脆弱性情報に係る調整不能案件の公表に関する
基礎調査報告書

2012 年 3 月

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

はじめに

ソフトウエアやウェブアプリケーションの脆弱性が発覚すると、それを悪用する攻撃が多発し、企業や個人、さらに社会全体にも大きな被害を与える可能性がある。したがって、ソフトウエアやウェブサイトの脆弱性が発見された場合、関係者間で秘密裏に共有するとともに、対策方法を整え、適切なタイミングでユーザに周知することが望まれる。

「情報セキュリティ早期警戒パートナーシップ」（以下「パートナーシップ」という。）は、独立行政法人 情報処理推進機構（以下「IPA」という。）、一般社団法人 JPCERT コーディネーションセンター（以下「JPCERT/CC」という。）等が中心となって、2004 年 7 月に運用を開始した。パートナーシップは、情報システム等の脆弱性について、その発見から対策の策定・公表に至るまでの過程に関与する関係者に期待する行動基準(「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「ガイドライン」という。)）を示すことにより、脆弱性関連情報を適切に流通させ、より迅速な対策方法の提供・適用を促す産官連携の取組みである。経済産業省告示「情報システム等脆弱性情報取扱基準」（2004 年 7 月 7 日公示)に基づく公的な制度として運用されているという点で、国際的にも例を見ない独自の制度といえるが、その一方、脆弱性関連情報の取扱いは国際的な連携により実施することが必要となることから、運用面では国際的な実務とも整合する形を採用している。

パートナーシップの立ち上げ・運用に際し、IPA では関係者や有識者で構成する「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。）を設置して、関係する様々な問題点とその改善策について検討・提言するとともに、ガイドラインの改訂、脆弱性対策に係る各種啓発資料の策定等を実施してきた。しかし一方で様々な理由により Japan Vulnerability Notes（以下「JVN」という。） 公表も終了もできない調整不能案件が発生している。そこで、2010 年度脆弱性研究会では、法務専門家や有識者による「脆弱性情報に係る調整手続検討ワーキンググループ」を設置し、調整不能案件の処理の具体化について検討した。具体的には、調整不能案件について IT ユーザが被害を受ける可能性をできる限り低減するため、調整不能のまま滞留することを可能な限り避け、必要に応じて公表も行う取扱手順など、関係者が実施すべき調整手続について、検討を行った。ただし、公表の具体的なプロセスについては、さらなる検討が必要である。

本報告書は、そうした検討に資する情報として、合意に至らない状況での公表に関する関連事例や製品開発者の意識などを調査し、ワーキンググループでとりまとめた成果である。本検討にご尽力いただいた関係各位にあらためて深

く御礼申し上げる。

2011 年 8 月
脆弱性情報に係る調整手続検討ワーキンググループ
主査　　高橋 郁夫

目　次

1. 調査の背景

2010 年度脆弱性研究会において、脆弱性情報に係る調整手続検討ワーキンググループ（以降本章では WG と呼ぶ）では、「調整不能状況」の整理に基づき、検討範囲を、製品開発者と JPCERT/CC 間で連絡がとれない場合に連絡をとるための活動（フェーズⅠ）と、それでも連絡がとれない場合もしくは調整が難航した場合に調整不能案件を公表する活動（フェーズⅡ）に分け検討することとした。

本調査では、フェーズⅡの基礎情報として、合意に至らない状況での公表に関する関連事例や製品開発者の意識などを調査し、その内容を WG においてとりまとめた。

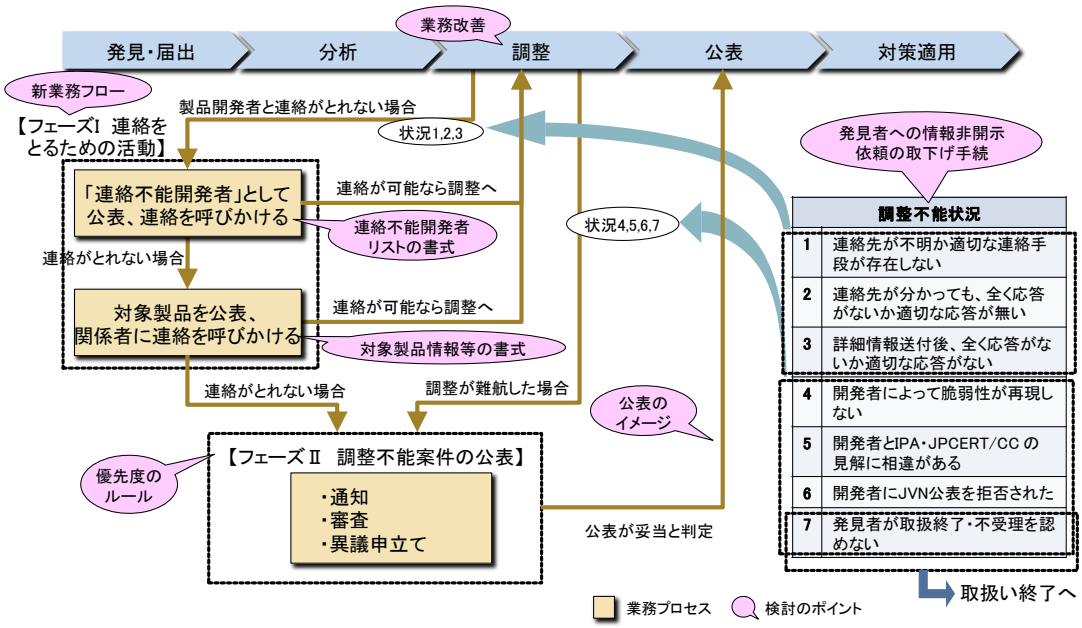

図 1-1　検討の全体イメージ

【フェーズⅠ：連絡をとるための活動】

調整不能案件において、製品開発者と連絡がとれないケースでは、まず連絡をとるため、できる限り努力する必要がある。具体的には、「連絡不能開発者」として JVN で公表する。さらに一定期間連絡がなければ、より具体的な情報（製品名等）を JVN で公表し、製品開発に係わる関係者に広く情報提供を呼びかける。

【フェーズⅡ：調整不能案件の公表】

連絡がとれない案件、または調整が難航して事実上調整が困難な案件については、JVN での公表を前提とした処理（「通知」「審査」「異議申立て」等のプロセスが想定される）に入る。

2. 調整不能案件の公表に関する関連事例調査

調整不能案件の公表に関連する事例を調査した。具体的には、以下の関連事例を明らかにするとともに、調整不能案件の公表プロセスとして具備すべき機能や想定されるリスク等を整理した。

2.1. 想定される調整不能案件の公表プロセスの参考となる既存の社会制度等の事例

調整不能案件の公表に関連する事例として、想定される調整不能案件の公表プロセスの参考となる既存の社会制度等について調査を行った。

(1) 独立行政法人 製品評価技術基盤機構（NITE）：事故情報収集制度

①制度の概要

- 本制度の根拠は、消費生活用製品安全法（昭和 48 年 6 月 6 日法律第 31 号）の付帯決議である。当初は、NITE が扱う任意の報告制度として始まり、必ずしも公表を前提とするものではなかったが、公益性に配慮して、平成 8 年以降は公表を前提としている。
- 対象は、一般消費者が使うもののうち、他の法律で規制されていない製品の事故（製品事故[1]）である。事故が発生した案件だけでなく、事故が発生するおそれがある場合も案件として扱う。
- 消費生活用製品安全法の改正（平成 18 年 12 月 6 日法律第 104 号）により、重大製品事故については製造・輸入事業者が経済産業省に届け出る義務を課すことになった。現在は、重大製品事故は消費者庁、非重大製品事故は NITE が通知先になっている。

②プロセス

- 本制度のプロセスは、以下の手順と処理で進められる。

1)事業者からの報告、消費生活センター・消防・警察等からの通知書の受付

[1] 一般消費者の生命又は身体に対する危害が発生した事故、あるいは、消費生活用製品が滅失し、又はき損した事故であって、一般消費者の生命又は身体に対する危害が発生するおそれのあるもののいずれかであって、消費生活用製品の欠陥によって生じたものではないことが明らかな事故以外のもの。

受理後に事業者側の見解（第二報）を要請する。

2)NITE の事故調査や事業者側の報告書に関する専門家のチェック

内容に不明な点がある場合には、その点を指摘し、再調査を要請する。

3)専門家ワーキンググループでの審議

4)事業者側の意見聴取

公表文書案を事業者に送付し、弁明の機会を与え、意見があれば１週間から 10 日以内に提出するよう要請する。

5)第三者委員会（事故動向等解析専門委員会）での審議

NITE と事業者の見解に相違があれば、第三者委員会で双方の意見を提示する。

6)文書の公表

NITE と事業者は見解の相違を調整する。NITE と事業者の見解に相違がなくなれば第三者委員会審議の後に公表する。NITE と事業者の見解に相違があれば両論併記で公表する。

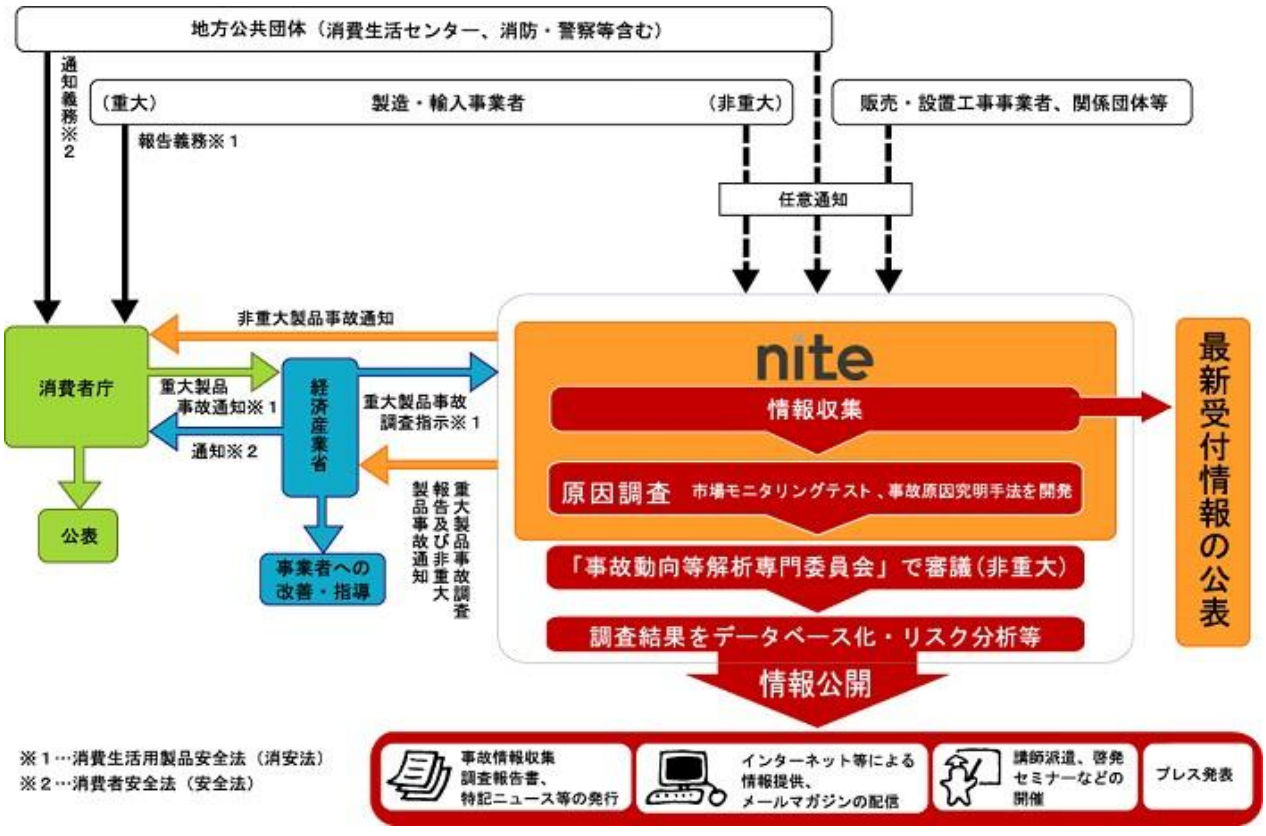

図 2-1　事故情報収集制度の概要

（出典：NITE ホームページ　http://www.nite.go.jp/jiko/index2.html）

・ 上記 4)、6)のステップを通じて、事業者に対し、「弁明の機会」を提供している。

③第三者委員会（事故動向等解析専門委員会）

・ 客観性を保つため、外部委員 12 名で構成。
・ OB を含む企業関係者や企業団体、弁護士等は、案件に直接関わる可能性があるため、委員に入れていない。
・ 年 4 回程度開催し、取扱件数は約 4000 件/年に達する。
・ 傘下に 3 つの専門家ワーキンググループを設置（電気技術、機械技術、化学・生体障害技術） し、詳細な検討を行う。
・ 委員には資料を事前送付して見てもらい、疑義があるもの等検討が必要な案件をあらかじめ選んで提示していただく。提示された案件については、詳細資料を用意して会議で説明し検討を行う（詳細資料は会議後回収、非公表）。
・ 委員長の判断で、参考人として当事者や他社のエンジニアを会議の場に呼び、意見を聴くことができる。

④その他

・ 非開示にしている詳細資料について、情報公開請求がなされることがあるが、その場合は「独立行政法人等の保有する情報の公開に関する法律」に基づき処理する。個人情報はマスクするが、企業側が営業機密と主張する技術情報は消費者の安全な生活確保の観点から基本的にはマスクできず開示することになる。

(2) 国民生活センター：相談情報の収集・分析・提供

①制度の概要

・ 独立行政法人国民生活センターでは、「消費者基本法」（「消費者保護基本法」(昭和 43 年 5 月 30 日法律第 78 号)を平成 16 年 6 月改正時に改題）及び「独立行政法人国民生活センター法」（平成 14 年 12 月 4 日法律第 123 号）に基づき、消費生活に関する情報を全国の消費生活センター等から収集し、消費者被害の未然防止・拡大防止に役立てている。
  1)商品に関するテスト結果に関する注意喚起
  2)市場に出回る商品による事故の危害案件に関する注意喚起
  3)サービスや取引に関する注意喚起
・ 事業者情報の公表は、法律に明確に記載されている事項ではないため、同センターは内部規程として「独立行政法人国民生活センター情報提供規程[2]」を設けている。

[2] http://www.kokusen.go.jp/hello/pdf/k_jouhou.pdf

②プロセス

【商品に関するテスト結果】

・ 商品テストは、まずテスト方法を企画し、必要に応じて商品テスト分析・評価委員会においてその妥当性を検証する。次に、テストを実施し、その結果を同委員会において検証した上で、事業者説明会を実施、公表に関する意見を聴取する。最終的に商品テスト結果を公表する。
・ 公表後に事業者からの意見があれば、国民生活センターの意見とあわせて公表している。

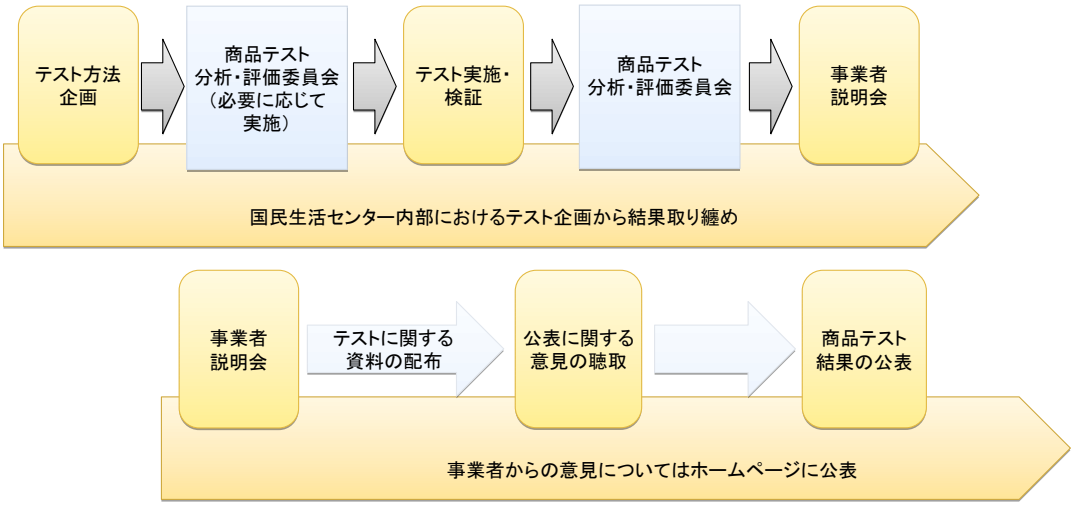

図 2-2　商品に関するテスト結果に関する注意喚起の概要

（出典：独立行政法人国民生活センターへのヒアリング結果を基に MRI が作成）

【サービスや取引に関する注意喚起】

・ サービスや取引による被害が多発しているケースでは、情報提供委員会での審議を経て、公表する。その場合、事業者に対し公表内容を内容証明郵便等で通知し、意見を求める。

③第三者委員会

【商品テスト分析・評価委員会】

・ 商品のテスト企画・テスト結果の評価を行う委員会。商品テストの企画を行うとき（必要に応じて）と、テスト結果が出たときに開催される。
・ 委員 10 人程度と特別委員 10 名程度（食品等の分野別）で構成される。

【情報提供委員会】

・ サービスや取引等に関する情報を提供する場合に開催される委員会。
・ 委員は 5 名（弁護士、学者、ジャーナリスト等）で構成されている。

(3) 行政手続法（平成 5 年 11 月 12 日法律第 88 号）

・ 行政手続法は、「処分、行政指導及び届出に関する手続並びに命令等を定める手続きに関し、共通する事項を定めることによって、行政運営における公正の確保と透明性（行政上の意思決定について、その内容及び過程が国民にとって明らかであること）の向上を図ること。上記目的の達成により国民の権利利益の保護に資すること」（第一条より抜粋）を目的とした法律で、以下の事項について定めている。

1) 営業の許可などの申請に対して許可する・しないという処分（申請に対する処分）についての手続
2) 許可を取り消したり一定期間の営業停止を命じたりする処分（不利益処分）についての手続
3)「行政指導」の手続
4)「届出」の手続
5)「命令等」を定める際の手続[3]

・ 不利益処分とは、「行政庁が，法令に基づき，特定の者を名あて人として，直接に，これに義務を課し，又はその権利を制限する処分」（行政手続法 2 条 4 号）と定義されている。脆弱性の公表は必ずしも製品開発者への不利益処分に相当するものではないが、不利益処分を巡る行政機関と事業者の関係は、調整不能案件の脆弱性の公表を巡る IPA・JPCERT/CC と製品開発者の関係に近いと見ることも可能である。そこで、表 2-1 に不利益処分に関する手続きの概要を示す。

・ つまり、行政機関は、不利益処分を下す上で、以下の手順を求められる。

- 処分基準の決定と提示
- 不利益処分の理由の提示
- 弁明の機会の付与
- 弁明の機会の付与の通知

[3]5)については「行政手続法の一部を改正する法律（平成 17 年法律第 73 号）による改正であり、平成１８年４月１日から施行されている。

表 2-1　不利益処分に関する手続きの概要

（処分の基準）
第十二条　行政庁は、処分基準を定め、かつ、これを公にしておくよう努めなければならない。
２　行政庁は、処分基準を定めるに当たっては、不利益処分の性質に照らしてできる限り具体的なものとしなければならない。

（不利益処分をしようとする場合の手続）
第十三条　行政庁は、不利益処分をしようとする場合には、次の各号の区分に従い、この章の定めるところにより、当該不利益処分の名あて人となるべき者について、当該各号に定める意見陳述のための手続を執らなければならない。
一　次のいずれかに該当するとき　聴聞
イ　許認可等を取り消す不利益処分をしようとするとき。
ロ　イに規定するもののほか、名あて人の資格又は地位を直接にはく奪する不利益処分をしようとするとき。
ハ　名あて人が法人である場合におけるその役員の解任を命ずる不利益処分、名あて人の業務に従事する者の解任を命ずる不利益処分又は名あて人の会員である者の除名を命ずる不利益処分をしようとするとき。
ニ　イからハまでに掲げる場合以外の場合であって行政庁が相当と認めるとき。
二　前号イからニまでのいずれにも該当しないとき　弁明の機会の付与

（不利益処分の理由の提示）
第十四条　行政庁は、不利益処分をする場合には、その名あて人に対し、同時に、当該不利益処分の理由を示さなければならない。ただし、当該理由を示さないで処分をすべき差し迫った必要がある場合は、この限りでない。
２　行政庁は、前項ただし書の場合においては、当該名あて人の所在が判明しなくなったときその他処分後において理由を示すことが困難な事情があるときを除き、処分後相当の期間内に、同項の理由を示さなければならない。
３　不利益処分を書面でするときは、前二項の理由は、書面により示さなければならない。

（弁明の機会の付与の方式）
第二十九条　弁明は、行政庁が口頭ですることを認めたときを除き、弁明を記載した書面（以下「弁明書」という。）を提出してするものとする。
２　弁明をするときは、証拠書類等を提出することができる。

（弁明の機会の付与の通知の方式）
第三十条　行政庁は、弁明書の提出期限（口頭による弁明の機会の付与を行う場合には、その日時）までに相当な期間をおいて、不利益処分の名あて人となるべき者に対し、次に掲げる事項を書面により通知しなければならない。
一　予定される不利益処分の内容及び根拠となる法令の条項
二　不利益処分の原因となる事実
三　弁明書の提出先及び提出期限（口頭による弁明の機会の付与を行う場合には、その旨並びに出頭すべき日時及び場所）
第三十一条　第十五条第三項*1 及び第十六条*2 の規定は、弁明の機会の付与について準用する。
*1）不利益処分の名あて人となるべき者の所在が判明しない場合の対応
*2）代理人の選定

（出典：行政手続法（平成 5 年 11 月 12 日法律第 88 号）より抜粋）

(4) 米国 消費者製品安全委員会（CPSC）

- 国内で販売される消費者用製品の安全性につき、製造業者、輸入業者、流通業者及び小売業者に対して指導監督権を有しており、消費者の安全性の確保に向けて正確、かつ包括的なデータに基づいて規制措置を迅速に取るため、多様な情報を収集する体制を整備している。
- 欠陥や危険製品に対して、年間約 300 件のリコールを行っている。

(5) 一般製品安全に関する EU 指令

- 本指令は、リコールを重視した方向で 2001 年に改正され、EU 各国がこれに従って順次法制度化を進めている。本指令の最初のバージョンは 10 年前に採決されたが、内容が十分ではなかったため、改正案が 2001 年に採択された。
- 本指令では、これまで行政庁へのリコール権限の付与、危険な製品の EU からの輸出禁止、安全情報の開示促進（特に製造業者の義務の強化）が示されている。
- 分野別又は製品別指令の対象とならない全ての消費者用製品に適用される。

(6) ドイツ 商品テスト財団（STIFTUNG WARENTEST）

- ここでは、ドイツにおける製品の評価を公表する制度的な取組みの事例として、ドイツの商品テスト誌「テスト」（test）と同誌を発行する商品テスト財団（STIFTUNG WARENTEST）について説明する。[4,5,6]
- 商品テスト財団は、60 年代初頭に発行されていた別の商品テスト誌が企業広告収入でテスト機関を運営していたために中立性を失い失敗したことを受けて、テスト機関の独立性、テスト実施者の中立性を念頭において設立が進められた。独立性を保障し経済的安定を確保するために行政機関ではなく財団法人という形式になっている。
- 財団の収入は、商品テスト誌等の出版物の売上に基づく。財団の定款で広告を禁止しており企業からの広告収入は一切ない。国家助成の割合は全収入の 1 割程度である。

---

[4] Stiftung Warentest　http://www.test.de/

[5] 岸 葉子、“商品テスト誌の日独比較と今後の課題”、季刊「公共研究」第 3 巻第 4 号、2007 年 3 月 http://mitizane.ll.chiba-u.jp/metadb/up/ReCPAcoe/34kishinote.pdf

[6] 三枝 一雄、“西ドイツにおける消費者組織”、法律論叢 56 巻 1-2 号、1983 年 9 月
https://m-repo.lib.meiji.ac.jp/dspace/bitstream/10291/3832/1/horitsuronso_56_1-2_67.pdf
https://m-repo.lib.meiji.ac.jp/dspace/bitstream/10291/3833/1/horitsuronso_56_4_41.pdf

- 財団は独自のテスト機関を持たず、公共団体や大学などに守秘義務を課した上でテストを委託している。この理由はコスト削減とノウハウ交換のためである。
- 「テスト」誌の国民への認知度は非常に高く、ドイツ国内で入手が容易な雑誌のひとつであり、市民が商品購入の際の参考にすることも多い。
- 「テスト」誌が示す評価は、現在は総合評価で 5 段階の評価であり、テストした事項の配点も割合で示している(例:機能 40%、耐用年数 20%、使用性 15%、技術 10%、環境配慮 15%)。
- テスト結果は実名で公表される。テスト結果は雑誌本誌に掲載する以外には、要約版を新聞や雑誌等のマスメディアに提供しており、これにより結果の普及を図っている。また、ウェブサイトでの情報提供、個々のテスト結果のパンフレット形式での配布、テスト年報の作成、展示会等の開催等も積極的に行っている。
- 「テスト」に示された結果はドイツにおける製品の売上に大きく響く。高評価は積極的に宣伝に用いられるが、低評価であれば製品が売り場から外されることもある。低評価の場合には企業から抗議の声や批判的談話が示されることもある。抗議や批判はテスト実施者と業界側との見解の相違が原因であることが多い。話し合いの場が持たれるが、評価に納得できないメーカにより訴訟に発展することも少なくない。

(7) 英国 消費者協会(Consumer's Association)

- 英国の製品評価結果を公表する公的性格の組織の事例として消費者協会(Consumer's Association)について調査を行なった。[7,8]
- 消費者協会の設立は 1957 年と古く、会員数は 104 万人と多い。法的権限が与えられており、団体訴訟やスーパーコンプレインツ[9] としての権限も持つ。
- 現在は、企業から独立性を確保した商品テストを実施し、その結果を載せ公表する雑誌「Which?」を販売するという事業モデルを確立し、多くの会員を獲得している。また、立法府や行政府に消費者保護の必要性を問いかけ、消費者問題に関するキャンペーンやロビイング活動の展開や、消費者相談活動を行っている。

---

[7] 消費者協会(Which?)　http://www.which.co.uk/

[8] 平成 20 年版 国民生活白書 第 2 節 2.消費者団体の役割
http://www5.cao.go.jp/seikatsu/whitepaper/h20/01_honpen/html/08sh020202.html

[9] 認定された消費者団体が直接公正取引委員会に対して苦情申し立てを行うことができる制度。この申し立ては放置されることなく、90 日以内に対応方針について回答されるよう定められている。

・ 資金については、収入のほぼ全てを会費と雑誌売上により得ている。発行雑誌には一切の宣伝広告を載せていない。政府や産業界から一切支援を受けない独立性の高い組織である。
・ 「Which?」ウェブサイトでも会員向けにレビュー結果を示すサービスを行っており、複数の製品を実名で挙げたレビューが示されている。

(8) 脆弱性情報を取扱う海外の組織の事例

① Core Security Technologies （米国）

・ 独自の調査研究の成果に基づく脆弱性情報を公表。
・ 製品開発者との調整を自ら行っている（調整機関を介在させていない）。
・ アドバイザリに含めている情報の量が多い。
  - 詳細な技術的記述、POC コード
  - 取扱いの経緯
・ タイムラインに沿って製品開発者との連絡の概要が示されている。
  同社から通知した事項、製品開発者が連絡してきた事項 等。
・ 日付を明確にし、対処にあたり双方の見解がどのようなものであったかを記録。

② Secunia （デンマーク）

・ 自社の脆弱性スキャン製品への反映と知名度向上のため、脆弱性の発見に注力する。
・ これまでの経験を踏まえた、独自の厳しい脆弱性情報公開ポリシーを持つ。

1) ベンダの脆弱性情報に関するコンタクト先が不明である場合には、公開されている代表メールアドレスに最初の連絡を送る。
2) 最初の連絡で、脆弱性の詳細情報と公開予定日（2 週間後の水曜日）を通知する。
3) ベンダが最初のメールに返答しなかった場合、1 週間後に再送する。
4) 公開予定日までに何の返答も無かった場合には、それ以上の調整は行わず脆弱性情報を直ちに公開する。
5) ベンダが最初の連絡あるいは再送した連絡に返答した場合、ベンダが合わせられないならば新たな公開予定日を設定することがある。
6) ベンダからの状況報告は月 1 回、定期的に受信することを期待する。
7) 状況報告の要求に返答がなければ 1 週間後に再要求する。
8) 状況報告をベンダに求めるメール 2 回に対して返答が無い場合、1 週間後に脆弱性情報が公開される旨を伝えるメールがベンダに送られる。こ

れに返答が無かった場合には、それ以上の調整を行わず脆弱性情報を直ちに公開する。

9) 最終的には脆弱性情報は次の条件で公開される。a)公開予定日が来た場合、b)ベンダが修正またはアドバイザリを公開した場合、c)当該脆弱性について第三者が情報を公表した場合、d)最初の連絡から 1 年が経過した場合

10)1 年以上は調整を行わない。最初の連絡から 9 ヶ月が経ったら、固定の公開日が通知される。この公開に際しては修正パッチの準備状況は一切問わない。

③ Tipping Point Zero Day Initiative （米国）

・ 2005 年８月より活動。ゼロデイ脆弱性について研究者に報酬を与え、影響を受けるベンダに責任ある報告を行わせることと、修正パッチが完成するまでの間に同社の顧客に適切な対策手段を提供することを狙っている。

・ 次のような公開ポリシーを示している。

- 最初の連絡はベンダのウェブサイトあるいはセキュリティコンタクトのメールアドレスに対して行う。通知と同時に脆弱性に対する防御手段を同社の顧客の IPS 装置に適用する。
- 最初の連絡から 5 日間返答が無かった場合､2 度目の連絡を電話で行う。さらに 5 日間返答が返って来なかった場合、仲介人を通して連絡を試みる。あらゆる手段を尽くして連絡を試みて返答が得られなかった場合、最初の連絡から 15 日後に脆弱性情報を公開する。
- 連絡が取れた場合、妥当な期間で修正プログラムを作成するか、効果的な回避策を作成するようにベンダを支援する。
- いかなる場合でも、ベンダが黙秘したいという理由から脆弱性情報について伏せることはしない。
- 公開に先立ち、信頼がおけるセキュリティベンダとは脆弱性情報の詳細について情報共有を行う。

2.2. 製品開発者が公表に同意していない脆弱性関連情報の開示に係わる事例

調整不能案件の公表に関連する事例として、製品開発者が公表に同意していない脆弱性関連情報の開示に係わる事例について文献調査を行った。

(1) Sage および Sage++における脆弱性（2006 年 12 月）

- Sage 1.3.6 から派生したバージョンである Sage++（以下では Sage++と記す）の製品開発者との調整においてトラブルが生じた。
- 2006 年後半から Sage++の製品開発者は本家 Sage の製品開発者と連絡を取り合い、脆弱性の発見・修正を繰り返していた。
- この製品開発者に JPCERT/CC から Sage および Sage++において任意のスクリプトが実行される脆弱性について連絡が 2006 年 12 月 14 日に行われた。Sage++の製品開発者は製品開発者登録のために個人情報を IPA に対して伝えることに抵抗感を感じ、製品開発者登録を断った。このため詳細な脆弱性情報は Sage++の製品開発者に送られなかった。
- その後、Sage++の製品開発者は、類似の他製品に関する脆弱性情報が JVN から公開されたことを受けて、2007 年 1 月 18 日に、IPA、JPCERT/CC による一般への公表の前に、Sage および Sage++に脆弱性が存在することと回避策を配布サイトで公表した。1 月 25 日に Sage++の製品開発者はサイトで Sage++の開発終了と利用中止の推奨をアナウンスした。
- この後、2007 年 1 月 29 日に Bugzilla から Sage に関する脆弱性情報が公開された。その後 JVN にて 2007 年 2 月 9 日に Sage および Sage++に関する脆弱性情報が公開された。
- Sage++の製品開発者は 2 月 9 日に脆弱性情報を確認した上で、Sage++について脆弱性を自己検証し、2007 年 7 月に脆弱性対策を行った新たなバージョンの Sage++を公開し開発を再開した。この新バージョンの Sage++に関しては JVN の情報は更新されておらず言及もされていない。依然、本家 Sage 1.3.x 系列についてはこの脆弱性の修正は行われていない模様である。

→ 発見者・製品開発者の中には「ある製品に未修正の脆弱性が存在すること」（脆弱性の存在）の公表に慎重になる必要を認識していない場合がある。

〈参考〉

1) https://www.mozdev.org/bugs/show_bug.cgi?id=16320

2) http://jvn.jp/jp/JVN84430861/index.html

(2) Sageにおける脆弱性（2007年4月）

- 2007 年 4 月 3 日に派生プログラム Sage++の製品開発者である発見者よりIPA に Sage の脆弱性が届出られる。
- 2007 年 5 月 21 日に発見者から IPA に取扱い状況について問合せ。6 月 11日 IPA より回答。公表目処が立たない旨を通知した。その後のやりとりで、この脆弱性を修正した Sage++の公開は OK だが Sage に脆弱性があること、Sage++が脆弱性修正をしたものであることを公開しないように IPA から発見者には依頼。2007 年 7 月 1 日に、修正を行った Sage++を発見者が公開。未公開の脆弱性については言及せず 「セキュリティ強化」と記載したに留めた。
- 2008年1月27日発見者より未公開の脆弱性について依然として調整不能となっていることが公開された。

→ 調整不能案件の取扱いを進める際には、発見者の守秘に関するお願いを取り消すスキームとの整合性を取る必要がある

〈参考〉

1) http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-6919

2) http://secunia.com/advisories/22809

(3) Windows Media Playerの脆弱性（2009年1月）

- 2009年1月にWindows Media Playerの脆弱性によりリモートのユーザにより「任意のコードの実行が可能」と発見者が公表した。Microsoft 社は検証を行い、セキュリティ対策部門のブログで検証結果として「任意のコード実行は可能ではない」旨を表明した。これを受けて発見者は公開する脆弱性情報を修正し、リモートのユーザにより「プレイヤーをクラッシュ」させて「サービス妨害攻撃が可能」と表現を改めた。

→ 公表後に製品開発者より検証結果や反論がブログ等で公開されることがありうる。これらが公表された後にリンクする等の必要も生じうる。

〈参考〉

1) http://www.itmedia.co.jp/news/articles/0812/29/news006.html

2) http://isc.sans.org/diary.html?storyid=5563
3) http://www.securitytracker.com/id/1021495
4) http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5745
5)http://blogs.technet.com/b/msrc/archive/2008/12/29/questions-about-vulnerability-claim-in-windows-media-player.aspx
6)http://blogs.technet.com/swi/archive/2008/12/29/windows-media-player-crash-not-exploitable-for-code-execution.aspx

(4) MS10-002 IE の脆弱性とゼロデイ攻撃（2010 年 1 月）

- Google の中国サイトに対して Internet Explorer の未公表の脆弱性に関するゼロデイ攻撃が行われたのを受け、Microsoft 社は定例外の修正プログラムを公開し、セキュリティ対策部門の公式ブログ上で適用範囲について説明を行った。

→ 届出受付／調整機関が脆弱性情報を公開せずに抱えていた場合には、それがゼロデイ脆弱性として公開された際に被害者から訴えられるリスクとなりうる

〈参考〉
1) http://japan.internet.com/webtech/20100122/11.html
2)http://blogs.technet.com/b/msrc/archive/2010/01/20/advance-notification-for-out-of-band-bulletin-release.aspx
3) http://www.microsoft.com/japan/technet/security/bulletin/ms10-002.mspx
4) http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0027
5) http://japan.zdnet.com/security/sp_07zeroday/20406781/
6) http://jvn.jp/tr/JVNTR-2010-04/index.html

(5) Windows 7 の Virtual PC の脆弱性(2010 年 3 月)

- Core Security 社は「Microsoft の仮想化ソフト「Virtual PC」に未修正の脆弱性があり、この問題を突かれると Windows に実装されている DEP や ASLR といったセキュリティ機能がかわされ、Virtual PC のゲスト OS 上でアプリケーションのバグを悪用される恐れがある」と公表した。公表の 1 ヶ月前に Core Security 社はこの問題に関し以下の 4 点について Microsoft 社に確認を求めていたが明確な回答は得られなかったとしている。(1).この件がセキュリティ修正とセキュリティ報告で解決されるべきセキュリティ問題であることについてのベンダの同意。(2).影響を受けるプラットフォー

ムの完全なリスト。(3).この問題の原因に関する明確かつ技術的な記述。(4).修正をリリースする期日に関する合理的な計画。これに対し、Microsoft 社は「これは Windows 7 のセキュリティに直接かかわるものではない。同社が取り上げている「機能性」は脆弱性ではなく、「システム上に既にあった脆弱性を、攻撃者がより簡単に悪用する方法を記述したにすぎない」と同社のブログで反論した。

→　製品開発者と見解が相違した場合には、製品開発者は公表前に見解を示さず、公表後に反論を行う可能性がある。

〈参考〉
1) http://www.itmedia.co.jp/enterprise/articles/1003/17/news020.html
2)http://www.coresecurity.com/content/Vulnerability-in-Key-Microsoft-Virtualization-Technology
3)http://www.coresecurity.com/content/virtual-pc-2007-hypervisor-memory-protection-bug
4)http://windowsteamblog.com/windows/b/windowssecurity/archive/2010/03/16/vulnerability-in-virtual-pc.aspx
5) http://www.itmedia.co.jp/enterprise/articles/1003/18/news019.html

(6) Adobe Reader および Acrobat における脆弱性（2010 年 3 月）

- 3 月 29 日にベルギーのセキュリティ研究者が脆弱性の存在と検証コードを公開した（この時点で Adobe には連絡済であった)。4 月 6 日に Adobe 社はブログにこの問題を確認した旨を掲載し回避策を示した。4 月には脆弱性を悪用したメール攻撃が IBM により報告された。これはマルウェア作成ツール Zeus/Zbot により作成されたものであった。6 月 29 日に Adobe 社よりセキュリティ更新プログラムが公開されたが、対策を迂回可能であったため、さらに 8 月 19 日に新たな更新プログラムが公開しなおされた。

→　脆弱性の詳細が公開され対策の提供が遅れると実被害が生じうる。

〈参考〉
1) http://jvn.jp/tr/JVNTR-2010-21/index.html
2) http://blog.didierstevens.com/2010/03/29/escape-from-pdf/
3) http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1240
4)http://blogs.adobe.com/adobereader/2010/04/didier_stevens_launch_function.html

5) https://www-950.ibm.com/blogs/tokyo-soc/entry/pdflaunch_20100428

6)http://www-935.ibm.com/services/jp/index.wss/press_release/secpriv/h616111f77274g58

7) http://www.adobe.com/jp/support/security/bulletins/apsb10-15.html

8) http://blog.bkis.com/en/adobe-fix-still-allows-escape-from-pdf/

9) http://www.adobe.com/jp/support/security/bulletins/apsb10-17.html

(7) Safari ブラウザのゼロデイ脆弱性（2010 年 5 月）

- Safari における window オブジェクトの不適切な処理に起因する未公表の脆弱性を悪用する攻撃コードがポーランドのセキュリティ研究者により公開され、US-CERT より脆弱性情報が公表された。脆弱性情報の公表後に Apple 社から修正が施された最新版が出された。

→ ゼロデイ攻撃の可能性が実際に高まった場合に当該脆弱性情報の公表をパッチ提供に先行させる判断もありうる。

<参考>

1) http://secunia.com/advisories/39670/

2) http://www.kb.cert.org/vuls/id/943165

3)http://www.computerworld.com/s/article/9176502/Researcher_reveals_Safari_zero_day_bug

4) http://www.itmedia.co.jp/enterprise/articles/1005/10/news024.html

5) http://internet.watch.impress.co.jp/docs/news/20100513_366696.html

6) http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1939

7) http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1750

8) http://jvn.jp/cert/JVNVU943165/

9) http://reviews.cnet.com/8301-13727_7-20004709-263.html

10) http://lists.apple.com/archives/security-announce/2010/Jun/msg00000.html

11) http://support.apple.com/kb/HT4196

(8) Windows のヘルプとサポートセンターの脆弱性（2010 年 6 月）

- Google に所属するセキュリティ研究者が Windows ヘルプに未修正の脆弱性を発見して Microsoft 社に 6 月 5 日に通知し、9 日には情報を一般に公表した。Microsoft 社は 10 日にアドバイザリを公表し注意喚起を行うとともに、同社の発表前に情報を公表した研究者に対して、問題解決の時間を与えずに公表する姿勢を強く批判した。また、研究者が回避策として示した方法

が不完全であることも指摘した。さらに、Google 社の業務とは無関係に公表したとする研究者の主張についても個人的行為とは考えない旨を述べた。この脆弱性の修正プログラムは 2010 年 7 月に公表された。

→　製品開発者側に問題解決に十分な時間を与えなかったとして非難される可能性がある。また、独自に示す回避策について製品開発者等から不備を指摘される可能性がある。

〈参考〉
1) http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1885
2) http://archives.neohapsis.com/archives/fulldisclosure/2010-06/0197.html
3)http://blogs.technet.com/b/msrc/archive/2010/06/10/windows-help-vulnerability-disclosure.aspx
4) http://www.microsoft.com/technet/security/advisory/2219475.mspx
5) http://www.itmedia.co.jp/enterprise/articles/1006/11/news019.html
6) http://jvn.jp/tr/JVNTR-2010-19/index.html

(9) QuickTime の脆弱性（2010 年 9 月）

- スペインのセキュリティ研究者により QuickTime に未解決の脆弱性が発見された。脆弱性は QuickTime の ActiveX コントロールの問題に起因し、攻撃者が任意のコードを実行できる恐れがあるものであった。脆弱性は Tipping Point 社の Zeroday Initiative を通じて 6 月 30 日に Apple に報告された。調整された公開日である 8 月 31 日に研究者によりエクスプロイトコードとともに公開された。Secunia 社他も 8 月 31 日以後に脆弱性情報を確認し公開した。Apple 社は 9 月 15 日に修正が施されたバージョンを公開した。このタイミングでの公表に製品開発者が最終的に同意していたかは不明である。

→　調整の経緯や公表ポリシーを示すことで公表の妥当性が確認できる。

〈参考〉
1) http://www.itmedia.co.jp/enterprise/articles/1009/01/news025.html
2) http://secunia.com/advisories/41213/
3)http://threatpost.com/en_us/blogs/new-remote-flaw-apple-quicktime-bypasses-aslr-and-dep-083010
4) http://reversemode.com/index.php?option=com_content&task=view&id=69&Itemid=1

5) http://jvn.jp/tr/JVNTR-2010-26/index.html

6) http://support.apple.com/kb/HT4339?viewlocale=ja_JP

7) http://zerodayinitiative.com/advisories/ZDI-10-168/

(10) Mac OS X の脆弱性（2010 年 11 月）

- Core Security 社は、Apple Type Service のメモリ破損問題に起因し、悪質な Compact Font Format（CFF）フォントを組み込んだ PDF 文書を Mac OS X 10.5 で閲覧したり、ダウンロードしたりすると、リモートの攻撃者が任意のコードを実行できてしまう恐れがある脆弱性が Mac OS X にも存在することを発見し、8 月に Apple に通報。Apple でも問題を確認し、この脆弱性を解決するパッチの公開予定日も両社の間で決めていたが、予定日になっても Apple からパッチが公開されず、それ以上の説明もなかったため、同社は情報の公開に踏み切った。

→　詳細な調整の経緯について公表することで公表の妥当性を示すことができる。

〈参考〉

1) http://www.itmedia.co.jp/enterprise/articles/1011/10/news052.html

2)http://www.coresecurity.com/content/Apple-OSX-ATSServer-CharStrings-Sign-Mismatch

2.3. まとめ

(1) 公表のプロセス

調整不能案件の公表プロセスの参考となる既存の社会制度等の事例から、以下の点が明らかになった。

- 事業者が不利益を被りうる調整不能案件の脆弱性情報の公表については、直接的な法的根拠がない場合でも、公益性に鑑み、設置法に準じた内規や行政手続法に準じた制度に則って取り組むことが妥当と考えられる。
- 公表のプロセスにおいては、事業者側に弁明の機会を付与すること、また公表時にも事業者側が意見を提示した場合には両論併記での公表を行うことで、公平性を担保することができる。特に、NITE や国民生活センターの事例では、両論併記の公表の仕組みを適用しており、公表後に異議申立てを受け付けるような仕組みは設けていない。
- 海外では、法的な根拠等によらず、自らの基準・ルールに則り、事業者と合意がとれていない脆弱性を公表する事例が見られた。その際、調整の経緯を詳細に明示することで、自らの取り組みの妥当性を主張するケースもある。
- そのほか海外で製品テスト結果の公表に携わる機関においては、組織の中立性を確保し公正なテストの実施に強く配慮している事例が見られた。

(2) 製品開発者が公表に同意していない開示事例

また、製品開発者が公表に同意していない脆弱性関連情報の開示に係わる事例として、以下のケースが確認された。

- 製品開発者と見解が相違した際に、脆弱性情報を公表した後に製品開発者から検証結果や反論がブログ等で公開された。
- ゼロデイ攻撃が先行し、未公表であった脆弱性が修正パッチなしで公開された。
- 発見者・製品開発者が「ある製品に未修正の脆弱性が存在すること」（脆弱性の存在）の公表に慎重になる必要を認識しておらず公表してしまった。
- 独自に公表した際に製品開発者側に問題解決に十分な時間を与えなかったとして非難された。
- 独自に示した回避策について製品開発者等から不備を指摘された。
- 長期間にわたり調整が続いたため、守秘のお願いにかかわらず、脆弱性について公表した。

(3) 課題およびその対応

上記を踏まえ、以下の課題が挙げられる。

- 脆弱性情報を公開せずに案件として抱えていた場合に被害者から訴えられるリスクがある。
- ゼロデイ攻撃が実際に行われた場合に当該脆弱性情報の公表をパッチ提供に先行させる判断もありうる。
- 調整の経緯や公表ポリシーを示すことで公表の妥当性を示すことが重要である。
- 独自の回避策を提示する場合には検証を数回繰り返す必要も生じうる。
- 調整不能案件の取扱いを進める際には、発見者の守秘に関するお願いを取り消すスキームとの整合性を取る必要がある。
- 脆弱性情報の公表に際して現場が活動しやすい環境を整えるためには、開発者等から訴訟を起こされる可能性を踏まえ、たとえば、開発者からのクレームが訴訟へとエスカレーションした際に対応にあたる担当者を組織内に設置しておくことが望ましい。

3. 調整不能案件の公表に関する製品開発者の意識調査

調整不能案件の公表に関するソフトウエア製品開発者の意識について、ヒアリング調査を行った。

具体的には、ソフトウエア製品開発者を規模（大手/中堅/中小（OSS 開発者を含む））や地域（国内/外資）で分類し、それぞれのカテゴリの代表的企業・組織を調査対象の候補として抽出した。ただし、数が多く、個社ベースの調査だけでは総括的分析が難しい中小事業者（OSS 開発者を含む）については、多数の中小事業者と取引のあるソフトウエア流通サイトや OSS の関連団体を調査対象に加えた。

調査にあたっては次のような仮説を設定し、ヒアリングを通じて検証することとした。

表 3-1　製品開発者の意識調査の仮説

カテゴリ*	仮説
大手事業者	(A1) 大手事業者の場合、連絡が取れなくなって調整不能に陥る可能性は低い。 (A2) ただし、再現性の問題や見解の相違から議論が停滞し、調整が難航した場合など、第三者の客観的な審査が必要となる可能性はある。 (A3) 調整が難航しただけで大手としての対応の適切性が問われるリスクがある。
中堅事業者	(B1) 中堅事業者も、通常は、連絡が取れなくなって調整不能に陥る可能性は低い。ただし、対象製品からの急な撤退や担当者の離職等により、応答が停滞することもありうる。 (B2) また、再現性の問題や見解の相違から議論が停滞し、調整が難航した場合など、第三者の客観的な審査が必要となる可能性はある。
中小事業者 *（OSS 開発者を含む）	(C1) 小規模の事業者や個人、ボランティア集団等の場合、脆弱性問題への関心が薄かったり、マンパワーの制約から対応が困難になったりして、連絡不能に陥る可能性がある。 (C2) 人気のある無料ソフトが脆弱性の問題でメンテナンスを放置され、ユーザが取り残された形になる。
外資系事業者	(D1) 外資系の場合、日本窓口を介した開発拠点とのやりとりで時間を要したり、言葉の壁で苦戦した結果、調整不能に陥る可能性はある。 (D2) 調整が難航した場合に、第三者の審査の意図が十分に本社に伝わらず、さらに問題がこじれる可能性もある。

*) 国内のソフトウエア製品開発者は全般的に規模が小さく、大半が一般的な中小企業の範疇（300 人以下）に含まれてしまうことから、本項ではこうした区分は適用せず、いわゆる零細や個人を「中小」と位置付け、それ以上を中堅・大手に区分した。

3.1. 方針・スタンスについて

(1) 全体的な方向性

- ユーザの利益が守れるなら、訴訟問題になってでも公表すべき。一方、公表しても誰の得にもならないなら、判定委員会で止めるべき。ただし、発見者のプライドは損ねることになる。(中小事業者)
- 消費者・利用者の不利益とベンダの不利益を鑑みて公表を判断すべき。(外資系事業者)
- 本来は、とるべき対処をとらない製品開発者にプレッシャーをかける仕組みであり、予算の制約がある以上、重要なものを適切に公表すべきであって、すべての案件を公表する必要はない。どうでもいいものまで対応を迫られるようだと、業界側は困るだろう。(中小事業者)
- 本制度の概要と、脆弱性を告知することの被害防止への意義、修正をあきらめることまでを含めて対応に様々な手段があることを製品開発者に説明できれば、調整に入りやすいのではないか。(ソフトウエア流通サイト)
- インパクトが大きい脆弱性については基本的には公表すべきである。例えば通信キャリアが利用しているソフトウエアに関する脆弱性は社会的にもインパクトが大きい可能性がある。キャリアの末端で利用しているソフトウエアについては確認が難しい場合もある。情報共有の仕組みを考慮していただきたい。(外資系事業者)
- 制度の方向性は合理的と考える。規定については例外となる場合を例示すると裏をかこうとする者が出てくるだろうから例示せず、適切な判例を積み重ねる方が良いだろう。(中堅事業者)

(2) 海外との調整

- 調整不能案件の公表についても、海外 CSIRT に連絡を取るなど、グローバルな対応を求めたい(外資系事業者)
- 調整不能案件の公表に際して海外のユーザに対するケアがなされるか心配である。海外 CSIRT 等の組織を通じて日本での公表について連絡が回るようにして欲しい。(外資系事業者)

(3) 制度の詳細

- 開発ベンダ側も調整不能となった場合に文書が届きうることを踏まえて組織内の体制を整えておく必要がある。製品開発者のどの部署に宛てて文書を送付したかについては明確にしておくべきである。(大手事業者)

・ 調整不能の取扱いとなった場合には、発見者にも状況を伝え、判定委員会において意見を言う機会を与えると良いのではないか。(大手事業者)
・ IPA・JPCERT/CC で脆弱性を検証できないソフトウエア、高額で入手困難なソフトウエアもある。大手企業等に協力を要請して検証用の機材、環境の提供を求めてみてはどうだろうか。今後、家電、制御系、組込み系等の脆弱性が報告されることを考えると検証環境作りを国が主導してもよいのではないか。(大手事業者)

3.2. 運用上の課題について

(1) 脆弱性の定義に係る課題
・ ソフトウエア製品の定義は議論の対象となりうる。例えばサンプル・プログラムに脆弱性がある場合も予想される。サンプルの問題箇所はベンダが作った部分にあるのか後からそれを利用して作成した部分にあるのかが分かり難い。ベンダによってはサンプルを製品の一部と認めていない場合もある。サンプルは分かりやすさ重視で作られているため完璧な品質を求めることが難しい。(大手事業者)
・ 連絡窓口を整備しているベンダが連絡不能という状況に陥ることはまずないだろうが、仕様か脆弱性かで意見が分かれるリスクはある。多くの事案は調整で解決可能な範囲に収まると考える。(中堅事業者)
・ サービス妨害攻撃のように理論的には脆弱性にカテゴライズされるが防御手段がリソース強化以外に無いものもある。そのような場合は脆弱性かどうかで議論となる可能性があるだろう。(大手事業者)
・ 製品開発者が脆弱性と認めがたい場合には、脆弱性の公表により印象を損ねて風評被害が起きる可能性を気にするだろう。そのような場合は両論併記をしても言い訳のように見えるので、ベンダは両論併記での意見表明を避ける可能性があるだろう。(大手事業者)

(2) 製品開発者との合意形成に関する課題
・ ベンダとしては製品を ASP やクラウドでサービス提供するために利用している顧客に手当てを済ませてから公表したいが、その場合には情報公開までの具体的期限を切り難く、円滑に調整が進むかがやや懸念される。(中堅事業者)
・ 他社の製品に固有の仕様に基づいた対策を提示されても、知財の関係上、自社の対策としては受け入れがたい場合がある。対策が提示できないトラブルになる可能性がある。(大手事業者)

・ 脆弱性公表が元となりインターネット上でネガティブな話題が広がると評判の低下が懸念される。企業としては熟慮の上で株主へのアピールのため訴訟を起こす可能性もある。IPA・JPCERT/CC には訴訟リスクとなり得る。（中堅事業者）

(2) 公表後の対応に関する課題
・ 公表できないケースは、影響が大き過ぎる、事実上対応が不可能、といった場合等もありうる。（中小事業者）
・ その部品がどこで使われているかわからないため、公表しても現実的には対応できないケースもありうる。（外資系事業者）
・ 売名目的で訴える事業者が出てくる可能性はある。（外資系事業者）

(3) その他の課題
・ 製品開発者が倒産した場合については、通常は顧客に迷惑がかかるためその製品の販売を停止する。（中堅事業者）
・ 調整不能となる前の段階に製品開発者への連絡に関してソフトウエア流通事業者が協力することも検討可能である。どのような協力ができるかは別途取り決めたい。この実現には製品開発者に対しての本制度の仕組みや IPA へのコンタクト方法等についての事前の啓蒙も必要である。（ソフトウエア流通サイト）
・ この制度への対応方法について相談する先が無い。どこかに相談する先があると良い。（大手事業者）

3.3. 海外の製品開発者について

・ 海外の製品開発者の場合、日本に支社・支店があるのか、単なる営業所なのかで対応が異なる。（外資系事業者）
・ 中小企業は、自社でソフトウエア開発をしていない場合の対応が難しい。特にローカライズの場合、コードの脆弱性がある機能的な部分には手を加えられない。パブリッシャーが顧客と海外の開発元との間で板ばさみになる。（ソフトウエア流通サイト）
・ 脆弱性が再現できた場合には放置せず修正を試みている。社外で開発している場合、特に海外の開発会社の場合には調整等に長い時間がかかる。制度が確立し目安の時間が示されれば事情は変わりうるだろう。（中堅事業者）

3.4. OEM 製品の脆弱性について

- OEM製品の脆弱性については手直しして用いている側では確認できない場合がある。問題の解決を 1 社だけでは求められない場合もある。（大手事業者）
- OEM 先に修正してもらう際に時間がかかりこじれる可能性はある。対応が悪ければ他社に切り替えることも考慮する。（中堅事業者）

3.5. 中小・個人の製品開発者について

- ソースコードを隠しオブジェクトだけダウンロードさせる人達は多くいるが、連絡もつかず、よくわからない抗議をしてくるかもしれない。連絡を求めている人は連絡先を明記してある。最初から求めていない人達は連絡先を載せていないので、連絡をしない方がコスト的に安く済む。（中小事業者）
- 会社と個人では対応を使い分けるべき。善意で取り組む個人の芽を摘むべきではない。ネガティブにさせない。メンテナンスが無理なら、オープンソースにすることを勧めてもよい。（外資系事業者）
- 配布・販売を行なうソフトウエア流通サイトとしては、IPA からの脆弱性情報を確認したら、よくダウンロードされる製品は脆弱性の深刻さをもとに公開停止が必要かを判断している。公開停止は独自の判断であり、これは製品開発者との規約にもある対応である。その後製品開発者に連絡し、対策された製品が準備されたら公開対象を切り替える。公開停止に至らない場合には注意喚起として使用中止と他のソフトウエアへの乗り換えを勧めることもある。（ソフトウエア流通サイト）
- 調整不能時に強制的に公表されるのは、個人や小規模な製品開発者には厳しい制度ではないか。公表を止めていたつもりでいて突然公表されて経営者等が怒るケースも想定できはしないか。（大手事業者）
- 開発ベンダとしては使っている OSS に脆弱性があって対応が遅れている場合に、他に手段がなければ自らパッチを作成することもありうる。（中堅事業者）
- 脆弱性の公表により個人の開発や OSS の開発が中断される可能性が懸念される。国内で開発される製品にも使っているものもある。重要なビジネスの部品となっている場合もあるので影響が生じうる。（大手事業者）

3.6. まとめ

(1) 仮説の検証

ヒアリングより得られたコメントを基にした仮説の検証を以下に示す。

大手事業者 (A1) 大手事業者の場合、連絡が取れなくなって調整不能に陥る可能性は低い。 (A2) ただし、再現性の問題や見解の相違から議論が停滞し、調整が難航した場合など、第三者の客観的な審査が必要となる可能性はある。 (A3) 調整が難航しただけで大手としての対応の適切性が問われるリスクがある。

大手事業者、特に脆弱性情報の取扱いに関する窓口を既に設けている企業においては、連絡が途絶えて調整不能に陥る可能性は殆ど無いだろうとの見解が示された。ただし、企業内でも特定の担当者が案件を抱え込んでしまい、退職や異動により連絡が取れなくなることや、全社的な対応体制との齟齬が生じうるとの指摘もあった。

製品の性能・仕様に係る部分で脆弱性であるかに関して見解が相違する場合については調整が難航する可能性があるとのコメントが得られた。

また、脆弱性と製品開発者である大手企業が認めない場合に情報が公表された場合の風評リスクを警戒する意見もあった。

中堅事業者 (B1) 中堅事業者も、通常は、連絡が取れなくなって調整不能に陥る可能性は低い。ただし、対象製品からの急な撤退や担当者の離職等により、応答が停滞することもありうる。 (B2) また、再現性の問題や見解の相違から議論が停滞し、調整が難航した場合など、第三者の客観的な審査が必要となる可能性はある。

中堅事業者についても、脆弱性情報の取扱いに関する窓口を設置済みの企業においては、連絡が途絶えて調整不能に陥る可能性は少ないとのコメントが得られた。

脆弱性公表に伴いネット上でネガティブな話題が広がることが懸念される。株主へのアピールを目的として、製品開発者側が訴訟を起こす可能性があり、IPA・JPCERT/CC にとってのリスクであるとの指摘もあった。

中小事業者（OSS 開発者を含む） (C1) 小規模の事業者や個人、ボランティア集団等の場合、脆弱性問題への

関心が薄かったり、マンパワーの制約から対応が困難になったりして、連絡不能に陥る可能性がある。
(C2) 人気のある無料ソフトが脆弱性の問題でメンテナンスを放置され、ユーザが取り残された形になる。

聴取先からは、中小・OSS の製品開発者においては脆弱性を公表すること自体が負担であり、開発のモチベーションを下げうるとの指摘があった。

中小・OSS が開発したソフトウエア製品の脆弱性が調整不能となり公表された場合に、自社製品にその製品を利用する大手・中堅の製品開発者は大きな影響を受けうる。

また、公表により中小・OSS の製品開発者が開発を中断・終了する可能性については懸念が示された。

外資系
(D1) 外資系の場合、日本窓口を介した開発拠点とのやりとりで時間を要したり、言葉の壁で苦戦した結果、調整不能に陥る可能性はある。
(D2) 調整が難航した場合に、第三者の審査の意図が十分に本社に伝わらず、さらに問題がこじれる可能性もある。

外資系事業者からは、調整不能になった場合の公表についてもグローバルな連携のもとで行うよう要望があった。

また、海外で開発された製品を国内で販売している場合、販売元である国内企業が自社で開発を行っていないため、脆弱性への対応が難しいだろうとの指摘があった。

(2) その他の意見

脆弱性公表により生じうる課題について次のような意見があった。

1) 調整不能案件の公表に際しては、企業と個人開発者とでは IPA・JPCERT/CC による対応を変える必要がある。個人開発者や OSS 開発者のモチベーションが低下しないよう配慮が望まれる。
2) ソフトウエアを直接開発していない企業の評判が低下する可能性がある（例えば、海外製品をローカライズしている場合、開発元が海外企業である場合など）。
3) 脆弱性が公表されたとしても自社が供給する部品的なソフトウエア製品がどのように利用されているか分からず、脆弱性修正の対応が困難である可能性がある。

またヒアリングを通じて次のような提案が得られた。

- 小規模開発者に連絡を取る段階でソフトウエア流通サイト等を運営する事業者に協力を求め、より確実な製品開発者へのリーチ手段を確保してはどうか。
- 高額・稀少で検証困難なソフトウエアについては、脆弱性検証環境の整備を大手企業と国の協力のもとで進めるべきである。
- 社会的影響の大きな脆弱性情報は基本的に公表すべきであるが、公表に先立つ情報共有等を考慮すべきである。

4. 調査を通じて明らかになった考慮点

4.1. 公表プロセスの製品開発者企業等への影響について

製品開発者等へのヒアリングにおいて、公表実施に伴うリスクについて次のような意見が得られた。IPA・JPCERT/CC において調整不能案件の公表を行う場合には、これらのリスクにも配慮することが望まれる。

(1) 個人開発者や OSS 開発者のモチベーション低下の可能性について

半ば強制的にソフトウエア製品の脆弱性公表する制度に変わることによって、ソフトウエア製品を開発する個人開発者や OSS 開発者への過度な負担を要求する恐れがあり、彼らのモチベーションを下げる可能性がある。これらの製品がビジネス上重要な位置を占める製品である場合もあり産業面での影響も懸念される。

(2) ソフトウエアを直接開発しない企業の評判が低下する可能性について

自社でソフトウエア開発をしていない企業が公表により評判低下等のデメリットを被る可能性がある(特に海外製品をローカライズしている場合、開発元が海外企業である場合など)。

(3) 部品供給している会社による対応が困難である可能性

脆弱性が公表されたとしても自社が供給する部品的なソフトウエア製品がどのように利用されているか分からず、脆弱性修正の対応が困難である可能性がある。

4.2. パートナーシップの課題について

製品開発者等へのヒアリングにおいて、次のような、パートナーシップにおける課題、およびパートナーシップの拡充・強化に関する意見が得られた。

(1) 小規模開発者との円滑な調整に向けた方策について

本調査の製品開発者等へのヒアリングを通じて、製品開発者に連絡を取る段階で、ソフトウエア流通サイト等を運営する事業者に協力を求め、より確実な製品開発者へのリーチ手段を確保すべきとのコメントを得た。特

に個人や小規模の製品開発者と JPCERT/CC が直接対話する場合、事情に明るくない製品開発者側が萎縮することも考えられる。

ソフトウエア流通事業者を通じて、本制度の分かりやすい説明と JPCERT/CC からの要望を伝えることができれば、より円滑な調整の進展も期待できるため、この方向でのコンタクト手法の積極的な推進は検討に値する。

(2) 高額・稀少で検証困難なソフトウエアの検証環境の整備について

IPA・JPCERT/CC で脆弱性を検証できないソフトウエア、高額で入手困難なソフトウエアについては、大手企業等に協力を要請して検証用の機材、環境の提供を求めてはどうか、という意見が得られた。今後、家電、制御系、組込み系等の脆弱性が報告されることを考えると検証環境作りについて国が主導することを考慮すべきとのコメントも得られた。

(3) 社会的影響の大きな脆弱性情報の公表について

公表により社会的混乱を招くことが予想される脆弱性についても、インパクトが大きい脆弱性については基本的には公表すべきとのコメントが得られた。例えば通信キャリアが利用しているソフトウエアに関する脆弱性は社会的にもインパクトが大きい可能性があるが、キャリアの末端で利用しているソフトウエアについては確認が難しい場合もある。事前調整、公表に先立つ情報共有の仕組みへの考慮が求められる。

(4) 公表を推進するための活動体制の整備について

脆弱性情報の公表に際して現場が活動しやすい環境を整えるためには、開発者等から訴訟を起こされる可能性を踏まえ、たとえば、開発者からのクレームが訴訟へとエスカレーションした際に対応にあたる担当者を組織内に設置しておくことが望ましい。

（参考）　脆弱性情報に係る調整手続検討ワーキンググループ

(1)参加者名簿（2011 年 8 月末現在）

主査	高橋 郁夫	株式会社 IT リサーチ・アート
委員	安藤 広人	英知法律事務所
	北島 周作	成蹊大学
	鈴木 裕信	NPO フリーソフトウエアイニシアティブ
	高木 浩光	独立行政法人産業技術総合研究所
	高橋 正和	日本マイクロソフト株式会社
	町村 泰貴	北海道大学
オブザーバ		
	乃田 昌幸	経済産業省 情報セキュリティ政策室 課長補佐
	林　弘毅	経済産業省 情報セキュリティ政策室 課長補佐
		（2011 年 8 月 9 日まで）
事務局	矢島 秀浩	独立行政法人 情報処理推進機構（前任）
	笹岡 賢二郎	独立行政法人 情報処理推進機構（新任）
	小林 偉昭	独立行政法人 情報処理推進機構
	金野 千里	独立行政法人 情報処理推進機構
	渡辺 貴仁	独立行政法人 情報処理推進機構
	板橋 博之	独立行政法人 情報処理推進機構
	相馬 基邦	独立行政法人 情報処理推進機構
	木曽田 優	独立行政法人 情報処理推進機構
	大森 雅司	独立行政法人 情報処理推進機構
	宮地 利雄	一般社団法人 JPCERT コーディネーションセンター
	古田 洋久	一般社団法人 JPCERT コーディネーションセンター
	佐藤 祐輔	一般社団法人 JPCERT コーディネーションセンター
	高橋 紀子	一般社団法人 JPCERT コーディネーションセンター
	村瀬 一郎	株式会社三菱総合研究所
	川口 修司	株式会社三菱総合研究所
	井上 信吾	株式会社三菱総合研究所

（以上、敬称略、順不同）