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改訂案

改訂案

2019 年 3 月

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
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

目　　次

Ⅰ．はじめに

○ 本ガイドラインの目的

2000 年頃より、日本国内においてソフトウエアやウェブアプリケーションの脆弱性が発見されることが増えており、これらの脆弱性を悪用した不正アクセス行為やコンピュータウイルスの増加により、企業活動が停止したり情報資産が滅失したり個人情報が漏えいしたりといった、重大な被害が生じています。そこで、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。

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。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。

具体的には、独立行政法人 情報処理推進機構（以下、「IPA」とする）が受付機関、一般社団法人 JPCERT コーディネーションセンター（以下、「JPCERT/CC」とする）が調整機関という役割を担い、発見者、製品開発者、ウェブサイト運営者と協力をしながら脆弱性関連情報に対処するための、その発見から公表に至るプロセスを詳述しています。

関係者の方々は、脆弱性関連情報の取扱いに際し、本ガイドラインを基本としてご対応くださいますようお願い申し上げます。

○ 本ガイドラインの想定する読者

本ガイドラインの想定する読者と、その方に特に参照いただきたい箇所を以下に示します。

1）ソフトウエアやウェブアプリケーションに脆弱性を発見した方

脆弱性を発見された際は IPA への届出をご検討ください。ソフトウエアの脆弱性を発見された方はⅣ．２．を、ウェブアプリケーションの脆弱性を発見された方はⅤ．２．をご参照ください。

2) 自組織が扱うソフトウエア製品の脆弱性について連絡を受けた方

JPCERT/CC からソフトウエア製品の脆弱性について製品開発者に連絡する場合があります。ソフトウエア製品の脆弱性関連情報の取扱いのプロセスはⅣ．に記しています。製品開発者による対応はⅣ．５．をご参照ください。

3) 自組織のウェブアプリケーションの脆弱性について連絡を受けた方

IPA からウェブアプリケーションの脆弱性についてウェブサイト運営者に連絡する場合があります。ウェブアプリケーションの脆弱性関連情報の取扱いのプロセスはⅤ．に記しています。ウェブサイト運営者による対応はⅤ．４．をご参照ください。

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）。

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。

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。ただし、本ガイドラインで、「対策方法」との記述がある場合、「回避方法または修正方法」の意味となります。

1）回避方法

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（修正方法は含まない）であり、ワークアラウンド（付録１を参照）と呼ばれます。

2）修正方法

脆弱性そのものを修正する方法であり、パッチ（付録１を参照）等と呼ばれます。

４．対応状況

対応状況とは、JPCERT/CC から脆弱性関連情報の通知を受けた製品開発者が報告する、脆弱性対応の取組みの状況等のことです。

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。

６．オープンソースソフトウエア（OSS）

オープンソースソフトウエア（OSS）とは、ソースコードが公開されていて、誰でも無償で入手、利用することができ、さらに改良、再配布ができるライセンスをもつソフトウエアのことです。

７．ウェブアプリケーション

ウェブアプリケーションとは、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。

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。

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（OSS 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（OSS を含む）の加工、輸入、販売または頒布する官庁、法人[1]、個人、またはコミュニティ

１０．脆弱性検証

脆弱性検証とは、受け取った脆弱性関連情報について、再現性、脆弱性に該当することを検証することです。

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。

[1] 海外のソフトウエア製品の国内での主たる販売権を有する会社（外国企業の日本法人や総代理店等）を含みます。

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。

１３．システム構築事業者

システム構築事業者とは、ソフトウエア製品を入手し、それを使ってシステムを構築し、利用者に提供する法人または個人のことです。システムの構築サービスや保守、運用のサービスを通じて、顧客であるウェブサイト運営者の脆弱性対策を実施することもあります。

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。

〇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。

〇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。

Ⅳ. ソフトウエア製品に係る脆弱性関連情報取扱

１. 概要

ソフトウエア製品に係る脆弱性関連情報取扱の概要は、図１の通りです。

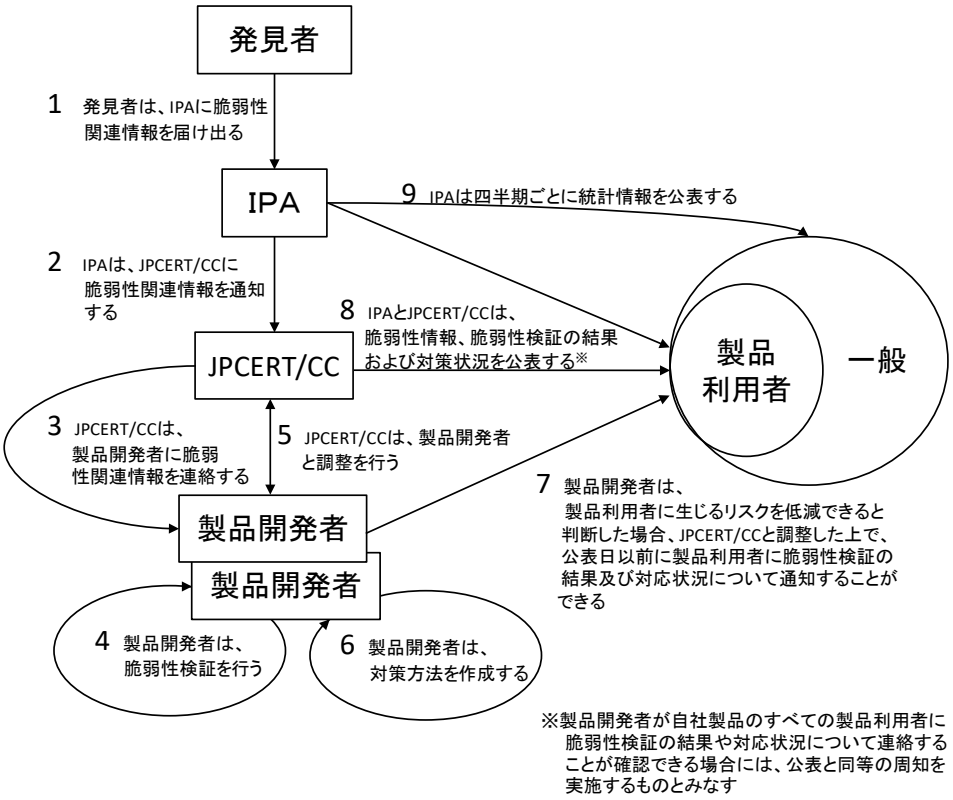


図１　ソフトウエア製品に係る脆弱性関連情報取扱の概要

（ソフトウエア製品における脆弱性情報取扱いの全体フローは付録２を参照）

1) 発見者は、IPA に脆弱性関連情報を届け出る
2) IPA は、受け取った脆弱性関連情報を、原則として JPCERT/CC に通知する
3) JPCERT/CC は、脆弱性関連情報に関係する製品開発者を特定し、製品開発者に脆弱性関連情報を通知する
4) 製品開発者は、脆弱性検証を行い、その結果を JPCERT/CC に報告する
5) JPCERT/CC と製品開発者は、対策方法の作成や海外の調整機関との調整に要する期間、当該脆弱性情報流出に係るリスクを考慮しつつ、脆弱性情報の公表に関するスケジュールを調整し決定する
6) 製品開発者は、脆弱性情報の公表日までに対策方法を作成するよう努める
7) 製品開発者は、製品利用者に生じるリスクを低減できると判断した場合、JPCERT/CC と調整した上で、公表日以前に製品利用者に脆弱性検証の結果、対策方法および対応状況について通知することができる
8) IPA および JPCERT/CC は、脆弱性情報と、3)にて JPCERT/CC から連絡したすべての製品開発者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

9) IPA は統計情報を、原則、四半期ごとに公表する

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。

2) 脆弱性関連情報の発見・取得

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。

3) 脆弱性関連情報の届出

発見者は、発見した脆弱性関連情報を IPA に届け出てください[2]。

ただし、発見者から直接の届出を受け入れる旨を承諾している製品開発者[3]の場合、直接届け出ることも可能です。

その際、IPA と製品開発者の両方に届け出る場合には、関係者間の調整が混乱しないように、脆弱性の解消に向けた製品開発者との調整を自ら行うか、IPA に任せるかを届出の際に、明確にしてください。さらに、以降の調整を IPA に任せる場合は、製品開発者へその旨を通知するとともに、その通知を行った旨を届出に明記してください。

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[4]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。

また、情報非開示依頼の効力のある間は、脆弱性関連情報が第三者に漏えいし

---

[2] 特に、複数の製品開発者の製品に影響する可能性がある脆弱性関連情報については、受け取れない製品開発者が出ないように、IPA へ届出を行うことが望まれます。

[3] IPA および JPCERT/CC が提供する脆弱性対策情報ポータルサイト Japan Vulnerability Notes（JVN）にある JPCERT/CC 製品開発者リストの中に掲載しています。

[4] 本ガイドラインのⅣ．４．2)において規定された連絡を最初に試みた日を起算日とします。

ないように適切に管理してください。

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[5]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

6) 製品開発者との直接の情報交換

発見者は、IPA に脆弱性関連情報を届け出た後、IPA および JPCERT/CC を介し、製品開発者の了解を得て、製品開発者と直接情報交換を行うことができます。

7) 届出後の対応

発見者は、届出後、IPA に進捗状況の問い合わせを行うことができます。IPA は、本ガイドラインの３．に則って処理を行い、発見者の問い合わせに対し、適切に情報の開示を行います。発見者は、開示された情報をみだりに第三者に開示しないでください。

[5] 具体的には、「検証コード」、「画面キャプチャ」、「ログ」等。

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

1) 脆弱性関連情報の受付

IPA の脆弱性関連情報の受付に関し、詳細は以下の URL をご参照ください。

https://www.ipa.go.jp/security/vuln/

届出は 24 時間受け付けますが、受け付けた情報について 2)以降の作業を行うのは原則営業日のみとなります。

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。

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。

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）。

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。

6) 発見者に係る情報の取扱い

IPA は、氏名・連絡先を含む発見者に係る情報を、発見者が望む場合以外には、JPCERT/CC と製品開発者および第三者に漏えいしないよう適切に管理します。

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）

8) 発見者との情報交換

IPA は、届出を受理した後、発見者に問い合わせをすることがあります。また、発見者から問い合わせがあった場合、JPCERT/CC と相談の上、適切な情報の開示を行います。なお、発見者との情報交換に際しては、第三者に情報が漏えいしないよう留意します。

9) 脆弱性関連情報の影響の分析

IPA は、JPCERT/CC 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、JPCERT/CC を介して、製品開発者に連絡します。

10) 対策方法および対応状況の共有

IPA は、JPCERT/CC を介して連絡した脆弱性関連情報に係る製品開発者の対策方法および対応状況を、JPCERT/CC と共有します。

11) 情報非開示依頼の取下げ

IPA は、起算日から 1 年以上経過した届出について、発見者から情報非開示依頼の取下げが求められた場合、これを取り下げます。そのとき、製品開発者が正当な理由により対応に時間を要する場合、IPA はその状況を発見者に適切に説明し、発見者が情報開示の必要性を客観的に判断できるようにします。

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」[6]で定める重要インフラ事業者等とします。

13) 一般への情報の公表

IPA および JPCERT/CC は、JVN を通じて、一般に対し、脆弱性情報と JPCERT/CC から連絡したすべての製品開発者の脆弱性検証の結果、対策方法および対応状況を公表します。さらに、一旦公表した後、製品開発者から新たな対策方法と対応状況のいずれかまたは両方を受け取った場合、その都度更新します。

また、IPA および JPCERT/CC は、JVN に関する問い合わせ先を明示し、主として OSS 等に関して、システム構築事業者や製品利用者の脆弱性対応を促すことを目的として、問い合わせ対応を実施します。なお、問い合わせに関する内容については、必要に応じて JVN の公表情報に反映します。

一般への情報の公表に際しては、IPA は、発見者にその旨を通知します。

14) 統計情報の集計と公表

IPA は、脆弱性に係る実態を周知徹底し危機意識の向上を図り、その結果としての被害の予防のために、受け付けた脆弱性関連情報を集計し、統計情報としてインターネット上等で原則、四半期ごとに公表します。統計情報には、届出件数の時間的推移等が含まれます。

[6]NISC　重要インフラの情報セキュリティ対策に係る行動計画
https://www.nisc.go.jp/active/infra/siryou.html

(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。

調整不能とは、具体的には以下のいずれかのケースに該当します。

(ア)Ⅳ．４．2)に示した連絡方法をすべて試みても製品開発者と 6 ヶ月以上連絡が取れない場合（以下、「連絡不能」という）

(イ)製品開発者と JVN 公表に関する調整を行った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

IPA は、公表判定委員会において、脆弱性情報を公表しない場合に製品利用者等が受けうる被害と、公表した場合に製品開発者、製品利用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、社会的影響も考慮し、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・妥当性のある判定プロセスを整備します。

IPA は、中立性を考慮し、当該調整不能案件に利害関係がない有識者、法律やサイバーセキュリティの専門家、当該ソフトウエア製品分野の専門家を公表判定委員会の委員に指名します。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。

2) 判定に必要な情報の収集・整理

IPA は、JPCERT/CC から製品開発者の連絡先（メールアドレス等)、当該脆弱性関連情報並びに製品開発者による脆弱性検証の結果、対策方法および対応状況を聴取し、公表判定委員会の判定に必要な資料を作成します。

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。

(ア)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。

(イ)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。

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。

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。

6) 結果の通知

IPA は、公表判定委員会が行った判定に基づいて、公表するかどうかの判断を行い、その結果と理由を JPCERT/CC および製品開発者に通知します。ただし、連絡不能案件の場合、製品開発者には通知しません。

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。

４. JPCERT/CC（調整機関）の対応

1) 製品開発者リストの整備

JPCERT/CC は、製品開発者に対して脆弱性関連情報を連絡するために、日頃より製品開発者リストの整備に努めます。この製品開発者リストには、

製品開発者ごとに、製品脆弱性対策管理者名、連絡窓口（メールアドレス、電話番号、住所等）等を登録します。

また、製品開発者が自身の名称等を公表することを承諾した場合、JPCERT/CC はそれを「JPCERT/CC 製品開発者リスト[7]」に掲載します。

なお、製品開発者が発見者からの直接届出を受け付けることを希望する場合、JPCERT/CC は当該製品開発者の脆弱性受付窓口の設置状況や自身のウェブサイトでの脆弱性公表の実績等を勘案して、「JPCERT/CC 製品開発者リスト」上に当該製品開発者の脆弱性受付窓口の情報を追記します。

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。

これは、製品開発者または開発コミュニティによる脆弱性対応が困難でかつ発表もされない場合に、当該 OSS を導入した製品の開発者や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は、それらの脆弱性対応が重要であるケースが想定されるためです。

なお、IPA から通知された脆弱性関連情報が、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）。

さらに、製品開発者が申告した連絡先情報や製品に添えられた宛先情報等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（連絡不能開発者一覧の公表については、付録５を参照）。それでも連絡が取れない場合には、JPCERT/CC は、対象製品（製品名およびバージョン）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（対象製品情報の公表と関係者へのお願いについては、付録５を参照）。

[7] 「JPCERT/CC 製品開発者リスト」https://jvn.jp/nav/index.html

3) 公表日の決定

JPCERT/CC は、製品開発者から脆弱性検証の結果を受け取り、製品開発者と相談した上で、脆弱性情報と製品開発者の対策方法および対応状況の公表日を決定し、IPA および関係する製品開発者に通知します。公表日は、JPCERT/CC が「製品開発者への連絡」（４．2）を参照）にて規定された連絡を最初に試みた日（起算日、２．注釈 4 を参照）から 45 日後を目安とします。ただし、公表日の決定に際しては、以下の点も考慮します。

①対策方法の作成に要する期間
②海外の調整機関との調整に要する期間
③脆弱性情報流出に係るリスク

また、通知した製品開発者が複数いて、その一部の製品開発者しか脆弱性検証の結果報告をしない場合、JPCERT/CC は、得られた結果報告を踏まえつつ、過去の類似事例や②③を参考にして公表日を決定し、IPA および関係する製品開発者に通知します。

4) 公表日決定後の対応

JPCERT/CC は、製品開発者から、一般への公表日の変更の要請を受けた場合、公表日を変更することがあります。その場合、変更した公表日を IPA および脆弱性関連情報に関して連絡を行ったすべての製品開発者に連絡します。

さらに、以下の場合、一般への公表を取りやめることがあります。その場合、その旨を製品開発者および IPA に連絡します。

(ア)通知を行った製品開発者から脆弱性情報に該当しないとの連絡を受けた場合
(イ)通知を行った製品開発者から脆弱性による影響がないとの連絡を受けた場合
(ウ)通知を行った製品開発者から脆弱性による影響が小さいとの連絡を受けた場合（付録４を参照）
(エ)脆弱性関連情報が既知であり、脆弱性情報等が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）

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。

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。

7) 対策方法および対応状況の受付

JPCERT/CC は、JPCERT/CC から連絡したすべての製品開発者に対して、脆弱性情報の一般公表日までに、脆弱性関連情報に係る対策方法および対応状況を報告するように要請します。一般への脆弱性情報の公表に際しては、対策方法および対応状況を IPA と共有します。

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。

なお、優先的な情報提供を受ける基盤保有事業者は、以下の条件をすべて満たす必要があります。

(ア)情報を提供された当該事業者の中で秘密情報管理を徹底すること

(イ)当該事業者自身の委託先(システム構築事業者、セキュリティベンダ等)各社において、秘密情報管理を徹底すること

(ウ)JPCERT/CC から優先的に提供される情報は当該基盤を防護する目的に対してのみ利用することを徹底すること

ただし、優先提供の趣旨を鑑み、運用方法および提供対象事業者を継続的に見直していくものとします。

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。

9) 一般への情報の公表

JPCERT/CC および IPA は、JVN を通じて、一般に対し、脆弱性情報と JPCERT/CC から連絡したすべての製品開発者の脆弱性検証の結果、対策方法および対応状況を公表します。さらに、一旦公表した後、製品開発者から新たな対策方法と対

応状況のいずれか一つ以上を受け取った場合、その都度更新します。

また、製品開発者が製品利用者に生じるリスクを低減できると判断した場合、JPCERT/CC は製品開発者と調整した上で、製品開発者が製品利用者に脆弱性検証の結果、対策方法および対応状況を公表前に通知することを認めることができます。

さらに、JPCERT/CC および IPA は、JVN に関する問い合わせ先を明示し、主として OSS 等に関して、システム構築事業者や製品利用者の脆弱性対応を促すことを目的として、問い合わせ対応を実施します。なお、問い合わせに関する内容については、必要に応じて JVN の公表情報に反映します。

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[8]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。

５．製品開発者の対応

製品開発者は、製品に脆弱性が存在する場合には、その対策に関して適切な対応をすることが望まれます。製品開発者に係る法的な論点は、付録３を参照してください。

以下で、製品開発者が脆弱性関連情報の対応のために、行うことが望ましい事項を説明します。

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。

また、窓口の変更があれば速やかに JPCERT/CC に連絡してください。

[8] 製品開発者が見解の併記を希望した場合のみ併記します。

さらに、製品開発者が発見者からの直接届出を受け付けるために「JPCERT/CC 製品開発者リスト」へ自身の窓口情報の掲載を希望する場合は、その旨を申し出てください。

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。

3) 脆弱性情報の公表日の調整

製品開発者は、検証の結果、脆弱性が存在することを確認した場合、対策方法の作成や外部機関との調整に要する期間、当該脆弱性情報流出に係るリスクを考慮しつつ、脆弱性情報の公表に関するスケジュールについて JPCERT/CC と相談してください。なお、公表日は、JPCERT/CC が「製品開発者への連絡」（４．2）を参照）にて規定された連絡を最初に試みた日（起算日、２．注釈 4 を参照）から 45 日後を目安とします。公表に更なる時間を要する場合は、JPCERT/CC と相談してください。

4) 発見者との直接の情報交換

製品開発者は、JPCERT/CC から脆弱性関連情報を受け取った後、JPCERT/CC および IPA を介し、発見者の了解を得て、発見者と直接情報交換を行うことができます。

5) 関連ウェブサイトに関する情報の取扱い

当該ソフトウエア製品がウェブサイトの構成要素であり、製品開発者が当該脆弱性を再現できない場合、 製品開発者は、届出に関連したウェブサイトの情報を JPCERT/CC に求めることができます。製品開発者は、関連ウェブサイトの情報が提供された場合、その情報を第三者に漏えいしないように適切に管理してください。

6) 問い合わせへの対応

製品開発者は、JPCERT/CC からの脆弱性関連情報に係る技術的事項および進捗状況に関する問い合わせに的確に答えてください。

7) 対策方法および対応状況の連絡

製品開発者は、脆弱性情報の一般への公表日までに脆弱性関連情報に係る対策方法を作成するように努めて、対策方法および対応状況を JPCERT/CC に連絡してください。JPCERT/CC に対する対策方法および対応状況の報告をもって、IPA にも報告したこととみなされます。また、新たな対策方法を作成した場合や対応状況が変わった場合、その都度、JPCERT/CC に最新の情報を連絡してください。

8) 対策方法の周知

製品開発者は、対策方法を作成した場合、脆弱性情報一般公表日以降、それを製品利用者に周知してください。望ましい公表の手順については、本ガイドラインの別冊「ソフトウエア製品開発者による脆弱性対策情報の公表マニュアル」を参考にしてください。

9) 製品開発者内の情報の管理と開示

製品開発者は、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でください。また、製品開発者は、上記 3)で作成した脆弱性情報の一般公表スケジュールおよび脆弱性関連情報を、脆弱性情報を一般に公表する日まで第三者に漏えいしないように管理してください。

ただし、製品利用者に生じるリスクを低減できると判断した場合、製品開発者は、JPCERT/CC と調整した上で、直接あるいはシステム構築事業者を介して製品利用者に脆弱性検証の結果、対策方法および対応状況を公表前に通知することができます。その際、製品開発者は、通知先に対し、脆弱性関連情報を第三者に開示しないこと、および脆弱性情報を一般に公表するまでの間、脆弱性情報と対策方法について、第三者に漏えいしないように適切に管理することを要請してください。

10) 公表判定委員会に関する対応

IPA および JPCERT/CC は、製品開発者と適切な連絡が取れない等の理由により進展が見込めなくなった場合には、３．(2)に定める手続きを行い、公表するかどうかを IPA が組織する公表判定委員会で判定することができます。脆弱性情報を公表すると判定した場合、IPA および JPCERT/CC は、製品開発者名とともに脆弱性情報等を JVN で公表します。

公表判定委員会による判定が行われる場合、製品開発者には意見を表明する機会が与えられます。公表判定委員会による判定のプロセスについては３．(2)を参照してください。

６．その他

1) 製品開発者自身による脆弱性関連情報の発見・取得

製品開発者は、自身のソフトウエア製品に関する脆弱性関連情報について自身で発見・取得した場合、または他の者によって開示された脆弱性関連情報を取得した場合、対策方法を作成し、製品利用者に対して当該脆弱性情報と対策方法を周知してください。

さらに、製品開発者は、当該脆弱性関連情報および対策方法を IPA または JPCERT/CC に通知してください。ただし、すべての製品利用者に当該脆弱性関連情報および当該対策方法を通知した場合、通知は不要です。

2) IPA および JPCERT/CC による普及支援

IPA および JPCERT/CC は、上記 1)で受け取った届出に関して、当該脆弱性情報および対策方法を JVN で公表します。公表する時期については、製品開発者と事前に調整を図ります。

Ⅴ．ウェブアプリケーションに係る脆弱性関連情報取扱

１．概要

ウェブアプリケーションに係る脆弱性関連情報取扱概要は、図２の通りです。

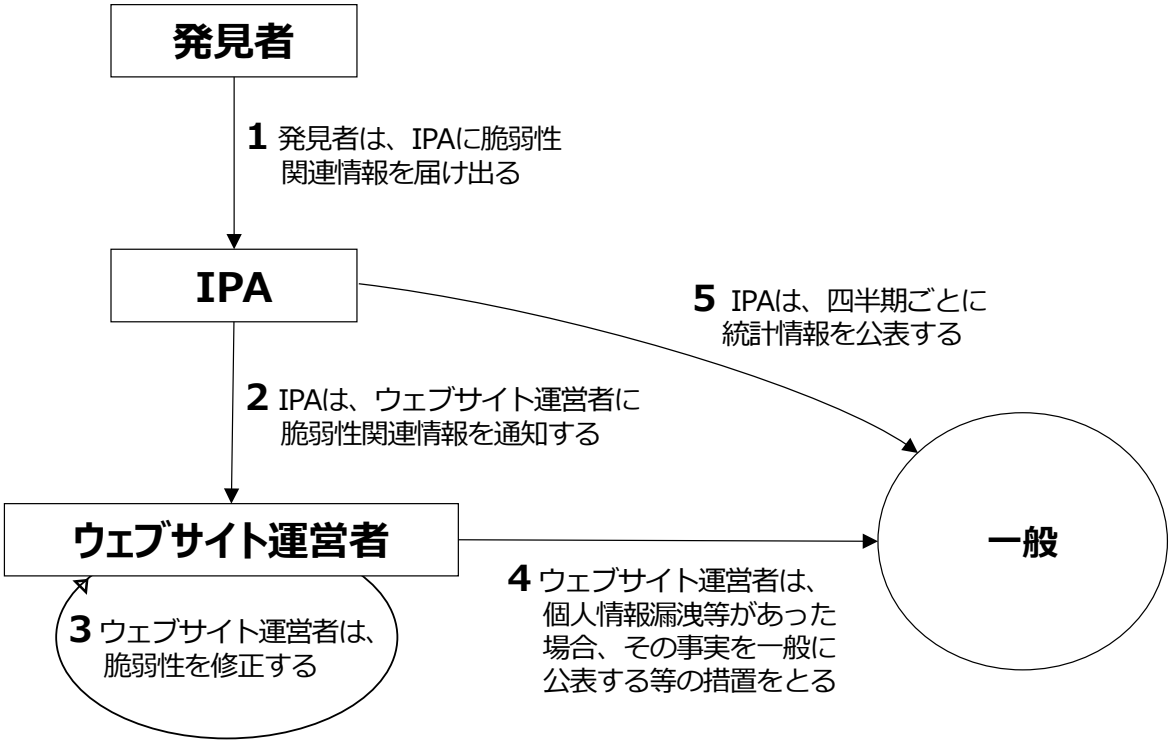


図２　ウェブアプリケーションに係る脆弱性関連情報取扱概要

（ウェブアプリケーションにおける脆弱性情報取扱いの全体フローは付録２を参照）

1）発見者は、IPA に脆弱性関連情報を届け出る
2）IPA は、受け取った脆弱性関連情報に関して、原則としてウェブサイト運営者に通知する
3）ウェブサイト運営者は、脆弱性関連情報の内容を検証し、影響の分析を行った上で、必要に応じて脆弱性の修正を行う
4）個人情報漏えい等の事件があった場合、ウェブサイト運営者は、その事実を一般に公表する等適切な処置をとる
5）IPA は統計情報を、原則、四半期ごとに公表する

２．発見者の対応

1）脆弱性関連情報の発見・取得

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無いように留意してください。法的な論点に関しては、付録３を参照してください。

2）脆弱性関連情報の届出

発見者は、発見した脆弱性関連情報を IPA に届け出てください。

なお、外部からの連絡窓口[9]を設置しているウェブサイト運営者については、直接届出を行うことも可能です。ウェブサイト運営者に直接届け出たが、脆弱性の解消に向けたウェブサイト運営者との調整が難航した場合には、IPA に連絡してください。

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。

4）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）のウェブサイト運営者への通知の可否

（エ）ウェブサイト運営者から直接連絡を受けることの可否

（オ）脆弱性関連情報に係るウェブアプリケーションが稼動しているウェブサイトの URL

（カ）脆弱性関連情報の内容（脆弱性関連情報を確認する環境と、手順および結果）

可能であれば、脆弱性が存在する証拠[10]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）。

（キ）個人情報の取扱い方法（ウェブサイト運営者との直接の情報交換の可否、ウェブサイト運営者への通知の可否）

発見者が望まない場合、IPA は、ウェブサイト運営者へ発見者を特定

[9] たとえば「ホームページに対するお問い合わせ窓口」のことです。

[10] 具体的には、「検証コード」、「画面キャプチャ」、「ログ」等。

しうる情報を連絡することはありません。

（ク）他の組織（製品開発者、他のセキュリティ関係機関等）への届出状況等

5）ウェブサイト運営者との直接の情報交換

発見者は、IPA に脆弱性関連情報を届け出た後、IPA と協議の上、ウェブサイト運営者の了解を得て、ウェブサイト運営者と直接情報交換を行うことができます。

6）届出後の対応

発見者は、届出後、IPA に進捗状況の問い合わせを行うことができます。IPA は、本ガイドラインの３．に則って処理を行い、発見者から問い合わせがあった場合、適切な情報の開示を行います。発見者は、開示された情報をみだりに第三者に開示しないでください。

３．IPA（受付機関）の対応

1）脆弱性関連情報の受付

脆弱性関連情報の受付に関し、詳細は以下の URL をご参照ください。

https://www.ipa.go.jp/security/vuln/

届出は 24 時間受け付けますが、受け付けた情報について 2)以降の作業を行うのは原則営業日のみとなります。

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）

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 による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。

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ことが明白な脆弱性関連情報に関しては、処理を取りやめることがあります。

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。

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。また、ウェブサイト運営者が脆弱性の再現する状況を特定できない場合等は、ウェブサイト運営者の了解を得た上で、IPA は IPA の内部または外部で脆弱性関連情報に関する技術的分析を行います。なお、届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）。

ウェブサイトに掲載された宛先情報をもとに電子メールや電話、FAX 等いずれの手段でウェブサイト運営者に脆弱性関連情報に係る問い合わせを試みても、一定期間にわたり的確な答えがない場合、IPA は、その脆弱性の影響範囲や取扱期間を考慮して取扱いを終了することがあります（ 4)(カ)を参照）。

6）発見者との情報交換

IPA は、届出を受理した後でも、発見者に問い合わせすることがあります。また、発見者から問い合わせがあった場合、ウェブサイト運営者と相談の上、適切な情報の開示を行います。

7）脆弱性関連情報の取扱い

IPA は、脆弱性関連情報に関して、発見者・ウェブサイト運営者以外の第三者に開示しません。ただし、下記のような正当な理由がある場合は、外部機関に脆弱性関連情報を開示することがあります。これらの場合、IPA は秘密保持契約を結びます。さらに、下記 8)に関しては例外とします。

（ア）脆弱性が再現する状況を特定できない等止むを得ない場合、IPA は国立研究開発法人産業技術総合研究所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

（イ）政府機関のウェブサイトの場合、IPA は内閣サイバーセキュリティセンター（NISC）へ当該ウェブサイト運営者への脆弱性関連情報の一部を開示し迅速な情報の取得を依頼する

（ウ）地方公共団体のウェブサイトの場合、IPA は総務省へ当該ウェブサイト運営者への脆弱性関連情報の一部を開示し迅速な情報の取得を依頼する

（エ）個人情報が漏えいしているおそれがあり、ウェブサイト運営者による対応がされない場合、IPA は個人情報保護委員会に脆弱性関連情報を連絡し、個人情報保護法（平成 15 年法律第 57 号）第 42 条に基づく措置を依頼する

8）ソフトウエア製品の脆弱性である場合の対応

IPA は、届け出られた脆弱性関連情報を分析する過程で、ソフトウエア製品の脆弱性であることを認識した場合、JPCERT/CC を介して製品開発者に連絡を行います。その際、原則としてウェブサイトを特定可能な情報を提供しないように適切に管理します。ただし脆弱性の再現のため必要な場合、ウェブサイト運営者の同意が得られれば、当該ウェブサイトに関する情報を製品開発者に提供することがあります。

9）発見者の個人情報の管理

IPA は、氏名・連絡先を含む発見者に係る情報を、発見者が望む場合以外には、ウェブサイト運営者および第三者に漏えいしないよう適切に管理します。

10）脆弱性の修正の通知

IPA は、ウェブサイト運営者から脆弱性を修正した旨の通知を受けた場合、そ

れを速やかに発見者に通知します。

11）統計情報の集計と公表

IPA は、脆弱性に係る実態を周知徹底し危機意識の向上を図り、その結果としての被害の予防のために、受け付けた脆弱性関連情報を集計し、統計情報としてインターネット上等で原則、四半期ごとに公表します。統計情報には、届出件数の時間的推移等が含まれます。その際に、当該ウェブアプリケーションの脆弱性関連情報に関して、サイト名・URL・ウェブサイト運営者名が判別可能な形式で公表することはありません。

４．ウェブサイト運営者の対応

ウェブアプリケーションに脆弱性が存在する場合には、ウェブサイト運営者は、これに関して適切な対応をすることが望まれます。

ウェブサイト運営者における法的な論点は、付録３を参照してください。

以下で、ウェブサイト運営者が対応すべき事項を説明します。

1）脆弱性関連情報への対処

ウェブサイト運営者は、通知を受けたら、脆弱性の内容を検証し、脆弱性が存在することを確認した場合には、脆弱性の及ぼす影響を正確に把握し、その大きさを考慮して脆弱性を修正してください。また、当該脆弱性関連情報に関して検証した結果、および修正した場合その旨を IPA に連絡してください。この連絡は、IPA から脆弱性関連情報の通知を受けてから、3 ヶ月以内を目処としてください。

2）問い合わせへの対応

ウェブサイト運営者は、IPA からの脆弱性関連情報に係る問い合わせに的確に答えてください。

3）発見者との直接の情報交換

ウェブサイト運営者は、脆弱性を修正するために、IPA と協議の上、発見者の了解のある場合、発見者と直接情報交換を行うことが可能です。

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。

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

付録１　用語の解説

１．ソフトウエア製品

ソフトウエア製品（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）の種類は、OS、ブラウザ、メーラ等のクライアント上のソフトウエア、DBMS（Database Management System)、ウェブサーバ等のサーバ上のソフトウエア、プリンタ、IC カード、PDA（Personal Digital Assistance)、コピー機等のソフトウエアを組み込んだハードウエア、制御システム用製品等を想定しています。

制御システムは、他の機器やシステムの動作を管理、指示、制御するシステムまたは装置であり、センサやアクチュエータ等のフィールド機器、制御用ネットワーク、コントローラ、監視制御システム（SCADA：Supervisory Control And Data Acquisition とも呼ばれる）等で構成されています。

制御システムは、一般にライフサイクルが長いこと、業務の性質上すぐに停止できないため、対策が用意されてもそれを実施することが難しい場合があることから、対策の実施に時間を要する点に配慮する必要があります。さらに、社会基盤を支える制御システムの場合、被害が生じたときの社会的影響が大きい点にも配慮する必要があります。

２．エクスプロイトコード

エクスプロイトコードは、攻撃コードとも呼ばれることもあり、脆弱性を悪用するソフトウエアのソースコードです。しかし、使い方によっては、脆弱性の検証に役立つこともあります。

３．ワークアラウンド

当該脆弱性を修正する以外の方法で脆弱性による影響を回避・低減する方法です。例えば、ソフトウエア製品においては、脆弱性のある機能の無効化や代替ソフトウエアへの移行等があります。ウェブサイトにおいては、脆弱性の影響を受けるサービスの停止や、WAF（ウェブ・アプリケーション・ファイアウォール）の導入等があります。

４．パッチ

脆弱性を有するソフトウエアから、脆弱性を解消するためにソフトウエアに対して適用する差分のソフトウエアあるいはデータのことです。

５．ウェブサイト運営者

ウェブサイト運営者とは、脆弱性関連情報が発見されたウェブアプリケーションを運営する主体です（例えば、ウェブサイト https://www.ipa.go.jp/ のウェブサイト運営者は IPA です）。ウェブサイトの管理を外部の事業者に委託している場合でも、あくまで委託元がウェブアプリケーションを運営する主体でありウェブサイト運営者となります。

６．プロトコルの実装に係る脆弱性

過去に報告があったプロトコルに関連する脆弱性の主なものを以下に挙げます。

(1) H.323 に係る脆弱性
(2) SSH2 に係る脆弱性
(3) OpenSSL に係る脆弱性
(4) ASN.1 に係る脆弱性

７．ウェブサイトの不適切な運用

ウェブサイトの不適切な運用の例を以下に挙げます。

・ウェブサイトにおいて、本来提供するべき対象外の機能（ウェブサイト管理画面等）やファイル（個人情報ファイル等）が、アクセス制限なしに公開されており、セキュリティが維持できなくなっている。
・ウェブサイトで使用されているソフトウエア製品に脆弱性が存在している。
・サービスを行っていないウェブサイトの脆弱性が放置されている。

付録２　脆弱性情報取扱いのフロー

　ソフトウエア製品、ウェブアプリケーションそれぞれの脆弱性情報取扱いに関する全体的な流れを図３、図４に示す。

図３　ソフトウエア製品における脆弱性情報取扱いの全体フロー

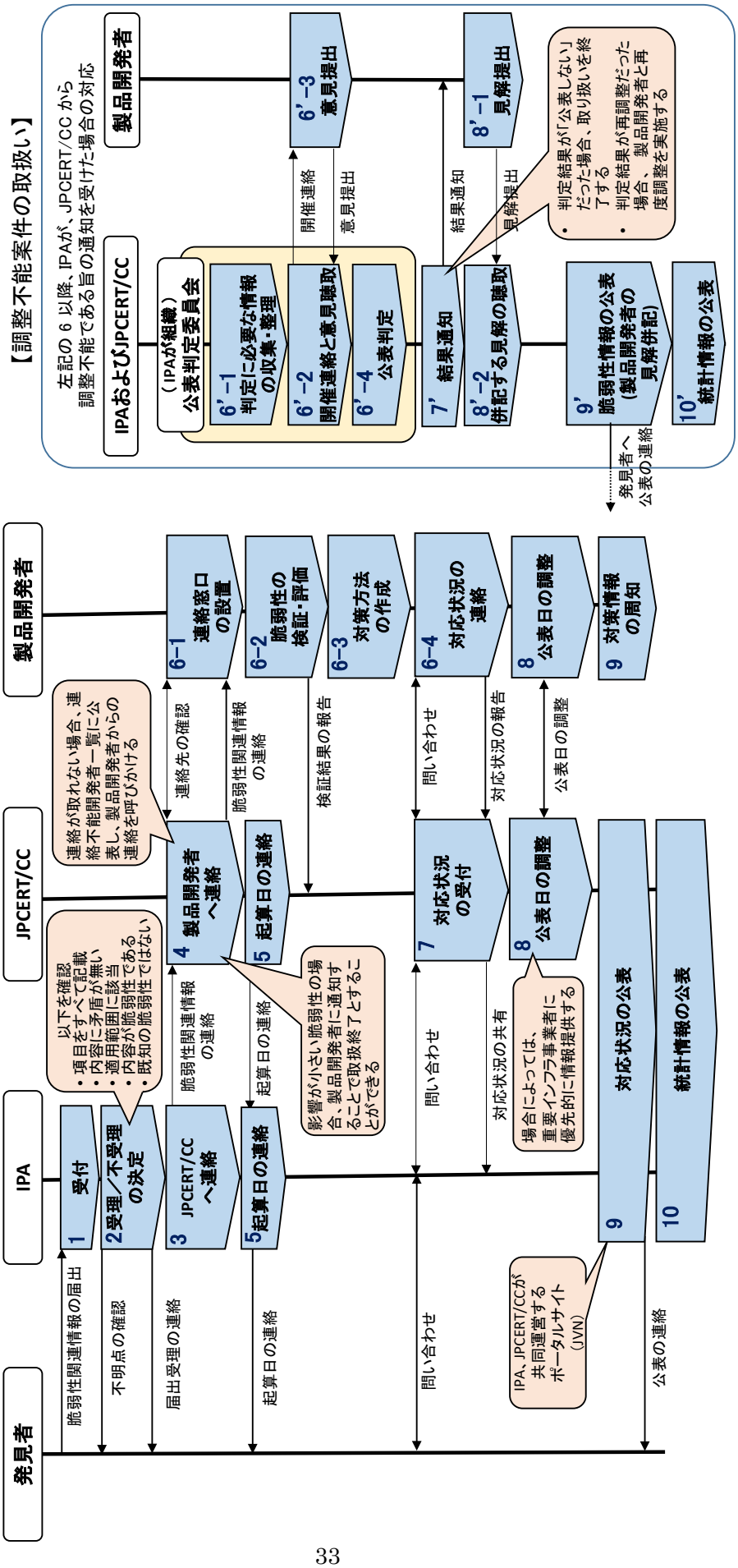
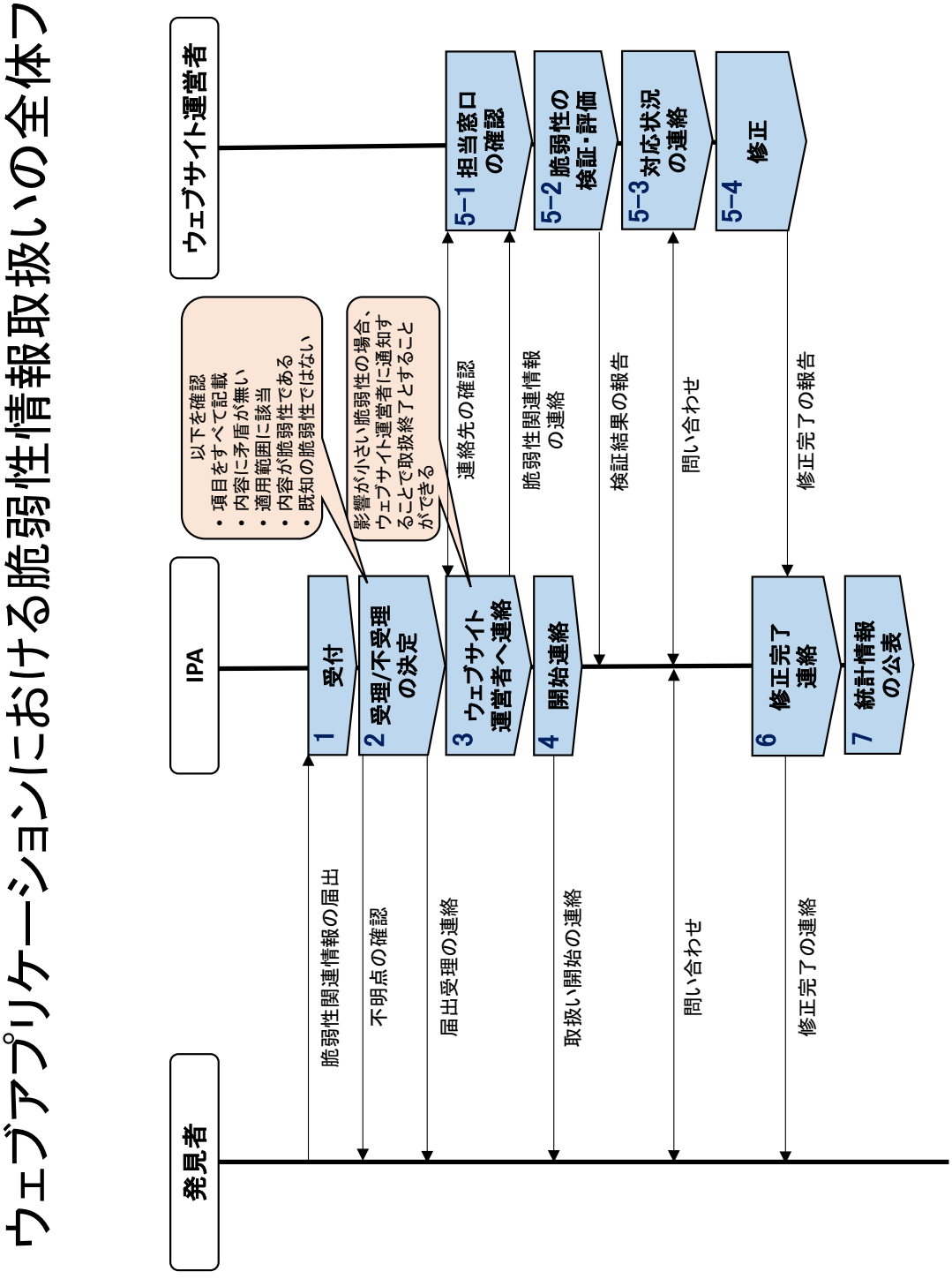


図4　ウェブアプリケーションにおける脆弱性情報取扱いの全体フロー



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）関係する行為と法令の関係

a）ネットワークを用いた不正

・例えば、脆弱性関連情報を利用して、アクセス制御機能を回避し、インターネット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。

・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。

・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。

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。

（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。

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。

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。
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。）

（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。

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。

1) 脆弱性についての調査・報告は、その率直な交換により、ソフトウエアやウェブアプリケーションシステムのセキュリティが結果として強化され・向上するという側面があります。
2) しかしながら、その情報については、悪用というデメリットがあるので、その点についての十分な配慮がなされるべきであり、その一つの方向性を提唱するのが、このガイドラインといえます。
3) また、情報自体そのような性格をもつので、発見者についても脆弱性関連情報の管理および開示について真摯な態度が必要とされます。

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

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。

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

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

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。

(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。

(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。

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４１

５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。

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

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

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。

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。

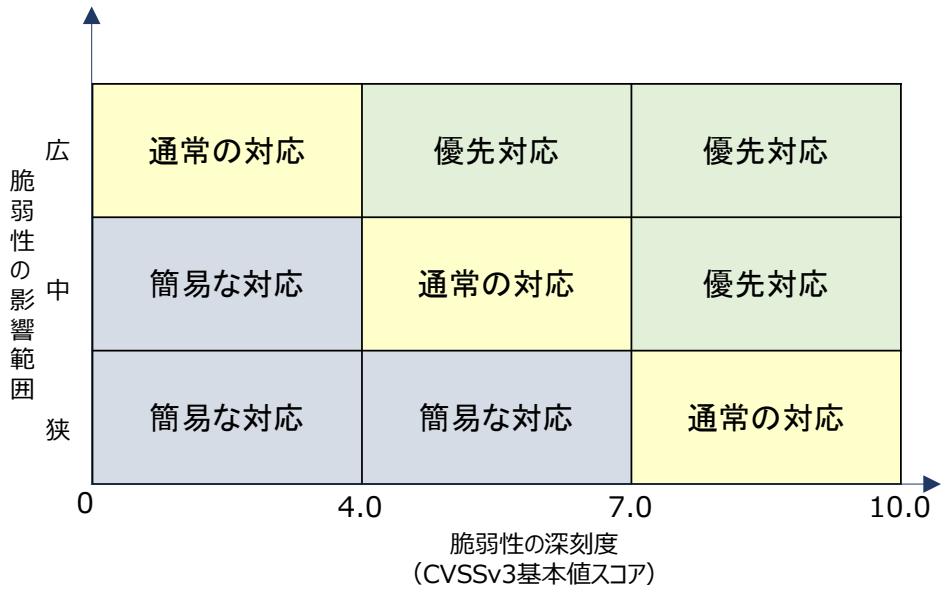
3) この場合、ウェブサイト運営者において、上記のセキュリティ維持等について過失がある場合、その過失による損害賠償の責めを免れるような規定は、消費者契約法上、全部免責の規定については無効となることがあります。

付録４　脆弱性の影響度に関する考え方について

脆弱性の「影響度」に関する考え方は、関係者から得られた情報や IPA・JPCERT/CC が把握している情報を勘案し、IPA および JPCERT/CC が総合的に判断した脆弱性の深刻度（CVSSv3 基本値スコア）と影響範囲により決定します。

ソフトウエア製品の脆弱性、ウェブアプリケーションの脆弱性のいずれも下記の考え方で実施します。ただし、ウェブアプリケーションについては、これまでの経緯を踏まえ、CVSSv3 基本値スコアが「4.0 ～ 6.9」でかつ脆弱性の影響範囲が中の場合でも、受動型の攻撃であれば、取扱いを終了することを可能とします。

影響度の考え方



脆弱性の深刻度　：脆弱性の深刻度として、CVSSv3 基本値スコアを適用する。

脆弱性の影響範囲：以下の要素を勘案して選択する。①～③がすべて不明の場合は「広」と判断する。

①利用者数

当該ソフトウエアの利用者数。

②社会的影響力

重要インフラ等でも取扱っていると思われるソフトウエア製品の脆弱性である。

③攻撃の容易性

攻撃コードの公表、または実際の攻撃の発生が確認された場合に「広」と判断する。届出についての取扱いを判断する時点の情報で判断を行う。

付録５　ソフトウエア製品における連絡不能案件の取扱いについて

１　連絡不能開発者一覧の公表[11]

製品開発者名や製品開発者を特定できるような情報を公表することで、掲載された製品開発者からの連絡を求めていることを周知します。想定読者は、製品開発者本人です。

製品開発者情報　公開調査

概要
IPA（独立行政法人 情報処理推進機構）および JPCERT コーディネーションセンターでは、情報セキュリティ早期警戒パートナーシップに基づいて届出られたソフトウエア製品の製品開発者、またはその関係者からのご連絡を求めています。

調査対象
情報セキュリティ早期警戒パートナーシップに基づいて届けられたソフトウエア製品で、インターネット等から入手しうる情報では連絡が取れない、以下の一覧に掲載されている製品開発者、またはその関係者が調査対象です。

連絡先
Subject に問い合わせ番号を明記し jvn@jvn.jp 宛に、ご連絡ください。

連絡不能開発者一覧

問合せ番号	開発者名	関連情報	一覧追加日	製品情報	備考
DID#AAAA	AAA	－	YYYY/MM/DD	－	－
DID#BBBB	BBB	－	YYYY/MM/DD	－	－
DID#CCCC	－	－	YYYY/MM/DD	－	XXXXX の製品開発者
DID#DDDD	－	http://ddd	YYYY/MM/DD	YYYY/MM/DD（開示）	YYYYY の製品開発者
DID#EEEE	EEE	http://eee	YYYY/MM/DD	YYYY/MM/DD（開示）	ZZZZZ の製品開発者

[11] 連絡不能開発者一覧　https://jvn.jp/reply/index.html

２　対象製品情報の公表と関係者へのお願い

製品開発者名や製品開発者を特定できるような情報に加えて、具体的な対象製品の名称やバージョンを公表することで、製品開発者だけでなく、製品関係者からの連絡を求めていることを周知します。想定読者は、製品開発者本人、または製品開発者との連絡方法を知っている方です。

【対象が官庁、法人の場合】

XXXXX の製品開発者に関する情報 製品名ｘｘｘ、バージョン xxxx の作者、または著作権を有している製品開発者の方、または販売代理店等、本製品に関係する方は下記の宛先までご連絡をお願いします。 連絡先： jvn@jvn.jp 公開日：yyyy 年 mm 月 dd 日

【対象が官庁、法人の場合（連絡期限追記）】

XXXXX の製品開発者に関する情報 製品名ｘｘｘ、バージョン xxxx の作者、または著作権を有している製品開発者の方、または販売代理店等、本製品に関係する方は下記の宛先までご連絡をお願いします。 本件に関するご連絡は、yyyy 年 mm 月 dd 日まで受け付けます。 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取れないため連絡不能と判断し、「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」の記載に準じて取り扱います。 連絡先： jvn@jvn.jp 公開日：yyyy 年 mm 月 dd 日 更新日：yyyy 年 mm 月 dd 日（連絡期限追記）

【対象が個人、コミュニティの場合】

XXXXX の製品開発者に関する情報
製品名ｘｘｘ、バージョン xxxx の作者、または著作権を有している製品開発者の方、または製品開発者との連絡方法をご存じの方は下記の宛先までご連絡をお願いします。また、同製品の派生・関連製品のコミュニティに所属する製品開発者の方で、修正版の提供が可能な方からのご連絡もお待ちしています。
連絡先： jvn@jvn.jp
公開日：yyyy 年 mm 月 dd 日

【対象が個人、コミュニティの場合（連絡期限追記)】

XXXXX の製品開発者に関する情報

製品名ｘｘｘ、バージョン xxxx の作者、または著作権を有している製品開発者の方、または製品開発者との連絡方法をご存じの方は下記の宛先までご連絡をお願いします。また、同製品の派生・関連製品のコミュニティに所属する製品開発者の方で、修正版の提供が可能な方からのご連絡もお待ちしています。
本件に関するご連絡は、yyyy 年 mm 月 dd 日まで受け付けます。

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取れないため連絡不能と判断し、「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」の記載に準じて取り扱います。

連絡先： jvn@jvn.jp
公開日：yyyy 年 mm 月 dd 日
更新日：yyyy 年 mm 月 dd 日（連絡期限追記）

付録６　ソフトウエア製品の脆弱性の取扱いに関する国際標準への対応

1.　ソフトウエア製品の脆弱性の取扱いに関する国際標準とベンダ

ソフトウエア製品の脆弱性の取扱いに関する国際標準として、ISO/IEC 29147:2014 (vulnerability disclosure)、ISO/IEC 30111:2013 (vulnerability handling processes)が規格化されました。

今後、我が国のベンダがグローバルな事業展開を図る場合には、これらの国際標準に対応する必要性が高まります。例えば、海外の調達案件等において、顧客側から脆弱性対応に関する取組みについて説明を要求された場合、ベンダとして国際標準に対応した体制・取組みを行っていることを説明することで、円滑な理解が得られると考えられます。

また、自身の脆弱性の公開ポリシーを公表することで、発見者の協力を得る効果も期待できます。

2.　国際標準の概要

ISO/IEC 29147:2014 はソフトウエア製品に係る事業者（製品開発者、オンラインサービス事業者（4.(1)を参照)、中間ベンダ（4.(4)を参照）等を指す。以下、「ベンダ」という。）の脆弱性に関する社外とのやりとり（外部からの脆弱性に関する情報の受領、ユーザに対する脆弱性対策のアドバイザリ配布等）を規定しています。一方、ISO/IEC 30111:2013 はベンダの社内での脆弱性取扱いのプロセス（脆弱性の検証、脆弱性対策の開発等）の指針を提供します。

これらの関係を次の図に示します。

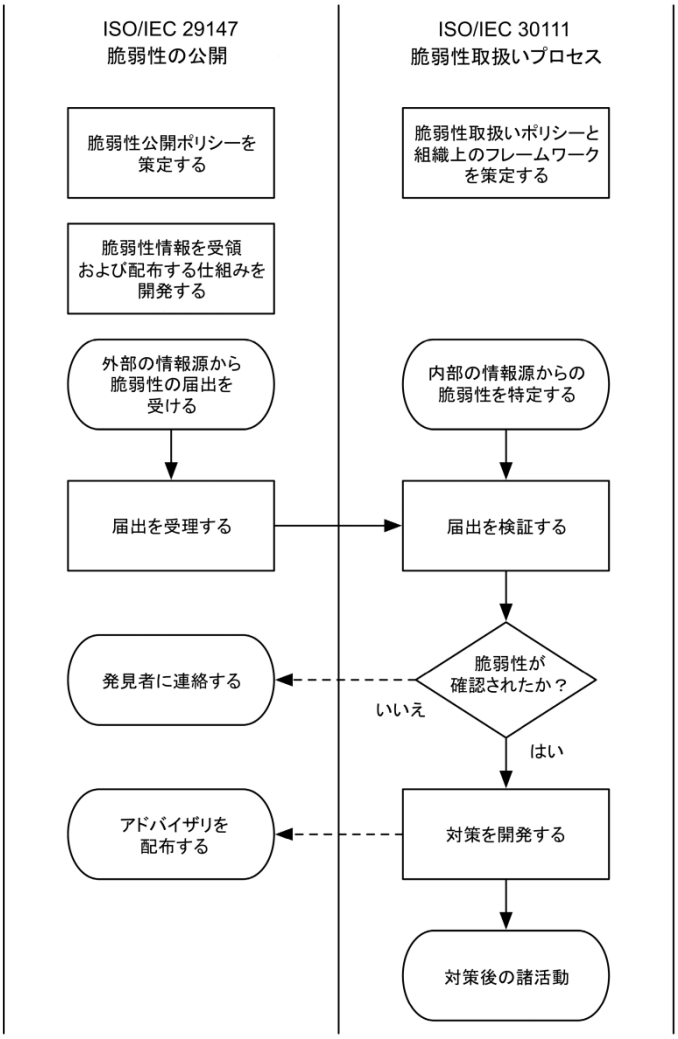


図 1　ISO/IEC 29147 と ISO/IEC 30111 の対応

（出所：ISO/IEC 29147:2014 を元に作成）

3. 情報セキュリティ早期警戒パートナーシップと国際標準の関係

これらの国際標準は、情報セキュリティ早期警戒パートナーシップの取組みと比較して、大きな矛盾や不整合はありません。したがって、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）に沿って脆弱性を取り扱っているベンダが国際標準に対応することも可能です。

ただし、ISO/IEC 29147:2014 への対応については、細かいレベルで留意すべき事項が指摘されています。そこで、本資料では、P ガイドラインに対応しているベンダが ISO/IEC 29147:2014 にも対応しようとする場合に留意すべき事項について補足します。

4.ISO/IEC 29147:2014 について留意すべき事項

P ガイドラインに対応しているベンダが ISO/IEC 29147:2014 にも対応しようとする場合に留意すべき事項についてまとめると、次のようになります。

留意すべき事項	ISO/IEC 29147 対応に取り組む場合の留意点
全体	・グローバルな事業展開を図るベンダにおいては、脆弱性取扱いについて国際標準に対応していることを顧客に説明する必要性が高まっていることがヒアリング調査から裏付けられた。
オンラインサービス	・脆弱性対策を適用したことについて、文書化し記録として残す。 ・クラウド事業者の場合、顧客の利用環境への影響を考慮し、ソフトウエアの更新については事前に周知することが重要。
脆弱性公開ポリシー	・脆弱性公開ポリシーを策定し、その一部を公開する。 ・脆弱性公開ポリシーには、ベンダへの連絡方法、セキュアな通信オプション、予想されるやり取りの説明、脆弱性と思われる届出を行う際に役立つ可能性がある情報、範囲外のサービス、届出をどうやって追跡するかを含める。 ・脆弱性公開ポリシーの一部を公開することにより、発見者から直接脆弱性が届け出られる可能性も高まる。 ・届け出られた脆弱性が他のベンダの供給する部品に内包されているケースも考えられるため、そうした場合の対応についてもあらかじめ検討しておく。
脆弱性の受領	・脆弱性公開ポリシーに則り、発見者や調整機関から脆弱性の届出を受け付ける対外的な窓口を用意する。 ・その上で、脆弱性の届出を受信した際には、受信した旨を 7 日以内に返信する。 ・お盆、正月等の長期休暇の際は、7 日以内に対応するのが難しい可能性がある。
中間ベンダ	・ベンダは、中間ベンダに求められる対応（脆弱性の問題の切り分け、他のベンダとの調整を行うこと、発見者・調整機関に調整状況と今後の進め方について説明すること）に取り組む。 ・中間ベンダとして他のベンダの商材を扱う場合、それらに自社の脆弱性対応基準を適用するのは難しく、実際には対応を要請するに留まることが多い。 ・クラウド事業者によっては、パートナー向けに審査基準を公開し、それに準拠するよう要請しているケースもある。

以下に、これらの詳細について説明します。

(1) オンラインサービス

ISO/IEC 29147:2014 における「オンラインサービス」についての記載を引用します。

章・節	内容
3 Terms and definitions 3 用語と定義	3.4 online services service which is implemented by hardware, software, or a combination of them and provided over a communication line or network Note 1 to entry: The vendor of an online service may also be referred to as a service provider. Online services are similar to products in that both are primarily software systems. Two main distinctions are that a service often appears to users as a single instance of software and that users do not install, manage, or deploy the software, but they only use the service. 3.4 オンラインサービス ハードウエア、ソフトウエアまたはその組み合わせによって実装され、通信回線またはネットワーク経由で提供されるサービス 注記１　オンラインサービスのベンダは、サービスプロバイダと呼ばれることもある。オンラインサービスと製品は、両者とも主にソフトウエアシステムであるという点で似ている。両者の主な違いは、サービスはユーザにとって１つのソフトウエアのように見えるという点と、ユーザはソフトウエアのインストール、管理または展開を行わず、サービスを利用するだけという点である。
5.5 Vulnerability disclosure process summary 5.5 脆弱性公開プロセスの要約	5.5.4 Release phase The vendor deploys the remediation. In an online service, the vendor deploys the remediation and documents the event. 5.5.4 公開フェーズ ベンダは対策を展開する。オンラインサービスの場合、ベンダは対策を展開し、その事象について文書化して記録として残す[12]。

（出所：ISO/IEC 29147:2014 を元に作成）

表中 3.4 節の定義から、オンラインサービスの事業者には、クラウド事業者、EC モール事業者、ウェブサイト運営者等が含まれます。オンラインサービスの場合、P ガイドライン上は対策の適用以上の取組みを求めていません[13]。しかし、オンラインサービス事業者が何らかの理由で ISO/IEC 29147:2014 対応に取り組む場合、脆弱性対策を適用したことについて、文書化し記録として

[12] 必ずしも「公表」を意味しているわけではない。
[13] 個人情報漏えい等の事案が起きた可能性がある場合は、二次被害を防止するため、公表を要請している。

残すことが望まれます。さらにクラウド事業者の場合、顧客の利用環境への影響を考慮し、ソフトウエアの更新については事前に周知することが重要です。

(2) 脆弱性公開ポリシー

ISO/IEC 29147:2014 における「脆弱性公開ポリシー」についての記載を引用します。

章・節	内容
6 Vulnerability disclosure policy considerations 6 脆弱性公開ポリシーに関する考察	6.1 General Vendors should define their responsibilities in the vulnerability disclosure policy. Vendors should publicize their vulnerability disclosure policy or point to an existing public vulnerability disclosure policy. 6.1 概要 ベンダは、脆弱性公開ポリシーにおける責任を定義する必要がある。ベンダは、自身の脆弱性公開ポリシーを公表する、もしくは、既存の一般的な脆弱性公開ポリシーを示す必要がある。
	6.2 Minimum policy aspects A vendor should create an overall vulnerability disclosure policy, but they may choose to publicize only select sections if the internal policy contains sensitive information. A vulnerability disclosure policy should, at least, include information about the following. a) How the vendor would like to be contacted Vendors who adopt a policy of vulnerability disclosure will typically offer a security website or page. This website/page provides information on the vendor's accepted method(s) for receiving vulnerability information from a finder. Contact information might include one or more of the following: 1) E-mail address;(例示は省略) 2) Phone number; 3) Web form. (以下タイトルのみ抜粋) b) Secure communication options c) Setting communication expectations d) Information that would be useful when submitting a possible vulnerability report e) Out-of-scope services f) How submitted reports are tracked

	6.2 最小限の要素 ベンダは脆弱性公開ポリシーを策定するが、ポリシーが機微な情報を含むこともあるため、公開するのはその一部だけとしてもよい。 脆弱性公開ポリシーは、少なくとも以下の情報を含める： a) どのようにベンダに連絡して欲しいか 脆弱性公開ポリシーを採用するベンダは、一般的にセキュリティのウェブサイトやページを提供する。このウェブサイト/ページは発見者から脆弱性情報を受信するためにベンダが認めた方法（複数可）に関する情報を提供する。問合せ先は、次の一項目以上含めることが望ましい： 1) 電子メールアドレス 2) 電話番号 3) ウェブフォーム b) セキュアな通信オプション c) 予想されるやり取りの説明 d) 脆弱性と思われる届出を行う際に役立つ可能性がある情報 e) 範囲外のサービス f) 届出をどうやって追跡するか
	6.3 Optional policy aspects A vulnerability disclosure policy may contain multiple optional elements. a) Credit to finder b) Synchronized public disclosure c) Distribution 6.3 オプショナルなポリシーの要素 脆弱性公開ポリシーには、複数のオプション情報を含めてもよい。 a) 発見者の功績 b) 一般公開の同期 c) 配布

（出所：ISO/IEC 29147:2014 を元に作成）

P ガイドラインでは、ベンダに脆弱性公開ポリシーの策定を求めていませんが、ISO/IEC 29147:2014 では、脆弱性公開ポリシーを策定することや、その一部を公開することを求めています。

したがって、ベンダが何らかの理由で ISO/IEC 29147:2014 対応に取り組む場合、

・脆弱性公開ポリシーを策定し、その一部[14]を公開すること
・脆弱性公開ポリシーには、ベンダへの連絡方法、セキュアな通信オプション、予想されるやり取りの説明、脆弱性と思われる届出を行う際に役立つ可能性がある情報、範囲外のサービス、届出をどうやって追跡するかを含

[14] どこまで公開すべきか判断が難しい可能性もあるため、先行事例を巻末に添付する。

めること

が望まれます。中でもベンダへの連絡方法は公開する必要があるでしょう。また、脆弱性公開ポリシーの一部を公開することにより、発見者から直接脆弱性が届け出られる可能性も高まります。

さらに、届け出られた脆弱性が他のベンダの供給する部品に内包されているケースも考えられるため、そうした場合の対応についてもあらかじめ検討しておくべきでしょう。

(3) 脆弱性の受領

ISO/IEC 29147:2014 における「脆弱性の受領」についての記載を引用します。

章・節	内容
7 Receipt of vulnerability information 7 脆弱性情報の受領	7.3 Acknowledgement of receipt from finder or a coordinator The vendor should respond to a vulnerability report within the time period specified in the vendor's vulnerability disclosure policy. It is recommended that an acknowledgement of receipt of a vulnerability report be provided to a finder within seven calendar days. 7.3 発見者や調整機関からの受領の確認 ベンダは、自身の脆弱性公開ポリシーの中で規定した期間以内に、脆弱性の届出に対処する。脆弱性届出を受領した旨の連絡は、発見者に対し暦で 7 日以内に行うことが推奨される。

（出所：ISO/IEC 29147:2014 を元に作成）

ISO/IEC 29147:2014 の「受領」は、その内容には言及せず、単に受信した旨を返信する作業を指しています。例えば、IPA では、受信した旨を発見者に返信する「受信連絡」という作業がありますが、これが該当します。このような作業はできるだけ迅速に行うことが望まれます。

したがって、ベンダが何らかの理由で ISO/IEC 29147:2014 対応に取り組む場合、まず、脆弱性公開ポリシーに則り、発見者や調整機関から脆弱性の届出を受け付ける対外的な窓口を用意すること、その上で、脆弱性の届出を受信した際には、受信した旨を 7 日以内に返信することが必要となります。

なお、お盆、正月等の長期休暇の際は、対応が難しい可能性があるので、留意が必要です。

(4) 中間ベンダ

ISO/IEC 29147:2014 における「中間ベンダ」についての記載を引用します。

章・節	内容

5.4 Stakeholders 5.4 利害関係者	5.4.3 Intermediate Vendor An intermediate vendor gets a subsystem from a vendor and uses it to supply a system or service (or a combination of both) to a user (or another intermediate vendor). Typical examples are the following: a) system houses that use a PC and an operating system to add their own healthcare administration software and sell the combined system to a medical doctor (maybe together with a maintenance contract); b) telecommunication providers that supply a mobile phone together with a service contract. 5.4.3 中間ベンダ 中間ベンダは、ベンダからサブシステムを入手し、それを使ってシステムまたはサービス（または両方の組み合わせ）をユーザ（または他の中間ベンダ）に提供する。典型的な例では次のようなものがある： 1）PC や OS と自社のヘルスケア管理ソフトウエアを合わせ、統合したシステムを医師に販売する（保守契約も一緒に提供することも）システムハウス; 2）携帯電話本体とサービス契約を合わせて提供する通信事業者。
7 Receipt of vulnerability information 7 脆弱性情報の受領	7.5 On-going communication with finder Vendors should evaluate the reported issue and make a determination whether it represents a vulnerability or not. The vendor should inform the finder and coordinator, if involved, on the results. An intermediate vendor should check whether it can decide on the potential vulnerability on its own or needs to involve the vendor it got the related subsystem from. If another vendor needs to be involved in the decision and if this delays the response, the intermediate vendor should inform the finder and/or the coordinator about this fact and about the further processing. 7.5　発見者との進行中のやり取り ベンダは届出を受けた問題を評価し、脆弱性かそうでないかを判断しなければならない。ベンダは、結果について発見者に（もし調整機関が関与していれば調整機関にも）知らせる。 中間ベンダは、潜在的な脆弱性に関して自身で判断できるか、関連するサブシステムを購入したベンダを巻き込む必要があるか、確認しなければならない。他のベンダの関与を必要とし、そのために回答が遅れる場合、中間ベンダは発見者および／または調整機関にその事実と今後の進め方について知らせる。

（出所：ISO/IEC 29147:2014 を元に作成）

中間ベンダとは、ユーザと対策を策定するベンダの間に介在するベンダであり、SIer やリセラーが該当する場合も、組み込みベンダが該当する場合もあります。例えば、自社が提供するプラットフォーム上で別のパートナーがサービスを行っているケースも該当すると考えられます。大半のベンダに中間ベンダとなる可能性があるため、中間ベンダへの要請は、実質的にはベンダ全体への

要請と考えることができます。ユーザや発見者から見えるのは中間ベンダなので、それらが対応すべき取組みを明確にすることは有益といえます。

Pガイドラインでは、「中間ベンダ」を定義しておらず、中間ベンダに求められる対応についても明示していません。

しかし、ベンダが何らかの理由でISO/IEC 29147:2014対応に取り組む場合には、ベンダは、中間ベンダに求められる対応（脆弱性の問題の切り分け、他のベンダとの調整を行うこと、発見者・調整機関に調整状況と今後の進め方について説明すること）に取り組むことが望まれます。

ただし、中間ベンダとして他のベンダの商材を扱う場合、それらに自社の脆弱性対応基準を適用するのは難しく、実際には対応を要請するに留まることが多いと考えられます。それでも、クラウド事業者によっては、パートナー向けに審査基準を公開し、それに準拠するよう要請しているケースもあります。

参考１ ISO/IEC 29147:2014 と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対応

ISO/IEC 29147:2014 の構成	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改訂案の対応箇所
1.適用範囲	Ⅲ．本ガイドラインの適用の範囲
2.引用規格	―
3.用語および定義	Ⅱ．用語の定義と前提
4.略語	―
5.概念 5.1　一般 5.2　ISO/IEC 29147: 脆弱性の公開と ISO/IEC 30111: 脆弱性取扱プロセスの間のインタフェース 5.3　製品とオンラインサービス 5.4　ステークホルダー 5.5　脆弱性公開プロセスの概要 5.6　脆弱性公開時における情報交換 5.7　交換情報の機密性 5.8　脆弱性アドバイザリ 5.9　脆弱性の悪用	Ⅰ．はじめに 1．本ガイドラインの目的 2．本ガイドラインの想定する読者 Ⅳ．ソフトウエア製品に係る脆弱性関連情報取扱 1．概要
6.脆弱性公開ポリシーにおける考慮事項 6.1 全般 6.2 最小限のポリシーの要素 6.3 オプショナルなポリシーの要素	―
7.脆弱性情報の受理 7.1 全般 7.2 潜在的な脆弱性報告およびその安全な受信モデル 7.3 発見者または調整機関からの受理確認 7.4 入ってくる報告の追跡 7.5 発見者との進行中の通信 7.6 詳細情報 7.7 調整機関からの支援	Ⅳ．ソフトウエア製品に係る脆弱性関連情報取扱 5．製品開発者の対応 1）窓口の設置 2）脆弱性検証の実施 3）脆弱性情報の一般への公表日の調整 4）発見者との直接の情報交換 5）関連ウェブサイトに関する情報の取扱い 6）問い合わせへの対応 7）対策方法および対応状況の連絡

8.ベンダ間における脆弱性の報告 8.1 全般 8.2 ベンダ間の脆弱性報告を求める典型的なケース 8.3 他ベンダに対する脆弱性情報の報告	ー
9.アドバイザリの配布 9.1 全般 9.2 アドバイザリの目的 9.3 アドバイザリの公開における配慮 9.4 アドバイザリのリリースのタイミング 9.5 アドバイザリの内容 9.6 アドバイザリの通信 9.7 アドバイザリのフォーマット 9.8 アドバイザリの真正性	Ⅳ. ソフトウエア製品に係る脆弱性関連情報取扱 5. 製品開発者の対応 8)対応方法の周知 9)製品開発者内の情報の管理
付録 A.（補足情報）脆弱性／アドバイザリ情報の取扱いに関する詳細 付録 B.（補足情報）ポリシー、アドバイザリ、国際的な調整機関の事例 文献目録	ー

参考 2 脆弱性公開ポリシーの事例

脆弱性公開ポリシーは、ISO/IEC 29147:2014 の Annex B の”B.1 Sample vulnerability disclosure policy”に例示されているが、既に国内外のベンダから開示されている事例も見られる。以下にそれらの参考例を示す。

■Cisco; “Security Vulnerability Policy”
https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html

■IBM; “Report Security Vulnerabilities”
https://www.ibm.com/security/secure-engineering/report.html

■Microsoft; “Coordinated Vulnerability Disclosure”
https://www.microsoft.com/en-us/msrc/cvd

■Salesforce.com;
「セールスフォース・ドットコムの脆弱性報告ポリシー」
https://www.salesforce.com/jp/company/disclosure/
「Force.com ISV セキュリティレビュー」
https://developer.salesforce.com/page/JP:Security_Review

■サイボウズ; 「脆弱性情報ハンドリングポリシー」
https://cybozu.co.jp/company/security-policy/

■日立製作所; 「日立グループにおける製品脆弱性情報の開示プロセス」
http://www.hitachi.co.jp/hirt/publications/hirt-pub10008/index.html

■GMO ペパボ; 「脆弱性報告制度」
http://pepabo.com/contact/vulnerability_reporting/

付録７　本ガイドラインの別冊・関連資料一覧

【別冊】

「ソフトウエア製品開発者による脆弱性対策情報の公表マニュアル」[15]

利用者に脆弱性関連情報が的確に届けられることを目標として、ソフトウエア製品開発者向けに、脆弱性対策情報の望ましい公表の手順について方針を示す資料です。

「ウェブサイト運営者のための脆弱性対応ガイド」[15]

ウェブサイト運営者向けに、ウェブサイトの脆弱性対策の必要性や脆弱性対応の手順を紹介する資料です。

「ウェブサイト構築事業者のための脆弱性対応ガイド」[15]

ウェブサイトの構築に係る方向けに、納入前と納入後に分けてウェブサイトの脆弱性対策のポイントを紹介する資料です。

「セキュリティ担当者のための脆弱性対応ガイド」[15]

企業等において情報システムのセキュリティ管理を担当する方向けに、脆弱性対策の基本的な考え方を紹介する資料です。

「制御システム利用者のための脆弱性対応ガイド」第３版[15]

工場やプラントにおける制御システムの導入・運用を行う企業の経営層・管理者の方向けに、セキュリティ対策や脆弱性対応を紹介する資料です。

【関連資料】

「平成二十九年経済産業省告示第十九号　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」[16]

旧告示「ソフトウエア等脆弱性関連情報取扱基準」が廃止となり、新たに定められた告示です。

「情報セキュリティ早期警戒パートナーシップの紹介
－ 脆弱性取扱プロセスの要点解説 －」[15]

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概要版として作成した資料です。

---

[15] https://www.ipa.go.jp/security/vuln/index.html
[16] http://www.meti.go.jp/policy/netsecurity/vul_notification.pdf

「Information Security Early Warning Partnership
- Overview of Vulnerability Handling Process -」[15]

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概要版を英訳した資料です。

「JPCERT/CC 脆弱性関連情報取扱いガイドライン」[17]

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」および IPA と JPCERT/CC による「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」に対応して、製品開発者の方々に、脆弱性関連情報の取扱いに関する事項をお知らせすることを目的として作成された資料です。

「製品開発ベンダーにおける脆弱性関連情報取扱に関する体制と手順整備のためのガイドライン」[18]

システムベンダを中心とする製品開発者が、発見者や調整機関から入手した脆弱性関連情報を社内的にどのように取り扱い、対応すべきか、必要な体制と手順を整備するために、JEITA および JISA がとりまとめた資料です。

「SI 事業者における脆弱性関連情報取扱に関する体制と手順整備のためのガイダンス」[19]

SI 事業者が、脆弱性情報が公表された後、製品開発ベンダや顧客と連携し、迅速かつ適切な対応をとるために必要な社内体制や対応手順を整備するために、JISA および JEITA がとりまとめた資料です。

「製品開発ベンダーにおける脆弱性関連情報取扱に関する体制と手順整備のためのガイドライン」[20]

PC ソフトウエアを中心とする製品開発者が、発見者や調整機関から入手した脆弱性関連情報を社内的にどのように取り扱い、対応すべきか、必要な体制と手順を整備するために、JPSA（現 CSAJ）がとりまとめた資料です。

[17] https://www.jpcert.or.jp/vh/vul-guideline2014.pdf
[18] http://it.jeita.or.jp/infosys/info/0407JEITA-guideline/guideline-v10.pdf
[19] https://www.ipa.go.jp/files/000002992.pdf
[20] http://www.csaj.jp/info/04/20041203_security.html

・脆弱性関連情報流通の基本枠組み

独立行政法人情報処理推進機構（IPA）では、経済産業省告示を踏まえ、2004 年 7 月からソフトウエア製品およびウェブアプリケーションの脆弱性に関する届出を受け付けています。

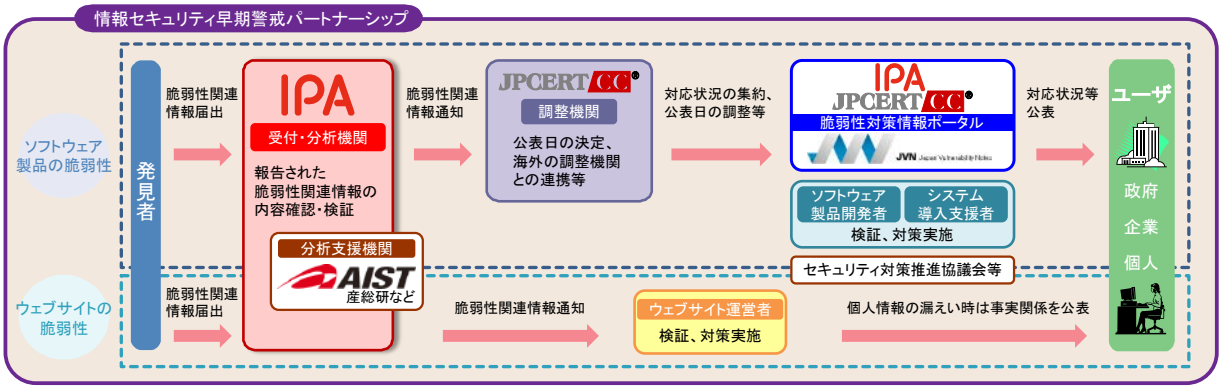
https://www.ipa.go.jp/security/vuln/report/index.html

（参考）

「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」（平成 29 年経済産業省告示第 20 号）

「情報セキュリティ早期警戒パートナーシップ」



※IPA:独立行政法人情報処理推進機構, JPCERT/CC:一般社団法人　JPCERTコーディネーションセンター、産総研：国立研究開発法人産業技術総合研究所

・本資料のダウンロード先

本資料の配布に制限はありません。本資料は、次の URL からダウンロードできます。

https://www.ipa.go.jp/security/ciadr/partnership_guide.html

https://www.jpcert.or.jp/vh/#link_japan

・本資料に関するお問合わせ先

独立行政法人情報処理推進機構（略称：IPA）　セキュリティセンター

〒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 16 階

https://www.ipa.go.jp/security/　TEL: 03-5978-7527　FAX: 03-5978-7552

一般社団法人　JPCERT コーディネーションセンター（略称：JPCERT/CC）

〒103-0023　東京都中央区日本橋本町 4-4-2　東山ビルディング 8 階

https://www.jpcert.or.jp/　TEL: 03-6271-8901　FAX 03-6271-8908

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

２００４ 年 ７ 月 ８ 日 制定第１版発行
２００５ 年 ７ 月 ８ 日 改訂第２版発行
２００６ 年 ９ 月 １ 日 改訂第３版発行
２００７ 年 ６ 月１１日 改訂第４版発行
２００８ 年 ４ 月 ４ 日 改訂第５版発行
２００９ 年 ７ 月 ８ 日 改訂第６版発行
２０１１ 年 ３ 月２８日 改訂第７版発行
２０１４ 年 ５ 月３０日 改訂第８版発行
２０１５ 年 ５ 月２２日 改訂第９版発行
２０１６ 年 ５ 月３０日 改訂第１０版発行
２０１７ 年 ５ 月３０日 改訂第１１版発行
２０１９ 年 ● 月●●日 改訂第１２版発行

［著作・制作］　情報システム等の脆弱性情報の取扱いに関する研究会

［事務局・発行］　独立行政法人情報処理推進機構