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
2005 年 7 月 8 日 改訂
2006 年 9 月 1 日 改訂

独立行政法人 情報処理推進機構
有限責任中間法人 JPCERT コーディネーションセンター
社団法人 電子情報技術産業協会
社団法人 日本パーソナルコンピュータソフトウェア協会
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

Ⅰ．本ガイドラインの位置づけ

近年、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洩したりといった、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」が制定されました。

本ガイドラインは、上記告示をふまえ、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など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。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、有限責任中間法人 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御対応くださいますようお願い申し上げます。

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．脆弱性の定義

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得るセキュリティ上の問題箇所です。

なお、ウェブアプリケーションにおいて、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４に示します。）

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
   脆弱性の性質及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です。例えば、エクスプロイトコード（付録４にて述べます）や、コンピュータウイルス等が該当します。

３．対策方法

対策方法は、脆弱性から生ずる問題を回避するまたは解決を図る方法のことであり、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４にて述べます）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４にて述べます）等と呼ばれます。

４．対応状況

調整機関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製品開発者の脆弱性に関する対策方法､取り組みの状況などを含む対応状況のことです。

５．ソフトウエア製品

ソフトウエア自体又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。ただし、オープンソースソフトウエアのように技術情報を統括する企業が一社に定まらないもの、複数の者又は団体によりその改善が行われるものも含みます。具体例は、付録４に示します。

６．オープンソースソフトウエア（OSS）

ソースコードを無償で公開し、誰でも改良や再配布ができるソフトウエアのことです。

７．ウェブアプリケーション

インターネットのウェブサイトなどで、公衆に向けて提供するサービスを構成するシステムで、そのソフトウエアがサイトごとに個別に設計・構築され、一般には配布されていないもののことを指します。

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人を含みます。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などが当てはまります。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、ソフトウエアを開発した企業または個人です。企業の場合それが外国の会社である場合には、そ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など）を指します。

１０．脆弱性検証

脆弱性検証とは、製品開発者が JPCERT/CC から脆弱性関連情報を受け取った際に、該当するソフトウエア製品の有無、およびその新規性の有無を検証する

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、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。当該ウェブアプリケーションが企業や組織によって運営されているのであれば、その企業や組織が該当します。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４に示します。**

III．本ガイドラインの適用の範囲

本ガイドラインの適用の範囲は、脆弱性により不特定多数の人々に被害を及ぼすもので、以下に挙げるものを想定しています。

◯ソフトウエア製品の場合：

・国内で利用されているソフトウエア製品

国内で、多くの人々に利用されている等のソフトウエア製品が該当します。プロトコルを実装しているものも含みます。（プロトコルの実装に係わる脆弱性は付録４に示します。）

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。

◯ウェブアプリケーションの場合：

・主に日本国内からのアクセスが想定されるサイトで稼動するウェブアプリケーション

例えば、主に日本語で記述されたウェブサイトや、URL が「jp」ドメインのウェブサイト等を指します。

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 Web アプリケーション、ユーザ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。

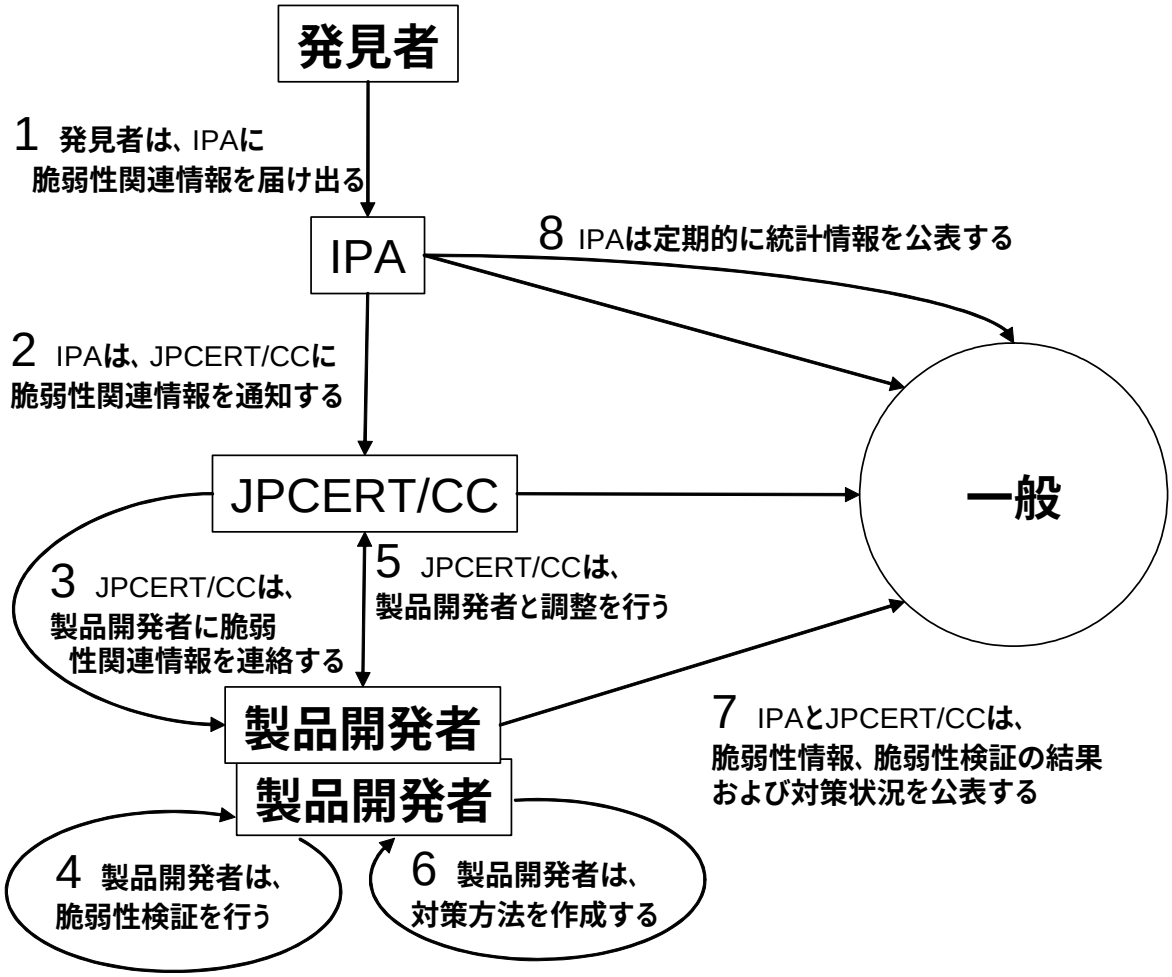

図１　ソフトウエア製品に係る脆弱性関連情報取扱の概要

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、脆弱性情報の公表に関するスケジュール調整

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) IPA および JPCERT/CC は、脆弱性情報と、3)にて JPCERT/CC から連絡した全ての製品開発者の脆弱性検証の結果および対応状況を公表する
8) IPA は、統計情報を少なくとも一年に一度は公表する

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（研究者など）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、自社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、他社のソフトウエア製品に類似の脆弱性があると推定されるものを発見・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１に示します。

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 に届け出ることができます。脆弱性関連情報に関係する製品開発者に対し、同一情報の届出を行う必要はありませんが、届け出ること自体は問題ありません。

4) 脆弱性関連情報の管理および開示

発見者は、IPA と JPCERC/CC が脆弱性情報を公表するまでの間は、脆弱性関連情報が第三者に漏れないように適切に管理してください。ただし、止むを得ず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。
脆弱性関連情報の管理および開示に係わる法的問題に関しては、付録１に示します。

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、http://www.ipa.go.jp/security/vuln/ を参照してください）。

・発見者の氏名・連絡先
・脆弱性関連情報に関連する製品の具体的な名称

・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
・個人情報の取り扱い方法（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）
・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
・対策情報の公表の連絡の必要性　等

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毎の脆弱性検証の結果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。

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。

３．IPA および JPCERT/CC の対応

(1)IPA

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 を御参照ください。
http://www.ipa.go.jp/security/vuln/
受付は 24 時間ですが、作業は原則営業日となります。

2) 届出の受理

IPA は、以下の条件が満たされ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) 原則として、上記２．5)の項目が十分に記述されていること

(イ) 匿名の届出でないこと（発見者への連絡が可能であることを確認できること）
(ウ) 脆弱性関連情報であること（一般のバグ情報ではないこと）
(エ) 既に報告されている脆弱性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時が IPA および JPCERT/CC が脆弱性関連情報の取り扱いを開始した日時となります（(2)　3）一般への公表日の決定　参照)。

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。

5) 脆弱性関連情報の取り扱い

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提供しないように適切に管理します。ただし、脆弱性が再現する状況を特定できない等止むを得ない理由がある場合、IPA は、守秘契約を結んだ上で、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ことがあります。

6) 発見者に係わる情報の取り扱い

IPA は、氏名・連絡先を含む発見者に係わる情報を、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開示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、JPCERT/CC から既知の脆弱性であるまたは脆弱性ではない等の理由により脆弱性情報の公表の中止の連絡を受けた場合、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。

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、第三者に情報が漏洩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わる製品開発者の対応状況を、JPCERT/CC と共有します。

11)優先的な情報提供

IPA は、届出がなされた脆弱性関連情報に関して、重要インフラに対し特に影響が大きいと推察される場合、JPCERT/CC および製品開発者と協議の上、脆弱性情報の一般公表より前に、脆弱性関連情報と対策方法を、政府・行政機関や重要インフラ事業者等に対して優先的に提供することがあります。この際、発見者に対して、その旨を通知します。重要インフラ事業者には、情報通信、金融、航空、鉄道、電力、ガス、医療、水道、物流の各事業者が含まれます。なお、優先的な脆弱性関連情報の提供が情報の漏洩につながると判断される場合は、この限りではありません。

12)一般への情報の公表

IPA および JPCERT/CC は、共同運営する脆弱性対策情報ポータルサイト JP Vendor Status Notes（JVN）を通じて、一般に対し、脆弱性情報と JPCERT/CC から連絡した全ての製品開発者の脆弱性検証の結果と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応状況を受け取った場合、その都度公表します。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。

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 などに関して、システム構築事業者（SI 事業者）やユーザ企業の脆

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、発見者が望む場合、発見者にその旨を通知します。

13)統計情報の集計と公表
IPA は、脆弱性に係わ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少なくとも一年に一度は公表します。統計情報には、届出件数の時間的推移等が含まれます。

(2)JPCERT/CC

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、製品開発者毎に、製品の情報、社名、窓口等を登録します。

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。
また、JPCERT/CC は、OSS に関する事前通知を、開発者コミュニティに加えて、必要に応じて以下へ通知します。
・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）
これは、開発者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、その事実を知りうる手段がないが、社会的影響を考慮すると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、重要インフラ等に深刻な影響

を与え得るものである等、緊急な対応を要すると判断される場合においては、受付の順序に関わらず、優先的に取扱いを行います。
さらに、製品開発者との連絡が取れない場合、JPCERT/CC は、その脆弱性の影響範囲や連絡のとれない期間を考慮して取扱いを終了することがあります。

3) 一般への公表日の決定

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 および IPA が脆弱性関連情報の取り扱いを開始した日時（(1) 2）参照）から起算して、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わるリスク

なお、製品開発者から脆弱性検証の結果の報告がない場合、過去の類似事例を参考にし、JPCERT/CC が公表日を決定することがあります。

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全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 IPA に連絡します。

(ア) 通知を行ったすべての製品開発者から既知の脆弱性情報であるとの連絡を受けた場合
(イ) 通知を行ったすべての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

5) JPCERT/CC における脆弱性関連情報の取り扱い

JPCERT/CC は、脆弱性情報を一般に公表するまでは、第三者に漏洩しないように管理します。ただし、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、海外に大きな影響を与える脆弱性関連情報の場合、および脆弱性関連情報の詳細な分析が必要な場合などは、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ことがあります。

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) 対応状況の受付

JPCERT/CCは、JPCERT/CCから連絡した全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わる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、対応状況をIPAと共有します。

8) 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から連絡した全ての製品開発者の脆弱性検証の結果と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応状況を受け取った場合、その都度公表します。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、JPCERT/CCおよびIPA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。

また、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などに関して、システム構築事業者（SI事業者）やユーザ企業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。

４．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。製品開発者に係わる法的な論点は、付録２に示します。

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。

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、他社のソフトウエア製品に類似の脆弱性があると推定される場合、JPCERT/CC に連絡してください。

3）脆弱性情報の一般への公表日の調整
製品開発者は、自社製品に新たな脆弱性の存在がある場合、脆弱性情報の一般への公表日について JPCERT/CC と相談してください。なお、一般への公表日は、IPA および JPCERT/CC が脆弱性関連情報の取扱いを開始した日時（(1) 2）参照）から起算して、45 日を目安とします。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）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わ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。

6）対応状況の連絡と対策方法の作成
製品開発者は、脆弱性情報の一般の公表日までに、脆弱性関連情報に係わる対応状況を JPCERT/CC に連絡するとともに、脆弱性関連情報に係わる対策方法を作成するよう努めてください。JPCERT/CC に対する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、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。

7）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、それを利用者に周知してください。

8）製品開発者内の情報の管理

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洩しないように管理してください。

５．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、自社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、他社のソフトウエア製品に影響を及ぼさないと認められるものを発見・取得し、調整機関からの通知によることなく、対策方法を作成した場合であっても、ユーザへの周知を徹底するために JPCERT/CC に連絡することが望まれます。この連絡をもって、IPA および JPCERT/CC に連絡したこととみなされます。

2) IPA および JPCERT/CC による普及支援

IPA および JPCERT/CC は、上記 1)の連絡を受け取った、当該脆弱性関連情報及び対策方法を 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。

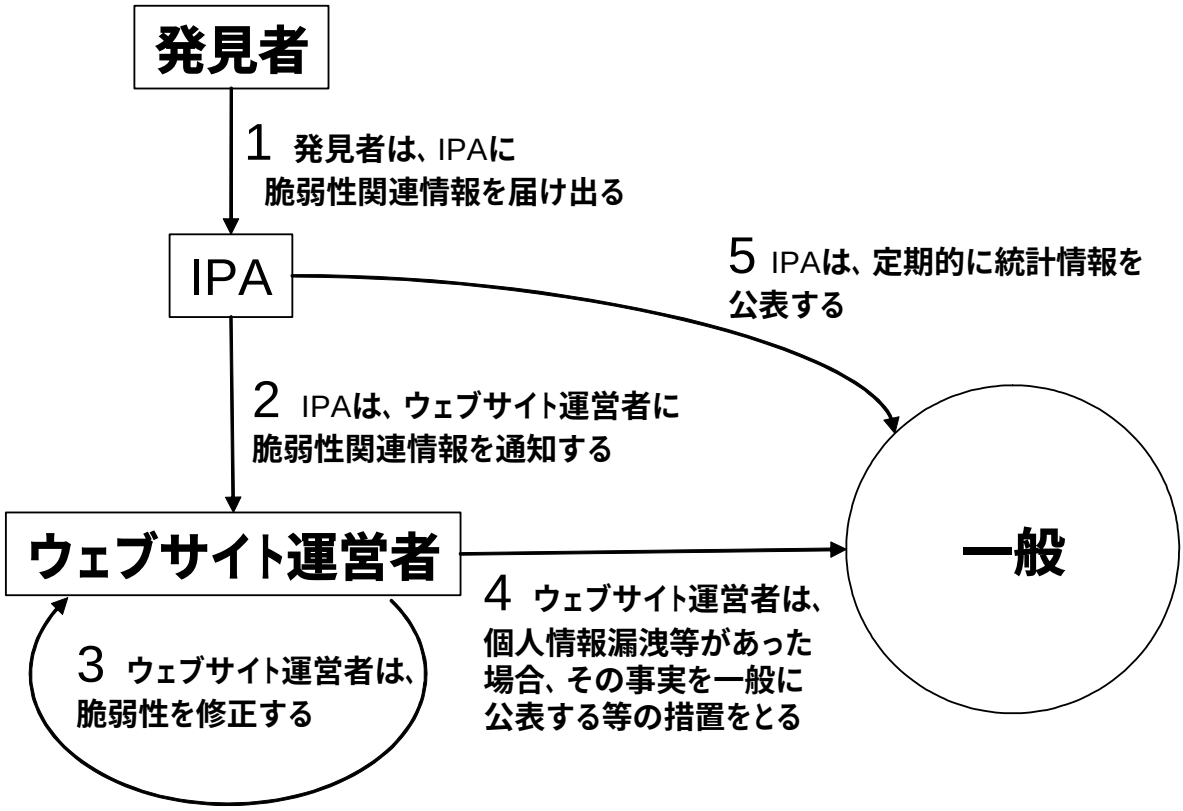

図２　ウェブアプリケーションに係る脆弱性関連情報取扱概要

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) 個人情報漏洩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など適切な処置をとる
5) IPA は、統計情報を少なくとも一年に一度は公表する

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１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 に届け出ることができます。ウェブサイト運営者に対し、同一情報の届出を行う必要はありませんが、届け出ること自体は問題ありません。

3)脆弱性関連情報の管理および開示

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れないように適切に管理してください。また、脆弱性関連情報を開示する場合には、IPA に問い合わせてください。脆弱性関連情報の管理および開示に係わる法的な論点に関しては、付録１に示します。

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、http://www.ipa.go.jp/security/vuln/ を参照してください）。

- 発見者の氏名・連絡先
- 脆弱性関連情報に関連するサイトの URL
- 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
- 個人情報の取り扱い方法（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）
- 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

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しうる情報を連絡することはありません。

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 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 を御参照ください。
http://www.ipa.go.jp/security/vuln/
受付は 24 時間ですが、作業は原則営業日となります。

2) 届出の受理
IPA は、上記２．4)の項目が十分に記述され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。

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発見者に連絡します。

(ア) IPA が脆弱性関連情報でないと確認した場合
(イ) IPA が既に報告されている脆弱性関連情報であると確認した場合
(ウ) ウェブサイト運営者から脆弱性関連情報でないと連絡があった場合
(エ) ウェブサイト運営者から既知の脆弱性関連情報であると連絡があった場合

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。

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) 脆弱性関連情報の管理
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提供しないように適切に管理します。ただし、脆弱性が再現する状況を特定できない等止むを得ない理由により IPA が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ことがあります。この場合、IPA は守秘契約を結びます。さらに、下記 9)に関しては例外とします。

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、JPCERT/CC を介して製品開発者に連絡を行います。この場合、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。

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わる情報を、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開示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、脆弱性に係わ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少なくとも一年に一度は公表します。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

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に示します。
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、脆弱性の内容の検証および脆弱性の及ぼす影響を正確に把握した後、影響の大きさを考慮し、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わ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での情報の管理

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洩しないように管理してください。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。
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、情報を適切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

報が漏洩したなど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。

- **個人情報漏洩の概要**
- **漏洩したと推察される期間**
- **漏洩したと推察される件数**
- **漏洩したと推察される個人情報の種類（属性など）**
- **漏洩の原因**
- **問合せ先**

付録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。脆弱性発見と脆弱性関連情報の管理に関しての記述があります。

１．脆弱性関連情報の発見に際しての法的な問題

（１）関係する行為と法令の関係

a) ネットワークを用いた不正

・例えば、脆弱性関連情報を利用して、アクセス制御機能を回避し、インターネットなどを介してシステムにアクセスした場合には、不正アクセス禁止法に抵触します。

・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 キーの解読など）は、第 159 通常国会にて改正された電波法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などして通常のアクセスをした際に、ブラウザとサーバとの通信の内容を観察したところ、それだけで脆弱性の存在を推定できた場合。
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。

２．脆弱性関連情報の管理に際しての法的な問題

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

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

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

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

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

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

以下があります。

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

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

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

付録２　製品開発者が心得ておくべき法的な論点

法律専門家の見解によると、製品開発者における法的な位置付けは、以下の通りです。

(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４１５条）、不法行為責任（民法７０９条）、瑕疵担保責任（同法５７０条、５６６条、商法５２６条１項等）の対象となる可能性があります。
(b) 提供の際の契約で、これを免除する場合については、消費者契約法の適用がある場合には、責任の全部免除が認められない場合がありえます。
(c) 製造物責任法上の問題として、現時点において、ソフトウエアそれ自体については製造物責任が問われないと一般に解釈されていますが、電気機器や電子部品その他の工業製品等に組み込まれたソフトウエアは動産である 製造物ですので製造物責任法に定める責任規定の適用がなされることがありえます。

付録３　ウェブサイト運営者の法的な論点

法律専門家の見解によると、ウェブアプリケーションの脆弱性に関する法的な位置づけ、論点は、以下の通りです。

1) **ウェブサイト運営者と、ユーザとの間においては、そのウェブアプリケーションの利用に際して、一定の契約関係にはいると考えられます。そして、ユーザが、そのサイトに一定の個人情報などをゆだねる場合には、ウェブサイト運営者は、そのサイトの利用契約に付随した義務として一定レベルのセキュリティ維持を果たすべき義務を負担していると考えることができます。**
2) **各サイトに「プライバシポリシ」などが記載されている場合には、その内容をも前提にユーザとウェブサイト運営者は、契約関係にはいると考えられます。**
3) **この場合、ウェブサイト運営者において、上記のセキュリティ維持等について過失が有る場合、その過失による損害賠償の責めを免れるような規定は、消費者契約法上、全部免責の規定については無効となることがあります。**

付録４　具体的な説明

１．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。

・URL の一部にパスワードが判別可能な形式で明示されている

・本来閉じられているべき telnet 等のポートが空いており、administrator のパスワードが付与されていない

・ウェブサイト運営者が公開を意図していないファイル（個人情報ファイル等）が、ウェブサーバに、誰にでも閲覧できる状態で（アクセス制限なしに）置かれている等

２．ソフトウエア製品

ソフトウエア製品の種類は、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等を想定しています。

３．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。

４．ワークアラウンド

脆弱性を回避するための方法であり、当該脆弱性を修正する以外の比較的簡単な方法で脆弱性の影響を受けないようにする方法です。具体的には、脆弱性に関連するポートを閉じる等があります。

５．パッチ

脆弱性を有するソフトウエアから、脆弱性部分を解消するためのソフトウエアを指します。

６．プロトコルの実装に係わる脆弱性

過去に脆弱性の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。

- H.323 に係わる脆弱性

- SSH2 に係わる脆弱性
- OpenSSL に係わる脆弱性
- ASN.1 に係わる脆弱性

７．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 http://www.ipa.go.jp/ のウェブサイト運営者は IPA です。IPA が、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、ウェブサイト運営者は IPA となります。