



INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

## 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

～ 脆弱性関連情報流通の枠組み構築に係る提言 ～

2004年3月

独立行政法人 情報処理推進機構



# 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 概要

## ～ 脆弱性関連情報流通の枠組み構築に係る提言 ～

近年、ソフトウェアを中心とする情報システム等の脆弱性がコンピュータ不正アクセスやコンピュータウイルス等の攻撃に悪用され、不特定多数のユーザに被害が及ぶケースが増えている。そこで、政府による「情報セキュリティ総合戦略」(平成15年10月発表)の提言に沿って、脆弱性と闘うIT業界の取り組みがより円滑かつ効果的に進むよう、国がそれを補完し支援する官民連携のしくみを構築し、ITユーザの被害発生を阻止することをめざす。

## 1. 背景

### 1.1. 問題意識

ソフトウェアを中心とする情報システム等の脆弱性<sup>1</sup>は、ソフトウェアの設計・開発段階に内包される潜在的問題であり、近年、コンピュータ不正アクセスやコンピュータウイルス等の攻撃に悪用されるケースが増加。

本来、関係者内で適切に共有され対策が策定されるべき脆弱性の情報が、適切に扱われず放置されたり、対策がない段階で暴露されることにより、大きな被害をもたらす危険性。さらに、脆弱性の公表から攻撃方法の出現までの期間が短縮。

我が国の問題は、脆弱性の公表に関する調整が不十分であること、情報システム等の脆弱性に関する研究・発見・対策策定は海外に依存しており日本のソフトウェアは脆弱性検証が不十分であること、ウェブアプリケーションの脆弱性は対処が進みにくいことが挙げられる。

### 1.2. 官民の取り組みの現状

経済産業省では、「コンピュータウイルス・不正アクセス届出事業」や「インターネット定点観測事業」を実施し、被害局限化を進めてきた。

しかし、情報システム等の脆弱性が狙われ、被害拡大がスピードはユーザが対処可能なレベルを遙かに超える勢いで早まりつつあること、IT業界の自律的な改善が進みにくいことから、今後は、IT業界の対策策定の取り組みがより円滑かつ効果的に進むよう、政府がそれを補完し支援していくことが必要。

<sup>1</sup> ソフトウェア等において、コンピュータ不正アクセス、コンピュータウイルス等の攻撃によりその機能や性能を損なう原因となり得る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

JPCERT コーディネーションセンター（以下 JPCERT/CC）は、海外関連機関の日本窓口として機能しており、送られてきた公表前の脆弱性の情報を国内の製品開発者に提供し、脆弱性情報の公表日の国際間調整を行う活動に着手。ただし、情報提供先の数は小規模にとどまっている。

## 2. 脆弱性関連情報流通の基本枠組み

### 2.1. 検討の前提

慎重に扱うべき脆弱性関連情報（脆弱性、検証方法、攻撃方法）と、周知徹底すべき対策方法（回避方法、修正方法）は分けて取り扱うのが適当。

脆弱性が不特定多数のユーザに発見される可能性があり、発見された場合の影響が不特定多数のユーザに及ぶことから、ソフトウェア製品<sup>2</sup>やウェブアプリケーションの脆弱性を主な対象とするのが適当。

ソフトウェア製品の脆弱性の場合、発見者と海外 CSIRT<sup>3</sup>が脆弱性関連情報の提供元。ウェブアプリケーションの脆弱性の場合、発見者が脆弱性関連情報の提供元。

ソフトウェア製品の脆弱性の場合、対策方法を策定するのは、そのソフトウェア製品を開発した製品開発者が適当。ウェブアプリケーションの脆弱性の場合、対策を適用するのは、そのウェブサイトについて対外的に責任を有するウェブサイト運営者が適当。

脆弱性関連情報の取り扱いに際しては、政府・重要インフラへの優先情報提供の可能性を検討すべき。ただし、そのモデルは本来機密に扱うべき脆弱性関連情報の漏洩リスクを高めてしまう点にも考慮する必要がある。

### 2.2. 「脆弱性関連情報流通の基本枠組み」の全体像

全体像に係る基本方針は以下の通り。

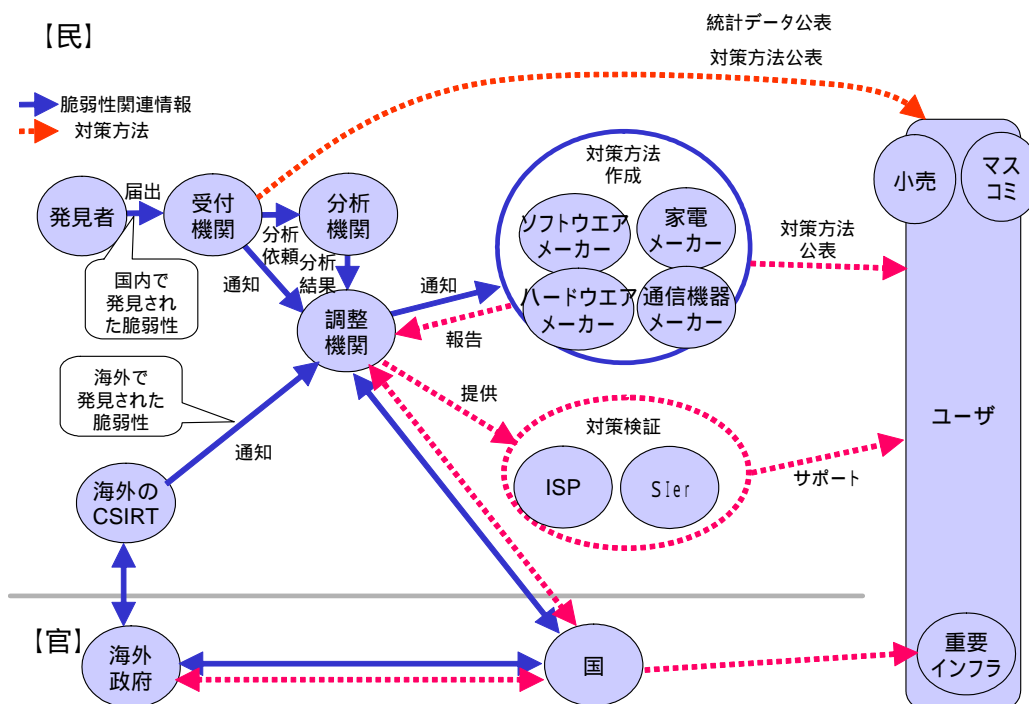
- 1) 本枠組みの適用範囲を、ソフトウェア製品の脆弱性と、ウェブアプリケーションの脆弱性とする
- 2) 脆弱性関連情報の届出を受け付ける機能（受付機関）が必要
- 3) ソフトウェア製品の脆弱性の公表時期を調整するしくみ（調整機関）が必要
- 4) 対策方法や届出件数等の統計データを集積・公表する機能が必要
- 5) 「脆弱性関連情報の流通制御」と「対策方法の適用の迅速化」を両立

<sup>2</sup> ここでは、ソフトウェア自体又はソフトウェアを組み込んだハードウェア等の汎用性を有する製品と定義する。いわゆるオープンソースソフトウェアのように技術情報を統括する企業が一社に定まらないもの、複数の者又は団体によりその改善が行われるものも含む

<sup>3</sup> Computer Security Incident Response Team：コンピュータセキュリティインシデント対応組織

- 6) 製品開発者自身による届出も想定
- 7) 個人情報漏洩等の事案が発生した場合、ウェブサイト運営者は事実を公表
- 8) 政府・重要インフラへの優先情報提供を想定
- 9) 脆弱性関連情報の公表に係るルールを策定
- 10) 発見者、製品開発者、ウェブサイト運営者が本枠組みに協力する意義を明示

<ソフトウェア製品の脆弱性の場合>



<ウェブアプリケーションの脆弱性の場合>

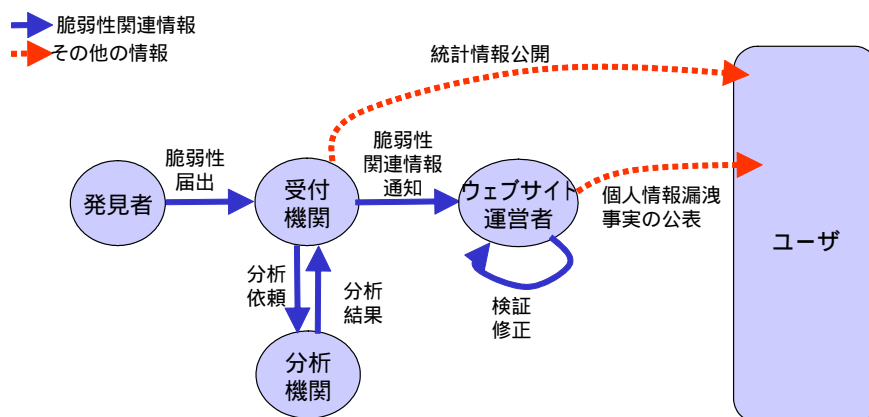


図 2-1 想定される脆弱性関連情報流通の機能構成

「脆弱性関連情報流通の基本枠組み」の実現に向けた課題は以下の通り。

- (1) 「基本枠組み」の各役割を担う主体の特定と不足する機能の付加
- (2) 「基本枠組み」の制度的担保
- (3) ユーザのサポートのあり方

本研究では、脆弱性の発見から対策策定・公表に至る情報流通の基本枠組みの構築をめざすこととし、(1)体制整備及び(2)制度的担保に焦点を絞る。

### 3. 「脆弱性関連情報流通の基本枠組み」を担う主体と枠組みの詳細

#### 3.1. 「基本枠組み」の各役割を担う主体の特定

「脆弱性関連情報流通の基本枠組み」を支える主な部分は、現在有する機能と今後の進むべき方向性を総合し、以下のように独立行政法人情報処理推進機構（IPA）及び有限責任中間法人 JPCERT コーディネーションセンター（JPCERT/CC）が分担することが適当。

- 1) 製品の脆弱性に関する発見者からの届出受付は IPA に一元化（「受付機関」は IPA）
- 2) 海外 CSIRT からの情報は、既存のルート（JPCERT/CC）で対応
- 3) 脆弱性関連情報の流通の要は JPCERT/CC（「調整機関」は JPCERT/CC）、対策方法の集積・開示は IPA が主担当
- 4) 対策方法の優先提供についても考慮

表 3-1 脆弱性関連情報流通の基本枠組みを支える役割分担

対象	受付	調整	分析・対策策定	公表	情報利用
ウェブアプリケーションの脆弱性	IPA ・一次受付 ・スクリーニング ・受理 / 不受理通知 ・当該ウェブサイト運営者への通知 ・統計データ化		当該ウェブサイト運営者 ・脆弱性の検証 ・対策の実施 ・IPAへ完了報告（IPAが必要と判断した場合、当該ウェブサイト運営者の許可を得て分析）	当該ウェブサイト運営者 ・個人情報漏洩の可能性がある場合には事実関係を公表 IPA ・統計データの集積・公表	ウェブサイト運営者 ・統計データを踏まえ、ウェブアプリケーションの脆弱性の実態について把握
ソフトウェア製品の脆弱性（発見者からの届出）	IPA ・一次受付 ・スクリーニング ・受理 / 不受理通知 ・統計データ化	JPCERT/CC ・配信先の抽出・通知 ・公表スケジュールの管理 ・IPAの分析成果を当該製品開発者に提供	当該製品開発者 ・対策方法の策定（ワークアラウンド、パッチ、ver-up等） IPA ・脆弱性分析（影響範囲の検証、リスク分析、脆弱性検証ツールの作成等）	当該製品開発者 ・スケジュールに沿って対策方法を公表 IPA、JPCERT/CC ・対策方法を公表 ・IPAがDB登録 ・IPAが統計データを集積・公表	製品開発者 ・JPCERT/CCから脆弱性関連情報の提供を受けて自社製品への影響を検証、報告 ・機密保持が前提 政府・重要インフラ事業者 ・IPAから公表前の対策方法や準備要請情報の提供を受けて対処
ソフトウェア製品の脆弱性（海外CSIRTからの連絡）		JPCERT/CC ・海外CSIRTからの受信 ・配信先の抽出・通知 ・公表スケジュールの管理 ・IPAの分析成果を当該製品開発者に提供 ・情報源への報告	当該製品開発者 ・対策方法の策定（ワークアラウンド、パッチ、ver-up等） IPA ・脆弱性分析（影響範囲の検証、リスク分析、脆弱性検証ツールの作成等）	当該製品開発者 ・スケジュールに沿って対策方法を公表 IPA、JPCERT/CC ・対策方法を公表 ・IPAがDB登録 ・IPAが統計データを集積・公表	機密保持が前提 システム構築者/運用者、ISP (Telecom-ISAC Japan) ・公表後の対策方法を受けてユーザに対策実施 ・JNSA等の活動と連携 IPAのDBを活用

### 3.2. 「基本枠組み」の詳細

IPA 及び JPCERT/CC がそれぞれ、受付機関、調整機関等の役割を担うことを前提として構築。

#### (1) ソフトウェア製品の脆弱性の場合

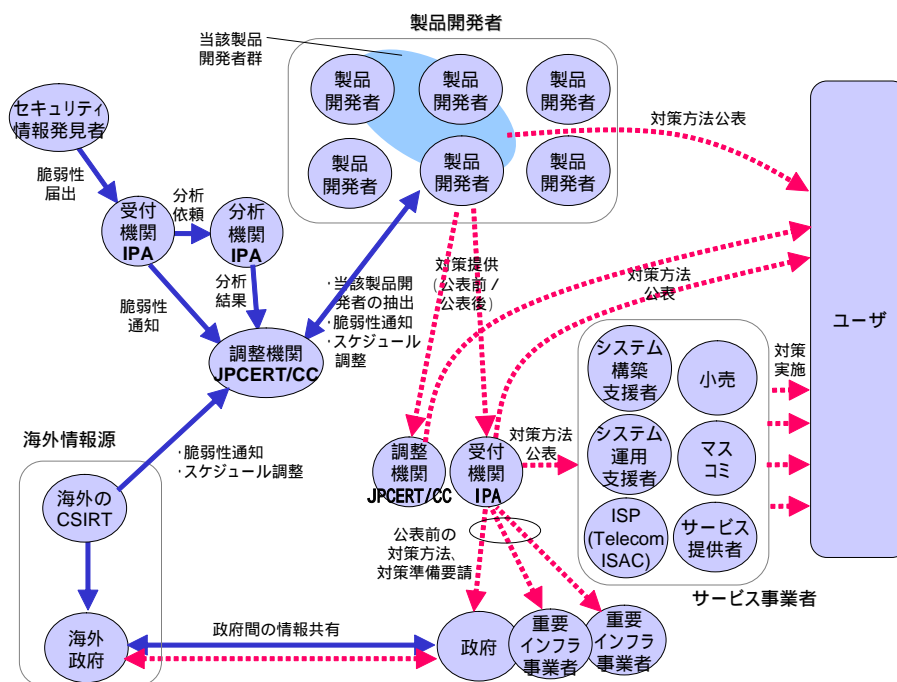


図 3-1 ソフトウェア製品の場合の脆弱性関連情報流通体制

#### (2) ウェブアプリケーションの脆弱性の場合

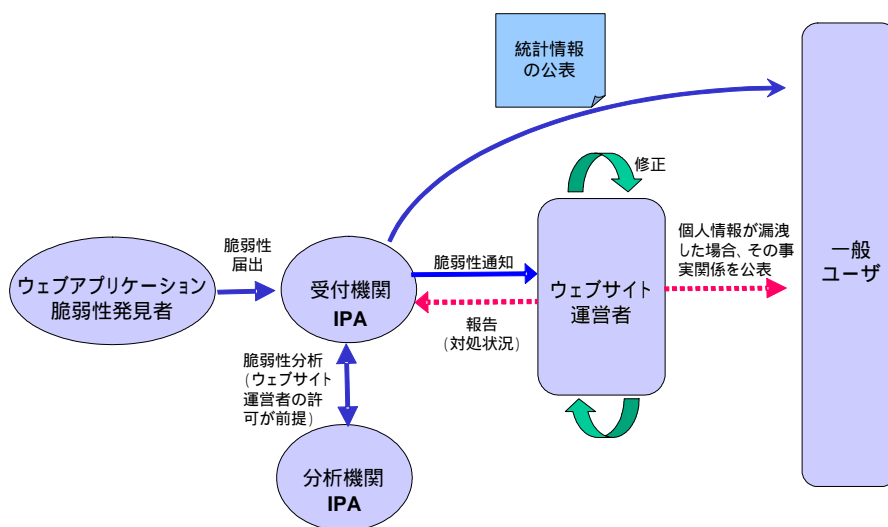


図 3-2 ウェブアプリケーションの場合の脆弱性関連情報流通体制

## 4. 「脆弱性関連情報流通の基本枠組み」を支える制度的担保等

### 4.1. 制度的担保の必要性

関係者の脆弱性関連情報に対する適切な行動を促すべく、それぞれの果たすべき役割や望ましい行動基準を明示した制度を導入する必要がある。

### 4.2. 制度的担保の具体策

脆弱性関連情報の発見者に受付機関の存在を周知するとともに、関係者の適切な対応を促す目的から政府の定める公的なルールが適当。

公的なルールと連動する形で、受付機関や調整機関等の役割・機能を規定し、処理の流れを明確化する意図から民間側のガイドラインを別途策定することが適当。

### 4.3. 公的ルールと民間ガイドラインのモデル案

公的ルールと民間ガイドラインのモデル案を策定。

公的ルールは、第三者が脆弱性関連情報を発見し、受付機関に届け出た際の、関係者間の必要最低限の努力義務を明示するものと位置づけている。

民間ガイドラインは、第三者が脆弱性関連情報を発見し、IPAに届け出た際の、関係者間のなすべき事項を自ら宣言するものと位置づけている。

### 4.4. 法的論点

脆弱性関連情報取扱に係わる法的論点に関しては、以下の観点から検討した。

#### (1) 脆弱性関連情報の発見者に係わる論点

##### 脆弱性関連情報の発見

脆弱性関連情報の発見に際して、発見者は、以下の法令に関する配慮が必要。

- (a) 不正アクセス禁止法
- (b) 刑法
- (c) 電波法
- (d) 著作権法

著作権法に関しては、留意は必要であるが、結果的にはガイドラインに留意事項として明記していない。

#### (e) その他関連する法規

- 1) 憲法 21 条 2 項後段「表現の自由」
- 2) 電気通信事業法 4 条「秘密の保護」

### 3) 有線電気通信法 9 条「有線電気通信の秘密の保護」

#### 脆弱性関連情報の開示

憲法第 21 条第 1 項において、「集会、結社、および言論、出版その他一切の表現の自由は、これを保障する」と記されている。しかし、以下への配慮が必要。

- (a) 刑法の名誉毀損罪
- (b) 刑法の信用毀損罪
- (c) 損害賠償責任などの民事責任

#### 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ない。ただし、不法な手段で入手されたことが明白な脆弱性関連情報に関しては、処理しないことがある。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なく、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もない。

#### (2) 受付機関・調整機関に係わる論点

受付機関・調整機関が脆弱性関連情報の通知を受けたのにも関わらず、迅速な対応ができなかった場合の法的論点については、各種業務や契約のさらなる詳細化を図る必要がある。

#### (3) 関連する製品開発者に係わる論点

ソフトウェアライセンスにおける製品開発者と購入者との契約においては、債務不履行責任、不法行為責任、瑕疵担保責任の対象となる可能性がある。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可能性がある。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ェアは、製造物責任法による製品の欠陥を根拠とした責任を負う可能性がある。製品開発者が自社製品の脆弱性に関連して損害賠償を請求された場合、本報告書の枠組みに則って真摯に対策をとっていることは、裁判所の過失の判断に影響を与えうると考えられる。

#### (4) 関連するウェブサイト運営者に係わる論点

ウェブサイトにおいて、ウェブサイト運営者とユーザとの間に、一定の契約関係があるものと推測される。ウェブサイトの過失による損害賠償の責めをすべて免れるような規定は、消費者契約法上無効となる可能性がある。

## 5. 今後の予定

### 5.1. 次年度以降の作業計画

次年度以降、表 5-1に示す作業を進めることが期待される。

表 5-1 次年度以降の作業イメージ

時期		制度的担保	基本枠組みを支える体制の整備
2004 年	3 月末	・ 研究会報告書とりまとめ	・ 脆弱性関連情報届出の受付システム の整備 ・ IPA・JPCERT/CC 間情報共有環境 の整備 ・ 脆弱性対策方法 DB の構築開始 ・ 脆弱性分析機能の充実 ・ JPCERT/CC・製品開発者間の提携 推進 ・ 脆弱性関連情報届出の受付開始
	4 月中	・ 関係者間調整	
	5 月上旬	・ 政府の公的ルール案公表 ・ パブリックコメント募集	
	6 月上旬	・ パブリックコメント締切	
	7 月上旬	・ 政府の公的ルールの運用開始 ・ 民間ガイドライン運用開始	
	7 月以降	・ 問題点の洗い出し	
2005 年度		・ 民間ガイドラインの修正	・ 情報流通体制の改善・本稼動

### 5.2. 次年度以降の検討課題

- (1) 脆弱性関連情報受付システムの整備
  - 秘匿性を重視した情報管理
  - 脆弱性の危険性、影響度、緊急度評価
  - 他のスキームとの連携
- (2) 機密情報流通の仕組みづくり
  - 受付機関 - 調整機関間の情報共有
  - 調整機関 - 製品開発者間の情報共有
  - 政府・重要インフラ事業者への優先情報提供
  - 情報流通に関するシミュレーションの実施
  - 情報流通の有効性に関するチェック機能の導入
- (3) 製品開発者側に望まれる対応
  - 脆弱性関連情報流通の枠組みへの参加
  - 脆弱性関連情報取扱いに関する社内ポリシーの策定

## 各製品開発者間の連携

- (4) 脆弱性分析機能の充実  
脆弱性分析体制の確立  
分析環境の整備
  
- (5) 脆弱性対策方法の集積・公表機能の整備  
公表スケジュールを反映した情報管理  
他の関連データベースとの連携  
データベースユーザのニーズの反映
  
- (6) ユーザ側に求められる対応  
企業ユーザ間の情報共有の仕組みづくり  
中小企業、個人ユーザの啓発・支援

## 「情報システム等の脆弱性情報の取扱いに関する研究会」について

独立行政法人情報処理推進機構（IPA）では2003年11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」を組織し、機密を保持したまま脆弱性情報を必要な機関間で流通させるとともに、有効な対策方法が効率的にユーザに供給されるためのしくみを検討した。

本研究会は、IPAを中心に中間法人 JPCERT コーディネーションセンター、独立行政法人産業技術総合研究所、NPO 日本ネットワークセキュリティ協会（JNSA）、ハード/ソフトウェアメーカー、セキュリティベンダなど約30機関・50人が参加した。

本研究会では平成16年3月に報告をとりまとめた後、その成果を踏まえ平成16年度にはそうした脆弱性関連情報の流通に関する制度や体制の試験運用、平成17年度には本稼動へと展開する方針である。

なお、IPAでは、本研究会の活動と平行する形で、IPAセキュリティセンター内にソフトウェアの脆弱性を検証しその影響規模等を分析する情報セキュリティ技術ラボラトリーを開設し、脆弱性に対処する体制整備に着手している。

### 【 活動記録 】

平成15年	9月 3日	準備会	
	11月 4日	情報システム等の脆弱性情報の取扱いに関する研究会(第一回)	
	12月 4日	脆弱性情報取扱いガイドライン WG(第一回)	
	12月 4日	脆弱性情報流通 WG(第一回)	
	12月12日	情報システム等の脆弱性情報の取扱いに関する研究会(第二回)	
平成16年	1月13日	脆弱性情報取扱いガイドライン WG(第二回)	
	1月13日	脆弱性情報流通 WG(第二回)	
	2月10日	脆弱性情報取扱いガイドライン WG(第三回)	
	2月10日	脆弱性情報流通 WG(第三回)	
	3月 8日	脆弱性情報取扱いガイドライン WG(第四回)	
	3月23日	脆弱性情報取扱いガイドライン WG(第五回)	} 合同開催
		脆弱性情報流通 WG(第四回)	
	3月26日	情報システム等の脆弱性情報の取扱いに関する研究会(第三回)	

## 【 委員構成 】( 順不同・敬称略 )

### 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	中央大学
( 座長代理 )	山口 英	JPCERT/CC / 奈良先端科学技術大学院大学
( 顧問 )	今井 秀樹	東京大学
	村井 純	慶應義塾大学
	村岡 洋一	早稲田大学
( 委員 )	高橋 正和	インターネットセキュリティシステムズ株式会社
	林 簡	株式会社インフォセック
	西尾 秀一	株式会社 NTT データ
	岡野 直樹	サン・マイクロシステムズ株式会社
	大和 敏彦	シスコシステムズ株式会社
	勝見 勉	株式会社シマンテック
	松島 正明	新日鉄ソリューションズ株式会社
	松本 泰	セコム株式会社
	安田 直義	株式会社ディアイティ
	中尾 康二	Telecom-ISAC Japan/ KDDI 株式会社
	才所 敏明	東芝ソリューション株式会社
	小屋 晋吾	トレンドマイクロ株式会社
	石垣 良信	日本アイ・ビー・エム株式会社
	石井 孝治	日本コンピュータセキュリティリサーチ株式会社
	杉浦 昌	日本電気株式会社
	能地 將博	日本ネットワークアソシエイツ株式会社
	佐藤 慶浩	日本ヒューレット・パカード株式会社
	松本 直人	株式会社ネットアーク
	小林 偉昭	株式会社日立製作所
	塩崎 哲夫	富士通株式会社
	古川 勝也	マイクロソフト株式会社
	長瀬 正人	三菱商事株式会社
	近藤 誠治	三菱電機株式会社
	横地 裕	横河電機株式会社
	新井 悠	株式会社ラック
( オブザーバ )	岡谷 貢	防衛庁
	高橋 郁夫	高橋郁夫法律事務所
	中村 彰二郎	サン・マイクロシステムズ株式会社
	堀内 弘司	サン・マイクロシステムズ株式会社
	井上 隆文	サン・マイクロシステムズ株式会社
	星澤 裕二	株式会社シマンテック
	斉藤 克敏	トレンドマイクロ株式会社
	村上 清治	日本コンピュータセキュリティリサーチ株式会社
	谷川 哲司	日本電気株式会社
	岸田 明	富士通株式会社
	岡田 興	三菱電機株式会社
	小林 伸太郎	三菱電機株式会社
	西岡 秀司	三菱電機株式会社
	金山 卓矢	横河電機株式会社
	水越 一郎	JPCERT コーディネーションセンター ( JPCERT/CC )

	伊藤 友里恵	JPCERT コーディネーションセンター (JPCERT/CC)
	武 智 洋	NPO 日本ネットワークセキュリティ協会 (JNSA)
	印南 朋浩	経済産業省
	山崎 琢矢	経済産業省
	川口 修司	経済産業省
	加来 芳郎	経済産業省
	佐藤 貴幸	経済産業省
	田 沼 均	独立行政法人産業技術総合研究所
	中村 章人	独立行政法人産業技術総合研究所
( 幹事 )	大林 正英	JPCERT コーディネーションセンター (JPCERT/CC)
	下村 正洋	NPO 日本ネットワークセキュリティ協会 (JNSA)
	川口 耕一	NPO ネットワークリスクマネジメント協会 (NRA)
	高木 浩光	独立行政法人産業技術総合研究所
	戸 村 哲	独立行政法人産業技術総合研究所
( 事務局 )	早貸 淳子	独立行政法人情報処理推進機構
	日下 保裕	独立行政法人情報処理推進機構
	小門 寿明	独立行政法人情報処理推進機構
	福澤 淳二	独立行政法人情報処理推進機構
	笠井 行弘	独立行政法人情報処理推進機構
	井上 信吾	独立行政法人情報処理推進機構
	加藤 昌和	独立行政法人情報処理推進機構
	宮川 寧夫	独立行政法人情報処理推進機構
	園田 道夫	独立行政法人情報処理推進機構
	花村 憲一	独立行政法人情報処理推進機構
	田原 美緒	独立行政法人情報処理推進機構
	高坂 史彦	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
	牧野 京子	株式会社三菱総合研究所
	村野 正泰	株式会社三菱総合研究所

### 脆弱性情報取扱いガイドラインワーキンググループ

( メンバー )	高橋 郁夫	高橋郁夫法律事務所
	高橋 正和	インターネットセキュリティシステムズ株式会社
	林 簡	株式会社インフォセック
	勝 見 勉	株式会社シマンテック
	安田 直義	株式会社ディアイティ
	斉藤 克敏	トレンドマイクロ株式会社
	杉 浦 昌	日本電気株式会社
	佐藤 慶浩	日本ヒューレット・パッカード株式会社
	松本 直人	株式会社ネットアーク
	藤田 耕作	株式会社日立製作所
	塩崎 哲夫	富士通株式会社
	古川 勝也	マイクロソフト株式会社
	小林 伸太郎	三菱電機株式会社
	金山 卓矢	横河電機株式会社
	武 智 洋	横河電機株式会社
( オブザーバ )	岡 谷 貢	防衛庁
	水越 一郎	JPCERT コーディネーションセンター (JPCERT/CC)

伊藤 友里恵	JPCERT コーディネーションセンター (JPCERT/CC)
山崎 琢矢	経済産業省
川口 修司	経済産業省
佐藤 貴幸	経済産業省
加来 芳郎	経済産業省

### 脆弱性情報流通ワーキンググループ

(メンバー)	高橋 正和	インターネットセキュリティシステムズ株式会社
	西尾 秀一	株式会社 NTT データ
	岡野 直樹	サン・マイクロシステムズ株式会社
	星澤 裕二	株式会社シマンテック
	松本 泰	セコム株式会社
	安田 直義	株式会社ディアイティ
	中尾 康二	Telecom-ISAC Japan/KDDI 株式会社
	才所 敏明	東芝ソリューション株式会社
	小屋 晋吾	トレンドマイクロ株式会社
	石井 孝治	日本コンピュータセキュリティリサーチ株式会社
	村上 清治	日本コンピュータセキュリティリサーチ株式会社
	谷川 哲司	日本電気株式会社
	能地 將博	日本ネットワークアソシエイツ株式会社
	松本 直人	株式会社ネットアーク
	田中 和雄	株式会社日立製作所
	岸田 明	富士通株式会社
	古川 勝也	マイクロソフト株式会社
	近藤 誠治	三菱電機株式会社
	横地 裕	横河電機株式会社
	(オブザーバ)	新井 悠
岡谷 貢		防衛庁
水越 一郎		JPCERT コーディネーションセンター (JPCERT/CC)
伊藤 友里恵		JPCERT コーディネーションセンター (JPCERT/CC)
山崎 琢矢		経済産業省
川口 修司		経済産業省
佐藤 貴幸		経済産業省
加来 芳郎		経済産業省
田沼 均		独立行政法人産業技術総合研究所
中村 章人		独立行政法人産業技術総合研究所



# 本 編



## はじめに

近年の情報システムやインターネットの普及は、情報のアクセスにおける時空間を超越した利便性、コミュニケーションツールとしてのコンピュータネットワークの有効性等をベースに、経済社会の変革を促進している。反面、コンピュータウイルスの蔓延や不正アクセスを助長し、多くのユーザを不安に陥れているだけではなく、情報システムやインターネット自身の有用性を低減させる結果にもなっている。

こうした状況下で、注目を浴びているキーワードが「脆弱性」である。本報告書において「脆弱性」は、「ソフトウェア等において、コンピュータ不正アクセス、コンピュータウイルス等の攻撃によりその機能や性能を損なう原因となり得る安全性上の問題箇所」と定義している。コンピュータウイルスや不正アクセスにおいても、脆弱性に起因するものが相当数に上ると推定される。

さらに、脆弱性に関連する情報を取り扱う際には、高度な専門性と現代の高度情報社会に対応する倫理観に根ざした大局的な判断が必要となる。しかしこうした判断は、特定の政策担当者や専門家が単独で行えるものではなく、関係者が、現状を共有し、その中で課題を認識し、議論の中での解決策の提示により、醸成されるものである。

本報告書は、このような背景と問題認識の下に、「情報システム等の脆弱性情報の取扱いに関する研究会」での活動の成果として作成されたものである。本報告書では、脆弱性に関連する情報を、関係者間で取り扱う際の解決策として、ルールと体制を示している。

本報告書が、関係者間のみならず、広く一般にも浸透し、脆弱性に関する共通の理解と認識が得られることにより、我が国のセキュリティカルチャの形成につながり、その結果として安全・安心な社会の構築に貢献することになれば幸いである。

平成16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

1. 背景	1
1.1. 問題意識	1
1.2. 官民の取り組みの現状	6
2. 脆弱性関連情報流通の基本枠組み	9
2.1. 検討の前提	9
2.2. 「脆弱性関連情報流通の基本枠組み」の全体像	13
3. 「脆弱性関連情報流通の基本枠組み」を担う主体と枠組みの詳細	23
3.1. 「基本枠組み」の各役割を担う主体の特定	23
3.2. 「基本枠組み」の詳細	26
4. 「脆弱性関連情報流通の基本枠組み」を支える制度的担保等	33
4.1. 制度的担保の必要性	33
4.2. 制度的担保の具体策	33
4.3. 公的ルールと民間ガイドラインのモデル案	34
4.4. 法的論点	34
5. 今後の予定	45
5.1. 次年度以降の作業計画	45
5.2. 次年度以降の検討課題	46
< 資料編 >	
資料1	ソフトウェア等脆弱性関連情報取扱基準モデル案
資料2	ソフトウェア等脆弱性関連情報取扱ガイドラインモデル案
資料3	海外における脆弱性情報取扱ガイドラインの事例

## 1. 背景

### 1.1. 問題意識

#### (1) 脆弱性とは

ソフトウェアを中心とする情報システム等の脆弱性<sup>1</sup>は、ソフトウェアの設計・開発段階に内包される潜在的問題であり、事前に完全に察知・回避することは難しいとされている。いわゆるバグの一種であるが、他者からの攻撃によって問題が顕在化する点で一般的なバグとは一線を画す。

脆弱性の発見は、開発元のスタッフが自ら行うケースもあるが、第三者によって指摘されるケースも少なくない。脆弱性がソフトウェア製品<sup>2</sup>に影響する場合、通常は脆弱性の対策方法<sup>3</sup>がその製品の開発元から提供され、ユーザがそれを自らのシステムに適用することによって解決する。また、脆弱性がウェブアプリケーション<sup>4</sup>のようにインターネット上で公開されているサービスシステムに影響する場合、ウェブサイト運営者が対策を実施することになる。

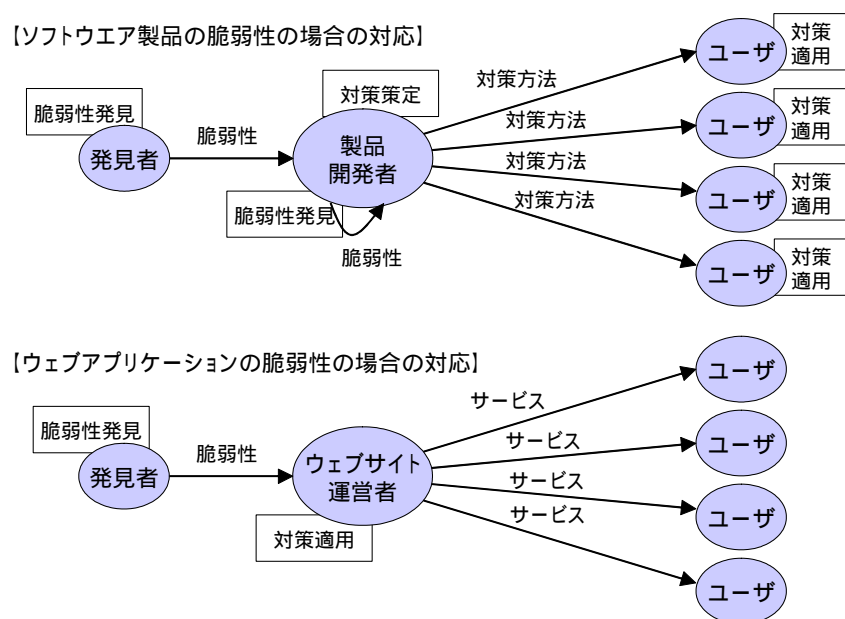


図 1-1 脆弱性の発見から対策適用まで

<sup>1</sup> ソフトウェア等において、コンピュータ不正アクセス、コンピュータウイルス等の攻撃によりその機能や性能を損なう原因となり得る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

<sup>2</sup> ここでは、ソフトウェア自体又はソフトウェアを組み込んだハードウェア等の汎用性を有する製品と定義する。いわゆるオープンソースソフトウェアのように技術情報を統括する企業が一社に定まらないもの、複数の者又は団体によりその改善が行われるものも含む

<sup>3</sup> 被害の回避方法（ワークアラウンド）や脆弱性そのものの修正方法（パッチ）

<sup>4</sup> インターネット上の各ウェブサイトで稼動するシステム。電子申請やネットバンキングなどインターネットを介したインタラクティブなサービスを実現する

近年、情報システム等の脆弱性は、コンピュータ不正アクセスやコンピュータウイルス等の攻撃に悪用されるケースが増加しており、IT社会の安全性を脅かすインシデントの主要な原因となっている。表 1-1に脆弱性の例を示す。

表 1-1 代表的な脆弱性の例 - ソフトウェア製品

脆弱性の例	概要
サーバ側イメージマップコンポーネントの脆弱性 (MS00-078)	<ul style="list-style-type: none"> <li>平成 12 年 4 月発表。</li> <li>Microsoft の Web サーバ製品に内在。悪意を持った Web サイト訪問者が、従来は実行する手段がなかった動作を実行できるようになる。</li> <li>平成 13 年 9 月にはこの脆弱性を悪用したワーム「Nimda」が発生、世界的に流行。</li> </ul>
Index Server ISAPI エクステンションの未チェックのバッファによる脆弱性 (MS01-033)	<ul style="list-style-type: none"> <li>平成 13 年 6 月発表。</li> <li>Web サーバ「Microsoft IIS」等に内在。攻撃者はバッファオーバーフローを引き起こし、サーバを完全に制御することが可能。</li> <li>平成 13 年 7 月にはこの脆弱性を悪用したワーム「Code Red」が発生。</li> </ul>
Apache Web サーバにおける chunk データ処理の脆弱性 (CAN-2002-0392)	<ul style="list-style-type: none"> <li>平成 14 年 6 月発表。</li> <li>Web サーバ「Apache」に内在。ChunkedEncoding で送られてきたリクエストを適切に処理できない場合に、Web サイトの改竄や DoS などの複数の攻撃が可能になる。</li> <li>平成 14 年 7 月にはこの脆弱性を悪用したワーム「Scalper」が発生。</li> </ul>
Microsoft SQL Server 解決サービスの脆弱性 (MS02-039)	<ul style="list-style-type: none"> <li>平成 14 年 7 月発表。</li> <li>DB 管理システム「Microsoft SQL Server 2000」等に内在。攻撃者はバッファオーバーフローを引き起こし、攻撃者のコードを実行させることが可能。</li> <li>平成 15 年 1 月にはこの脆弱性を悪用したワーム「SQL Slammer」が発生。大量の packets を送出し、韓国のインターネットがダウンするなどの被害が発生。</li> </ul>
Sendmail におけるメールヘッダー処理の脆弱性 (CAN-2003-0161)	<ul style="list-style-type: none"> <li>平成 15 年 3 月発表。</li> <li>メールサーバ「Sendmail」のメールヘッダー処理部分にバッファオーバーフローを起こす脆弱性が内在。ヘッダーを細工した攻撃のメールは、ファイアウォールを通過し、IDS や ワクチンサーバでも検出されず内部のメールサーバにも転送され攻撃される可能性がある。</li> </ul>
Cisco IOS の脆弱性 (CAN-2003-0161)	<ul style="list-style-type: none"> <li>平成 15 年 7 月発表。</li> <li>Cisco のスイッチ/ルータ製品に搭載されている OS「IOS」に内在。巧妙に作成した一連の IPv4 パケットを処理すると、入力キューが一杯になったと誤認し、トラフィック処理を停止してしまう可能性。</li> <li>発表の翌日には攻撃コードが公表された。</li> </ul>
Microsoft Windows RPC インタフェースの脆弱性 (MS03-026)	<ul style="list-style-type: none"> <li>平成 15 年 7 月発表。</li> <li>OS「Microsoft Windows」に内在。攻撃者はバッファオーバーフローを引き起こし、全アクセス権を持つ新規アカウントの作成など、いかなる操作も可能。</li> <li>平成 15 年 8 月にはこの脆弱性を悪用したワーム「MS Blaster」が発生。対策未適用の PC はインターネットに接続しているだけで感染。</li> </ul>

出典：各種記事より構成

表 1-2 代表的な脆弱性の例 - ウェブアプリケーション

脆弱性の例	概要
Web メールサービスの脆弱性	<ul style="list-style-type: none"> <li>平成 12 年度発表。</li> <li>国内 18 カ所の web メールサービスのうち 7 カ所において、URL に含まれるセッション ID の漏洩が原因でメールの内容を盗み見られる欠陥があることが判明。</li> </ul>
クロスサイトスクリプティングの脆弱性	<ul style="list-style-type: none"> <li>平成 13 年度発表。</li> <li>国内大手サイト 8 カ所において個人情報漏洩の可能性がある、うち 3 サイトではクレジットカード番号も盗まれ得る状態であることが判明。また、プライバシーマーク及びオンラインマークの取得事業者から無作為に抽出した 50 サイトと銀行 22 サイトのうち、約 8 割にこの脆弱性があることが判明。</li> </ul>
秘密情報を含まない cookie によるアクセス制御方式の脆弱性	<ul style="list-style-type: none"> <li>平成 14 年度発表。</li> <li>cookie によるアクセス制御方式をもつ国内の 5 つのサイトにおいて、計 400～500 万人分の個人情報を、誰もがいつでも閲覧可能な状態にあることが判明。</li> </ul>
非 secure モードの cookie が盗聴される脆弱性	<ul style="list-style-type: none"> <li>平成 15 年度発表。</li> <li>SSL による暗号化で情報保護するサイトのうち、cookie を用いたアクセス制御方式を採用している 22 サイトのうち、アクセス制御用 cookie が secure モードで発行されていない欠陥が 20 サイトにあり、パケット盗聴により個人情報が盗まれる可能性があることが判明。</li> </ul>

出典：「インターネットアプリケーションのセキュリティ脆弱性に関する研究」(独立行政法人産業技術研究所グリッド研究センター)を基に構成

## (2) 脆弱性の特性

情報システム等の脆弱性に係る特性について以下にまとめる。

### 脆弱性の情報は適切かつ慎重な取扱いが必須

脆弱性に関する情報は、適切に扱われず放置されたり、対策がない段階で暴露されることによって、コンピュータ不正アクセスやコンピュータウイルス等の攻撃に悪用され、システムやネットワークのダウン、個人情報の漏洩など大きな被害をもたらす危険性がある。

脆弱性の発見者は、脆弱性の存在を製品開発者<sup>5</sup>やウェブサイト運営者<sup>6</sup>に通知する際、脆弱性を顕在化させるための条件設定や操作手順など詳細な説明が要求されることが多い。こうした要求への対応は脆弱性の情報の発見者にとって負担が大きいいため、通知をあきらめてしまう可能性もある。

<sup>5</sup> ソフトウェア製品を開発した企業もしくは個人。また、ソフトウェア製品の開発、加工、輸入又は販売に関して当該ソフトウェア製品の実質的な開発者と認められる者。ソフトウェア製品の開発者が外国の会社である場合は、そのソフトウェア製品の国内での主たる販売を行っている会社。

<sup>6</sup> そのウェブサイトについて対外的に責任を有する事業者(個人の場合を含む)。依頼されて Web サイトの作成・運用を代行する事業者や第三者は含まない。

また、修正を促すため発見者が発見した脆弱性を掲示板等に暴露し、その結果、脆弱性を指摘されたウェブサイトから個人情報漏洩する事態が発生している。

さらに、放置や暴露もなく製品開発者やウェブサイト運営者に脆弱性の情報が届いた場合でも、脆弱性対策が利益に直結する性質のものではないため、彼らがそうした情報に適切に対応しない可能性がある。

### 脆弱性の公表から攻撃方法の出現までの期間が短縮

図 1-2に示すように、脆弱性の発見から対策方法の適用までの流れにおいて、攻撃より前に対策方法を適用した場合には被害は発生しないが、攻撃が先じた場合には被害が発生する可能性がある。

一方で、ソフトウェアの脆弱性の公表から exploit コード<sup>7</sup>やコンピュータウイルス等攻撃方法<sup>8</sup>の出現までの期間が急速に短縮しつつある。例えば、2003 年 2 月に韓国のネットワークをダウンさせた「SQL Slammer」の場合、脆弱性の対策方法の公表からワームの発生までに約半年の期間を要したが、2003 年 8 月に国内で猛威を振るった「MS Blaster」の場合、脆弱性の対策方法が公表されてからわずか 3 週間強でワームが発生した。

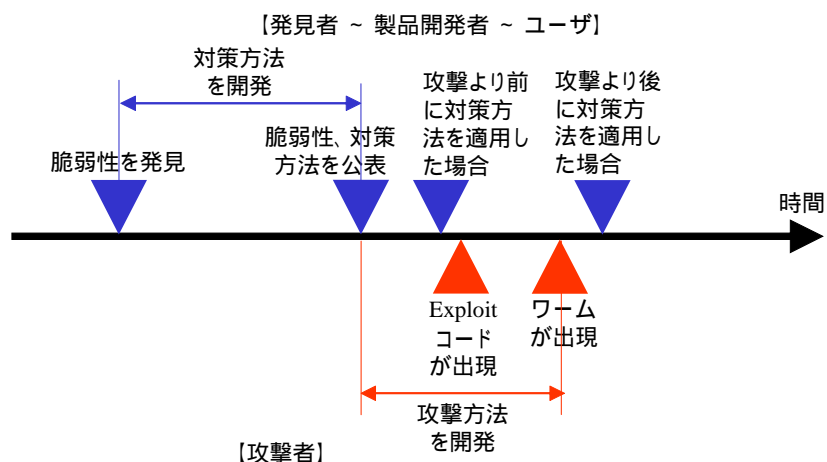


図 1-2 脆弱性の発見から対策方法の適用までの流れ

### (3) 我が国における問題点

(2)を踏まえ、情報システム等の脆弱性を巡る我が国の問題として、以下の点

<sup>7</sup> 脆弱性を悪用するソフトウェアのソースコード。使い方によっては、脆弱性の検証に役立つこともある

<sup>8</sup> 脆弱性を悪用してソフトウェアの動作に不具合を発生させるプログラムやコマンド、データおよびそれらの使い方

が挙げられる。

### **情報システム等の脆弱性の公表に関する調整が不十分**

脆弱性が複数の製品開発者に影響する場合、脆弱性の情報を入手していなかった製品開発者の製品は、対応した製品開発者の対策公表をきっかけにして「ゼロデイアタック<sup>9</sup>」の被害に遭う可能性がある。例えば、プリンタに搭載された OS について、メーカーが対策実施の必要性に気づかずパッチの適用が遅れた結果、ワームの感染を招いたという事例がある。現在、JPCERT コーディネーションセンター(以下 JPCERT/CC)が国内の調整に着手しているが、より大規模な活動が望まれる。

### **情報システム等の脆弱性に関する研究・発見・対策策定は海外に依存**

現在、ソフトウェアを中心とする情報システム等の脆弱性に関する研究・発見の大半は海外に依存している。一方、海外ソフトの日本語版、携帯電話や情報家電等を含む国産ソフトウェアは、海外の研究者の研究対象となることが少なく、脆弱性検証が不十分な状況にあるため、脆弱性が改善されにくいと考えられる。

また、海外ソフトの脆弱性対策について、日本語版の対応が完了していない段階で本社が公表に踏み切ったため、日本のユーザが、脆弱性は知られているが対策方法がないという危険な状況に陥ったケースも見られる。

### **ウェブアプリケーションの脆弱性は対処が進みにくい**

ウェブアプリケーションの場合、検査を経なければ脆弱性の存在が判明しにくいいため、ウェブサイト運営者が気づかないケースが多い。脆弱性検査の必要性についても認識が十分でなく、第三者から脆弱性の指摘がなされても前向きに捉えることができない傾向にあると考えられる。その結果、そうした問題が放置されたり、掲示板等に暴露されるなどして、不特定多数のユーザに被害が及ぶ可能性もある。

なお、第三者がウェブサイト運営者の許可なく脆弱性検査を行うことは、運営者に危険性を伝える目的であっても、脆弱性の種類によっては不正アクセス禁止法等に抵触する可能性もあり、奨励できる行為ではない。その一方、ユーザが適法にウェブサイトを利用している最中に、偶然に脆弱性を見つけてしまった場合には、運営者に事実関係を伝えることが望ましいが、不正アクセス禁止法等への抵触を疑われることを恐れて放置してしまうことが起

---

<sup>9</sup> 対策方法が提供される前に行われる脆弱性への攻撃

きやすいと考えられる。

## 1.2. 官民の取り組みの現状

### (1) 政府の取り組み

我が国政府としては、世界最高水準の高度情報通信ネットワーク社会をめざす e-Japan 戦略の重点政策「高度情報通信ネットワークの安全性と信頼性の確保」を実現するための施策展開に取り組んでいる。中でも、コンピュータ不正アクセスやコンピュータウイルス等を防止することは、インターネットを介して世界が相互に依存し、一国で発生したトラブルが他国にも波及しうるネットワーク社会において、我が国の IT 基盤の安全性向上だけでなく、国際社会の一員としての重要な貢献にもつながる。

経済産業省では、平成 2 年から「コンピュータウイルス・不正アクセス届出事業」<sup>10</sup>や平成 15 年から「インターネット定点観測事業」<sup>11</sup>を実施し、コンピュータウイルスやコンピュータ不正アクセスなどコンピュータ・セキュリティ問題の早期発見・公表による被害局限化を進めてきた。

しかし、近年、こうした攻撃の矛先がソフトウェアを中心とする情報システム等の脆弱性に向けられるケースが増えた結果、被害拡大のスピードはユーザが対処可能なレベルを遙かに超える勢いで早まりつつあり、被害はますます拡大・深刻化しつつある。

従来、情報システム等の脆弱性の問題は IT 業界各社の取り組みが主であったが、それが不特定多数のユーザに影響が及ぶこと、その一方、脆弱性への対応が製品開発者の利益に直結しない上に 1.1 に示した問題もあって自律的な改善が進みにくいことから、今後は、IT 業界の対策策定の取り組みがより円滑かつ効果的に進むよう、政府がそれを補完し支援していくことが必要である。こうした状況を踏まえ、経済産業省では平成 15 年 10 月に公表した「情報セキュリティ総合戦略」(産業構造審議会情報セキュリティ部会(部会長;寺島実郎(財)日本総合研究所理事長))において「脆弱性に対処するためのルールと体制の整備」「IT 事業者間における情報共有・活用・協力体制の設置」を提言している。

このように、我が国高度情報通信ネットワーク社会の安全性・信頼性の確保

<sup>10</sup>情報処理推進機構 (IPA) において、平成 2 年よりコンピュータウイルスの届出受付・分析及び実績の公表を実施。JPCERT コーディネーションセンター (JPCERT/CC) において、平成 8 年より不正アクセスの相談窓口業務を実施。

<sup>11</sup> JPCERT/CC において、平成 15 年より、インターネット上に設置した複数のセンサーから得られる情報を解析し、ネットワーク・システム管理者向けにホームページ上で公開する「インターネット定点観測事業」を実施

のために、IT 業界とユーザのそれぞれが、市場メカニズムを活用しながら被害の抑制と局限化に努力し、政府がその機能を補完する形で官民が連携協力して取り組む仕組みを構築することが適当である。

(経済産業省「情報セキュリティ総合戦略」(平成 15 年 10 月 10 日発表)より抜粋)

### 3.3.2. 企業・個人における新たな事前予防策

#### (1) 官民連携した脆弱性対応体制の整備

##### 脆弱性に対処するためのルールと体制の整備

我が国では、情報システムの脆弱性やコンピュータウイルス、ワーム等の詳細を把握し対策を講じるための情報を収集し分析する体制が弱く、米 CERT/CC やウイルスワクチンソフトベンダ などの情報を基に危険性を判断しているのが現状である。そのため、国内を中心に使用されるソフトの脆弱性への対応や急速に広がるコンピュータウイルス感染の被害を食い止める緊急対応を行うことが難しい。

そこで、政府と IT 事業者 が中心となって、情報システムの脆弱性情報を集積するためのルールを構築し、それを分析する体制を整備する。具体的には、

- 1) 不正アクセスやコンピュータウイルス感染等の被害通報の受付
- 2) ネットワークのトラフィック観測に基づく異常予測
- 3) 脆弱性の通知と公開に関する一連の手続きルールの明確化 (IT 事業者や研究者等が発見した製品・システムの脆弱性の通報の受け付け、製造元もしくはサービス提供者の対処、一定期間後の公開等)
- 4) 脆弱性及びウイルス、ワーム等の危険性を検証・解析する体制
- 5) 脆弱性及びウイルス、ワーム等の危険性を警告・公表する体制

が必要である。

特に、電子政府の拡大に対応し、通報されたシステムの脆弱性やコンピュータウイルス、ワームの危険性について迅速に検証・解析する体制を、政府として整備することが重要である。中でも、オープンソース のツールや製造元が倒産した製品のように責任を負うべき事業者が明確でない場合の対応、ネットワーク全体に障害をもたらすような緊急性が高く社会的影響の大きい問題への対応等について、本体制の持つ役割は重要である。

### 3.3.2. 企業・個人における事故対応策

#### IT 事業者間における情報共有・活用・協力体制の設置

情報システムの脆弱性を出荷・納品の時点で完全に排除しておくことは困難であるため、IT 事業者は修正用ソフトウェア等の開発体制を確保するとともに、新たな脆弱性が報告された場合には、速やかに対策を講じ、それを企業や個人等のユーザに正しく伝え、修正用ソフトウェアの適用を促す姿勢が求められる。しかし、コスト的な制約や情報・ノウハウの不足のため、個々の IT 事業者は場当たりの対策に終始せざるを得ない状況にある。例えば、ソフトウェアの部品化・再利用化に伴い、メーカーやシステムインテグレータにとってもシステムがブラックボックスと化しており、その脆弱性の影響範囲を正確に把握できずにいる。

また、情報システムの運用を請け負う IT 事業者は、システムダウン等の原因となる脆弱性について情報収集を効率的に行うとともに、被害を最小化し、サービスを継続するための計画や訓練を進めることが重要である。

そこで、IT 事業者が協同して情報システムの事故・事件の予防と事後対応の推進を図る

ための情報共有・協力体制を設置する。この体制では、次の機能を確立することを目指す。

- ・ IT 事業者が運用する SOC 間の連携
- ・ IT 事業者間のトラブルシューティング情報の共有化
- ・ IT 事業者間での脆弱性情報の共有化
- ・ 自社の製品やシステムに採用した組み込みソフトウェアの情報の開示
- ・ 個人ユーザに対する修正用ソフトウェアやセキュリティ情報の効果的な提供
- ・ コンピュータウイルスやワームの発生に関する予測

さらに、本体制と JPCERT/CC、Telecom-ISAC Japan、情報処理振興事業協会セキュリティセンター（IPA-ISEC）、NIRT、自治体・重要インフラの情報共有体制が相互に連携して、国全体の情報共有を効率的に実現する体制を整える。特に、IT ベンダの SOC や、IPA-ISEC、Telecom-ISAC Japan 等が有するリアルタイムのトラフィック監視情報をベースに、迅速な被害拡大防止の実現を図る。

## (2) 民間の取り組み

我が国では、JPCERT/CC が海外の CSIRT<sup>12</sup> に対する日本の窓口として機能しており、送られてきた公表前の脆弱性の情報を国内の製品開発者に提供し、脆弱性情報の公表日の国際間調整を行う活動に着手している。ただし、製品開発者側も脆弱性に対する意識が十分でない状況において、機密を保持しつつ情報を流通させることは容易ではない。そこで、現在は JPCERT/CC が信頼のおけると判断した相手方にのみ情報を提供する方法を採用しているが、情報提供先の数は小規模にとどまっている。また、国際的に見ても、JPCERT/CC が脆弱性に関する情報を国内で流通させる機能を今以上に充実させることを求められており、今後そうした機能強化を進めることは有用と考えられる。

---

<sup>12</sup> Computer Security Incident Response Team：コンピュータセキュリティインシデント対応組織

## 2.脆弱性関連情報流通の基本枠組み

以上の問題点及び現状を踏まえ、我が国における「脆弱性情報流通の基本枠組み」を確立し、関係者間で適切な役割分担を行いながら、情報セキュリティ確保のための基礎インフラを構築していく活動を行うことが有益である。

そのために、本報告書では、以下、

- 1) 確立すべき「脆弱性関連情報流通の基本枠組み」の全体像を提示した上で（本章）、
- 2) その「基本枠組み」における各役割を担う適切な主体を具体的に特定し、それを前提とした詳細なルールを提示し（第3章）、
- 3) その「基本枠組み」を有効に機能させるために必要な制度的担保等について（第4章）

述べていくこととする。

### 2.1. 検討の前提

脆弱性に関する情報を取り扱う体制を検討する際、前提となる次のポイントが存在する。

- ・ 取り扱う情報の種類と取扱い方針
- ・ 適用範囲
- ・ 脆弱性関連情報の発信源
- ・ 脆弱性への対応
- ・ 政府・重要インフラ<sup>13</sup>への優先情報提供

これらの前提について以下に示す。

#### 2.1.1. 取り扱う情報の種類と取扱い方針

取り扱うべき情報の種類とそれぞれの取扱い方針に関して、表 2-1 のように規定できる。

---

<sup>13</sup> 内閣の情報セキュリティ対策推進会議「重要インフラのサイバーテロ対策に係る特別行動計画」（2000年12月）においては、重要インフラ7分野として 情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）を挙げている

表 2-1 脆弱性関連情報の種類と取扱い方針

情報の種類		内容	取扱い方針
脆弱性 関連 情報	脆弱性	ソフトウェア等において、コンピュータ不正アクセス、コンピュータウイルス等の攻撃によりその機能や性能を損なう原因となり得る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。	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	脆弱性を悪用するプログラム、コマンド、データ及びそれらの使用方法。	公表しない。
	検証方法	脆弱性が存在することを調べるための方法	公表しない。
対策方法	回避方法	脆弱性を修正するのではないが、それが原因となって生じる被害を回避するための方法。ワークアラウンドと呼ばれる。	公表後迅速にユーザに流通させる。
	修正方法	脆弱性を修正する方法。	公表後迅速にユーザに流通させる。

一般に、脆弱性が発見された場合、製品開発者は攻撃方法が作成される以前に、回避方法や修正方法を作成することが望ましい。したがって、製品開発者が、回避方法や修正方法を策定するまでは、脆弱性や攻撃方法が一般に流通することを防ぐことが重要である。

また、回避方法や修正方法を製品開発者が発表した後には、広く企業や家庭の一般のユーザまで流通させることが肝要となる。

このように、慎重に扱うべき脆弱性関連情報（脆弱性、検証方法、攻撃方法）と、周知徹底すべき対策方法（回避方法、修正方法）は分けて取り扱う形で「基本枠組み」を構築することが適当である。

### 2.1.2.適用範囲

汎用性を有するソフトウェア製品の場合、脆弱性が不特定多数のユーザに発見される可能性があり、さらに脆弱性が発見された場合には不特定多数のユーザに対策方法を適用させる必要があるため、その影響範囲は大きいと考えられる。また、通信プロトコルや標準化されたフォーマットなどの仕様に曖昧な点があつて解釈によっては実装に脆弱性が含まれる場合も、その仕様を採用したソフトウェア製品が多数存在することから、その脆弱性が及ぼす影響は非常に

大きいと見られる。

一方、ユーザ企業自身が開発した専用システムの場合、基本的にはエンドユーザも組織内のスタッフであるため、脆弱性の発見が組織内に限定されており、脆弱性が発見された場合の影響も小規模にとどまる。ただし、ウェブアプリケーションのようにインターネットを介して一般ユーザが利用可能なサービスシステムの場合には、脆弱性が不特定多数のユーザに発見される可能性があり、それが悪用されれば不特定多数のユーザに影響を受ける可能性がある。

したがって、脆弱性が発見される可能性や発見された場合の影響規模を踏まえ、脆弱性関連情報の流通において扱うべき対象としては、ソフトウェア製品及びウェブアプリケーションを採り上げることが適当である<sup>14</sup>。

ただし、ソフトウェア製品に脆弱性がある場合、発見された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、脆弱性関連情報の通知先や公表のタイミングについて適切な調整が必要となる。その一方、ウェブアプリケーションに脆弱性がある場合、基本的にはそれぞれのウェブアプリケーションに固有の問題であるため、当該ウェブサイト運営者に通知すれば対応できる。したがって、ソフトウェア製品に脆弱性がある場合と、ウェブアプリケーションに脆弱性がある場合で、脆弱性関連情報の取扱プロセスは異なるものになる。

以上のことから、ソフトウェア製品の脆弱性に関する情報、ウェブアプリケーションの脆弱性に関する情報のそれぞれに適用する「基本枠組み」を構築することが望まれる。

### 2.1.3.脆弱性関連情報の提供元

#### (1) ソフトウェア製品の脆弱性の場合

ソフトウェア製品の場合、脆弱性関連情報の提供元は以下の3つのケースが想定される。

脆弱性関連情報の発見者<sup>15</sup>

海外のCSIRT

国内外のセキュリティベンダ（情報提供サービス）

ただし、国内外のセキュリティベンダは、自らが発見した脆弱性関連情報を契約したベンダや顧客等にクローズドなルートで提供することをビジネスとし

---

<sup>14</sup> 暗号アルゴリズムの脆弱性については、総務省及び経済産業省により推進されている暗号技術評価プロジェクト「CRYPTREC」の活動において対応がなされていること、一般に理論的要素が極めて強いことから、本枠組みでは積極的には扱わないこととする。ただし、既に普及している暗号ツールに重大な影響が及ぶ脆弱性が発見された場合には、本枠組みを活用することも考えられる

<sup>15</sup> 脆弱性関連情報を発見又は取得した者（組織または個人）

ているケースがある。そうしたビジネスベースの情報提供については本検討の枠外とすべきである。

したがって、ソフトウェア製品の脆弱性の場合、脆弱性関連情報の提供元が脆弱性関連情報の発見者の場合と、海外のCSIRTの場合の2つを想定した「基本枠組み」を構築することが適当である。

さらに、発見者を詳細化すると、次のように分けられる。

- ・研究者または研究機関（脆弱性が研究対象）
- ・セキュリティベンダ（脆弱性検査の実施時に発見）
- ・システムインテグレータ（システム構築時に発見）
- ・製品開発者（自社製品の検証で発見）

これらのいずれも、脆弱性関連情報の発見・取得時には同様に「発見者」のスタンスで届け出ることが望まれる。なお、責任ある届出を促すため、匿名での届出については、原則認めないものとすべきである。

## (2) ウェブアプリケーションの脆弱性の場合

ウェブアプリケーションの場合、脆弱性関連情報の発見者が主要な提供元となる。したがって、ウェブアプリケーションの脆弱性については、発見者の届出を想定とした「基本枠組み」を構築することが適当である。

発見者は、脆弱性を研究対象とする研究者または研究機関、セキュリティベンダやシステムインテグレータに加え、一般ユーザも想定される。ただし、セキュリティベンダやシステムインテグレータは顧客のウェブアプリケーションの脆弱性を発見した場合、契約上、顧客であるウェブサイト運営者に直接報告する可能性が高い。

### 2.1.4.脆弱性への対応

#### (1) ソフトウェア製品の脆弱性の場合

ソフトウェア製品の脆弱性の場合、対策方法を策定するのは、「製品開発者」が適当である。なお、「製品開発者」は、ソフトウェア製品を開発した者（企業もしくは個人）、ソフトウェア製品の開発、加工、輸入又は販売に関して当該ソフトウェア製品の実質的な開発者として認められる者、と位置付ける。

で想定しているのは、例えば、外国の会社が開発したソフトウェア製品について、外国の開発元の代理として国内の子会社又は販売代理店等の販売を行っている会社である。これは、脆弱性の存在が発覚した際、海外の開発元に対策方法の策定を働きかけることができる影響力を有すると考えるからである。

## (2) ウェブアプリケーションの脆弱性の場合

ウェブアプリケーションの脆弱性の場合、対策を適用するのは、そのウェブサイトについて対外的に責任を有するウェブサイト運営者が適当である（個人の場合を含む）。依頼されて Web サイトの作成・運用を代行する事業者を指すものではない。

### 2.1.5.政府・重要インフラへの優先情報提供

脆弱性関連情報の取り扱いに際しては、政府・重要インフラへの優先情報提供の可能性を検討すべきである。これは、政府・重要インフラにおいては、脆弱性の波及範囲が他分野より大きくなることが想定されるためであり、重要インフラの保護が社会基盤維持に必要なためである。ただし、そのモデルは本来機密に扱うべき脆弱性関連情報の漏洩リスクを高めてしまう点にも考慮する必要がある。米国 CERT/CC<sup>16</sup>では、公表前に重要インフラ等への情報提供が行われていることなどを踏まえ、適切な判断を下す必要がある。

## 2.2.「脆弱性関連情報流通の基本枠組み」の全体像

### 2.2.1.基本方針

以上の前提条件を踏まえ、「脆弱性関連情報流通の基本枠組み」を確立するにあたっては、以下の基本方針に従うことが適当である。

#### **1) 本枠組みの適用範囲を、ソフトウェア製品の脆弱性と、ウェブアプリケーションの脆弱性とする**

本枠組みの適用範囲は、2.1.2に示した通り、その脆弱性が不特定多数のユーザに被害を及ぼしうるという観点から、以下の2つを想定している。

国内で利用されているソフトウェア製品の脆弱性

市販のパッケージソフトウェアや共通に利用されるソフトウェア部品、また組み込みソフトウェ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、不特定多数のユーザに影響が及ぶ。また、共通のモジュールやプロトコル、フォーマット等の実装に脆弱性が発見された場合には、複数の製品に関わるため、影響範囲はさらに広がることになる。

---

<sup>16</sup> Computer Emergency Response Team / Coordination Center : 米国のコンピュータ緊急対応センター

ウェブアプリケーションの脆弱性

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ユーザ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い。

## 2) 脆弱性関連情報の届出を受け付ける機能（受付機関）が必要

脆弱性関連情報の届出先を決め、それを国民に周知することで、脆弱性関連情報が放置されたり、暴露されたりすることを防ぐ効果が期待できる。また、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することで、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ぐ効果が期待できる。

## 3) ソフトウェア製品の脆弱性の公表時期を調整する仕組み（調整機関）が必要

ソフトウェア製品の脆弱性の場合、一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、それを公表するタイミングを調整する必要があり、脆弱性関連情報を効率的に取り扱うためには、その機関を受付期間とは別に設けることが望ましいと考えられる。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。

## 4) 対策方法や届出件数等の統計データを集積・公表する機能が必要

システム構築支援事業者やインターネットアクセスプロバイダ、ユーザ等に対し脆弱性の対策方法の周知徹底を図るため、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を提供することが有用である。

また、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・公表を行うことにより、その実態を明らかにして、関係者が脆弱性のリスクを適正に評価できるよう促すことができる。

## 5) 「脆弱性関連情報の流通制御」と「対策方法の適用の迅速化」を両立

脆弱性関連情報は機密保持を前提として必要な関係者にのみ知らせる必要がある。その一方、対策方法についてはユーザへの迅速な適用を進めることが求められる。それらを両立するためには、機密保持を前提とする関係者のグループとそれ以外を分けて、グループ内外の情報の出入りを集約する形が望ましい。すなわち、関係者以外から見える関係者グループの窓口を設け、その窓口が発

見された脆弱性関連情報を届け出たり、その窓口から対策方法を入手できる構造が適当である。具体的には、上記の受付機関に対策方法、届出件数や処理状況に関する統計データの集積・公表機能を集約し、かつ関係者グループの中で調整機関が機能する形が想定される。

## 6) 製品開発者自身による届出も想定

製品開発者は、脆弱性関連情報の入手経路や特徴に応じて、異なる行動が求められる。ケースごとの具体的な行動を整理した結果を表 2-2に示す。

表 2-2 脆弱性関連情報のタイプに応じて製品開発者に望まれる行動

	他社製品にも影響を及ぼし得る脆弱性関連情報の場合	自社製品にのみ影響を及ぼすと認められる脆弱性関連情報の場合
調整機関から通知された脆弱性関連情報の場合	<ul style="list-style-type: none"> <li>・ 自社製品に影響を及ぼすかどうかを分析</li> <li>・ 必要に応じて対策方法作成</li> <li>・ 他社に影響を及ぼすときは調整機関に通知</li> <li>・ 調整機関を通して公表日を他社と調整</li> <li>・ 対策方法を受付機関・調整機関に通知</li> </ul>	<ul style="list-style-type: none"> <li>・ 自社製品に影響を及ぼすかどうかを分析</li> <li>・ 必要に応じて対策方法作成</li> <li>・ 他社との調整なし</li> <li>・ 対策方法を受付機関・調整機関に通知</li> </ul>
自社で発見・取得した脆弱性関連情報の場合（発見者からの直接の通知を含む）	<ul style="list-style-type: none"> <li>・ 脆弱性関連情報を受付機関に届け出る（発見者としての対応）</li> <li>・ 自社内で対策方法作成</li> <li>・ 調整機関を通して公表日を他社と調整</li> </ul>	<ul style="list-style-type: none"> <li>・ 自社内で対策方法を作成</li> <li>・ 対策方法を受付機関・調整機関に通知</li> </ul>

## 7) 個人情報漏洩等の事案が発生した場合、ウェブサイト運営者は事実を公表

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洩等の事案が発生した場合は、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。

上記の方針については、個人情報の保護に関する法律第7条第1項の規定に基づき策定された「個人情報の保護に関する基本方針」（平成16年4月2日閣議決定）では、「6 個人情報取扱事業者等が講ずべき個人情報の保護のための措置に関する基本的な事項」において、「又、事業者において、個人情報の漏えい等の事案が発生した場合は、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ことが重要である。」との記載に則ったもの。また、個人情報漏洩の被害に遭った可能性のある当該個人に対し、その事実を伝えることを求める意見も出たが、そうした新たな行動基準の提案は本研究会の目的に外れると判断した。

## 8) 政府・重要インフラへの優先情報提供を想定

重大な事案については、我が国の社会基盤の維持を図るため、政府・重要インフラに対する対策方法の優先情報提供を可能にする。その場合、例えば関係者との協議・通知を前提とすることで、政府へ情報が集中するのを避けることができる。

検討段階では、政府による情報の独占と誤解される可能性を配慮し、「明記しないことで『優先提供されないことを保証しない』」という案も出たが、最終的には、「政府および重要インフラに優先提供する場合がある」ということを明示した上で、その事実を関係者に示し透明性を確保するという方針を選択した。

## 9) 脆弱性関連情報の公表に係るルールを策定

### 発見者

発見者は、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。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する。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る。

脆弱性情報の届出を自社で受け付けている製品開発者の場合、基本的には製品開発者が脆弱性や対策方法を公表した後であれば、発見者が公表してもかまわないという方針をとっている。また、ルールとして「一定期間公表されない場合は公表を認める」「正当な理由なしに公表できない」等の提案もでた。

### 製品開発者

製品開発者は、脆弱性と対策方法について、調整機関から最初の連絡を行った後、別途定める一定期間後に公表する。ただし、製品開発者の都合等により、相談の上公表日時を変更することがある。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する。

公表までの期間を明示することにより、製品開発者が対応方針について検討する目安になると考えられる。ただし、具体的な日数については製品開発者側の意見を踏まえ設定することが望ましいと判断した。なお、米国 CERT/CC では、製品開発者に対し CERT/CC が最初の連絡を行った後、45 日間で公表することを原則としている。

## 10) 発見者、製品開発者、ウェブサイト運営者が本枠組みに協力する意義を明示

### 発見者

発見者は、本枠組みを活用することで、製品開発者と直接交渉に要する負担を軽減できる上に、適切に対処される可能性が高まる。また、発見者が望む場合、製品開発者による対策方法の公表時に発見者名を付記することを推奨する。

*現在、製品開発者が対策方法の公表時に発見者の氏名を挙げて謝辞を述べることもあり、発見者のインセンティブとして有効と見られている。*

### 製品開発者、ウェブサイト運営者

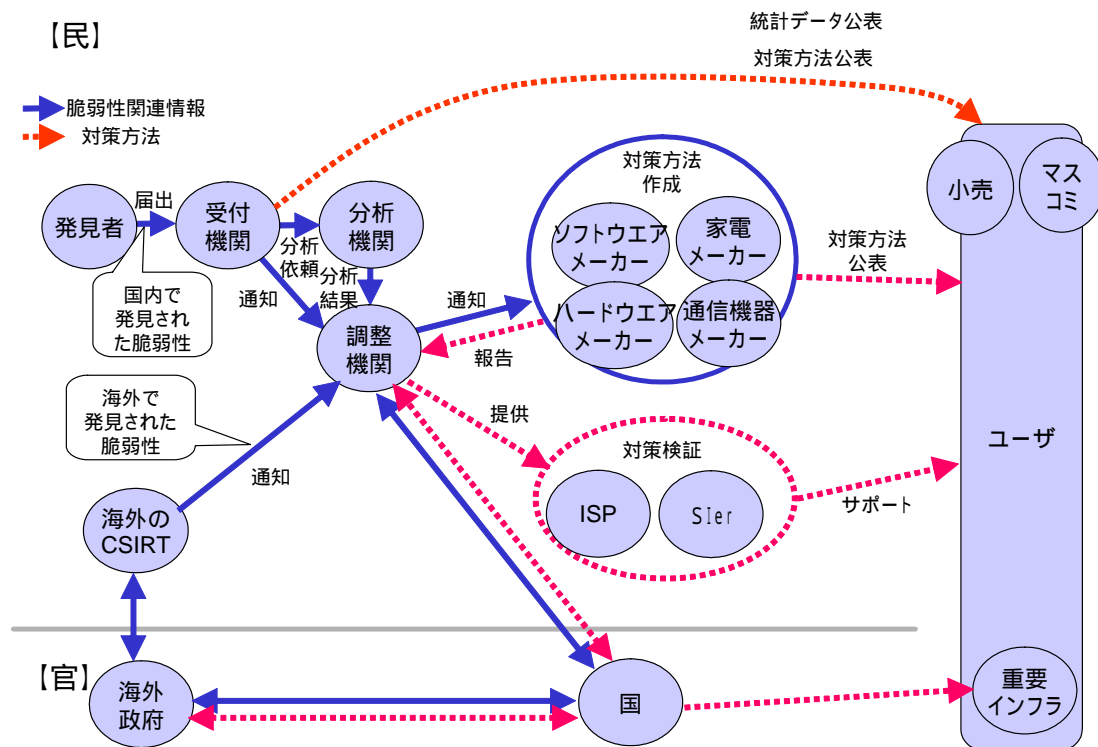
製品開発者やウェブサイト運営者は、本枠組みを活用することで、脆弱性関連情報を適切に入手することができる。また、本枠組みに沿って適切に行動することにより、万一裁判等になった場合にも、その心証が比較的良くなる可能性がある。

*製品開発者やウェブサイト運営者の協力を得るためには、脆弱性に積極的に対処するよう経営者層の意識を変えていく必要があるとの指摘が出ている。*

## 2.2.2. 「基本枠組み」の全体像

2.2.1の基本方針を踏まえ、以下、「脆弱性関連情報流通の基本枠組み」の全体像を提示する。

### <ソフトウェア製品の脆弱性の場合>



### <ウェブアプリケーションの脆弱性の場合>

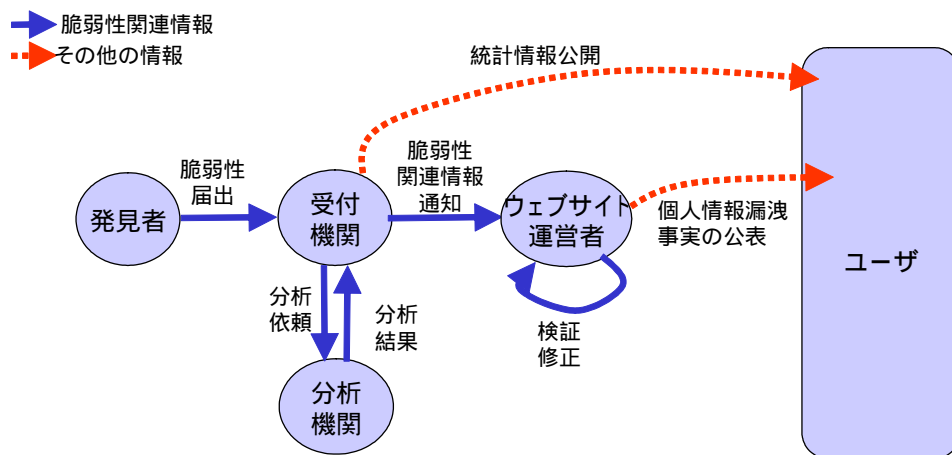


図 2-1 想定される脆弱性関連情報流通の機能構成

#### (1) ソフトウェア製品の脆弱性についての方針

情報の発信源に沿って、発見者からの届出と、海外 CSIRT からの連絡のそれぞれの方針が必要である。

### 発見者からの届出

ソフトウェア製品の脆弱性が発見者からの届出があった場合の方針は次の通りとする。

情報源が発見者の場合、受付機関に脆弱性関連情報の届出がなされ、調整機関を介して当該脆弱性関連情報に関連すると予想される製品開発者に提供される。製品開発者はその影響を検証し、その結果をフィードバックするとともに、対策方法の策定についてのスケジュールを調整機関と相談する。

- ・ 第三者からの届出を受け付ける受付機関、製品開発者と調整を行う調整機関を設置する
- ・ 違法な手段で発見又は取得された届出であることが明白な場合は原則として処理しない
- ・ 調整機関は、国内の関係する製品開発者を特定し、製品開発者に連絡する
- ・ 調整機関は、当該脆弱性関連情報に関連する製品開発者が複数となる場合も想定し、予め製品開発者リストを整備しておく
- ・ 製品開発者と調整機関は、両者が連携し、対策方法策定方針（主として対策方法策定および公表に係わるスケジュール）を決定する
- ・ 製品開発者は、対策方法策定方針に則り、対策を策定する
- ・ 製品開発者と受付機関および調整機関は、対策方法策定後に、脆弱性関連情報と対策方法を公表する
- ・ 公表以前は、発見者、受付機関、調整機関、製品開発者は、脆弱性関連情報が漏洩することを防止する。
- ・ 受付機関は、重大な事案の際、関係者の了解が得られている場合は、政府や重要インフラに対して、公表前に優先的に情報提供を行う
- ・ 受付機関は、届出件数や処理状況等に関する統計情報を公表する

### 海外 CSIRT からの連絡

海外 CSIRT から脆弱性関連情報の連絡を受けた場合の方針は、以下の通りである。

情報源が海外の CSIRT の場合、脆弱性関連情報が調整機関に通知され、調整機関から当該脆弱性関連情報の影響が予想される製品開発者に提供される。製品開発者はその影響を検証し、その結果をフィードバックするとともに、対策方法の策定についてのスケジュールを調整機関と相談する。

- ・ 海外 CSIRT からの連絡の受付は、調整機関が行う
- ・ 調整機関は、国内の関係する製品開発者を特定し、製品開発者に脆弱性関連情報を連絡する
- ・ 調整機関は、当該脆弱性関連情報に関連する製品開発者が複数となる場合も想定し、予め製品開発者リストを整備しておく
- ・ 調整機関は、海外 CSIRT と製品開発者との間で、対策方法策定方針に係わる調整を一括して行う
- ・ 製品開発者は、調整機関の仲介により策定された対策方法策定方針に則り、対策方法を策定する
- ・ 製品開発者は、海外 CSIRT や他の関連製品開発者と同時に、脆弱性と対策方法を公表する

## (2) ウェブアプリケーションの脆弱性についての方針

ウェブアプリケーションの場合の脆弱性関連情報流通の基本方針は、以下の通りである。

発見者から受付機関に脆弱性関連情報の届出がなされ、受付機関が当該ウェブサイト運営者に通知する。

- ・ 脆弱性関連情報の提供元は、第三者たる発見者を想定している
- ・ 違法な手段で発見又は取得された届出であることが明白な場合は原則として処理しない（不正アクセス禁止法等との関係についての考察を 4.4.3 に示す）
- ・ 受付機関は、当該ウェブサイトの運営者に脆弱性関連情報を連絡する
- ・ 受付機関は、必要と判断し、ウェブサイト運営者の許可があれば、分析機関にて、脆弱性関連情報を分析することができる
- ・ ウェブサイト運営者は、脆弱性関連情報の影響範囲を見据えた上で、修正を行い、受付機関にその旨を報告する
- ・ ウェブサイト運営者は、個人情報漏洩があれば、事実関係等を公表する
- ・ 受付機関は、届出件数や処理状況等に関する統計情報を公表する

### 2.2.3. 実現に向けた課題

上に示した「脆弱性関連情報流通の基本枠組み」の実現に向けて対処すべき課題として以下の点が挙げられる。

#### (1) 「基本枠組み」の各役割を担う主体の特定と不足する機能の付加

まず、2.2.2に示した情報の流れを実現するための体制整備が必要になる。すなわち、現状を踏まえつつ、製品開発者が脆弱性に迅速に対応できるようにするためには、関係者がどのような役割を担う形が適当か、新たに必要な機能は何かを明らかにすることが重要である。特に、脆弱性や攻撃方法に関しては関係者内に限定して流通させ、かつ対策方法は一般ユーザに広め対策をとらせる仕組みが求められる。

例えば、米 CERT/CC や英 UNIRAS<sup>17</sup> といった海外 CSIRT からの脆弱性に関する情報は、現在 JPCERT/CC が日本の窓口として受け取り、国内の製品開発者に提供している。ただし、そうした脆弱性の情報に対応する組織体制を社内に整備できている国内の製品開発者はほとんどなく、JPCERT/CC も人対人の信頼関係に依存して情報提供先を確保しているのが現状である。しかし、本来は製品開発者各社が脆弱性への対処を業務として認識し、機密保持を前提として、担当者の交替等に左右されない社内体制を整えることが望ましい。

これについては、次章（第3章）で明示する。

#### (2) 「基本枠組み」の制度的担保

第三者が脆弱性関連情報を発見した際の、発見者、受付機関、調整機関、製品開発者やウェブサイト運営者の取るべき対応を明示したルールを策定し、関係者の行動を規定するための制度的担保が必要である。発見された脆弱性が放置されたり暴露されることなく、適切に対処されるようにするために必要なルールであり、発見者の届出を受け入れ、製品開発者やウェブサイト運営者の対応を促す影響力を持つものであることが期待される。

これについては、第4章で明示する。

#### (3) ユーザのサポートのあり方

ユーザと直接接するシステム構築支援事業者（システムインテグレータ）やシステム運用・保守事業者は、製品開発者が公表した対策方法を手に入れ、それをユーザの IT 環境に適用することを促進する取り組みが求められる。ただし、パ

---

<sup>17</sup> Unified Incident Reporting and Alert Scheme：英国のインシデント対応組織

ッチ等の適用が他のアプリケーションに深刻な影響を及ぼすこともあるため、システム構築支援事業者やシステム運用・保守事業者は企業ユーザに対する対策方法の適用に際し、十分な検証が必要となる。

また、システム構築支援事業者やシステム運用・保守事業者だけでなく、一般ユーザに対しては小売店やマスコミの役割も極めて重要である。そこで、NPO 日本ネットワークセキュリティ協会（JNSA）、Telecom-ISAC Japan<sup>18</sup>等を中心とする「インターネットセキュリティ対策推進協議会（仮称）」（平成16年2月3日発表）では、小売店やマスコミも含めた一般ユーザへの脆弱性対策の適用を促すしくみづくりをめざして検討が進められている。

例えば、国内で利用されているソフトウェアや装置を対象とする脆弱性情報並びに対策情報が散々しているとの問題意識から、国内の各製品開発者が提供する対策情報や更新情報を取りまとめたサイトを構築するプロジェクト「JPCERT/CC Vendor Status Notes（JVN）」が進められている。

なお、将来的には、社会基盤を支える重要インフラにおいて、優先情報提供も含めた脆弱性対策の迅速化・効率化のため、対策方法を共有・適用する業種ごとの連携体制の整備が望まれる。

本研究会では、まず、脆弱性の発見から対策策定・公表に至る情報流通の基本枠組みの構築をめざすこととし、以降の章では基本枠組みを実現するための(1)体制整備及び(2)制度的担保に焦点を絞ることとする。

本研究会で提言している脆弱性関連情報流通の基本枠組み実現のための体制や制度が(3)ユーザサポートの取り組みと連携して、発見から対策適用までの一貫した流れを確立することは極めて有意義であるといえよう。

---

<sup>18</sup> 通信サービスの提供を妨げる各種インシデントを収集・分析し、その分析結果を会員間で共有することにより、インシデントに対する強固な情報通信基盤の提供をめざすために設立されたISPの会員制組織

### 3. 「脆弱性関連情報流通の基本枠組み」を担う主体と枠組みの詳細

#### 3.1. 「基本枠組み」の各役割を担う主体の特定

「脆弱性関連情報流通の基本枠組み」を支える主な部分は、現在有する機能と今後の進むべき方向性を総合し、以下のように独立行政法人情報処理推進機構（IPA）及び有限責任中間法人 JPCERT コーディネーションセンター（JPCERT/CC）が分担することが適当である。

#### 1) 製品の脆弱性に関する発見者からの届出受付は IPA に一元化（「受付機関」は IPA）

IPA は、これまでもコンピュータウイルス、コンピュータ不正アクセスの届出受付として実績を積んでいることから、本件についても受付機関としての役割を担うのに適している。

#### 2) 海外 CSIRT からの情報は、既存のルート（JPCERT/CC）で対応

JPCERT/CC は、米 CERT/CC や英 UNIRAS との関係を築き、それらから提供された脆弱性関連情報の国内流通について実績を積んでいることから、それを継続・発展させていく形が適当である。

#### 3) 脆弱性関連情報の流通の要は JPCERT/CC（「調整機関」は JPCERT/CC）、対策方法の集積・開示は IPA が主担当

機密性が要求される脆弱性や攻撃方法の情報の流通については、これまで実績のある JPCERT/CC が製品開発者との協力関係を強化していく形で進めることが適当である。一方、対策方法を集約し、広く社会に提供していくことを考えると、独自の脆弱性分析機能を有し、公的性格の強い IPA が対策方法を集積・開示することが適当である。なお、IPA は影響度検証、脆弱性検証ツールの作成等の分析を行い、JPCERT/CC、製品開発者を支援する。

この前提として、IPA - JPCERT/CC 間は綿密な情報共有を実現すること、JPCERT/CC は製品開発者と守秘義務付きの情報共有を契約 / 同意書に則った形で実現すること、IPA は対策方法をデータベース化して開示することが必要になる。

#### 4) 対策方法の優先提供についても考慮

すべての製品開発者にとってではなく、すべての事案についてではないが、重大な影響が予想される場合には、政府や重要インフラに対し対策方法の優先提供を行う可能性についても考慮する。

優先提供する情報として、例えばパッチの 版、対策準備要請等が想定される。優先提供先にはシステム構築/運用支援者(システムインテグレータ)ではなく、政府・重要インフラの運営者(もしくは内閣官房経由)が想定される。

上記3.1全体の総括を表 3-1に示す。

表 3-1 脆弱性関連情報流通の基本枠組みを支える役割分担

対象	受付	調整	分析・対策策定	公表	情報利用
ウェブアプリケーションの脆弱性	<p>IPA</p> <ul style="list-style-type: none"> <li>・一次受付</li> <li>・スクリーニング</li> <li>・受理 / 不受理通知</li> <li>・当該ウェブサイト運営者への通知</li> <li>・統計データ化</li> </ul>		<p>当該ウェブサイト運営者</p> <ul style="list-style-type: none"> <li>・脆弱性の検証</li> <li>・対策の実施</li> <li>・IPA へ完了報告 (IPA が必要と判断した場合、当該ウェブサイト運営者の許可を得て分析)</li> </ul>	<p>当該ウェブサイト運営者</p> <ul style="list-style-type: none"> <li>・個人情報漏洩の可能性がある場合には事実関係を公表</li> <li>IPA</li> <li>・統計データの集積・公表</li> </ul>	<p>ウェブサイト運営者</p> <ul style="list-style-type: none"> <li>・統計データを踏まえ、ウェブアプリケーションの脆弱性の実態について把握</li> </ul>
ソフトウェア製品の脆弱性 (発見者からの届出)	<p>IPA</p> <ul style="list-style-type: none"> <li>・一次受付</li> <li>・スクリーニング</li> <li>・受理 / 不受理通知</li> <li>・統計データ化</li> </ul>	<p>JPCERT/CC</p> <ul style="list-style-type: none"> <li>・配信先の抽出・通知</li> <li>・公表スケジュールの管理</li> <li>・IPA の分析成果を当該製品開発者に提供</li> </ul>	<p>当該製品開発者</p> <ul style="list-style-type: none"> <li>・対策方法の策定 (ワークアラウンド、パッチ、ver-up 等)</li> <li>IPA</li> <li>・脆弱性分析 (影響範囲の検証、リスク分析、脆弱性検証ツールの作成等)</li> </ul>	<p>当該製品開発者</p> <ul style="list-style-type: none"> <li>・スケジュールに沿って対策方法を公表</li> <li>IPA、JPCERT/CC</li> <li>・対策方法を公表</li> <li>・IPA が DB 登録</li> <li>・IPA が統計データを集積・公表</li> </ul>	<p>製品開発者</p> <ul style="list-style-type: none"> <li>・JPCERT/CC から脆弱性関連情報の提供を受けて自社製品への影響を検証、報告</li> <li>・機密保持が前提</li> <li>政府・重要インフラ事業者</li> <li>・IPA から公表前の対策方法や準備要請情報の提供を受けて対処</li> <li>・機密保持が前提</li> </ul>
ソフトウェア製品の脆弱性 (海外 CSIRT からの連絡)		<p>JPCERT/CC</p> <ul style="list-style-type: none"> <li>・海外 CSIRT からの受信</li> <li>・配信先の抽出・通知</li> <li>・公表スケジュールの管理</li> <li>・IPA の分析成果を当該製品開発者に提供</li> <li>・情報源への報告</li> </ul>	<p>当該製品開発者</p> <ul style="list-style-type: none"> <li>・対策方法の策定 (ワークアラウンド、パッチ、ver-up 等)</li> <li>IPA</li> <li>・脆弱性分析 (影響範囲の検証、リスク分析、脆弱性検証ツールの作成等)</li> </ul>	<p>当該製品開発者</p> <ul style="list-style-type: none"> <li>・スケジュールに沿って対策方法を公表</li> <li>IPA、JPCERT/CC</li> <li>・対策方法を公表</li> <li>・IPA が DB 登録</li> <li>・IPA が統計データを集積・公表</li> </ul>	<ul style="list-style-type: none"> <li>システム構築者/運用者、ISP(Telecom-ISAC Japan)</li> <li>・公表後の対策方法を受けてユーザに対策実施</li> <li>・JNSA 等の活動と連携</li> <li>IPA の DB を活用</li> </ul>

### 3.2. 「基本枠組み」の詳細

3.1で示したように、IPA 及び JPCERT/CC がそれぞれ、受付機関、調整機関等の役割を担うことを前提とすると、本「基本枠組み」の詳細は以下のように構築することが適当である。

#### 3.2.1. ソフトウェア製品の脆弱性

以下の図 3-1にソフトウェア製品の場合の情報流通の全体像を示す。

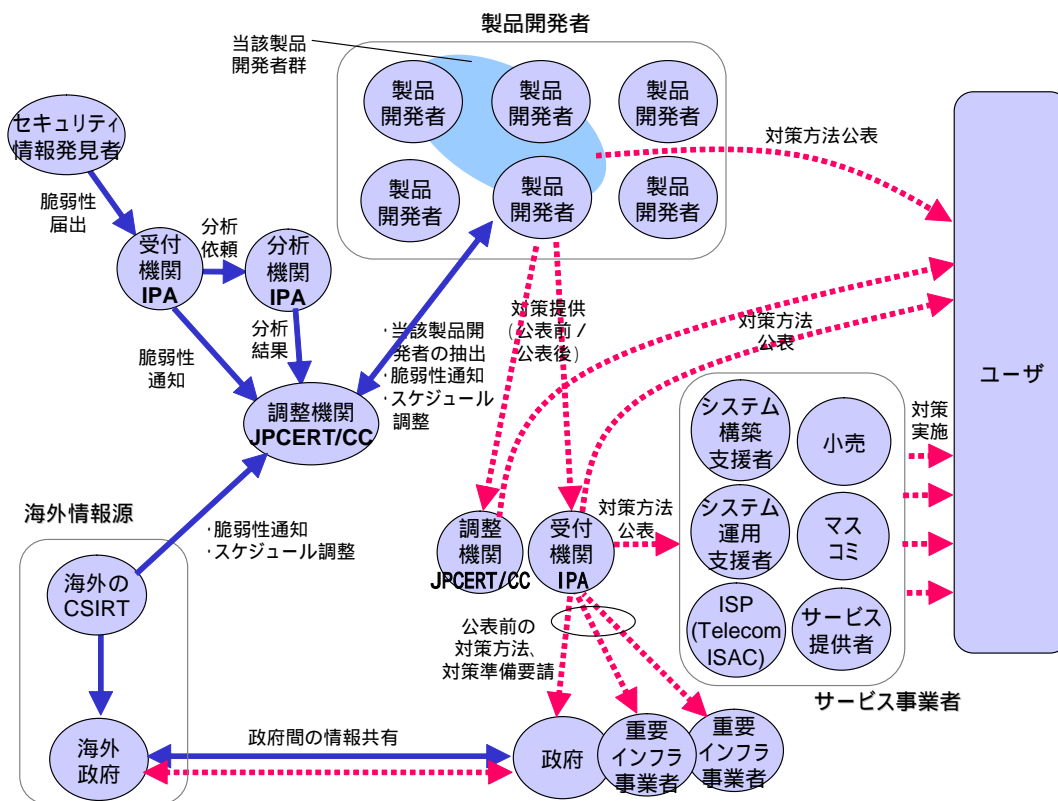


図 3-1 ソフトウェア製品の場合の脆弱性関連情報流通体制

上記に関して、以下で、発見者から脆弱性関連情報を受け取る場合と、海外CSIRT から脆弱性関連情報を受け取る場合に分けて述べる。

## (1) IPA が発見者から脆弱性関連情報を受け付ける場合

### 発見者

ソフトウェア製品の脆弱性の発見者は、IPA に脆弱性関連情報を届け出ることが可能である。この際に、発見者は、直接製品開発者に届け出ることもあり得、それに関しては、特に妨げない。

なお、発見者は、違法な手段で脆弱性関連情報を取得しないことが肝要である。

### IPA

IPA は、発見者からの脆弱性関連情報の受付を行い、必要であれば IPA 内の脆弱性分析機関にて分析を行う。受付の際に、脆弱性関連情報の取得手段は問わないが、明らかに違法な手段で取得したことが明白な届出については、対応しないことがある。また、IPA が受け取った場合でも、発見者の脆弱性関連情報取得手段を適法であると判断したわけではない。

IPA は、脆弱性関連情報に関し、過去の脆弱性関連情報との峻別を行うために、脆弱性関連情報データベースの整備を行う必要がある。バグ等の情報ではなく、かつ過去の脆弱性関連情報に合致しない新規の脆弱性関連情報である場合、速やかに JPCERT/CC に通知する。

IPA は、JPCERT/CC に通知した後、必要であれば脆弱性分析機関にて脆弱性関連情報の分析を続行する。さらに、製品開発者が対策方法を策定した後に、製品開発者から対策方法を受領する。この時に当該脆弱性関連情報が重大な影響を及ぼしうる場合、関係者の合意が得られれば、IPA は、政府や重要インフラに脆弱性関連情報と対策方法を優先的に情報提供する。

通信インフラに影響する脆弱性の対策方法については、Telecom-ISAC Japan に対し情報を提供することが有効である。

さらに、IPA は、届け出られた脆弱性関連情報に関して、少なくとも 1 年に一度程度の割合で、届出件数や処理状況等に関する統計情報を公表する。

### JPCERT/CC

JPCERT/CC は、IPA から脆弱性関連情報を受け取る。脆弱性関連情報を受け取ったら速やかに、関連する製品開発者全てに脆弱性関連情報を送信する。この際には、以下の点に関する留意が必要である。

- ・ 事前に、製品開発者のリスト（コンタクトパーソンを含む）を構築しておくこと

- ・ 脆弱性関連情報の送信に際しては、各製品開発者と個別またはそれに準ずる方法で、秘密保持契約（nondisclosure agreement (NDA) もしくはそれに類するもの）を締結すること
- ・ 秘密保持契約の内容は、JPCERT/CC と製品開発者が合意した日時まで製品開発者外へ脆弱性関連情報を開示しないことが中心となる

JPCERT/CC は、製品開発者と連携し、対策方法策定方針（対策方法策定スケジュールおよび公表スケジュール）を作成する。そして、その対策方法策定方針に則り作業が進められていることを随時確認する。なお、対策方法策定に際しては、全ての関連製品開発者が同時に脆弱性と対策方法を公表するように、調整することが重要である。

JPCERT/CC は、製品開発者が対策方法を策定後、対策方法を受け取り、全ての関連製品開発者と同時に、脆弱性と対策方法を公表する。

#### 製品開発者

製品開発者は、JPCERT/CC から脆弱性関連情報を受け取る。その際に、秘密保持契約を締結することを前提とする。そして、その際に、製品開発者は、JPCERT/CC と連携し、対策方法策定方針を作成する。対策方法策定方針における対策方法策定スケジュールと公表スケジュールに則り作業を進める。なお、公表までのスケジュールは、原則として JPCERT/CC が製品開発者に通知した後、あらかじめ対策方法策定期限として定められた期間を設定することとなるが、製品開発者と JPCERT/CC の相談により変更する等柔軟に対応することが可能である。

製品開発者は、上記のスケジュールに則って作業を進めるが、作業上の技術等の問題から、スケジュールの見直しが必要となった場合には JPCERT/CC と連携し、適宜対策方法策定方針を改訂する。

製品開発者は、対策方法のうち、回避方法策定が完了した後、脆弱性関連情報と回避方法を公表する。また、公表は、関連する全製品開発者が同時に行うことが必須である。

修正方法に関しては、必ずしも回避方法と同時に公表する必要は無いが、可能な限り迅速かつ適切な対応が、製品開発者には求められる。

製品開発者は、公表前には、社外だけではなく社内でも当該製品に関係の無い部署に脆弱性関連情報を開示することは控えなければならない。また、一般に、一つの脆弱性関連情報に複数の製品開発者が関係する場合、談合のような見方をされることのないよう、製品開発者間での当該脆弱性関連情報に係わる直接の連絡は控えるべきであり、こうした情報交換は JPCERT/CC を介して行うことが適切である。

## (2) JPCERT/CC が海外 CSIRT から脆弱性関連情報を受け取る場合

### JPCERT/CC

JPCERT/CC は、海外 CSIRT から脆弱性関連情報を受け取る。脆弱性関連情報を受け取ったら速やかに、関連する製品開発者全てに脆弱性関連情報を送信する。この際には、以下の点に関する留意が必要である。

- ・ 事前に、製品開発者のリスト（コンタクトパーソンを含む）を構築しておくこと
- ・ 脆弱性関連情報の送信に際しては、各製品開発者と個別またはそれに準ずる方法で、秘密保持契約（nondisclosure agreement、NDA もしくはそれに類するもの）を締結すること
- ・ 秘密保持契約の内容は、JPCERT/CC と製品開発者が合意した日時まで製品開発者外へ脆弱性関連情報を開示しないことが中心となる

JPCERT/CC は、製品開発者と連携し、対策方法策定方針（対策方法策定スケジュールおよび公表スケジュール）を作成する。この際には、海外の CSIRT が既に公表スケジュールを決定している場合、それに従うことになる。海外 CSIRT と製品開発者の間で調整の余地がある場合は調整を行う。そして、その対策方法策定方針に則り作業が進められていることを随時確認する。なお、対策方法策定に際しては、全ての関連製品開発者が同時に脆弱性関連情報と対策方法を公表するように、調整することが重要である。

JPCERT/CC は、製品開発者が対策方法を策定後、対策方法を受け取り、海外 CSIRT に報告する。また、この際に、海外 CSIRT および製品開発者の了解が得られる場合、公表前に IPA に対策方法を連絡する。

### IPA

IPA は、JPCERT/CC から脆弱性関連情報の提供を受けた場合、IPA 内の脆弱性分析機関にて分析を行う。

また、IPA は、当該脆弱性関連情報が重大な影響を及ぼしうる場合、海外 CSIRT および製品開発者の了解が得られるのであれば、公表前の対策方法の情報を政府や重要インフラに優先的に提供する。

さらに、IPA は、届け出られた脆弱性関連情報に関して、少なくとも 1 年に一度程度の割合で、届出件数や処理状況等に関する統計情報を公表する。

### 製品開発者

製品開発者は、JPCERT/CC から脆弱性関連情報を受け取る。その際に、秘密保持契約を締結することを前提とする。そして、その際に、製品開発者は、JPCERT/CC と連携し、対策方法策定方針を作成する。対策方法策定方針における対策方法策定スケジュールと公表スケジュールに則り作業を進める。なお、ガイドラインにおいて、公表までのスケジュールは、原則として JPCERT/CC が製品開発者に通知した後、あらかじめ対策方法策定期限として定められた期間を設定することになるが、海外 CSIRT が既に公表に係わるスケジュールを決定している場合、それに従うことになる。変更の余地がある場合、製品開発者は JPCERT/CC を介して、海外 CSIRT との折衝を行う。

製品開発者は、上記のスケジュールに則って作業を進めるが、作業上の技術等の問題から、スケジュールの見直しが必要となった場合には JPCERT/CC と連携し、適宜対策方法策定方針を改訂する。

製品開発者は、対策方法のうち、回避方法策定が完了した後、脆弱性と回避方法を公表する。また、公表は、関連する全製品開発者が同時に行うことが必須である。

修正方法に関しては、必ずしも回避方法と同時に公表する必要は無いが、可能な限り迅速かつ適切な対応が、製品開発者には求められる。

製品開発者は、公表前には、社外だけではなく社内でも当該製品に関係の無い部署に脆弱性関連情報を開示することは控えなければならない。また、一般に、一つの脆弱性関連情報に複数の製品開発者が関係する場合、談合のような見方をされることのないよう、製品開発者間での当該脆弱性関連情報に係わる直接の連絡は控えるべきであり、こうした情報交換は JPCERT/CC を介して行うことが適切である。

なお、海外 CSIRT が、脆弱性関連情報の取り扱いに関して取り決めを行っている場合、上記の記述よりそれに従うべきである。

### 3.2.2. ウェブアプリケーションの脆弱性

ウェブアプリケーションの場合、関係者は、発見者・IPA（受付機関、分析機関）・ウェブサイト運営者となる。

全体像を、図 3-2に示す。

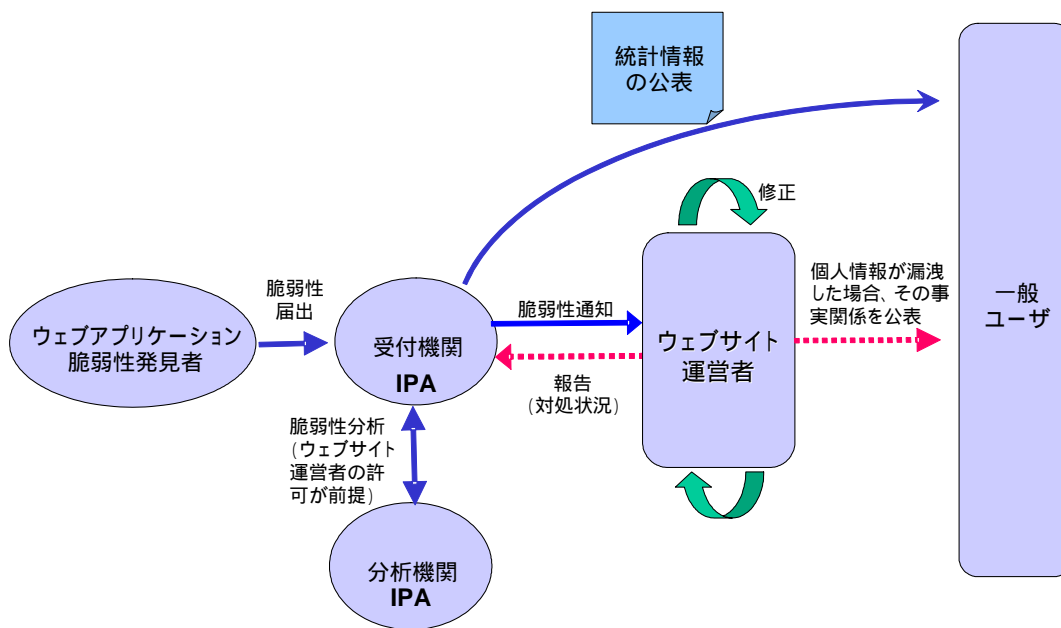


図 3-2 ウェブアプリケーションの場合の脆弱性関連情報流通体制

### 発見者

発見者は、IPA に脆弱性関連情報を届け出ることが可能である。この際に、発見者は、直接ウェブサイト運営者に届け出ること有り得、それに関しては、特に妨げない。

なお、発見者は、違法な手段で脆弱性関連情報を取得しないことが肝要である。

検討の中では、不正アクセス禁止法に抵触しない脆弱性の発見があり得るのかとの質問も出された。この点については4.4.3(1) に整理した。

### IPA

IPA は、発見者からの脆弱性関連情報の受付を行い、IPA が必要と判断しウェブサイト運営者が許可すれば IPA 内の脆弱性分析機関にて分析を行う。受付の際に、脆弱性関連情報の取得手段は問わないが、明らかに違法な手段で取得したことが明白な脆弱性関連情報については処理しないことがある。また、IPA が受け取った場合でも、発見者の脆弱性関連情報取得手段を適法であると判断したわけではない。

IPA は、ウェブサイト運営者に通知後、IPA が必要と判断しウェブサイト運営者が許可すれば脆弱性分析機関で脆弱性関連情報の分析を行う。

さらに、IPA は、届け出られた脆弱性関連情報に関して、少なくとも 1 年に一度程度の割合で、届出件数や処理状況等に関する統計情報を公表する。

### ウェブサイト運営者

ウェブサイト運営者は、IPA から脆弱性関連情報の連絡を受け取ったら、可能な限り迅速に、当該情報の影響範囲を確認することが重要である。

大量の個人情報漏洩するなど重大な影響の可能性が確認された場合、早急にウェブアプリケーションの修正を行うことが必要である。また、修正が完了した段階で、その旨を IPA に報告する。

なお、当該脆弱性が原因で生じたと推定される個人情報漏洩の事実が確認された場合、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ことが求められる。

## 4. 「脆弱性関連情報流通の基本枠組み」を支える制度的担保等

### 4.1. 制度的担保の必要性

本「基本枠組み」を構築する目的の一つは、発見者、受付機関、調整機関、製品開発者、ウェブサイト運営者のそれぞれが適切な行動をとることにより、脆弱性への適切・迅速な対応を実現することにある。しかし、製品開発者やウェブサイト運営者にとってはその対応によって直接的な利益が生じないため、実際には消極的な取り組みに終始し、その結果、そうした問題が放置されることにより、不特定多数のユーザに被害が及ぶ可能性がある。そこで、関係者が脆弱性関連情報に対し適切な行動を促すべく、それぞれの果たすべき役割や望ましい行動基準を明示した制度を導入する必要がある。

また、公的な受付窓口を設置することによって、第三者が発見した脆弱性関連情報を暴露することを防ぐという効果も期待できる。そのためには、脆弱性関連情報の発見者に受付機関の存在を周知する必要があり、制度的な担保が重要な意味を持つ。

なおこの際、脆弱性関連情報が多数届けられ、流通が促進されることを期待しているが、違法な行為による脆弱性関連情報の発見を奨励しているわけではない。

### 4.2. 制度的担保の具体策

まず脆弱性関連情報の発見者に受付機関の存在を周知するとともに、関係者の適切な対応を促す目的を考慮すれば、政府が公的なルールを制定し、その目的や枠組みを広報するとともに、関連業界団体に対しても積極的に協力を呼びかけていくことが適当である。

また、公的なルールと連動する形で、受付機関や調整機関等の役割・機能を規定し、処理の流れを明確化する意図で、民間側のガイドラインを別途策定することが適当である。

したがって、公的ルールは、第三者が脆弱性関連情報を発見し、受付機関に届け出た際の、関係者間の必要最低限の推奨事項を明示するものとなる。また、民間ガイドラインは、第三者が脆弱性関連情報を発見し、IPA に届け出た際の、関係者間のなすべき事項を自ら宣言するものとなる。

それぞれの位置付けを、整理すると表 4-1に示すところとなる。

表 4-1 制度的担保の位置付け

大項目	政府の定める公的ルール	民間ガイドライン
主旨	第三者が脆弱性関連情報を発見し、受付機関に届け出た際の、関係者間の必要最低限の推奨事項を明示	第三者が脆弱性関連情報を発見し、IPA に届け出た際の、関係者間のなすべき事項を自ら宣言するもの
内容上の特徴等	<ul style="list-style-type: none"> <li>・ 受付機関の指定</li> <li>・ 関係者に望まれる行動基準</li> </ul>	<ul style="list-style-type: none"> <li>・ 発見者、製品開発者、ウェブサイト運営者それぞれに係わる法的関連事項の明示</li> <li>・ 製品開発者の脆弱性関連情報公表に関する記載事項</li> <li>・ ウェブサイト運営者の個人情報漏洩時の事実関係公表に関する記載事項</li> </ul>

#### 4.3. 公的ルールと民間ガイドラインのモデル案

本報告書においては、4.2に示した政府の公的ルールと民間ガイドラインのモデル案を提示することとする（資料1及び資料2）。政府及び関係機関においては、今後、本モデル案にしたがって、可及的速やかにこれを提示することが期待される。

#### 4.4. 法的論点

4.3で提示した「公的ルール」及び「民間ガイドライン」のモデル案を前提とし、法的論点を以下の観点から検討した。

- ・ 脆弱性関連情報取扱に係わる公的ルール及び民間ガイドラインの法的位置付け
- ・ 脆弱性関連情報の定義
- ・ 脆弱性関連情報の発見者に係わる論点
- ・ 受付機関および調整機関に係わる論点
- ・ 関連する製品開発者に係わる論点
- ・ 関連するウェブサイト運営者に係わる論点

以下にこれらの検討の結果を述べる。

#### 4.4.1.脆弱性関連情報取扱に係わる文書の法的位置付け

##### (1) 政府の公的ルールの位置付け

政府の公的ルールに関する論点は、強制力の程度である。強制力を明示する場合関係者から、脆弱性関連情報の国による管理であるという批判を浴びる可能性があり、強制力が全く無い場合実際に利用されることがなくなる可能性がある。この両面のバランスを取るために、本案は、「関係者に推奨するものである」ことを主旨で明示している。

##### (2) 民間ガイドラインの位置付け

本ガイドラインは、関係者の連名で発行されることを想定しており、法的強制力は無い。基本的には、政府の公的ルールの存在を前提としており、政府の公的ルールが関係者への推奨事項を前提とした文書であるため、本ガイドラインも同一の前提を有している。内容は、関係者向けに行動の基準を平易に解説したものとなっている。

#### 4.4.2.脆弱性関連情報の定義

「脆弱性」という言葉は、不正アクセス対策基準やコンピュータアクセス対策基準において定義されていない言葉である。「脆弱性」に関しては、以下の視点が必要である。

- 1) プログラムが意図しない動きをすること
- 2) セキュリティに関連するものであること
- 3) 外部からの攻撃を誘発するものであること
- 4) 上記2)および3)に関連する1)を引き起こす要因となるものであること

#### 4.4.3.脆弱性関連情報の発見者に係わる論点

脆弱性関連情報の発見者に係わる論点は、脆弱性関連情報の発見と、脆弱性関連情報の開示に係わる論点に分けて論ずることが可能である。

##### (1) 脆弱性関連情報の発見

脆弱性関連情報の発見に際して、発見者は、以下の法令に関する配慮が必要である。

## 不正アクセス禁止法

ウェブアプリケーションの脆弱性の発見は、不正アクセス禁止法に抵触しないような形で実施する必要がある。以下に不正アクセス禁止法に抵触する行為と抵触しない行為を例示する。

### (ア) 不正アクセス禁止法の条文

発見者の行為に関連が深い不正アクセス禁止法の条文( 第二条および第三条 ) は以下の通りである。

( 定義 )

#### 第二条

この法律において「アクセス管理者」とは、電気通信回線に接続している電子計算機( 以下「特定電子計算機」という。 ) の利用( 当該電気通信回線を通じて行うものに限る。以下「特定利用」という。 ) につき当該特定電子計算機の動作を管理する者をいう。

2 この法律において「識別符号」とは、特定電子計算機の特定利用をすることについて当該特定利用に係るアクセス管理者の許諾を得た者( 以下「利用権者」という。 ) 及び当該アクセス管理者( 以下この項において「利用権者等」という。 ) に、当該アクセス管理者において当該利用権者等を他の利用権者等と区別して識別することができるように付される符号であって、次のいずれかに該当するもの又は次のいずれかに該当する符号とその他の符号を組み合わせたものをいう。

一 当該アクセス管理者によってその内容をみだりに第三者に知らせてはならないものとされている符号

二 当該利用権者等の身体の一部若しくは一部の影像又は音声を用いて当該アクセス管理者が定める方法により作成される符号

三 当該利用権者等の署名を用いて当該アクセス管理者が定める方法により作成される符号

3 この法律において「アクセス制御機能」とは、特定電子計算機の特定利用を自動的に制御するために当該特定利用に係るアクセス管理者によって当該特定電子計算機又は当該特定電子計算機に電気通信回線を介して接続された他の特定電子計算機に付加されている機能であって、当該特定利用をしようとする者により当該機能を有する特定電子計算機に入力された符号が当該特定利用に係る識別符号( 識別符号を用いて当該アクセス管理者の定める方法により作成される符号と当該識別符号の一部を組み合わせた符号を含む。次条第二項第一号及び第二号において同じ。 ) であることを確認して、当該特定利用の制限の全部又は一部を解除するものをいう。

( 不正アクセス行為の禁止 )

#### 第三条

何人も、不正アクセス行為をしてはならない。

2 前項に規定する不正アクセス行為とは、次の各号の一に該当する行為をいう。

一 アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。）

二 アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。次号において同じ。）

三 電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為

#### （イ）抵触する行為

不正アクセス禁止法第三条に抵触する行為の例を以下に列挙する。

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

上記のアクセス制御機能の定義は、第二条第3項にあるが、具体的な技術に関して判例は示されていない。しかし、特定のウェブサイトにアクセスする場合、現時点において法律的判断が困難な行為は、不正アクセス禁止法第三条に抵触すると推察すべきである。

- 2) 例えば、管理者やユーザ本人の了解無く、他人のパスワードを取得し、それを用いて権限なしで、インターネットなどを介してシステムにアクセスした場合には、不正アクセス禁止法に抵触する

社会通念上、パスワードの設定はアクセス制御機能の設定に該当することは当然であると推察されるため、上記は明確に不正アクセス禁止法第三条に抵触する。

#### （ウ）抵触しないと推察される行為

不正アクセス禁止法に抵触しないと推察される行為を以下に列挙する。

- 1) 当該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には抵触しないと推察される
- 2) Web ページのデータ入力欄に HTML のタグを含む文字列を入力したところ、入力した文字列がそのまま表示された。この段階ではアクセス制御機能の制限を回避するに至らなかったが、悪意ある者に別の文字列を入力されれば、このサイトにセキュリティ上の問題が引き起こされかねないと予想できた場合には抵触しないと推察される  
(ただし、悪質な結果を招くタグを人にアクセスさせることを意図して公衆が閲覧する場書き込み放置した場合等には、刑法の不正指令電磁的記録作成罪に触れる可能性がある。不正指令電磁的記録作成罪は「犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案」にて規定(4.4.3(1) 3)参照))
- 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には抵触しないと推察される(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得る。)

3)については、不正アクセス行為に該当するが故意がないケース(この場合の「故意」とは、アクセス制御による制限を免れる目的であることをさす。故意が認められなければ罰せられることがない)であり、上記の枠の例としては適当でないとの意見もあった。本報告書では、発見者の届出が望まれるケースの例示として、本節で紹介することとした。ただし、上記のような形で、脆弱性の発見を目的とした検査を、ウェブサイト運営者の許可なく実施することを奨励するものではない。

## 刑法

刑法に関しては、発見者は、以下の点において留意すべきである。

- 1) 故意にサーバの機能や性能の異常を来たそうとして何らかの行為をなし、コンピュータの性能を低下させたりした場合、刑法上の偽計(もしくは威力)業務妨害罪に抵触する可能性がある

発見者が脆弱性の発見や確認等の目的のために、故意にサーバの機能や性能を低下させた場合、偽計業務妨害罪となる可能性がある。

- 2) 上記 1)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る

上記 1)の行為により、サーバのディスク上のデータが消去される等機能や性能に係わる被害が大きい場合、電子計算機損壊等業務妨害罪にも抵触する可能性がある。

- 3) 悪意を持って攻撃コードやコンピュータウイルスを作成すると、「犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案」(平成16年2月20日閣議決定され、国会に上程)にて規定されている不正指令電磁的記録作成罪(新設)に触れる可能性がある

研究目的は悪意ではないが、発見者は注意が必要である。

#### 電波法

電波法に関しては、暗号化されている無線通信を傍受し、復号する行為(無線LANのWEPキーの解読など)は電波法に触れる可能性がある点に留意する必要がある。

本件は、第159回通常国会で審議中の、「電波法及び有線電気通信法の一部を改正する法律案」(平成16年2月17日閣議決定され国会に上程)第109条の2において規定されている、「暗号通信を傍受した者又は暗号通信を媒介する者であつて当該暗号通信を受信したものが、当該暗号通信の秘密を漏らし、又は窃用する目的で、その内容を復元したときは、一年以下の懲役又は五十万円以下の罰金に処する。」に該当する。

#### 著作権法

研究会においては、リバース・エンジニアリングが著作権法または特許法を侵害する可能性があるとの議論があったが、結果的には民間ガイドラインに留意事項として明記していない。

一般に、ソフトウェアのライセンス契約においては、ソフトウェアの著作権を保護するために、リバース・エンジニアリングを禁止する条項が設置される

ことがある。リバース・エンジニアリングに関しては、逆アセンブル、逆コンパイルといった解析の過程でプログラムの複製物が作成されることから、著作権侵害に該当するかという議論が従前よりなされている。通説は、技術の研究・解析は技術の進歩に資するものであること等を理由に、著作権侵害性を否定する。そのため、ライセンサーはライセンス契約中にリバース・エンジニアリング禁止条項を設け、特約をもって対処しようとしているが、当該条項の有効性に関しては、独占禁止法に抵触するとの問題提起がなされている。この点、平成14年3月20日に公正取引委員会より公表された「ソフトウェアライセンス契約等に関する独占禁止法上の考え方 - ソフトウェア独占禁止法に関する研究会中間報告書 - 」においては、ソフトウェアの製品市場、技術市場におけるライセンシーの研究開発活動が阻害され、ハードウェアの製品市場等における公正な競争が阻害される場合には、不公正な取引方法（具体的には一般指定13項拘束条件付取引）に該当し、違法になるとの見解が示されている

以上の検討により、民間ガイドラインにおいて、リバース・エンジニアリングに係わる注意喚起を行うことは不相当と考え、記載を外した。

#### その他関連する法規

発見者による行為が通信の秘密を侵した場合、以下に抵触する。

- 1) 憲法21条2項後段は、「通信の秘密は、これを侵してはならない」と定めている。
- 2) 「通信の秘密」の内容として、一般には「通信」の「秘密」にかかる事実を「通信当事者以外の第三者が積極的意思をもって知得してはならず」「第三者にとどまっている秘密を、漏洩（他人が知りうる状態にしておくこと）することおよび窃用（本人の意思に反して自己または他人の利益のために用いること）してはならない」の二つの意味を包含するものにとらえられている。
- 3) 電気通信事業法4条は、「電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。」との記述がある。
- 4) 有線電気通信法9条は「有線電気通信（電気通信事業法第四条第一項又は第九十条第二項の通信たるものを除く。）の秘密は、侵してはならない。」として、それぞれ通信の秘密の保護を定めている。
- 5) 電気通信事業者の取り扱うもの以外の無線通信については、電波法が、59条において、「特定の相手方に対して行われる無線通信・・・を傍受してその存在もしくは内容を漏らし、又はこれ窃用」することを禁じている。特に、無線通信による暗号の復号に関しては、上記(c)の通りである。

## (2) 脆弱性関連情報の開示

脆弱性関連情報の開示に関しては、憲法第21条の表現の自由との係わりを検討する必要がある。

憲法第21条第1項において、「集会、結社、および言論、出版その他一切の表現の自由は、これを保障する」と記されている。脆弱性関連情報に関しても、それ自体を公表することは、表現の自由として、憲法上、保護されるべき権利として保証される。

しかし、公共の福祉の下、ある程度の表現の自由が制限されるとの議論もあり、本文書はこの点を強調し、発見者に対する協力を求めているものといえる。さらには、脆弱性関連情報を公表することによる製品開発者に対する名誉毀損や信用毀損といった観点での注意も必要である。具体的には、以下の通りである。

- 1) 脆弱性についての調査・報告は、その率直な交換により、ソフトウェ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る
- 2) しかしながら、その情報については、悪用というデメリットがあるので、その点についての十分な配慮がなされるべきであり、その一つの方向性を提唱するのが、この民間ガイドラインといえる
- 3) また、情報自体そのような性格をもつので、発見者についても脆弱性関連情報の管理について真摯な態度が必要とされる
- 4) そのような真摯な態度を保つ限り脆弱性関連情報についての調査・報告は、社会的に有用なものと考えられる
- 5) 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、上述の限りではなく、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る
  - a) 脆弱性関連情報の公表は、その情報の内容が真実と異なることを知っていた場合、あるいは、真実である場合であっても、特定人の名誉を毀損する意図で公表がなされ、かつ、公共の利益と無関係である場合には、刑法の名誉毀損罪に触れる可能性がある
  - b) 特定人の信用を毀損する意図で事実と異なる脆弱性関連情報を、事実と異なると認識して公表がなされる場合には、刑法の信用毀損罪に触れる可能性がある
  - c) 一般的に要求される程度の注意をもって調査・検証することをせず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る

### (3) IPA の対応と発見者の法的責任

受付機関の受付に係わる論点に関しては、次の通りである。

IPA は、脆弱性関連情報の入手方法に関して関知しない。ただし、違法な手段で入手されたことが明白な脆弱性関連情報に関しては、処理しないことがある。

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ない。

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ない。これらを、民間ガイドラインに明記している。

#### 4.4.4. 受付機関・調整機関に係わる論点

まず、受付機関・調整機関における脆弱性関連情報の開示の論点については、発見者における開示の論点（4.4.3(2)参照）とほぼ同様と考えられる。

また、受付機関・調整機関が脆弱性関連情報の通知を受けたのにも関わらず、迅速な対処ができなかった場合の法的論点を検討する必要がある。例えば、

脆弱性関連情報に関する対処に迅速性が欠けている場合

調整機関が脆弱性関連情報を通知する製品開発者の特定に誤りがあった場合

調整機関が作成した公表スケジュールに則って、関係者が脆弱性関連情報を機密にしていた状態で、ウイルスや不正アクセスによる被害が生じてしまった場合

などの、受付機関・調整機関の法的責任を検討する必要がある。

しかし、当該問題は全く新しい業務を行うものであり、上記の論点を扱うにはさらに各種業務や契約の詳細化を図る必要があり、本報告書には記述していない。今後この点については、将来的に民間ガイドラインに明記することも視野に入れ、継続的に議論していく。

#### 4.4.5. 関連する製品開発者に係わる論点

製品開発者に係わる法的関連事項に関しては、ソフトウェアライセンスにおける製品開発者と購入者との契約に係る論点、製造物責任法上の論点等が挙げられる。

ソフトウェアの提供行為について言えば、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ェ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)として求められる場合がある。

提供したソフトウェアにおいて、設計上の問題、プログラミング上の問題、運用上の問題を問わず、社会通念上、安心して使える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ることが求められる。もっともその対策方法の選択については、以下の考慮が必要になる。

- 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る。
- 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る。
- 3) 製造物責任法上の論点として、現時点において、ソフトウェ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るが、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ェアは動産である製造物なので製造物責任法による製品の欠陥を根拠とした責任を負う可能性がある。

なお、紛争の終局的解決は裁判所の判断によるため、本報告書の枠組みに則って真摯に対策をとっていることは、直ちに訴訟上の免責を導くものではない。ただし、責任の基礎としての過失の判断においては、一般人の能力、具体的には、事故当時において一般的に求められる行為の水準が決め手となることから、本報告書の枠組みに則って真摯に対策をとっていることは、裁判所の過失の判断に影響を与え、有責のリスクを軽減することとなると考えられる。

#### 4.4.6. 関連するウェブサイト運営者に係わる論点

ウェブサイトにおいて、ウェブサイト運営者とユーザとの間に、一定の契約関係があるものと推測され、そこで、ユーザが、個人情報等を入力する場合には、その利用契約に付随した義務をウェブサイト運営者が担うべきといえる。例えば、各サイトの「プライバシーポリシー」を前提に契約関係にはいる場合、ウェブサイトの過失による損害賠償の責めをすべて免れるような規定は、消費者契約法上無効となる。その理由には以下の通りである。

- 1) ウェブサイト運営者と、ユーザとの間においては、そのウェブアプリケーションの利用に際して、一定の契約関係にはいると考えられる。そして、ユーザが、そのサイトに一定の個人情報などをゆだねる場合には、ウェブサイト

運営者は、そのサイトの利用契約に付随した義務として一定レベルのセキュリティ維持を果たすべき義務を負担していると考えられる。

- 2) 各サイトに「プライバシーポリシー」などが記載されている場合には、その内容をも前提にユーザとウェブサイト運営者は、契約関係にはいると考えられる。
- 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すべて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可能性がある。

## 5. 今後の予定

### 5.1. 次年度以降の作業計画

本研究会における本年度の成果を踏まえ、次年度以降、表 5-1に示す作業を進めることが期待される。

表 5-1 次年度以降の作業イメージ

時期		制度的担保	基本枠組みを支える体制整備
2004 年	3 月末	・ 研究会報告書とりまとめ	
	4 月中	・ 関係者間調整	<ul style="list-style-type: none"> <li>・ 脆弱性関連情報届出の受付システムの整備</li> <li>・ IPA・JPCERT/CC 間情報共有環境の整備</li> <li>・ 脆弱性対策方法 DB の構築開始</li> <li>・ 脆弱性分析機能の充実</li> <li>・ JPCERT/CC・製品開発者間の提携推進</li> </ul>
	5 月上旬	<ul style="list-style-type: none"> <li>・ 政府の公的ルール案公表</li> <li>・ パブリックコメント募集</li> </ul>	
	6 月上旬	・ パブリックコメント締切	
	7 月上旬	<ul style="list-style-type: none"> <li>・ 政府の公的ルールの運用開始</li> <li>・ 民間ガイドライン運用開始</li> </ul>	・ 脆弱性関連情報届出の受付開始
	7 月以降	・ 問題点の洗い出し	
2005 年度		・ 民間ガイドラインの修正	・ 情報流通体制の改善・本稼動

## 5.2. 次年度以降の検討課題

### (1) 脆弱性関連情報受付システムの整備

#### 秘匿性を重視した情報管理

脆弱性関連情報の届出を受け付けるシステムには、外部からのアクセスはもちろん、内部からも特定のスタッフ以外にはアクセスを認めない厳重なアクセス制御機能や、トラブル発生時にトレースが可能なアクセスログ管理機能が不可欠である。

#### 脆弱性の危険性、影響度、緊急度評価

ある程度実績を重ねた段階で、得られた知見を背景に、受け付けた脆弱性の危険性、影響度、緊急度等を評価し、その結果に応じて最適な対応を判断する機能を確立することが求められる。

#### 他のスキームとの連携

Telecom-ISAC Japan では「システムの脆弱性に関する報告及び情報交換」の機能を整備しており、有料の情報提供サービスの利用に加え、会員からの報告も受け付ける方針とされる。これは、基本的には会員を対象とした仕組みであるが、日本全体で考えれば、本報告書で提示した脆弱性関連情報流通の枠組みとの合理的な連携が望まれる。例えば、脆弱性を報告した会員もしくは Telecom-ISAC Japan が「発見者」として本枠組みに当該脆弱性関連情報を提供することにより、その脆弱性について慎重かつ広範に製品開発者に対処を呼びかけることが可能となる。さらに、連携してより密接な情報共有を整備する可能性についても検討すべきである。

### (2) 機密情報流通の仕組みづくり

#### 受付機関 - 調整機関間の情報共有

受付機関となる IPA と調整機関となる JPCERT/CC の間では、緊密な情報共有が前提となる。例えば、今後段階的に共有を進める上での情報の種類や範囲、共有化の方法、ルール等について適切なモデルを策定する必要がある。

また、海外 CSIRT からの情報については開示範囲に制約が生じるので、そうした制約を緩和し円滑な情報共有を実現するためにも、IPA は FIRST (Forum of Incident Response and Security Teams: インシデント対応とセキュリティのチームによる世界規模のフォーラム。JPCERT/CC は 1998 年に加盟) に加盟するなど海外 CSIRT との関係構築にも今以上に注力することが望まれる。

#### 調整機関 - 製品開発者間の情報共有

調整機関である JPCERT/CC は、製品開発者と情報共有を図るため、製品開発者に広く協力を呼びかけるとともに、各社と秘密保持契約を取り交わすことが望ましい。

また、製品開発者側での内部調整が困難で窓口を一本化できない場合、上記の契約やフィードバックされる情報の集約方法等も含め、JPCERT/CC としての対応方針を明確にすることが求められる。

加えて、製品開発者が対策方法を策定する期限についての目安となる期間設定に係る合意形成、JPCERT/CC が実際に脆弱性関連情報を取り扱う際に配信先の抽出を的確かつ効率的に行うための方法や、情報流通を効率的かつ安全に行うためのツールについても今後検討を進める必要がある。

#### 政府・重要インフラ事業者への優先情報提供

IPA は重大事案の際、政府や重要インフラ事業者に対し、未公表の対策方法（版のパッチ、対策準備要請等）を優先提供する可能性がある。ただし、その位置付けや有効性、既存のチャンネルの活用、機密保持の仕組み、優先提供先が漏洩元になった場合の責任範囲、重大事案の判断、所管省庁との整合などの事項について、さらに検討を深める必要がある。

#### 情報流通に関するシミュレーションの実施

環境がある程度整備された段階で、脆弱性関連情報の流通体制が適切に機能するか検証すべく、シミュレーションを実施することが必要である。脆弱性関連情報の入手経路や重要度、影響範囲等に応じて複数のモデルを設定し、様々な観点から、流通体制に内在する問題点を洗い出すことをめざす。

#### 情報流通の有効性に関するチェック機能の導入

調整機関の情報提供活動が効果的に機能していたか、それを受けた製品開発者各社の対応が適切であったかなど、脆弱性関連情報流通体制の有効性を客観的に評価する仕組みを導入して、問題点を改善するよう調整機関にフィードバックしていく取り組みが必要になる。

### (3) 製品開発者側に望まれる対応

#### 脆弱性関連情報流通の枠組みへの参加

製品開発者は、本報告書で提言した脆弱性関連情報流通の枠組みに自ら参加し、ユーザの被害発生抑制に寄与することが期待される。そのためには、製品開発者の一員として、調整機関である JPCERT/CC との脆弱性関連情報提供に

係る契約を行い、本枠組みで明示した推奨される行動基準に則り、企業として脆弱性に対処する積極的な姿勢を示すことが求められる。

#### 脆弱性関連情報取扱いに関する社内ポリシーの策定

企業として脆弱性関連情報へのスムーズな対応や適切な機密保持を実現するためには、脆弱性関連情報を入手した際の社内的な対応手順・ルールを明確化する必要がある。例えば、脆弱性対策に企業として取り組むという経営層の意思決定、脆弱性関連情報にアクセス可能なスタッフを限定するなど、社内に対しても厳格な機密情報の取扱いルール、調整機関とのコンタクトパーソンをはじめとする社内緊急対応チーム、脆弱性と対策方法の公表フォーマット、マスコミ対策など様々な事項の設定が要求される。

こうした点を踏まえ、製品開発者各社は、今後発生しうる脆弱性関連情報の通知に備え、その取扱いに関する社内ポリシーを整備しておくことが望ましい。

#### 各製品開発者間の連携

調整機関との連絡窓口となる製品開発者各社の連絡担当者は、調整機関から提供される脆弱性関連情報を受け、客観的な指標のないまま社内での調整を担うことが要求される。受け取った脆弱性関連情報に係わる情報交換は控えるべきだが、一般的な体制や社内ルール、現在の問題点等の情報を連絡担当者間で交換し、改善を図ることは有益と考えられる。したがって、連絡担当者同士が連携するための土壌となるコミュニティ的環境の必要性について検討することが望まれる。

### (4) 脆弱性分析機能の充実

#### 脆弱性分析体制の確立

脆弱性関連情報を入手した際には、当該脆弱性が国内に与える影響を判断し、注意を喚起し、対策の普及を促す必要がある。そのために、分析機能においては、攻撃方法の有無や、対象ソフトウェアおよびバージョンなどの影響範囲の確認を、検証を通じて実施する。特に日本語環境における緊急度や重要度といったリスク分析や、脆弱性の悪用の難易度の把握が重要である。

また、開発者との協力関係を築くことにより、脆弱性の存在を確認するツールの開発や、対策方法の検討および動作確認といった対策方法策定に携わることが可能となる。さらに、対策方法が公表された後には、その脆弱性を悪用した攻撃の検知方法の検証情報の提供を実施する。

#### 分析環境の整備

脆弱性の迅速な分析のためには、再現環境を構築する必要がある。発足当初は機材や分析対象範囲に限られるが、よりいっそうの分析機能の充実のために、分析対象の拡充および機材の充実が求められる。また、分析員の技術向上のためのトレーニングや分析状況の評価を実施し、問題点を解決していくことが望ましい。

#### (5) 脆弱性対策方法の集積・公表機能の整備

##### 公表スケジュールを反映した情報管理

脆弱性の対策方法には、公表されたものだけでなく、パッチの版や対策準備依頼（例： 日後に対策方法を公表するので人員を確保してほしい等）といった公表前の情報も含まれる。こうした公表前の情報については、例えば政府や重要インフラ事業者など社会的影響の大きい対象に限定して提供し、緊急の対策実施を推進する使い方が有用である。従って、本データベースは、情報によって開示範囲を調整できるようにすることが求められる。

##### 他の関連データベースとの連携

対策方法データベースは、単体での完全性を追求するより、国内外の関連データベースと相互に連携する方が有用である。その場合、それらが同様の情報をカバーするのではなく、各々が自身の特徴を明確にすることによってより効果的な連携が期待できる。例えば、IPA セキュリティセンターの場合、脆弱性分析機能のアウトプットをコンテンツに反映することで、他の関連データベースにはない付加価値を創出することができる。

##### データベースユーザのニーズの反映

対策方法データベースの直接的なユーザ層（システムインテグレータや ISP、マスコミ等を想定）にとって利用しやすいシステムに改善していく取り組みが重要である。具体的には、Telecom-ISAC Japan や「インターネットセキュリティ対策推進協議会（仮称）」等の組織と連携して、そのニーズを吸収し、データベースの改善に反映していく方向が考えられる。

#### (6) ユーザ側に求められる対応

##### 企業ユーザ間の情報共有の仕組みづくり

企業ユーザにおいては、脆弱性の対策方法について情報を得ても、その適用によって現行システムにトラブルが発生する可能性があるため、十分な検証を要するケースが少なくない。実際には、検証期間中にコンピュータウイルス等の攻撃を受ける可能性があり、これをいかに短縮しリスクを軽減するかが企業

ユーザの大きな課題と言える。そこで、企業ユーザが、脆弱性対策に係る情報を共有し、実務的な知見の集約や製品開発者との交渉を行うための仕組みを整備して、合理的・効率的な対策実施をめざすことが有効である。

#### 中小企業、個人ユーザの啓発・支援

中小企業や個人ユーザについては、知識不足やコスト的な制約から十分な対策を適用できないケースも見られる。高度情報通信ネットワーク社会の一員としての自覚を促すべく、小売店やマスコミ等を通じた啓発活動、ITコーディネーター等を活用した実際的な取り組みの支援などが期待される。

# 資料編



## 資料1 ソフトウェア等脆弱性関連情報取扱基準モデル案

### ．主旨

本基準は、ソフトウェ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。

### ．用語の定義

本基準で用いられる用語の定義は、以下のとおりである。

#### 1．脆弱性

ソフトウェア等において、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つては、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つて、以下に掲げる種類のいずれかに該当するもの。

##### (1) 脆弱性

##### (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

脆弱性によって生ずる問題を解決又は回避するための方法であつて、以下に掲げる種類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．ソフトウェア製品

ソフトウェア又はそれを組み込んだハードウェアであって、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7月7日通商産業省告示第429号制定）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8月13日法律第128号）における「不正アクセス行為」をいう。

．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、以下のとおりである

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

ソフトウェ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) ソフトウェア製品を開発した者

(2) (1)に掲げる者のほか、ソフトウェア製品の開発、加工、輸入又は販売に関する形態その他の事情からみて、当該ソフトウェ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。

## ．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ェア製品  
（ソフトウェ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稼働するウェブアプリケーション

## ．対象がソフトウェア製品である場合の脆弱性関連情報取扱基準

対象がソフトウェア製品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は、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とともに、処理の進捗状況を当該発見者に通知する。
- (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、当該製品開発者との協議の上で、当該脆弱性関連情報の取扱い及び対策に係る方針（以下、「方針」とする）を作成する。
- (iv) 当該製品開発者は、作成された方針に従い、当該脆弱性に係る対策方法を作成する。
- (v) 受付機関及び調整機関は、当該製品開発者が当該脆弱性及び対策方法を公表する時期に合わせて、当該脆弱性及び対策方法を公表する。

関係者における詳細な行動基準は以下に定める。

### 1．発見者基準

- (1) 発見者（自社製品についての脆弱性関連情報であって、他社のソフトウェア製品に影響を及ぼし得るものを発見又は取得した製品開発者を含む）は、発見又は取得した脆弱性関連情報を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。
  - 発見者の氏名、連絡先等の情報及びその取扱い
  - 脆弱性を有する製品の名称等
  - 当該製品の有する脆弱性の内容
- (3) 発見者は、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、当該対策方法が公表されるまでの間は、第三者に漏えいしないように当該脆弱性関連情報を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は、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は、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は、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、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は、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。
  - 再現性が確認できない場合
  - 脆弱性関連情報に該当しない場合
  - 既知の脆弱性関連情報である場合
  - 違法な方法により発見又は取得されたおそれがある場合
- (3) 受付機関は、届出を受理した後においても、必要に応じ、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ができる。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、当該対策方法が公表されるまでの間は、第三者に漏えいしないように当該脆弱性関連情報を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は、当該製品開発者及び調整機関と協議の上、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、当該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は、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、当該製品開発者が当該脆弱性及び対策方法を公表する時期に合わせて、当該脆弱性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。その際、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、受付機関から通知された脆弱性関連情報を、速やかに当該製品開発者に通知すること。
- (2) 調整機関は、当該製品開発者が既に対策方法を作成している等の場合については、当該脆弱性関連情報に関して新規に対応する必要がないと判断することができる。この場合においては、受付機関に対しその旨及びその理由を通知すること。
- (3) 調整機関は、当該製品開発者と協議の上、当該脆弱性及び対策方法を作成し又は公表する時期を定めた方針を作成し、当該製品開発者及び受付機関に通知すること。ただし、当該製品開発者との更なる協議の結果必要と認められる場合は、一度作成した方針を変更することができる。
- (4) 調整機関は、当該対策方法が公表されるまでの間は、第三者に漏えいしないように当該脆弱性関連情報を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は、当該製品開発者と協議の上、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。
- (5) 調整機関は、当該製品開発者が当該脆弱性及び対策方法を公表する時期に合わせて、当該脆弱性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。また、当該製品開発者が当該方針に従って対策を講じていないと認められる場合は、必要に応じてその名称を公表することができる。

### 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) 当該製品開発者は、調整機関から通知された脆弱性関連情報に関して、その内容を検証するとともに、作成された方針に従って対策方法を作成すること。
- (3) 当該製品開発者は、調整機関及び受付機関と協議し、当該発見者の同意がある場合には、当該脆弱性関連情報に関して、当該発見者と直接連絡をとることができる。
- (4) 当該製品開発者は、当該脆弱性関連情報が他社のソフトウェア製品に影響を及ぼすと認める場合には、その旨及びその理由を調整機関に通知すること。
- (5) 当該製品開発者は、当該方針に従って、当該脆弱性関連情報を第三者に漏えいしないように適切に管理すること。
- (6) 当該製品開発者は、作成した対策方法を速やかに調整機関及び受付機関に通知し、調整機関と協議の上、当該脆弱性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。

## ．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は、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とともに、処理の進捗状況を当該発見者に通知する。
- (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は以下に定める。

### 1．発見者基準

- (1) 発見者は、発見又は取得した脆弱性関連情報を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。  
発見者の氏名、連絡先等の情報及びその取扱い  
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  
当該ウェブアプリケーションの有する脆弱性の内容
- (3) 発見者は、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は、第三者に漏えいしないように当該脆弱性関連情報を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は、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は、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は、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は、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。

再現性が確認できない場合

脆弱性関連情報に該当しない場合

既知の脆弱性関連情報である場合

違法な方法により発見又は取得されたおそれがある場合

- (3) 受付機関は、届出を受理した後においても、必要に応じ、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ができる。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に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は、当該ウェブサイト運営者と協議の上、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が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) 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) 当該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) 当該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は、当該脆弱性関連情報を第三者に漏えいしないように適切に管理すること。
- (4) 当該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は、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。

. その他

受付機関及び調整機関による対策方法の普及支援を以下のとおり行う。

- (1) 製品開発者は、自社製品についての脆弱性関連情報であって、他社のソフトウェア製品に影響を及ぼさないと認められるものを発見又は取得し、調整機関からの通知によることなく、対策方法を作成した場合であっても、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ができる。
- (2) 受付機関及び調整機関は、この通知を受けたときは、当該脆弱性関連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、公表する時期については当該製品開発者と協議の上決定すること。



## 資料2 ソフトウェア等脆弱性関連情報取扱ガイドラインモデル案

### ・本ガイドラインの位置づけ

近年、日本国内においてソフトウェアやウェブアプリケーションの脆弱性が発見されることが増えており、これらの脆弱性を悪用した不正アクセス行為やコンピュータウイルスの増加により、企業活動が停止したり情報資産が滅失したり個人情報漏洩したりといった、重大な被害が生じています。しかし、それらの脆弱性が発見された場合の被害発生を阻止するために、脆弱性関連情報をどのように取り扱うべきかを示した国内の指針やガイドラインはありませんでした。

こうした状況の下、独立行政法人情報処理推進機構（IPA）は、平成15年11月以来「情報システム等の脆弱性情報の取扱いに関する研究会」を組織し、国内の指針やガイドラインの整備を進めてきました。その結果、本研究会は、政府の公的ルール「ソフトウェア等脆弱性関連情報取扱基準」と本ガイドラインの必要性を認識するに至りました。

本ガイドラインは、そうした検討過程により作成されたものです。内容は、脆弱性関連情報の適切な流通により、コンピュータ不正アクセス、コンピュータウイルスなどによる被害発生を阻止を図るために、関係者に推奨する行為をとりまとめたものです。

本ガイドラインは、政府の公的ルール「ソフトウェア等脆弱性関連情報取扱基準」を平易に解説したものです。具体的には、IPAが受付機関、有限責任中間法人JPCERTコーディネーションセンター（以下、「JPCERT/CC」とする）が調整機関という役割を担うことを前提として、発見者、製品開発者、ウェブサイト運営者と協力をしながら脆弱性関連情報に対処するための、その発見から公表に至るプロセスを詳述することを目的としています。

関係者の方々は、本ガイドラインを、脆弱性関連情報の取扱いに際しての行動の基本として尊重して頂くようお願い申し上げます。

## ．用語の定義と前提

本ガイドラインに用いられる用語の定義は以下の通りです。

### 1．脆弱性の定義

脆弱性とは、ソフトウェア製品やウェブアプリケーションにおいて、コンピュータ不正アクセスやコンピュータウイルス等の攻撃により、その機能や性能を損なう原因となり得るセキュリティ上の問題箇所です。

なお、ウェブアプリケーションにおいて、ウェブサイト運営者の不適切な運用によって、個人情報等が適切なアクセス制御の下に管理されておらずセキュリティが維持できなくなっている状態も含まれます。(ウェブサイトの不適切な運用に関しては付録4に示します。)

### 2．脆弱性関連情報の種類

脆弱性関連情報とは、脆弱性に関する情報であり、次のいずれかに該当するものです。

#### 11)脆弱性

上記の1．の脆弱性の定義に準じます。

#### 12)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、プロトコルの検証ツール、付録1の(2)に示す方法等が該当します。

#### 13)攻撃方法

脆弱性を悪用するプログラムやコマンド、データおよびそれらの使い方です。例えば、エクスプロイトコード(付録4にて述べます)や、コンピュータウイルス等が該当します。

### 3．対策方法

対策方法は、脆弱性から生ずる問題を回避するまたは解決を図る方法のことであり、回避方法と修正方法から成ります。ただし、本ガイドラインで、「対策方法」との記述がある場合、「回避方法または修正方法」の意味となります。

#### 1)回避方法

脆弱性が原因となって生じる被害を回避するための方法(修正方法は含まない)であり、ワークアラウンド(付録4にて述べます)と呼ばれます。

#### 2)修正方法

脆弱性そのものを修正する方法であり、パッチ（付録4にて述べます）等と呼ばれます

#### 4．ソフトウェア製品

ソフトウェア自体又はソフトウェアを組み込んだハードウェア等の汎用性を有する製品のことです。ただし、いわゆるオープンソースソフトウェアのように技術情報を統括する企業が一社に定まらないもの、複数の者又は団体によりその改善が行われるものも含まれます。具体例は、付録4に示します。

#### 5．ウェブアプリケーション

インターネットのウェブサイトなどで、公衆に向けて提供するサービスを構成するシステムで、そのソフトウェ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を指します。

#### 6．発見者

発見者とは、脆弱性関連情報を発見または取得した人を含みます。例えば、ソフトウェアの脆弱性を発見した人や、インターネット上で脆弱性関連情報を入手した人などが当てはまります。ソフトウェアの脆弱性を発見した人のみを対象としているわけではありません。

#### 7．製品開発者

製品開発者とは、ソフトウェアを開発した企業または個人です。企業の場合それが外国の会社である場合には、そのソフトウェア製品の国内での主たる販売権を有する会社（外国企業の日本法人や総代理店など）を指します。

#### 8．ウェブサイト運営者

ウェブサイト運営者とは、脆弱性関連情報が発見されたウェブアプリケーションを運営する主体です。当該ウェブアプリケーションが企業や組織によって運営されているのであれば、その企業や組織が該当します。個人によって運営されているのであれば、その個人が該当します。ウェブサイト運営者の例は、付録4に示します。

## ・本ガイドラインの適用の範囲

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

ソフトウェア製品の場合：

- ・国内で利用されているソフトウェア製品

国内で、非常に多くの人々に利用されている等のソフトウェア製品であり、プロトコルを実装しているものを含みます。プロトコルの実装に係わる脆弱性は付録4に示します。

ソフトウェア製品に係る脆弱性関連情報の取扱いは、 で記述します。

ウェブアプリケーションの場合：

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

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

ウェブアプリケーションに係る脆弱性関連情報の取扱いは、 で記述します。

## ソフトウェア製品に係る脆弱性関連情報取扱

### 1. 概要

ソフトウェア製品に係る脆弱性関連情報取扱の概要は、図1の通りです。

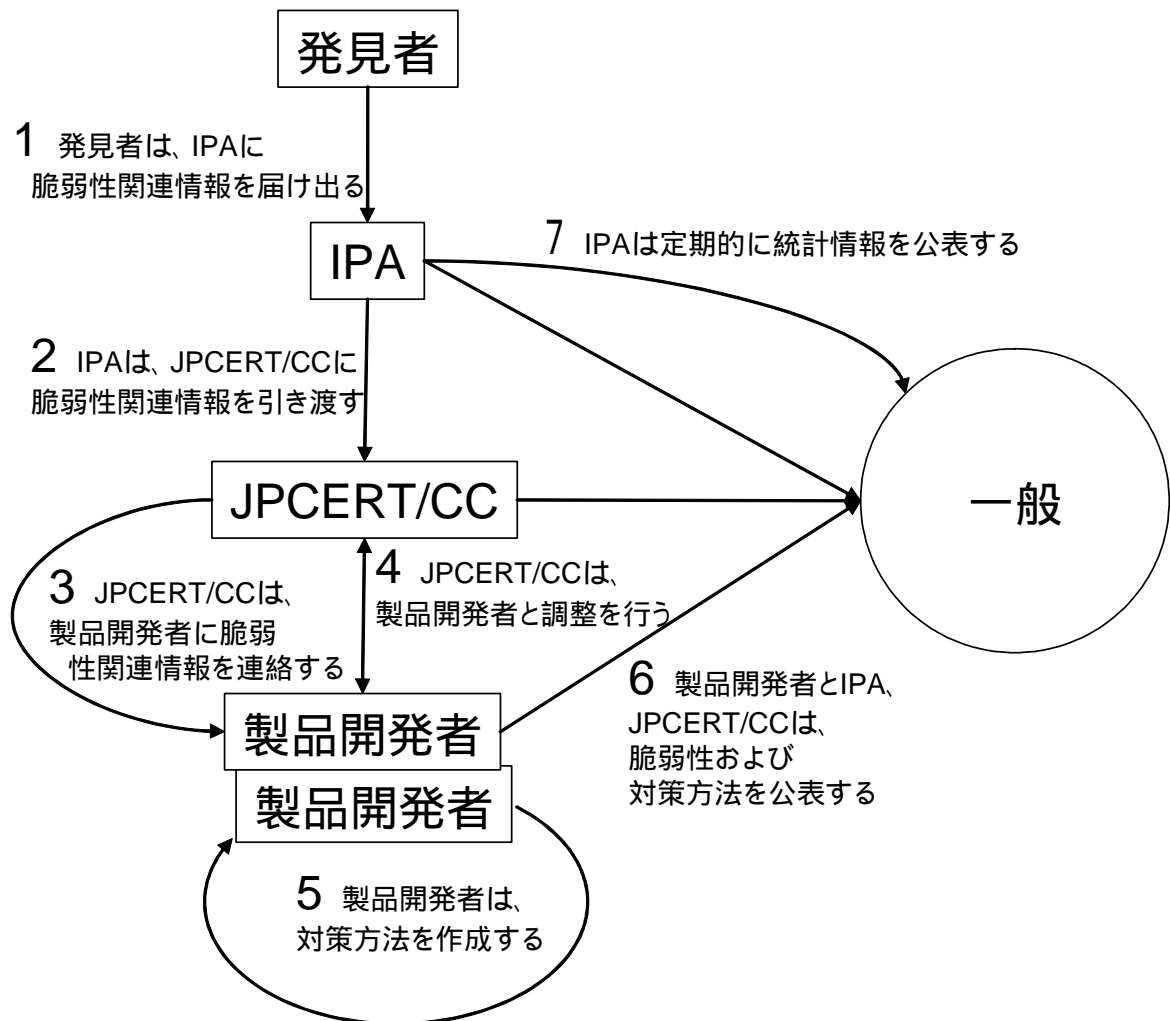


図1 ソフトウェア製品に係る脆弱性関連情報取扱の概要

- 1) 発見者は、IPA に脆弱性関連情報を届け出る
- 2) IPA は、受け取った脆弱性関連情報を、原則として JPCERT/CC に引き渡す
- 3) JPCERT/CC は、脆弱性関連情報に関する製品開発者を特定し、製品開発者に脆弱性関連情報を連絡する
- 4) JPCERT/CC は、製品開発者と対策方法の策定・公表に関するスケジュール調整を行う

- 5) 製品開発者は、上記 4) で決められたスケジュールに則って、対処を進める
- 6) 製品開発者と IPA および JPCERT/CC は、対策方法策定後に脆弱性および対策方法を公表する
- 7) IPA は、統計情報を少なくとも一年に一度は公表する

## 2. 発見者の対応

### 1) 発見者の範囲

における発見者とは、製品開発者以外の者（研究者など）のみを指しているわけではありません。製品開発者自身であっても、自社のソフトウェア製品についての脆弱性関連情報であって、他社のソフトウェア製品に影響を及ぼす可能性があるものを発見・取得した場合、発見者としての対応が推奨されます。

### 2) 脆弱性関連情報の発見・取得

脆弱性関連情報の発見・取得に際しては、関連法令に触れることがないように留意してください。詳細は、付録 1 に示します。

### 3) 脆弱性関連情報の届出

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

### 4) 脆弱性関連情報の管理および開示

発見者は、対策方法が公表されるまでの間は、脆弱性関連情報が第三者に漏れないように適切に管理してください。また、脆弱性関連情報を開示する場合には、IPA に連絡してください。対策方法が公表された後に脆弱性関連情報を開示する場合でも、対策方法が徹底されていないと考えられる状況下では、IPA に連絡してください。脆弱性関連情報の管理および開示に係わる法的問題に関しては、付録 1 に示します。

### 5) 届け出る情報の内容

届け出る脆弱性関連情報に関しては、脆弱性である必要はありません。攻撃方法等を発見した場合なども、IPA に届け出ることができます。また、発見者は、届け出る情報の中で以下の点を明示してください。

- ・発見者の氏名・連絡先

- ・脆弱性関連情報に関連する製品の具体的な名称
- ・脆弱性関連情報の内容
- ・脆弱性関連情報を確認する環境と手順（再現性）
- ・個人情報の取り扱い方法（製品開発者への通知および直接の情報交換の可否、一般への公表の可否）

発見者が望まない場合、IPA は、JPCERT/CC および製品開発者に対して、発見者を特定しうる情報を通知することはありません。さらに、JPCERT/CC および製品開発者以外にも、発見者を特定しうる情報を開示することはありません。

逆に、発見者が望む場合、IPA または JPCERT/CC は、脆弱性関連情報と対策方法を公表する際に発見者名を付記するとともに、製品開発者の公表時に発見者名を付記することを製品開発者に推奨します。

#### 6) 製品開発者との直接の情報交換

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

#### 7) 届出後の対応

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

### 3 . IPA および JPCERT/CC の対応

#### (1) IPA

##### 1) 脆弱性関連情報の受付

IPA の受付は、以下の URL に示す Web ページ上で行われます。入力された情報は暗号化された形で IPA 内の担当者に届けられます。受付は24時間ですが、作業は原則営業日となります。

<https://.....>

##### 2) 届出の受理

IPA は、以下の条件が満たされていると判断した時、その時点で届出を受理

し、発見者に連絡します。

(ア) 原則として、上記 2 . 5)の項目が十分に記述されていること

(イ) 匿名の届出でないこと(発見者への連絡が可能であることを確認できること)

なお、IPA は、これらの条件が満たされない場合、発見者に対し条件を満足して頂くことを促す対応を行い、やむを得ない場合以外は届出を受理します。

### 3) 対応の続行の判断

IPA は、当該脆弱性関連情報について、以下の観点から対応の続行の必要性を判断し、該当するときは処理を取りやめることがあります。

- ・ 脆弱性関連情報であること(一般のバグ情報ではないこと)
- ・ 既に報告されている脆弱性関連情報ではないこと
- ・ 届け出られた脆弱性関連情報について、再現性が確認できること

IPA は、対応の続行に当たり常に上記の判断を行い、対応を取りやめる時はその理由とともに発見者に連絡します。

### 4) 違法な手段で入手された脆弱性関連情報への対応

IPA は、脆弱性関連情報の入手方法に関して関知しません。ただし、違法な手段で入手された脆弱性関連情報であることが明白な場合、処理を取りやめることがあります。

### 5) JPCERT/CC への連絡

IPA は、上記 2)、3)および 4)における対応の是非の判断の結果、対応することが妥当との判断を下した脆弱性関連情報について、速やかに JPCERT/CC に通知します。また、脆弱性が再現する状況を特定できない場合等は、IPA 内部または外部において脆弱性関連情報に関する技術的分析を行います。

### 6) IPA の脆弱性関連情報の取り扱い

IPA は、脆弱性関連情報に関して、対策方法が公表されるまでの間は、発見者・JPCERT/CC・当該製品開発者および上記 5)に示す場合以外に第三者に提供しないように適切に管理します。対策方法が公表された後についても、その脆弱性関連情報に起因する被害が予想されるなどの場合については、第三者に提供することはありません。

### 7) 発見者との情報交換

IPA は、届出を受理した後、発見者に問い合わせをすることがあります。ま

た、発見者から問い合わせがあった場合、JPCERT/CC と相談の上、適切な情報の開示を行います。

#### 8) 対策方法の受付

IPA は、JPCERT/CC を介して製品開発者に連絡した脆弱性関連情報に関し、製品開発者から対策方法を受け取ります。

#### 9) 優先的な情報提供

IPA は、届出がなされた脆弱性関連情報に関して、重要インフラに対し特に影響が大きいと推察される場合、JPCERT/CC および製品開発者と協議の上、脆弱性関連情報と対策方法を、一般公表より前に、政府機関や重要インフラ事業者等に対して優先的に提供することがあります。この際、発見者に対して、その旨を通知します。重要インフラ事業者には、電力、ガス、鉄道、航空、通信、金融の各事業者が含まれます。

#### 10) 一般への情報の公表

IPA は、製品開発者の公表に合わせて、一般に対し脆弱性と対策方法を、インターネット上で公表します。情報の公表の際には、その旨を発見者に連絡します。なお、当該脆弱性関連情報が複数の製品開発者に関係している場合、IPA と複数の製品開発者の、一般への情報の公表は同時とすることを原則とします。

#### 11) 統計情報の集計と公表

IPA は、脆弱性に係わる実態を周知徹底し危機意識の向上を図り、その結果としての被害の予防のために、受け付けた脆弱性関連情報を集計し、統計情報としてインターネット上等で少なくとも一年に一度は公表します。統計情報には、脆弱性の種類、脆弱性の種類ごとの届出件数の時間的推移等が含まれます。

### (2) JPCERT/CC

#### 1) 製品開発者への連絡

JPCERT/CC は、届け出られた脆弱性関連情報の IPA からの通知を受け、速やかに製品開発者を特定し、その製品開発者に連絡を行います。

#### 2) 対応の判断

JPCERT/CC は、製品開発者に脆弱性関連情報を連絡した後、以下の場合は対応しないと判断することがあります。その際には、その旨を IPA と製品開発者に通知します。

- ・ 関係する全ての製品開発者がすでに対策方法を作成している場合
- ・ 全ての製品開発者が当該脆弱性関連情報について、再現できない場合

### 3) 製品開発者との調整

JPCERT/CC は、製品開発者と協議の上、脆弱性関連情報に関する対策方法の策定に関するスケジュール、および脆弱性関連情報と対策方法の一般公表に関するスケジュールを決定します。以後、JPCERT/CC は、JPCERT/CC が製品開発者に最初の連絡を行った後から起算して一定期間内に公表するように促します。ただし、製品開発者の都合等により、相談の上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関連情報の場合、複数の製品開発者が同時に公表することを原則とします。

### 4) 発見者への連絡

JPCERT/CC は、当該脆弱性関連情報の対策方法策定に関するスケジュール、および脆弱性と対策方法の一般公表に関するスケジュールを、IPA を通して発見者に連絡します。

### 5) JPCERT/CC における脆弱性関連情報の取り扱い

JPCERT/CC は、脆弱性関連情報に関して、製品開発者が対策方法を公表するまでは、第三者に漏洩しないように管理します。ただし、海外製品であり外国企業の日本法人や総代理店が無い場合や、海外に大きな影響を与える脆弱性関連情報の場合などは、海外の CSIRT (CERT 等) に連絡することがあります。

### 6) 対策方法の受付

JPCERT/CC は、JPCERT/CC から連絡した脆弱性関連情報に係わる対策方法を製品開発者から受け取ります。

### 7) 一般への情報の公表

JPCERT/CC は、製品開発者と同時に、一般に対し脆弱性と対策方法をインターネット上で公表します。情報の公表の際には、その旨を発見者に連絡します。なお、当該脆弱性関連情報が複数の製品開発者に関係している場合、

JPCERT/CC と複数の製品開発者の一般への情報の公表は同時とすることを原則とします。さらに、当該製品開発者の作業に関し上記 3) で決められたスケジュールに則っていないという判断を JPCERT/CC が下す場合、必要に応じて JPCERT/CC は製品開発者名を公表することがあります。

#### 4. 製品開発者の対応

製品開発者は、製品に脆弱性が存在する場合には、その対策に関して適切な対応をすることが望まれます。製品開発者に係わる法的関連事項は、付録 2 に示します。

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

##### 1) 窓口の設置

製品開発者は、JPCERT/CC との間で脆弱性関連情報に関する情報交換を行うための窓口を設置し、あらかじめ JPCERT/CC に連絡してください。

##### 2) 脆弱性関連情報への対応

製品開発者は、JPCERT/CC から脆弱性関連情報を受け取ったら、対策方法の策定スケジュールおよび脆弱性と対策方法の一般公表スケジュールを、JPCERT/CC と協議します。そして、決定されたスケジュールに則り、対策方法を作成するための作業を行ってください。なお、製品開発者の脆弱性および対策方法の一般公表は、製品開発者が脆弱性関連情報を受け取った後、一定期間以内に行うことが望ましいでしょう。無理な場合は、JPCERT/CC と再協議の上スケジュールを決定してください。また、他社製品に類似の脆弱性があることが想定される場合、JPCERT/CC に連絡してください。

##### 3) 発見者との直接の情報交換

製品開発者は、対策方法の作成のために、IPA および JPCERT/CC と協議の上、発見者の了解のある場合、発見者と直接情報交換を行うことが可能です。

##### 4) 問い合わせへの対応

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

##### 5) 対策方法の連絡

製品開発者は、JPCERT/CC からの脆弱性関連情報の連絡に関して、作成した

対策方法を、IPA および JPCERT/CC に連絡してください。

#### 6) 製品開発者内の情報の管理

製品開発者は、上記 2) で作成した脆弱性と対策方法の一般公表スケジュール、脆弱性関連情報を第三者に漏洩しないように管理してください。

#### 7) 脆弱性および対策方法の公表

上記 2) で作成した脆弱性と対策方法の一般公表スケジュールに則って、脆弱性および対策方法を公表してください。公表内容は、以下の項目が含まれるようにすることが望まれます。

- ・ 製品名およびバージョン
- ・ 受付日時
- ・ 脆弱性の概要
- ・ 対策方法
- ・ 関連情報へのリンク
- ・ 当該脆弱性関連情報に係わる連絡先
- ・ 発見者の個人情報(発見者が望んだ場合)

## ．ウェブアプリケーションに係る脆弱性関連情報取扱

### 1．概要

ウェブアプリケーションに係る脆弱性関連情報取扱概要は、図2の通りです。

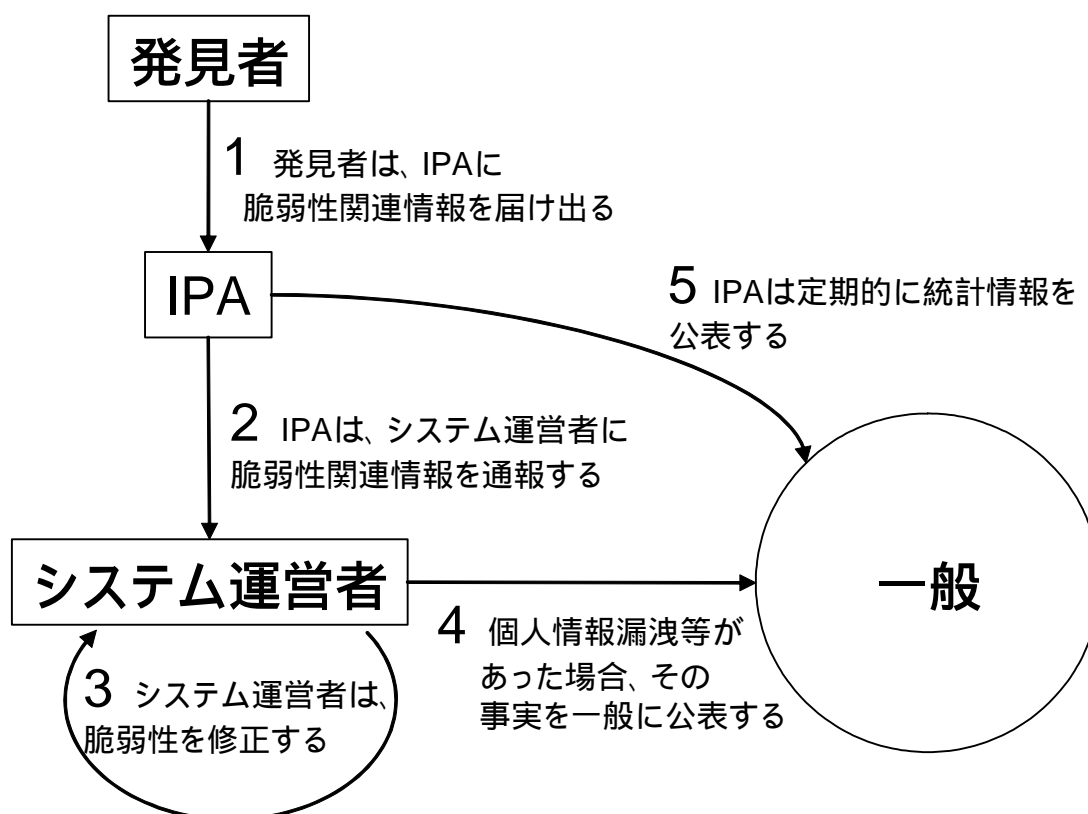


図2 ウェブアプリケーションに係る脆弱性関連情報取扱概要

- 1) 発見者は、IPA に脆弱性関連情報を届け出る
- 2) IPA は、受け取った脆弱性関連情報に関して、原則としてウェブサイト運営者に通報する
- 3) ウェブサイト運営者は、脆弱性の影響分析を行った上で、必要に応じて脆弱性の修正を行う
- 4) 個人情報漏洩等の事件があった場合、ウェブサイト運営者は、その事実を一般に公表するなど適切な処置をとる
- 5) IPA は、統計情報を少なくとも一年に一度は公表する

## 2. 発見者の対応

### 1) 発見者の範囲

における発見者とは、ウェブサイト運営者以外の者（研究者など）のみを指しているわけではありません。ウェブサイト運営者自身であっても、自ら運営するウェブアプリケーションに係る脆弱性関連情報を発見・取得した場合、発見者としての対応が推奨されます。

### 2) 脆弱性関連情報の発見・取得

脆弱性関連情報の発見・取得に際しては、関連法令に触れることが無いように留意してください。法的問題の詳細は付録1を参照してください。

### 3) 脆弱性関連情報の届出

発見者は、発見した脆弱性関連情報をIPAに届け出ることができます。ウェブサイト運営者に対し、同一情報の届出を行う必要はありませんが、届け出ること自体は問題ありません。

### 4) 脆弱性関連情報の管理および開示

発見者は、脆弱性が修正されるまでの間は、脆弱性関連情報が第三者に漏れないように適切に管理してください。また、脆弱性関連情報を開示する場合には、IPAに連絡してください。脆弱性関連情報の管理および開示に係わる法的問題に関しては、付録1に示します。

### 5) 届け出る情報の内容

届け出る脆弱性関連情報に関しては、脆弱性自体である必要はありません。脆弱性を有することが明白でなく単に疑わしい場合や、検証方法を発見した場合なども、IPAに届け出ることができます。

また、発見者は、届け出る情報の中で以下の点を明示してください。

- ・発見者の氏名・連絡先
- ・脆弱性関連情報に関連するサイトのURL
- ・脆弱性関連情報の内容
- ・脆弱性関連情報を確認する環境と手順（再現性）
- ・個人情報の取り扱い方法（ウェブサイト運営者との直接の情報交換の可否、ウェブサイト運営者への通知の可否）

発見者が望まない場合、IPAは、ウェブサイト運営者へ発見者を特定しうる情報を連絡することはありません。

### 5) ウェブサイト運営者との直接の情報交換

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

### 6) 届出後の対応

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

## 3 . IPA の対応

### 1) 脆弱性関連情報の受付

IPA の受付は、以下の URL に示す Web ページ上で行われます。入力された情報は暗号化された形で IPA 内の担当者に届けられます。受付は24時間ですが、作業は原則営業日となります。

https://.....

### 2) 届出の受理

IPA は、以下の条件が満たされていると判断した時、その時点で届出を受理し、発見者に連絡します。

- (ア) 原則として、上記 2 . 5) の項目が十分に記述されていること
- (イ) 匿名の届出でないこと (発見者への連絡が可能であることを確認できること)

なお、IPA は、これらの条件が満たされない場合、発見者に対し条件を満足して頂くことを促す対応を行い、やむを得ない場合以外は届出を受理します。

### 3) 対応の続行の判断

IPA は、当該脆弱性関連情報について、以下の観点から対応の続行の必要性を判断し、該当するときは処理を取りやめることがあります。

- ・ 脆弱性関連情報であること (一般のバグ情報ではないこと)
- ・ 既に報告されている脆弱性関連情報でないこと
- ・ 届け出られた脆弱性関連情報について、再現性が確認できること

IPA は、対応の続行に当たり常に上記の判断を行い、対応を取りやめる時はその理由とともに発見者に連絡します。

#### 4) 違法な手段で入手された脆弱性関連情報への対応

IPA は、脆弱性関連情報の入手方法に関して関知しません。ただし、違法な手段で入手されたことが明白な脆弱性関連情報に関しては、処理を取りやめることがあります。

#### 5) ウェブサイト運営者への連絡

IPA は、上記 2)、3)および 4)における対応の是非の判断の結果、対応することが妥当との判断を下した脆弱性関連情報について、速やかにウェブサイト運営者に通知します。また、ウェブサイト運営者が脆弱性の再現する状況を特定できない場合等は、IPA の内部または外部で脆弱性関連情報に関する技術的分析を行います。

#### 6) 発見者との情報交換

IPA は、届出を受理した後でも、発見者に問い合わせすることがあります。また、発見者から問い合わせがあった場合、適切な情報の開示を行います。

#### 7) IPA 内での情報の管理

IPA は、脆弱性関連情報を第三者に漏洩しないように管理します。

#### 8) 統計情報の集計と公表

IPA は、脆弱性に係わる実態を周知徹底し危機意識の向上を図り、その結果としての被害の予防のために、受け付けた脆弱性関連情報を集計し、統計情報としてインターネット上で少なくとも一年に一度は公表します。統計情報には、脆弱性の種類、脆弱性の種類ごとの届出件数の時間的推移等が含まれます。その際に、当該ウェブアプリケーションの脆弱性関連情報に関して、サイト名・URL・ウェブサイト運営者名が判別可能な形式で公表することはありません。

### 4 . ウェブサイト運営者

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

ウェブサイト運営者における法的関連事項は、付録 3 に示します。

以下で、ウェブサイト運営者が対応すべき事項を説明します。

#### 1) 脆弱性関連情報への対処

ウェブサイト運営者は、通報を受けたら、脆弱性の及ぼす影響を正確に把握した後、影響の大きさを考慮し、脆弱性を修正してください。また、当該脆弱性関連情報に関して検証した結果、および修正した場合その旨を IPA に連絡してください。

#### 2) 問い合わせへの対応

ウェブサイト運営者は、IPA からの脆弱性関連情報に係わる技術的事項に関する問い合わせに的確に答えてください。

#### 3) 発見者との直接の情報交換

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

#### 4) ウェブサイト運営者内での情報の管理

ウェブサイト運営者は、脆弱性が修正されるまでの間は、脆弱性関連情報を第三者に漏洩しないように管理してください。

#### 5) 脆弱性関連情報の公表

ウェブサイト運営者は、ウェブアプリケーションの脆弱性関連情報に関して、積極的に公表する必要はありません。ただし、この脆弱性が原因で、個人情報漏洩したなどの事案が起こったまたは起こった可能性がある場合、二次被害の防止および関連事案の予防のために、以下の項目を含むように公表してください。また、当該個人からの問い合わせに的確に回答するようにして下さい。

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

・ IPA および JPCERT/CC による対策方法の普及支援

1) 製品開発者自身による脆弱性関連情報の発見・取得

製品開発者は、自社のソフトウェア製品についての脆弱性関連情報であって、他社のソフトウェア製品に影響を及ぼさないと認められるものを発見・取得し、調整機関からの通知によることなく、対策方法を作成した場合であっても、IPA および JPCERT/CC に届け出ることができます。

2) IPA および JPCERT/CC による普及支援

IPA および JPCERT/CC が上記 1) の通知を受け取ったときは、当該脆弱性関連情報及び対策方法をインターネット上で公表します。公表する時期については、製品開発者と事前に調整を図ります。

## 付録1 発見者が心得ておくべき法的な問題

発見者が心得ておくべき法的な問題について述べます。脆弱性発見と脆弱性関連情報の管理に関する記述があります。

### 1. 脆弱性関連情報の発見に際しての法的な問題

#### (1) 関係する行為と法令の関係

##### a) ネットワークを用いた不正

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

・例えば、管理者の了解無く、他人のパスワードを取得し、それを用いて権限なしでシステムにアクセスした場合には、不正アクセス禁止法に抵触します

・故意にサーバの機能や性能の異常を来たそうとして何らかの行為をなし、コンピュータの性能を低下させたりした場合、刑法上の偽計(もしくは威力)業務妨害罪に抵触する可能性があります。さらに、その妨害の程度によっては、刑法の電子計算機損壊等業務妨害罪にも抵触すると解される可能性があります。

##### b) 暗号化されている無線通信の復号化

・暗号化されている無線通信を傍受し復号する行為(無線LANのWEPキーの解読など)は、第159通常国会で改正の審議がなされている電波法に触れる可能性があります。

#### (2) 不正アクセス禁止法に抵触しないと推察される行為の例

脆弱性の発見に最も関係が深い不正アクセス禁止法に対しては慎重な扱いが求められます。といっても脆弱性を発見する際に、必ずしも不正アクセス禁止法に抵触するとは限りません。以下に、不正アクセス禁止法に抵触しないと推察される行為の例を挙げます。

- 1) ウェブアプリケーションの利用権者が、正規の手順でログインするなどして通常のアクセスをした際に、ブラウザとサーバとの通信の内容を観察したところ、それだけで脆弱性の存在を推定できた場合。
- 2) ウェブページのデータ入力欄にHTMLのタグを含む文字列を入力したところ、入力した文字列がそのまま表示された。この段階ではアクセス制御

機能の制限を回避するに至らなかったが、悪意ある者に別の文字列を入力されれば、このサイトにセキュリティ上の問題が引き起こされかねないと予想できた場合。

- 3) アクセス制御による制限を免れる目的ではなく、通常の自由なページ閲覧を目的として、日付やページ番号等を表すと推察される URL 中の数字列を、別の数字に差し替えてアクセスしてみたところ、社会通念上、本来は利用できてはならないはずと推定される結果が、偶発的に起きてしまった場合。(ただし、積極的に多数の数字列を変えて試す行為等は、制限を免れる目的とみなされる可能性があります。)

### (3) IPA の対応と発見者の法的責任

IPA は、脆弱性関連情報の入手方法に関して関知しません。ただし、違法な手段で入手されたことが明白な脆弱性関連情報に関しては、受け付けないことがあります。

また、IPA が脆弱性関連情報を受け付けた場合でも、IPA は脆弱性関連情報の入手手段に関して合法であると判断したわけではありません。さらに、IPA が脆弱性関連情報を受け付けた場合、発見者の脆弱性関連情報の発見に係る法的責任が免責されるわけではありません。

## 2 . 脆弱性関連情報の管理に際しての法的な問題

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

- (1)脆弱性についての調査・報告は、その率直な交換により、ソフトウェアやウェブアプリケーションシステムのセキュリティが結果として強化され・向上するという側面があります
- (2)しかしながら、その情報については、悪用というデメリットがあるので、その点についての十分な配慮がなされるべきであり、その一つの方向性を提唱するのが、このガイドラインといえます。
- (3)また、情報自体そのような性格をもつので、発見者についても脆弱性関連情報の管理について真摯な態度が必要とされます。
- (4)そのような真摯な態度を保つ限り脆弱性関連情報についての調査・報告は、社会的に有用なものと考えられます  
しかしながら、管理について真摯な態度を欠く場合については、上述の限りではありません。そのような真摯な態度を欠く場合の具体的な例として

以下があります。

- a) 脆弱性関連情報の公表は、その情報の内容が真実と異なることを知っていた場合、あるいは、真実である場合であっても、特定人の名誉を毀損する意図で公表がなされ、かつ、公共の利益と無関係である場合には、刑法の名誉毀損罪に触れる可能性があります。
- b) 特定人の信用を毀損する意図で事実と異なる脆弱性関連情報を、事実と異なると認識して公表がなされる場合には、刑法の信用毀損罪に触れる可能性があります。
- c) 通常人に求められる程度の相当の注意をもって調査・検証したりしたのではなしに脆弱性関連情報であるとして公表し、かつ、脆弱性関連情報の開示に起因して損害が発生した場合、損害賠償責任などの民事責任を追及される可能性があります。

## 付録2 製品開発者が心得ておくべき法的な問題

製品開発者における法的な位置付けは、以下の通りです。

- (2) ソフトウェ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ェ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。
- (3) もし、提供したソフトウェアにおいて、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。
- (4) もっともその対策方法の選択については、種々の考慮が必要になります。

この対策方法の選択に際しては、以下の点を論点として意識する必要があります。

- (a) 上記の対策方法の選択について、状況に応じて債務不履行責任(民法415条)、不法行為責任(民法709条)、瑕疵担保責任(同法570条、566条、商法526条1項等)の対象となる可能性があります。
- (b) 提供の際の契約で、これを免除する場合については、消費者契約法の適用がある場合には、責任の全部免除が認められない場合があります。
- (c) 製造物責任法上の問題として、現時点において、ソフトウェ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ェ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ます。

### 付録3 ウェブサイト運営者の法的関連事項

ウェブアプリケーションの脆弱性に関する法的な位置づけ、論点は、以下の通りです。

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

## 付録4 具体的な説明

### 1. ウェブサイトの不適切な運用

ウェブサイトの不適切な運用の例を以下に挙げます。

- ・ URLの一部にパスワードが判別可能な形式で明示されている
- ・ 本来閉じられているべき telnet 等のポートが空いており、administrator のパスワードが付与されていない
- ・ ウェブサイト運営者が公開を意図していないファイル(個人情報ファイル等)が、ウェブサーバに、誰にでも閲覧できる状態で(アクセス制限なしに)置かれている等

### 2. ソフトウェア製品

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

### 3. エクスプロイトコード

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

### 4. ワークアラウンド

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

### 5. パッチ

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

### 6. プロトコルの実装に係わる脆弱性

過去に脆弱性の報告があったプロトコルに関連する脆弱性の主なものを以下に挙げます。

- ・ H.323 に係わる脆弱性

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

## 7 . ウェブサイト運営者

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



### 資料3 海外における脆弱性情報取扱ガイドラインの事例

策定機関	CERT/CC	IETF	OIS	ISS	NTBugtraq	@Stake	
策定/更新日付	2000.10.9	2002.2	2003.7.28	2002.11.18		2002.6.5	
脆弱性情報の定義と範囲	定義:規定なし 範囲:検証ツール、公表スケジュール等周辺情報を含む	定義:リスクの増大もしくはセキュリティ上の攻撃(Exploit)に繋がるような、アプリケーション、システム、デバイス、サービスに含まれる全てのバグ、欠陥、動作、出力、結果もしくはイベント	定義:規定された設計に反した動作を引き起こす可能性があり、攻撃されることでシステムの規定されたセキュリティポリシーを侵害可能性のある、ソフトウェアシステムにおける欠陥 範囲:ソフトウェア製品、ハードウェア製品のソフトウェア、ファームウェアコンポーネント	定義:規定無し 範囲:ソフトウェア、ハードウェア、ファームウェア・アプリケーション(製品もしくはフリー配布の一部として開発、提供されるもの)	規定なし 「ホットな話題」としてNTBugtraq List Charterに掲載	定義:規定無し 範囲:セキュリティ脆弱性のある製品	
プレイヤー	情報元 CSIRT、窓口 CSIRT、ベンダ	脆弱性の報告者、製品ベンダ、メンテナ、第三者(機関)、セキュリティコミュニティ、カスタマ、ユーザ	発見者(個人/組織)、ベンダ、コーディネータ、調停者、	発見者(X-Forceの研究者)、ベンダ	報告者、NTBugtraq 編集者(コーディネータ)、ベンダ	発見者(@Stake)、コンピュータ業界のベンダ、顧客、一般	
発見者の規定(第三者、ベンダ内等)	なし(研究者、プログラマ、システム管理者、IT 専門家、等を想定)	なし	区別はされているが、ベンダが発見した場合はガイドラインの範囲外であることが明記されている	ISS 内に設置されたセキュリティ専門家グループの組織である X-Force の研究者	なし	発見者(@Stake)	
発見者の責任	規定なし	ベンダに適切なチャネルで通知する。ベンダに通知できない場合は、コーディネータに通知を依頼する。脆弱性の実証、再現性、既知の情報でないことの確認を行い、既知の情報をベンダに提供する。ベンダとともに検証にあたる。	脆弱性要約報告(VSR)をベンダに提供する。読者がセキュリティアドバイザーの作成者と信頼性を確認する手段を提供する	脆弱性の再現に関する情報(脆弱性情報の詳細、コード、テスト方法等)をベンダに提供する。	脆弱性の再現に必要な情報をベンダに提供する。脆弱性情報の再現性の確認については、まずNTBugtraq 編集者が行なう。	脆弱性の発見を実証する。脆弱性概要報告書(概要、設定における潜在的リスクの範囲、脆弱性再現のための技術的詳細情報、等を含む)を作成する。e-mail でベンダに通知する。	
ベンダの責任	公表された脆弱性情報に対し CERT/CC にフィードバックする。	脆弱性通知窓口の設置 脆弱性の再現、脆弱性の存在有無/既知の脆弱性の判断を行なう。脆弱性発生と特定環境との関連について報告者と検証する。 同類の脆弱性がないことを確認する。 欠陥の基本的な性質を認識した上で、パッチの提供、設定変更、代替手段の提供を行い、不具合の理由や対応内容について報告者とコーディネータに通知する。	受付窓口(個人/組織)を特定し、コンタクト情報をセキュリティレスポンスポリシーに明記する。 発見者との安全な通信手段の確保と、コンタクト情報にその方法を示す。 脆弱性の存在確認後、脆弱性のリスクを削除または低減するパッチを開発、提供する。	X-Force との連絡窓口の確立	脆弱性を再現できるか確認し、脆弱性がバグか特性かを判断する。	自社の Web 上にセキュリティ連絡先を提供する。問題解決のための計画(脆弱性の再現。脆弱性の存在有無、既知の脆弱性の判断、特定環境との関連)を提案する。 同類の脆弱性がないことを確認する。 パッチ、コンフィグレーションの変更、次善策を通知、提供する。	
スケジュール概念の有無	有り	有り	有り	有り	有り	有り	
有	期限(開示/改修/その他)	公表:関係するベンダからパッチの利用可能性、次善策のある無しに関わらず、第1次報告後45日	報告者に対する受信の通知:7日以内(自動の場合は10日以内) 状況報告:7日毎 脆弱性解消:通知後30日以内 公表:報告者、コーディネータと協議の上決定する	発見者に対するVSR受信の通知:7日以内 状況報告:7日毎 発見者からの報告要求の応答:3日以内 調査期間(目標):VSR受領確認後30日	開示:他に取り決めがない限り、最初の通知後30日後	脆弱性の再現性確認期間:48時間 最終期限:14日	@Stakeに対するVSR受信の通知:7日以内 状況報告:7日毎 回避策提供:最初の通知から30日以内 必要時には期間延長要求 公表:@Stakeとベンダでタイムテーブル作成
	条件(延期の場合の条件等)	実際の公表にあたっては、ベンダとの公表スケジュールの調整有り。 特に深刻な脅威については期限短縮 ハードウェアの変更を要求する脅威については期限延長	ベンダが脆弱性の解消に努めており、対応に要する時間が必要な理由を示すことにより期限延長可能	実際の公表日は、パッチ入手可能後、発見者とベンダで協議の上決定。協調して公表する。 公表前に第三者により公表された場合は、個別に対応する。	以下の場合、開示が促進される。 ベンダがパッチ提供、公のMLによる議論、メディアによる報告、ベンダの反応無し、等	ベンダが提出した修正スケジュールを報告者とNTBugtraq 編集者が判断して延長決定。 報告者はベンダの対応に満足しない場合、期限の短縮を希望できる。	ベンダが脆弱性の解決に誠意ある努力をしている場合、解決策の発見、作成がなされるまで脆弱性情報の公表を延期する。 第三者が脆弱性情報の公表に合意しない場合、30日を上限に猶予期間を認める。
開示	情報の内容	勧告:影響を受けるシステム、解説、影響、対策	規定なし	影響を受ける製品名とバージョン、プラットフォーム、影響、脆弱性識別子、概要、詳細、勧告、利害関係通告、署名情報	勧告、警報:要約、影響、影響を受けるバージョン、詳細、修正案、その他関連情報 概要:要約、影響を受けるバージョン 脅威分析サービス(XFTAS):脆弱性、ウイルス/ワームの脅威の現状と予測、推奨修正策とアドバイスリンク(無償購読サービス)	影響を受ける製品名とバージョン、プラットフォーム、CVE候補、概要、修正情報、参考資料	勧告:影響を受ける製品名とバージョン、プラットフォーム、重大度、著者、ベンダステータス、CVE候補、参考資料、概要、詳細、ベンダ対応、勧告、公表方針、署名情報
	範囲(一般/特定等)	ベンダ、専門家コミュニティ、CERT/CC スポンサー、Internet Security Alliance、国家重要インフラ施設、等 勧告はWebサイト上で公表される。	規定なし	調査期間中:インターネット、重要インフラ、ユーザセキュリティに対して重大な役割を果たす特定の対象者(個人/組織) 調査期間終了後:一般	勧告、警報:Webサイト上で公表される。 概要:ISS警戒ML、FIRST、ISSフォーラム、Vuln-Watch 脅威分析サービス(XFTAS):サービス加入者のみ部外秘(再配布は許可されていない。)	NTBugtraq 契約者	@Stakeの顧客、ベンダの顧客、一般 セキュリティ勧告:一般。ただし、一般公表の前に、特定ユーザや組織に公表される場合もある(限界公表)
発見者の保護規定	規定なし	規定なし	規定なし	規定なし	規定なし	規定なし	