で、告示の 4 要件に適合するか等も確認することにより実質的に公表が適当かを判断することとされている。

本項は、当該規定に対応するものであって、IPA が経済産業大臣について確認をもとめるものとしている。

④ 公表する内容について製品開発者から併記を希望する見解を聴取します

公表判定委員会の判定をふまえて判定される場合に、製品開発者が、自らの見解を併記して公表することをもとめた場合には、その見解が併記されて公表されることになる。その手続のために IPA が、見解を聴取するとしているものである。

⑤ JPCERT/CC に、公表日と製品開発者から得られた併記を希望する見解を通知

この併記の趣旨については、本報告書「IV.ソフトウエア製品に係る脆弱性関連情報取扱　4　JPCERT/CC（調整機関の対応）10）IPA への通知と判定に基づく公表」を参照のこと。

４．JPCERT/CC（調整機関）の対応

①調整機関の概念について

取扱規程は、調整機関について「ソフトウエア製品の脆弱性関連情報について、製品開発者への連絡及び公表に係る調整を行う機関として、経済産業大臣の定めるものをいう。」と定義している。

脆弱性の公表に際しては、発見者のベンダの識別・連絡の支援、複数のベンダに影響する脆弱性の調整、技術的分析・脆弱性報告の検証などの機能（調整）が重要であると考えられている。

1) 製品開発者リストの整備

これについては、特段、法的観点からコメントするべきものはない。

2) 製品開発者への連絡

JPCERT/CC は、届け出られた脆弱性関連情報の IPA からの通知を受け、製品開発者リストの活用や脆弱性関連情報を分析することにより、速やかに製品開発者を特定し、必要に応じて製品開発者リストに当該製品開発者を追加した上で、その製品開発者に連絡を行います。その際に、各製品開発者に対して、脆弱性検証を行い、その結果を報告することを求めます。

JPCERT/CC は、届け出られた製品と実質的な相互関係にある製品を特定した場合には、その製品開発者に連絡を行い、調整することができます。

また、JPCERT/CC は、OSS に関する事前通知を、製品開発者または開発コミュニティに加えて、必要に応じて OSS を導入した製品の開発者・ディストリビュータ・製品の仕様を決定するサービス提供者（例：携帯電話会社）へ通知します。

（解説）

① 速やかに製品開発者を特定し

製品開発者については、本報告書「Ⅱ.用語の定義と前提　9. 製品開発者」を参照のこと。

なお、JPCERT/CC が、調整者の機能のひとつとして他のソフトウエアやシステムに及ぼす影響の分析を行うよう努めるべきであるのは、以下、6）で触れられている。

② JPCERT/CC は、届け出られた製品と実質的な相互関係にある製品を特定した場合には、その製品開発者に連絡を行い、調整することができます。

上述のように他のソフトウエアやシステムに及ぼす影響の分析を行うことがもとめられているが、それによって影響を受ける製品に対して通知をなす場合のもっとも典型的

なひとつの例として、OSS などについて、通知をおこなうことを定めているものである。

ソフトウエア製品の開発者の定義は、きわめて広いため、当該規定の解釈として、OSS を導入した製品の開発者・ディストリビュータ・製品の仕様を決定するサービス提供者（例：携帯電話会社）は、この早期警戒パートナーシップの枠組み上、製品開発者として調整の連絡をなすことが可能となる。

3) 公表日の決定　から 4) 公表日決定後の対応

これについては、特段、法的観点からコメントするべきものはない。

5) 脆弱性関連情報の取扱い

JPCERT/CC は、脆弱性関連情報を第三者に開示しません。ただし、以下のような正当な理由がある場合、JPCERT/CC は第三者に情報を開示することがあります。

(ア)海外製品であり外国企業の日本法人や総代理店が無い場合

(イ)海外に大きな影響を与える脆弱性関連情報の場合

(ウ)脆弱性関連情報の詳細な分析が必要な場合　等

具体的には、秘密保持契約を締結した上で、海外の調整機関または IPA を含む外部機関に連絡や分析を依頼するケースがあります。

また、JPCERT/CC は、脆弱性情報を一般に公表するまでは、第三者に漏えいしないように管理します。

（解説）

① 脆弱性関連情報を第三者に開示しません。

これは、脆弱性関連情報について、JPCERT/CC が、意図的に第三者が了知しうる状態にはしないという意味である。ここでいう、第三者は、発見者、IPA、JPCERT/CC、製品開発者をいう。

ただし、正当な理由がある場合については、この限りではなく、下記で論じられる。

② 正当な理由がある場合、JPCERT/CC は第三者に情報を開示することがあります

「正当な理由」とは、脆弱性関連情報を第三者に提供することにつき合理的な事情が存在することをいう。正当な理由の有無については、届出からの期間、当該脆弱性関連情報の内容、開示による即時の攻撃の可能性の有無・程度、対策の可能性、公表の目的・態様等の観点から総合的に判断される。

開示とは、意図的に第三者が了知しうる状態にすることをいう。

③ 第三者に漏えいしないように管理します

「漏えい」とは、他人が知り得る状態にしておくことをいう。対策方法が示されないままに脆弱性関連情報が第三者に漏えいした場合、それが悪用されるおそれがあるので、適切に管理する旨を定めたものである。

6) 脆弱性関連情報の影響の分析

JPCERT/CC は、IPA と連携して、届け出られた脆弱性関連情報が他のソフトウエアやシステムに及ぼす影響の分析を行うよう努めます。影響の分析結果については、製品開発者に連絡します。

（解説）

① 脆弱性関連情報が他のソフトウエアやシステムに及ぼす影響の分析

脆弱性関連情報が存在しているソフトウエア製品は、その利用される状況によって他のソフトウエアやシステムに影響を及ぼす可能性が存在する。また、その脆弱性関連情報が存在する製品が、他の製品と統合されて、あたかもひとつの部品のような働きをする場合もある。それらの場合について JPCERT/CC は、影響を及ぼす範囲を確定して、場合によっては、製品開発者として調整を行うという趣旨である。

② 行うよう努めます。

JPCERT/CC にとっては、上記の影響範囲の確定は、義務ではないが、行うのが望ましいものとして定められている。このような場合に、JPCERT/CC が、通知をなすことは、本報告書「IV.ソフトウエア製品に係る脆弱性関連情報取扱　4. JPCERT/CC（調整機関）の対応　2）製品開発者への連絡」で触れられているし、また、当該開発者への通知が、本報告書「IV.ソフトウエア製品に係る脆弱性関連情報取扱　4. JPCERT/CC（調整機関）の対応　5) JPCERT/CC における脆弱性関連情報の取扱い」で触れられているように脆弱性情報の提供の禁止に触れるものではないことはいうまでもない。

7) 対策方法および対応状況の受付

これについては、特段、法的観点からコメントするべきものはない。

8) 優先的な情報提供

JPCERT/CC は、届出がなされた脆弱性関連情報に関して、国民の日常生活に必要不可欠なサービスを提供するための基盤となる設備に対し特に影響が大きいと推察される場合、IPA および製品開発者と協議の上、対策方法が作成されてから一般公表日までの間に、脆弱性情報と対策方法を、政府機関や当該基盤保有事業者等に対して優先的に提供することができます。 （以下、略）

（解説）

① 趣旨

一般公表前に脆弱性情報が明らかになると、当該脆弱性情報を元に攻撃コードが作成され、当該ソフトウエア製品の脆弱性への攻撃が開始される危険性がある。そのため、脆弱性情報の公表は調整機関が定めた脆弱性情報公表日に行うのが原則である（公表日一致の原則）。

しかしながら、当該脆弱性関連情報が国民生活に必要不可欠なサービスを提供するための基盤となる設備に重大な影響を与えた場合には、国民経済への重大な影響や場合によって生命・身体・財産の損失を被るおそれがある。そこで、届出のあった脆弱性関連情報が、国民の日常生活に必要不可欠なサービスを提供するための基盤となる設備に重大な影響を与えるおそれがあると認められるときには、一般への公表に先立って優先提供ができるとしたのが、早期警戒パートナーシップの趣旨ということになる。

② 国民の日常生活に必要不可欠なサービスを提供するための基盤となる設備

内閣サイバーセキュリティセンター（NISC）の最新の「重要インフラの情報セキュリティ対策に係る第４次行動計画」は、特に情報通信、電力、金融等、その機能が停止又は低下した場合に多大なる影響を及ぼしかねないサービスは、重要インフラとして官民が

一丸となり、重点的に防護していく必要があるとしている。上述の設備というのは、このようなサービスを提供するための基盤となる設備のことをいう。

また、P ガイドライン「IV.ソフトウエア製品に係る脆弱性関連情報取扱　3. IPA（受付機関）の対応　(1)脆弱性関連情報の届出受付と取扱いについて　12)優先的な情報提供実施時の発見者への通知」においても、同計画の重要インフラ事業者を優先提供の対象としている。

③ 特に影響が大きいと推察される場合

影響については、本報告書「III.本ガイドラインの適用の範囲　①脆弱性に起因する影響」を参照のこと。また、P ガイドライン付録 4 も参考のこと。

④ 対策方法が作成されてから一般公表日までの間

優先提供の対象となるのは、脆弱性情報と対策方法であるので、その定義から、対策方法が作成されていることが前提となっている。また、優先提供の実施は、一般公開までの間であることとされている。

⑤ 脆弱性情報と対策方法

旧告示では、その対象を、攻撃方法等も含める「脆弱性関連情報及び対策方法」としていたが、あくまで一般に公表するよりも先に政府機関等に優先提供を行うものであることからすれば、脆弱性情報と対策方法の通知にとどめるのが適当であるとされたものである。

9) 一般への情報の公表

これについては、特段、法的観点からコメントするべきものはない。

10) IPA への通知と判定に基づく公表

JPCERT/CC は、製品開発者との公表に係る調整が不可能と判断した場合には、その旨を IPA に通知します。 JPCERT/CC は、IPA から脆弱性情報を公表すると判定した旨の通知を受けた場合、脆弱性情報等を JVN で公表します。また、IPA から製品開発者の見解が通知された場合、その見解を併記 して公表します。判定により脆弱性情報を公表しないこととなった場合、公表せず取扱いを終了します。 なお、公表に係る調整を再度行うように IPA から通知された場合には、その内容に応じて、JPCERT/CC は脆弱性関連情報に係る処理を再開します。

（解説）

① 公表に係る調整が不可能と判断した場合

これについては、本報告書「IV.ソフトウエア製品に係る脆弱性関連情報取扱　3　IPA（受付機関）の対応　（2）調整不能案件の公表判定について　1) 公表判定委員会の組織　②公表に係る調整が不可能であると判断した場合」を参照のこと。IPA は、この通知を受けて、公表判定委員会を組織することになる。

② 脆弱性情報を公表すると判定した旨の通知を受けた場合

これは、IPA が、P ガイドライン「IV.ソフトウエア製品に係る脆弱性関連情報取扱　3　IPA（受付機関）の対応　(2)調整不能案件の公表判定について　6)結果の通知」にもとづ

いて、通知をなした場合と同様の規定である。

③ 脆弱性情報等を JVN で公表します

公表されるべき脆弱性情報等とは、当該脆弱性情報並びに製品開発者または IPA による脆弱性検証の結果、対策方法および対応状況をいう。

④ IPA から製品開発者の見解が通知された場合、その見解を併記して公表

脆弱性の公表をなすという見解がしめされた場合に、製品開発者が、その見解に不満がある場合には、製品開発者は、見解を IPA に対して連絡することによって、その見解を併記することを認めるというものに応じたものである。

これは、公表判定委員会によって判定がなされており、再度、考案することを制度として求めるということはあまり意味がないのではないかと考えられること、また、一度、脆弱性情報が公表されてしまったあとに再度、判断をやり直すというのも制度として考えにくいこと、脆弱性関連情報の判定内容について意見が相違する場合においては、これをかならず併記することにすれば、不服の申出が果たすべき機能を果たすものと考えられること、によるものである。

⑤ 公表に係る調整を再度行うように IPA から通知された場合

これは、P ガイドライン「IV.ソフトウエア製品に係る脆弱性関連情報取扱　3　IPA（受付機関）の対応　(2)調整不能案件の公表判定について　7）判定後の対応　（ウ）脆弱性情報の公表に係る調整が可能であると判定された場合の対応」、と同様の規定である。判定手続や公表の連絡について、開発者と連絡がとれていなかった／もしくは意見が相違していたのにかかわらず、その後、状況に応じて製品開発者が、調整に応じるつもりがあると考えるにいたったという場合は、別個に調整が可能であると判定される場合もあるものと考えられる。この場合においては、むしろ、調整を試みる段階にいわば復帰するということになる。「その内容に応じて、JPCERT/CC は脆弱性関連情報に係る処理を再開します。」というのは、調整が再開されるということを意味する。

５．製品開発者の対応

1) 窓口の設置

製品開発者は、JPCERT/CC との間で脆弱性関連情報に関する情報交換を行うための窓口を設置し、あらかじめ JPCERT/CC に連絡してください。この窓口が、JPCERT/CC の製品開発者リストに登録されることになります。併せて、製品開発者名等を「JPCERT/CC 製品開発者リスト」に掲載し公表することを承諾するかどうか連絡してください。（略）

（解説）

① 脆弱性関連情報に関する情報交換を行うための窓口

「情報交換を行うための窓口」とは、調整機関と脆弱性関連情報や調整に係るやり取りを行う窓口のことをいう。JPCERT/CC と製品開発者との連絡や調整を円滑に行うことが可能になる。取扱規程「第 2 ソフトウエア製品に係る脆弱性関連情報に関する取扱い　2　具体的な手続及び行動指針　（4）製品開発者　ア」と同趣旨の規定である。

2) 脆弱性検証の実施

製品開発者は、JPCERT/CC から脆弱性関連情報を受け取ったら、ソフトウエア製品への影響を調査し、脆弱性検証を行い、その結果を JPCERT/CC に報告してください。また、脆弱性が外部のソフトウエア製品に含まれることが推定される場合、JPCERT/CC に連絡

してください。
　何らかの理由で JPCERT/CC からの連絡を受け取れなかった場合も、JPCERT/CC から連絡不能開発者として示された場合には、速やかに JPCERT/CC に連絡してください。

（解説）

① ソフトウエア製品への影響を調査し、脆弱性検証を行い

　影響については、本報告書「III.本ガイドラインの適用の範囲　①脆弱性に起因する影響」を参照のこと。

② 外部のソフトウエア製品に含まれることが推定される場合

　製品開発者において、そのソフトウエアが、外部のソフトウエア製品に利用されている場合、また、脆弱性の要因であるそのソフトウエアの特定の処理が、外部のソフトウエアでも同様に利用されている場合などにおいては、外部のソフトウエア製品に脆弱性が含まれることが推定される場合になる。このような場合には、JPCERT/CC に連絡がなされることになる。連絡をうけた JPCERT/CC は、それらの外部のソフトウエア製品の開発者にたいしても脆弱性の通知をなして、その脆弱性についての調整を試みることもある。

③ JPCERT/CC から連絡不能開発者として示された場合

　連絡不能開発者については、P ガイドライン付録 5 を参照のこと。

3) 脆弱性情報の公表日の調整ないし 8) 対策方法の周知

　これについては、特段、法的観点からコメントするべきものはない。

6. その他

　これについては、特段、法的観点からコメントするべきものはない。

V.ウェブアプリケーションに係る脆弱性関連情報取扱

（解説）

1　制度の趣旨と位置づけ

　ウェブアプリケーションは、「インターネット上のウェブサイトで稼働する固有のシステム」と定義されており、脆弱性が存在したとしても、ウェブサイト運営者が対応すれば、脆弱性の対応としては足りることになる。従って、例えば、脆弱性が修正されないままであるとしても、それが脆弱性であることを公表してそのウェブサイトの一般利用者に生じるリスクを減少させる必要性は乏しいものということができる。しかしながら、脆弱性から生じるリスクとしては、なおも存在するので早期警戒パートナーシップの枠組みでこれを処理しようというのが、ウェブアプリケーションに係る脆弱性関連情報取扱の規定の趣旨ということになる。

　なお、このような規定の趣旨に対応して、法的な枠組みも異なってくる。

　情促法 43 条 3 項では、IPA が「調査のうちサイバーセキュリティに関するものを行つた場合において、必要があると認めるときは、（略）事業者その他の電子計算機を利用する者が講ずべき措置の内容を公表するものとすると」している。取扱規程は、「必要があると認めるとき」の一つとしてソフトウエア製品に関して脆弱性が存在する場合に、IPA が調査をなして、その情報を公表することが、業務のひとつになることを示している。取扱規程が、脆弱性関連情報の対象範囲や判定の基準等を規定していることは、その業務の詳細を示し

ていると解されることになる。

これに対して、ウェブアプリケーションに係る脆弱性は、ウェブサイト運営者が対応すれば不特定多数への公表は適切でないため、情促法 43 条 3 項の「必要があると認めるとき」には該当しないと解されている。そのため、取扱規程の「ウェブアプリケーションに係る脆弱性関連情報に関する取扱い」の規定は、情促法 43 条 4 項の委任の範囲ではないものの、「必要があると認めるとき」の解釈に係るという意味で、同 3 項の規定を実施するためのものとして定められていると解されている。

また、ウェブアプリケーションに係る脆弱性については、ウェブサイト運営者に通知がなされて、ウェブサイト運営者がその脆弱性を検証して、実際に存在すれば、それを修正するということを制度として念頭においている。その場合に、もし、ウェブサイト運営者が通知を受領するにもかかわらず、検証をなさない、または、検証しても、修正をなさないということが社会通念上、明らかな場合においては、この取扱いの目的を実現することができないことが明確になったものとして、取扱いとしては、終了することになる。

なお、P ガイドラインの法的な意味については、基本的にはソフトウエア製品の P ガイドラインが参考になるために、本章においては、特に、ウェブアプリケーションに関する取扱いで独自のものについて、触れるものとする。

2. 発見者の対応

以下に記載していないものについては、特にコメントをなすべき事項はない。

3) 脆弱性関連情報の管理および開示

発見者は、脆弱性関連情報を正当な理由がない限り第三者に開示しないでください。ただし、正当な理由があって脆弱性関連情報を開示する場合には、事前に IPA に相談してください。発見者は、脆弱性が修正されるまでの間は、脆弱性関連情報が第三者に漏えいしないように適切に管理してください（発見者に対する情報非開示依頼、以下「情報非開示依頼」という）。脆弱性関連情報の管理および開示に係る法的な問題に関しては、付録３を参照してください。

（解説）

これらの用語の意味等については、本報告書「IV.ソフトウエア製品に係る脆弱性関連情報取扱　2　発見者の対応　4)脆弱性関連情報の管理および開示」の解説を参照のこと

3. IPA（受付機関）の対応

以下に記載していない物については、特にコメントをなすべき事項はない。

2) 届出の受理

IPA は、届出の記載が以下の条件をすべて満たしていると判断した時、その時点で届出を受理し、発見者に連絡します。 (ア) 上記 2. 4)の項目がすべて記載されていること (イ) 届出内容に矛盾等が無いこと (ウ) 届出の対象が本ガイドラインの適用範囲に該当すること（Ⅲ章を参照） (エ) 記載されている内容が脆弱性であること

(オ)既知の脆弱性とは異なる脆弱性の関連情報であること（ウェブサイト運営者により既に修正された脆弱性ではないこと）

（解説）

これらの用語の意味等については、本報告書「IV.ソフトウエア製品に係る脆弱性関連情報取扱　3　IPA（受付機関）の対応　(1)脆弱性関連情報の届出受付と取扱いについて　2）届出の受理」の解説を参照のこと。

4) 脆弱性関連情報への対応続行の判断

IPA は、以下の条件のいずれかと合致した場合、処理を取りやめるとともにウェブサイト運営者および発見者に連絡します。なお、取扱いを終了する場合、IPA の発見者に対する情報非開示依頼は効力を失います。

(ア)脆弱性関連情報に該当しない場合

(イ)本ガイドラインの適用範囲外である場合

(ウ)脆弱性による影響が小さい場合（付録 4 を参照）

(エ)ウェブサイト運営者から脆弱性関連情報が既知であり、その脆弱性が 修正されていると連絡があった場合

(オ)ウェブサイトの不適切な運用（付録 1 を参照）のうち、脆弱性の原因が下記と判明したもので、IPA が注意喚起等の方法で広く対策を促した後、処理を取りやめる判断をした場合

・ウェブサイトが利用しているソフトウエア製品の設定情報が誤っている場合や初期状態のままとなっている場合。

・ウェブサイトが利用しているソフトウエア製品の修正プログラムが適用されていない場合。

(カ)ウェブサイト運営者から適切な応答が得られない場合（5）を参照）

(キ)ウェブサイト運営者から脆弱性による影響度が低い等の理由により対応を行わないと連絡があった場合

上記(オ)の注意喚起後は、該当するソフトウエア製品の製品開発者も対策方法の再度の周知をウェブサイト運営者へ行うことを推奨します。

（解説）

① 以下の条件のいずれかと合致した場合

IPA が処理を終了させることができる場合の条件が記載されている。もっとも、以下で記される条件については、そもそも、処理の前提条件であることから、それが欠けていることが明らかになった段階で処理が終了すべきもの（（ア）から（ウ））、本制度の趣旨からして取扱いの目的を達成して終了するもの（（エ）から（オ））、同目的を達成することが不可能であることが確定することによって、取扱いとしては、終了と認識されるもの（（カ）ないし（キ））などのバリエーションがある。

個別の条件の趣旨については、後述する。

② 処理を取りやめる

IPA が処理を終了させるという規定である。

③ ウェブサイト運営者および発見者に連絡します

届出の取扱い状況を発見者に知らせるために、処理が終了した場合に連絡する規定

である。取扱規程においては、「処理を取りやめるときは、発見者にその旨及びその理由を通知すること。」と定めている。

④ 取扱いを終了する場合、IPA の発見者に対する情報非開示依頼は効力を失います

情報非開示依頼については、本報告書「IV.ソフトウエア製品に係る脆弱性関連情報取扱　2　発見者の対応　4)脆弱性関連情報の管理および開示」を参照のこと。

⑤個別の場合について

（ア）および（イ）の場合は、IPA による取扱いをなすことが妥当ではなかったものであり、取扱いを終了するものとしている。

（ウ）の場合は、脆弱性関連情報の取扱いに係る業務の効率化の観点から、処理を取りやめることができるとされている。

（エ）の場合は､取扱いによる目的が既に自主的に達成された場合に該当するのであり、取扱いは終了すべきものとなることから、処理を取りやめることができるとされている。

（オ）の場合は、ウェブサイトが利用しているソフトウエア製品の設定情報が誤っている場合や初期状態のままとなっている場合、修正プログラムが適用されていない場合等の不適切な運用が原因で、脆弱性が存在する状況になっている場合においては、IPA が当該ソフトウエア製品の対策を広く促すことによって、不特定多数への影響を回避できる場合は、取りやめることができるとされている。

（カ）の場合は、ウェブアプリケーション脆弱性については、ウェブサイト運営者において自主的に修正をなすことによって取扱いが終了するのみであって、脆弱性を公表するということは、考えられないことから、自主的な修正が実現されることが起こり得ないと判断される場合には、取扱いが終了することとなっている。

（キ）の場合は、（カ）と同様の趣旨である。

5) ウェブサイト運営者への連絡

IPA は、上記 2)、3)および 4)における対応の是非の判断の結果、対応することが妥当との判断を下した脆弱性関連情報について、速やかにウェブサイト運営者に通知します。

（解説）　これは、IPA が受理した場合、IPA がウェブサイト運営者に通知することを定めたものである。

4. ウェブサイト運営者の対応

以下に記載していないものについては、特にコメントをなすべき事項はない。

4) ウェブサイト運営者内の情報の管理と開示

ウェブサイト運営者は、脆弱性関連情報を正当な理由がない限り第三者に開示しないでください。ただし、ウェブサイト運営者が脆弱性修正を依頼した外部機関、およびウェブサイトの管理を委託している外部機関には、秘密保持契約を締結した上で脆弱性関連情報を連絡することを推奨します。 また、ウェブサイト運営者は、脆弱性が修正されるまでの間は、脆弱性関連情報を第三者に漏えいしないように管理してください。なお、ウェブサイト運営者は、脆弱性の修正の過程でソフトウエア製品の脆弱性であることを認識した場合、脆弱性関連情報を第三者に正当な理由がない限り開示しないでください。また、当該脆弱性情報等が公表される

まで情報を第三者に漏えいしないように管理してください。

（解説）

①脆弱性関連情報を正当な理由がない限り第三者に開示しないでください。

当該規定の趣旨については、本報告書「Ⅳ.ソフトウエア製品に係る脆弱性関連情報取扱　2.発見者の対応　4)　脆弱性関連情報の管理および開示」で解説したとおりである。ウェブサイト運営者が、外部機関に対して、脆弱性修正を依頼すること、また、ウェブサイトの管理を委託している場合において、その委託を受けている者に対して、脆弱性関連情報を開示することは、「正当な理由」に基づいて開示される例となる。

②ただし、ウェブサイト運営者が脆弱性修正を依頼した外部機関、およびウェブサイトの管理を委託している外部機関には、秘密保持契約を締結した上で脆弱性関連情報を連絡することを推奨します。

①において「正当な理由」に基づいて開示される場合であっても、第三者へと漏えいした場合においては、悪用される可能性が存在するために、開示される場合には、秘密保持の締結が推奨されることとなる。

5) 脆弱性関連情報の公表

ウェブサイト運営者は、ウェブアプリケーションの脆弱性関連情報に関して、積極的に公表する必要はありません。ただし、この脆弱性が原因で、個人情報が漏えいした等の事案が起こったまたは起こった可能性がある場合、二次被害の防止および関連事案の予防のために、以下の項目を含むように公表してください。

また、当該個人からの問い合わせに的確に回答するようにしてください。

- 個人情報漏えいの概要
- 漏えいしたと推察される期間
- 漏えいしたと推察される件数
- 漏えいしたと推察される個人情報の種類（属性等）
- 漏えいの原因
- 問合せ先

（解説）

旧告示においては、「ウェブサイト運営者は、「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、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」こととされていたものであり、それに対応するものである。なお、取扱規程においては、個人情報漏えい時に対策を取ることの重要性は認識できる一方で、取扱規程が情報の適切な流通等を目的としたものであることや、マイナンバー法改正等の個人情報に係る他の制度整備の現状等に鑑み、取扱規程では規定しないこととされている。

① 「ウェブサイト運営者」については、本報告書「II. 用語の定義　11. ウェブサイト運営者」、「脆弱性関連情報」については本報告書「II. 用語の定義　2. 脆弱性関連情報の種類」を参照のこと。

② 積極的に公表する必要はありません

ウェブサイト運営者が、脆弱性が存在したという事実関係を公表する必要はないことを意味する。

③ 個人情報

個人情報保護法の第 2 条 1 項は、「個人情報」について「生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう」として、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。）などをいうとされている。

④ 漏えいした等

「等」には、個人情報の改竄、消去などが含まれる。

⑤ 事案が起こったまたは起こった可能性がある場合

個人情報保護委員会は、個人情報保護法のガイドライン等を定めている。そのうち、個人情報保護法ガイドライン（通則編）においては、「漏えい等（※）の事案が発生した場合等において、二次被害の防止、類似事案の発生防止等の観点から、個人情報取扱事業者が実施することが望まれる対応については、別に定める。」としており、これに対応するものとして「個人データの漏えい等の事案が発生した場合等の対応について（平成 29 年個人情報保護委員会告示第 1 号）」がある。この記述は、同告示における 2. 漏えい等事案が発覚した場合に講ずべき措置の「（6）事実関係及び再発防止策等の公表」（漏えい等事案の内容等に応じて、二次被害の防止、類似事案の発生防止等の観点から、事実関係及び再発防止策等について、速やかに公表する）に対応するものである。

⑥ 公表

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。

⑦ 当該個人からの問い合わせに的確に回答するようにしてください。

これは、⑤でふれた「個人データの漏えい等の事案が発生した場合等の対応について（平成 29 年個人情報保護委員会告示第 1 号）」の「（5）影響を受ける可能性のある本人への連絡等」（漏えい等事案の内容等に応じて、二次被害の防止、類似事案の発生防止等の観点から、事実関係等について、速やかに本人へ連絡し、又は本人が容易に知り得る状態に置く。）に対応するものである。

付録 3 法的な論点について

1.発見者が心得ておくべき法的な論点

発見者が心得ておくべき法的な問題に関する法律専門家の見解を述べます。

1－1. 脆弱性関連情報の発見に際しての法的な問題

（1）関連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、インターネット等を

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（不正アクセス行為の禁止等に関する法律）に抵触します。

① 脆弱性関連情報を利用して

「脆弱性関連情報」については、本報告書「II. 用語の定義　2. 脆弱性関連情報の種類」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 インターネット等を介して

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 アクセスした場合には、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、取扱規程「第 1　総則　3 定義　(7) コンピュータ不正アクセス」を参照のこと。

・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 2 条 4 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 2 条 4 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かかる利用権者の承諾を得てするものについては、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。

・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。なお、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）。

② 電子計算機損壊等業務妨害罪にも抵触する

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、専門的には、上記の偽計（もしくは威力）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が、刑が上記の業務妨害罪に対して重いため、「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」という中間結果についての認定は、軽微なウイルス等による攻撃行為に対しての適用は、困難をきたすであろうと考えられる。

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 キーを解読して通信内容を復号すること）は、電波法 109 条の 2 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傍受し

「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。

② 複合する行為

「復号」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。

③ 電波法 109 条の 2 に触れる

電波法 109 条の 2 は、「暗号通信を傍受した者又は暗号通信を媒介する者であっ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。」と定めており、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 不正アクセス禁止法に抵触しないと推察される行為

これは、不正アクセス禁止法の構成要件に該当する違法・有責な行為ではないと「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、「電子商取引及び情報財取引等に関する準則」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等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 に関する情報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 2 条 4 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)に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「1.5 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　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。

これは、P ガイドライン「IV. ソフトウエア製品に係る脆弱性関連情報取扱　3. IPA（受付機関）の対応　（1）脆弱性関連情報の届出受付と取扱いについて　3) 違法な手段で入手された脆弱性関連情報への対応」等と対応するものであって、届出として受理しないことを意味する。具体的な意味については、本報告書「1.5　脆弱性発見と不正アクセス、そして、届出の受理について」を参照のこと。

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。

1－2. 脆弱性関連情報の管理および開示に際しての法的な問題

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

3) 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。
4) 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。
5) 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および開示について真摯な態度が必要とされます。
6) 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、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」としているのである。

③ その一つの方向性を提唱する

早期警戒パートナーシップの方向性であり、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、製品開発者やウェブサイト運営者および届出機関に対して、これを報告し、正当な事由のないかぎり、不用意な開示を慎むという方向性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

管理および開示にあたって、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。P ガイドラインにおいては、 本報告書「IV.ソフトウエア製品に係る脆弱性関連情報取扱 2. 発見者の対応 4) 脆弱性関連情報の管理および開示」の「正当な理由なく」という文言の解釈で示された種々の事由が、開示にあたって考慮にいれるべき事項として参照されることが推奨されることとなる。

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。脆弱性関連情報の開示について、何らかの問題が生じた場合に、違法性が阻却されるべきであるとかと提唱しているものではない点に留意が必要である。

この体制は、この脆弱性関連情報の取扱いについて、この体制に則った場合に一定の法的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、管理および開示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。

（解説）

① 名誉毀損罪

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 条の 2 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。

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。

（解説）

① 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、信用毀損罪を認めている。条文上「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。

②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。

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、損害賠償責任等の民事責任を追及される可能性があります。

（解説）

① 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。

② 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問題は、明確な判断基準が明らかであるとはいえないが、それがない場合に、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。

2. 製品開発者が心得ておくべき法的な論点

製品開発者が心得ておくべき法的な問題に関する法律専門家の見解を述べます。

(1) 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。

（解説）

① ソフトウエアの提供行為

ユーザと開発者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、保守を受ける行為と考えられる。

「提供」時について考えれば、ソフトウエアの使用許諾時と考えられる。

「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。

② 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。

(2) 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。

（解説）

① 提供したソフトウエア／設計上の問題／プログラミング上の問題／運用上の問題

前述（1）についての解説を参照のこと。

② 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

脆弱性のある箇所を指す。

③ 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。

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り、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

本報告書「II. 用語の定義　3. 対策方法」を参照のこと。

(3)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　対策方法の選択

本報告書「II. 用語の定義　3. 対策方法」を参照のこと。

②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、対策方法はサポート条項の合理的な解釈によって定められることになるためである。個々の対策方法の種類については、本報告書「II. 用語の定義　3. 対策方法」を参照のこと。

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）の対象となる可能性があります。

①対策方法の選択

対策方法」の種類については、本報告書「II. 用語の定義　3. 対策方法」参照のこと。

①　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」で触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）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。

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。

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「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

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かしがあるとき（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」

と規定し、上記の条項を無効であるとしている。

（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

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

される場合があり得る。ソフトウエ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得、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」[29]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、故意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侵害、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。

3. ウェブサイト運営者が心得ておくべき法的な論点

ウェブサイト運営者が心得ておくべき法的な問題に関する法律専門家の見解を述べます。

1）ウェブサイト運営者と、ウェブサイト利用者との間においては、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、ウェブサイト利用者が、そのサイトに一定の個人情報等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 ウェブサイト利用者が、そのサイトに一定の個人情報等をゆだねる場合

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」をいう。個人情報保護法 2 条 8 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、個人情報保護法の「利用目的の特定」（同法 15 条）、「利用目的による制限」（16 条）、「適正な取得」（17 条）、「取得に際しての利用目的の通知等」（18 条）、「データ内容の正確性の確保等」（19 条）、「安全管理措置」（20 条）、「従業者の監督」（21 条）、「委託先の監督」（22 条）、「第三者提供の制限」（23 条）

[29] 消費者庁　「製造物責任（PL）法の逐条解説」第 2 条（定義）
（https://www.caa.go.jp/policies/policy/consumer_safety/other/product_liability_act_annotations/pdf/annotations_180907_0003.pdf）

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ライバシポリシ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。

2）各サイトに「プライバシポリシ」等が記載されている場合には、その内容をも前提にウェブサイト利用者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」等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ウェブサイト利用者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。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、この点については、「電子商取引および情報財取引等における準則」[30]のI－2－1「ウェブサイトの利用規約の契約への組入れと契約締結後の規約変更」を参照されたい。

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ある場合、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ある場合、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 を免れるような規定

上記の義務違反で生じる損害賠償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、本報告書「付録 3 法的な論

[30] 経済産業省 「電子商取引および情報財取引等における準則」（2018 年 7 月）（http://www.meti.go.jp/press/2018/07/20180727001/20180727001-1.pdf）

点について　2. 製品開発者が心得ておくべき法的な論点」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。

以上