脆弱性情報に係る調整不能案件の公表のあり方に関する調査報告書

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。

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、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 年度脆弱性研究会において、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、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、調整不能案件の取扱方針や滞留の改善に向け関係者が実施すべき工夫等について、検討を行った。さらに、同ワーキンググループは、関連の検討会において整理された法的な論点や解決策をもとに、2010 年度脆弱性研究会終了後も引き続き調整不能案件の公表手順について検討を重ね、望ましいプロセスやガイドラインの改訂案をとりまとめた。本報告書は、その成果を 2011 年度脆弱性研究会において審議し、加筆修正した結果である。

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 12 月

情報システム等の脆弱性情報の取扱いに関する研究会

座長　　土居 範久

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）では以下の内容と方針を検討した。

・「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）に分けることとする。

・フェーズⅠは 2010 年度脆弱性研究会の検討で具体化し、フェーズⅡは WG での検討を踏まえ 2011 年度脆弱性研究会にて具体化する。

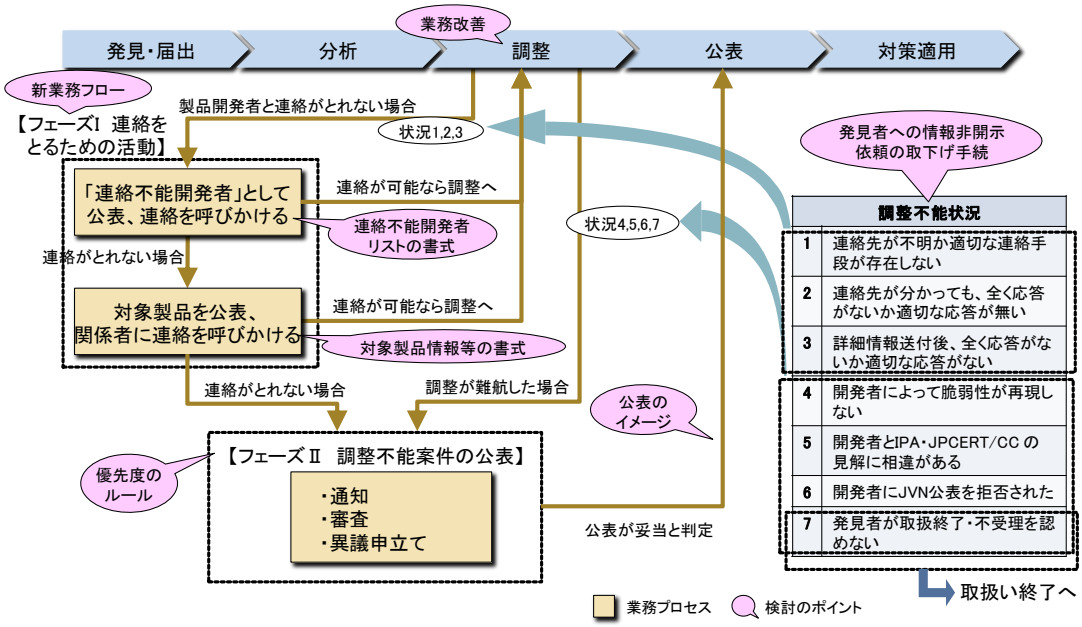

図 1-1　検討の全体イメージ

【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。

WG では、まず、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、その内容をとりまとめ（「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」）、そうした基礎情報や法的な問題を踏まえて再度 WG で検討し、実現可能な公表モデルの実装方法について分析した。

これらの後半部分については 2011 年度脆弱性研究会において審議を行った。本報告書はその検討、分析、審議の結果を示すものである。

2. 脆弱性情報に係る調整不能案件を公表する仕組みの実装に関する調査

2.1. 脆弱性情報に係る調整不能案件の公表モデル

調整不能案件を公表する仕組みをモデル化し、その実装方法についてとりまとめた。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に関して行った調査の結果(「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」)より得られた知見を「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)に報告し、WG の検討結果を基に、調整不能案件を公表する仕組みを具体化した。

まとめに当たっては、下記のような公表に至るまでのプロセスを想定し、WG での検討に先立って「脆弱性情報公表制度の法的研究委員会」(以下「法的研究委員会」という)がとりまとめた「脆弱性情報の調整不能案件に係る法的問題に関する調査報告書」を参考とした。

(1) 基本的な考え方

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、IT ユーザが被害に遭う可能性をできる限り低減すべく、IT 業界の関係者が相互に連携して努力する活動である。

パートナーシップは、IT ユーザを守るために関係者が協力する枠組みであって、脆弱性に対処しない関係者を懲らしめる枠組みではない。ただし、関係者間の信頼・協力関係を前提としている現状のガイドラインでは、何らかの理由で製品開発者との合意が得られない場合にどのように対処すべきか明確でない。たとえば、製品開発者が応答しなくなるなど不誠実な対応をとることにより、調整不能の状況に陥って公表も終了もできなくなってしまうケースも起きている。

案件を調整不能のまま滞留させることには以下のような問題がある。

- 当該ソフトウエアの製品利用者が脆弱性の存在を長期間知らされないままとなってしまう。
- 発見者のモチベーションの低下、本制度への信頼の低下につながる。
- 滞留させることにより公表を避けられると製品開発者が誤解しかねない。
- 案件を常時多数抱え込むことになり、制度に係る人的資源がより多く必要となる。

そこで、このような調整不能の状況において、製品利用者が被害に遭う可能性をできる限り低減すべく、関係者がどのように対処すべきか検討した。検討では、関係者が相互に連携して努力するパートナーシップの理念を尊重しつつ、調整不能のケースを包含できるようにガイドラインの拡充を図るものとした。

ガイドラインの拡充においては、訴訟リスクに配慮し、

- 透明性・妥当性のある処理プロセス
- 不利益を被る関係者に向けた弁明の機会の提供

を実装することが必須となる。

脆弱性の存在を公表することで、製品利用者のリスクが高まるとの考え方もあるが、ここで公表を挙げた目的は、製品利用者に当該製品を使い続けるリスクを伝え、そのリスクへの対処を自ら判断する機会を提供することにある。

(2) 公表モデルのフロー

公表モデルのフローを図 2-1に示す。このうち、フェーズⅠ（連絡をとるための活動）は 1 章で示したとおり、2010 年度脆弱性研究会でとりまとめたもので、本章の対象は主にフェーズⅡ（調整不能案件の公表）である。

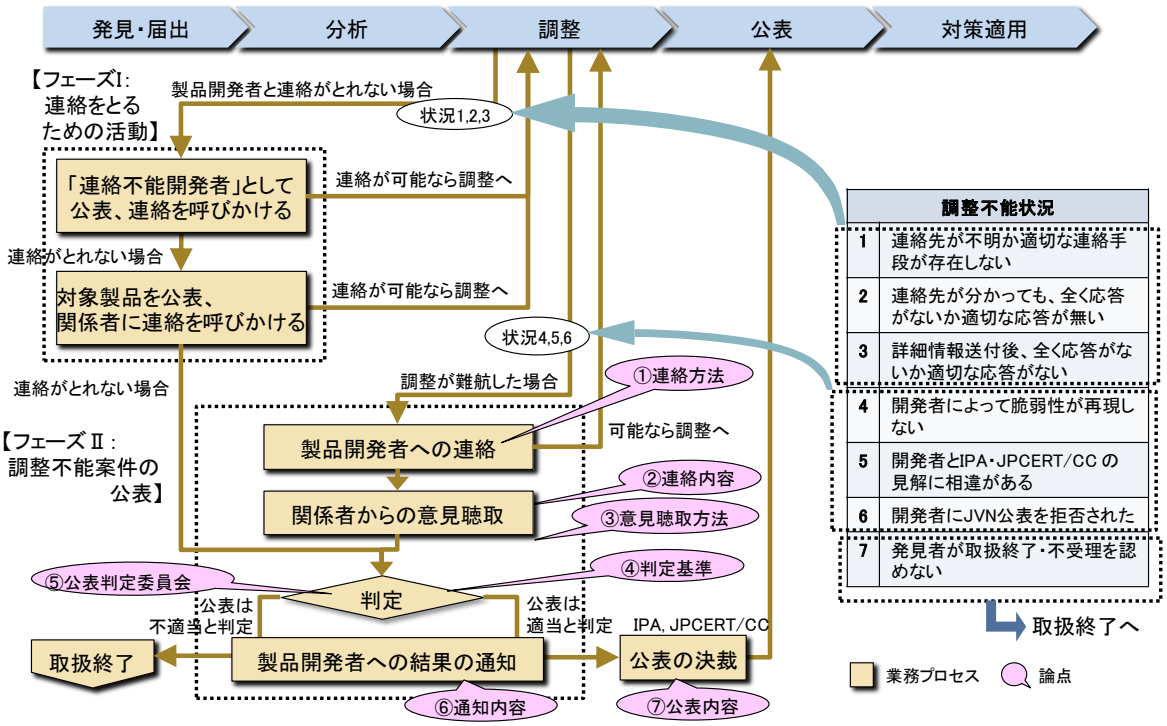

図 2-1　公表モデルのフロー

(3) 公表モデルのプロセスと論点

法的研究委員会の検討結果を踏まえ、フェーズⅡ（調整不能案件の公表）のプロセスと論点を表 2-1に示す。

表 2-1　公表モデルのプロセスと論点

	製品開発者への連絡	製品開発者からの意見聴取	判定	製品開発者への結果の通知	公表
プロセス	製品開発者に対し、当該案件を公表する旨を連絡する。	製品開発者からの意見聴取を行う。	製品開発者の意見を踏まえ、脆弱性情報の公表に関する判定を行う。	判定の結果を、製品開発者と IPA に対して通知する。	IPA および JPCERT/CC は、判定結果を踏まえ、脆弱性情報等を JVN 上 で公表する。
論点	1)連絡方法 2)連絡内容 － 連絡事項 － 公表文案	3)意見聴取方法	4)判定基準 5)公表判定委員会 － 位置づけ、構成 － 判定方法	6)通知内容	7)公表内容

公表モデルのプロセスを設定する上で、次の前提を置く。

- 「公表」以外のプロセスの主体として、「公表判定委員会」の設置を想定する。
- 「公表」プロセスの主体は、IPA および JPCERT/CC が担当する。

以下に、各プロセスの作業イメージと論点、対応方針を示す。

①製品開発者への連絡

(a) 連絡方法

公表判定委員会が、調整不能案件の当事者である製品開発者に対し、当該案件を公表するべきか否かの審議を行う旨を連絡する。連絡は、十分にプライバシーに配慮し、合理的な方法で行う。

具体的には、以下の方法で連絡を行うことが想定される。

電子メール　→　配達証明・内容証明郵便

→　その他（ISP やコミュニティを介した連絡 等）

これらの方法で連絡を試みたにもかかわらず、1 ヶ月間連絡がとれない場合には、脆弱性関連情報を公表する。

＜論点１：連絡方法＞

- 個人への連絡の場合、勤務先に連絡すべきか

　←　プライバシーに配慮し、勤務先への連絡は避けることが望ましい。

・ 連絡先が不明もしくは適切な連絡手段が存在しない場合、改めて連絡不能開発者に関する追加情報要求を行うべきか

← 連絡先が不明もしくは適切な連絡手段が存在しない場合、すでにフェーズⅠで「連絡不能開発者一覧に掲載する」「対象製品を公表し、関係者に連絡を呼びかける」等の方法を実施していることをもって、通達努力を果たしたとみなす。

(b) 連絡事項

公表判定委員会が製品開発者に連絡する内容は、行政手続法第三十条「弁明の機会の付与の通知の方式」（表 2-2参照）に倣い、以下の事項を含める。

- 公表の理由（脆弱性検証結果、経済産業省告示、判定基準等）
- 公表文案
- 意見書の提出先・期限（口頭による意見表明の場合はその日時・場所）

表 2-2 行政手続法における「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）

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

連絡内容の文案を表 2-3に示す。この案では、「公表判定委員会」の存在が理解されにくいため、差出人を IPA、JPCERT/CC および公表判定委員会の三者連名の形を採用している。

また、「判定基準」「公表文案」については以降の節で具体的に示す。

＜論点 2：連絡内容＞

・ 脆弱性検証の結果についての開示を控えてもらうべきか

← 脆弱性検証の結果は、その内容を攻撃に悪用することが可能であるため、通常は公表を避けるべきものである。しかし、そのリスクに気づかず、公表判定委員会からの連絡をそのまま公表する事業者もいる可能性があることから、「本項の記載内容については十分ご留意ください。」と伝えることが望ましい。

表 2-3　連絡内容の文案

年　月　日

（製品開発者名）様

独立行政法人 情報処理推進機構
一般社団法人 JPCERT コーディネーションセンター
公表判定委員会

脆弱性情報公表に関する審査手続きのご案内

平素は格別のご高配を賜り、厚くお礼申し上げます。

独立行政法人 情報処理推進機構（IPA）並びに一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）は、貴社/貴殿のソフトウエア製品「 ○○○」の脆弱性関連情報の届出を受け、「ソフトウエア等脆弱性情報取扱基準*1」（経済産業省告示 第 235 号、以下「告示」という。）及び「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*2」（以下「ガイドライン」という。）に基づき検証した結果、当該製品が公表すべき脆弱性を有すると判断しました。そこで、IPA が主催する公表判定委員会では、脆弱性検証結果に対する貴社/貴殿のご意見を考慮した上で、脆弱性情報を公表すべきか判定する必要があると判断するに至りました。公表は、JVN（Japan Vulnerability Notes）*3 等の IPA・JPCERT/CC のサイトで行います。

つきましては、下記の内容を確認いただき、ご意見がございましたら、以下に示す期限までに文書（FAX・電子メールも可）にて下記担当へご提出くださいますよう、お願い申し上げます。

なお、ご連絡をいただけない場合には、下記の内容をご了承いただいたものとして処理させていただきます。

■意見提出期限：平成 2○年○月○日（○）

■意見提出先：　独立行政法人 情報処理推進機構 技術本部 セキュリティセンター
情報セキュリティ技術ラボラトリー 公表判定委員会事務局
〒113-6591　東京都文京区本駒込二丁目 28 番 8 号
文京グリーンコートセンターオフィス
TEL 03-****-****　FAX 03-****-****　E-mail *****@ipa.go.jp

*1) http://www.meti.go.jp/policy/netsecurity/downloadfiles/vulhandlingG.pdf
*2) http://www.ipa.go.jp/security/ciadr/partnership_guide_200407.html
*3) http://jvn.jp/

記

(1) 判定基準（ ← 2.1(3) ③(a)を参照）

(2) 脆弱性検証結果
※本項の記載内容については取扱いに十分ご留意ください
■検証環境　Microsoft Windows *****, Client Software: ●●●
言語：English, 設定情報：基本的にデフォルト
■結果　1. ●●●を起動し、***** で attach します。
2. ●●●上のブラウザから、発見者の提供する******.zip を開きます。この ZIP ファイルは実際には zoo ファイルであり、拡張子を偽造しています。結果、以下（省略）のような例外が発生し、アーカイブ（******）の内容を変更することで任意のコードが実行出来る可能性が高いことを確認しました。

(3) 公表する場合の文案（ ← 2.1(3) ⑤を参照）

②関係者からの意見聴取

公表判定委員会は、製品開発者からの意見聴取を行う。

意見聴取については、行政手続法第二十九条「弁明の機会の付与の方式」（表 2-4参照）を踏襲し、書面（意見書）の提出を前提とする。

表 2-4　行政手続法における「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。

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

＜論点 3：意見聴取方法＞

- 口頭による意見説明はどうするか
  - ← 書面での意見提出を原則とするが、公表判定委員会の裁量によって、口頭による意見説明を認めることができるようにする。その場合の具体的な手順は、現場の運用ルールでカバーすることとし、ガイドラインでは口頭による意見表明を行う場合があることを示すに留める。
- 代理人の参加は可能か
  - ← 行政手続法第三十一条「聴聞に関する手続の準用」（表 2-5参照）を踏まえ、代理人や製品開発者以外の利害関係者の意見表明を認めることとする。

表 2-5　行政手続法における「聴聞に関する手続の準用」

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）

③判定

(a) 判定基準

公表判定委員会は、脆弱性検証結果や当該製品開発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う。

具体的には、表 2-6の 4 項目の判定基準に照らして、すべての条件を満たす場合のみ、IPA および JPCERT/CC により公表することが適当と判定する。

表 2-6　判定基準

1）当該案件が調整不能であること 2）脆弱性が存在すると判断できること 3）製品利用者に必要な情報が届かない可能性があること 4）公表が適当ではないと判断する理由・事情がないこと

＜論点 4：判定基準＞

・ 「影響の大きさ」を公表の要件に含めるべきか

← 「影響の大きさ」は、客観的な尺度での計測が困難であることから、「影響の大きさ」は公表の要件に含めるべきではないと判断した。

- CVSS（Common Vulnerability Scoring System）の基本値だけでは、実際の影響規模は評価できない。
- その時点での脅威の有無、製品利用者側の環境によって影響は大きく幅がある。
- 普及状況が把握困難なケースもある。

なお、脆弱性情報として取扱うかを決める際には、製品利用者が不特定多数であるか特定可能な少数であるかという観点からではなく、不特定多数のものが影響を受けうる脆弱性である可能性があることを受理の要件とすべきである、という意見が挙げられた。

特に、告示の本来の主旨に沿うならば、製品利用者が特定可能で修正が徹底され得るかどうかとは別の観点で、不特定多数のものが影響を受けうる脆弱性である場合には脆弱性情報の公表に向けて動くことが望ましい、とする意見もあった。

(b) 委員会

公表判定委員会は、脆弱性検証結果や当該製品開発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う。

＜論点 5：公表判定委員会＞

・ 公表判定委員会の位置付けや構成をどうすべきか

	外部機関	内部機関
設置方法（例）	IPA や JPCERT/CC 以外の機関（METI 等）が設置	IPA が設置
メリット	客観性の説明が容易	IPA が事務局として動きやすい
デメリット	IPA が事務局として動きにくい	客観性の担保が必要

← 取り扱う情報の機密性や委員への事実関係の説明義務等を考慮すれば、委員会事務局は IPA や JPCERT/CC が担当することが合理的である。さらに、JPCERT/CC は当該製品開発者と直接やりとりをしていた立場であることから、客観性を高める意味で、国の機関である IPA が設置すべきと

考えられる。

← その場合、NITE の例を参考にして、客観性を担保するため、外部委員で構成される専門家委員会（IPA および JPCERT/CC への勧告機関）と位置付けてはどうか。

← なお、対象が委員の直接的・間接的に関係する案件であった場合、当該委員は速やかにその旨を事務局に報告し、当該案件の判定には関与しないようにすることが重要である。したがって、委員委嘱の際は、その点についての誓約書を交わすことが望ましい。

・ 運営方法をどうすべきか

← 案件数次第ではあるが、NITE のケースを参考に想定する。たとえば、次のような想定が可能である。

- 委員の負担や事務局の作業量を考慮し、四半期または半年に 1 回程度の開催
- 議決を行う場合は出席委員の過半数をもって議決、賛否同数の場合は委員長が決定

④製品開発者への結果の通知

公表判定委員会は、公表に関する判定結果を、製品開発者および IPA に対して通知する。

公表が適当と判定された場合、製品開発者への通知には、製品開発者が併記を希望する意見を申し出る期間を定めて、付記する。

公表は不適当と判定された場合、IPA は判定結果の通知をもって、当該案件の取扱いを終了する。

＜論点 6：通知内容＞

・ 公表判定委員会が製品開発者に連絡する内容には、以下の事項を含める。
  - 製品開発者は意見を併記できること
  - 意見の提出先、期限、分量の上限（例：1000 字以内）、提出方法（ FAX・電子メール）
・ 連絡内容の文案を表 2-7 に示す。

表 2-7　通知内容の文案

年　月　日

（製品開発者名）様

独立行政法人 情報処理推進機構
一般社団法人 JPCERT コーディネーションセンター
公表判定委員会

脆弱性情報の公表判定結果のご連絡

平素は格別のご高配を賜り、厚くお礼申し上げます。
独立行政法人 情報処理推進機構が主催する公表判定委員会では、貴社/貴殿のソフトウエア製品「○○○」の脆弱性関連情報の届出に関して、「ソフトウエア等脆弱性情報取扱基準*1」(経済産業省告示 第 235 号)及び「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*2」（以下「ガイドライン」という）に基づき審議した結果、脆弱性情報等を公表すべきと判定しましたので、その旨ご連絡いたします。公表は、JVN（Japan Vulnerability Notes）サイト*3で行います。
つきましては、下記の公表内容について、併記を希望するご意見がございましたら、以下に示す期限までに、文書（FAX・電子メールも可。1000 文字以内）にて下記担当へご提出くださいますよう、お願い申し上げます。 ご提出いただいた文書の内容は、ガイドライン付録○に基づき、当該脆弱性情報等に併記されることになります。

■意見提出期限：平成 2○年○月○日（○）
■意見提出先：　独立行政法人 情報処理推進機構 技術本部 セキュリティセンター
情報セキュリティ技術ラボラトリー 公表判定委員会事務局
〒113-6591　東京都文京区本駒込二丁目 28 番 8 号
文京グリーンコートセンターオフィス
TEL 03-****-****　FAX 03-****-****　E-mail *****@ipa.go.jp

*1) http://www.meti.go.jp/policy/netsecurity/downloadfiles/vulhandlingG.pdf
*2) http://www.ipa.go.jp/security/ciadr/partnership_guide_200407.html
*3) http://jvn.jp/

記

(1) 公表文案（　←　2.1(3) ⑤を参照）

⑤公表

IPA および JPCERT/CC は、公表判定委員会の判定結果を受けて、公表について決裁する。

IPA および JPCERT/CC は、公表判定委員会の判定した脆弱性情報等を、JVN を通して公表する。

製品開発者から、併記を希望する意見が提出された場合、その内容を公表内容に併記する。

＜論点 7：公表内容＞

・　公表文案の内容は JVN 公表と同様でよいか

← 通常の JVN 公表と異なり、製品開発者から十分な説明がなされない可能性が高いため、より詳細な説明が必要となる。(例:公表に至る経緯)
← JVN 公表文案を表 2-8、表 2-9、
補足:「太字」は既存 JVN 公表内容から新規追加となる項目、「斜字」は既存 JVN 公表より内容の詳細化を図った項目
表 2-10に示す。

・ 製品開発者からの意見併記の方法について、運用段階には決めておく必要がある。(例:後ろに添付)

なお、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公表をせずに終了すべきではないという意見が示された。このような社会的にも大きな影響を及ぼしうる脆弱性情報について、どのように扱うべきかについて、具体的・実際的な観点から検討を行う必要がある。

表 2-8　JVN 公表文面の構成と JVN 公表文面の構成の差異

項目名	調整案件の JVN 公表	調整不能案件の JVN 公表	備考
タイトル	○	○	
概要	○	○	
影響を受けるシステム	○	－	
ベンダ情報、製品情報	－	◎	
詳細情報	○	△	
検証情報	－	◎	IPA,JPCERT/CC で実施した検証結果を記載
想定される影響	○	○	
対策方法	○	○	
ベンダ情報	○	－	
ベンダの見解	－	◎	
参考情報	○	－	
JPCERT/CC からの補足情報	○	○	公表に至る経緯を記載
JPCERT/CC による脆弱性分析結果	○	○	
IPA による脆弱性分析結果	－	◎	
謝辞	○	－	
関連文書	○	－	

＜凡例＞　「○」: 記載

「－」: 項目なし

「△」: 内容を詳細化して記載

「◎」: 新規追加で記載

表 2-9　調整不能案件における JVN 公表文面案（連絡不能案件の例）

■タイトル
JVN#********
圧縮展開ソフト A におけるバッファオーバーフローの脆弱性

■概要
圧縮展開ソフト A には、ZOO ファイル処理に関するバッファオーバーフローの脆弱性が存在します。

■ベンダ情報、製品情報
〇〇〇〇株式会社　圧縮展開ソフト A ver*.*

■詳細情報
圧縮展開ソフト A には、ZOO ファイルにおけるコメントフィールドの領域において、長い値(例:0xffff)が指定されているファイルを取り扱う際にバッファオーバーフローが発生します。

■検証情報
IPA 及び、JPCERT/CC にて、届出されたバッファオーバーフローの脆弱性について再現検証を行った結果、Windows XP SP3 の環境において、ファイル名のレジスタ値（EIP）が書き換わることを確認しました。なお、Windows Vista SP2, Windows 7 SP1 の環境においては、圧縮展開ソフト A が異常終了することのみを確認しました。それぞれにおいて、シェルコードの実行までは確認していません。また、V2.7 においても同様となることを確認しました。

■想定される影響
第三者によって細工された ZOO ファイルを圧縮展開ソフト A で展開させることで任意のコードを実行される可能性がある。

■対策方法
ワークアラウンドとして、ZOO ファイルを圧縮展開ソフト A で展開しない。

■ベンダの見解
なし

■JPCERT/CC からの補足情報
公表に至る経緯は以下の通りです。
YYYY/MM/DD:製品開発者に連絡を行う
YYYY/MM/DD:上記に対する応答がなかったため、再度製品開発者に連絡を行うが応答なし
YYYY/MM/DD:製品開発者に再度連絡を行うが応答なし
YYYY/MM/DD:「連絡不能開発者一覧」に掲載を行う
YYYY/MM/DD:「連絡不能開発者一覧」に掲載後、期限内に開発者から応答なし
YYYY/MM/DD:「連絡不能開発者一覧」に「補足情報」の掲載を行う
YYYY/MM/DD:「連絡不能開発者一覧」に「補足情報」を掲載後、期限内に製品開発者から応答なし
YYYY/MM/DD:本情報を「JVN」にて公表

■JPCERT/CC による脆弱性分析結果

評価尺度	攻撃成立条件	評価値
攻撃経路	インターネット経由からの攻撃が可能	高
認証レベル	匿名もしくは認証なしで攻撃が可能	高
攻撃成立に必要なユーザーの関与	ユーザーが何もしなくても脆弱性が攻撃される可能性がある	高
攻撃の難易度	ある程度の専門知識や運（条件が揃う確率は高い）が必要	高

■IPA による脆弱性分析結果
基本値: 5.1 (警告) [IPA 値]
*** 攻撃元区分: ネットワーク**
*** 攻撃前の認証要否: 不要**
*** 完全性への影響(I): 部分的**
*** 攻撃条件の複雑さ: 高**
*** 機密性への影響(C): 部分的**
*** 可用性への影響(A): 部分的**

補足:「太字」は既存 JVN 公表内容から新規追加となる項目、「斜字」は既存 JVN 公表より内容の詳細化を図った項目

表 2-10　調整不能案件における JVN 公表文面案（見解相違案件の例）

■タイトル
JVN#********
サーブレットコンテナ B におけるクロスサイトリクエストフォージェリの脆弱性

■概要
サーブレットコンテナ B には ExampleManager においてクロスサイトリクエストフォージェリの脆弱性が存在します。

■ベンダ情報、製品情報
B プロジェクト
サーブレットコンテナ B *.*.*およびそれ以前

■詳細情報
*サーブレットコンテナ B には **** におけるファイルアップロード機能において、WAR ファイルのアップロードの際に、アプリケーション起動時に実行される****の contextInitialized メソッドの処理に問題があるため、ログインした管理者が罠ページを踏むことで、任意の WAR ファイルが実行されるクロスサイトリクエストフォージェリの脆弱性が存在します。*

■検証情報
IPA 及び、JPCERT/CC にて、届出されたクロスサイトリクエストフォージェリの脆弱性について再現検証を行った結果、クロスサイトリクエストフォージェリの脆弱性が存在することを確認しました。
また、*.*.*においても同様の問題が存在することを確認しました。

■想定される影響
第三者によって、任意の WAR ファイルが実行される可能性があります。

■対策方法
回避策は確認できていません。

■ベンダの見解
本来、ログインをしながら、他のページを閲覧するということは想定していない。
そのため、本問題の根本はログインをしながら他のページを閲覧しているユーザーの責任であると考えているため、脆弱性ではない。

■JPCERT/CC からの補足情報
公表に至る経緯は以下の通りです。
YYYY/MM/DD：製品開発者に連絡を行う
YYYY/MM/DD：製品開発者から脆弱性ではないと連絡を受ける
YYYY/MM/DD：IPA の見解を製品開発者へ伝える
YYYY/MM/DD：再度製品開発者から脆弱性ではないと連絡を受ける
YYYY/MM/DD：脆弱性公表判定委員会に本件の公表打診を行う
YYYY/MM/DD：脆弱性公表判定委員会より公表が妥当と連絡を受ける
YYYY/MM/DD：本情報を「JVN」にて公表

■JPCERT/CC による脆弱性分析結果

評価尺度	攻撃成立条件	評価値
攻撃経路	インターネット経由からの攻撃が可能	高
認証レベル	匿名もしくは認証なしで攻撃が可能	高
攻撃成立に必要なユーザーの関与	リンクをクリックしたり、ファイルを閲覧するなどのユーザ動作で攻撃される	中
攻撃の難易度	ある程度の専門知識や運（条件が揃う確率は高い）が必要	中

■IPA による脆弱性分析結果
基本値: 5.1 (警告) [IPA 値]
*** 攻撃元区分: ネットワーク**
*** 攻撃前の認証要否: 不要**
*** 完全性への影響(I): 部分的**
*** 攻撃条件の複雑さ: 高**
*** 機密性への影響(C): 部分的**
*** 可用性への影響(A): 部分的**

補足：「太字」は既存 JVN 公表内容から新規追加となる項目、「斜字」は既存 JVN 公表より内容の詳細化を図った項目

2.2. 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の改訂

WG の検討結果に基づき、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ついて、2.1節に示したモデルを実装するために必要な改訂案を策定した。

改訂案の検討に際しては、これまでのガイドライン改訂と同様、記載内容の統一性やバランスに十分配慮するとともに、2010 年度脆弱性研究会及び WG の検討成果との整合性を確保した。改訂案全体を別紙１に示す。

(1) ガイドラインへの反映

フェーズⅡをガイドライン上に反映する方針として、フェーズⅡの各項を付録に置き、ガイドライン本体には、当該付録の処理へ進む条件を記載する。

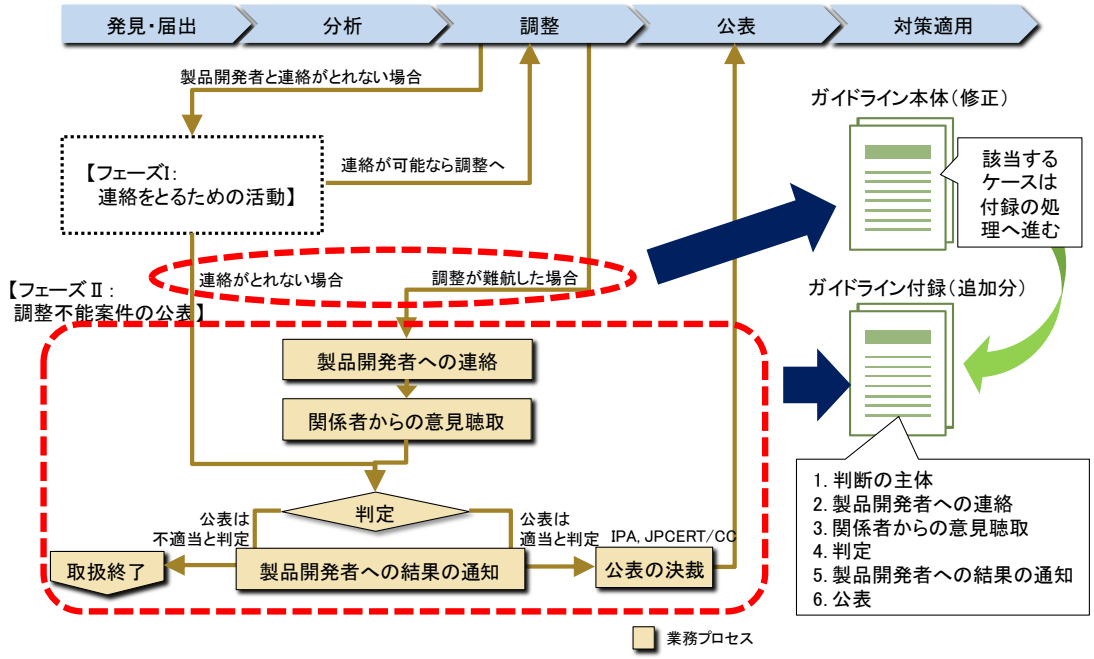

図 2-2　ガイドラインへの反映方針

(2) 調整不能案件の公表プロセスへの移行

① 一般への情報の公表

【ガイドラインの改訂内容】

Ⅳ. ソフトウエア製品に係る脆弱性関連情報取扱　３. IPA および JPCERT/CC の対応
「(1) IPA　13) 一般への情報の公表」

なお、脆弱性検証の結果の報告および対応状況の報告がない場合、IPA および JPCERT/CC は、その旨を、製品開発者名とともに JVN で公表することがあります。

「14) IPA および JPCERT/CC の判断に基づく公表」を新たな項目として追記

IPA および JPCERT/CC は、製品開発者と連絡が取れない、脆弱性検証の結果の報告および対応状況の報告がないなど、公表に向けて製品開発者との合意を得ることが困難な場合には、付録 11 に定める手続をへて、製品開発者名とともに脆弱性情報などを JVN で公表することがあります。

Ⅳ. ソフトウエア製品に係る脆弱性関連情報取扱　３. IPA および JPCERT/CC の対応
「(2) JPCERT/CC　9) 一般への情報の公表」

なお、製品開発者と連絡が取れない場合、また、脆弱性検証の結果の報告および対応状況の報告がない場合、IPA および JPCERT/CC は、その旨を、製品開発者名とともに JVN で公表することがあります。

「10) JPCERT/CC および IPA の判断に基づく公表」を新たな項目として追記

JPCERT/CC および IPA は、製品開発者と連絡が取れない、脆弱性検証の結果の報告および対応状況の報告がないなど、公表に向けて製品開発者との合意を得ることが困難な場合には、付録 11 に定める手続をへて、製品開発者名とともに脆弱性情報などを JVN で公表することがあります。

【解説】　（法的研究委員会からの推奨事項を含む）

- 調整不能に陥った案件の取扱いを公表プロセスに移行する条項を追加する。
- 公表が従来の「連絡がとれない場合」、「結果報告や対応状況の報告がない場合」に限らず、脆弱性についての評価の不一致の場合などにも及ぶこと、さらに公表の対象となる事項が、脆弱性情報等を含み総合的に公表されることを明らかにする。

② 製品開発者への連絡

【ガイドラインの改訂内容】

Ⅳ. ソフトウエア製品に係る脆弱性関連情報取扱　３. IPA および JPCERT/CC の対応
「(2)JPCERT/CC　2) 製品開発者への連絡」

さらに、製品に添えられた宛先情報をもとに電子メールや郵便、電話、FAX 等いずれの手段で製品開発者に連絡を試みても一定期間にわたりまったく応答がない場合には、「連絡が取れない」と判断します。その場合、JPCERT/CC は、該当する製品開発者を「連絡不能開発者」と位置づけて公表し、連絡を呼びかけます（付録８）。それでも連絡がとれない場合には、JPCERT/CC は、対象製品（製品名及びバージョン）を公表し、広く一般に情報提供を呼びかけます（付録９）。
これらの呼びかけにも関わらず連絡が取れない場合、JPCERT/CC は、その脆弱性の再現性確認の状況を考慮して取扱いを終了することがあります。

さらに、製品に添えられた宛先情報をもとに電子メールや郵便、電話、FAX 等いずれの手段で製品開発者に連絡を試みても一定期間にわたりまったく応答がない場合には、「連絡が取れない」と判断します。その場合、JPCERT/CC は、該当する製品開発者を「連絡不能開発者」と位置づけて公表し、連絡を呼びかけます（付録８）。それでも連絡がとれない場合には、JPCERT/CC は、対象製品（製品名及びバージョン）を公表し、広く一般に情報提供を呼びかけ**ることがあります**（付録９）。
これらの呼びかけにも関わらず連絡が取れない場合、JPCERT/CC は、その脆弱性の再現性確認の状況を考慮して取扱いを終了すること**、または、公表に向けた製品開発者との合意形成が困難であると判断し、製品開発者名とともに脆弱性情報などを JVN で公表**することがあります。**JVN で公表する場合は付録 11 に定める手続に基づき行います。**

【解説】

- 製品開発者への連絡の際、連絡先がわからない場合には、付録８、付録９の方法を試みた後、付録 11（調整不能案件の公表）において公表に向けた処理に進むことが可能な表現に改める。

【ガイドラインの改訂内容】

付録９　対象製品情報の公表と関係者へのお願い

連絡期限を追記した段階で、以下の内容を付与する。

なお、yyyy 年 mm 月 dd 日までにご連絡をいただけなかった場合は、製品開発者と連絡がとれないため調整不能と判断し、「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」の「Ⅳ. ソフトウエア製品に係る脆弱性関連情報取扱」および付録 8、9 及び 11 の記載に準じて取り扱います。

【解説】

• 製品開発者への連絡の際、連絡先がわからない場合には、付録８、付録９の方法を試みた後、付録 11（調整不能案件の公表）において公表に向けた処理に進む。

(3) 調整不能案件の公表プロセス

① フレーム全体

【ガイドラインの改訂内容】

付録 11. 調整不能案件の公表

調整不能に陥った案件について、被害が生じる可能性をできる限り低減するために、IPA および JPCERT/CC は、以下の手続きにしたがって、脆弱性情報を公表することができます。ただし、ここで扱う案件は、IPA および JPCERT/CC と製品開発者の間で合意に至らなかったものであることから、脆弱性を公表しない場合に生じうる被害と、公表により製品開発者等が被りうる不利益とのバランスに配慮するとともに、社会的影響も思料し、不利益を被りうる関係者が意見を表明することも可能な、透明性・妥当性のある処理プロセスを整備します。

【解説】　（法的研究委員会からの推奨事項を含む）

• 調整不能案件の公表プロセスについて、付録にとりまとめる。
• 公表行為が違法であると認識されないための要件：
- 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、公表の緊急性の論点を十分に考慮し、事業者の利益を不当に害さないよう注意義務を尽くすこと

  すなわち、
- 基準／ガイドラインによって調整および処理がなされること
- その手続きにおいて、ソフトウエア製品開発者も脆弱性の有無について意見を述べる機会が保障されること
• 公表によって社会的混乱を招く場合には公表を控える可能性も視野に入れる。

② 判断の主体

【ガイドラインの改訂内容】

付録 11. 調整不能案件の公表

1. 判断の主体

IPA は、調整不能案件について、公表する条件を満たしていることを判定する「公表判定委員会」を組織します。公表判定委員会は、関係者に意見表明の機会を提供し、その意見を踏まえ、公表が適当か否かを判定します。

【解説】 （法的研究委員会からの推奨事項を含む）

- 調整不能案件の公表プロセスにおける主体として、公表判定委員会を設置する。
- 公表判定委員会は、IPA 及び JPCERT/CC から一定の独立した組織であり、判断の中立性・公正性を確保するとともに、その判断の責任を明確にする必要がある。
- 主宰者たる公表判定委員会が、脆弱性情報の判定の趣旨および判定基準に基づいて判定基準の個々の要素について、判定を行う。
- なお、ガイドラインの記載事項ではないが、公表判定委員会の位置づけ、構成は以下の方向が考えられる。

- IPA の主催だが、客観性を担保するため、外部の有識者による委員で構成する専門家委員会（IPA・JPCERT/CC への勧告機関）とする。
- 対象が委員の関係する案件であった場合、委員は速やかにその旨を事務局に報告し、当該案件の判定には関与しないよう、委員委嘱の際に誓約書を得る。
- 年数回開催、さらに必要に応じて書面審議を行う 。
- 議決を行う必要が生じた場合には、出席委員の過半数をもって議決する。また、賛否同数の場合には、委員長が決定する。

③ 製品開発者への連絡

【ガイドラインの改訂内容】

付録 11. 調整不能案件の公表

2. 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。

さらに、製品開発者の連絡先が不明である場合には、付録９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。

【解説】　（法的研究委員会からの推奨事項を含む）

- 調整不能に陥った案件について、以下の事項を製品開発者に連絡する。この手続が公表の適法性を支えることになる。
  - 当該脆弱性情報を公表する方針であること
  - それに対し、製品開発者から意見書を提出できること
- 連絡は、電子メール、郵送等の手段を想定している。連絡先が不明の場合には、連絡不能開発者一覧や対象製品情報の公表等を行ったことで、連絡のための必要な努力を果たしたとみなし、次の工程に進む。

④ 関係者からの意見聴取

【ガイドラインの改訂内容】

付録 11. 調整不能案件の公表

3. 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】　（法的研究委員会からの推奨事項を含む）

- 製品開発者への連絡において、公表判定委員会は、意見表明の方法を明示する。
- 口頭による意見聴取の機会を付与する場合には、製品開発者への連絡にお

いて、口頭による意見聴取の日時及びに意見聴取の日時及び場所を伝える。
- 意見表明は、製品開発者のほか、その取引先や代理人等の関係者からなされることもある。

⑤ 判定

【ガイドラインの改訂内容】

付録 11. 調整不能案件の公表

4. 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。

1) 当該案件が調整不能であること

IPA および JPCERT/CC と製品開発者が合意に至ることが社会通念上困難になったと判断される場合を「調整不能」と位置づけます。ガイドラインⅣ章 3 節(2) 2)に示した連絡方法をすべて試みても製品開発者と 9 カ月以上連絡が取れない場合、または、製品開発者と JVN 公表に関する調整を行ったがこれ以上の調整や議論の余地が残っていない場合、当該案件は調整不能と判断します。

2) 脆弱性が存在すると判断できること

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得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るとき、脆弱性があると判断します。

3) 製品利用者に必要な情報が届かない可能性があること

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。たとえば、ソフトウエア製品が市販されている場合や、ホームページ等でダウンロード可能である場合はこれに該当します。

4) 公表が適当では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、公表を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】　（法的研究委員会からの推奨事項を含む）
- 公表判定委員会が公表の是非を判断する際の基準に相当する。
- 判定基準を明らかにすることで、本プロセスにおける公表の対象を明確化する。
- 1)では、当該案件が調整不能という特殊な状況にあることを明確にする。調整不能な状況とは、
  - 製品開発者と連絡が取れない場合

- 双方の主張が平行線で調整や議論の余地がない場合

のいずれかに該当する。

- 3)において、「不特定多数に影響する可能性があること」とした場合、公表も通知もされないケースが出てくる。そこで、不利益を被る製品利用者が出ないように、「脆弱性の修正を行うべき人に必要な情報が届かない可能性があること」とする。
- 4)は、必ずしも公表することが妥当ではないケースの場合に、公表を回避する安全措置として組み込む。

  公表することが適当ではないケースとは、以下のいずれかに該当する。
  - 製品開発者が適切に対応している場合
  - 公表によって社会的混乱を招く場合

⑥ 製品開発者への結果の通知

【ガイドラインの改訂内容】

付録 11. 調整不能案件の公表

5. 製品開発者への結果の通知

公表判定委員会は、製品開発者に対して、判定の結果を伝えます。これに対し、製品開発者が意見を有し、その併記を希望する場合には、その意見を申し出ることができます。

【解説】 （法的研究委員会からの推奨事項を含む）

- 公表判定委員会は、公表に関する判定結果を、製品開発者と IPA および JPCERT/CC に対して通知する。
- 製品開発者への通知には、製品開発者が併記を希望する意見の提出方法について付記する。
  - 併記を希望する意見の提出先
  - 期限
  - 分量の上限
  - 提出方法
- 公表が不適当と判定された場合、取扱を終了する。

⑦ 公表

【ガイドラインの改訂内容】

付録 11. 調整不能案件の公表

6. 公表

IPA および JPCERT/CC は、 JVN を通して、製品開発者名と当該脆弱性情報を公表します。製品開発者から、併記を希望する意見が申し出期間内に提出された場合、その意見の趣旨および根拠が、脆弱性情報に併記される形で公表します。

【解説】 （法的研究委員会からの推奨事項を含む）

- 公表判定委員会が公表について判定した上で、IPA および JPCERT/CC がそれぞれの組織内決裁を経て、当該脆弱性情報を JVN 上で公表する。
- IPA および JPCERT/CC は、製品開発者名とともに公表判定委員会の判定した脆弱性情報等を、JVN を通して公表する。
- 製品開発者から、併記を希望する意見が提出された場合、その内容を公表内容に併記する。
- 調整不能案件の場合、製品開発者から提供される脆弱性情報が乏しいため、通常の JVN 公表に比べ、内容が詳細になる可能性がある。
- 製品開発者からの意見は、IPA および JPCERT/CC の公表内容の後に併記する。

(4) 用語の定義

① 製品利用者の定義

【ガイドラインの改訂内容】

Ⅱ．用語の定義と前提

「１２．製品利用者」を新たな項目として追記

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・管理する企業または個人です。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】

- 「付録 11.調整不能案件の公表」において公表判定委員会が公表の是非を判断する際の基準を明確にする際に、不利益をこうむり得る製品利用者について明確化する必要が生じたため、新たに定義した。
- これに合わせてガイドラインの付録において用いられるユーザ、利用者等の用語についても再検討を行い、適宜、ガイドラインに揃えて「製品利用者」へと記載を改めた。

3. 調査を通じて明らかになった考慮点

公表プロセスの実施に関して次のような問題点を挙げて検討を加えた。

(問題点 1) 現在抱えている調整不能案件のうち、対象製品が古く、今回の公表プロセスを経て公表した場合に「今さら」感が強い（それを公表しても社会的な有益性は乏しく、JVN の価値を落としかねない）ケースが含まれている。これらについては新設する公表判定委員会で、判定基準の基準 4 に基づいて「公表しない」と判断することも難しい。

→ 「今さら JVN 公表する必要があるか否か」については、現場の担当者レベルで判断するのではなく、公表判定委員会にかけて判断する。

(問題点 2) 公表プロセスの基準を満たさず、公表判定委員会での審議にかけられない調整不能案件が存在する。その中でも、事象の原因が対象製品の脆弱性であることを確認できない場合、現在のガイドライン上は IPA・JPCERT/CC は取扱いを終了することができない。

→ これらを解消する方法については、調整不能案件の公表プロセスを運用していく中で考慮する。

（参考 1）　情報システム等の脆弱性情報の取扱いに関する研究会

(1)参加者名簿（2011 年 11 月末現在）

主査	土居 範久	中央大学
委員	秋山 卓司	社団法人日本インターネットプロバイダー協会
	今井 秀樹	中央大学
	大谷 俊一	NEC ソフト株式会社
	北澤 繁樹	三菱電機株式会社
	小島 健司	東芝ソリューション株式会社
	下村 正洋	NPO 日本ネットワークセキュリティ協会
	鈴木 裕信	NPO フリーソフトウェアイニシアティブ
	高木 浩光	独立行政法人産業技術総合研究所
	高橋 郁夫	株式会社 IT リサーチ・アート
	高橋 正和	日本マイクロソフト株式会社
	谷川 哲司	日本電気株式会社
	千葉 寛之	株式会社日立製作所
	土屋 昭治	富士通株式会社
	中尾 康二	KDDI 株式会社
	西尾 秀一	株式会社 NTT データ
	早貸 淳子	一般社団法人 JPCERT コーディネーションセンター
	前田 和貴	パナソニック株式会社
	山口 英	奈良先端科学技術大学院大学
	山崎 圭吾	株式会社ラック

（五十音順、敬称略）

オブザーバ

江口 純一	経済産業省 情報セキュリティ政策室長
乃田 昌幸	経済産業省 情報セキュリティ政策室 課長補佐
鈴木 啓紹	社団法人コンピュータソフトウェア協会
渕 眞澄	社団法人日本情報システム・ユーザー協会
安田 直義	NPO 日本ネットワークセキュリティ協会
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

（順不同、敬称略）

独立行政法人 情報処理推進機構

	藤江 一正	理事長
	仲田 雄作	理事

事務局	笹岡 賢二郎	独立行政法人 情報処理推進機構
	湯原 孝志	独立行政法人 情報処理推進機構
	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
	中野 学	独立行政法人 情報処理推進機構
	寺田 真敏	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
	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
	松崎 和賢	株式会社三菱総合研究所

（順不同、敬称略）

(2)検討経緯

研究会第 1 回会合（2011 年 10 月 4 日）

メール審議（2011 年 10 月 17 日　～　10 月 29 日）

ガイドライン改訂案最終稿確定（2011 年 11 月 8 日）

（参考 2）　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 フリーソフトウェアイニシアティブ
	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）

(2)検討経緯

WG 第 1 回会合（2011 年 4 月 8 日）
・主旨説明、論点整理
  - 調査方針
  - 論点
・今後の予定

WG 第 2 回会合（2011 年 5 月 19 日）
・検討
  - 公表モデル案

WG 第 3 回会合（2011 年 6 月 29 日）
・検討
  - 関連事例調査
  - 製品開発者の意識調査
  - 公表モデル案
  - ガイドライン改訂案

WG 第 4 回会合（2011 年 7 月 20 日）
・成果まとめ
  - 報告書案
  - ガイドライン改訂案