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

2011 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
社団法人 電子情報技術産業協会
社団法人 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

目　次

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、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。

〇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。「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。

〇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。

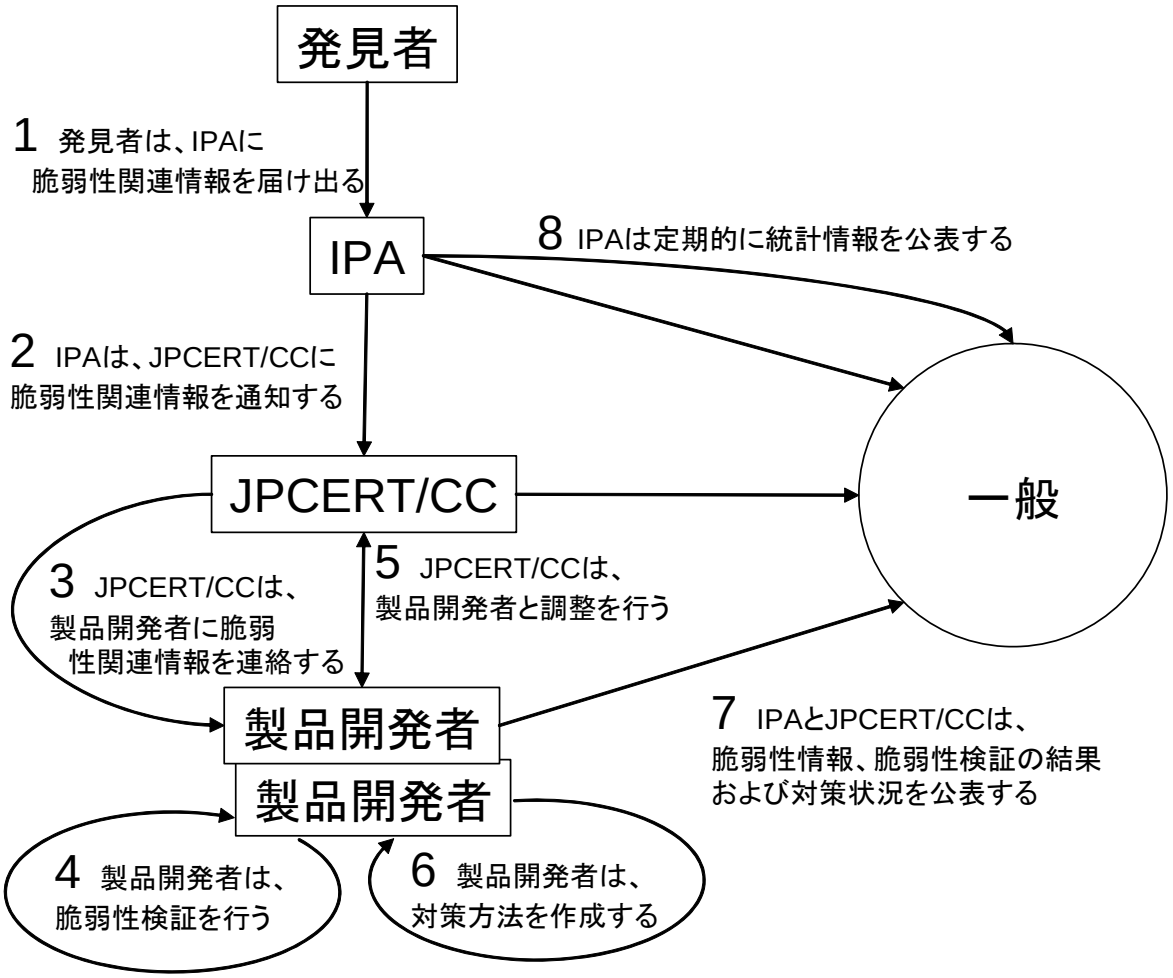


図１　ソフトウエア製品に係る脆弱性関連情報取扱の概要

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 JPCERT/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（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、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。

なお、起算日[1]から１年間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。

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

[1] 本ガイドラインの「IPA および JPCERT/CC 対応」において「製品開発者への連絡」(3-(2)-2)として規定された連絡を最初に試みた日を起算日とします。

・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、独立行政法人産業技術総合研究所など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)情報非開示依頼の取下げ
IPA は、起算日から 1 年間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 はその状況を取下げを求めた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
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。

13)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 Japan Vulnerability 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、製品開発者と連絡が取れない場合、または、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。

14)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。

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、製品開発者と連絡が取れない場合、または、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) 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、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、IPA 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 IPA を通じて通知します。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。

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、製品開発者と連絡が取れない場合、または、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。
また、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、すみやかに 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。望ましい公表の手順を、付録５に示します。

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 または IPA 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。

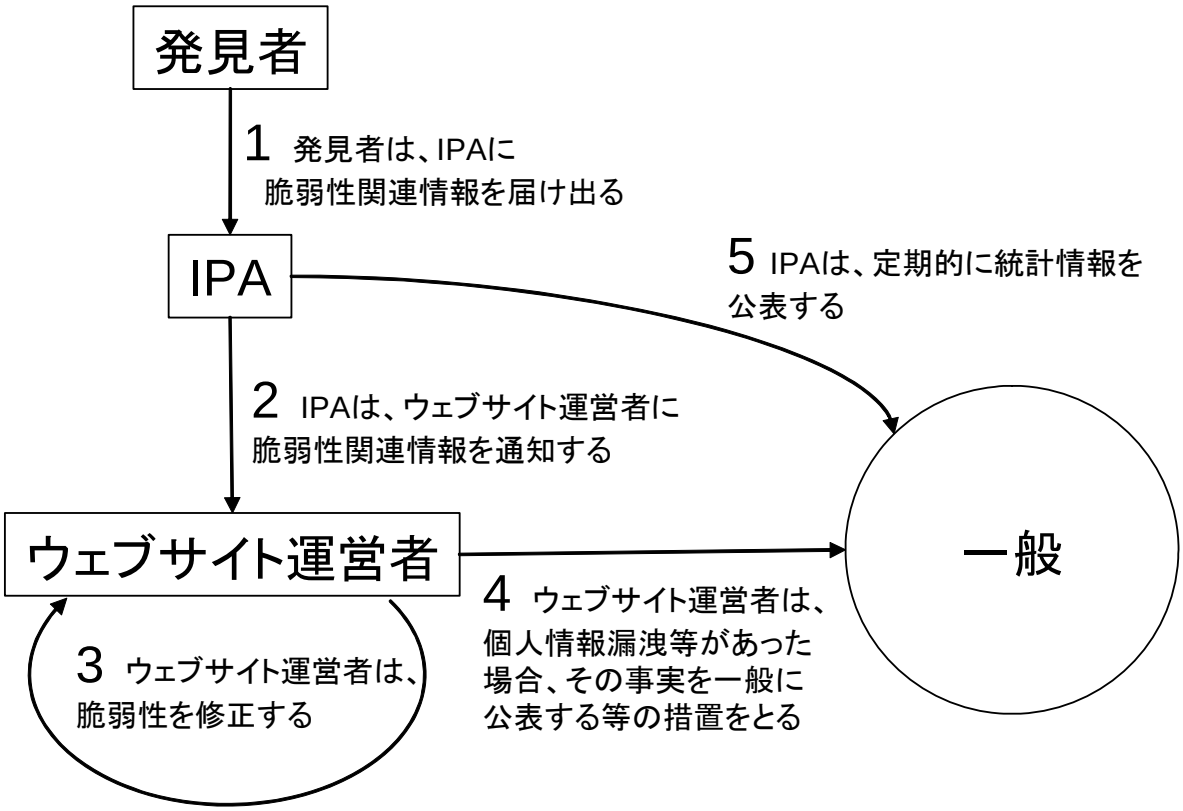


図 2　ウェブアプリケーションに係る脆弱性関連情報取扱概要

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
（オ） ウェブサイトの不適切な運用（付録４）のうち、脆弱性の原因が下記と判明したもので、IPA が注意喚起など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、誤っていたり初期状態のままとなっている。
・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。

なお、上記(オ)の注意喚起後は、該当する製品の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、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郵便、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わ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い期間を考慮して取扱いを終了することがあります。

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 が独立行政法人産業技術総合研究所など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（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 キーの解読など）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。

・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。

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。

(1) H.323 に係わる脆弱性
(2) SSH2 に係わる脆弱性
(3) OpenSSL に係わる脆弱性
(4) 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。

付録５　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

1.　本資料の目的

ソフトウエア製品を開発した企業や個人（以下「製品開発者」という）にとって、その利用者（一般消費者やシステム構築事業者など。以下「利用者」という）に安全なソフトウエア製品を提供することは品質に対する信頼確保の観点から重要とされるところですが、現実には周到な安全設計のもとに開発された製品であっても、安全上の問題点（以下「脆弱性」という）が生じてしまうことがあります。

過去にリリースした製品に脆弱性が存在することを知りながら、脆弱性対策情報を公表せず、被害が生ずる可能性を隠したり、不十分な内容の公表にとどめたり、虚偽の内容を公表することは、利用者の情報資産や社会活動を危険にさらす結果を招きかねません。製品開発者は可及的速やかに自主的に脆弱性対策を施し、利用者に的確な脆弱性対策情報を提供することが望まれます。

しかしながら、製品開発者によっては、このような情報公開を経験した前例がないことなどが原因となって、不十分な情報公開や、不適切な方法での情報提供が行われる場合があり、利用者に必要な情報が届かない事態が生じているのが現状です。

本資料は、必要としている利用者に必要な情報が的確に届けられることを目標として、製品開発者が行うべき脆弱性対策情報の望ましい公表の手順について、一つの方針を示すものです。

2.　脆弱性対策について利用者が必要としている情報

脆弱性対策情報を利用者に提供するにあたり、製品開発者は、どのような情報が利用者に必要とされているかを知っておくべきです。製品開発者が、十分な説明なしに修正プログラムの提供のみを行った場合、利用者に不利益が生ずることがあります。以下に、修正プログラムの適用方法の情報のほかに、一般的に利用者が必要としていると考えられる情報の種類と、その理由を示します。

(1) 製品の名称およびバージョン

利用者は、まず自分がその脆弱性の影響を受けるかどうかを見分けたいと考えるはずです。したがって、脆弱性の影響が及ぶ製品の名称とバージョン番号を容易に確認できるような情報公開が求められます。

(2) 脆弱性対策情報の公表時期

ウェブサイトでの情報公開においては、古い情報が閲覧されることがあります。新しい情報であれば利用者に影響する可能性が高く、古い情報であれば既に対策済みの場合があります。利用者が対策済みの情報を何度も確認することにならないよう、情報の公表日付が示されることが求められます。

(3) 脅威

脆弱性情報が公表された際、それによりもたらされる危険が小さければ対策しないで済ませ、重大な危険がある場合のみ対策するという判断をする利用者が存在します。したがって、その脆弱性の修正プログラムを適用しなかった場合にもたらされ得る具体的な脅威がどのようなものかについて、公表することが求められます。

(4) 回避策

修正プログラムを適用できない場合に、攻撃を受けない、もしくは受けても被害が発生しないための回避策が存在するならば、その手段に関する情報が求められます。製品開発者が修正プログラムだけ提供して脆弱性の詳細を公表しなかった場合、回避策が不明となり、修正プログラムを適用できない利用者が不利益を被ることがあります。回避策が存在する場合には、製品開発者がその方法を適切に公表するべきです。

(5) 他に公表されている脆弱性関連情報

製品開発者が公表する脆弱性対策情報以外にも、深刻さや緊急性を測るための参考情報があるならば、利用者はそれもあわせて確認するものです。したがって、それらの情報を参考情報として示すことが求められます。

3. 脆弱性対策情報の公表項目と公表例

製品開発者がウェブサイト上で脆弱性対策情報を公表する際に示すべき情報の項目を列挙し、望ましい公表と、望ましくない公表の例を示します。

3.1. 脆弱性対策情報の公表項目

求められる情報は、利用者がシステム構築事業者か一般消費者かによって、重視される情報が異なることがあります。システム構築事業者は脅威や回避策についての詳細な情報を重視するのに対し、一般消費者は、該当する製品を利用の確認方法や、対策の手順がわかりやすく解説されていることを重視します。製品の性質に応じて利用者層を想定するなどして、情報を見やすい構造で提供することを心がけることが重要です。

以下、一般的に考えられている脆弱性対策情報の望ましい公開の手順を、情報の項目ごとに区切って示します。

3.1.1. タイトル

製品の名称で検索して情報に辿り着く利用者のために、ページタイトルに製品名を記載します。また、過去および将来において同じ製品に複数の脆弱性が生ずる場合があることから、それらを区別可能なように、タイトルに脆弱性名称を記し、脆弱性情報のシリアル番号等を含めます。また、検索サイトなど外部サイトから直接に当該ページへ誘導される場合に備えて、そのページが脆弱性対策情報についての記述であることを明示します。

3.1.2. 概要

利用者が脆弱性の要点を迅速に把握できるよう、内容を簡潔にまとめた概要を冒頭に示します。

3.1.3. 該当製品の確認方法

脆弱性のある製品のバージョン情報と、利用者が使用している製品のバージョン情報を確認する方法を説明します。

3.1.4. 脆弱性の説明

利用者が同じ製品に存在した他の脆弱性と混同するなどの混乱が生じないよう、脆弱性の名称やその原因箇所などを記載して、その脆弱性の存在を説明します。

3.1.5. 脆弱性がもたらす脅威

脆弱性を悪用された場合に生じ得る被害の内容、危険の度合い、攻撃が成功する可能性の大きさ等、脆弱性の深刻度を評価するために必要な情報を記載します。

3.1.6. 対策方法

対策を施した製品のインストール方法やバージョンアップ方法、修正プログラムの適用方法を記載します。

3.1.7. 回避策

修正プログラムを適用しないままで、製品の利用方法を制限することや、運用を工夫すること等によって被害を防止できる場合には、その方法を回避策として記載します。

3.1.8. 関連情報

製品開発者による情報以外に、その脆弱性について公表されている情報がある場合には、利用者に有益な参考情報として、当該情報へのリンク等を記載します。

3.1.9. 謝辞

製品開発者によっては、脆弱性発見者への謝辞を記載することがあります。

3.1.10. 更新履歴

当該脆弱性対策情報を最初に公表した日時を明示します。後に記載内容を改変した場合は、更新日を示すとともに、更新内容の説明を記載します。

3.1.11. 連絡先

公表した脆弱性対策情報に疑問が生じたり、修正プログラムに不具合が生じたりする場合に備えて、問い合わせ先を明記します。

3.1.12. 脆弱性対策情報の公表例

脆弱性対策情報の望ましい公表の例は、使用者等の情報提供の対象者を特定できない場合に、製品開発者が使用者に告知する例とし、参考文献「消費者生活製品のリコールハンドブック」を参考に作成しています。

- **望ましい公表の例**

☆☆☆☆株式会社 ＞ セキュリティ脆弱性情報 ＞ ○○○○製品

IPASA2007-001: ○○○○製品における×××の脆弱性

公開日 2007 年 1 月 4 日
最終更新日 2007 年 1 月 9 日

■概要

○○○○のバージョン△△以前に×××の脆弱性が存在することが判明しました。この脆弱性を悪用された場合、悪意ある第三者の攻撃により、○○○○が動作しているコンピュータ上で□□□□が実行されてしまう危険性があります。

この問題の影響を受ける○○○○のバージョンを以下に示しますので、以下の修正プログラムを適用してください。

■該当製品の確認方法

影響を受ける製品は以下の製品です。

製品名称 ○○○○
該当バージョン
1.5.4 (Windows XP SP2 版) 以前の全てのバージョン
1.5.4 (Linux 版) 以前の全てのバージョン

使用しているバージョン番号の確認方法は以下の通りです。

1. ○○○○を起動し、「ヘルプ」メニューから「バージョン情報」を選択する。
2. 現れたウィンドウの下記の部分が起動している○○○○のバージョン番号です。

バージョン表示ウィンドウの図 （省略）

■脆弱性の説明

○○○○製品は、ファイルの■■■■のために▽▽▽▽の機能を搭載しています。◎◎◎◎データの一部として提供され▲▲▲▲で配布された▽▽▽▽の機能に、××××の脆弱性が存在するため、外部の第三者からインターネット越しに□□□□を実行される脆弱性が存在します。

■脆弱性がもたらす脅威

システム管理者権限でログインして本ソフトウエアを利用している場合、攻撃が成功すると、悪意のある第三者によってコンピュータを完全に制御されてしまう可能性があります。これにより、悪意のある第三者は、不正プログラムのインストール、データの変更や削除など、システム管理者の権限でコンピュータを任意に操作する可能性があります。

・ IPASA2007-001 技術詳細情報

■対策方法

〇〇〇〇バージョン 1.0.0 より前の製品を利用されているお客様は、一度製品をアンインストールしてから対策版製品をインストールしてください。〇〇〇〇1.0.0 以降の製品を利用されているお客様は、修正プログラムをインストールしてください。

各プログラムのインストール方法に関しては同梱の readme.txt を参照してください。

対象製品名称 〇〇〇〇

修正プログラムのダウンロード

1.5.5 patch.zip (WindowsXP SP2 版) 2007.1.4

1.5.5 patch.tgz (Linux 版) 2007.1.4

・ 修正プログラムによって置き換えられる設定ファイル

xxxxx.cfg、yyyyy.dif

■回避策

この脆弱性は、次に示す手順で影響を緩和できる場合があります。

・ 回避策

〇〇〇で使用する管理用ポート番号宛ての通信を信頼できる IP アドレスのみに限定するよう、IP フィルタリング機能またはルータ等にてフィルタリング設定を行うことで、影響を緩和することができます。

■関連情報

JVN#12345678 〇〇〇〇製品における××××の脆弱性

■謝辞

□□□の□□□氏よりこの問題をご報告いただき(略)

■更新履歴

2007.01.4 この脆弱性情報ページを公開しました。

2007.01.9 脆弱性がもたらす脅威に、権限の低い設定のアカウントで利用している場合についての技術詳細情報を追加しました。

■連絡先

脆弱性連絡窓口

電話 : 03-xxxxx-xxxx (平日 10:00 - 17:00)

メール: example@example.co.jp

- **望ましくない公表の例 (1)**

〇〇〇〇製品の更新について

平素は格別のご愛顧を賜り厚くお礼申し上げます。

さて、この度弊社で開発しました〇〇〇〇に開発工程にて、ごく稀に△△△△機能にて動作が不安定になることがございます。

この現象は限定された利用環境において発生するものです。しかし、万が一のため、ここに〇〇〇〇製品のアップデートプログラムの公表を連絡させていただくものです。

今後とも、お客様の身になって、品質の向上に努めてまいりたい所存ですので、本製品をご愛顧いただけますよう、お願いいたします。

■アップデートプログラム

〇〇〇〇1.5.5 (Windows 版)　　〇〇〇1.5.5 (Linux 版)

望ましくない理由

- 脆弱性対策を目的とした告知であることが不明確で、利用者に分かりません。
- 日頃から送付している宣伝メッセージと間違われかねない形式で書かれているため、脆弱性対策情報であることに気づけません。
- どのような危険が差し迫っているか、詳細が不明確なため、利用者は脆弱性対策を早急に行うべきか判断できません。
- アップデート方法について具体的な記述が無いため、対策方法が分かりません。
- 公表された時期が不明なため、利用者が既に対策済みの脆弱性情報かどうかの判断ができません。

- **望ましくない公表の例 (2)**

〇〇〇〇リリースノート

2007.1.4　　バージョン 1.5.5

・メール送信機能に任意のヘッダの編集機能を追加

・ファイルアップロード機能で長いファイル名を指定したときにバッファオーバーフローが生ずる不具合を修正

・そのほかの細かなバグの修正

2006.11.28　バージョン 1.5.4

・ファイルアップロード機能を追加

・・・・・・・

望ましくない理由

- 新バージョンのリリース情報が、一般的な機能改善だけを目的としたものか、脆弱性修正を含むかを、利用者には容易に判別できません。

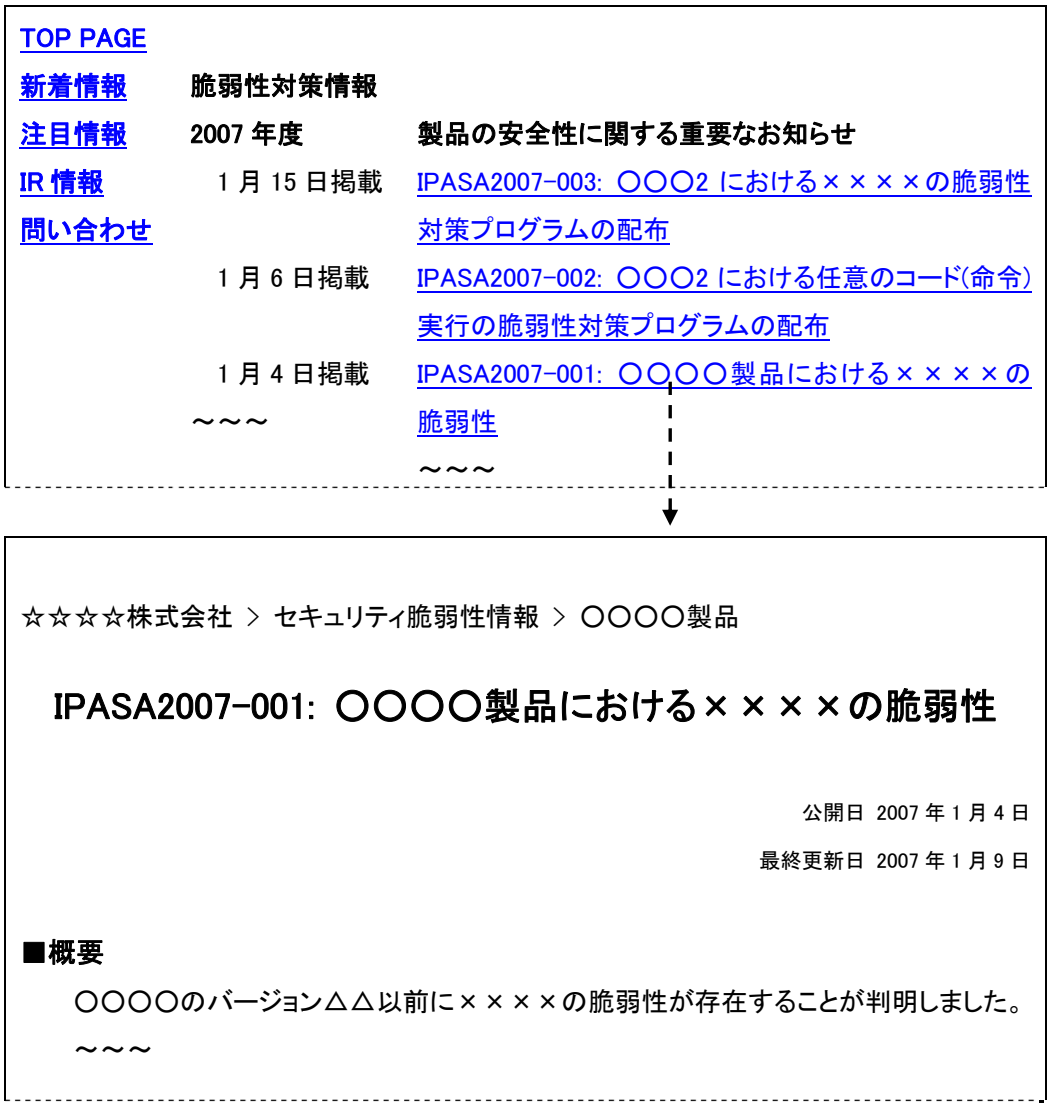
4. 脆弱性対策情報への誘導方法

製品開発者がウェブサイトのトップページから脆弱性対策情報へ利用者を誘導する方法として望ましい誘導方法の例と、望ましくない誘導方法の例を示します。

脆弱性対策情報への誘導する際に望ましい構成

- ウェブサイトの階層が深くなったり、表示される情報が複雑化したりすると、利用者は脆弱性対策情報にたどり着きにくくなります。したがって、ウェブサイトのトップページから脆弱性対策情報にリンクで誘導する際は、階層が深くならないような工夫が必要です。
- ・誘導する際のリンクの名称は、タイトルと同様にします。
- ・リンクで脆弱性対策情報に誘導する際は、3.1.10 と同様に更新日時を記載します。

- **望ましい誘導方法の例**



- **望ましくない誘導方法の例**

TOP PAGE
サービス
ニュース
2002 年　2003 年　2004 年　2005 年　2006 年　2007 年
ソリューション
新着情報
IR 情報
弊社からのお知らせ
Q&A

Q.〇〇〇〇製品は、SQL インジェクション脆弱性の影響をうけますか？

A.以下のバージョンに問題が見つかっています。
対象バージョン： 1.4 以前

〇〇〇〇のヘルプ画面にて、悪意ある第三者により送信された不正な SQL 文を含むリクエストを受けると、データベースを任意に操作される可能性があります。
〇〇〇〇をバージョン 1.5 に更新してください。

望ましくない理由

- Q&A などの他の情報に脆弱性情報が混在しています。
- FAQ に脆弱性対策情報が掲載されているため、この情報が脆弱性対策情報であることが分かりません。
- 脆弱性対策情報を探している利用者がここにその情報があることを予想できません。
- いつ掲載された脆弱性対策情報か利用者が分かりません。

5. 参考文献

消費者生活製品のリコールハンドブック，製品安全研究会，2002.5
P.47 参考2 社告の例 望ましい社告の例
http://www.meti.go.jp/policy/consumer/seian/contents/recall/handbook.pdf

付録６　ウェブサイト運営者のための脆弱性対応マニュアル

ウェブサイト運営者は、脆弱性の有無についての調査を基に確認し、必要であれば脆弱性修正プログラムの適用といった対策を行います。また、脆弱性について関係する内部・外部の相手や、サイトの利用者との間の連絡窓口を設置し、ウェブサイト運営関係者への情報の集約と管理を担当します。

対処にあたっては全体方針や、対策の計画をウェブサイト運営者自身の判断に基づいて行うことが必要となります。

対処の流れ

ウェブサイト運営者が脆弱性に関する連絡を外部から受け取った際の対処の流れを下図に示します。

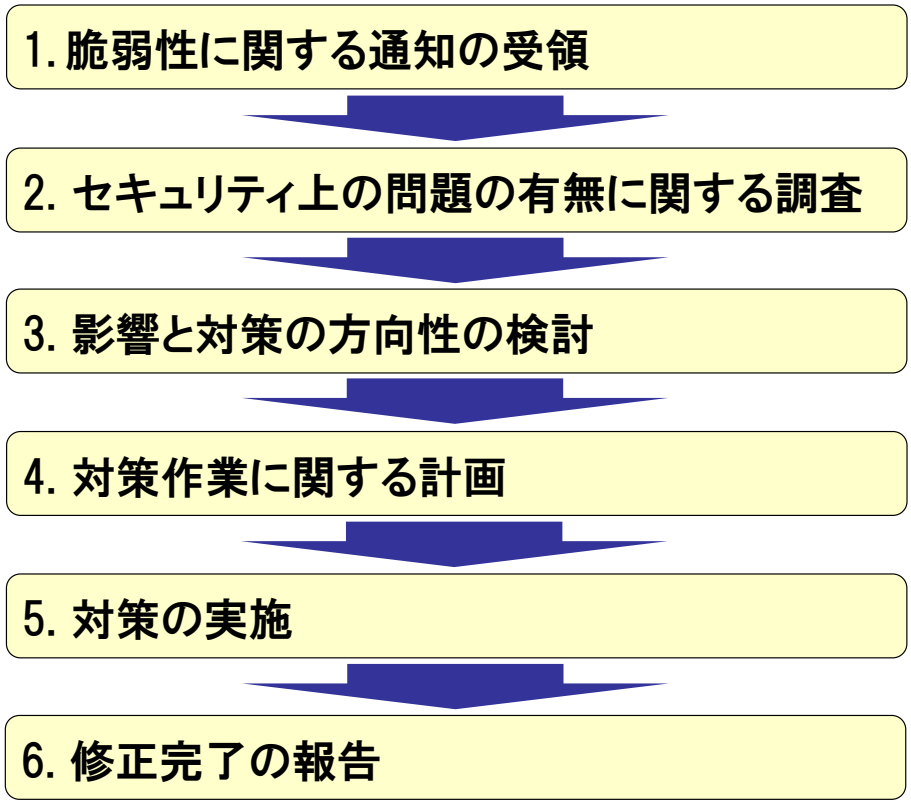


図１　脆弱性関連情報への対処の流れ

対応の全体に係る留意点

(1) 外部から連絡を受けた際の対応

外部から脆弱性関連情報の通知を受けた際には、IPA／発見者を含む関係者間で良いコミュニケーションを維持することが対応を成功させる鍵となります。

自発的・定期的に行われる脆弱性修正に比べると、外部から事実確認を急ぐよう求められることとなります。ウェブサイト運営者にとっては負担にもなりますが、対処の方針・計画を整理した上で、可能な範囲で説明し理解を求めることが大切です。

(2) トラブルが発生している時の脆弱性への対応

ウェブサイトにおけるセキュリティ上のトラブルに対しては、発見後の迅速な対応が必要です。不正アクセスの踏み台にされている場合、フィッシング詐欺等に悪用されている場合、ウイルスを撒き散らしている場合には、まずウェブサイトを停止し被害拡大を防ぎます。加えて、個人情報の漏洩や利用者へのウイルス送信等が発生した際には、速やかな被害事実の公表も望まれます。

トラブルは、ウイルスや不正アクセス等にウェブサイトの弱点＝脆弱性を狙われて起きます。被害防止のためには、ウイルス等の駆除や監視強化等の処置だけでなく、ウェブサイトの脆弱性が原因である可能性を考慮し、丁寧な調査を行って「穴を見つけて塞ぐ」ことが大切です。

脆弱性への手当てが十分でないままサービスを継続して提供すれば再び被害を受ける可能性もあります。脆弱性の調査や修正には作業時間を取る必要があります。場合によってはサイトを一時的に停止するといった決断も必要です。

ウェブサイト運営者は、被害事実の公表やサービス再開のタイミングを考慮しながら、脆弱性に関する技術的作業を進めていく必要があります。

(3) SI 事業者との協力

サイトの運営形態によっては、SI 事業者に情報を渡して相談し、脆弱性の確認や対策実施に関する具体的作業を依頼する場合も想定されます。脆弱性への対処について SI 事業者の協力を得る場合については各手順に留意点を示しますので参考にしてください。

対処の詳細な作業については「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」（社団法人情報サービス産業協会、社団法人電子情報技術産業協会も参考となります。（詳細は http://www.jisa.or.jp/report/2004/vulhandling_guide.pdf を参照してください）。

1. 脆弱性に関する通知の受領

ウェブサイト運営者は、サイトのウェブアプリケーションの脆弱性関連情報について通知を受け付ける立場にあります。

この段階では、ウェブサイト運営者は以下の作業を行います。

(1) 脆弱性関連情報の適切な担当者への受け渡し (2) 通知を受領した旨の返信 (3) IPA／発見者との連絡手段の確立(窓口の一元化、暗号化メールの使用、返答期限の設定、連絡記録の作成) (4) 組織内の対応体制の確認(担当者、報告先・報告内容、意思決定プロセス) (5) SI 事業者への作業依頼を行うかどうかの判断 (6) 発見者と直接情報交換を行うかどうかの判断 (7) IPA／発見者への確認(当該脆弱性を知る人は誰か、脆弱性関連情報が今後公表される可能性と時期 等)

通知は、IPA がウェブサイト運営者に通知してくる場合と、発見者がサイト運営者に直接通知してくる場合の 2 つに大きく分けることができます。以下にそれぞれの場合について示します。

いずれの場合についても、ウェブサイト運営者は、通知を受け取った旨の返信を速やかに行うよう努めてください。

■ IPA から連絡を受ける場合の対応

ウェブサイトに関する脆弱性関連情報が発見者から IPA に届出られた際には、IPA からウェブサイト運営者に通知を行います。IPA からの通知は主に電子メール(vuln-contact@ipa.go.jp)を利用し 3 段階で行われます。

第 1 段階： IPA は脆弱性の可能性があるウェブサイトに記載された連絡先アドレス宛にメールを送ります。このメールでは脆弱性の可能性があるウェブサイトの URL を知らせますが、脆弱性の詳細な情報は送りません。

ウェブサイト運営者は、より詳細な情報を受け取る連絡先(対応窓口とするアドレス)を記載したメールを IPA に返信してください。

第 2 段階： ウェブサイト運営者が示した対応窓口アドレスに宛てた電子メールで、今後の連絡メールに用いる暗号化について確認します。

第 3 段階: ウェブ運営者が示した対応窓口アドレス宛ての電子メールで、より詳細な脆弱性関連情報を通知します。脆弱性関連情報は、主に技術的な情報で、脆弱性の種類や、現状から想定されるリスク等の情報を含みます。

また、この通知以後のメールには、取扱番号(例:IPA＃12345678)が付されます。IPA と連絡を行う際にはこの番号を用います。

IPA から詳細情報を受け取った後には、受領した旨を IPA に返信してください。

IPA に脆弱性関連情報を通知した発見者の名前はウェブサイト運営者には通知されません。しかしながら、調査などでウェブサイト運営者が希望し、発見者もこれに同意した場合には、交換されるすべての写しを IPA に提供することを条件に、脆弱性関連情報の詳細に関して発見者と直接情報交換を行うことも選べます。

■ 発見者から直接連絡を受ける場合の対応

発見者が IPA を介さずに直接ウェブサイト運営者に脆弱性関連情報を通知してくることがあります。この場合は、発見者と誠実な対話に努めるようしてください。改めて IPA に届出るように発見者に求めるという選択もあります。

脆弱性関連情報を通知された場合には、以下の関連情報が含まれるかを確認します。これらの情報が含まれていない場合には IPA あるいは発見者に問い合わせてください。

1) 脆弱性関連情報を既に IPA や他者に通知（公表）したかどうか。
2) 脆弱性関連情報を発見者が公表する意思、公表手段と予定する時期。

＜SI 事業者に相談する場合＞

サイト運用について SI 事業者に依頼している場合、あるいは、通知を受けたもののウェブサイト運営者自身による対処が困難と判断される場合には、SI 事業者と相談しながら対応を進める事をお奨めします。

2. セキュリティ上の問題の有無に関する調査

ウェブサイト運営者は、通知を受けた脆弱性についてその有無を確認し、受け取った情報の正誤を評価します。

この段階では、ウェブサイト運営者は以下の作業を行います。

(1) 確認作業に必要なリソースの確保、関係者への協力要請
(2) 問題があるウェブシステムの特定
(3) 指摘された脆弱性につながる現象の再現
(4) 脆弱性の原因と発生条件の特定
(5) IPA あるいは発見者への進捗連絡

脆弱性の存在を確認しただけのこの段階では、もたらされ得る被害、適切な対策は未だ明確ではありません。想定される被害や対策を明らかにする作業については、ある程度の状況把握を済ませた後に改めて計画的に作業を行います。

脆弱性の存在の有無が明確になった段階で、脆弱性に関して連絡を寄せてきた相手（IPA あるいは発見者）に、脆弱性の存在および通知内容について正誤を確認した旨を連絡してください。

IPA より通知を受けた際には、IPA に相談しながら対処を進めることもできます。もし脆弱性をうまく再現できない等の場合にはご相談ください。

＜SI 事業者に調査を依頼する場合＞

確認作業について SI 事業者に依頼する場合には、経緯と既に得た情報について説明してください。SI 事業者に脆弱性関連情報等を提供した際には受領通知をもらうようにします（以後の手順でも同様です）。この時点において SI 事業者が確認した内容については簡潔な報告を受け取ってください。

3. 影響と対策の方向性の検討

具体的ウェブサイトの調査を行い、問題箇所が及ぼす影響をより明確にし、修正方法を検討します。この段階では以下の作業を行います。

(1) 作業に必要なリソースの確保、関係者への協力要請
(2) 脆弱性の影響範囲の調査
(3) 対策適用の影響度の調査
(4) 修正方法の検討
(5) スケジュールの見積もり
(6) 対応費用の見積り
(7) 検討報告および対応方針案のとりまとめ

IPA より通知を受けた場合、スケジュールについては、詳細情報の通知を受けてから 3 ヶ月以内を目処に対応してください。3 ヶ月以内での対応が難しい場合、対応に要する期間の見積りを IPA にご連絡ください。

＜SI 事業者に対策の検討を依頼する場合の進め方＞

SI 事業者には上記の(2)～(7)の具体的項目についての調査検討を依頼します。ウェブサイト運営者はSI事業者に上記の調査作業を進める上で必要なシステムに関する情報、作業に必要な環境や権限等を適宜提供し、SI 事業者がとりまとめた検討報告および対応方針案を受けとってください。

4. 対策作業に関する計画

対策作業に取り掛かる前に計画を立てます。SI 事業者に対策の実施を依頼する場合には、作業計画他幾つかの事項について調整をはかり合意をとります。この段階では以下の作業を行います。

(1) これまでに収集した情報の整理と共有
(2) 当該サイトに関する契約の確認
(3) 対策基本姿勢・優先事項の明確化
(4) 費用、人員、作業時間、その他対策実施に必要なリソースの確保
(5) 対策計画の確定
(6) 作業時の連絡体制の確認
(7) 作業実施に係る SI 事業者との調整

問題のあったサイトに関して、外部の構築担当者や運用担当者との間で結んだ契約があれば、その内容を確認しておきます。

ここまでに明らかになった情報を整理して関係者で共有し、要点を確認します。ウェブサイト運営者として、問題となる脆弱性にどのような対応を行うかについて基本的な対応方針を決定します。合わせて対策作業に必要な費用、人員、作業時間等のリソースの確保についても組織内で同意を取っておきます。

これまでの作業で作成した対策案をベースに対策に関する計画を確定させます。また、作業時の連絡体制についても確認しておきます。

＜SI 事業者に対策の実施を依頼する場合＞

SI 事業者に対策の実施（次項）を依頼する場合には、検討報告・対応方針案をベースにして、ウェブサイト運営者とSI事業者の双方で計画を具体化します。これには費用、スケジュール、その他リソースの確保についての調整が含まれます。また、SI 事業者から進捗報告を受けるタイミングについても計画しておきます（作業の大きな節目、作業が長引く場合には一定期間 等）。

5. 対策の実施

作業計画に基づく対策を実施します。技術者による修正作業が中心となりますが、同時にサイトの運用に関する留意も必要となります。

ウェブサイト運営者から SI 事業者に実施を依頼する場合には、SI 事業者は事前に調整した作業を実施します。この段階では以下の作業を行います。

(1)　対策作業に伴う一時停止等に関するサイト利用者へのアナウンス
(2)　利用者への作業実施期間中の代替手段の提供・案内
(3)　修正の作成
(4)　試験環境でのテストと実施手順作り
(5)　対策の実施適用
(6)　対策効果の確認
(7)　利用者からの問い合わせへの対応
(8)　進捗報告の作成

ウェブサイト運営者は、サイトの利用者に対して作業に伴うサイト一時停止等のアナウンスを行います。あわせて作業中に生じうる利用者への対応（代替手段の提供、問い合わせへの返答　等）について必要な手配を行います。

対策実施の技術的な部分の手順は、修正の作成、試験環境でのテストと実施手順作り、対策の実施適用、対策効果の確認、の 4 段階からなります。

対策効果の確認に際しては、適切かつ有効な対策が施されていることを診断・確認します。最新の対策について情報を持つ外部の監査ベンダを利用することも有効です。

＜SI 事業者に対策の実施を依頼する場合＞

対策の実施について SI 事業者に作業を依頼する場合には、前項に示すように計画に沿って進めてください。進捗については適宜報告を受けるようにします。

6. 修正完了の報告

脆弱性の対応が完了したら、ウェブサイト運営者は以下の作業を行います。

(1)　IPA／発見者への修正完了報告

IPA より連絡を受けて対応に当たった場合には修正完了報告（取扱番号、対象のウェブサイト URL、対応の内容）を IPA へお願いします。

その他

問題となった脆弱性に関連して、個人情報漏えい等のトラブルが発生した場合には、事故に関する報告を行います。これには、サイト利用者への告知、主務官庁等への報告等が含まれます。また、個人情報が流出した場合には、二次被害を防ぐために、影響を受ける可能性のある本人に可能な限り連絡することが望まれます。（詳細は「内閣府　個人情報保護　個人情報の保護に関するガイドラインについて」 http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou.html を参照してください）。

付録７　ウェブサイト構築事業者のための脆弱性対応マニュアル

1. 納入前に考慮すべきこと

1.1. 契約段階で望まれること

顧客が、情報システムの有するリスク（脆弱性が突然発覚する可能性があること、そのような未知の脆弱性は開発時に排除できないため、運用時の対応が不可欠であること）を理解していないと、適切な保守が行われない可能性があります。

したがって、ウェブサイト構築事業者の方は、契約の段階から脆弱性に係る問題について十分に説明し、保守の重要性を顧客に理解していただけるよう努力することが期待されます。

■顧客に向けた事前説明

顧客企業における情報システムの統括責任者の方には、ウェブサイトの脆弱性対策に関する以下の点を理解していただく必要があります。

まず、脆弱性のない完璧なシステムを構築することは非常に難しいという点です。完全なシステムを追求するためには膨大な予算を投入しなければならず、コスト的に割に合いません。

また、これまでに触れてきたとおり、コンピュータシステムは、時間が経つと内在していた脆弱性が発覚するリスクを常に抱えていて、今は安全でもいつ安全でなくなるかわかりません。つまり、システムの安全性は時間とともに劣化すると考えるべきです。安全性を維持するためには適切なメンテナンスが不可欠であり、保守・運用にも予算と人手をかける必要があります。保守・運用のスタッフを確保できない場合には、外部の事業者に委託することも有効です。

さらに、運用中のウェブサイトに脆弱性が発見された場合には、予想される脅威や影響を勘案して、適切な対策を選択すべきです。予算や人手の不足を理由に脆弱性を放置していると、1.2 で示したようなトラブルが発生してユーザや取引先に迷惑をかけることになりかねません。

■契約時に合意すべき事項

契約時には、以下のような脆弱性対策の取扱いについて、顧客や再委託先等の関係者と合意を取り付けることが望まれます。

- **納入後に公表された新規の脆弱性対策**

  ソフトウエア製品の脆弱性のうち、納入後に製品開発ベンダや JVN で公表された新規のものについては、対策を有償とすべきであり、開発とは別の保守契約で対応するのが適切と考えられます。

- **既知の重要な脆弱性対策**

  ソフトウエア製品の既知の重要な脆弱性やウェブアプリケーションの著名な脆弱性の対策に

関する著しい認識不足、ウェブアプリケーションに対する必要な設定漏れ、設定ミスなどウェブサイト構築事業者の責に帰する場合は無償とすべきです。

- **セキュリティ検査の実施の有無**

  ウェブサイトに対し脆弱性の有無を確認するセキュリティ検査を納入前に行うか否かにより、既知の脆弱性対策でカバーできる範囲が大きく異なります。顧客のニーズや予算に依存しますが、検査の実施と既知の脆弱性対策については連動することを説明すべきです。

- **緊急事態時の費用負担**

  緊急事態の際は迅速な対策を要求されるため、顧客との間で作業範囲、費用負担について十分な協議のないまま、作業を進める状況が多々あると予想されます。契約の段階で明確にしておくべきですが、それが難しい場合にも、極力、覚書として残しておくことが望ましいと考えられます。

また、これらの事項は、顧客企業と一次請けのウェブサイト構築事業者の間の契約を想定していますが、二次請け、三次請けの事業者も同様な観点での対応を考慮しておくべきです。

■その他望ましい対応

さらに、顧客企業の担当部門のニーズによっては、経営層が投資規模について的確に判断できるよう、発見された脆弱性によって引き起こされる事件・事故による被害の大きさと対策案費用を比較した資料を作成するなどの支援を行うことも考えられます。

また、ウェブサイトは、ウェブアプリケーションとその基盤となるソフトウエア（OS, ミドルウェア等）で構成されるが、それぞれの脆弱性の対処策が異なることに留意すべきです。前者は、ウェブサイト構築事業者が新規開発する部分であり、設計・開発段階で脆弱性を残さないよう考慮する必要があります。一方、後者は、納入前の時点で既知の脆弱性については、あらかじめ修正プログラム（パッチ）を適用して、脆弱性対策を済ませておくことが期待されます。

1.2. 安全性を確保するための取組み方

脆弱性対策は、ウェブシステムの企画・設計・開発から運用・保守まで、様々な局面で継続的に取り組む必要があります。予算や人手、開発期間等の制約があるのは当然ですが、顧客のウェブサイトに問題が生じた場合にユーザや取引先が被る影響を考慮し、ウェブサイト構築事業者としてはできる限りの対応を行うよう、顧客と調整すべきです。すでに運用を開始しているウェブサイトにセキュリティ上の問題が発覚した場合、設計・開発レベルから修正することは難しい場合が少なくなく、場あたり的な対策で済まさざるをえないこともあります。したがって、対策は可能な限り、設計・開発段階で適用することが望まれます。

■企画段階の取組み

企画時には、ウェブシステムのセキュリティ方針について検討します。特に社外向けのサービスを提供するウェブシステムの場合、セキュリティポリシーを含む多面的な視点から、セキュリティ機能に必要な要件を十分に検討する必要があります。

【考慮すべき事項の例】

- ウェブサイトを用途（公開・管理）別に分離する必要はあるか
- アクセス制御（認証・許可・管理）を行う必要はあるか、どうやって行うか
- 個人情報を収集するか／どういったポリシーで扱い、どうやって保護するか
- ログ情報をどこまで収集するか／いつまで保護するか
- ユーザを識別するか／セッション管理をどうするか
- 予算と工数から、どれだけセキュリティの設計に回せるか
- 新技術・新製品を採用するか

■設計・開発段階の取組み

設計・開発時には、扱う情報資産の重要性、サービスの継続性・信頼性に対する要求レベル、サービスの公開範囲などを踏まえ、望まれるセキュリティ要件について顧客と合意する必要があります。さらに、業務上の機能要件だけでなく、保守も含めた運用時の脆弱性対策を考慮した要求仕様を用意するよう、顧客と調整すべきでしょう。

もちろん、予算や期間の制約から十分な対応ができない可能性もありますが、そのような状況であっても、最低限行うべきことがあります。たとえば、ウェブサイトの脆弱性の中でも独立行政法人情報処理推進機構（IPA）への届出件数が非常に多いクロスサイト・スクリプティングと SQL インジェクションの脆弱性は、プログラミングの際に残されるケースが大半であり、開発段階でこの 2 つの脆弱性に気をつけるだけでも大きな効果があります。これらの具体的な対策については、「安全なウェブサイトの作り方」（IPA、 http://www.ipa.go.jp/security/vuln/websecurity.html ）を参照してください。

1.3. 問題を招きやすいケース

契約から納入までのプロセスにおいて、脆弱性に係るトラブルを招く原因となりやすい事象として、たとえば以下のケースが挙げられます。

■曖昧なセキュリティ要件

仕様におけるセキュリティ要件が曖昧であったために、本来は契約外である脆弱性対策の負担をウェブサイト構築事業者に求められることがあります。本来の機能・処理に関する仕様が優先され、セキュリティ要件の策定は後回しにされやすいこと、また技術的な詳細が理解しにくいため、包括的な記載になりがちであることなどから、結果的に、納入後に判明した新しい脆弱性の対策

まで、すべて対応するように読める場合があります。

したがって、脆弱性対策の部分については、記載事項を定型化しておき、契約段階であらかじめ意思表示しておくことが望ましいと考えられます。

■サンプルプログラムの流用

予算や開発期間を抑制するため、サンプルプログラムを流用することもありますが、そこに脆弱性が含まれているケースが見られます。一般に、サンプルプログラムは、わかりやすさを優先するため、セキュリティ的な配慮が乏しいことが多いためと考えられます。

したがって、安全性が担保されていないサンプルプログラムを安易に流用することは避けるべきでしょう。少なくとも、ID・パスワードの処理（セッション管理を含む）、ユーザの入力欄の処理、データベースの処理等については、慎重に検討すべきです。できれば、広く利用されている開発フレームワークを活用することが望ましいと考えられます。

■不十分なコードレビュー

予算や開発期間の制約等により、コードレビューが不十分になることがあります。その場合、ブラックボックステスト（ペネトレーションテスト）では見つけられない脆弱性を内包してしまう可能性が高くなります。

少なくとも重大なリスクが想定されるコードについては重点レビューを行ったり、コード検査を自動化するなどして、より早期のコーディング段階で脆弱性を作りこまないように対処しておくべきです。

■不十分な開発標準、自作の開発フレームワークの使用

Spring や Struts など、広く利用されている開発フレームワークはセキュアな機能を内包していますが、開発者がそうした機能を使用していないケースが見受けられます。

そのようなことのないよう、設計者は、開発プロジェクトで使用する開発標準を作成する際、セキュリティに関して十分考慮し、全ての開発者が徹底順守するようにルールを定める必要があります。

また、自作の開発フレームワークの場合は、脆弱性対策が不十分になりやすいため、セキュリティ専門家の設計レビューを行うなど、より注意が必要と考えられます。

2. 納入後に考慮すべきこと

納入後のウェブサイトに影響する脆弱性が発見される可能性があります。たとえば、基盤ソフトやアプリケーション、ソフトウエア部品等の脆弱性が突然発見されるようなケースです。それらの脆弱性対策情報が公表された際に適切に対応できるように、システム構成を把握し、継続的に管理することが必要です。また、改修後には脆弱性の確認・検査を行うことも効果的です。

ウェブサイト構築事業者は、保守・運用のサポートを受けていない顧客から、脆弱性対策について助言を求められることがあります。したがって、少なくとも瑕疵担保期間は、ドキュメント等を管理し、そうした問合せに対応できるようにしておく必要があります。

2.1. 脆弱性はどのように見つかるか

ウェブサイトに深刻な脆弱性があったとしても、トラブルもなく稼動している場合、問題に自ら気づくことは容易ではありません。多くの場合、外部からの情報によって発覚すると考えられます。

■脆弱性の公表

ウェブサイトで使用している基盤ソフトやアプリケーションの脆弱性が製品開発ベンダや JVN で公表されることがあるので、常に情報収集に目配りする必要があります。バージョンによっても対応は異なるので、保守業務を受託していない場合には、ウェブサイトの構成情報を確認しておくことを顧客に薦めるべきでしょう。

■第三者からの指摘

ウェブサイトの脆弱性について、第三者から指摘を受けることがあります。たとえば、ユーザがウェブサイトを利用していて、偶然、重要情報にアクセスできてしまう可能性や、プログラムの動作から何らかの問題を内包している疑いに気づくことがあります。また、「ソフトウエア等脆弱性関連情報取扱基準」（平成 16 年経済産業省告示第 235 号）に基づき、独立行政法人情報処理推進機構（IPA）がウェブサイトの脆弱性について当該サイトの運営者に連絡し、脆弱性対策の実施を促すこともあります。

そうした問い合わせを受けた場合には、速やかに脆弱性の有無を調査するよう、顧客に薦めてください。

■悪意の第三者による攻撃

悪意の第三者による不正アクセス、コンピュータウイルスへの感染等のトラブルやその予兆をきっかけとして、プログラムの問題や設定ミスに気づくことがあります。ウェブシステムが不審な挙動を示した場合、外部から脆弱性を攻撃されたことが原因である可能性を検討するよう、助言すべきです。

2.2. 問題を招きやすいケース

納入後のプロセスで、脆弱性に係るトラブルを招く原因となりやすい事象として、たとえば以下のケースが挙げられます。

■システムのメンテナンスや統合・移行時の設定

納入当初は適切な設定であっても、システムのメンテナンスや統合・移行の際に、設定上のミスが生じることがあります。保守・運用を受託していないウェブサイト構築事業者には、対応の義務があるわけではありませんが、顧客のシステムにトラブルが生じる可能性をできる限り抑制するため、システムの構成情報や設定上の留意点に関する情報をドキュメント化して、顧客側に適切に引き継いでおくことが望まれます。

■環境の変化

開発当初の想定から逸脱した構成に移行したため、脆弱ではなかったものが脆弱になってしまうことがあります。たとえば、開発当初はクローズドな社内システムとして運用されていたものが、その後、会社の方針が変更され、外部ネットワークと接続されたことで、様々なセキュリティ上の問題が顕在化してしまうようなケースです。

こうした事態を避けるためには、変更を行う前に予想される問題を洗い出し、対策の適用に要するコストと変更による利便性の向上を比較して、その是非を判断することが望まれます。

■担当者や責任者の不在

システムを立ち上げた際の開発担当者や責任者がすでに退職していて、当時の状況がわからなくなることがあります。また、企業買収や倒産等が原因で開発事業者そのものが存続しておらず、開発担当者に連絡を取ることできなくなるケースも考えられます。

したがって、システムの構成情報や設定上の留意点に関する情報をドキュメント化して、保守・運用の契約がない場合には、顧客側に適切に引き継いでおくことが望まれます。

■委託元と委託先の連携不足

委託元と開発・運用の委託先が遠方の場合、脆弱性発覚時の切迫感が共有できず、柔軟な対応や細かい打合せができない可能性があります。

また、海外にサイトを設置し、その運用を現地の事業者に委託している場合、脆弱性が発見されると、その対応について英語でやりとりしなければならないため、意思疎通がスムーズにいかなかったり、時間がかかったりする可能性があります。

■配布するソフトウエアの版管理

必ずしもウェブサイト構築事業者の担当する部分とは限りませんが、顧客がウェブサイトで配布する目的で用意したソフトウエアに影響する脆弱性が発見された場合、顧客には問題について関

係者に連絡するとともに、当該ソフトウエアの脆弱性を解決した版を配布し直すことが求められます。

ウェブサイト構築事業者は、ダウンロード等の処理を委託されている場合、配布ソフトの脆弱性対策を早急に行うよう、顧客に促すことが望ましいと考えられます。

2.3. 脆弱性対応

ウェブサイト運営者である顧客は、脆弱性の可能性があれば調査・確認作業を行い、必要に応じてパッチ（脆弱性修正プログラム）の適用等の対策作業を行うことが求められます。脆弱性について関係する内部・外部の相手や、サイトの利用者との間の連絡窓口を設置し、情報の集約や管理にも取り組む必要があります。

こうした状況は、多くの顧客において不測の事態であり、自力では適切な対応が困難なことも考えられます。したがって、ウェブサイト構築事業者は、契約に基づきそうした顧客の危機をサポートするとともに、可能な範囲で対応について助言することが望まれます。

ウェブサイト構築事業者が調査・確認作業を代行する場合には、経緯と既に得た情報について顧客（ウェブサイト運営者）から説明を受けてください。顧客（ウェブサイト運営者）から脆弱性関連情報等の提供を受けた際には、受領通知を提出するようにします。この時点でウェブサイト構築事業者が確認した内容について顧客（ウェブサイト運営者）に簡潔に報告してください。

対処の詳細な作業については「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」（社団法人情報サービス産業協会、社団法人電子情報技術産業協会、http://www.jisa.or.jp/report/2004/vulhandling_guide.pdf ）を参考としてください。

■外部から連絡を受けた場合

外部から脆弱性関連情報の通知を受けた際には、通知者を含む関係者間で良いコミュニケーションを維持することが対応を成功させる鍵となります。

自発的・定期的に行われる脆弱性修正に比べると、外部から事実確認を急ぐよう求められることとなります。顧客（ウェブサイト運営者）にとっては負担にもなりますが、対処の方針・計画を整理した上で、可能な範囲で説明し理解を求めることが大切です。ウェブサイト構築事業者は、顧客（ウェブサイト運営者）とともに通知者との情報交換を行い、方針・計画の策定や対外説明を支援します。

通知は、IPA が顧客（ウェブサイト運営者）に通知してくる場合と、発見者が顧客（ウェブサイト運営者）に直接通知してくる場合の 2 つに大きく分けることができます。以下にそれぞれの場合について示します。

いずれの場合についても、顧客（ウェブサイト運営者）には、通知を受け取った旨の返信を速やかに行うよう説明してください。

・IPA から連絡を受ける場合の対応

ウェブサイトに関する脆弱性関連情報が発見者から IPA に届出られた際には、IPA からウェブサイト運営者に通知を行います。IPA からの通知は主に電子メール（ vuln-contact@ipa.go.jp ）を利用し行われます。また、迅速な対応をするためには、IPA からの連絡窓口（セキュリティ対応部署）を設置しておくことも有効です。

・発見者から直接連絡を受ける場合の対応

発見者が IPA を介さずに直接ウェブサイト運営者に脆弱性関連情報を通知してくることがあります。この場合は、発見者と誠実な対話に努めるようしてください。改めて IPA に届出るように発見者に求めるという選択もあります。

■トラブルが発生している場合

ウェブサイトにおけるセキュリティ上のトラブルに対しては、発見後の迅速な対応が必要です。不正アクセスの踏み台にされている場合、フィッシング詐欺等に悪用されている場合、ウイルスを撒き散らしている場合には、まずウェブサイトを停止し被害拡大を防ぎます。加えて、個人情報の漏洩や利用者へのウイルス送信等が発生した場合には、速やかな被害事実の公表も望まれます。

トラブルは、ウイルスや不正アクセス等にウェブサイトの弱点＝脆弱性を狙われて起きます。被害防止のためには、ウイルス等の駆除や監視強化等の処置だけでなく、ウェブサイトの脆弱性が原因である可能性を考慮し、丁寧な調査を行って「穴を見つけて塞ぐ」ことが大切です。

脆弱性への手当てが十分でないままサービスを継続して提供すれば再び被害を受ける可能性もあります。脆弱性の調査や修正には作業時間を取る必要があります。場合によってはサイトを一時的に停止するといった決断も必要です。

ウェブサイト運営者は、被害事実の公表やサービス再開のタイミングを考慮しながら、脆弱性に関する技術的作業を進めていく必要があります。ウェブサイト構築事業者は、顧客（ウェブサイト運営者）を支援し、問題解決やその技術的支援を行います。

付録８　連絡不能開発者一覧

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する。想定読者は、製品開発者本人である。

※対象製品の情報や脆弱性の内容の掲載は不要

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ェ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ェア製品で、インターネット等から入手し得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

付録９　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する。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ある。※脆弱性の内容の掲載は不要

【対象が企業の場合】

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

【対象が企業の場合（JVN 公開日追記）】

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。
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）

【対象が非企業（コミュニティを含む）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

【対象が非企業（コミュニティを含む）の場合（JVN 公開日追記）】

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。
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１０　セキュリティ担当者のための脆弱性対応ガイド

1. 欠かせない脆弱性への対処

1.1. 情報セキュリティ対策と脆弱性対策

情報セキュリティ対策には、技術面、管理面、法令対応など様々な観点があり、組織内の状況に応じてそれらを適切なバランスで実施する必要があります。

脆弱性対策は情報セキュリティ対策の一つで、攻撃を受ける弱点を減らす対策です。他の対策に注力していたとしても、脆弱性対策が不十分だと、次節に示すようなトラブルを招きかねません。セキュリティ担当者は、情報セキュリティ対策の一環として、情報システムの設計・開発、運用等の各フェーズで必要な脆弱性対策を実施することが求められます。また、脆弱性に起因するトラブルが発生した場合には、一連の対処業務の一つとして脆弱性対策を施し、問題が再発することを防がなければなりません。

1.2. 脆弱性に起因するトラブルとその影響

組織内の情報システムに脆弱性があると、どのような問題が生じるのでしょうか。情報システムに脆弱性があっても、それを悪用する攻撃がなければトラブルは起こりません。しかし、脆弱性が狙われて攻撃が成功すると、組織にとって深刻なトラブルに発展することがあります。

独立行政法人 情報処理推進機構（IPA）が 2010 年に実施した実態調査（IPA、http://www.ipa.go.jp/security/ciadr/vuln_report2010.pdf ）によると、脆弱性に起因するウイルスやワーム、不正アクセス等の被害経験については、ウェブサイト、組織内向けシステム、クライアント PC のいずれに関する被害についても 3 割前後の組織が「被害あり」としています。

生じる被害は、情報漏えいに伴う補償や事業中断、復旧対策等の直接的なコストだけではありません。それまで築き上げてきたブランドや社会的信用が失墜し、大切な顧客を失う影響は深刻なものです。

1.3. セキュリティ担当者に期待される役割

組織は、情報システムに起こりうるトラブルや影響を踏まえ、必要な脆弱性対策を実施する必要があります。もちろん、組織の情報システムにおいては、多くの場合、脆弱性対策が最優先課題ではないため、利用可能なリソースは限定的にならざるをえません。

したがって、組織のセキュリティ担当者（情報セキュリティ責任者、セキュリティ管理者）は、自組織に必要な脆弱性対策を無理のない形で適用するために、以下の役割を果たすことが期待されます。

■組織の情報セキュリティ責任者として

情報セキュリティ責任者は、組織としての観点から、脆弱性対策をどこまで徹底すべきか適切に判断し、取り組みの方針を明確に示すことが求められます。その線引きは容易ではありませんが、従業員の負担を含む対策コストと想定される被害を勘案し、実現可能な方針を示す必要があります。たとえば、組織外になるべく迷惑をかけないように、組織の外とつながっているシステムや外部からの預かり情報、業務上重要なシステムの安全性を優先して脆弱性対策を行う方向が考えられます。

また、情報セキュリティ責任者は、組織としての取り組みの方針に基づき、必要な予算、人員、作業時間等のリソースを確保する役割を担います。

さらに、情報セキュリティ責任者は、必要に応じて、セキュリティ管理者と情報システムのオーナー部門の間の調整を求められることもあります。

■現場のセキュリティ管理者として

現場のセキュリティ管理者は、組織としての取り組み方針を踏まえ、現実的な対策を検討し、それを推進することが期待されます。

具体的には、まず、現状の把握を行う役割があります。ソフトウェアの新たな脆弱性が見つかると、攻撃者はそれを狙った攻撃ツールやコンピュータウイルスを作成します。したがって、現場のセキュリティ管理者は、自組織の情報システムがどのようなソフトウェアで構成されているか、それらの脆弱性が発見されていないか、明らかになった脆弱性について対策すべきか、そうした現状の把握を継続的に行いつつ、必要に応じて対策を実施すること、また対策を実施するよう情報システムのオーナー部門に働きかけることが求められます。

また、このような現状把握の結果から対策の方針を定め、情報セキュリティ責任者に的確に説明することが期待されます。さらに、従業員に対しては、脆弱性対策の必要性を理解できるよう、研修等にも工夫を行うべきでしょう。

2. 脆弱性対策のポイント

脆弱性対策は、情報システムのライフサイクルの様々な場面に適用することが望まれます。たとえば、システム構築時には、発注者としての要求事項の中に、既知の脆弱性の解消とテストを組み込むべきです。また、運用時に脆弱性の存在が発覚することもあります。脆弱性がもたらすリスクを的確に判断し、場合によってはシステムを停止しても対策を適用しなければなりません。

しかし、システムオーナーであるユーザ部門によっては、脆弱性の問題を充分に理解せず、組織として適切な対処がとられない可能性があります。セキュリティ担当者は、そのような状況において必要な脆弱性対策を実施するよう、適切に指導・対応する立場にあります。

以下に、システムの設計・開発段階、運用段階の各フェーズにおける脆弱性対策の考え方を紹介します。また、脆弱性の存在が判明した際の対処手順や、システム開発・構築、運用等における委託先との関係についても説明します。

2.1. 設計・開発・導入段階における対策実施

すでに運用を開始しているシステムにおいてセキュリティ上の問題が発覚した場合、システムの作り直しは困難なため、場あたり的な対策で済ませたり、リスクを容認せざるをえないこともあります。そうした事態を避けるため、設計・開発段階で脆弱性をできる限り解消しておく必要があります。

また、システム開発の予算や開発期間を抑制するため、既存のソフトウェア部品やサンプルプログラムを流用することがあります。そうした既存のプログラムに脆弱性が内在していた場合、最悪トラブルが生じて初めてその問題が発覚するということになりかねません。したがって、安全性が担保されていないサンプルプログラムの安易な流用は避け、参考元の確認やプログラム作成後のレビューなどのルールを設けるべきでしょう。

■ウェブサイトの場合

IPA が実施した実態調査によると、インターネットに公開し、主に組織外とのやり取りに用いるウェブサイトについて、計画・設計から構築までの間に脆弱性の検査や修正などの対策を実施している組織は 5 割に満たない状況です。これは、公開ウェブサイトの構築において、デザインやコストが重視され、脆弱性対策に留意すべきことが認知されていないためと思われます。しかし、ウェブサイトは外部から攻撃を受けるリスクが高いことを踏まえれば、より手厚い脆弱性対策を施すことが望まれます。

頻出する「作り込まれやすい」脆弱性は、設計・開発段階で未然に解消することが望まれます。特に、脆弱性届出の上位を占めるクロスサイト・スクリプティングや SQL インジェクションの脆弱性は、プログラミングの際作り込んでしまうケースが大半であり、開発段階での確認・修正が不可欠です。したがって、セキュリティ担当者は、組織が用意する公開用のウェブサイトについて、

・開発委託の要件に脆弱性対策を加えること

・公開前に脆弱性を検査すること

を組織内のルールにするよう働きかけましょう。費用はかかりますが、脆弱性に起因するトラブル

を避けるための必要経費と考えるべきです。

また、キャンペーンや調査等の目的で一時的に設置するウェブサイトの場合、管理体制やチェックが曖昧になりがちです。個人情報を取り扱う可能性が高いこと、一旦トラブルになれば組織の責任は免れないことから、安全性を担保する方策を講じておくことが重要です。

詳しくは「ウェブサイト運営者のための脆弱性対応ガイド」や「ウェブサイト構築事業者のための脆弱性対応ガイド」を参照してください。

■組織内システムの場合

グループウェアサーバ、ファイルサーバ、ディレクトリサーバ、バックアップサーバ等、イントラネット上に配置される組織内向けシステムの場合、外部ネットワークに直接つながっていないため、脆弱性に起因するトラブルが発生する可能性は低いと思われがちです。しかし、1.2 に示したとおり、約 3 割の組織が組織内向けシステムの脆弱性対策の遅れやミスが原因で被害を経験しています。これを考慮すれば、組織内システムの脆弱性を放置することはリスク管理上妥当とは言えません。そのシステムで扱う情報資産の重要性、サービスの継続性・信頼性に対する要求レベル、サービスの公開範囲などを踏まえ、重要なシステムについては脆弱性対策を適用すべきでしょう。たとえば、次のようなシステムについては、対策が必要と考えられます。

・個人情報を扱うシステム

・取引先や顧客等からの預かり情報を扱うシステム

（受発注、技術情報、顧客の内部情報等）

・業務上の重要情報を扱うシステム

（経営、人事、製品設計、研究開発、生産管理、知財等）

具体的には、既製のソフトウェアを用いる場合には既知の脆弱性について設計・開発段階で解消することが望まれます。納入前にソフトウェアの構成やパッチの適用状況について把握し、必要に応じて最新パッチの適用が必要です。

また、システムを構成するソフトウェアとその脆弱性および修正状況に関する情報は運用においても重要なので、適切に管理し継続的に把握するようにしてください。独自のソフトウェアを用いて構築されるシステムの場合には、ウェブサイトの脆弱性と同様に、プログラミング段階で作り込んでしまいやすい脆弱性を設計・開発段階で未然に解消することが大切です。

■クライアント PC の場合

IPA が実施した実態調査によると、従業員のクライアント PC を導入する際に、ソフトウェアの脆弱性の検査や修正などの対策を「特にしていない」と回答した組織は 23.5%にもなります。「インターネットにはファイアウォールを介してつながっているので安全である」との判断があるかもしれませんが、近年、そのような従来の防御策を迂回して直接的に PC ユーザを狙う攻撃（偽サイトへの誘導、標的型攻撃、USB 経由のウイルス感染等）が急増している点を考慮すれば、そうした過信が危険なことは明らかです。

クライアント PC のセキュリティ確保のためには、脆弱性の修正（パッチの適用）がとても重要です。未対策の脆弱性はトラブルの根本的な原因となり、重大な問題を引き起こしうるものです。セ

キュリティ担当者、委託先、エンドユーザの誰が脆弱性対策を施すかは組織の規模や体制、予算等によって異なりますが、クライアントPCは導入時にできる限り必要なパッチの適用を済ませておくことをお薦めします。

また、OS、アプリケーション、プラグイン等のソフトウェアは長期にわたり使い続けることになりますが、古い製品には多数の脆弱性修正を施す必要があるだけでなく、サポートの期限が切れた場合には脆弱性が発見されてもパッチが提供されない事態にもなり得ます。導入時にソフトウェアをいつまで使い続けるかを計画し、サポートが途絶える前に円滑に新たなソフトウェアに移行することもトラブルを未然に防ぐ脆弱性対策のひとつです。

2.2. 運用段階における対策実施

ソフトウェア製品の脆弱性は突然公表されることがあります。新たな脆弱性が発見されれば、日を置かずにそれを狙う攻撃ツールやコンピュータウイルスが作られ流布されます。新たな脆弱性が自組織の情報システムの中にある場合には、その脆弱性を速やかに改修する必要があります。

したがって、情報システムの運用段階においては、脆弱性対策に継続して取り組むことが求められます。

■組織のソフトウェア構成や変更の状況を管理すること

公表された脆弱性が自組織に影響するかどうかを判断するためには、自組織における情報システムのソフトウェア構成（ソフトウェアの種類、バージョン等）や変更履歴（パッチの適用等）を日頃から把握しておくことが大切です。これによって、新たに明らかになった脆弱性の情報を得て迅速な対応を始めることができます。

ソフトウェア構成や変更の状況を管理するためには、たとえば、情報システム導入に際し、導入部門が必要なデータを登録するルールやしくみを整備する必要があります。また、管理を支援するツールも活用可能です。たとえば、IPA では利用しているソフトウェア製品のバージョン確認を支援する「MyJVN バージョンチェッカ」を無料提供しています。

ただし、組織の規模が大きくなると、管理を徹底することが難しくなる場合もあります。また、組織内のシステムの中には、組織変更や異動、移転等により、構成を把握している担当者がいなくなって管理が曖昧になった機器があるかもしれません。そうしたシステムの脆弱性が放置され、トラブルの原因となることがあります。2003 年に猛威をふるったコンピュータワーム「Blaster」は、放置されたシステムの脆弱性対策が遅れたため、被害が拡大しました。

このような問題の解決策として、統合管理ツールを活用して、機器に搭載されているソフトウェアの種類とバージョン、パッチの適用状況等を集中管理する方法があります。

なお、運用時に不要になったサービスは停止するなど、セキュリティを考慮した設定変更も重要です。

また、情報システムのライフサイクルを意識することは重要です。古い OS やアプリケーションは新しい攻撃への耐性に乏しいものです。リスクが徐々に高まることを考慮して導入当初から計画を立てておき、適正な時期がきたら次バージョンへの切り替えを進めることが望まれます。アプリ

ケーションの動作環境を維持する必要がある場合には、仮想マシン上に動作環境を移行することも選択肢の一つです。

■脆弱性情報を収集すること

脆弱性情報を収集し、自組織のシステムに影響しうる脆弱性については対応を検討します。脆弱性情報は一部の例外を除き、製品ベンダから予告なく突然公表されますから、常に情報収集を心がける必要があります。情報源としては、製品ベンダがホームページ等に示すカスタマ向け情報、セキュリティ製品・サービスのベンダや情報セキュリティ関連機関がホームページやメール等で提供する脆弱性関連情報のアドバイザリなどが挙げられます。

こうした情報収集はユーザ部門では難しいため、セキュリティ担当者が実施し、必要に応じて組織内に提供することが望まれます。スタッフが足りず、網羅的な常時収集が難しい場合であっても、特に業務に影響が大きいソフトウェアに対象を絞り込んで、何名かで分担し定期的な確認に取り組むべきです。ソフトウェア構成に基づいて収集する範囲を絞り込み、効率的な情報収集を行うことも有効です。たとえば、IPA では「MyJVN 脆弱性対策情報収集ツール」

（IPA、 http://jvndb.jvn.jp/apis/myjvn/ ）を無料提供しています。これは、いくつかの情報を登録するだけで、自分に関係する脆弱性対策情報を自動的に収集・表示するツールです。なお、運用管理を外部に委託している場合には、脆弱性情報の収集を委託業務に含めるよう調整することも可能でしょう。

また、自組織が公開するウェブサイト等について脆弱性があるという連絡を組織外から受けることがあります。その場合は放置せずに、連絡を受けた内容と実態を確認して、対処について適切な判断を示すべきです。業務継続の必要性や改修の難度から、対策実施を先延ばしにする判断もありますが、それによってウェブサイト等にアクセスした利用者が影響を受けるリスクも高まることを熟慮し、適切に対処することが望まれます。

■脆弱性検査を行うこと

公開用ウェブサイトは、組織内のスタッフもしくは外部の事業者に委託して、脆弱性検査を行うようルール化することをお薦めします。予算等の制約で定期的な実施が難しい場合には、構築・改変時に実施する形でも有効です。

IPA が実施した実態調査でも、全体で 5 割超、大企業等では約 8 割が運用中のウェブサイトの脆弱性検査を実施しており、2 割の組織が検査を通じて脆弱性に気づいた経験を有することが報告されています。

■修正プログラム（パッチ）を適用すること

脆弱性が自組織の情報システムのソフトウェアに存在していると判明した場合、対策を適用すべきか否かを判断する必要があります。専門的な知識が必要なため、セキュリティ担当者が判断を行ないます。その際、セキュリティ製品・サービスのベンダが示す脅威レベルの評価やソフトウェア製品ベンダの提供する脅威及び修正適用に伴う影響の情報等が参考になります。また、外部の事業者に運用を委託している場合は、相談することも有効です。

また、最終的にはシステムのオーナー部門の合意が不可欠となります。対処を円滑に進めるた

めに、組織内の合意形成を含む対処手順を定め、文書化しておくことが重要です。

たとえ外部と接続していないネットワークシステムの場合でも、内部にウイルスを持ち込まれる可能性も踏まえて、対策の要否を検討すべきです。

パッチの適用にあたっては、可能な限り事前にテストを行い、運用に支障がないことを確認した上で改修に着手することが望まれます。また、クライアント PC など、台数が多く手作業でのパッチ適用に手間がかかる場合は、統合管理ツールを活用すれば作業の自動化が可能です。

最近増えている、未公表の脆弱性を悪用する「ゼロデイ攻撃」については、パッチが提供されるまでの間は一時的な対策として IPS（侵入防御システム）で攻撃を抑止し、提供され次第パッチを適用するという対処が可能です。

2.3. 脆弱性の存在が判明した際の対処手順

脆弱性の存在が明らかになった場合、セキュリティ担当者は以下の作業を行ないます。場合によっては、外部の委託先と連携した取り組みも可能です。

① **セキュリティ上の問題の有無に関する調査**

入手した脆弱性情報について、組織内の情報システム上の脆弱性の有無や問題が発生する条件等を調査します。

② **影響と対策の方向性の検討**

問題箇所が及ぼす影響を明確にして、修正方法や回避方法を検討します。

③ **対策作業計画の策定**

対策作業を進める手順や期間等について計画を策定します。費用、人員等を勘案しつつ、代替機でのテスト、対策実施に伴うサービスの停止と再開等を計画します。代替機を用意できない場合、ソフトウェアの仮想環境の利用などで、比較的低予算でテストを行うことが可能です。

④ **対策の実施**

作業計画に基づき対策を実施します。

なお、ウェブサイトの脆弱性については、脆弱性検査で発見される場合だけでなく、外部から連絡を受けて知らされる場合や、実際に問題が発生する場合も想定されます。

■第三者から指摘された場合

第三者から脆弱性の存在を指摘された際には、通知者を含む関係者間で良いコミュニケーションを維持することが対応を成功させる鍵となります。

通知には、IPA がウェブサイトの運営者に通知してくる場合と、発見者がウェブサイトの運営者に直接通知してくる場合の 2 つがあります。いずれの場合についても、連絡を受ける部署（問い合わせ窓口等）には、通知を受け取った旨の返信を速やかに行うよう説明してください。

・ **IPA から連絡を受ける場合の対応**

ウェブサイトに関する脆弱性関連情報が発見者から IPA に届出られた際には、IPA からウェブサイト運営者に通知を行います。IPA からの通知は主に電子メール

（vuln-contact@ipa.go.jp）を利用して行われます。

- **発見者から直接連絡を受ける場合の対応**

  発見者が IPA を介さずに脆弱性情報を直接ウェブサイト運営者に通知してくることもあります。この場合は、発見者との誠実な対話に努めるようしてください。

■トラブルが発生している場合

ウェブサイトにおけるセキュリティ上のトラブルに対しては、発見後の迅速な対応が必要です。特に、外部に悪影響を及ぼす状態にある（不正アクセスの踏み台にされている、フィッシング詐欺等に悪用されている、ウイルスを撒き散らしている等）場合には、まずウェブサイトを停止し被害の拡大を防ぎます。また、個人情報の漏洩や利用者へのウイルスの配布等が発生した場合には、速やかな被害事実の確認と公表、主務官庁等への報告も望まれます。

応急措置的な対策としては、WAF（ウェブ・アプリケーション・ファイアウォール）を用いて攻撃を凌ぐことも可能です。より恒久的な対策としては、ウイルス等の駆除や監視強化等の処置だけでなく、ウェブサイトの脆弱性が原因で侵害された可能性を考慮し、丁寧な調査を行って「入口にされた穴を見つけて塞ぐ」ことや「不正に開けられた裏口を探して閉じる」ことが重要です。手当てが不十分なままサービスを継続／再開すればトラブルを再発する可能性もあります。調査や脆弱性修正には十分な作業時間を取る必要があります。場合によっては作業のためにサービスを一時的に停止するといった決断も必要です。

セキュリティ担当者は、組織のリスク管理担当者や当該システムのオーナー部門、外部の専門事業者等と調整し、被害事実の公表やサービス再開のタイミングを考慮しながら、対策実施を主導する必要があります。

2.4. 委託について

脆弱性対策を含む情報システムの設計・開発、運用のセキュリティ管理に関する人的資源が充分でない場合、適切なスキルを有する事業者に委託することも有効です。ただし、曖昧な取り決めや不十分な合意形成が原因となって、問題化する可能性もあります。

■契約時に合意すべき事項

契約時には、以下のような脆弱性対策の取扱いについて、委託先と合意を取り付けることが望まれます。セキュリティ担当者は契約主体である情報システムのオーナー部門を支援し、合意形成を推進します。

- **納入後に公表された新規の脆弱性対策**

  ソフトウェア製品の脆弱性のうち、納入後に公表されたものについては、対策は有償と捉え、システム開発とは別の保守契約で対応することが適切と考えられます。

- **既知の重要な脆弱性対策**

  ソフトウェア製品の既知の重要な脆弱性やウェブサイトの著名な脆弱性の対策に関する著しい認識不足、ウェブサイトに対する設定ミスなど、委託先の責に帰する場合は無償とすべきです。

・ **脆弱性検査の実施の有無**

稼動中のウェブサイトに対し（もし可能であるならば納入前に）脆弱性検査を行い、脆弱性が見つかった場合にはその対策を施すことを契約に含めるべきです。引渡し段階ではウェブサイトが稼動していない場合も多いため、検査を計画的に実施するための配慮も必要です。

・ **緊急事態時の費用負担**

緊急事態の際は迅速な対策を要求されるため、組織と委託先との間で作業範囲、費用負担について十分な協議のないまま、作業を進める状況が多々あると予想されます。契約の段階で明確にしておくべきですが、それが難しい場合にも、極力、覚書として残しておくことが望ましいと考えられます。

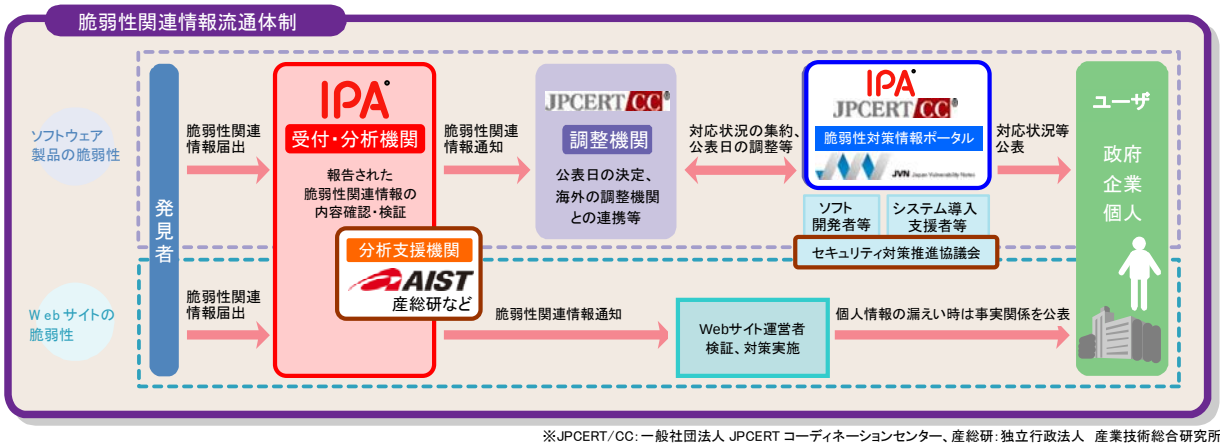
詳しくは経済産業省「アウトソーシングに関する情報セキュリティ対策ガイダンス」を参照してください。

・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、「ソフトウエア等脆弱性関連情報取扱基準」（平成 16 年経済産業省告示第 235 号）の告示を踏まえ、2004 年 7 月からソフトウエア製品及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。

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

「情報セキュリティ早期警戒パートナーシップ」



※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：独立行政法人　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。

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

http://www.jpcert.or.jp/vh/#guideline

・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

http://www.ipa.go.jp/security/　TEL: 03-5978-7527　FAX: 03-5978-7518

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

〒101-0054　東京都千代田区神田錦町 3-17　廣瀬ビル 11 階

http://www.jpcert.or.jp/　TEL : 03-3518-4600　FAX : 03-3518-4602

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

［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