IPA

Information-technology Promotion Agency, Japan

# 脆弱性ハンドブック

## Vulnerability Handbook

独立行政法人**情報処理推進機構**

# まえがき

2011年3月の東日本大震災や原発事故、さらに燃料供給網の寸断や電力不足等により、我が国の経済活動や社会生活は激しく動揺し、様々な方向から事業継続が脅かされる事態に陥った。

一方、情報セキュリティの分野においても、民間企業や政府機関を標的としたサイバー攻撃による被害が次々と発覚し、改めてITリスクの深刻な影響規模が注目を集めることとなった。たとえば、複数の有力ゲームメーカが相次いで海外子会社のウェブサイトに不正アクセスを受け、大量の個人情報やメールアドレス等が流出したと見られるケース、また、防衛産業の重要拠点や衆議院・参議院の管理サーバが標的型攻撃により侵入され、一部のデータが流出した可能性があるケースなど、枚挙に暇がない。

このように、我が国の情報セキュリティを取り巻く情勢は、急速に変貌しつつある。特に、攻撃者がより巧妙かつ戦略的なスタイルにシフトしていることから、政府や企業はこれまで以上に効率的・効果的な対策に取り組む必要がある。特に、様々な脆弱性が攻撃に悪用されている現況を鑑みれば、脆弱性対応が情報セキュリティの確保に重要な意味を持つことは明らかである。

政府やIT業界、セキュリティ機関等が情報セキュリティ確保のために協力する形で実現した「情報セキュリティ早期警戒パートナーシップ」は、2004年7月の運用開始より、ソフトウエアの脆弱性という問題に対処する官民連携の枠組みとして機能してきた。2012年9月末の時点で届け出られた件数の累計は7,950件（ソフトウエア製品に関する脆弱性：1,424件、ウェブサイトに関する脆弱性：6,526件）に達している。

独立行政法人情報処理推進機構においては、「情報システム等の脆弱性情報の取扱いに関する研究会」の主導のもと、脆弱性対策の実態を把握するとともに、企業を中心とした利用者、ソフトウエア製品開発者、ウェブサイト運営者における脆弱性対応の取組みを促す方策の推進に取り組んでいる。本書は本研究会のこれまでの成果を集約し、幅広い読者にむけて提供するものである。これまでの検討と活動にご尽力いただいた関係各位にあらためて深く御礼申し上げる。

2013年3月

情報システム等の脆弱性情報の取扱いに関する研究会

座長 土居 範久

# 目　次

# 目的別インデックス

■「脆弱性に関するトラブルの事例について知りたい」

→　10 ページ、2.2. 脆弱性に起因するトラブルとその影響

■「ウェブサイトの脆弱性について連絡を受けたので対処方法を知りたい」

→　39 ページ、4.2. ウェブサイト運営者における脆弱性対応

■「開発するソフトウエアの脆弱性をなくすための取り組みについて知りたい」

→　62 ページ、5.1. ソフトウエア製品ライフサイクルにおける脆弱性への取り組み

→　101 ページ、7. システムライフサイクルと脆弱性対策

# 1. はじめに

## 1.1. 謝辞

独立行政法人情報処理推進機構（以下、「IPA」という。）では、2003年11月に有識者や研究者、専門家等で構成される「情報システム等の脆弱性情報の取扱いに関する研究会」を設置し、未公表のソフトウエアの脆弱性の取扱いについて検討を重ね、その結果を踏まえ現在の届出制度（情報セキュリティ早期警戒パートナーシップ）が整備されました。

2004年7月の運用開始以降も、同研究会は継続して開催され、制度に関連する様々な課題について検討が重ねられてきました。本研究会やWGの委員の方々、関連の調査にご協力くださった関係各位に深く御礼申し上げます。

また、本書を作成するにあたり、一般社団法人JPCERTコーディネーションセンター（以下、「JPCERT/CC」という。）をはじめとする関係機関のコンテンツを参考にさせていただきました。この場を借りて、厚く御礼申し上げます。

## 1.2. 本書の構成と使い方

### 1.2.1. 構成

まず、2 章では、全ての読者を対象に、脆弱性とはどのようなものか、その概要を説明し、実際に起きた脆弱性に起因するトラブルや影響について事例を紹介します。また、国内の脆弱性関連情報の取扱いの枠組みである「情報セキュリティ早期警戒パートナーシップ」の活動についても解説します。

次に 3 章では、企業等の組織において情報システムのセキュリティを担当する方を主な対象として、脆弱性について SI 事業者に委託する際に考慮すべき点などを含めた全般的な脆弱性対策を説明します。

4 章では、ウェブサイトを運営される方、ウェブサイトの構築・運用に携わる方を主な想定読者としています。この章では、ウェブサイト運営の意思決定者や組織において脆弱性の確認や修正作業を担当するウェブサイト技術者を対象に、ウェブサイトの脆弱性について運営者が問われる責任、求められている継続的な対策、脆弱性に関する通知を受けた場合の望ましい対応手順などを説明します。

また、情報サービス企業の技術者やウェブデザイナー、企業内でウェブサイトの構築・運用を担当する技術者を対象に、システムの納入前や納入後に考慮すべきことをまとめて解説します。

5 章では、ソフトウエア製品開発者を主な想定読者としています。ソフトウエア製品開発における脆弱性対策の推進に関して、脆弱性情報の取扱いに関する連絡体制の整備、実際に連絡が来たときの対応方法について述べ、ソフトウエア製品開発者による脆弱性対策情報の公表の参考として、望ましい公表手順について示します。また、特に組込みソフトウエアの開発における脆弱性対策を推進する方策について解説します。

6 章では、参考情報として、国外における脆弱性対策の状況に関して、米国政府の推進する取り組みを解説します。また、脆弱性対策に関する国際標準化の現在の動向を説明します。

7 章では、参考情報として、ソフトウエア製品やウェブサイトなどのライフサイクルに沿って、その時々に実施すべき脆弱性対策について述べます。本文で該当する箇所を示すとともに、IPA ウェブサイト等より入手可能な脆弱性関連の各種資料について概要を紹介します。

### 1.2.2. 本書における記号や表記

難解な用語や本書以外の資料などについては、ページ下部に脚注で説明しています。記載された内容が本書の他の箇所と関係している場合には、参照する先を脚注で「⇒」と表記しています。

# 2. 脆弱性対応の意義

情報セキュリティ上の「弱点」を突いて、情報システムに侵入したり、コンピュータウイルスを感染させたりといった攻撃が目立つようになってきました。プログラムや設定上の問題に起因するこのような「弱点」は脆弱性（ぜいじゃくせい）と呼ばれます。

この章では、脆弱性とはどのようなものか、その概要を説明し、実際に起きた脆弱性に起因するトラブルや影響の事例を紹介します。また、国内の脆弱性関連情報の取扱いの枠組みである「情報セキュリティ早期警戒パートナーシップ」の活動について解説します。

## 2.1. 欠かせない脆弱性への対処

### 2.1.1. 時間が経つと情報システムの安全性は低下する

現在の社会活動は、様々な局面において情報システムに支えられています。コンピュータ・ソフトウエアの機能は劣化せずにいつまでも問題なく動くように思われています。ところが、情報システムを取り巻く脅威は日々変化しています。ある日突然情報システムに対する新しい攻撃手法が編み出されたり、情報セキュリティ上の「弱点」が発見されたりします。開発・構築時から何年間も更新されていないシステムは、そのような脅威の変化に対応できません。昨日まで安全だった情報システムが今日も安全であるとは限らないのです。

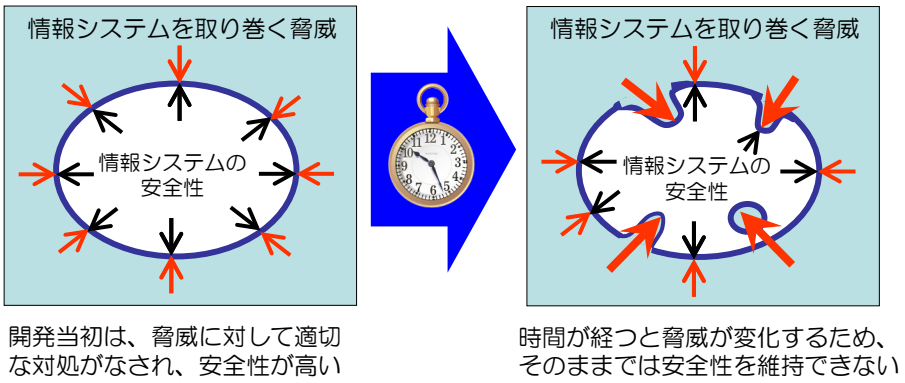



**図 2-1 情報システムの脅威と安全性の変化**

### 2.1.2. 脆弱性とはなにか

数年前から、情報セキュリティ上の「弱点」を突いて、情報システムに侵入したり、コンピュータウイルスを感染させたりといった攻撃が目立つようになってきました。プログラムや設定上の問題に起因するこのような「弱点」は脆弱性（ぜいじゃくせい）と呼ばれています。

悪意を持った者（攻撃者）は、脆弱性を利用し、インターネットにつながる利用者の PC やウェブサイトを動かすサーバを攻撃し、機器やサービスを利用不可能にしたり情報を盗み出したりといった犯罪的行為を行います。脆弱性を悪用した攻撃が行われると、たとえば想定外の入力データがメモリ上にあふれたり、本来許容しないはずのコマンドを受け入れてしまったりといったトラブルがコンピュータの上で起きます。そのような混乱を悪用されてコンピュータへの不正な操作をされてしまいます。

「自分は悪意や攻撃などとは無縁だ」と考えるかもしれませんが、既知の脆弱性を有するパソコンをインターネットに接続すれば、わずか数十秒で自動的にコンピュータウイルスに感染すると言われています。脆弱性の問題は決して他人事ではありません。

脆弱性を放置していると、大きなトラブルを招く可能性があります。ある企業では、放置していた

自社ウェブサイトの脆弱性を悪用され不正侵入された結果、利用者のメールアドレスが大量に流出した上に、サービスも停止せざるをえなくなりました。その結果、数億円規模の売上が失われ、株価も急落し、社会的信用まで失う事態に陥っています。

### 2.1.3. 脆弱性対策が必要な理由

脆弱性は日々発見されていて、すでに数万種類もの脆弱性が公表されています 。情報システムへの攻撃者は、まず、このような既に判明している脆弱性の悪用を試みます。したがって、情報システムを利用する立場の方にあっては、自分の管理する情報システムに存在する既知の脆弱性をできるだけ残さずに直すことが重要です。脆弱性対策を行わなければその脆弱性を狙うコンピュータウイルスの駆除を行っても後に同じ脆弱性を狙う新たなコンピュータウイルスに感染する可能性が残ります。

また、インターネットにつながるコンピュータや情報機器は、昨日まで安全であっても、脆弱性が発見されれば、突如として危険な状態になります。なぜなら、脆弱性の存在が知られると、それを攻略する攻撃プログラムやツールがインターネット上に公開され、脆弱性を狙ったコンピュータウイルスが登場する可能性が急速に高まるからです。新たな脆弱性については攻撃に悪用される前に速やかに対処することが望まれます。

ソフトウエア製品の脆弱性の場合、製品開発者が提供する修正プログラム（パッチ）[1]を適用して解決します。また、ウェブサイトのように自ら開発したプログラムの脆弱性の場合、自身で問題箇所を改修する必要があります。

脆弱性を根絶することは容易ではありません。しかし、脆弱性を悪用する攻撃が実際にある以上は、安全性向上のために脆弱性を減らす努力が求められています。

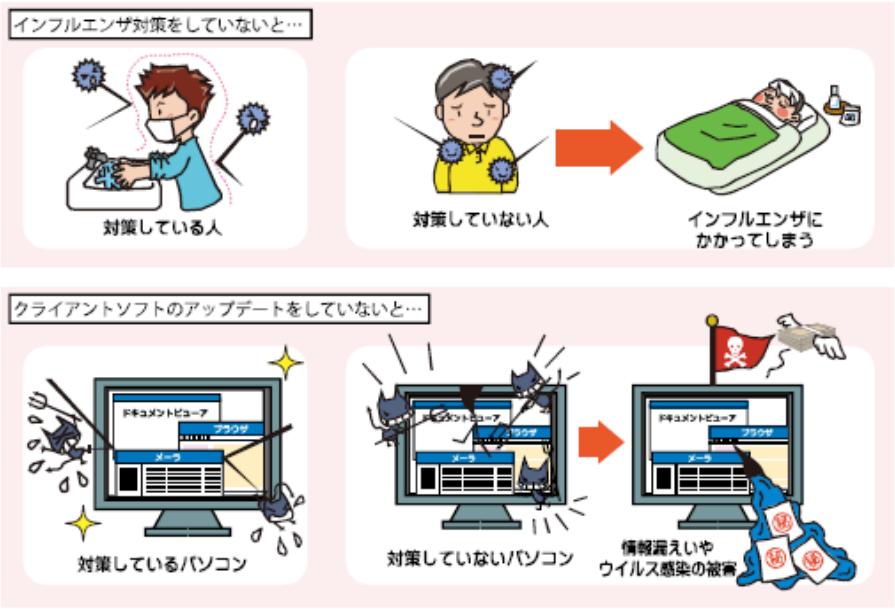



**図 2-2 脆弱性対策のイメージ**

[1] ⇒ 本書用語集「パッチ」

## 2.2. 脆弱性に起因するトラブルとその影響

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。

IPA が 2010 年に実施した実態調査[2] によると、脆弱性を狙ったコンピュータウイルスやワーム、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。別の調査では 2009 年に被害に遭った企業では平均 200 万ドルの損失が発生したことが報告されています[3]。

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。

実際に起きている脆弱性に起因するトラブルとは、どのようなものでしょうか。以下では、近年の脆弱性に起因するウェブサイトのトラブル事例をいくつか紹介します。

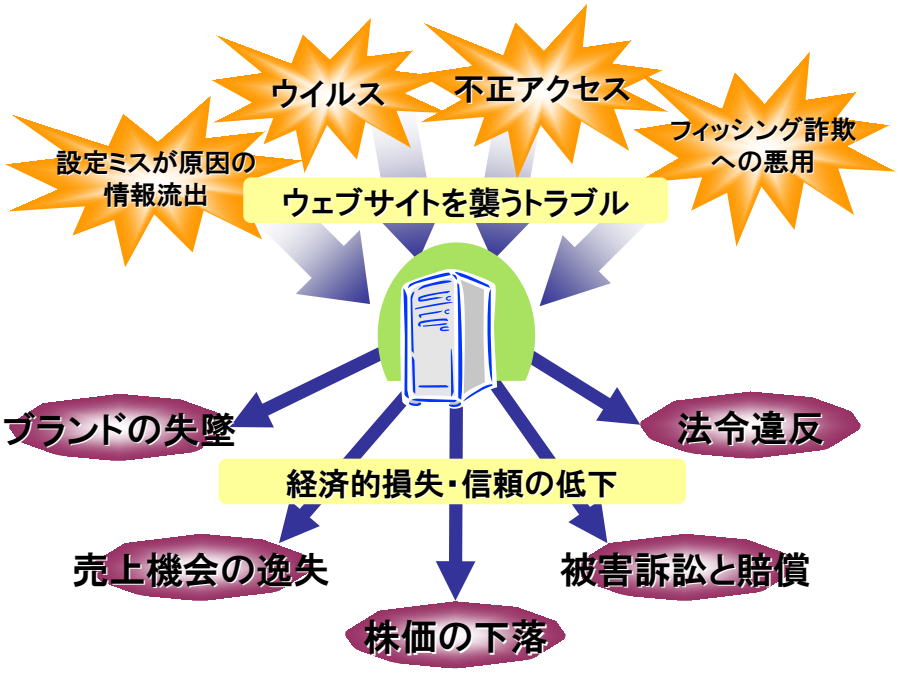



**図 2-3 ウェブサイトで起きるトラブル**

---

[2] IPA, “企業等における脆弱性対策に関する実態調査報告書”, (2010 年 7 月実施。310 機関回答), http://www.ipa.go.jp/security/ciadr/vuln_report2010.pdf

[3] Symantec; “2010 State of Enterprise Security Report”, 2010/03 http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=sesreport2010

### 2.2.1. 不正アクセスによる情報流出と事業中断

悪意のある第三者がウェブサイトに対し侵入を行ったり、ウェブサイトのシステムがコンピュータウイルスに感染した結果、個人情報などの重要情報が詐取されたり、ウェブサイトをさらに悪用するために改造されることがあります。このようにして脆弱性を悪用された結果、事業そのものを中断する事態にまで発展することがあります。

#### (1) トラブル事例 1　情報流出と事業中断

複数の中堅小売のネットスーパー運営を請け負う事業者のウェブサイトが不正アクセスを受け、クレジットカード番号や名義、有効期限など約 1 万 2000 件が外部へ流出しました。これらの不正アクセスの手口はデータベースを操作するウェブアプリケーション[4]の脆弱性を狙う比較的良く知られた手法であり、対策の必要性がセキュリティ専門家により繰り返し指摘されているものでした。当該事業者のいくつかでは、よりセキュリティレベルの高いシステムを導入するまでウェブサイトの運用を停止することを発表しました。

#### (2) トラブル事例 2　情報流出と事業中断

2005 年 5 月、情報提供サービス A 社では、自社の情報サイトに侵入されその対応が遅れたため、エンドユーザのメールアドレスが大量に流出した上に、サービスを約 10 日間停止せざるをえない事態に陥りました。その結果、売上は 1 億 5000 万円～2 億 5000 万円程度減少し、90 万円台後半だった株価は一時 80 万円台後半に急落するなどの金銭的被害を受けました。さらに、こうした影響は自社内にとどまらず、株主や取引先、エンドユーザなどのステークホルダにも及び、A 社の社会的信用は大きく損なわれました。

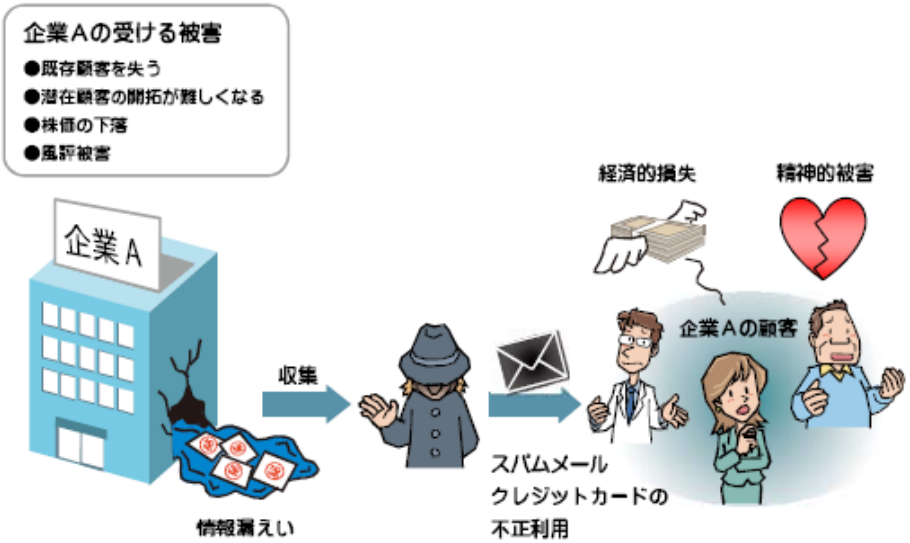



**図 2-4 情報漏えいによる影響**

[4] ⇒ 本書用語集「ウェブアプリケーション」

### 2.2.2. コンピュータウイルスへの感染

たった1台のPCに修正されていない脆弱性があったために、コンピュータウイルスへの感染から事業が脅かされることもあります。

#### (1) トラブル事例3　ウイルス感染が元で起きたウェブサイトの改ざん

2009年から2010年にかけてはGumblar(ガンブラー)と呼ばれる手口が猛威を振るいました。この手口では、ウェブサイト更新用のPCが、脆弱性を悪用するコンピュータウイルスに感染することで、企業ウェブサイトの大きな被害につながります。FTP(File Transfer Protocol)のログインアカウント情報が盗み出されて、閲覧者を不正なウェブサイトへと誘導するように企業ウェブサイトが改ざんされたため被害は拡大しました。有名企業のウェブサイトが次々と改ざんされた結果、企業自身が提供する本物のウェブサイトも信用できない状況にまで陥りました。

このように、組織が提供するウェブサイトが改ざんされると、組織の信用失墜や顧客離れにつながりかねません。

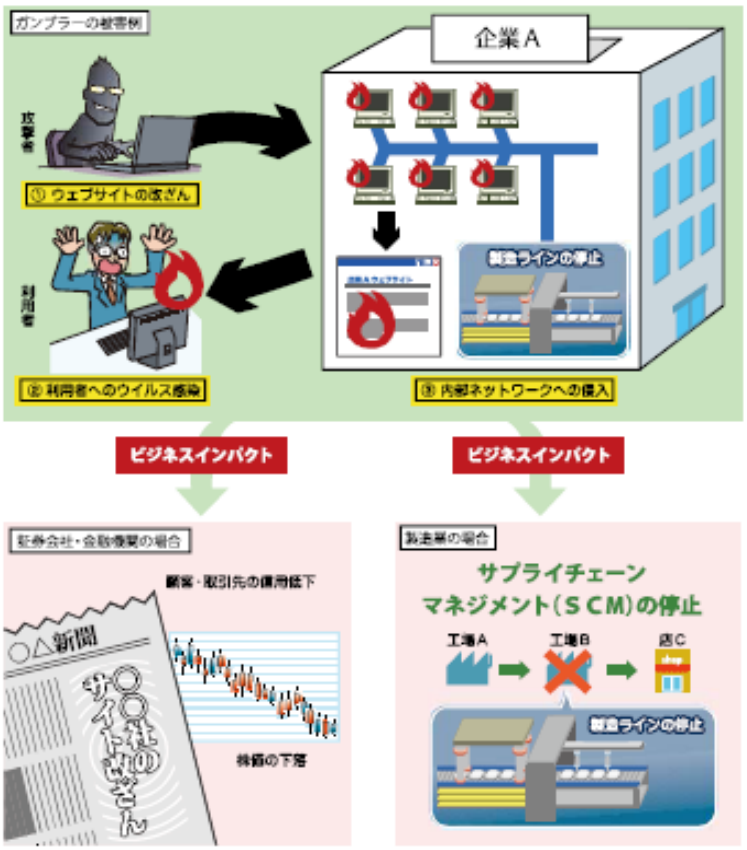



**図 2-5　Gumblar(ガンブラー)がもたらすビジネスインパクト**

### 2.2.3. 設定ミスによる個人情報の流出

システム管理者の設定ミスが情報流出のトラブルを招くこともあります。たとえば、個人情報の含まれた重要ファイルが、誤ってウェブサイトの公開ディレクトリに置かれているケースです。こうしたミスは、サーバの更新や新システムへの移行などの変更時に生じることが多いと考えられます。

#### (1) トラブル事例 4　設定ミスによる個人情報の流出

2002 年 5 月、エステティック事業の B 社が運営するウェブサイトで、約 5 万人分の個人情報を含む電子ファイルが誤って閲覧可能な状態になっていたため、外部に流出してしまいました。流出した電子ファイルは、回収することが事実上不可能で、今なおファイル共有ソフトを介してネットワーク上で流通していると見られます。複数の被害者が B 社を相手にプライバシー侵害に関する訴訟を起こし、地裁は B 社に一人当たり数万円の賠償金を支払うよう命じる判決を下しました。

### 2.2.4. フィッシング詐欺へのウェブサイトの悪用

自組織のウェブサイトをフィッシング詐欺[5]などの犯罪行為に悪用されることもあります。

フィッシング詐欺の手口としては、本物のウェブサイトによく似た URL で偽のウェブサイトを作り、誤ってアクセスした利用者を騙す手口が広く知られていますが、本物のウェブサイトにある脆弱性を狙い、利用者に見破り難い偽ページを閲覧させて情報を奪う手口もあります。ウェブサイトにクロスサイト・スクリプティング[6]の脆弱性がある場合、これを悪用されてしまうと、自社のウェブサイトにアクセスしてきた利用者が偽サイトへ誘導され ID・パスワードやクレジットカード番号などを詐取される可能性があります。

このように組織のウェブサイトが攻撃に悪用され、結果的に実害が発生した場合、当該組織は社会的責任の観点から厳しく非難され、大きく信用を失う可能性もあります。

#### (1) トラブル事例 5　ウェブサイト上へのフィッシング詐欺サイトの設置

自治体が運営するウェブサイトが不正アクセス[7]を受け、ウェブサイトをフィッシング詐欺サイトに仕立て上げられていたことが判明しました。当該自治体では謝罪の連絡をとりつつ、再発防止策に取り組みました。

---

[5] ⇒ 本書用語集「フィッシング詐欺」
[6] ⇒ 本書用語集「クロスサイト・スクリプティング」
[7] ⇒ 本書用語集「不正アクセス」

### (2) トラブル事例 6　ウェブサイト脆弱性のフィッシング詐欺への悪用

2006 年には、米最大手のオークションサイトにクロスサイト・スクリプティングの脆弱性が発見され、さらに、この脆弱性を悪用したフィッシングサイトも出現しました。同ウェブサイトの利用者が脅威にさらされたことによって、顧客との信頼関係がビジネス基盤である同社のブランドの失墜が懸念されました。


**図 2-6 フィッシング詐欺のイメージ**

## 2.2.5. 脆弱性によるその他のトラブル

そのほか、ウェブシステム [8]がダウンしサービス停止に陥ったり、表示内容が書き換えられたりといったトラブルが発生する可能性があります。

[8] ⇒ 本書用語集「ウェブシステム」

## 2.3. 情報セキュリティ早期警戒パートナーシップとは

ソフトウエア製品やウェブサイトなどの情報システム等の脆弱性は、近年、不正アクセスやコンピュータウイルス等[9]の攻撃に悪用されその原因となっています。

脆弱性については発見者から開発者へ適切に情報が伝えられた上で対策が用意されるべきですが、適切に扱われずに問題が放置されたり、対策が整わない段階で暴露されたりすることで大きな被害をもたらす危険性があります。また、脆弱性の存在が知られてからそれを攻撃する方法が流布するまでの期間は近年非常に短くなっています。

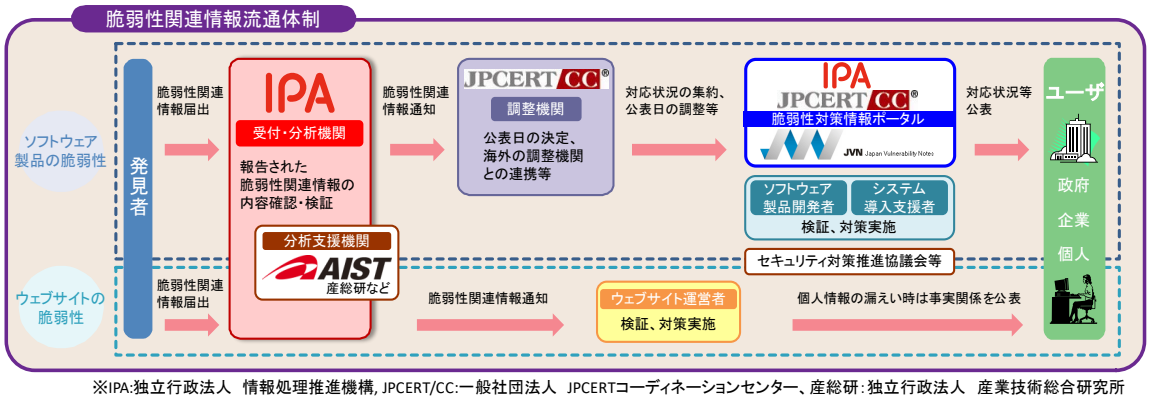
そこで、対策が講じられる前の脆弱性情報を適切に流通させ、対策を推進するための取り組みとして、脆弱性情報の取扱いに関する枠組み「情報セキュリティ早期警戒パートナーシップ」が作られています。この取り組みは適切な公表に関して関係者間で調整を行うこと、日本国内のソフトウエアの脆弱性検証を推進すること、ウェブアプリケーションの脆弱性の対処を促すこと等を目的としています。

国内で利用されるソフトウエア製品やウェブサイトに脆弱性を発見した場合には、この取り組みによる届出制度を利用することで、製品開発者やウェブサイト運営者との連絡をより円滑に進め、対策が取られることをより確実なものにすることができます。

### 2.3.1. 脆弱性関連情報流通の基本方針

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)[10]の告示を踏まえて、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おり、脆弱性関連情報[11]の適切な流通に関する活動に取り組んでいます。

以下では、この情報セキュリティ早期警戒パートナーシップの基本方針について説明します。詳細については、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[12]を参照してください。




※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:独立行政法人 産業技術総合研究所

**図 2-7 情報セキュリティ早期警戒パートナーシップのしくみ**

---

9 ⇒ 本書用語集「不正アクセス」、「コンピュータウイルス」

10 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), 2004年7月, http://www.meti.go.jp/policy/netsecurity/downloadfiles/vulhandlingG.pdf

11 ⇒ 本書用語集「脆弱性関連情報」

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

### (1) 適用範囲

脆弱性が発見された場合に不特定多数の利用者が影響を受けるか否かという観点から、以下を適用範囲としています。

- 国内で利用されている汎用性を有するソフトウエア製品:
  市販のパッケージソフトウエアや共通に利用されるソフトウエア部品、組込みソフトウエアを搭載したアプライアンス型のハードウェアに脆弱性が発見された場合、不特定多数の利用者に影響が及びます。また、共通のモジュールや通信プロトコル、標準化されたフォーマット等の実装に脆弱性が発見された場合には、複数の製品が関わるため、影響範囲はさらに広がることになります。
- 国内においてアクセスされているウェブサイトのウェブアプリケーション[13]:
  ウェブアプリケーションは、インターネットを介して不特定多数の利用者が利用可能なサービスを提供しているため、脆弱性が内在した場合の社会的影響は大きなものとなります。

### (2) 取り扱う情報の種類と取扱い方針

脆弱性関連情報とその対策方法については異なる方針で取り扱います。

- 脆弱性関連情報[14]: 脆弱性、検証方法、攻撃方法などは流通範囲を限定して慎重に取り扱うべき情報として取り扱う。脆弱性については対策方法が公表されるまでは原則として公表しない。攻撃方法および検証方法については公表しない。
- 対策方法[15]: 脆弱性の修正方法や回避方法(修正するのではないが、被害を避けるための方法。ワークアラウンドとも呼ばれる)は広く周知すべき情報として取り扱う。いずれも公表後迅速に利用者に流通させることを意図している。

### (3) 脆弱性関連情報の届出を受け付ける機関 (受付機関)

脆弱性関連情報が放置されたり、不用意に暴露されたりすることを防ぐために、第三者機関が脆弱性関連情報の届出を受付け、発見者(または届出者)に代わって製品開発者やウェブサイト運営者への提供を行うこととしています。経済産業省告示により IPA が届出受付機関に指定されています。

受付機関は、発見者本人が望まない限り、発見者の氏名、連絡先等の情報を調整機関、製品開発者には提供せず、発見者の代理として機能します。これにより発見者が製品開発者に比べ不利な立場に置かれることを防いでいます。

---

13 ⇒ 本書用語集「ウェブアプリケーション」
14 ⇒ 本書用語集「脆弱性関連情報」
15 ⇒ 本書用語集「対策方法」

### (4) ソフトウエア製品の公表時期を調整する機関（調整機関）

ソフトウエア製品の脆弱性の場合、ひとつの脆弱性が複数の製品開発者の製品に影響する可能性があるため、脆弱性関連情報の提供を受けるべき製品開発者を特定し、各製品開発者の対策作成状況を把握して一斉に公表を行うタイミングを調整する機関が必要となります。経済産業省告示により JPCERT/CC が調整機関に指定されています。

一方、ウェブアプリケーションの脆弱性については、受付機関が受理した脆弱性関連情報を当該ウェブサイト運営者に直接通知する形で処理可能であるから、受付機関（IPA）が直接ウェブサイト運営者に通知することとなっています。

### (5) 対策方法や届出件数等の統計データを集積・公表する機能

システム構築支援事業者（SI 事業者）やインターネットアクセスプロバイダ、利用者等に脆弱性の対策方法を周知するために、対策方法を集積・公表し、現状の脆弱性対策に係る主要な情報を入手できる環境として「脆弱性対策情報ポータル JVN」[16]を提供しています。

また、脆弱性関連情報に関する実態を明らかにして、関係者が脆弱性のリスクを正しく評価できるよう促すために、IPA および JPCERT/CC では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関連情報の届出件数や処理状況等に関するデータの集計・公表を行っています [17]。

### (6) 脆弱性関連情報の公表に係るルール

情報セキュリティ早期警戒パートナーシップでは脆弱性関連情報の公表に関して次のようなルールを定めています。

- 発見者： 発見者には、対策方法が公表されるまでの間は、第三者に脆弱性関連情報を漏洩しないようにすることが望まれます。ただし、正当な理由により脆弱性関連情報を第三者に提供する場合は、事前に受付機関と相談してください。なお、発見者が論文発表等正当な理由で公表を望む場合でも、その対策方法の策定が未完了、または対策方法の普及が不十分な状況で、脆弱性の公表が即座に攻撃につながるといった段階では、公表をある程度留保するのが望ましいケースがあります。
- 製品開発者： 製品開発者は、脆弱性と対策方法について、調整機関と連絡し協議して定めた一定期間後に公表します。ただし、製品開発者の都合等により、相談の上で公表日時を変更することがあります。また、複数の製品開発者に関連する脆弱性の場合、原則として複数の当該製品開発者が同時に公表します。

[16] ⇒ 本書 7.4.2.の「脆弱性対策情報ポータル JVN (Japan Vulnerability Notes)」 を参照
[17] 脆弱性関連情報の届出状況, http://www.ipa.go.jp/security/vuln/report/press.html

## 2.3.2. 情報セキュリティ早期警戒パートナーシップに関する法的な論点

ここでは、情報セキュリティ早期警戒パートナーシップの活動に係るそれぞれが心得ておくべき法的な問題に関して、法律専門家が示した見解を説明します。

### (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

a) 関係する行為と法令の関係

① 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き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。

② 暗号化されている無線通信の復号

- 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(Wired Equivalent Privacy)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。

b) 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(HyperText Markup Language)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。)

c) 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。

a) 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

b) 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。

c) 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。

d) 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。

① 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。

② 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。

③ 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。

## (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。

① 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。
② 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。
③ 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、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。

## コラム： わが国における脆弱性情報の取扱いの枠組みが作られるまで

我が国では、発見された脆弱性に関する情報を、発見者、製品開発者等の関係者がどのように取り扱うべきなのかという指針やガイドラインが存在しておらず、脆弱性情報が暴露されたケースや、製品開発者が脆弱性情報に適切に対処しないケースが散見されました。また、必要な者が必要なタイミングで脆弱性関連情報を入手できる仕組みが未整備であったため、製品開発者の提供した対策方法がユーザに伝わらず、対策が間に合わないケースも生じていました。さらに、我が国では脆弱性への関心が乏しく、国産のソフトウエアに対する脆弱性検証が十分とはいえないという問題も指摘されていました。

そこで、2003 年 10 月に経済産業省が公表した「情報セキュリティ総合戦略」において、「脆弱性に対処するためのルールと体制の整備」が提言されました。これを受けて、IPA が同年 11 月に「情報システム等の脆弱性情報の取扱いに関する研究会」を設置、JPCERT/CC、独立行政法人産業技術総合研究所（AIST）、社団法人電子情報技術産業協会（JEITA）、社団法人情報サービス産業協会（JISA）、NPO 日本ネットワークセキュリティ協会（JNSA）、ハード/ソフトウエアメーカ、セキュリティベンダなど、30 機関が参加して、発見から公表までの脆弱性情報の取扱いのあり方について議論を重ね、2004 年 4 月にその検討結果を公表しました。この成果は、パブリックコメントを経て、平成 16 年経済産業省告示第 235 号「ソフトウエア等脆弱性関連情報取扱基準」（2004 年 7 月 7 日制定、翌 8 日施行）、IPA、JPCERT/CC、JEITA、JISA、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（JPSA）（当時）[18]、JNSA「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 日発表）として結実し、これらに基づく「情報セキュリティ早期警戒パートナーシップ」の運用が 2004 年 7 月 8 日から始まりました。

さらに、これらに連動する形で、ソフトウエア製品開発者向けの JEITA、JISA「製品開発ベンダーにおける脆弱性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」（2004 年 7 月 26 日概要版公表、同年 10 月 13 日本文公表）、ソフトウエア製品開発者の担当者向けの JPCERT/CC「脆弱性関連情報取扱いガイドライン」（2004 年 8 月 25 日公表）、パーソナルコンピュータ用ソフトウエア製品開発者向けの JPSA（当時）「製品開発ベンダーにおける脆弱性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」（2004 年 12 月 3 日公表）、システムインテグレータ向けの JISA、JEITA「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」（2005 年 8 月公表）等、関係者がそれぞれ必要な行動と体制を理解するためのガイドライン・ガイダンスが次々と公表され、運用のための環境が整備されました。

このように、情報セキュリティ早期警戒パートナーシップは、政府や IT 業界、セキュリティ機関等が我が国の情報セキュリティ確保のために協力する形で実現し、経済産業省告示に基づく官民連携の枠組みとして機能しているという点で、国際的にも例を見ない独自の制度といえます。

[18] 現 社団法人コンピュータソフトウェア協会 （CSAJ）

# 3. 情報システムにおける脆弱性対応

この章では、企業等の組織において用いられる情報システムのセキュリティ担当者を主な対象として、脆弱性について SI 事業者に委託する際に考慮すべき点などを含めた全般的な脆弱性対策を説明します。また、特に地方公共団体において情報システムのセキュリティ対策に携わる方を対象に脆弱性対応のポイントについて述べます。

## 3.1. 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。たとえば、ISO/IEC 27001[19] 附属書 A では、情報セキュリティ管理策を以下のように分類整理しています。

1. セキュリティ基本方針
2. 情報セキュリティのための組織
3. 資産の管理
4. 人的資源のセキュリティ
5. 物理的及び環境的セキュリティ
6. 通信及び運用管理
7. アクセス制御
8. 情報システムの取得, 開発及び保守
9. 情報セキュリティインシデントの管理
10. 事業継続管理
11. 順守

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。

## 3.2. セキュリティ担当者による脆弱性対応[20]

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。

セキュリティ担当者には、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

[19] ISO/IEC 27001 は情報セキュリティ・マネジメント・システム（ISMS：Information Security Management System）の国際規格。

[20] セキュリティ担当者のための脆弱性対応ガイド
http://www.ipa.go.jp/security/ciadr/guide4vuln.pdf

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。

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。

### 3.2.1. 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。ソフトウエ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エ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。

### 3.2.2. 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かったりすることもあります。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、既存のソフトウエ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[21]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[22]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。

詳しくは本書の「4.2. ウェブサイト運営者における脆弱性対応」「4.3. ウェブサイト構築事業者における脆弱性対応」を参照してください。

---

[21] IPA, “企業等における脆弱性対策に関する実態調査報告書”, 2011 年 2 月, http://www.ipa.go.jp/security/ciadr/vuln_report2010.pdf

[22] ⇒ 本書用語集「クロスサイト・スクリプティング」、「SQL インジェクション」

## ■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、2.2 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、既製のソフトウエ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。納入前にソフトウエアの構成やパッチ[23]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エ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。独自のソフトウエ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[24]によると、従業員のクライアント PC を導入する際に、ソフトウエ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[25]、USB 経由のコンピュータウイルス感染等）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。

---

[23] ⇒ 本書用語集「パッチ」

[24] IPA, “企業等における脆弱性対策に関する実態調査報告書”, 2011 年 2 月, http://www.ipa.go.jp/security/ciadr/vuln_report2010.pdf

[25] ⇒ 本書用語集「標的型攻撃」

また、OS、アプリケーション、プラグイン等のソフトウエ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。導入時にソフトウエ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エ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。

### 3.2.3. 運用段階における対策実施

ソフトウエ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。

#### ■組織の情報システムのソフトウエ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エア構成（ソフトウエアの種類、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。

ソフトウエ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エ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」[26]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エ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

[26] ⇒ 本書 7.4.2.「MyJVN バージョンチェッカ」

も選択肢のひとつです。

### ■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、製品開発者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、製品開発者がホームページ等に示す製品利用者向け情報、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エ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。ソフトウエ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」[27]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ウェブサイト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 [28]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エ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エア製品開発者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。

---

[27]⇒ 本書 7.4.2.「MyJVN 脆弱性対策情報収集ツール」

[28] IPA, “企業等における脆弱性対策に関する実態調査報告書”, 2011 年 2 月, http://www.ipa.go.jp/security/ciadr/vuln_report2010.pdf

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、内部にコンピュータ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。

### 3.2.4. 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、ソフトウエ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、コンピュータウイルスを撒き散らしている等）[29]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、個人情報の漏洩やウェブサイト利用者へのコンピュータ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）[30]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、コンピュータ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。

---

[29] ⇒ 本書用語集「不正アクセス」、「踏み台」、「フィッシング詐欺」、「コンピュータウイルス」

[30] ⇒ 本書用語集「WAF」

### 3.2.5. 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**

  ソフトウエ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**

  ソフトウエ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」[31]を参照してください。

[31] 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”, 2009 年 6 月, http://www.meti.go.jp/policy/netsecurity/secgov-documents.html#outsourcing-guidance

## 3.3. 地方公共団体における脆弱性対応

地方公共団体においてはウェブサイト等のインターネットにつながる住民向けサービスの基盤として情報システムは欠かすことができません。

しかし、それらのシステムの脆弱性対策を怠ると、地方公共団体や住民に様々な影響を及ぼす可能性があります。住民の財産を守り安全な IT サービスを提供するためには情報システムの脆弱性への対応が重要となります。

以下では特に地方公共団体における脆弱性対応のポイントについて述べます。

### 3.3.1. 幹部の方へ

情報システムは、「動いているから大丈夫」なように見えても、経年的に安全性が低下していきます。情報システムはいつまでも安全ではありません。安全性を維持するためには脆弱性の検査、脆弱性への対応が必要になります。脆弱性への対応を怠って問題が発生すると、住民からの信頼を失うリスクがあります。

脆弱性は突然見つかることがあり、突発的な対応が要求されます。脆弱性が見つかると情報システムを保有する各担当課、IT 担当課、委託業者に作業が発生します。予算や人的資源等の柔軟な組み換えが必要となることをご理解ください。

### 3.3.2. 情報システムを保有する各担当課の方へ（原課の方へ）

脆弱性対策を怠って保有する情報システムに問題が発生した際の責任は、各担当課が担うことになります。情報システムの安全性は時間が経つにつれて低下するので、脆弱性検査などの継続的な対策が必要です。また、脆弱性対策のためにシステムを停止することがありますが、住民向けサービスは、代替システムを用いてでも維持すべき場合があります。

委託業者との契約時の調整などで IT 担当課から協力を得ることができれば、脆弱性の対策に関して問題を避けることがより容易になります。

### 3.3.3. IT 担当課の方へ（情報政策課の方へ）

脆弱性対策は、開発・運用事業者に一任するだけで解決するものではありません。開発・運用における委託する事業者との間の曖昧な取り決めや不十分な合意形成がもとで問題が生じる場合もあります。契約時に合意に向けて調整すべき事項には次のことがあります。

- 開発の契約:
  - 開発時の段階で見つけた既知の重要な脆弱性の対策は契約に含める
  - 納入前のウェブサイトに対し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

- ソフトウエア製品の既知の重要な脆弱性に関する著しい認識不足、ウェブアプリケーションに必要な設定の漏れ、設定ミスなど開発事業者の責に期する場合は対策を無償とする

・ 保守・運用の契約

- 保守フェーズの新規脆弱性への対策は保守契約で対応する
- 当該情報システムに関する深刻な脆弱性の情報が公開されたら連絡してもらう
- 緊急事態の際に生じる調査費用・対策費用の負担については、契約段階で明確にしておく

必要に応じて庁内の調達ガイドラインを策定し、情報システムを保有する各担当課に提供しておくことが望まれます。

脆弱性対策を進める上で、IT 担当課の人事ローテーションは各地方公共団体の悩みとなっています。IT やシステムを理解できる人材の育成に時間がかかる、システムの管理レベルが属人化してしまう、委託業者に依存してしまうといった課題があります。

基準や手順をガイドラインにまとめるなどして、経験・知見を共有している地方公共団体では、人事ローテーションがあっても脆弱性対策はうまく機能しています。

また、脆弱性対策を円滑に実施するためには、情報システムを保有する各担当課と IT 担当課との間の連携・情報共有が重要となります。

### 3.3.4. 地方公共団体における脆弱性情報の取り扱いの難しさ

地方公共団体は、住民向けサービスのシステムについて未公表の脆弱性関連情報を得ると、以下の判断に悩まされます。

・ 情報の公開/非公開:

透明性を優先して脆弱性を修正する前にその情報を公表すれば広い影響が出る可能性があります。システムが攻撃され、住民の情報が流出するなどの被害が生じえますし、他の地方公共団体や民間企業等の類似システムが攻撃対象となる可能性もあります。

・ サービスの継続/停止:

住民向けサービスの継続は、地方公共団体の業務にとって非常に重要です。しかし脆弱性をシステムに抱えたまま住民にサービスを提供し続けて、その間にシステムが攻撃されれば、住民の情報等が流出する可能性もあります。

この問題点の取扱いについてどのような方針をとるべきか、事前に検討しておくことが望まれます。以下に実際にどのような判断が行われたか事例を紹介します。

取扱いの判断例:

- 攻撃を受けるリスクなど脆弱性の影響について、IPA、LASDEC[32]などから情報提供を受け、サービスの継続性を判断する。深刻な場合は、サービスを止めることも視野に入れる。
- 脆弱性情報は、情報公開条例の例外条項に該当すると判断し、対策が適用されるまでは非公開の扱いとする。

公表の例:

- 脆弱性のあるシステムは、可能であればサービスを停止することの告知を事前に行った上で停止し、改修する。その際、必要に応じて代替サイトを立ち上げサービスを継続する。

脆弱性情報の取り扱いに対する組織的な対応例:

- 運営するウェブサービスに脆弱性が発見された場合の対応手順を文書化して、組織内で共有する。
- 委託先との契約も、脆弱性対策を念頭に置いたものとする。

[32] 財団法人地方自治情報センター

# 4. ウェブサイトにおける脆弱性対応

この章では、ウェブサイト運営の意思決定者や組織において脆弱性の確認や修正作業を担当するウェブサイト技術者を対象に、ウェブサイトの脆弱性について運営者が問われる責任、求められている継続的な対策、脆弱性に関する通知を受けた場合の望ましい対応手順などを説明します。

また、情報サービス企業の技術者やウェブデザイナー、企業内でウェブサイトの構築・運用を担当する技術者を対象にして、システムの納入前や納入後に考慮すべきことをまとめて解説します。

## 4.1. ウェブサイトで起こるトラブルと脆弱性

誰もが容易にアクセスできるウェブサイトは、インターネットの利用拡大とともに爆発的な発展を遂げました。現在インターネット上には膨大な数のウェブサイトが稼動しており、その役割は情報発信や検索、コンテンツの投稿・共有、受発注や予約などに多様化・高度化しています。

企業が自社のホームページを開設することは当前のこととなり、顧客向けの広報活動はもちろん、商品の受発注や在庫管理、コンサルティングやサポート等の窓口など、ウェブサイトが企業のビジネスプロセスの一端を担っています。

インターネットには、世界に向けて情報を発信しサービスを提供できるメリットがあります。さらに、携帯電話や無線 LAN の進化により、今やユーザはどこにいても自由にウェブサイトを利用することができます。

その一方で、誰にでも利用できるように常に公開されているウェブサイトは、悪意を持った者からネットワーク越しに狙われるリスクを抱えています。

また、設定ミスなどの不備により、重要な情報がインターネット上に流出するリスクもあります。一度ネットワーク上に流出した情報をすべて回収することは不可能です。

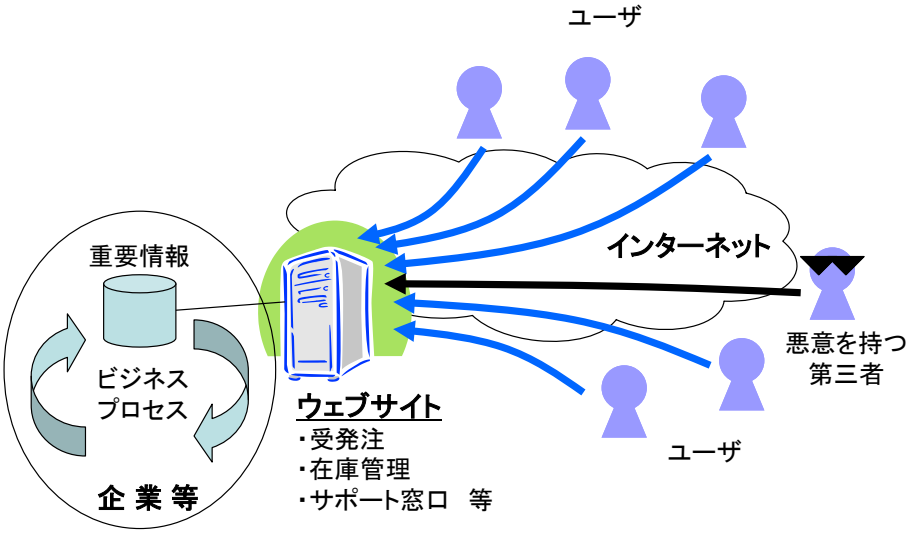



**図 4-1 ビジネスプロセスの一端を担うウェブサイトとリスク**

ウェブサイトで起こる情報セキュリティ上のトラブルの原因には、ソフトウェアの脆弱性もあります。ウェブサイトの脆弱性は、CGI[33](Common Gateway Interface)プログラムなどシステムの作り方や設定ミスに起因するものが多く見られます。さらに、OS 等の基盤ソフトウェア[34]やウェブサーバ等アプリケーションソフトの脆弱性などもトラブルの原因となります。

実際にウェブサイトで起きている情報セキュリティ上のトラブルについては本書 2 章に示した事例も参照してください。[35]

---

[33] ⇒ 本書用語集「CGI」
[34] ⇒ 本書用語集「基盤ソフトウェア」、「OS」
[35] ⇒ 本書 2.2.「脆弱性に起因するトラブルとその影響」

## 4.2. ウェブサイト運営者における脆弱性対応[36]

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、ウェブサイト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。

### 4.2.1. 運営者に問われる責任

ウェブサイトで情報セキュリティ上のトラブルが発生した場合、そのウェブサイトの運営者は、どのような立場に置かれるでしょうか。

まず、個人情報の流出が発生した場合には、ウェブサイトの運営者はその事実を所管省庁に報告するとともに、架空請求などの二次被害を防ぐ意味でも、流出した個人情報の本人にその旨を連絡する必要があります。

また、ウェブサイトの運営者は、ユーザに対してサイトのセキュリティを確保する責任を果たしていなかった点を問われて、訴訟の対象となる可能性があります。実際にはそのウェブサイトの運営を外部の事業者に委託していて、自身ではトラブルの発生に関与していなかったとしても、被害者から見た「責任者」は一義的にはそのサイトの運営者であり、訴訟の際に被告となることは免れません。

トラブルを起こしたウェブサイトを停止した結果、取引先の売上げに悪影響を及ぼす可能性があります。契約によっては、損害賠償を要求されることになります。

さらに、自らが被害者であるにもかかわらず、コンピュータウイルスを撒き散らす「加害者」となっていた場合、ネットワーク社会の一員である企業として社会的責任を果たしていないと非難されるでしょう。この場合、コンピュータウイルスの駆除だけでなく、その感染の原因を調べて問題を解決しない限り、再びサイトが感染し、同じトラブルを繰り返すことになりかねません。

### 4.2.2. ウェブサイトに脆弱性が見つかった場合には

#### (1) 脆弱性をどのように見つけるか

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、問題に気づくことは容易ではありません。

まず、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、自

[36] ウェブサイト運営者のための脆弱性対応ガイド
http://www.ipa.go.jp/security/ciadr/vuln_website_guide.pdf

ウェブサイトの最新の構成情報を確認しておくべきでしょう。

また、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[37]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[38]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べきです。

さらに、自社の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。そうしたユーザから問い合わせを受けた場合には、速やかに調査し、脆弱性の有無を確認すべきでしょう。

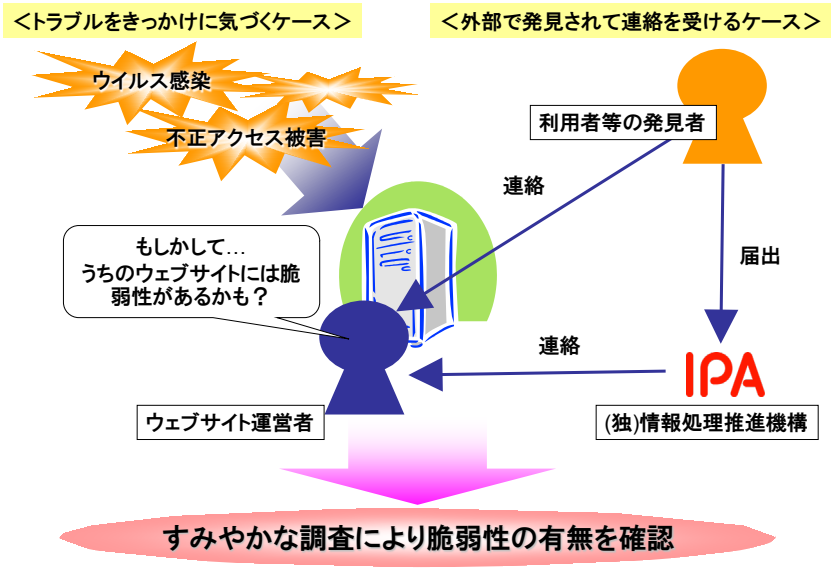



**図 4-2 脆弱性に気付いたら**

### (2) IPA から脆弱性に関する連絡を受けた場合

独立行政法人 情報処理推進機構（IPA）では、「ソフトウェ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 月からソフトウェ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 。

IPA では、ウェブサイトの脆弱性に関する届出を受け付けた場合、当該ウェブサイトの運営者にその旨を連絡し、脆弱性対策の実施を促します。

### (3) 対応は意思決定から始まる

ウェブサイトの脆弱性が発見されたり、悪意の第三者の攻撃やコンピュータウイルスの問題が発生した場合のトラブル対応は、扱いを誤るとブランドイメージの失墜や経営基盤を揺るがす損失につながりかねません。したがって、事務機器の故障のような日常的問題の延長として捉えるのではなく、事業継続管理や危機管理の観点で捉え、企業としての意思決定に基づく対処指針や姿勢を提示すべきです。

---

37 ⇒ 本書用語集「不正アクセス」、「コンピュータウイルス」
38 ⇒ 本書用語集「ウェブシステム」

また、外部の事業者に保守業務を委託している場合には、脆弱性対策についても契約に含め、緊急時にも円滑な対応が得られるよう、体制や費用等についてあらかじめ合意しておくことが望まれます。

### 4.2.3. 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が実際に脆弱性に関する通知を受けた際には、調査を行い、必要な対策を適切にとることが望まれます。以下では留意点と望ましい対応手順を示します。

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には、下図に示すように対処を進めることが望まれます。

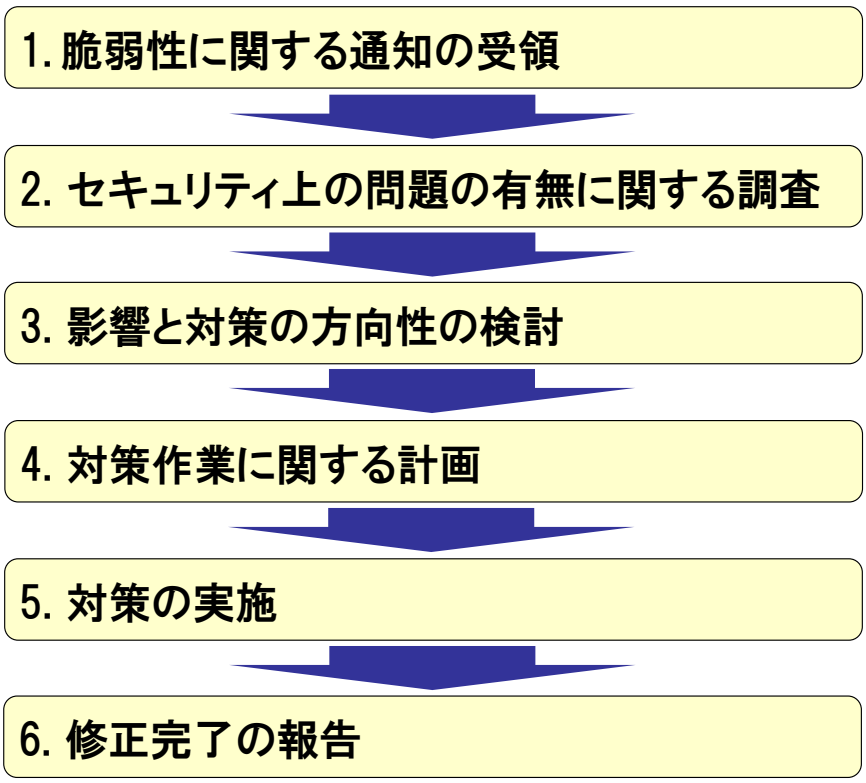



**図 4-3 脆弱性関連情報への対処の流れ**

対応の全体に係る留意点を以下に示します。

#### 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、コンピュータウイルスを撒き散らしている場合[39]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、個人情報の漏洩やウェブサイト利用者へのコンピュータ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、コンピュータ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、コンピュータ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。場合によってはウェブ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

ウェブ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」[40]も参考となります。

以下では各手順においてウェブサイト運営者が行う作業について説明します。

---

[39] ⇒ 本書用語集「不正アクセス」、「踏み台」、「フィッシング詐欺」、「コンピュータウイルス」

[40] 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, “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”, 2005 年 8 月
http://www.jisa.or.jp/report/2004/vulhandling_guide.pdf

## (1) 脆弱性に関する通知の受領

ウェブサイト運営者は、ウェブ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 つに大きく分けられます。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: ウェブサイト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＞

ウェブサイトの運用について 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. 当該ウェブ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

問題のあったウェブサイトに関して、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、同時にウェブ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ウェブサイト利用者へのアナウンス
2. ウェブサイト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. ウェブサイト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、ウェブサイト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ウェブサイト利用者への対応（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、対応の内容を含む報告）を IPA へお願いします。

<u>その他</u>

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、ウェブ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「消費者庁　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」[41]を参照してください）。

## 4.2.4. 脆弱性について通知を受けた場合の作業 チェックリスト

IPA／発見者より脆弱性に関する連絡を受けた際の対処について、全体の流れが分かるように、各段階の概要を簡潔に示し、各段階でウェブサイト運営者が取る行動を一覧形式で示します。

[41] 消費者庁　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://www.caa.go.jp/seikatsu/kojin/gaidorainkentou.html

## 脆弱性について通知を受けた場合の作業 チェックリスト

| チェック項目 | チェック | SI 事業者が協力可能な項目 |
|---|---|---|
| 脆弱性に関する通知の受領 | | |
| 脆弱性関連情報の適切な担当者への受け渡し | | |
| 通知を受領した旨の返信 | | |
| IPA／発見者との連絡手段の確立 | | |
| 組織内の対応体制の確認 | | |
| SI 事業者への作業依頼を行うかどうかの判断 | | |
| 発見者と直接情報交換を行うかについての判断 | | ○ |
| IPA／発見者への確認 | | ○ |
| セキュリティ上の問題の有無に関する調査 | | |
| 確認作業に必要なリソースの確保、関係者への協力要請 | | |
| 問題があるウェブシステムの特定 | | ○ |
| 指摘された脆弱性につながる現象の再現 | | ○ |
| 脆弱性の原因と発生条件の特定 | | ○ |
| IPA あるいは発見者への進捗連絡 | | |
| 影響と対策の方向性の検討 | | |
| 作業に必要なリソースの確保、関係者への協力要請 | | |
| 脆弱性の影響範囲の調査 | | ○ |
| 対策適用の影響度の調査 | | ○ |
| 修正方法の検討 | | ○ |
| スケジュールの見積もり | | ○ |
| 対応費用の見積り | | ○ |
| 検討報告および対応方針案のとりまとめ | | ○ |
| 対策作業に関する計画 | | |
| これまでに収集した情報の整理と共有 | | ○ |
| 当該サイトに関する契約の確認 | | |
| 対策基本姿勢・優先事項の明確化 | | ○ |
| 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 | | |
| 対策計画の確定 | | ○ |
| 作業時の連絡体制の確認 | | ○ |
| 作業実施に係る SI 事業者との調整 | | ○ |
| 対策の実施 | | |
| 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 | | |
| 利用者への作業実施期間中の代替手段の提供・案内 | | ○ |
| 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 | | ○ |
| 利用者からの問い合わせへの対応 | | |
| 進捗報告の作成 | | ○ |
| 修正完了の報告 | | |
| IPA あるいは発見者への修正完了報告 | | |

## 4.3. ウェブサイト構築事業者における脆弱性対応[42]

### 4.3.1. 構築事業者に期待される役割

ウェブサイト構築事業者は、顧客の求めるウェブシステムを構築する立場にあります。発注仕様に基づき、機能やデザインに配慮したシステムを開発・納入することが求められているのは当然ですが、「安全」を求められていることが大前提なのはいうまでもありません。

ウェブサイトは企業各社で独自に開発されるため、異なる企業のウェブサイトに類似の脆弱性があっても、横断的に対策を進めることができません。また、ユーザ企業は脆弱性の問題について必ずしも詳しいとは限りません。したがって、ウェブサイト構築事業者が脆弱性対策に配慮し、トラブルの発生を抑制することが望まれます。

しかし、残念ながら、顧客に納入したシステムやその中に組み込まれたソフトウエアが脆弱性を内包している可能性は否定できません。少なくとも、既に公表されている脆弱性について適切な対策を行わずにシステムを納入したり、ウェブサーバに設定漏れや設定ミス等があった結果、事件・事故が発生した場合、ウェブサイト構築事業者は自らの問題として真摯に対応することが求められます。

そのような事態を避けるために、ウェブサイト構築事業者はあらかじめセキュリティ上の品質についても担保し、対策しておく必要があります。特に、個人情報や営業秘密等、顧客にとって機微な情報を扱うシステムであれば、設計・開発の段階から適切に対処しておく必要があります。

### 4.3.2. 納入前に考慮すべきこと

#### (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には、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。

---

42 ウェブサイト構築事業者のための脆弱性対応ガイド
http://www.ipa.go.jp/security/ciadr/vuln_sier_guide.pdf

また、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、トラブル[43]が発生してウェブサイト利用者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、納入後に製品開発者や JVN[44]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[45]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

---

43 ⇒ 本書 2.2.「脆弱性に起因するトラブルとその影響」
44 ⇒ 本書 7.4.2.「脆弱性対策情報ポータル JVN (Japan Vulnerability Notes)」
45 ⇒ 本書用語集「セキュリティ検査」

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）[46]で構成されますが、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）[47]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。

## (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ウェブサイト利用者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[48]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[49]をどうするか

---

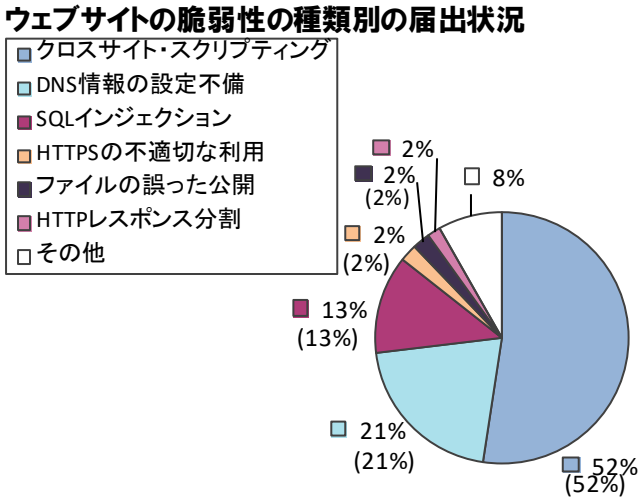
46 ⇒ 本書用語集「基盤ソフトウェア」、「OS」、「ミドルウェア」
47 ⇒ 本書用語集「パッチ」
48 ⇒ 本書用語集「セキュリティポリシー」
49 ⇒ 本書用語集「セッション管理」

・　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[50]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[51]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」[52]を参照してください。




（6,364件の内訳、グラフの括弧内は前四半期までの数字）

**脆弱性の種類別の届出件数の割合**

（出典：2012 年第 3 四半期資料別紙 1 より抜粋）

**図 4-4 ウェブサイトの脆弱性の種類別の届出状況**

### (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

[50] ⇒ 本書用語集「セキュリティ要件」
[51] ⇒ 本書用語集「クロスサイト・スクリプティング」、「SQL インジェクション」
[52] IPA. “安全なウェブサイトの作り方”, http://www.ipa.go.jp/security/vuln/websecurity.html

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[53]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[54]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[55]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）[56]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[57]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[58]や Struts[59]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

---

53 ⇒ 本書用語集「セッション管理」
54 ⇒ 本書用語集「開発フレームワーク」
55 ⇒ 本書用語集「コードレビュー」
56 ⇒ 本書用語集「ブラックボックステスト」、「ペネトレーションテスト」
57 ⇒ 本書用語集「コード検査」
58 Struts は Java 言語を用いたウェブアプリケーション開発の際に必要な基盤となるオープンソースのソフトウェア。
59 Struts は Java プラットフォーム向けのオープンソースのアプリケーションフレームワーク。

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。

### 4.3.3. 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。

#### (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者や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、ウェブサイト利用者が、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、外部からの脆弱性への攻撃の可能性を検討するよう助言すべきです。

### (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、海外にウェブサイトを設置し、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。

#### ■配布するソフトウェアの版管理

必ずしもウェブサイト構築事業者の担当範囲とは限りませんが、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。

### (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)[60]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、ウェブサイト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」[61]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。

---

60 ⇒ 本書用語集「パッチ」

61 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, “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”, 2005 年 8 月
http://www.jisa.or.jp/report/2004/vulhandling_guide.pdf

### ・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 との連絡窓口（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、コンピュータウイルスを撒き散らしている場合 [62]には、まずウェブサイトを停止して被害の拡大を防ぎます。加えて、個人情報の漏洩やウェブサイト利用者へのコンピュータ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、コンピュータ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、コンピュータ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。

---

62 ⇒ 本書用語集「不正アクセス」、「踏み台」、「フィッシング詐欺」、「コンピュータウイルス」

# 5. ソフトウエア製品と脆弱性対応

この章では、ソフトウエア製品開発者における脆弱性対策の推進に関して、脆弱性情報の取扱いに関する連絡体制の整備、実際に連絡が来たときの対応方法について述べ、ソフトウエア製品開発者による脆弱性対策情報の公表の参考として、望ましい公表手順について示します。また、特に組込みソフトウエアの開発における脆弱性対策を推進する方策について解説します。

## 5.1. ソフトウエア製品開発者における脆弱性関連情報の取扱い [63]

脆弱性情報ハンドリング [64]とは、脆弱性関連情報を必要に応じて適切に開示することで、脆弱性情報の悪用、または障害を引き起こす危険性を最小限に食い止めるためのプロセスです。

このプロセスの調整役(コーディネーター)として、影響のある製品を持つ製品開発者に脆弱性情報の連絡、対応を依頼する役割は一般社団法人 JPCERT/CC が担っています [65]。

### 5.1.1. 組織内体制の構築と窓口の登録

#### (1) 組織内体制の構築

製品開発者は脆弱性関連情報の取扱いを行うため組織内体制を整備してください。体制構築については社団法人電子情報技術産業協会(JEITA)、社団法人情報サービス産業協会(JISA)が公開するガイドライン [66]が参考になります。

体制構築に関しては以下の項目が挙げられます:

a) 脆弱性ハンドリングに関する文書を確認する:

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」[67]

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 [68]

b) 担当者やルールを定める

担当者(製品脆弱性対策管理者)の決定、情報取扱いルールの作成 等

c) 連絡窓口を設置する

製品脆弱性対策管理者が JPCERT/CC や外部からの連絡を受け付けるためのもの

専用のメールアドレス、電話番号等

連絡窓口は JPCERT/CC に登録してください

d) 暗号化通信の準備(PGP 等でのやりとりの準備)

#### (2) 規約への合意と規約の遵守

脆弱性情報ハンドリングの枠組みにご協力いただける場合、JPCERT/CC が用意する「JPCERT コーディネーションセンター製品開発者リスト登録規約」に合意していただく必要があ

---

63 JPCERT/CC 脆弱性関連情報取扱いガイドライン
http://www.jpcert.or.jp/vh/vul-guideline2010.pdf

64 ⇒ 本書用語集「脆弱性情報ハンドリング」

65 JPCERT/CC, “脆弱性情報ハンドリングとは？” http://www.jpcert.or.jp/vh/index.html

66 社団法人電子情報技術産業協会(JEITA)、社団法人情報サービス産業協会(JISA), “製品開発ベンダーにおける脆弱性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”, 2004 年 10 月
http://it.jeita.or.jp/infosys/info/0407JEITA-guideline/index.html

67 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)
http://www.meti.go.jp/policy/netsecurity/downloadfiles/vulhandlingG.pdf

68 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
http://www.ipa.go.jp/security/ciadr/partnership_guide.html

ります。製品開発者の皆様には、本枠組みへのご参加と共に、上記規約を遵守していただきますようお願いします。

### (3) 日常の対応

製品毎のソフトウエア構成を常日頃から管理しておくことをお奨めします。脆弱性関連情報を受け取った際には、その脆弱性に該当する製品を特定する必要が生じますが、製品のソフトウエア構成が事前に分かっていないと特定作業が困難となる場合があります。

## 5.1.2. 受け取った脆弱性情報の取扱い

新たに発生した脆弱性関連情報については、JPCERT/CC から製品開発者の窓口(製品脆弱性対策管理者)に連絡が行われます。JPCERT/CC からは二段階に分けて情報が送られます。

### (1) 脆弱性概要情報の取扱い

JPCERT/CC からは「脆弱性概要情報」が送られてきます。製品開発者はその内容をもとにして、自組織の開発製品のなかに脆弱性に該当する可能性のある製品があるかどうかを判断し、必要であれば「脆弱性詳細情報」を送るように JPCERT/CC に請求してください。また、該当する製品がないと判断した場合は JPCERT/CC にその旨を連絡してください。

### (2) 脆弱性詳細情報の取扱い

脆弱性詳細情報を請求した製品開発者は、詳細情報を JPCERT/CC から受け取ります。製品開発者は受け取った脆弱性詳細情報をもとに脆弱性に該当する可能性があると判断した製品について調査・検証を進めてください。脆弱性に該当する製品があった場合、その製品に関して対策方法等を策定するかどうかについて検討してください。脆弱性詳細情報は機密情報として慎重な取扱いをお願いします。

また、脆弱性詳細情報を受け取った場合には、脆弱性情報の公表時に製品開発者名と共にその対応状況が公表される場合があります。

## 5.1.3. 調整

脆弱性情報の公表に向けては関係する製品開発者とJPCERT/CCとで調整がはかられます。

### (1) JPCERT/CC における公表日時の決定

脆弱性情報の公表に際しては一般公表日が設定されます。製品開発者は、対策情報なども含む脆弱性関連情報の公表に関して、一般公表日を遵守してください。

脆弱性情報の一般公表日は、製品開発者と JPCERT/CC で協議した上で決定します。特に、複数の製品開発者が関係する脆弱性情報の場合には、JPCERT/CC が製品開発者間のスケジ

ュール調整を主導的に行います。また、決定した一般公表日は JPCERT/CC より各製品開発者と関係機関に連絡します。

一般公表日を決めるにあたっては、JPCERT/CC が脆弱性関連情報の取扱いを開始した日時から起算して 45 日以内を目安としています。ただし公表日時は以下の点も考慮して検討し、場合により 45 日を超えることもあります。

- 製品開発者が対策方法の作成に要する期間
- 海外の調整機関との調整に要する期間
- 脆弱性情報の流出に係わるリスク

なお、製品開発者から脆弱性調査・検証結果等についての報告がなく、JPCERT/CC からの問合せへの応答もない場合、過去の類似事例や影響範囲等を考慮したうえで、JPCERT/CC が公表日を決定することがあります。また、製品開発者と連絡が取れない場合、製品利用者が受ける脅威の軽減を目的とした情報公開を行うため、JPCERT/CC が公表日を決定することがあります。

決定された一般公表日に関して、作業進捗等の理由で見直しが必要となった場合には、すみやかに JPCERT/CC に連絡してください。JPCERT/CC では他の製品開発者との調整の上、公表日の変更を検討します。

#### (2) 公表日一致の原則

一般公表前の脆弱性関連情報をハンドリングする場合、脆弱性への対策方法が整わない時点で、脆弱性関連情報が一般に公開または悪意のある第三者に漏洩すると、悪意のあるコード(攻撃コード)が開発され、流通し、システムの脆弱性への攻撃が始まる可能性があります。結果としてシステムに危険が及ぶ事態を招く可能性があります。

また、特に複数の製品が影響を受ける脆弱性の場合には、関係者間で一定の足並みをそろえることが重要です。関係者間で調整した一般公表日を待たずに、単独で情報を公表することは、他の製品の利用者を危険にさらす可能性があります。

情報開示の時期を誤った場合(一般公表日前に単独での情報公開を行った場合)、当該開発者が今後の脆弱性関連情報のハンドリングから外されるだけでなく、最悪のケースでは、脆弱性情報ハンドリングの国際的な枠組みから日本の製品開発者や関連機関が外され、日本全体として公表前の脆弱性関連情報のコーディネーションに支障が生じることも考えられます。

### 5.1.4. 対策情報の作成と状況連絡

脆弱性調査・検証の結果、脆弱性に該当する製品が見つかった場合は、一般公表日までに対策方法の作成や、公表する情報の作成などの対応をお願いします。

### (1) 対策方法の作成

脆弱性に該当する製品について、回避方法(ワークアラウンド)や修正方法(パッチ等)[69]の作成をお願いします。併せて、脆弱性公表の際に一般への公表が可能な情報があれば、公表する情報の準備もお願いします。さらに、脆弱性情報の公表後も引き続き、対策方法の作成と公表、情報の周知をお願いします。

### (2) 対策情報の作成における注意点

脆弱性情報の一般公表の際に対策方法が存在しない場合、製品の利用者等に危険が及ぶ可能性が考えられます。修正方法(パッチ等)の作成が困難な場合には、回避方法(ワークアラウンド)のみでも作成してください。この場合修正方法(パッチ等)の作成に関しては製品開発者の判断に委ねられますが、可能な限り作成をお願いします。

### (3) 対応状況の連絡

脆弱性情報の一般公表日まで、脆弱性関連情報に係わる対応状況をJPCERT/CC に連絡するよう努めてください。

JPCERT/CC と製品開発者との間のコミュニケーションは、原則として全て製品脆弱性対策管理者を通して行います。製品脆弱性対策管理者には組織内の関係部署との調整をお願いします。

## 5.1.5. 対策情報の連絡と公表

脆弱性情報は製品開発者とJVN(Japan Vulnerability Notes)の両方で公表することとなります[70]。

### (1) JVN における公表

脆弱性情報の一般への公表は、全世界で関係する組織が同時に行う場合があります。IPA およびJPCERT/CC が脆弱性情報を公表する場合にはJVN ウェブサイトを通じて情報を公表します。

### (2) 製品開発者における公表情報の作成

製品開発者は、脆弱性情報に関して公表可能な情報がある場合には、一般公表日までに公表情報の作成をお願いします。公表する内容については適切な方法で製品利用者に伝えることが望まれます。本書の次章に示した脆弱性情報の公表の方法を参考にしてください。

---

[69] ⇒ 本書用語集「ワークアラウンド」、「パッチ」

[70] 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、決定された一般公表日より前に、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。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。

## 5.2. ソフトウエア製品開発者における脆弱性情報の公表[71]

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「製品利用者」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、被害が生じ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、製品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。製品開発者には可及的速やかに自主的に脆弱性対策を施し、製品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、製品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、必要としている製品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。

### 5.2.1. 脆弱性対策について利用者が必要としている情報

脆弱性対策情報を製品利用者に提供するにあたり、製品開発者は、どのような情報が製品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、製品利用者に不利益が生じることがあります。以下に、修正プログラムの適用方法の情報のほかに、一般的に製品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

製品利用者は、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。

---

71 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
http://www.ipa.go.jp/security/ciadr/vuln_announce_manual.pdf

### (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製品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。製品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製品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製品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、製品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。

## 5.2.2. 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。

求められる情報は、製品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。

### (1) タイトル

製品の名称で検索して情報に辿り着く製品利用者のために、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じ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。

### (2) 概要

製品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) 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、製品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。

### (4) 脆弱性の説明

製品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。

### (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。

### (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。

### (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。

### (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、製品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。

### (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。

### (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。

### (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。

## 5.2.3. 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、製品利用者等の情報提供の対象者を特定できない場合に、製品開発者が製品利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」[72]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

[72] 製品安全研究会,“消費者生活製品のリコールハンドブック”, 2002 年 5 月 (P.47 参考 2 社告の例 望ましい社告の例が参考になります)
http://www.meti.go.jp/policy/consumer/seian/contents/recall/handbook.pdf

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ェ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**

　○○○○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。○○○○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　○○○○
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）**

> ○○○○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○○○○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○○○○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
>
> ○○○○1.5.5 (Windows 版)　　○○○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、製品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、製品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、製品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じる不具合を修正
>
> ・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、製品利用者には容易に判別できません。

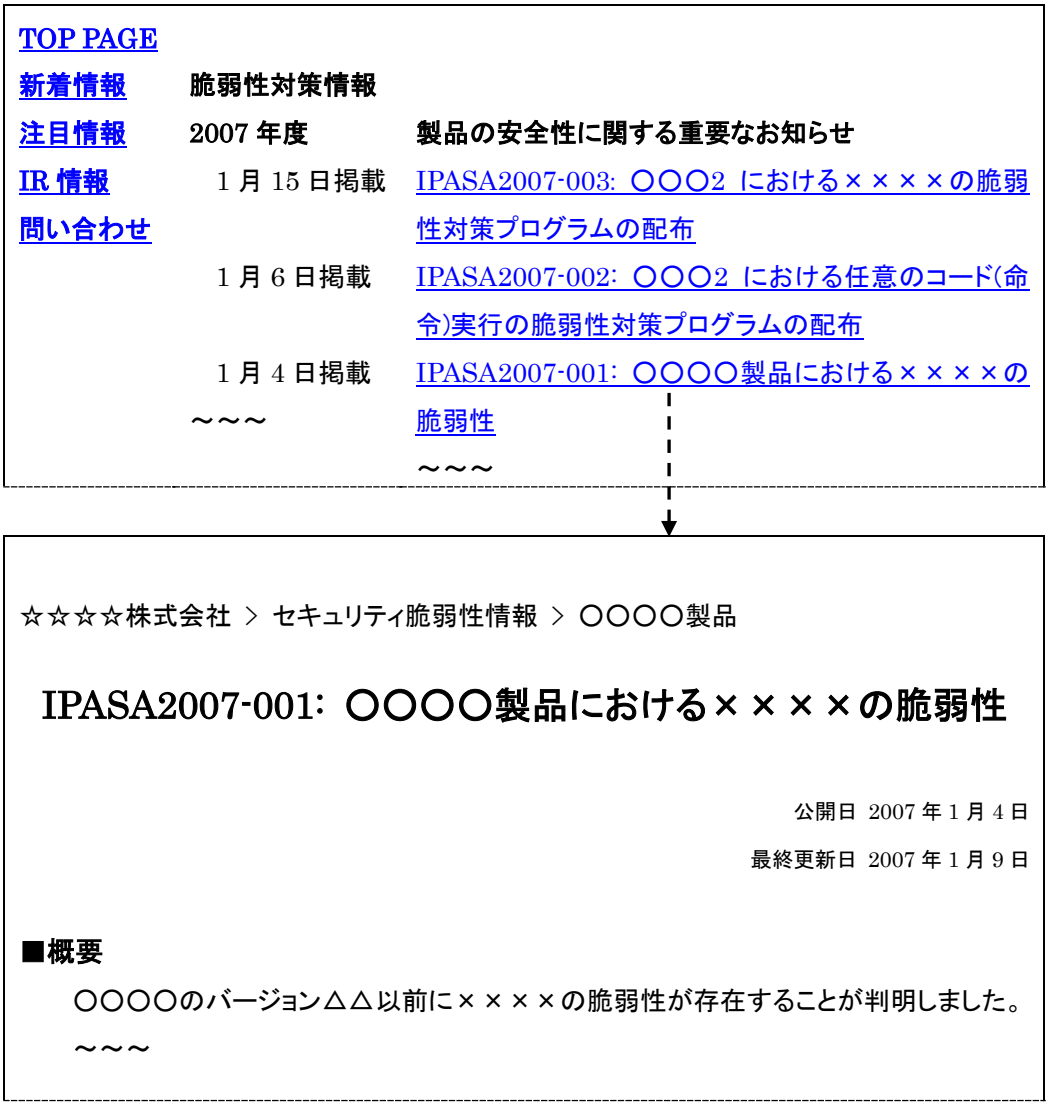
### 5.2.4. 脆弱性対策情報への誘導方法

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製品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すると、製品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、本書の 5.2.2.(10)に示したよう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製品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製品利用者には分かりません。

## 5.3. 組込みソフトウェアを用いた機器の脆弱性対策 [73]

インターネットは、私たちのビジネスモデルやライフスタイルを大きく変えました。さらにネットワークは、コンピュータ間の接続から多様な機器間接続へと発展しつつあります。今や家電機器や携帯電話、自動車、工場の FA(Factory Automation)システムまで、あらゆるものがネットワークにつながる時代を迎えていると言っても過言ではありません。

しかし、多様化・複雑化したネットワーク環境は、新たなトラブルをもたらしました。コンピュータの世界では、ネットワークを介した攻撃により、サービスの停止やファイルの損壊、情報流出等の被害が生じています。

今後は、組込みソフトウェアを用いた機器(以下、「組込み機器」という)もネットワーク化が進み、同様のトラブルに巻き込まれるかもしれません。その場合、コンピュータソフトウェアのメーカと同様に、組込み機器メーカにも何らかの対処が求められると考えられます。さらに、組込み機器メーカはそうした被害について、製造物責任法(PL 法)の観点から損害賠償責任を問われる可能性を考慮すれば、より難しい立場にあると理解すべきでしょう。

近い将来、組込み機器においてもセキュリティが問題化すると予想されます。組込み機器の分野において、実際に発生したトラブルの事例はまだ少ないですが、今後頻発する可能性は否定できません。では、どうしたらよいのでしょうか。

セキュリティ対策は品質向上の一部として適用していくことも可能です。ただし、従来の品質向上の枠組みにおいては十分にカバーされていなかった領域であり、今後はさらに強化していく必要があります。

この節の狙いは、組込み機器を提供している企業が、安全なネットワーク社会の実現と製品の欠陥による事業リスクを回避するためになすべき取組みを理解していただくことにあります。

### 5.3.1. 組込み機器と脆弱性

#### (1) 組込み機器が抱えるリスク

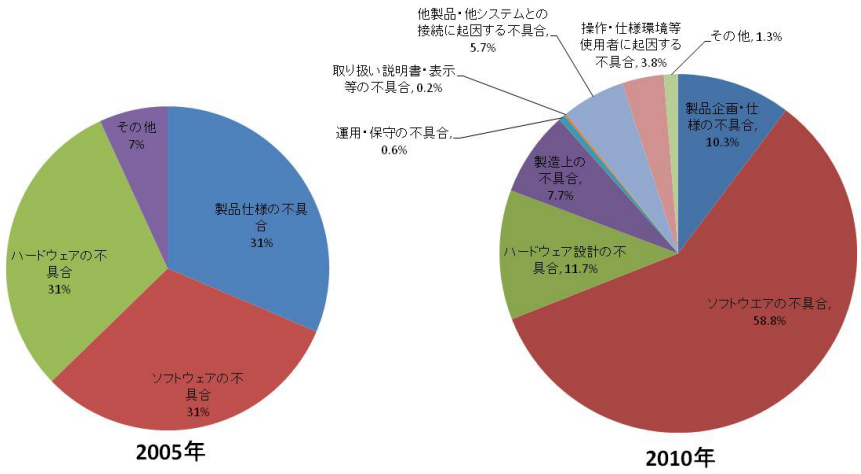
組込み機器の不具合

経済産業省「2010 年版組込みソフトウェア産業実態調査報告書」によると、組込み機器の出荷後に生じた不具合の主な原因として、ソフトウェアの問題が 58.8%を占めており、組込みソフトウェアの品質が経営基盤を揺るがしかねない状況がうかがえます。

また、ソフトウェアの不具合は 2005 年度の同報告書では 32%と報告されていたことと比較して大幅に増加しています。近年ソフトウェアが複雑化してきたことから不具合原因に占めるソフトウェアの割合が増加しています。今後もソフトウェアに起因する不具合は様々な製品に拡大してくものと思われます。

---

73 組込みソフトウェアを用いた機器におけるセキュリティ(改訂版)
http://www.ipa.go.jp/security/ciadr/kiki2.pdf




（出所：（左図）IPA「2005 年版組込みソフトウェア産業実態調査報告書」[74]、（右図）経済産業省「2010 年版組込みソフトウェア産業実態調査報告書」[75]）

**図 5-1 組込み機器の出荷後に生じた設計品質問題の主な原因の割合**

製品回収が必要になるケースも

それでは、市場に供給している組込み機器に脆弱性が発見された場合はどうなるでしょうか。コンピュータソフトウェアの場合、ソフトウェア製品のメーカ、販売会社（ベンダ）は脆弱性の存在を把握すると、それを修正するプログラム（パッチ）[76]を開発し、インターネット経由でユーザに配布するという対応が一般化しています。また、近年ではその他に放送用電波を用いたソフトウェアの改修を行ない、テレビのソフトウェアを更新するというといった方法も採られています。

しかし、組込みソフトウェアの場合、コンピュータのソフトウェアのようにパッチをインターネット経由で配布する方法が適用できないケースもあります。そうした場合、製品を回収し、メモリや基板などのハードウェアを交換するなど、その対応に巨額のコストを必要とする可能性があります。具体的には機器回収にかかる費用は製造者だけでなく、販売店の費用も含まれることから組込みソフトウェアの改修は経営者にとって留意する必要があります。

さらに、脆弱性を悪用した攻撃の影響が制御系にまで波及し、物理的事故を引き起こす危険性もゼロとは言い切れません。そうした事故が発生した場合、組込み機器メーカの損害賠償責任を問われることは必至です。

したがって、脆弱性対策は単なるセキュリティ対策の一つというより、組込み機器メーカの経営を揺るがしかねない経営リスクの一つとして捉えるべきでしょう。

---

74 IPA, “2005 年版組込みソフトウェア産業実態調査 報告書”, 2005 年 6 月
http://sec.ipa.go.jp/download/200506es.php

75 経済産業省, “2010 年版組込みソフトウェア産業実態調査報告書”, 2010 年 7 月
http://www.meti.go.jp/policy/mono_info_service/joho/downloadfiles/2010software_research/index.htm

76 ⇒ 本書用語集「パッチ」

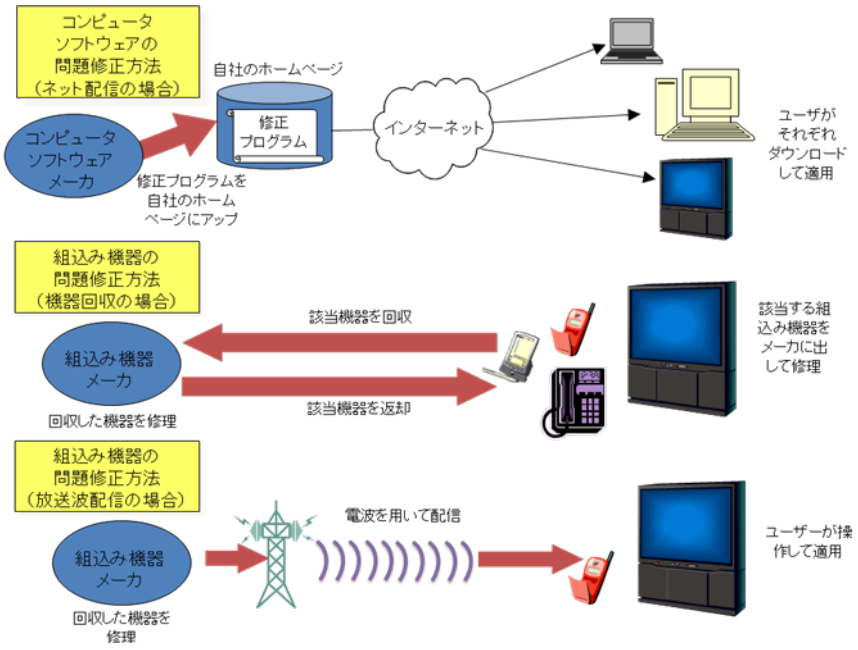



**図 5-2 コンピュータソフトウェアと組込み機器の問題修正方法**

技術の進展に伴う危険性に対応した改修の必要性

技術は日進月歩で進展しています。過去に販売された組込み製品のソフトウェアは、技術の進歩に対応すべく改修（バージョンアップ）を行う必要も出てきていることから新製品だけでなく過去に販売された製品に関しても注意を払う必要があります。

例えば暗号技術の進展は安全・安心な機器の利用に多大な恩恵をもたらしました。現在では PC やサーバだけでなく携帯電話、ゲーム機、情報家電といったネットワークに接続する機器に暗号技術を駆使したソフトウェアが組込みまれ安全・安心な暮らしを支えています。

一方で計算機能力が向上することで当初安全と思われていた暗号のアルゴリズムが必ずしも安全とは言い切れない状況となりました。このような状況に対して米国標準技術研究所（NIST）はより安全な暗号への移行を促しており、過去に使用されていた暗号方式ハッシュ関数 SHA-1 及び RSA 1024 について暗号の利用を中止する方針を打ち出しています。

このように技術の進展によるソフトウェアの改修の必要性が高まっていますが、過去に販売された製品の改修に必要なコストの問題等、技術の進展によるソフトウェア改修は経営者にとっても重要な課題です。

### (2) 組込み機器におけるトラブル事例

組込み機器の分野でも脆弱性に起因するトラブルは、絵空事ではなく実際に発生しています。

トラブル事例 1:家庭用ルータがボットウイルスに感染する

インターネットに接続するための機器の一つであるルータの脆弱性を利用して、ボットウイルスというコンピュータウイルスの一種に感染してしまう事例が報告されています。ボットウイルスはコンピュータに感染し、外部からネットワークを通じて操ることを目的としたプログラムです。このボットウイルスは、指令サーバからの攻撃命令によって感染したルータ等を踏み台[77]とした DDoS 攻撃を可能としてしまい、感染ルータが加害者になるなどの脅威があります。

このような事例は 2009 年 3 月に組込み機器に感染するボット Psyb0t がウェブサイト「DroneBL」に DDoS 攻撃をしたとして報告されており、組込み機器であっても、PC と変わらず、適切な ID/パスワード管理、脆弱性対策をする必要が有ります。

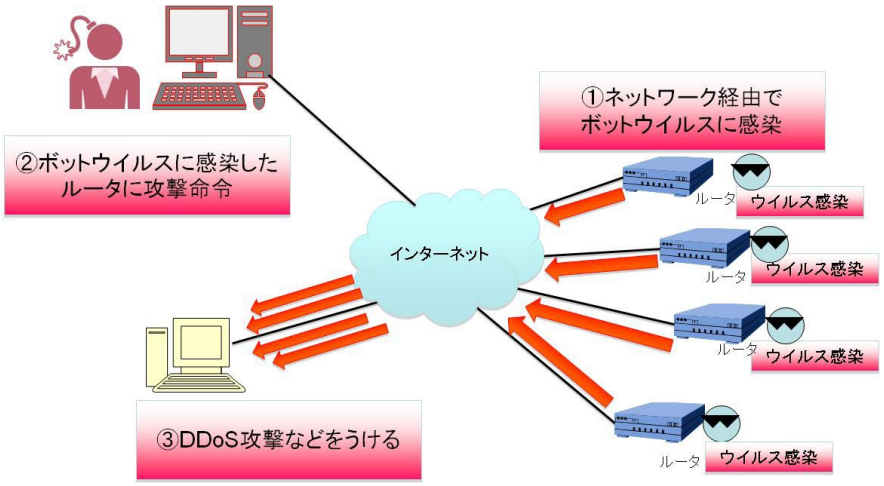



**図 5-3 ボットウイルスに感染したときの攻撃**

トラブル事例 2:スマートフォンの普及により、脆弱性対策の重要性が一段と高まる

インターネットに接続し様々なソフトウェアをインストールし利用出来るスマートフォンが登場し普及しています.利用者がインストールしたソフトウェアと組込まれていたソフトウェアの両方の脆弱性が報告されています。

2010 年 8 月にスマートフォンの脆弱性を悪用した攻撃の可能性についての情報が公開されました。2010 年 8 月時点でこの脆弱性を利用したコンピュータウイルス等はありませんでしたが、普及するスマートフォンに対する脆弱性対策の重要性は高まっています。これまでスマートフォンや携帯電話にはウイルス対策ソフトをインストールするといった習慣が無かったことから、脆弱性を利用したウイルスが出現した場合、被害範囲が大きくなる可能性があります。

スマートフォンに関するコンピュータウイルスに関する報告はゲームに見せかけて利用者の位置情報を第三者に送信するといったものが報告されています。

また、スマートフォンで利用するソフトウェアの開発が利用者によっても行われるといった利用環境の変化も起こっています。これにより脆弱性を抱えるソフトウェアが利用者から配信される可

[77] ⇒ 本書用語集「踏み台」

能性もあり、そういった場合の対処方法等も検討課題の一つでしょう。

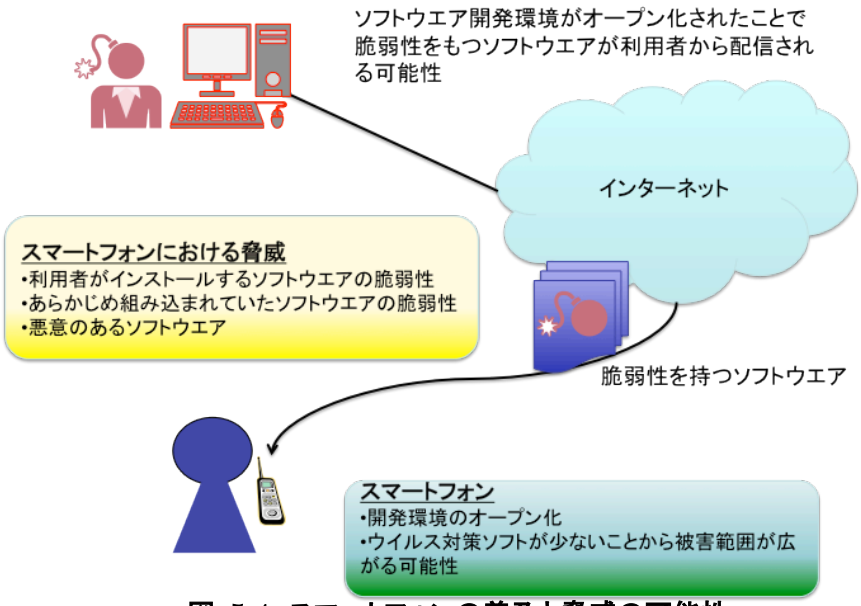



**図 5-4 スマートフォンの普及と脅威の可能性**

トラブル事例 3:組込み機器の管理用ウェブ画面における脆弱性

近年ネットワーク接続機能を利用する家電製品が増加しています。これらの家電製品にはネットワークを介してウェブ画面からサービスを利用する製品や、設定変更を行う機能を有している製品があります。これらのウェブ画面がもつ脆弱性を利用することで悪意のある者が機器の設定変更が可能になるなど、組込み機器の機能が多様化する一方で脆弱性とその脅威の種類も多様化しています。

2009 年 2 月にはウェブブラウザを利用した映像モニタリング用カメラにおいて、組込まれていたウェブサーバにアクセスすると利用者側のコンピュータにおいて任意の命令が実行される可能性のある脆弱性が判明し、製品開発者は対策プログラムを作成し配付しました。

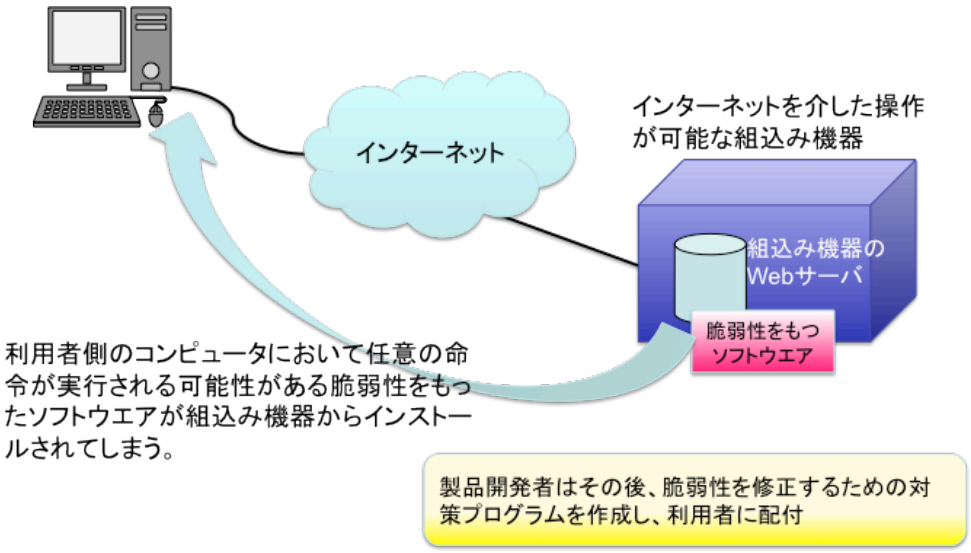



**図 5-5 組込み機器からインストールしたソフトウェアの脆弱性**

## 5.3.2. 組込み機器における情報セキュリティ対策のあり方

### (1) 対策に取り組む姿勢

組込み機器のセキュリティ対策を考えるべき時期

現在、PC に何のセキュリティ対策やパッチの適用も施さずにインターネットに接続すると、わずか数十秒でコンピュータウイルスに感染すると言われています。そうした状況において、組込み機器を無防備にインターネットに接続することは危険と考えるべきでしょう。
組込み機器のネットワーク接続の流れが本格化しつつある今、組込み機器のセキュリティ対策に取り組むべき時期に来ているのではないでしょうか。

対策についての基本的な考え方

組込み機器の脆弱性の問題は、事後対応に要する莫大なコストを考えれば、潜在する問題点をいかに前工程でつぶすか、企画段階からの対応が重要になります。こうした方向からの安全性の追求は、製品・サービスの全工程において、品質向上の一環として取り組むことが可能です。ただし、これまでの品質向上で扱ってきた領域とは異なる専門性が要求される点に配慮する必要があります。

また、開発時のセキュリティ対策の障害となるのはリソース(人、資産)の問題です。より手間をかけて安全に開発することが商品の価値・価格に必ずしも直接反映できないわけですが、それでも、自社の社会的責任に鑑み、相応の対策を行えるよう、トップの判断として必要なリソースを確保すべきでしょう。

さらに、組込み機器の脆弱性が出荷後に発覚した場合には、顧客や消費者が被害に遭わないようにできる限りの努力をすること、また、万が一、事件・事故が発生してもそれが深刻な事態に陥ることのないよう適切な対応をとることは、メーカとしての責務と言えるでしょう。そのため出荷時に個人情報を消去するための機能に関するセキュリティ検証を行うことで、利用が終了した後に入力された個人情報が機器に残ってしまうことを未然に防いでいる事例もあります。

### (2) 組込み機器におけるセキュリティ対策の取組み

セキュリティ確保のための体制

体制については、いくつかの考え方があります。例えば、脆弱性対策を含む製品セキュリティの推進を図る専任チームを設置する方向、事業部間を横断的につなぐ委員会を組織し情報共有と共通認識・合意を形成する方向、既存の組織(例:品質向上)の新たな使命として付与する方向などが考えられます。いずれにせよ、全社的なセキュリティ管理部門や品質管理部門との整合・連携は必要になります。特に、既存の品質保証体制と、セキュリティ固有の技術問題に関する比較的新しい知見をうまく組み合わせることが重要です。近年ではセキュリティ検証をシステムテストの最終段階で行う部門、部署を設置するといった取り組みも行われています。

メーカ A 社では、全社横断的な情報セキュリティの統轄部署を社長直下に設置し、「社内の情

報セキュリティ」、「個人情報・営業秘密情報の保護、「製品セキュリティ」の3つのカテゴリに係る全社的な推進を使命として位置づけました。脆弱性は「製品セキュリティ」の範疇であり、社内分社や子会社を含む全社的な委員会で推進しています。また、脆弱性情報等の情報展開については、委員会の下の技術部会で実施しています。さらに、脆弱性も含む技術的な指針、対策などの検討、出荷前のテストなどは、本社研究開発（R&D）の中のグループで担当しています。

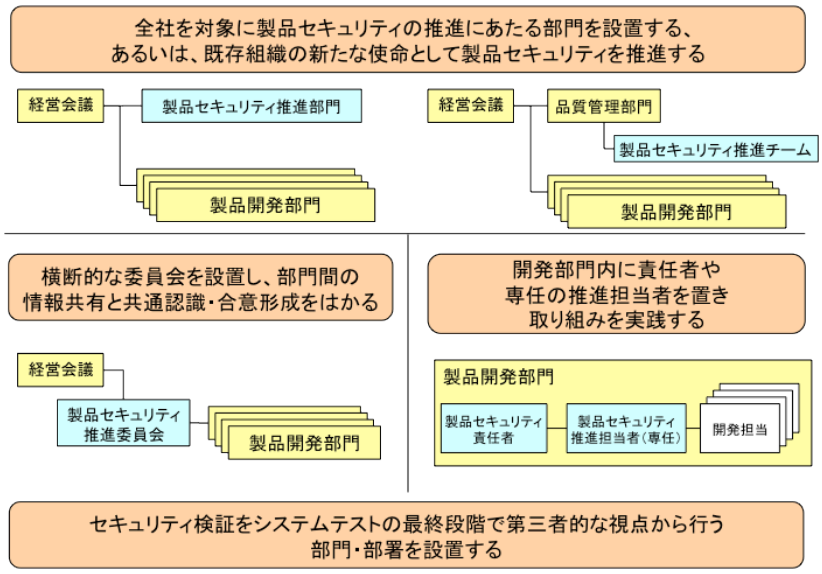



**図 5-6 セキュリティ確保のための体制の例**

セキュリティに関する教育・ルール

開発スタッフは、内包された脆弱性を排除するとともに、そうした取組みが必要な理由を正しく認識することが期待されます。そのためには、セキュリティ確保のためのチェックリストや「べからず集」のような指針・ガイドラインを開発プロセスに応じた形で整備するとともに、その教育を徹底する必要があります。

また、組込み機器の開発は多くの場合、プロジェクト単位で稼動しており、プロジェクトが終わってチームが解散すると、情報が散逸することがあります。そのため、後に脆弱性が発見された場合の事後対処に必要不可欠な各工程の記録・情報を収集・管理する仕組みや、それを共有し必要に応じて利用するルールが必要になります。

メーカ B 社では、R&D の組織内でセキュリティを専門とする研究者が中心になって、組込みソフトウェア開発ガイドラインの作成に着手しています。

また、メーカ C 社では、国際標準 ISO/IEC15408（コモンクライテリア） の認証取得および同レベルの開発品質を設定し、開発プロセスの中に脆弱性を排除する仕様・設計・検査を組込みんでいます。ISO/IEC15408 は、政府調達要件として位置付けられており、メーカとしては今後対応が必須となる可能性もあることから、有用な取組みと言えるでしょう。

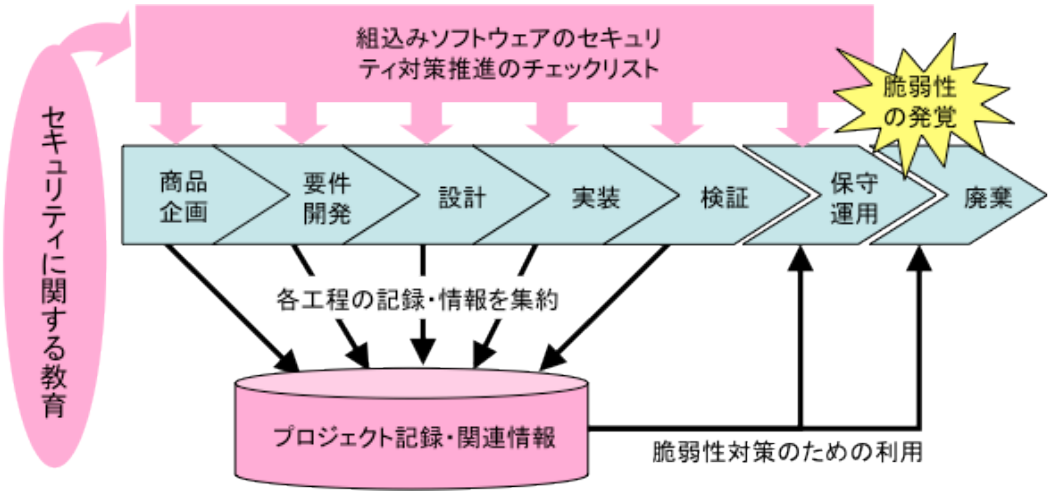



**図 5-7 セキュリティに関する教育・ルールの構造**

セキュリティ評価・監査

開発プロセスの各工程で適切なレビュー（検査）を実施することで、全体としての大幅な手戻りを削減することが期待されます。実際にどれだけ実施するかは予算や開発期間との兼ね合いであり、基本的にはプログラム不具合の修正（バグフィックス）など品質向上の取組みと同様な考え方で判断することができます。特に、開発部隊とは別の、セキュリティ担当者を含むスタッフによるプロジェクト監査等を実施することは重要です。

例えば、メーカ D 社では、セキュリティ検証をシステムテストの最終段階で第三者的な視点から行う部門・部署を設置することで、セキュリティ機能が正しく実装され動作しているか、セキュリティ上の脆弱性が残されていないかを確認している。このセキュリティ検証は企画段階での脅威分析と対をなし、システムテストの最終段階におけるセキュリティ対策として検証を行っています。

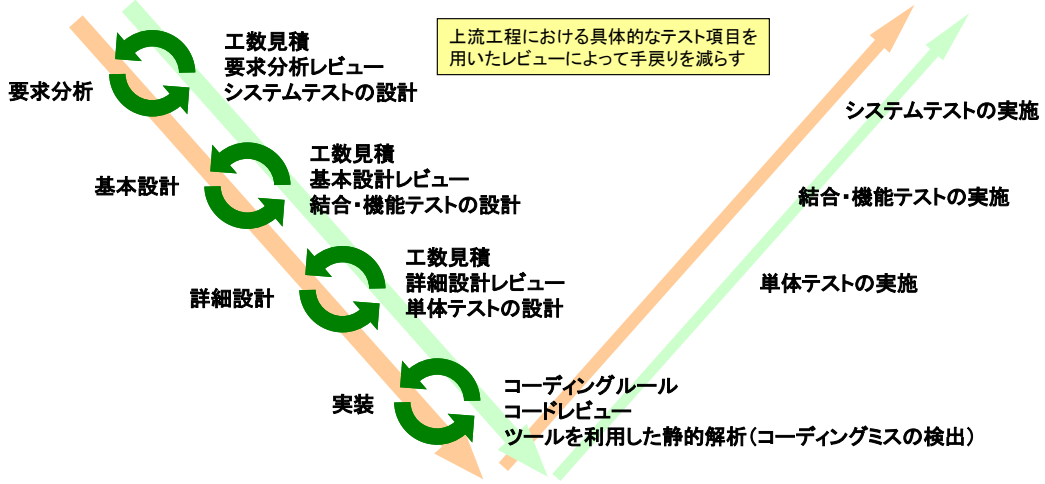



**図 5-8 各プロセスにおけるレビューの実施**

トラブルの事後対応

トラブル発生時の事後対応としての改修方法が変化しています。具体例としてウェブアクセスによるパッチダウンロード、販売店への持ち込み、放送波・インターネットによる改修プログラムの配信について紹介します。

対処事例(1):ウェブアクセスによるパッチダウンロード

ユーザが事業者から提供されたソフトウェアで改修を行う事例として、ルータに対する改修プログラム適用の例を紹介します。メーカ側は、既に数万台出荷されていた当該製品について、ネットワークを通じた修正プログラムの配布と並行して、サービスマンがユーザに電話をかけて修正プログラム適用を依頼する作業を実施しました。この作業ではユーザが修正プログラム(パッチ)をダウンロードし、機器に適用するといったユーザが関与する方法が取られました。

後に同メーカでは、本件を品質問題の一つとして捉え、社内告知するとともに、対策チームを結成し、こうした問題を未然に防ぐためのチェック項目を追加することとなりました。

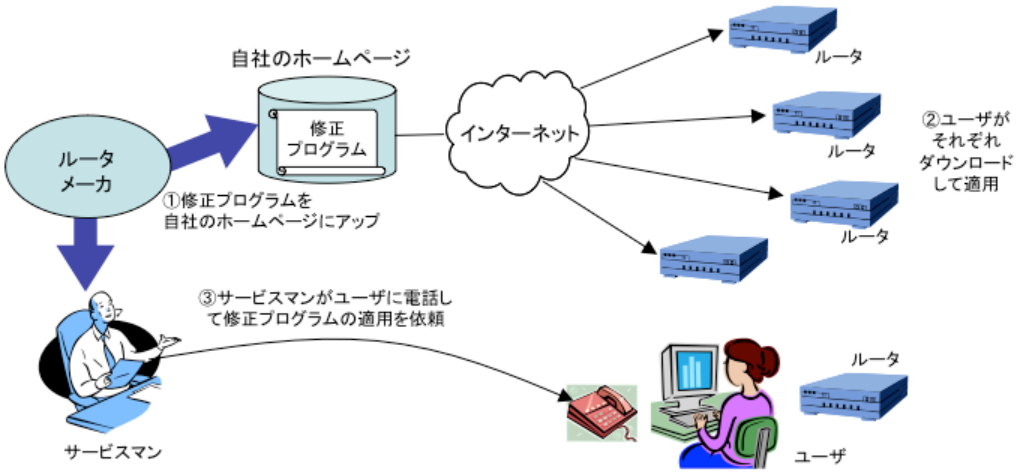



**図 5-9 ルータの改修方法**

対処事例(2):販売店への持ち込み

事業者が製品を回収しソフトウェアの改修を行う事例として、携帯電話に組み込まれていたソフトウェアの一つであるブラウザの改修の例を紹介します。携帯電話のブラウザの改修を行うにあたってサービス会社では、携帯電話の販売店において、無償でソフトの書換えを実施しました。1 回の書換えに 30 分～1 時間程度を要したとされます。

携帯電話のように消費者へ大量に普及する製品は、対策適用の実施が容易ではありません。販売店の店頭における対策の適用は、店舗にも消費者にも時間的なコストを強いる点で難しい選択であったと考えられます。

また、近年では自動車に関する製品回収も発生しており、リコールの結果として発生する費用や企業イメージの低下も懸念となっています。

一方でこのような対策は機器がインターネットなどを利用した改修に対応していない場合の対処としての改修方法であり、対策の徹底などは行ないやすくなります。

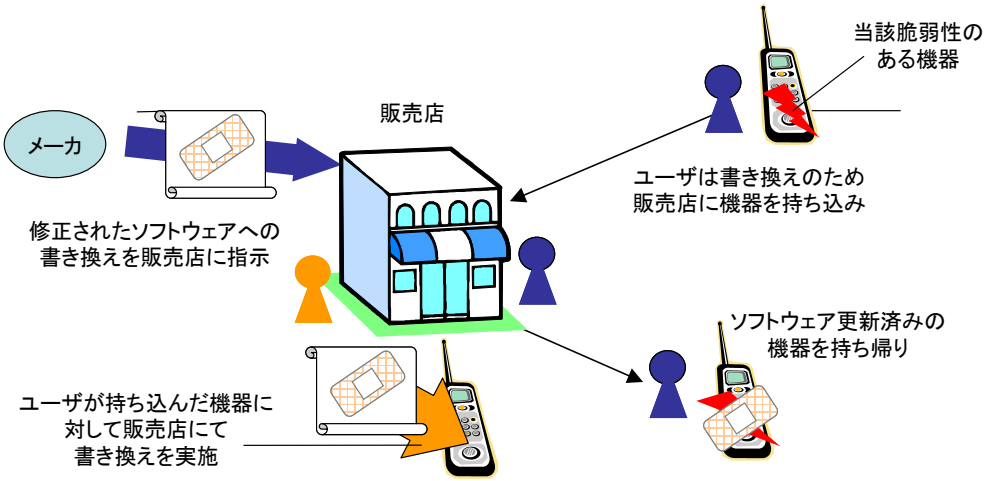



**図 5-10 携帯電話ブラウザの改修方法**

対処事例(3):放送波・インターネットによる改修プログラムの配信

近年新たに見られる事例として、放送波やインターネットによる改修プログラムの配信の例を紹介します。デジタルテレビには、放送波やインターネットを通じて、利用者には無料でプログラムのダウンロードが行われる仕組みがあります。これによってソフトウェアの不具合などを改修し性能を向上させることができます。

テレビ機器メーカは放送波を利用したファームウェアアップデートを行うことが可能であり、不具合のある製品のソフトウェアを回収するために改修プログラムを放送波経由で自社製品に配信し、ユーザが利用していない時間帯にアップデートを行う機能を備えています。近年では機能改修のためのアップデートだけでなく録画したデジタル放送のコピー回数を制限する「ダビング10」などの機能を追加するためのアップデートにも利用されています。

しかしながら、これらのソフトウェアを配信する際に不具合のあるプログラムを配信すると、脅威を広げてしまう可能性があります。

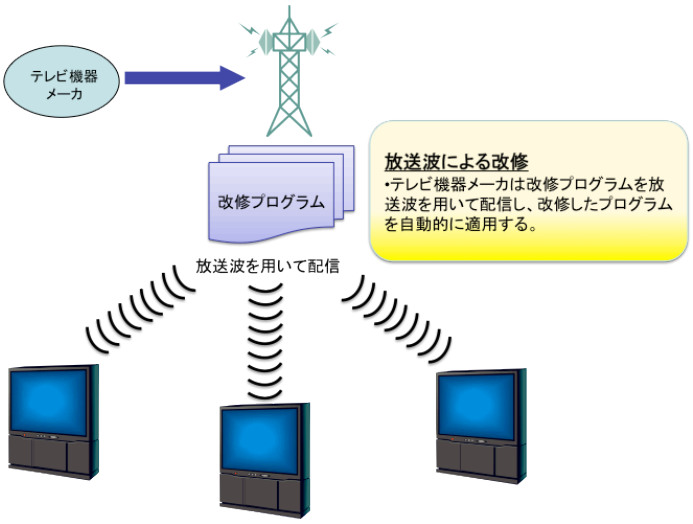



**図 5-11 放送波を用いた改修プログラムの配信**

### (3) その他の留意点

法制度

(1) 製造物責任法

経済企画庁国民生活局消費者行政第一課「逐条解説　製造物責任法」においては、「ソフトウェア自体については、無体物であり、製造物責任の対象とはしていない。ただし、ソフトウェアを組込んだ製造物については、本法の対象と解される場合がありうる。ソフトウェアの不具合が原因でソフトウェアを組込んだ製造物による事故が発生した場合、ソフトウェアの不具合が当該製造物自体の欠陥と解されることがあり、この場合、その欠陥と損害との間に因果関係が認められるときには、当該製造物の製造業者に本法に基づく損害賠償責任が生ずる」と記載されています。

これを踏まえると、脆弱性自体が、「欠陥」と考えられる場合に、他の要件を満たせば、損害賠償責任が生じると考えることができます。脆弱性が「欠陥」と考えられる場合とは、たとえば、提供時 において通常備えられている「セキュリティ」を備えていない状況が挙げられます。ネットワークでの利用が前提となっている機器については、外部からの攻撃を想定し、それに耐えられるものとされるべきと考えてよいのではないでしょうか。

(2) 消費生活用製品安全法

消費生活用製品安全法では、製品事故情報報告・公表制度が設けられています。この制度は、重大製品事故（一般消費者の生命又は身体に対する危害が発生した事故、または消費生活用製品が滅失し、又はき損した事故であって、一般消費者の生命又は身体に対する危害が発生するおそれのあるもの）が発生した場合に、消費生活用製品を製造・輸入する事業者が、消費者庁に報告することを義務化している制度です。

経済産業省「消費生活用製品安全法に基づく製品事故情報報告・公表制度の解説～事業者用ハンドブック～」 には、ソフトウェアについて以下の記述があります。

「ソフトウェアは無体物であり、消費生活用製品に該当しません。通常、ソフトウェアの場合、それを組み込んだ製品が消費生活用製品に該当します。」

これを踏まえると、ソフトウェアを組み込んだ家電機器等において、ソフトウェアの脆弱性が原因となる製品事故が発生またはそのおそれがあることを認識した事業者は、報告義務があるといえるでしょう。

ユーザとのインタフェース

幅広いユーザ層を対象とする組込み機器では、ユーザに負担感や誤解を与えることなく、セキュリティに配慮した設定や操作方法を選択するように誘導する必要があります。また、ユーザが危険な操作・変更を行おうとした場合には警告画面を提示するなどの配慮も有効です。単に機器そのものの機能だけでなく、リモコン等を含むユーザインタフェースについても、安全寄りの配慮について十分に検討しておくことが望まれます。

また、ユーザとメーカの接点であるマニュアルには、ソフトウェアの不具合や脆弱性が発覚した際

の対処方法、その機器を廃棄する際にユーザが行うべきプライバシー情報の削除方法なども記載しておくことが望まれます。

さらに、トラブルが発生した場合、最初に連絡が来るのはお客様相談窓口です。窓口のスタッフに対し、従来の不具合だけでなく、攻撃によるトラブル発生の可能性やその際の適切な応対・処理について教育しておく必要があります。

# 6. 海外動向と国際標準

この章では、国外における脆弱性対策の状況に関して、米国政府の推進する取り組みを解説します。また、脆弱性対策に関する国際標準化の動向について紹介します。

## 6.1. 米国における脆弱性対策の現状

米国では、2002 年の FISMA[78]の施行以降、セキュリティ規格やガイドラインに従い、情報システムにセキュリティ要件を反映する活動が進められています。特に、セキュリティ設定に関する作業を手作業で行なうと、設定ミスや設定者のセキュリティ知識の程度や判断の相違などにより、セキュリティ要件を損なう可能性があることから、作業の自動化が試みられています。
NIST[79]では、米国政府を対象とした情報セキュリティ管理の技術面での自動化と標準化を規定した仕様群である SCAP[80]の展開を推進しています。SCAP では、情報システムに対するセキュリティ対策の負荷軽減を支援しています。脆弱性対策の管理やコンプライアンス管理への組織対応を自動化することにより、組織が費やす時間と費用を節約することを目指しています。

本節では、組織の内部で複雑化する脆弱性対策を、自動化することによって確実に実施し、情報システムのセキュリティをこれまで以上に強化するための、米国政府の取り組みを紹介します。

### 6.1.1. 米国政府の取り組み

政府省庁では、様々な法律（FISMA、SOX 法等）や FIPS[81]、ガイドライン（NIST SP800 シリーズ）等からセキュリティ要求事項を洗い出し、あらゆる情報システム（モバイル、エンタープライズ、クライアント等）に対して、セキュリティ要求事項を設定しました。そのため、政府省庁では、セキュリティコンプライアンスへの技術的対応に膨大な時間と労力を費やし、その上、複雑化したコンプライアンスへの管理に対する負荷も増大しました。また、設定作業を手作業で行うと、設定ミスや設定者のセキュリティ知識の程度、判断の相違等からセキュリティが損なわれる可能性があります。これらの理由から、各種の設定を自動化することが求められるようになりました。そのため、NIST は情報セキュリティ対策の自動化と標準化を目指した SCAP の開発を推進しています。

2007 年に入ると、OMB[82]の主導により、Windows ソフトウェアを米国政府が定めた「共通セキュリティ設定」に準拠させることを決定しました。これにより、ベースラインのセキュリティを確保しつつ、ヘルプデスク及びパッチ検証にかかる費用を大幅に削減することを目的とした FDCC[83]が開始されました。FDCC では、米国政府のデスクトップ環境が FDCC に沿っているかを自動チェックする手段の 1 つとして SCAP を普及展開しました。

---

78 Federal Information Security Management Act：連邦情報セキュリティマネジメント法
http://csrc.nist.gov/groups/SMA/fisma/index.html
79 National Institute of Standards and Technology：米国国立標準技術研究所
http://www.nist.gov/index.html
80 Security Content Automation Protocol：セキュリティ設定共通化手順
http://scap.nist.gov/
81 Federal information Processing Standards：連邦情報処理規格
http://www.itl.nist.gov/fipspubs/
82 Office of Management and Budget：行政管理予算局
http://www.whitehouse.gov/omb
83 Federal Desktop Core Configuration：連邦政府共通デスクトップ基準
http://nvd.nist.gov/fdcc/index.cfm

2008 年には、連邦政府 CIO 評議会（Federal CIO Council）配下の AIC 委員会（Architecture and Infrastructure Committee）の TIC（Technology Infrastructure Subcommittee）が FDCC を維持管理するようになり、制度面と技術面の双方から情報セキュリティ対策の推進が加速されました。

AIC 委員会は、FDCC を更に発展させ、米国政府で広く使われているプラットフォームを対象に「共通セキュリティ設定」に準拠させるため、2010 年 5 月 7 日に USGCB（The United States Government Configuration Baseline：米国政府共通設定標準）の導入を発表しました。同年 9 月 24 日には、NIST から、USGCB Major Version 1.0 がリリースされ、運用が開始されました。Windows XP と Windows Vista については FDCC で対応済みであることから、USGCB では、Windows 7 と Internet Explorer 8 のセキュリティ設定を中心に整備を進めています。

## 6.1.2. SCAP の概要

現在、SCAP は表に示す 6 つの標準仕様から構成されています。

SCAP を構成する仕様群の概要

| 共通基準 | 概要 |
|---|---|
| 共通共通識別子<br>CVE (Common Vulnerabilities and Exposures) | プログラム自身に内在するプログラム上のセキュリティ問題に一意の番号(脆弱性識別子)を付与する仕様 |
| 共通セキュリティ設定一覧<br>CCE (Common Configuration Enumeration) | プログラムが稼働するための設定上のセキュリティ問題に一意の番号を付与する仕様 |
| 共通プラットフォーム一覧<br>CPE (Common Platform Enumeration) | 情報システム，プラットフォーム，ソフトウェアパッケージに一意の名称を付与する仕様 |
| 共通脆弱性評価システム<br>CVSS (Common Vulnerability Scoring System) | 脆弱性自体の特性，パッチの提供状況，ユーザ環境での影響度などを考慮し脆弱性の影響度を評価する仕様 |
| セキュリティ設定チェックリスト記述形式<br>XCCDF (EXtensible Checklist Configuration Description Format) | 情報セキュリティチェックリストやベンチマークなどの文書を記述するための仕様 |
| セキュリティ検査言語<br>OVAL (Open Vulnerability Assessment Language) | プログラム上のセキュリティ問題や設定上のセキュリティ問題をチェックするための手続き仕様 |

以下に、これらの標準仕様について概要を説明します。

(a) 脆弱性を職別するための CVE

CVE は、個別製品中の脆弱性を対象として、米国政府の支援を受けた非営利団体の米国 MITRE 社が採番している識別子です。脆弱性検査ツールや脆弱性対策情報提供サービスの多くが CVE を利用しています。個別製品中の脆弱性に一意の識別番号「CVE 識別番号(CVE-ID)」を付与することにより、組織 A の発行する脆弱性対策情報と、組織 B の発行する脆弱

性対策情報とが同じ脆弱性に関する対策情報であることの判断や、対策情報同士の相互参照や関連付けに利用できます。

「情報セキュリティ早期警戒パートナーシップ」を通した脆弱性対策の技術仕様面での国際連携も進んでいます。2008 年 10 月には、MITRE 社が公表する「CVE 情報源サイト」の一つとして JVN と JVNiPedia が公示されるようになりました。また、JVN、JVNiPedia、MyJVN 脆弱性対策情報収集ツール（MyJVN Filtered Vulnerability Countermeasure Information Tool）も 2010 年 1 月に CVE 互換認定を受けました。さらに、同年 6 月には、CVE 採番の役割を担う CNA（CVE Numbering Authority）として JPCERT/CC が認定されました。

(b) セキュリティ設定を識別するための CCE

SCAP では、セキュリティに関連するシステム設定項目を識別するために CCE を利用しています。CCE は、システム設定情報に対して共通の識別番号「CCE 識別番号(CCE-ID)」を付与することで、脆弱性対策情報源やセキュリティツール間のデータ連携を実現します。

例えば、パスワード設定に関連した項目には、パスワードの有効期間、パスワードの長さ、パスワードの複雑さ、パスワードの履歴管理などがありますが、これらの各項目に一意の CCE 識別番号を付与して管理しています。

CCE は、コンピュータのベースラインのセキュリティを確保するために必要となる設定項目を一覧として利用できるため、IPA では、Windows Vista／Windows XP のパスワード関連項目を対象とした CCE 識別番号と推奨値に基づきチェックすることのできる MyJVN セキュリティ設定チェッカを 2010 年 11 月から提供しています。

(c) 製品を識別するための CPE

CPE は、ハードウェア、オペレーティングシステム、アプリケーションなどのプラットフォームを識別するための、構造化された名称体系を規定しています。CPE を用いると、ベンダ、セキュリティ専門家、情報システム管理者、ユーザ等の間で、脆弱性の存在する対象となるプラットフォームを共通の言葉で議論できるようになります。

CPE は、MITRE 社が中心となって仕様策定を進め、2007 年 1 月に第 1 版を公開、さらに米国の脆弱性情報データベースである NIST の NVD（National Vulnerability Database）、米国政府のデスクトップ基準である FDCC の適用を通して仕様改善が行われています。また、規定に沿ってプラットフォームに付与した名称の一覧が CPE Dictionary として、2008 年 4 月に NIST から公開されています。

IPA では、CPE Dictionary を参考に、JVN iPedia で公開するそれぞれの脆弱性対策情報を CPE 名で関連付ける MyJVN 脆弱性対策情報収集ツールを 2008 年 10 月に公開しています。

(d) 脆弱性の深刻度を評価するための CVSS

CVSS は、①脆弱性そのものの特性を評価する基本評価基準（Base Metrics）、②脆弱性の現在の深刻度を評価する現状評価基準（Temporal Metrics）、③製品利用者の利用環境も含め最終的な脆弱性の深刻度を評価する環境評価基準（Environmental Metrics）の 3 つの視点か

ら評価を行ないます。CVSS を用いると、脆弱性の深刻度を同一の基準で定量的に比較できます。現在、CVSS は、30 を超える組織で採用されています。

CVSS は、FIRST（Forum of Incident Response and Security Teams：コンピュータセキュリティインシデント対応チームフォーラム）の CVSS-SIG（Special Interest Group）で適用推進や仕様改善が行われています。IPA も CVSS-SIG に参画しており、JVN iPedia[84]や脆弱性関連情報の調査結果のウェブサイトにおける CVSS 基本値の公表、多言語対応した CVSS バージョン 2 用計算機のウェブサイト公開を通して、CVSS の普及に努めています。

(e) チェックリストを記述するための XCCDF

XCCDF は、セキュリティチェックリストやベンチマークなどを記述するための仕様言語です。ソフトウェアの設定上のセキュリティ問題について、組織としてチェックすべき項目を CCE と共にリストアップし、XCCDF の仕様に沿ってチェックリストを作成します。プログラム自身に内在する脆弱性についても、例えば「セキュリティ修正プログラムの適用」という項目を XCCDF の仕様に沿ってチェックリストを作成します。

XCCDF で記述されたチェックリストは、情報システムに対するセキュリティ設定規則を構造化した集合体で、その仕様は、情報交換、文書生成、組織または状況への適合、整合性のテスト及び評価の自動化をサポートするようデザインされており、データモデルやベンチマークのテスト結果を格納するフォーマットとしても定義されています。

IPA では、チェックリストに基づき PC のセキュリティ設定を確認するという考え方を普及するため、2009 年 12 月に、XCCDF で記述した PC のセキュリティ設定チェックリストを自動で確認する「MyJVN セキュリティ設定チェッカ」[85]を公開しました。

(f) 脆弱性やセキュリティ設定をチェックするための OVAL

OVAL は、コンピュータのセキュリティ設定状況を検査するための仕様です。ソフトウェアに脆弱性が発見されると、製品ベンダ、セキュリティベンダなどが提供する脆弱性対策情報に基づき、その脆弱性がコンピュータに存在するかを確認する場面はまだまだ多く見られます。OVAL は、このような文書による脆弱性対策情報を、機械処理可能な XML ベースの OVAL 言語で記述します。

OVAL を用いると、脆弱性対策のための確認作業の自動化により管理工数が低減できます。また、文書という脆弱性対策情報と手作業による確認作業で発生しうる漏れを防止し、情報システムの資産管理への適用など、情報システムの全般の管理にも役立てることができます。

IPA では、NIST が公開している FDCC を参考に、JVN iPedia に登録されている製品の中から、コンピュータウイルスやボットの感染経路の対象となりやすいソフトウェア製品を中心に、最新のバージョンであるかどうかをチェックするためのバージョンチェックツール「MyJVN バージョンチェッカ」[86]を開発し、2009 年 11 月から公開しています。

---

84 ⇒ 本書 7.4.2.「脆弱性対策情報データベース（JVN iPedia）」
85 ⇒ 本書 7.4.2.「MyJVN セキュリティ設定チェッカ」
86 ⇒ 本書 7.4.2.「MyJVN バージョンチェッカ」

## コラム： 脆弱性対策に係る機械化処理

JVN(Japan Vulnerability Notes)は、セキュリティに関わるシステム管理者ならびにシステムエンジニア向けに脆弱性対策情報を広く告知することを目的とした情報公開サイトです。2003 年 2 月に JPCERT/CC の試行サイトとして運用を開始しました。2004 年 7 月には経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」を受け、日本国内の製品開発者の脆弱性対応状況を公開するサイトとして情報発信を行なっています。2007 年 4 月からは，即時性と網羅性とを備えた情報提供を実現するため、JVN と JVN iPedia の 2 つのコンポーネント構成に拡張してきました。

しかし、2008 年以降、普段の業務や日常的に使用しているアプリケーションの脆弱性を狙った攻撃が、標的型攻撃 [87]や Web 誘導型マルウェアの流布において利用される傾向にあります。この背景には、受動型攻撃を主流とする侵害活動に変わってきたこと、良く利用されているアプリケーション、いわゆる定番ソフトウェアに内在する脆弱性の増加が挙げられます。国内の脆弱性対策データベース JVN iPedia によれば、定番ソフトウェアとして良く利用されているアプリケーションの脆弱性登録件数は、2008 年から 2010 年にかけて 2 倍近く増えています。特に、2009 年に流布した Web 誘導型マルウェアである Gumblar 以降、アプリケーションの脆弱性を悪用したマルウェア感染への対策は急務であり、アプリケーションを常に最新バージョンに維持することが必要となってきている状況にあります。

国内においては、上述のように JVN や JVN iPedia など脆弱性対策情報の提供環境は充実し、脆弱性の傾向などを把握しやすくなってきています。しかし、対策情報の多くは主に文書として構成されており、脆弱性の有無をチェックして対策を促すなど脆弱性対策に関わる処理の機械化については発展途上にありました。

このような問題解決に向けて、2008 年から、JVN で整備を進めている脆弱性対策に関わる処理の機械化を目指すフレームワーク MyJVN(JVN 脆弱性対策機械処理基盤)を推進しています。MyJVN では、これまでに、JVN と JVN iPedia に登録された脆弱性対策情報を製品視点でフィルタリング可能な情報提供サービス、アプリケーションの最新状態をチェックリストを用いて機械的に確認する、「MyJVN バージョンチェッカ」、パソコンのセキュリティ設定をチェックリストを用いて機械的に確認する「MyJVN セキュリティ設定チェッカ」を公開してきました。

### MyJVN 脆弱性対策情報収集ツール

情報セキュリティの専門家を持たない企業や組織にとって、必要な脆弱性対策情報のみを収集することは容易ではありません。「MyJVN 脆弱性対策情報収集ツール」は JVN iPedia に登録された情報の中から利用者に関係するソフトウェア製品に関する情報のみを効率的に収集できるようにするツールです。MyJVN においては，セキュリティ問題をチェックする手続き仕様 OVAL を用いて、セキュリティ問題をチェックする手続き仕様を整備し、脆弱性対策に係る処理の機械化を実現しています。

[87] ⇒ 本書用語集「標的型攻撃」

URL：http://jvndb.jvn.jp/apis/myjvn/mjcheck.html

**MyJVN バージョンチェッカ**

「MyJVN バージョンチェッカ」は PC にインストールされているソフトウェア製品が最新バージョンであるかどうかを確認するツールです。セキュリティチェックリストやベンチマークなどを記述するための仕様言語である XCCDF と、NIST が公開する FDCC（Federal Desktop Core Configuration：連邦政府共通デスクトップ基準）を参考に、XML ベースの OVAL 言語で記述された脆弱性対策情報を機械処理しています。

URL：http://jvndb.jvn.jp/apis/myjvn/vccheck.html

**MyJVN セキュリティ設定チェッカ**

「MyJVN セキュリティ設定チェッカ」は USB メモリの自動実行機能などの Windows のセキュリティ設定を簡単な操作で確認可能なツールです。セキュリティチェックリストやベンチマークなどを記述するための仕様言語である XCCDF で記述した PC のセキュリティ設定チェックリストと XML ベースの OVAL 言語を用いて機械処理しています。

URL：http://jvndb.jvn.jp/apis/myjvn/sccheck.html

## 6.2. 脆弱性対策に関する標準

製品や技術を、国境を超えて利用できるようにするために制定された、国際的な共通規格を国際標準と言い、国際標準を策定する活動を国際標準化活動と言います。本節では、情報セキュリティにおける技術の標準化団体である ISO/IEC[88]（国際標準化機構/国際電気標準会議）やITU-T[89]（国際電気通信連合電気通信標準化部門）における脆弱性対策関連の国際標準化活動について紹介します。

### 6.2.1. ISO/IEC JTC1/SC27 における検討

ISO/IEC JTCl/SC27[90]では複数の TC（Technical Committee）/SC（Sub-Committee）やITU-T 等に共通する情報セキュリティの要素、管理システム、及びサービス技術の標準化を担当してます。SC27 には、5 つの WG(Working Group)が設置されている。各 WG の業務概要を以下に示します。

・WG1：ISMS に関する 27000 シリーズやそれに関連する標準化
・WG2：暗号アルゴリズムや暗号プロトコルを含む暗号のセキュリティメカニズムの標準化
・WG3：情報セキュリティシステムのセキュリティ評価及び認証や暗号モジュールの試験及び認証等の情報セキュリティ評価や脆弱性情報開示に関する標準化
・WG4：セキュリティコントロールに関する標準化である 27030 シリーズの作成
・WG5：アイデンティティ管理とプライバシーフレームワーク等の標準化

このうち、脆弱性対策関連のテーマは、WG3 において検討が進められています。日本からは、JPCERT/CC、IPA 等の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関係者を中心に、SC27 国際会議への参加ならびに日本の標準化組織である情報規格調査会を通じて、これらの国際標準が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整合したものとなるよう、働きかけています。

（1） 脆弱性情報の開示（ISO/IEC 29147：Vulnerability Disclosure）

「脆弱性情報の開示」は、ベンダが脆弱性情報を受信する際の心得、ベンダが脆弱性情報に関する情報を開示する際の心得など、運用上、考慮すべき点を標準化の対象としています。当初、タイトルは「Responsible Vulnerability Disclosure」でしたが、2010 年 4 月のマラッカ会合で「Vulnerability Disclosure」に変更されました。さらに、記述内容が拡大してきたことから、2011 年 1 月には、製品開発者等のベンダが他の組織と行う脆弱性関連情報のやり取りを扱う部分（ISO/IEC 29147）と、製品開発者等のベンダの内部プロセスを扱う部分（「脆弱性対応手順」、(2)で紹介）に分割して検討されることになりました。

---

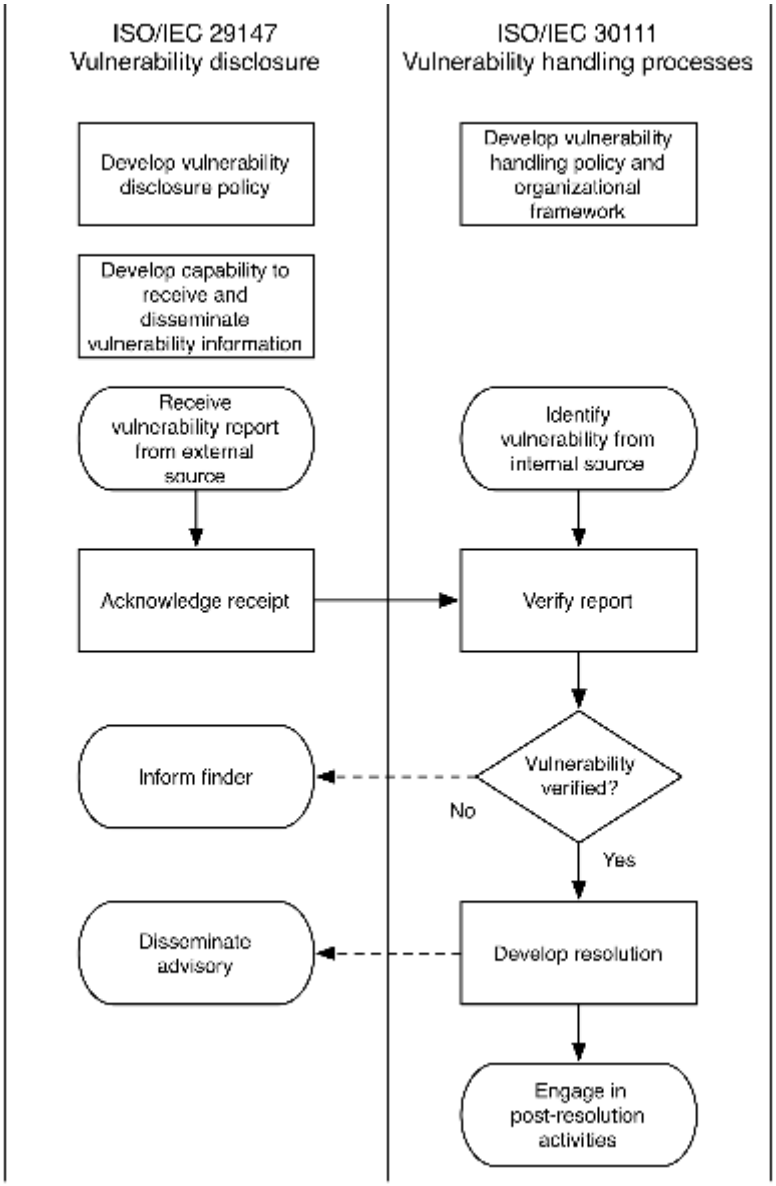
88 International Organization for Standardization / International Electrotechnical Commission
89 International Telecommunication Union Telecommunication Standardization Sector
90 Joint Technical Committee 1 / Sub-Committee 27

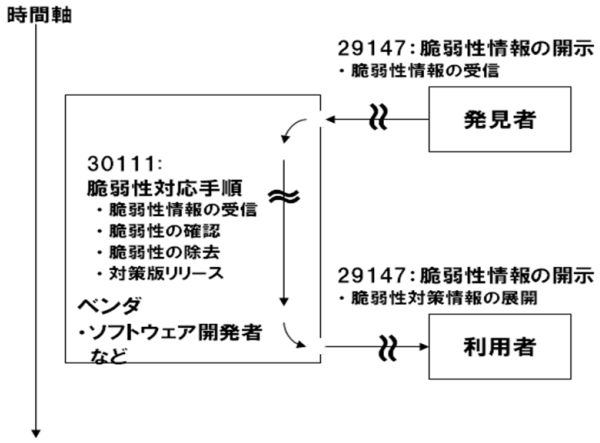
ISO/IEC 29147 は、2011 年 6 月に CD（Committee Draft）第 3 版が発行され、今後の改訂作業については、計画を 2 年遅らせて 2013 年春に次の標準化段階に進めることを目指しています。

（2） 脆弱性対応手順（ISO/IEC 30111: Vulnerability Handling Processes）

「脆弱性対応手順」は、ベンダが脆弱性情報を受信してから、対策を完了させるまでの内部プロセスの手順を中心に、考慮すべき点を標準化しています。2010 年 10 月に「脆弱性情報の開示」から分割され新規規格として提案されました。

2011 年 6 月には WD(Working Draft) 30111 が提示されました。WD では、日本の提案に基づき、脆弱性情報を取り扱うためのベンダの社内体制について新たな章が設けられ記述が拡充されました。なお、社内体制に関する記述については、情報セキュリティ早期警戒パートナーシップの発足時（2004 年 8 月）に社団法人電子情報技術産業協会が中心になってとりまとめた「製品開発ベンダ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」の中の関連する記述を参考に提案しています。




ISO/IEC 29147 と ISO/IEC 30111 の関係

### 6.2.2. ITU-T における検討

ITU-T の SG17（Sub-Group）では、サイバーセキュリティ情報交換のためのデータの構造化、サイバーセキュリティ情報とエンティティの識別と発見、ネットワークを介して安全にサイバーセキュリティ情報を交換するための規格である「サイバーセキュリティ情報交換フレームワーク」（CYBEX: Cybersecurity Information Exchange Framework）シリーズの標準化を推進しています。

フレームワーク全体については、X.cybex（X.1500）として審議が進められています。

サイバーセキュリティ情報交換のためのデータの構造化では、脆弱性や脆弱性対策情報の交換、イベント／インシデントなどの交換、LEA(Law Enforcement Agency)との情報交換や証拠情報の交換のためのデータフォーマット、評価手法の整備を目的とし、SCAP、CWE などの仕様を標準として取り込んでいます。

X.cybex は、2009 年 9 月に ITU-T SG17 において NWI(New Work Item)として採択されました。この NWI 化の背景には、2008 年の国際電気通信連合の総会（WTSA08）決議 58（開発途上国における CSIRT 構築支援）と、決議 58 を実行するためにまとめられた TD0366（2009 年 6 月）があります。TD0366 では、「CSIRT 構築に関するフレームワーク開発」、「サイバーセキュリティ組織へのサイバーセキュリティ情報交換識別子」、「FIRST との連携」、「グローバルなサイバーセキュリティ情報交換フレームワークの整備」の 4 つを活動項目に挙げています。

2009 年の秋以降、ITU-T SG17 と ISO SC27 の間では、活動概要に関する情報交換が継続的に行われています。X.cybex は、セキュリティ情報交換フレームワークの技術仕様側面での整備を対象としており、製品開発者等のベンダが他の組織と脆弱性関連情報をやりとりする方法等運用仕様側面での整備を対象とする「脆弱性情報の開示」（ISO/IEC 29147）、「脆弱性対応手順」(ISO/ISC 30111)とは、相互に補完する関係として位置付けられます。

また、X.cybex(X.1500)の付録では、サイバーセキュリティ情報交換のユースケースとして、米国の FDCC（Federal Desktop Core Configuration：連邦政府共通デスクトップ基準）、日本の JVN、MyJVN(JVN 脆弱性対策機械処理基盤)の取り組みが取り上げられています。

# 7. ソフトウェアやシステムのライフサイクルと脆弱性対策

この章では、情報システムやそれを構成するソフトウェアのライフサイクルに沿って、その時々に実施すべき脆弱性対策について述べます。本文で該当する箇所を示すとともに、IPA ウェブサイト等より入手可能な脆弱性関連の各種資料について概要を紹介します。

## 7.1. 情報セキュリティをライフサイクルに組み込む

情報セキュリティを効率的にソフトウェア製品やウェブサイトに組み込むためには、それらのライフサイクルに最初から情報セキュリティに関する取り組みを組み込むことがもっとも効率的で効果的です。

本書では、簡単なモデルとして、ライフサイクルを企画、設計・開発・製造、運用／利用、廃止の5つのフェーズで表し、情報セキュリティのなかでも特に脆弱性対策をそれぞれに組み込むために有用な方策について参考となる資料を紹介します。

## 7.2. 企画

### 7.2.1. 企画段階における脆弱性対策

ライフサイクルの企画段階におけるセキュリティ対策としては、脅威の動向について情報を集めて現状を把握し、開発方針や体制にこれらの情報を反映することが重要です。

最新の脆弱性、特にこれから開発・構築する情報システムに用いることとなるソフトウェアの脆弱性についての情報を集めましょう。また、情報システムを開発・構築する上で、作りこむ可能性が特に高いと考えられる脆弱性や狙われる可能性が高い脆弱性については、事前に洗い出しておきたいものです。企画段階では、これらの脆弱性について対策を要件化し、開発プロセスにおいてどのようにそれらの対策を組み込むかを検討します。

### 7.2.2. 「企画」段階に関して入手可能なコンテンツ

#### (1) 2012 年版 10 大脅威 変化・増大する脅威！

IPA は、2011 年に IPA へ届出のあった脆弱性情報や一般報道を基にし、近年の情報セキュリティを取巻く状況を解説した「2012 年版 10 大脅威 変化・増大する脅威！」をまとめ、IPA のウェブサイトで公開しています。2012 年版 10 大脅威は、2011 年に IPA へ届出のあった脆弱性情報や一般報道を基にして、情報セキュリティ分野の研究者や実務担当者 123 人で構成する「10 大脅威執筆者会」でまとめたものです。2005 年から毎年公開し、累計で 100 万件のダウンロードがされており、企業の研修やセキュリティ教育等で活用されています。また、海外の技術者も活用できるように、英語版資料も公開しています。(2012 年 9 月公開)

URL: http://www.ipa.go.jp/security/vuln/10threats2012.html

URL: http://www.ipa.go.jp/security/vuln/documents/10threats2012_en.pdf

#### (2) 情報セキュリティ白書 2012

IPA は、IT の専門家や技術者だけでなく、一般の利用者にも情報セキュリティの現状を周知す

ることを目的に、国内外の注目すべき情報セキュリティ事件・事故や、新しいサービス・情報機器の利用拡大による新たな脅威など、広く情報セキュリティに関する出来事や状況をまとめ、「情報セキュリティ白書 2012」として出版しています。

「情報セキュリティ白書」は、公的機関としての IPA が毎年発行する情報セキュリティに関する報告書です。企業のシステム開発者・運用者に対して情報セキュリティの現状や、今後の対策のために役立つ情報を提供するとともに、パソコンやスマートフォン等の情報機器を使用する一般の利用者にも情報セキュリティの概観や身近な話題を提供することを目的としています。(2012 年 6 月より販売)

URL: http://www.ipa.go.jp/security/publications/hakusyo/2012/hakusho2012.html

### (3) 知っていますか？脆弱性 (ぜいじゃくせい)

IPA は、ウェブサイト運営者や一般利用者にウェブサイトの脆弱性(ソフトウェア等におけるセキュリティ上の弱点)について理解を深めていただくため、ウェブサイトの脆弱性を分かりやすく解説するコンテンツ「知っていますか？脆弱性(ぜいじゃくせい)-アニメで見るウェブサイトの脅威と仕組み-」を IPA のウェブサイトで公開しています。

今日、インターネットを利用する上でセキュリティの知識や対策は必要不可欠です。「知っていますか？脆弱性(ぜいじゃくせい)」は、脆弱性についての理解を広め、対策の普及･向上を図るため、多くのウェブサイト運営者や製品開発者の方々に活用されている「安全なウェブサイトの作り方」等で取り上げている代表的な 10 種類の脆弱性を、一般の方々にもわかりやすく、アニメーションで解説しています。(2007 年 7 月公開)

URL: http://www.ipa.go.jp/security/vuln/vuln_contents/

### (4) 組込みソフトウェアを用いた機器におけるセキュリティ (改訂版)

IPA は、情報家電など組込みソフトウェアを用いた機器のセキュリティ対策の推進に役立てるために、組込みソフトウェアの生産・販売企業の経営層・管理層を対象にした啓発資料を公表しています。この資料で脆弱性対策をセキュリティ対策の中心的な対策として取り上げています。

経営層・管理層向けには、脆弱性対策が不十分であった場合の影響等を具体的な事例で示すことに重点をおいた『組込みソフトウェアを用いた機器におけるセキュリティ』を作成しています。この啓発資料は最初は 2006 年に公開しましたが、その後の組込みシステムを取り巻く環境の変化や技術の進展などを反映し、改訂版を 2011 年に公開しています。

URL: http://www.ipa.go.jp/security/fy22/reports/vuln_handling/index.html

### (5) 組込みソフトウェアのセキュリティ ～機器の開発等における 40 のポイント～

IPA は組込みソフトウェア開発の技術者を対象とした開発ポイント集をとりまとめています。現場の技術者向けに組込みソフトウェアの各工程における 40 のポイントを提示した『組込みソフトウ

ェアのセキュリティ ～機器の開発等における 40 のポイント～』を公表しています。(2006 年 5 月)
URL: http://www.ipa.go.jp/about/press/20060518.html

### (6) 組込みシステムのセキュリティに関するその他の資料

その他にも IPA では組込みシステムのセキュリティに関して次のような資料を公開しています。

・「組込みシステムのセキュリティへの取り組みガイド(2010 年改訂版)」
URL: http://www.ipa.go.jp/security/fy22/reports/emb_app2010/

・「自動車と情報家電の組込みシステムのセキュリティに関する調査報告書」(2008 年度)
URL: http://www.ipa.go.jp/security/fy20/reports/embedded/

・「複数の組込み機器の組み合わせに関するセキュリティ調査報告書」(2007 年度)
URL: http://www.ipa.go.jp/security/fy19/reports/embedded/

・「組込みシステムの脅威と対策に関するセキュリティ技術マップの調査報告書」(2006 年度)
URL: http://www.ipa.go.jp/security/fy18/reports/embedded/

## 7.3. 設計・開発・製造

### 7.3.1. 「設計・開発・製造」における脆弱性対策

ライフサイクルの設計段階では、次のような観点から脆弱性への対策を行います。

まず、セキュリティの観点からソフトウェアの構造を定義し、重要なセキュリティ機能のコンポーネントを定義します。特に攻撃対象となり脆弱性を狙われることが多いと考えられる機能を特定することで、続くプロセスで可能な限り安全にすることができます。

また、ソフトウェアに危害が及ぶ可能性について見積もり、脅威についてモデル化を試みます。脅威をモデル化することで必要なセキュリティ機能と慎重なセキュア・コーディング、セキュリティテストが特に必要となる箇所を特定し、脆弱性を低減化することが可能になります。

開発・製造の段階での主要な脆弱性対策としては、セキュア・コーディングによりソフトウェアを作成しテストを進めることが挙げられます。標準的なコーディング手法は脆弱性につながる欠陥をソフトウェアに作りこむのを防止するために有用です。標準的なテスト手法は脆弱性検出に役立ちます。コードレビュー[91]によっても脆弱性を発見し修正することができます。特に狙われることが多い機能を重点的にレビューすることが重要です。

製造段階に入る前に専門家によるペネトレーションテスト [92]を行うこともあります。このテストに

[91] ⇒ 本書用語集「コードレビュー」
[92] ⇒ 本書用語集「ペネトレーションテスト」

より、脆弱性を洗い出すだけでなく、これ以前のプロセスにおける対策がどの程度有効であったかをはかることができます。

### 7.3.2. 「設計・開発・製造」に関して入手可能なコンテンツ

#### (1) 安全なウェブサイトの作り方 改訂第5版

IPA は、ウェブサイト開発者・運営者が適切なセキュリティを考慮したウェブサイトを作成するための資料「安全なウェブサイトの作り方」をウェブサイトで公開しています。

「安全なウェブサイトの作り方」は、IPA が届出を受けた脆弱性関連情報を基に、届出件数の多かった脆弱性や攻撃による影響度が大きい脆弱性を取り上げ、ウェブサイト開発者や運営者が適切なセキュリティを考慮したウェブサイトを作成するための資料です。

これまでに 4 度の改訂を行い、脆弱性とその対策の実態を踏まえて注意点や失敗例等の記述を都度拡充しています。(現在は第 5 版。2011 年 4 月公開)

URL: http://www.ipa.go.jp/security/vuln/websecurity.html

#### (2) 安全な SQL の呼び出し方

近年ウェブサイトを狙った SQL インジェクション [93]攻撃が継続し深刻な被害が発生している実態を踏まえ、SQL インジェクション攻撃への具体的な対策書として、IPA はウェブアプリケーションの安全な実装方法を解説した資料「安全な SQL の呼び出し方」をウェブサイトで公開しています。

「安全な SQL の呼び出し方」では、SQL インジェクション対策が安全なものであるための要件を掘り下げて検討し、どの製品をどのように使えば安全な SQL 呼び出しを実現できるのか、その考え方を整理しながら、いくつかの具体的ケースについて調査結果を示しています。「安全な SQL の呼び出し方」は「安全なウェブサイトの作り方」の別冊という位置づけです。(2010 年 3 月公開)

URL: http://www.ipa.go.jp/security/vuln/websecurity.html

#### (3) セキュア・プログラミング講座

IPA はソフトウェア開発者を対象に「セキュア・プログラミング講座」を公開しています。この「セキュア・プログラミング講座」は、ソフトウェア開発工程に沿うように編集されています。従来、ソフトウェア開発の下流工程においてセキュリティ脆弱性が発見され、それらについて対処されることが多くありましたが、作り込まれた脆弱性によっては、容易に修正できなくなったり、例え修正できたとしても不経済な事態となったりします。そこで「セキュア・プログラミング講座」では、下流工程において取り返しがつかない脆弱性を作り込まないために、上流工程(要件定義、設計)から脆弱性対策のポイントを意識できるようにすることを狙っています。(Web アプリケーション編:2007 年 6 月公開。C/C++言語編:2007 年 9 月公開)

URL: http://www.ipa.go.jp/security/awareness/vendor/programming/

[93] ⇒ 本書用語集「SQL インジェクション」

### (4) ファジング活用の手引き（別冊：「ファジング実践資料」）

IPA は、ソフトウェア製品の脆弱性を検出する技術の一つである「ファジング」の概要から実践方法、および製品開発組織におけるファジングの活用方法などをまとめた資料「ファジング活用の手引き」をウェブサイトで公開しています。この手引きには、IPA における「脆弱性検出の普及活動」で培ったノウハウや知見を基に、「ファジングを活用すると、どんな効果が得られるか」、「実際にどのようにファジングを実践すればよいのか」などファジングを実践するために必要な知識をまとめました。

また、「ファジングを試してみたい」ときにオープンソースソフトウェアなどを活用してすぐにファジングを実践できるように、「ファジングツールの使い方」などを別冊「ファジング実践資料」にまとめました。

これらの手引きが活用され、ソフトウェア製品の開発ライフサイクルへのファジング導入につながり、ソフトウェア製品の脆弱性が減少することを期待します。（2012 年 3 月公開）

URL: http://www.ipa.go.jp/security/vuln/fuzzing.html

### (5) 脆弱性体験学習ツール AppGoat

IPA は、安全なアプリケーション開発技法を幅広く学習できる対話型ツール「AppGoat（アップゴート）」をウェブサイトで公開しています。このツールにより、学生から技術者まで様々なレベルの利用者が脆弱性の発見／検証の方法から対策までを実習形式で体系的に学習できます。

「AppGoat」は IPA が運営する脆弱性届出制度や各種研究会等の知見を集約し、学習教材と演習環境をセットにし、脆弱性の検証手法から原理、影響、対策までを演習しながら学習できる国内で初めての体験型学習ツールとして開発されました。「AppGoat」は、IPA やベクターのウェブサイトからダウンロードし、利用者自身の PC にインストールして利用できます。利用者は、学習テーマ毎に用意された演習問題を通して、埋め込まれた脆弱性の発見、プログラミング上の問題点の把握、対策手法などについて対話的に学習できます。

IPA では、このツールが企業や教育機関での技術教育やソフトウェア開発者の学習に活用され、安全なアプリケーション開発に役立てられることを期待しています。（2011 年 1 月公開）

URL: http://www.ipa.go.jp/security/vuln/appgoat/

### (6) TCP/IP に係る既知の脆弱性検証ツール

IPA は、TCP/IP 実装製品開発者向けに、「TCP/IP に係る既知の脆弱性検証ツール」を開発し、開発者に貸し出しています。このツールは、TCP/IP を実装したソフトウェアの脆弱性を体系的に検証し、新たに開発されるソフトウェアでの既知の脆弱性の“再発”を防止するためのツールです。2008 年 2 月より公開しています。

近年、携帯端末や情報家電、ゲーム機などに組込まれている TCP/IP ソフトウェアに関して多

数の脆弱性が公表されています。TCP/IP 実装製品開発者は本ツールを使用することで、自身が開発したソフトウェアにおいて既知の脆弱性を作り込んでいないかをチェックし、脆弱性対策に役立てることができます。

ツールは、「TCP/IP に係る既知の脆弱性に関する調査報告書 改訂第 5 版」に記載された 30 項目の脆弱性のうち、IPv4(Internet Protocol Version 4)環境で 19 項目、IPv6 環境で 14 項目の脆弱性を体系的に検証できます。

IPA では、2008 年 2 月から「TCP/IP に係る既知の脆弱性検証ツール」の貸出しを開始し、累計で約 120 件の利用実績があります。2010 年 11 月に公開された最新バージョンでは、近年普及が進み、今後脆弱性対策が一層重要となる IPv6 に対する検証機能の拡充と、使い勝手を向上するための機能追加を行いました。

このツールの利用を希望する製品開発者は IPA に申込めば利用できます。下記の URL のページを参照してお申込ください。

TCP/IP に係る既知の脆弱性検証ツール V5.0（2010 年 11 月）
URL: http://www.ipa.go.jp/security/vuln/vuln_TCPIP_Check.html
TCP/IP に係る既知の脆弱性に関する調査報告書 改訂第 5 版（2010 年 11 月）
URL: http://www.ipa.go.jp/security/vuln/vuln_TCPIP.html

### (7) SIP に係る既知の脆弱性検証ツール V2.0

IPA は、マルチメディアデータを端末間でリアルタイムに双方向通信するための標準的な通信開始手順である SIP（Session Initiation Protocol）に関して、「SIP に係る既知の脆弱性検証ツール」を開発し、SIP 実装製品の開発者向けに貸し出しています。このツールを利用することで SIP 実装製品開発者は出荷前に既知の脆弱性を作りこまないように確認することができます。

SIP は、マルチメディアデータを端末間でリアルタイムに双方向通信するための通信開始プロトコルとして、コンピュータをはじめ、情報家電や携帯端末などの組込み機器へも使用が広まっています。SIP を実装した製品については、これまで多くのソフトウェアの脆弱性が公表されており、機器ごとに対策が施されてきました。しかしながら SIP の脆弱性を体系的に検証するツールが整備されていなかったことから、新たに開発されるソフトウェアで、既に公表されている脆弱性の対策が実装されず、脆弱性が「再発」するケースが見受けられます。

そこで、IPA では、SIP 実装製品開発者向けに、SIP を実装したソフトウェアの脆弱性を体系的に検証し、新たに開発されるソフトウェアでの既知の脆弱性の“再発”を防止するためのツールとして「SIP に係る既知の脆弱性検証ツール」を開発しました。このツールは 2010 年 11 月に検証項目を拡充し V2.0 としており、「SIP に係る既知の脆弱性に関する調査報告書（改訂第 3 版）」に記載されている 22 項目の脆弱性のうち、11 項目（当該脆弱性項目を検証するために必要な 265 シナリオ）を体系的に検証できます。

IPA では 2009 年 4 月から本ツールを CD-ROM で貸し出しています。利用を希望される製品開発者は下記 URL のページを参照してお申込ください。

SIP に係る既知の脆弱性検証ツール V2.0

URL: http://www.ipa.go.jp/security/vuln/vuln_SIP_Check.html

SIP に係る既知の脆弱性に関する調査報告書 改訂第 3 版

URL: http://www.ipa.go.jp/security/vuln/vuln_SIP.html

### (8) ソースコードセキュリティ検査ツール

IPA は、C 言語で作成されたソースコードに脆弱性が存在しないかどうかを確認するツール「iCodeChecker」をウェブサイトで公開しています。このツールを利用することで、ソースコード診断を実際に体験しながら、ソースコード診断の活用イメージや脆弱性の対策方法を理解することができます。

「iCodeChecker」に、脆弱性を確認したいソースコードを読み込ませると、脆弱性の原因となるコードの箇所とその修正方法を解説するレポートを出力します。利用者は、「iCodeChecker」の利用を通して、脆弱性に関する理解やソースコードセキュリティ検査手法を用いた安全なソフトウェア開発についての理解を深めることができます。「iCodeChecker」は、VM イメージ、パッケージ形式、ソースコード形式の 3 つの配布形式があり、利用方法や利用環境に応じて、使い分けることができます。

IPA では、このツールが「ソースコードセキュリティ検査」の実用性・有効性を認識するための一助となり、実際の開発現場における開発プロセスへの「ソースコードセキュリティ検査」の導入が促進されることを期待します。

ソースコードセキュリティ検査ツール iCodeChecker(2012 年 8 月)

URL: http://www.ipa.go.jp/security/vuln/iCodeChecker/

## 7.4. 運用・利用

### 7.4.1. 「運用／利用」段階における脆弱性対策

本書でも多くのページで「運用／利用」段階における脆弱性対策について述べています。ライフサイクルの運用／利用の段階では、実際に使われている製品やウェブサイトについて最新の脆弱性情報が報告されます。製品開発者やウェブサイト運営者は、新たにみつかった脆弱性に対応する準備をしておく必要があります。

製品開発者は、報告を受けた脆弱性について評価分析を行い、必要であれば対応策（セキュリティ修正プログラムや回避策）を作り、脆弱性情報をセキュリティ勧告としてリリースします。

ウェブサイト運営者も、報告を受けた脆弱性について評価分析を行い、必要であればこれを修正します。個人情報が漏洩する等の大きな被害が想定される場合には、脆弱性を修正した旨を公表するべきです。

また、運用／利用の際に脆弱性が発見された場合、将来、同じような脆弱性が生じないように製品開発の担当者に報告をフィードバックすることも重要です。

ウェブサイトに対しては脆弱性をつく攻撃が行われます。攻撃と脆弱性について最新の情報をもとにツールで検出を行うことも重要です。

## 7.4.2. 「運用／利用」に関して入手可能なコンテンツ

### (1) ウェブサイト攻撃の検出ツール iLogScanner V3.0

ウェブサイトの脆弱性対策を促進するために、IPA ではウェブサイト攻撃検出ツール「iLogScanner」(アイ・ログ・スキャナ)を公開しています。

「iLogScanner」は利用者のウェブブラウザ上でウェブサーバのアクセスログの中からウェブサイトへの各種の攻撃を解析し、ウェブサイトの脆弱性を検出するツールです。ウェブサイト管理者は、このツールで自組織のウェブサイトがどれほどの攻撃を受けているかを把握できます。

ログ解析等により把握できる攻撃状況は、セキュリティ対策上の指針のひとつとなります。ウェブサイト管理者には本ツールを活用して日頃からログ分析の習慣をつけることをお奨めします。

このツールは 2008 年 4 月の公開以来、数度のバージョンアップを重ねて、検出可能な攻撃パターンの強化、対応プラットフォームの追加、使いやすさの向上などがはかられています。ツールは月平均 1,500 件以上ダウンロードされています。

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

### (2) Web Application Firewall 読本 改訂第 2 版

IPA では、ウェブサイト運営者が Web Application Firewall(ウェブ・アプリケーション・ファイアウォール、WAF)[94]を導入する際の参考となる解説資料「Web Application Firewall 読本」を公開しています。

「Web Application Firewall 読本」は、ウェブサイト運営者が WAF の導入を検討する際に、WAF に関する理解を手助けするための手引書です。この資料では、WAF の概要、機能の詳細、導入におけるポイント、海外組織・機関における WAF に関する取り組み等をまとめています。

Web Application Firewall(WAF)は、ウェブアプリケーションの脆弱性を悪用した攻撃などからウェブアプリケーションを保護するソフトウェア、またはハードウェアです。WAF は脆弱性を修正するといったウェブアプリケーションの実装面での根本的な対策ではなく、攻撃による影響を低減する対策となります。特にウェブサイトの脆弱性の修正作業が長期化する場合などに、WAF の導入による対策が取られます。WAF は、WAF を導入したウェブサイト運営者が設定する検出パターンに基づいて、ウェブサイトと利用者間の通信の中身を機械的に検査します。

WAF 読本は改訂を行い、WAF の導入事例を追加しました。(改訂第 2 版。2011 年 2 月公開)

URL: http://www.ipa.go.jp/security/vuln/waf.html

---

[94] ⇒ 本書用語集「WAF」

### (3) 安全なウェブサイト運営入門

今日、ウェブサイトを利用したショッピングなどが普及する一方、セキュリティ施策の不足により、ウェブサイトから利用者の個人情報などが漏えいし、犯罪に悪用される事件や事故が繰り返し発生しています。資金面などから情報セキュリティ専門の担当者や部門を持つことが難しい中小規模の組織など、セキュリティ施策が不十分な場合、ウェブサイトの脆弱性などを原因とする事件が発生しても適切に対処できない可能性があります。

IPA では、ウェブサイトの脆弱性による被害を中心とした、7 つのウェブサイト運営上の事件を体験的に学習できるソフトウェア「安全なウェブサイト運営入門—7 つの事件を体験し、ウェブサイトを守り抜け！—」を公開しています。

「安全なウェブサイト運営入門」では、ウェブサイトの脆弱性による被害を中心とした 7 つの具体的な事件を題材に、ロールプレイング形式で体験学習を行います。事件や事故が発生した場合の被害を理解し、事前対策の必要性を学ぶことができます。組織のウェブサイト運営者、情報システム担当者、セキュリティ担当者、また一般利用者等を対象としており、このコンテンツでの学習によって、情報セキュリティに関する意識、知識の底上げにつながります。(2008 年公開)

URL: http://www.ipa.go.jp/security/vuln/7incidents/

### (4) 5 分でできる！情報セキュリティポイント学習

一般に中小企業では経営資源が限られているため、大企業に比べて情報セキュリティ対策への取り組みが遅れがちになります。また、業種・従業員の構成が様々なことから求められる対策も多岐にわたります。

IPA ではこのような現状を踏まえ、各企業の現状に即した情報セキュリティ対策を学習できるツールとして、主に中小企業の方を対象にした情報セキュリティ学習ツール「5 分でできる！情報セキュリティポイント学習～事例で学ぶ中小企業のためのセキュリティ対策～」を公開しています。

職場の日常の 1 コマを取り入れた親しみやすい学習テーマで、セキュリティに関する様々な事例を疑似体験しながら正しい対処法を学ぶことができます。学習時間は 1 テーマあたり 5 分程度です。テーマは IPA で公開している「5 分でできる自社診断シート」の診断項目と連動しています。実務に生かせる学習内容とするため、物を作ることを主体とする企業(建設業・製造業等)と、物を売ることを主体とする企業(小売業・卸売業等)の 2 種類の分野別、経営者・管理者・一般社員の職位別に、合計 105 の学習テーマから構成されており、学習者と所属する組織の現状に合わせた学習が可能です。

本学習ツールは社内研修や自己学習などで活用されることを想定し、IPA のウェブサイトからダウンロードが可能です。日頃のセキュリティ対策の確認にご活用ください。(2009 年 10 月公開)

URL: http://www.ipa.go.jp/security/vuln/5mins_point/

### (5) 「新しいタイプの攻撃」の対策に向けた設計・運用ガイド 改訂第 2 版

昨今、石油関連企業や国際的金融機関、米国のインターネット関連企業やセキュリティ企業を標的とした攻撃が相次いで発生しています。ソフトウェアの脆弱性を悪用し、複数の既存攻撃を組

み合わせ、ソーシャルエンジニアリングにより特定企業や公的機関をねらい、対応が難しく執拗（しつよう）なサイバー攻撃を、IPA では「新しいタイプの攻撃」と呼んでいます。「新しいタイプの攻撃」は、「攻撃に気付けない」「バックドアが設置される」等の特徴があり、従来のセキュリティ対策では完全な防御が行えなくなっています。

昨今は、国内外の防衛産業や政府機関を狙った「新しいタイプの攻撃」の 1 種である標的型の諜報（ちょうほう）攻撃による事件が複数報道されています。これらの攻撃は機密情報の窃取が目的といわれており、攻撃対象となった業界および政府関係機関はもちろん、その他の業界や組織においても大きな脅威となってきています。

このような「新しいタイプの攻撃」の発生を受け、IPA では 2011 年 8 月に対策の手引きである「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド」を作成・公開しました。本ガイドでは、従来行われているウイルス対策ソフトや FireWall（ファイアウォール）等での対策では防御しきれない点や、コンピュータウイルスに感染したとしても組織の知的財産や個人情報などの重要情報を窃取される事態を避ける方法を重点的に記載しています。なお、本ガイドは IPA が主催する「脅威と対策研究会」にて取りまとめた資料になります。

また、その後に、攻撃仕様の分析、実証実験を交えた対策の検討を行い、「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド 改訂第 2 版」としてまとめ直しています。改訂第 2 版では、情報を外部に流出させない出口対策として、新たに 2 つの対策を追加し、合計 8 つの対策を解説しています。また、システム構築事業者やシステム管理者が適切な対応を行えるように、攻撃手法の分類と対応する対策方針を追加しています。（改訂第 2 版。2011 年 11 月公開）

URL: http://www.ipa.go.jp/security/vuln/newattack.html

### (6) 脆弱性対策情報ポータル JVN (Japan Vulnerability Notes)

JVN は、"Japan Vulnerability Notes" の略です。日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資することを目的とする脆弱性対策情報ポータルサイトです。製品開発者の脆弱性への対応状況を公開し、システムのセキュリティ対策を支援しています。

JPCERT コーディネーションセンターと独立行政法人情報処理推進機構 (IPA)が共同で運営しています。

JVN では、脆弱性関連情報（脆弱性とその存在を調べる方法、さらに脆弱性の悪用につながる情報）とそれに対する対策、製品開発者の対応状況を公開しています。JVN ではさまざまな脆弱性関連情報を収集し、原則として製品開発者との調整を通じて対策方法を準備したうえで、それらを分かりやすくまとめた形で掲載しています。製品開発者の対応状況には、脆弱性に該当する製品の有無、回避策（ワークアラウンド）や対策情報（パッチなど）も含まれます。

日本国内では、製品開発者や脆弱性情報発見者の協力のもと、JPCERT/CC と IPA が中心となり、脆弱性関連情報の受付と安全な流通を目的とした「情報セキュリティ早期警戒パートナーシップ」が 2004 年 7 月より運用されています。JVN では、この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報告され、JPCERT/CC が製品開発者との調整を行なった脆弱性関連情報お

よび協力関係を結んでいる米国 CERT/CC の Technical Cyber Security Alerts や Vulnerability Notes や、英国 CPNI の CPNI Vulnerability Advice を掲載しています。この他、一般に公開された脆弱性情報を独自に収集し、製品開発者との調整を行なって JVN に掲載しています。

URL: http://jvn.jp/

### (7) 脆弱性対策情報データベース (JVN iPedia)

今日、社会や経済の基盤は IT に依存しています。この基盤を安全に維持するには、自然災害やシステム障害に備えるだけでなく、コンピュータウイルスや不正アクセスなど、インターネットを介したサイバー攻撃への対策が必要です。最近でも、OS やウェブブラウザを中心に深刻な脆弱性が多数報告されており、ソフトウェアのアップデートなどの対策が不可欠です。

一方で従来、有効な対策をとりたくても脆弱性に関する日本語の情報は不十分でした。そこで IPA では JVN に掲載される情報などをもとに、国内向けソフトウェアの脆弱性関する概要や対策の情報を蓄積し、「JVN iPedia」(脆弱性対策情報データベース)として公開しています。2011 年 3 月時点で約 10,200 件の情報があり、データは日々増え続けています。

JVN iPedia では、この大量のデータから目的の脆弱性を探し出すための検査機能や RSS 配信機能を備えています。入手したい情報が特定されている場合には検索機能により効果的に探すことができます。RSS 配信機能の利用により定期的に脆弱性情報を取得することができます。さらに MyJVN 脆弱性対策情報収集ツールを利用することで、脆弱性の対策情報の収集が効率的になります。

また、昨今、製品のグローバル化により、国内製品に関する脆弱性対策情報は国内のみならず海外でも重要性が高まっています。IPA では JVN iPedia 英語版も公開しています。

URL: http://jvndb.jvn.jp/ (日本語版)、 http://jvndb.jvn.jp/en/ (英語版)

### (8) MyJVN 脆弱性対策情報収集ツール

最近では、各種サイトで多数の脆弱性対策情報が提供されていますが、情報セキュリティの専門家を持たない企業や組織にとって、必要な情報の収集は容易ではありません。そこで IPA では、JVN iPedia に登録された情報の中から利用者自身に関係する情報のみを効率的に収集できるようにしたツール「MyJVN 脆弱性対策情報収集ツール」を提供しています。

このツールは、フィルタリング条件設定機能、自動再検索機能、脆弱性対策チェックリスト機能等を持ち、自組織で利用しているソフトウェア製品を選択することにより、JVN iPedia から必要な脆弱性対策情報だけを効率よく入手できます。

URL: http://jvndb.jvn.jp/apis/myjvn/mjcheck.html

### (9) MyJVN バージョンチェッカ

近年、特定の企業や組織の社員に向け、関係者を装ってウイルス添付メールを送信する攻撃(標的型攻撃)や、有名な企業や組織のウェブサイトを改ざんし、ウェブブラウザや動画再生ソフト

などの脆弱性を狙う攻撃など、攻撃手法の多様化が進んでいます。これらの攻撃の多くは古いバージョンのソフトウェアの脆弱性を悪用しています。

そこで IPA では、PC にインストールされているソフトウェア製品が最新バージョンであるかを確認できるツール「MyJVN バージョンチェッカ」を開発し公開しています。マウスクリックだけの簡単な操作で複数の主要なソフトウェア製品のバージョンが最新であるかをチェックできます。また、対象ソフトウェア製品の更新情報を確認することもできます。(2009 年 11 月公開)

URL: http://jvndb.jvn.jp/apis/myjvn/vccheck.html

### (10) MyJVN セキュリティ設定チェッカ

最近、USB メモリの自動実行機能(オートラン機能)を悪用して感染範囲を拡大するコンピュータウイルスが増加しています。自動実行機能とは USB メモリを PC に接続した際に USB メモリ内のファイルを自動的に開く Windows OS の機能のことです。

このようなウイルス感染を防ぐ対策のひとつは、USB メモリの自動実行機能を無効にすることですが、無効化や確認の方法は一般利用者には分かり難いものです。

そこで IPA では、USB メモリの自動実行機能などの Windows のセキュリティ設定を簡単な操作で確認可能なツール「MyJVN セキュリティ設定チェッカ」を開発、公開しています。(2009 年 12 月公開)

URL: http://jvndb.jvn.jp/apis/myjvn/sccheck.html

## 7.5. 廃棄

### 7.5.1. 「廃棄」段階における脆弱性対策

ライフサイクルの廃棄段階で行える脆弱性対策はあまり多くありませんが、ソフトウエア製品の利用を中止する際に、システムに脆弱性を残さずにアンインストールすることが挙げられます。

# 8. あとがき

本書は、「情報システム等の脆弱性情報の取扱いに関する研究会」のこれまでの成果を中心に、情報システム等の脆弱性対策に関するコンテンツを集約・整理したものです。

一般に、情報セキュリティ全般もしくは特定の技術について、その全体像をカバーした文献は多数存在しますが、本書のようにソフトウエア製品の脆弱性に焦点を当てて、利用者の種別やライフサイクル、さらに海外動向・国際標準化動向などの観点から全般的にとりまとめた文献は多くはありません。これは、システムを運用している間は常に脆弱性対策に取り組まなければならないという意識が未だに利用者の間に十分に浸透していないことと無関係ではないでしょう。したがって、本書が、こうした状況に一石を投じ、利用者における脆弱性対策の取組みの一助になることを、強く期待しています。

また、本書に挙げた様々な論点には、関係者が情報セキュリティ早期警戒パートナーシップを立ち上げ、その運用を続ける中で、見えてきた部分も多くあります。それは、こうした活動が単なるルーティンワークに留まるのではなく、常に課題の認識と改善に務めてきた成果のひとつであり、今回、それらを改めて社会にフィードバックできる機会を得たことに改めて感謝いたします。

なお、現在、脆弱性管理を機械化・自動化することで脆弱性対策の負担を軽減し、パッチの適用漏れ等のミスを減らす取組みや、セキュア・プログラミングを導入して企画、設計・開発・製造の段階から脆弱性そのものを作りこまないようにする取組みも進展しています。これらの取組みを今後さらに高度化・一般化させることで、より安全で脆弱性対策の負担の少ない社会を実現できるよう、これからも努力していきたいと考えます。

# 用語集

**CGI（Common Gateway Interface）**

CGI とは、ウェブサーバが、ユーザから入力された要求を外部のプログラムに渡し、その実行結果をユーザのウェブブラウザに返す仕組みです。動的なウェブページの作成に利用されます。

**DMZ（Demilitarized Zone）**

DMZ とは、外部のネットワークと組織内のネットワークの中間に位置する緩衝地帯で”DeMilitarized Zone”（非武装地帯）の頭文字を取って DMZ と呼ばれます。インターネットからのアクセスを受けるウェブサーバ、メールサーバ、DNS サーバなどは通常この DMZ に置かれます。

**OS（Operating System）**

OS とは、コンピュータの基本的な働きに係るソフトウエア製品で、メモリやディスク等のハードウェア機器を抽象化してアプリケーションソフトウエアに提供する役割を果たします。「基本ソフト」とも呼ばれます。一般に OS というとウィンドウシステムやデータベース管理システムなどのミドルウェアや、設定ツールなどのユーティリティ、ウェブブラウザなどを含みます。

**SQL インジェクション**

データベースと連携したウェブアプリケーションの多くは、利用者からの入力情報をもとにデータベースへの命令文を組み立てている。この命令文の組み立て方法に問題があると、攻撃によってデータベースの不正利用をまねく可能性がある。この問題を悪用した攻撃手法を一般に「SQL インジェクション」と呼びます。SQL は、リレーショナルデータベース（RDB）において、データベースの操作やデータの定義を行うための問い合わせ言語です。

**WAF（Web Application Firewall）**

WAF とは、ウェブアプリケーションの脆弱性を悪用した攻撃などからウェブアプリケーションを保護するソフトウエア、またはハードウェアです。WAF は脆弱性を修正するといったウェブアプリケーションの実装面での根本的な対策ではなく、攻撃による影響を低減する対策です。

WAF は導入する際に設定する検出パターンに基づいて、ウェブサイトと利用者間の通信の中身を機械的に検査します。WAF の使用により脆弱性を悪用する攻撃を検出し、脆弱性を悪用する攻撃からウェブアプリケーションを防御する効果を期待できます。

**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。

**ウェブシステム**

ウェブシステム（ウェブアプリケーションサーバシステム）とは、Web（World Wide Web）をクライアントとサーバ間の接続手段に用いたサーバシステムのことを指します。利用者のブラウザに入力されたデータをウェブアプリケーションが受け取り、処理した結果を返してブラウザに表示します。

**開発フレームワーク**

開発フレームワークとは、アプリケーションを開発する場合に必要となる部品や、実装上の制約などを提供するもので、ソフトウェア開発における生産性や保守性の向上を目的としたものです。アプリケーションの骨組み部分が、よく洗練された形であらかじめ提供されるため、開発担当者のスキルへ依存する部分を減らすことができ、設計レベルの欠陥を最小限に止め、一定の成果物品質を維持することができます。

**基盤ソフトウエア**

基盤ソフトウェアとは、OS やミドルウェア等のコンピュータシステムにおいて基盤となるソフトウエアのことを指します。

**クロスサイト・スクリプティング**

クロスサイト・スクリプティングとは、ウェブサイトで実行されるスクリプトを用いた攻撃です。罠を仕掛けたサイトでユーザが不要意にリンクをクリックすると、別のサイトに強制的に飛ばされ、用意されたスクリプトが実行され被害に遭います。被害としては、Cookie が読み取られ、ユーザの個人情報が漏えいするなどがあります。

**コード検査**

コード検査とは、プログラムのバグを除く手段のひとつです。プログラム開発工程において、セキュリティを考慮した適切なコーディングが行われているか調査することで、より高いレベルのセキュリティを実現できます。手段としては人が目視でみつけるコードレビューの他に、コード検査ツールを用いる手段があります。コード検査ツールを用いると短時間で効率的に問題箇所を発見できます。

**コードレビュー**

コードレビューとは、開発者担当者が書いたコード（プログラムコード）を読んでセキュリティ脆弱性やそのきざしを読み取る作業を指します。コードレビューで発見された脆弱性については開発作業にフィードバックしてコードの修正を行います。

**コンピュータウイルス**

コンピュータウィルスとは、第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、 次の機能を一つ以上有するものです。

(1) 自己伝染機能

自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、 他のシステムに伝染する機能

(2) 潜伏機能

発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能

(3) 発病機能

プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能

**システム構築事業者**

システム構築事業者とは、システムの構築を行う SI 事業者のことを指します。本文では特にウェブサイトを構築するシステム構築事業者を「ウェブサイト構築事業者」と呼んでいます。

**脆弱性関連情報**

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や、コンピュータウイルス等が該当します。

**脆弱性修正プログラム**

脆弱性修正プログラムとは、セキュリティ上の問題点を除去するプログラムで、一般に「パッチ」または「フィックス」と呼ばれる。セキュリティパッチとよばれることもある。製品開発者は、脆弱性の発見に対して修正プログラムを提供する。利用者は、これらのファイルをコンピュータシステムにインストールする必要がある。

**脆弱性情報ハンドリング**

脆弱性情報ハンドリングとは、一般に公表される前のソフトウエアやハードウェア等におけるセキュリティ上の欠陥（脆弱性）に関する情報を、適切な方法で取り扱い、製品開発者によって用意された対策情報とともに公表することによって問題解決方法を広く示し、製品利用者における

安全の確保に貢献する活動のことです。

**セキュリティ検査**

セキュリティ検査とは、一般に、プログラム上のセキュリティ問題や設定上のセキュリティ問題の検査です。セキュリティ検査はシステムの構築段階や、納入の段階で行います。

**セキュリティポリシー**

セキュリティポリシーとは、企業や組織として一貫したセキュリティ対策を行うために、技術的対策だけでなく、利用・運用面、管理面、組織体制をも含めたセキュリティ方針と対策の基準を示したものです。通常は、基本方針、対策基準、実施手順の三層で構成されます。

**セキュリティ要件**

セキュリティ要件とは、情報システムにおいて情報セキュリティを確保するために満たすべき条件のことです。情報システムの調達仕様書に適切に組み込んで記載することが望まれます。
セキュリティ要件のベースライン（最低限のセキュリティ管理策）としては、組織のセキュリティポリシー等を用いることができます。

**セッション管理**

セッション管理とは、ウェブサイトが、一連の操作として複数のリクエストを行う利用者を一意に識別するための仕組みです。

**対策方法**

対策方法とは、脆弱性から生ずる生じ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。情報セキュリティ早期警戒パートナーシップにおいては「対策方法」とは「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、パッチ等と呼ばれます。

**パッチ**

「脆弱性修正プログラム」（p.119 参照）

**標的型攻撃**

標的型攻撃とは、主に電子メールを用いて特定の組織や個人を狙う攻撃です。攻撃対象の組織や個人に合わせてメールの内容がカスタマイズされているので、怪しいメールと区別がしにくい。また、不特定多数を攻撃対象としていないため、攻撃サンプルの入手が難しく、ウイルス対

策ソフトへの反映が困難になります。

**フィッシング詐欺**

フィッシング詐欺とは、巧妙な文面のメールなどを用い、実在する企業（金融機関、信販会社、ネットオークション等）のウェブサイトを装った偽のサイトにユーザを誘導し、機密情報（クレジットカード番号、ID、パスワードなど）を盗み取る不正行為のことです。

**不正アクセス**

不正アクセスとは、システムを利用する者が、その者に与えられた権限によって許された行為以外の行為をネットワークを介して意図的に行うことです。

**踏み台**

踏み台とは、不正アクセスを行う際の中継地点として他人のコンピュータを使用する不正行為です。例えば、ボットに感染すると、DoS 攻撃や DDoS 攻撃に利用されたり、スパムメールの発信に利用されることがあります。ゾンビ（zombie）と呼ばれる、踏み台に利用されたコンピュータは、所有者が気づかないうちに、攻撃に加担していることになります。

**ブラックボックステスト**

ブラックボックステストとは、一般的にプログラムの内部の作りや処理内容とは関係無く、外部からシステムの機能を検証する方法です。セキュリティに関して行うブラックボックステストでも、同様に外部との入出力（だけ）に着目してプログラムの動作を確認します。

**ペネトレーションテスト**

ペネトレーションテストとは、ネットワークの外部からネットワークに接続されたコンピュータシステムの内部へ実際に攻撃して侵入を試みるテストのことを言います。「侵入テスト」とも呼ばれます。ペネトレーションテストにより、コンピュータやネットワークの脆弱性を検証できます。典型的にはインターネット側から DMZ ネットワークに侵入するテストが行われます。ペネトレーションテストはブラックボックステストの一種です。

**ミドルウェア**

ミドルウェアは、コンピュータの基本ソフトウエアであるオペレーティングシステム（OS）と、各業務処理を行うアプリケーションソフトウエアとの中間に入るソフトウエアのことです。

**ワークアラウンド**

ワークアラウンドとは、脆弱性を回避する方法であり、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。

# 参考文献・URL 一覧

## ■「情報セキュリティ早期警戒パートナーシップ」に関する文献

●告示

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）

http://www.meti.go.jp/policy/netsecurity/downloadfiles/vulhandlingG.pdf

●ガイドライン

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

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

●ガイド・マニュアル等

JPCERT/CC 脆弱性関連情報取扱いガイドライン

http://www.jpcert.or.jp/vh/vul-guideline2010.pdf

社団法人電子情報技術産業協会（JEITA）、社団法人情報サービス産業協会（JISA），“製品開発ベンダーにおける脆弱性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”，2004 年 10 月

http://it.jeita.or.jp/infosys/info/0407JEITA-guideline/index.html

社団法人コンピュータソフトウェア協会（CSAJ）（旧・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），“製品開発ベンダーにおける脆弱性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”，2004 年 12 月

http://www.csaj.jp/info/04/20041203_security.html

社団法人電子情報技術産業協会（JEITA）、社団法人情報サービス産業協会（JISA），“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”、2005 年 8 月

http://www.jisa.or.jp/report/2004/vulhandling_guide.pdf

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

http://www.ipa.go.jp/security/ciadr/vuln_announce_manual.pdf

ウェブサイト運営者のための脆弱性対応ガイド

http://www.ipa.go.jp/security/ciadr/vuln_website_guide.pdf

ウェブサイト構築事業者のための脆弱性対応ガイド
http://www.ipa.go.jp/security/ciadr/vuln_sier_guide.pdf

セキュリティ担当者のための脆弱性対応ガイド
http://www.ipa.go.jp/security/ciadr/guide4vuln.pdf

パンフレット「情報システムの安全を維持していただくために」
http://www.ipa.go.jp/security/ciadr/vuln_taisaku.pdf

■「情報システム等の脆弱性情報の取扱いに関する研究会」の報告書・成果物

●2004 年公開
情報システム等の脆弱性情報の取扱いに関する研究会 報告書
http://www.ipa.go.jp/security/fy15/reports/vuln_handling/index.html
情報システム等の脆弱性情報の取扱いにおける法律面の調査
http://www.ipa.go.jp/security/fy15/reports/vuln_law/index.html

●2005 年公開
情報システム等の脆弱性情報の取扱に関する研究会 報告書（概要版）
http://www.ipa.go.jp/security/fy16/reports/vuln_handling/index.html

●2006 年公開
情報システム等の脆弱性情報の取扱いに関する研究会 報告書
http://www.ipa.go.jp/security/fy17/reports/vuln_handling/index.html
報告書 本編
http://www.ipa.go.jp/security/fy17/reports/vuln_handling/documents/0_honpen.pdf
別紙 1：研究会及びワーキンググループ名簿
http://www.ipa.go.jp/security/fy17/reports/vuln_handling/documents/1_meibo.pdf
別紙 2：組込みソフトウェアを用いた機器におけるセキュリティ
http://www.ipa.go.jp/security/fy17/reports/vuln_handling/documents/2_kiki.pdf
別紙 3：組込みソフトウェアのセキュリティ ～機器の開発等における 40 のポイント～
http://www.ipa.go.jp/security/fy17/reports/vuln_handling/documents/3_software.pdf
別紙 4：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
http://www.ipa.go.jp/security/fy17/reports/vuln_handling/documents/4_guideline.pdf
別紙 5：JVN で公表された脆弱性の内容
http://www.ipa.go.jp/security/fy17/reports/vuln_handling/documents/5_jvn.pdf

●2007 年公開

情報システム等の脆弱性情報の取扱いに関する研究会 報告書

http://www.ipa.go.jp/security/fy18/reports/vuln_handling/index.html

報告書 本編

http://www.ipa.go.jp/security/fy18/reports/vuln_handling/0_honpen.pdf

別紙 1:情報システム等の脆弱性情報の取扱いに関する研究会 名簿

http://www.ipa.go.jp/security/fy18/reports/vuln_handling/1_meibo.pdf

別紙 2:情報セキュリティ早期警戒パートナーシップガイドライン改訂案

http://www.ipa.go.jp/security/fy18/reports/vuln_handling/2_guideline.pdf

別紙 3:2006 年に JVN で公表された脆弱性

http://www.ipa.go.jp/security/fy18/reports/vuln_handling/3_jvn.pdf

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

http://www.ipa.go.jp/security/ciadr/vuln_announce_manual.pdf

●2008 年公開

情報システム等の脆弱性情報の取扱いに関する研究会 報告書

http://www.ipa.go.jp/security/fy19/reports/vuln_handling/index.html

報告書 本編

http://www.ipa.go.jp/security/fy19/reports/vuln_handling/0_honpen.pdf

別紙 1:情報システム等の脆弱性情報の取扱いに関する研究会 名簿

http://www.ipa.go.jp/security/fy19/reports/vuln_handling/1_meibo.pdf

別紙 2:情報セキュリティ早期警戒パートナーシップガイドライン改訂案

http://www.ipa.go.jp/security/fy19/reports/vuln_handling/2_guideline.pdf

ウェブサイト運営者のための脆弱性対応ガイド

http://www.ipa.go.jp/security/ciadr/vuln_website_guide.pdf

●2009 年公開

情報システム等の脆弱性情報の取扱いに関する研究会 報告書

http://www.ipa.go.jp/security/fy20/reports/vuln_handling/index.html

報告書 本編

http://www.ipa.go.jp/security/fy20/reports/vuln_handling/0_honpen.pdf

別紙 1:情報システム等の脆弱性情報の取扱いに関する研究会 名簿

http://www.ipa.go.jp/security/fy20/reports/vuln_handling/1_meibo.pdf

別紙 2:情報セキュリティ早期警戒パートナーシップガイドライン改訂案

http://www.ipa.go.jp/security/fy20/reports/vuln_handling/2_guideline.pdf

パンフレット「情報システムの安全を維持していただくために」

http://www.ipa.go.jp/security/ciadr/vuln_taisaku.pdf

ウェブサイト構築事業者のための脆弱性対応ガイド

http://www.ipa.go.jp/security/ciadr/vuln_sier_guide.pdf

●2011 年公開

情報システム等の脆弱性情報の取扱いに関する研究会 報告書

http://www.ipa.go.jp/security/fy22/reports/vuln_handling/index.html

報告書 本編

http://www.ipa.go.jp/security/fy22/reports/vuln_handling/0_honpen.pdf

別紙 1:情報システム等の脆弱性情報の取扱いに関する研究会 名簿

http://www.ipa.go.jp/security/fy22/reports/vuln_handling/1_meibo.pdf

別紙 2:情報セキュリティ早期警戒パートナーシップガイドライン改訂案

http://www.ipa.go.jp/security/fy22/reports/vuln_handling/2_guideline.pdf

セキュリティ担当者のための脆弱性対応ガイド

http://www.ipa.go.jp/security/ciadr/guide4vuln.pdf

企業等における脆弱性対策に関する実態調査報告書

http://www.ipa.go.jp/security/ciadr/vuln_report2010.pdf

組込みソフトウェアを用いた機器におけるセキュリティ(改訂版)

http://www.ipa.go.jp/security/ciadr/kiki2.pdf

■組込みシステムセキュリティに関する文献

組込みシステムのセキュリティへの取り組みガイド(2010 年改訂版)

http://www.ipa.go.jp/security/fy22/reports/emb_app2010/

自動車と情報家電の組込みシステムのセキュリティに関する調査報告書(2008 年度)

http://www.ipa.go.jp/security/fy20/reports/embedded/

複数の組込み機器の組み合わせに関するセキュリティ調査報告書(2007 年度)

http://www.ipa.go.jp/security/fy19/reports/embedded/

組込みシステムの脅威と対策に関するセキュリティ技術マップの調査報告書(2006 年度)

http://www.ipa.go.jp/security/fy18/reports/embedded/

# 付録Ａ：2011 年度 情報システム等の脆弱性情報の取扱いに関する研究会 参加者名簿

座長

土居 範久 中央大学

委員

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

（五十音順、敬称略）

オブザーバ

江口 純一 経済産業省 情報セキュリティ政策室長
乃田 昌幸 経済産業省 情報セキュリティ政策室 課長補佐
枝川 慶彦 経済産業省 情報セキュリティ政策室 総括係長
鈴木 啓紹 社団法人コンピュータソフトウェア協会（CSAJ）
渕　眞 澄 社団法人日本情報システム・ユーザー協会（JUAS）
安田 直義 NPO 日本ネットワークセキュリティ協会（JNSA）
宮地 利雄 一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）
古田 洋久 一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）
佐藤 祐輔 一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）
高橋 紀子 一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）

（順不同、敬称略）

独立行政法人情報処理推進機構

藤江 一正 理事長
仲田 雄作 理事

事務局

笹岡 賢二郎 独立行政法人情報処理推進機構
湯原 孝志 独立行政法人情報処理推進機構
小林 偉昭 独立行政法人情報処理推進機構
金野 千里 独立行政法人情報処理推進機構
中 野　学 独立行政法人情報処理推進機構
寺田 真敏 独立行政法人情報処理推進機構
渡辺 貴仁 独立行政法人情報処理推進機構
板橋 博之 独立行政法人情報処理推進機構
相馬 基邦 独立行政法人情報処理推進機構
木曽田 優 独立行政法人情報処理推進機構
大森 雅司 独立行政法人情報処理推進機構
村瀬 一郎 株式会社三菱総合研究所
川口 修司 株式会社三菱総合研究所
井上 信吾 株式会社三菱総合研究所
松崎 和賢 株式会社三菱総合研究所

（順不同、敬称略）

以上

# 付録Ｂ：ソフトウエア等脆弱性関連情報取扱基準

○経済産業省告示第二百三十五号

ソフトウエア等脆弱性関連情報取扱基準を次のように定めたので、告示する。

平成十六年七月七日

経済産業大臣　中川　昭一

ソフトウエア等脆弱性関連情報取扱基準

Ⅰ. 主旨

本基準は、ソフトウエア等に係る脆弱性関連情報等の取扱いにおいて関係者に推奨する行為を定めることにより、脆弱性関連情報の適切な流通及び対策の促進を図り、コンピュータウイルス、コンピュータ不正アクセス等によって不特定多数の者に対して引き起こされる被害を予防し、もって高度情報通信ネットワークの安全性の確保に資することを目的とする。

Ⅱ. 用語の定義

本基準で用いられる用語の定義は、以下のとおりとする。

1. 脆弱性

ソフトウエア等において、コンピュータウイルス、コンピュータ不正アクセ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安全性上の問題箇所。ウェブアプリケーションにあっては、ウェブサイト運営者がアクセス制御機能により保護すべき情報等に誰もがアクセスできるような、安全性が欠如している状態を含む。

2. 脆弱性関連情報

脆弱性に関する情報であって、以下に掲げる類型のいずれかに該当するもの。

（1）脆弱性情報

脆弱性の性質及び特徴を示す情報。

（2）検証方法

脆弱性が存在することを調べる方法。

（3）攻撃方法

脆弱性を悪用するプログラム、コマンド又はデータ及びそれらの使用方法。

3. 対策方法

脆弱性によって生じる問題を解決又は回避するための方法であって、以下に掲げる類型のいずれかに該当するもの。

（1）回避方法

脆弱性を修正することなく、それが原因となって生じる被害を回避するための方法。

（2）修正方法

脆弱性を修正する方法。

4. ソフトウエア製品

ソフトウエア又はそれを組み込んだハードウエアであって、汎用性を有する製品。

5. ウェブアプリケーション

インターネット上のウェブサイトで稼働する固有のシステム。

6. コンピュータウイルス

コンピュータウイルス対策基準（平成7年通商産業省告示第429号）における「コンピュータウイルス」をいう。

7. コンピュータ不正アクセス

不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）における「不正アクセス行為」をいう。

Ⅲ. 本基準における関係者の定義

本基準における関係者の定義は、以下のとおりとする。

1. 発見者

脆弱性関連情報を発見又は取得した者。

2. 受付機関

発見者が脆弱性関連情報を届け出るための機関。

3. 調整機関

脆弱性関連情報に関して、製品開発者への連絡及び公表等に係る調整を行う機関。

4. 製品開発者

ソフトウエア製品の開発等を行う者であって、以下のいずれかに該当する者。

（1）ソフトウエア製品を開発した者。

（2）（1）に掲げる者のほか、ソフトウエア製品の開発、加工、輸入又は販売に関する形態その他の事情からみて、当該ソフトウエア製品の実質的な開発者と認められる者。

5. ウェブサイト運営者

ウェブサイトを運営する者。

Ⅳ. 本基準の適用範囲

本基準は、以下に掲げるものの脆弱性であって、その脆弱性に起因する被害が不特定多数の者に影響を及ぼし得るものに適用する。

1. 日本国内で利用されているソフトウエア製品

（ソフトウエア製品において通信プロトコル等の仕様を実装した部分を含む。）

2. 主に日本国内からのアクセスが想定されているウェブサイトで稼働するウェブアプリケーション

Ⅴ. 対象がソフトウエア製品である場合の脆弱性関連情報取扱基準

一. 発見者が製品開発者ではない、又は、発見者が製品開発者であり発見若しくは取得した脆弱性関連情報の影響範囲が自社のソフトウエア製品に限らない場合

対象がソフトウエア製品であり、かつ、発見者が製品開発者ではない、又は、発見者が製品開発者であり発見若しくは取得した脆弱性関連情報の影響範囲が自社のソフトウエア製品に限らない場合における脆弱性関連情報の取扱いの流れを以下に示す。

（ⅰ）発見者は、脆弱性関連情報を受付機関に届け出る。

（ⅱ）受付機関は、届出を受理した場合、一定の場合を除き、調整機関に当該脆弱性関連情報を通知する。

（ⅲ）調整機関は、受付機関から通知された脆弱性関連情報を、製品開発者に速やかに通知するとともに、当該製品開発者が開発等を行ったソフトウエア製品における当該脆弱性の有無及びその新規性の検証結果について、当該製品開発者に報告を求める。

（ⅳ）調整機関は、当該脆弱性情報の公表日を定める。

（ｖ）当該製品開発者は、当該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。

（vi）受付機関及び調整機関は、当該脆弱性情報の公表日に、当該脆弱性情報、その日までに得られた製品開発者による当該脆弱性の有無及びその新規性の検証結果並びに当該脆弱性に関する対策方法、取組みの状況等を含む対応状況について、インターネット等を通じて公表する。

関係者における詳細な行動基準を以下に定める。

1．発見者基準

（1）発見者（自ら開発等を行ったソフトウエア製品に影響範囲が限られると認められる脆弱性関連情報を発見又は取得した製品開発者を除く。）は、発見又は取得した脆弱性関連情報を経済産業大臣が別に指定する受付機関に届け出ること。ただし、当該製品開発者に対し同じ内容を届け出ることを妨げない。

（2）発見者は、以下の点を明示した上で脆弱性関連情報を届け出ること。

①発見者の氏名、連絡先等の情報及びその取扱い

②脆弱性を有する製品の名称等

③当該脆弱性関連情報

（3）違法な方法により脆弱性関連情報を発見又は取得しないこと。

（4）発見者は、当該脆弱性情報が受付機関及び調整機関から公表されるまでの間、当該脆弱性関連情報を第三者に漏えいしないよう適切に管理すること。ただし、当該脆弱性関連情報を正当な理由により第三者に開示する場合、あらかじめ受付機関に問い合わせをすること。

2．受付機関基準

（1）受付機関は、1．（1）による届出が1．（2）で定めた届出事項を満たしているか否かを判断し、満たすと判断した場合、これを受理したものとし、当該発見者に対しその旨を速やかに通知すること。また、届出を不受理とした場合、当該発見者に対しその旨及びその理由を速やかに通知すること。

（2）受付機関は、届出を受理したときは、速やかに、経済産業大臣が別に指定する調整機関に対し当該脆弱性関連情報を通知すること。ただし、当該脆弱性関連情報が以下に該当すると認められる場合、当該届出に係る処理を取りやめることができる。この場合においては、当該発見者にその旨及びその理由を通知すること。

①受付機関が既知の脆弱性関連情報であると確認した場合

②受付機関が調整機関から既知の脆弱性関連情報である旨の通知を受けた場合

③受付機関が脆弱性関連情報に該当しないと確認した場合

④受付機関が調整機関から脆弱性関連情報に該当しない旨の通知を受けた場合

⑤受付機関が違法な方法により発見又は取得されたおそれがあると認めた場合

（3）受付機関は、届出を受理した後においても、対策上必要と認められる場合、当該脆弱性関連情報について、当該発見者に問い合わせをすること。また、発見者からの問い合わせに対しては、調整機関と協議した上で、適切な情報を提供すること。その際、発見

者の本人確認に留意すること。

（4）受付機関は、氏名、連絡先等の発見者を特定し得る情報を適切に管理し、当該発見者の同意がない場合は他者（調整機関及び製品開発者を含む。）に開示しないこと。

（5）受付機関は、当該脆弱性情報が公表されるまでの間、当該脆弱性関連情報を第三者に漏えいしないよう適切に管理すること。ただし、対策上必要と認められる場合、当該脆弱性関連情報の適切な管理を前提として、第三者に分析を依頼することができる。

（6）受付機関は、対策方法が作成されてからそれが公表されるまでの間であって、当該脆弱性関連情報が、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重大な影響を与えるおそれがあると認められる場合、調整機関及び当該製品開発者と協議をした上で、政府機関等に当該脆弱性関連情報及び対策方法をあらかじめ通知することができる。その際、当該発見者に対して、その旨を事前に通知すること。

（7）受付機関は、調整機関が当該脆弱性情報を公表した場合には、その公表時期に合わせて当該脆弱性情報及び調整機関から当該脆弱性情報の通知を受けた製品開発者から報告された当該製品開発者の当該脆弱性に関する対策方法、取組みの状況等を含む対応状況（以下「対応状況」という。）を公表するとともに、当該発見者に対しその旨を通知すること。

（8）受付機関は、脆弱性に起因する被害の予防に資するため、脆弱性関連情報の届出状況等を公表すること。

3．調整機関基準

（1）調整機関は、脆弱性関連情報を製品開発者に適切に通知するために必要な製品開発者の名簿（以下「名簿」という。）を作成すること。その際、製品開発者と調整の上、当該製品開発者が調整機関との連絡をとるために設置した窓口を名簿に記載すること。

（2）調整機関は、受付機関から脆弱性関連情報の通知を受けた場合には、その内容に照らして当該脆弱性関連情報を通知すべき製品開発者を名簿から特定し、速やかに通知するとともに、当該製品開発者に対し、当該製品開発者のソフトウエア製品における当該脆弱性の有無及びその新規性を検証（以下「脆弱性検証」という。）しその結果を報告するよう求めること。また、名簿に記載のない製品開発者の中から新たに通知すべき者を特定した場合には、それを名簿に加えた上で、同様に通知を行い、脆弱性検証の結果を報告するよう求めること。

（3）調整機関は、製品開発者から脆弱性検証の結果報告を聴取し、その結果を踏まえつつ、対策方法の作成及び海外の調整機関との調整に要する期間、当該脆弱性情報の流出するリスク等の要素を考慮した上で、当該脆弱性情報を公表すべき日（以下「脆弱性情報公表日」という。）を定めるとともに、当該脆弱性情報公表日を受付機関及び当該製品開発者に通知すること。また、通知を行ったいずれの製品開発者からも脆弱性検証の結果報告が得られなかった場合には、国内外における脆弱性情報の取扱事例、海外の調整機関との調整に要する期間、当該脆弱性情報の流出するリスク等の要素を考慮した上で、脆弱性情報公表日を独自に定め、同様に、受付機関及び当該製品開発者に通知すること。

（4）調整機関は、製品開発者から脆弱性情報公表日を変更したい旨の申し出を受けた場合、当該製品開発者から意見を聴取した上で、当該脆弱性情報公表日を変更することができる。脆弱性情報公表日を変更した場合、新たに定めた脆弱性情報公表日を受付機関及び当該脆弱性情報に関して通知を行った製品開発者に対し通知すること。

（5）調整機関は、通知を行った製品開発者に対して、脆弱性情報公表日までに当該製品開発者の対応状況を報告するよう求めること。

（6）調整機関は、脆弱性情報公表日に、当該脆弱性情報並びにその日までに得られた製品開発者による脆弱性検証の結果及び対応状況について、インターネット等を通じて公表すること。なお、通知を行った製品開発者が調整機関に脆弱性検証の結果及び対応状況のいずれか又は双方を報告しない場合、当該製品開発者の名称とともに、それらについて報告がない旨を公表することができる。

（7）調整機関は、脆弱性情報公表日までに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旨の通知を受けた場合、その公表を取りやめることができる。公表を取りやめた場合、受付機関にその旨を通知すること。

（8）調整機関は、脆弱性情報公表日までに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旨の脆弱性検証の結果報告を受けた場合、受付機関から通知された情報は脆弱性関連情報には該当しないものと判断し、その公表を取りやめることができる。公表を取りやめた場合、受付機関にその旨を通知すること。

（9）調整機関は、脆弱性情報公表日までの間、当該脆弱性関連情報を第三者に漏えいしないよう適切に管理すること。ただし、対策上必要と認められる場合、当該脆弱性関連情報の適切な管理を前提として、第三者に分析を依頼し又は通知することができる。

4. 製品開発者基準

（1）製品開発者は、調整機関と調整の上、調整機関と連絡をとるための窓口を設置し、調整機関に通知すること。

（2）製品開発者は、調整機関から通知された脆弱性関連情報に関して、遅滞なく脆弱性検証を行い、その結果を調整機関に報告すること。

（3）製品開発者は、当該脆弱性が他社のソフトウエア製品に含まれることが推定される場合には、その旨及びその理由を調整機関に通知すること。

（4）製品開発者は、脆弱性情報公表日までの間、当該脆弱性関連情報を第三者に漏えいしないよう適切に管理すること。

（5）製品開発者は、脆弱性情報公表日までに、対応状況を受付機関及び調整機関に報告するとともに、対策方法を作成するよう努めること。

（6）製品開発者は、対策方法を作成した場合、受付機関及び調整機関に報告し、脆弱性情報公表日以降、自らもそれを利用者に周知すること。

二. 発見者が製品開発者であり、発見又は取得した脆弱性関連情報の影響範囲が自社のソフトウエア製品に限られる場合

対象がソフトウエア製品であり、かつ、発見者が製品開発者であり、発見又は取得した脆弱性関連情報の影響範囲が自社のソフトウエア製品に限られる場合における関係

者の行動基準を以下に定める。

（1）製品開発者は、自ら開発等を行ったソフトウエア製品に影響が限られると認められる脆弱性関連情報を発見又は取得した場合、対策方法を作成し、当該脆弱性関連情報及び対策方法を受付機関及び調整機関に通知すること。

（2）受付機関及び調整機関は、（1）による通知を受けたときは、当該脆弱性情報及び対策方法をインターネット等を通じて公表すること。ただし、調整機関はそれらを公表すべき日について、当該製品開発者から意見を聴取した上で定めること。

Ⅵ. 対象がウェブアプリケーションである場合の脆弱性関連情報取扱基準

対象がウェブアプリケーションである場合における脆弱性関連情報の取扱いの流れを以下に示す。

（ⅰ）発見者は、脆弱性関連情報を受付機関に届け出る。

（ⅱ）受付機関は、届出を受理した場合、一定の場合を除き、当該ウェブサイト運営者に当該脆弱性関連情報を通知する。

（ⅲ）当該ウェブサイト運営者は、受付機関から通知された脆弱性関連情報を検証し、必要に応じて当該脆弱性を修正する。

関係者における詳細な行動基準を以下に定める。

1. 発見者基準

（1）発見者（自ら運営するウェブサイトのウェブアプリケーションについての脆弱性関連情報を発見又は取得したウェブサイト運営者を除く。）は、発見又は取得した脆弱性関連情報を経済産業大臣が別に指定する受付機関に届け出ること。ただし、当該ウェブサイト運営者に対し同じ内容を届け出ることを妨げない。

（2）発見者は、以下の点を明示した上で脆弱性関連情報を届け出ること。

①発見者の氏名、連絡先等の情報及びその取扱い

②脆弱性を有するウェブアプリケーションを稼働しているウェブサイトの名称等

③当該脆弱性関連情報

（3）違法な方法により脆弱性関連情報を発見又は取得しないこと。

（4）発見者は、当該脆弱性が修正されるまでの間、当該脆弱性関連情報を第三者に漏えいしないよう適切に管理すること。ただし、当該脆弱性関連情報を正当な理由により第三者に開示する場合、あらかじめ受付機関に問い合わせをすること。

2. 受付機関基準

（1）受付機関は、1.（1）による届出が1.（2）で定めた届出事項を満たしているか否かを判断し、満たすと判断した場合、これを受理したものとし、当該発見者に対しその旨を速やかに通知すること。また、届出を不受理とした場合、当該発見者に対しその旨及びその理由を速やかに通知すること。

（2）受付機関は、届出を受理したときは、速やかに、当該ウェブサイト運営者に対し当該脆弱性関連情報を通知すること。ただし、当該脆弱性関連情報が以下に該当する場合、当該届出に係る処理を取りやめることができる。この場合においては、当該発見者にその旨及びその理由を通知すること。

①受付機関が既知の脆弱性関連情報であると確認した場合
②受付機関がウェブサイト運営者から既知の脆弱性である旨の通知を受けた場合
③受付機関が脆弱性関連情報に該当しないと確認した場合
④受付機関がウェブサイト運営者から脆弱性関連情報に該当しない旨の通知を受けた場合
⑤受付機関が違法な方法により発見又は取得されたおそれがあると認めた場合

（3）受付機関は、届出を受理した後においても、対策上必要と認められる場合、当該脆弱性関連情報について、当該発見者に問い合わせをすること。また、発見者からの問い合わせに対しては、当該ウェブサイト運営者と協議し、適切な情報を提供すること。その際、発見者の本人確認に留意すること。

（4）受付機関は、氏名、連絡先等の発見者を特定し得る情報を適切に管理し、当該発見者の同意がない場合は他者（ウェブサイト運営者を含む。）に開示しないこと。

（5）受付機関は、当該脆弱性関連情報を第三者に漏えいしないよう適切に管理すること。ただし、対策上必要と認められる場合、当該脆弱性関連情報の適切な管理を前提として、第三者にその分析を依頼することができる。

（6）受付機関は、当該ウェブサイト運営者から当該脆弱性を修正した旨の通知があったときは、それを速やかに発見者に通知すること。

（7）受付機関は、脆弱性に起因する被害の予防に資するため、脆弱性関連情報の届出状況等を公表すること。

3．ウェブサイト運営者基準

（1）ウェブサイト運営者は、受付機関から通知された脆弱性関連情報に関して、その内容を検証し、必要に応じて当該脆弱性を修正すること。

（2）ウェブサイト運営者は、当該脆弱性関連情報に関して検証した結果又は当該脆弱性を修正した旨を速やかに受付機関に通知すること。

（3）ウェブサイト運営者は、当該脆弱性が修正されるまでの間、当該脆弱性関連情報を第三者に漏えいしないよう適切に管理すること。

（4）ウェブサイト運営者は、当該脆弱性に起因する個人情報の漏えい等の事案が発生した場合、二次被害の防止、類似事案の発生回避等の観点から、可能な限り事実関係等を公表するなど必要な対策をとること。

附則

この基準は、平成16年7月8日から、施行する。

○経済産業省告示第二百三十六号

平成十六年経済産業省告示第二百三十五号により公示したソフトウエア等脆弱性関連情報取扱基準に基づき、経済産業大臣が別に指定する受付機関及び経済産業大臣が別に指定する調整機関を次のように定めたので、告示する。

平成十六年七月七日

経済産業大臣　中川　昭一

一、経済産業大臣が別に指定する受付機関について

1. 名称　　独立行政法人情報処理推進機構

2. 主たる所在地　東京都文京区本駒込二丁目二十八番八号

二、経済産業大臣が別に指定する調整機関について

1. 名称　　有限責任中間法人ＪＰＣＥＲＴコーディネーションセンター

2. 主たる所在地　東京都千代田区神田錦町三丁目十七番地

# 脆弱性ハンドブック

2013 年 3 月 15 日 発行

**企画・著作・制作・発行**　独立行政法人情報処理推進機構（IPA）
〒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
URL　https://www.ipa.go.jp/
電話　03-5978-7527
E-Mail　vuln-inq@ipa.go.jp

# 脆弱性ハンドブック