

平成16年7月8日  
経済産業省

## 「情報セキュリティ早期警戒パートナーシップ」の運用を開始

～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」、本日より施行～

経済産業省では、情報セキュリティ早期警戒体制の拡充・強化の一環として、ソフトウェア製品や Web サイト等に内在する安全性上の問題箇所（脆弱性）への対応を促進すべく、本日より上記経済産業省告示を施行し、関係機関にてソフトウェア等の脆弱性関連情報流通を図る「情報セキュリティ早期警戒パートナーシップ」の運用を開始した。

### 1. 概要

昨年8月に発生したMS ブラスターや本年5月に発生したサッサーなど、コンピュータウイルス・不正アクセス等の攻撃は、ソフトウェアの脆弱性<sup>( )</sup>を悪用することによってより高度化・効率化しており、被害拡大のスピードは、ユーザが対処可能なスピードを遙かに超える勢いで早まりつつある。

( )「脆弱性」とは、「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。

こうした状況に対処すべく、経済産業省では、情報セキュリティ問題の早期警戒体制の構築・拡大の一環として、昨年11月から独立行政法人情報処理推進機構（IPA）に委託し官民の関係有識者による研究会を開催した。本年4月に公表された研究会の提言<sup>1</sup>に基づき、経済産業省や関係機関・団体において、以下の取り組みが進められてきた。

経済産業省では公的ルールの位置づけを検討し、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**」として7月7日に制定（官報掲載）し、本日から施行。

（別添1参照）

また、これに合わせて、IPA、有限責任中間法人 JPCERT コーディネーションセンター（JPCERT/CC）、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）、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）、特定非営利法人日本ネットワークセキュリティ協会（JNSA）では、本枠組みに参画

<sup>1</sup> 「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/about/press/20040406.html>）

する関係者及び関係業界としての指針「情報セキュリティ早期警戒パートナーシップガイドライン」(以下「**パートナーシップガイドライン**」という。)を連名で発表(別添2参照)。また、IPA、JPCERT/CCでは、**脆弱性関連情報の取扱業務を本日から開始**(別添3,4参照)。

さらに、7月中旬に公表される予定である、ソフトウェア製品の開発者が脆弱性関連情報を扱う上での業務プロセスや社内体制等の在り方を示す「**(仮称)製品開発者向けガイドライン**」(JEITA及びJISA連名)、ソフトウェア製品開発者における脆弱性関連情報の窓口担当者が把握すべき作業事項を示す「**(仮称)窓口担当者向けマニュアル**」(JPCERT/CC)等を活用することにより、本制度の実効的な運用をめざす。

経済産業省では、こうした一連の取り組みを通じて、官民連携したソフトウェア等の脆弱性関連情報流通の枠組み ~ **情報セキュリティ早期警戒パートナーシップ** ~ の円滑な運用を促進し、高信頼性社会の実現をめざす所存である。

## 2. ポイント

### (1) 早期警戒体制の枠組みの強化・拡充の一環として構築

経済産業省では、1990年から、「コンピュータウイルス・不正アクセス届出事業」を、2003年から「インターネット定点観測事業」を実施し、届出情報や観測データ等の分析・公表によって、被害の局限化を図る情報セキュリティ問題の早期警戒体制を整備してきた。

しかし、コンピュータウイルスや不正アクセスによる攻撃がソフトウェアの脆弱性を悪用したものと発展しつつあることから、早期警戒体制の対象をソフトウェア製品及びWebサイトの脆弱性に広げ、その対策を官民連携して促進することで、被害の発生そのものを未然に抑制することをめざすこととした。

### (2) 告示において関係者に望まれる行動基準を規定

情報セキュリティ早期警戒パートナーシップを推進する手段として、経済産業省では経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」を制定した。本告示では、ソフトウェア製品またはWebアプリケーションの脆弱性関連情報に関する基本的な処理の流れと、関係者(発見者、受付機関、調整機関、製品開発者、Webサイト運営者)に望まれる行動基準を規定している。また、告示では、受付機関としてIPA、調整機関としてJPCERT/CCを指定した。

### (3) 自らの役割を宣言する「パートナーシップガイドライン」を関連機関・団体が連名で公表

「パートナーシップガイドライン」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」を踏まえ、脆弱性関連情報に関する処理の流れや取り組む行動

をより詳細に示すとともに、関係者が担う役割や推奨される事項を明示した指針である。IPA、JPCERT/CC、JEITA、JISA、JPSA、JNSA が連名で公表した。

#### **(4) IPA、JPCERT/CC が脆弱性関連情報の取扱業務を開始**

告示が本日（7月8日）より施行されたのを受けて、受付機関である IPA、調整機関である JPCERT/CC において脆弱性関連情報の取扱業務を本日から開始した。

#### **(5) JEITA、JISA による製品開発者向けガイドライン等も公表予定**

本枠組みに参画するソフトウェア製品の開発者においては、脆弱性関連情報の通知に伴い対策を策定する上で、社内の体制や手続き、情報管理ルール等を調整する必要が生じる。そこで、JEITA では、製品開発者の社内体制やルール等の在り方を検討する WG を設置、JISA メンバーを加え、検討を重ねている。7月中旬には検討成果を「(仮称)製品開発者向けガイドライン」としてとりまとめ、JEITA 及び JISA の連名で公表する予定である。

また、JPCERT/CC でも、製品開発者における脆弱性関連情報の窓口担当者が把握すべき作業事項を示す「(仮称)窓口担当者向けマニュアル」を策定中であり、7月中旬に公表する予定としている。

### **3 . 期待効果**

上記の取り組みは、情報セキュリティ早期警戒パートナーシップの基盤強化とその円滑な立ち上げを促進するものである。情報セキュリティ早期警戒パートナーシップを本格運用することによって、以下の効果が期待される。

ソフトウェア製品開発者及び Web サイト運営者による脆弱性対策を促進

脆弱性関連情報の放置・危険な公表を抑制

個人情報等重要情報の流出や重要システムの停止を予防

### **4 . 今後の予定**

情報セキュリティ早期警戒パートナーシップの実効的な運用のためには、発見者からの脆弱性関連情報の届出促進（取扱業務の周知）と、ソフトウェア製品開発者側の積極的な参画が不可欠である。このため、本事業に関する説明会（主催：IPA、JPCERT/CC）を7月中～下旬に全国5カ所にて開催し、関係者への啓発を促す予定である。（<http://www.ipa.go.jp/security/vuln/event/20040720.html>）

また、公表した脆弱性対策の情報をユーザに適切に活用してもらえよう、企業ユーザや個人ユーザの対策適用を促すしくみについても検討を進める。

さらに、本制度を一定期間運用した上で、関係者によるフォローアップを行い、実務的な問題点を洗い出し、本格的な運用に向けてさらなる改善を進めて参りたい。

(本発表資料のお問い合わせ先)

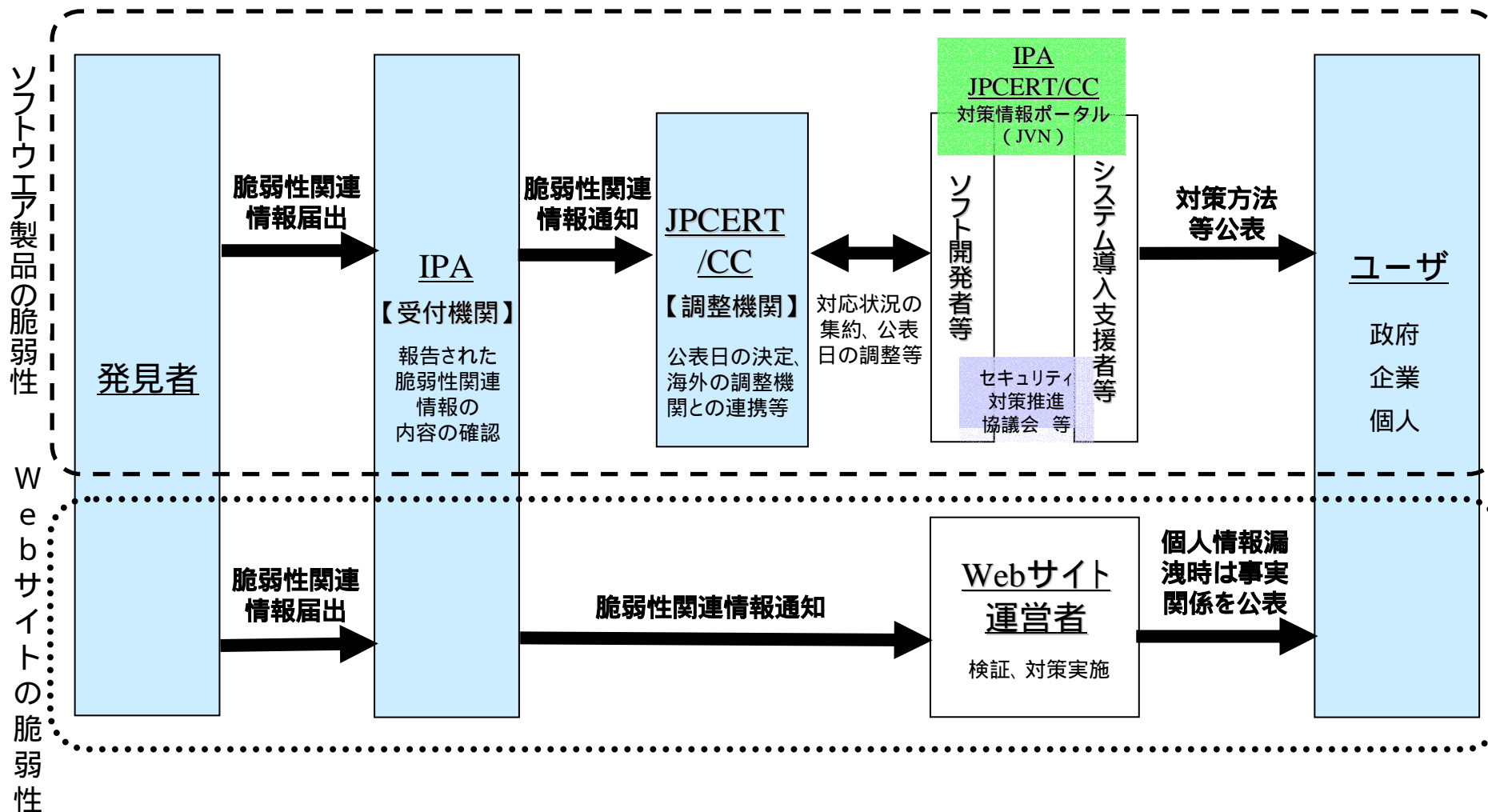
商務情報政策局 情報経済課 情報セキュリティ政策室

担当者：川口、佐藤

電話：03 - 3501 - 1511 (内線 3961)

03 - 3501 - 0397 (直通)

官民連携の体制で、ソフトウェア製品やWebアプリケーションの脆弱性関連情報の円滑な流通と対策の普及促進を図る。



## 業界側の参加促進

<7月中旬発表予定>

### 窓口担当者向けマニュアル

【JPCERT/CC】

製品開発者における脆弱性関連情報の窓口担当者が把握すべき作業事項

<7月中旬発表予定>

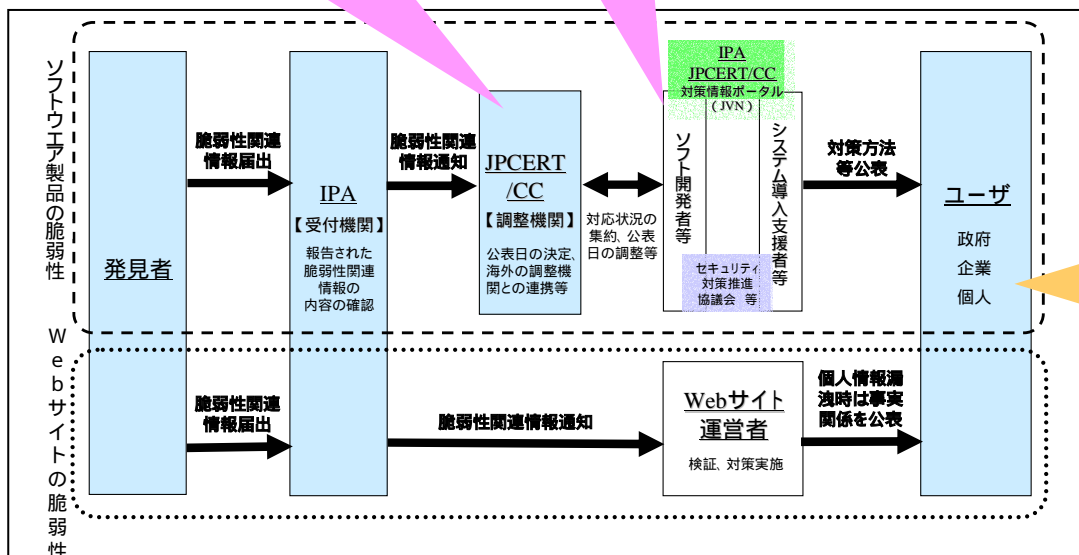
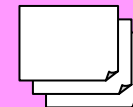
### 製品開発者ガイドライン

【JEITA, JISA】

脆弱性関連情報を扱う上で業務プロセスや社内体制等の在り方を提示

波及効果

他の業界団体版  
ガイドライン



## ユーザ側の対策促進

ユーザ側から見た、脆弱性問題に関する改善方策の検討

## 官民連携した枠組みの支持

<7月7日制定>

### ソフトウェア等脆弱性関連情報取扱基準

(経済産業省告示)

- 脆弱性関連情報の基本枠組みを規定
- 関係者に求められる役割を要請

<7月8日公表>

### パートナーシップガイドライン

【IPA, JPCERT/CC, JEITA, JISA, JPSA, JNSA】

枠組みに参加する関係者及び関係業界が、自らの役割や推奨される事項を明示した指針

経済産業省告示第二百三十五号

ソフトウェ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

## ソフトウェア等脆弱性関連情報取扱基準

### . 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、以下のとおりとする。

#### 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。

### ．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で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

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ェア製品に限らない場合

対象がソフトウェア製品であり、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ェ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。

- ( ) 発見者は、脆弱性関連情報を受付機関に届け出る。
- ( ) 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。
- ( ) 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ェ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。
- ( ) 調整機関は、当該脆弱性情報の公表日を定める。
- ( ) 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。
- ( ) 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ェ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。
  - 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。

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

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

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

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

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ェ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ェ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ェア製品に限られる場合

対象がソフトウェア製品であり、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ェ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ェ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。

## ．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。

- ( ) 発見者は、脆弱性関連情報を受付機関に届け出る。
- ( ) 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。
- ( ) 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が妨げない。
- ( 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。

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

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

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

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

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ェ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

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

独立行政法人 情報処理推進機構  
有限責任中間法人 JPCERT コーディネーションセンター  
社団法人 電子情報技術産業協会  
社団法人 日本パーソナルコンピュータソフトウェア協会  
社団法人 情報サービス産業協会  
特定非営利活動法人 日本ネットワークセキュリティ協会

．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。そこで、脆弱性関連情報が発見された場合に、それらをどのように取り扱うべきかを示した、経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」が制定されました。

本ガイドラインは、上記告示をふまえ、脆弱性関連情報の適切な流通により、コンピュータ不正アクセス、コンピュータウイルスなどによる被害発生を抑制するために、関係者に推奨する行為をとりまとめたものです。具体的には、独立行政法人 情報処理推進機構（以下、「IPA」とする）が受付機関、有限責任中間法人 JPCERT コーディネーションセンター（以下、「JPCERT/CC」とする）が調整機関という役割を担い、発見者、製品開発者、ウェブサイト運営者と協力をしながら脆弱性関連情報に対処するための、その発見から公表に至るプロセスを詳述しています。

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

## ．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等において、コンピュータ不正アクセスやコンピュータウイルス等の攻撃により、その機能や性能を損なう原因となり得るセキュリティ上の問題箇所です。

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

#### 1) 脆弱性情報

脆弱性の性質及び特徴を示す情報のことです。

#### 2) 検証方法

脆弱性が存在することを調べるための方法です。例えば、特定の入力パターンにより脆弱性の有無を検証するツール等が該当します。

#### 3) 攻撃方法

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

### 3．対策方法

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

#### 1) 回避方法

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

#### 2) 修正方法

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

#### 4．対応状況

調整機関から脆弱性関連情報の通知を受けた製品開発者が報告する製品開発者の脆弱性に関する対策方法、取り組みの状況などを含む対応状況のことです。

#### 5．ソフトウェア製品

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、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。

#### 6．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。

#### 7．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。

#### 8．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。

#### 9．脆弱性検証

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

#### 10．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

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、多くの人々に利用されている等のソフトウェア製品が該当します。プロトコルを実装しているものも含まれます。(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。

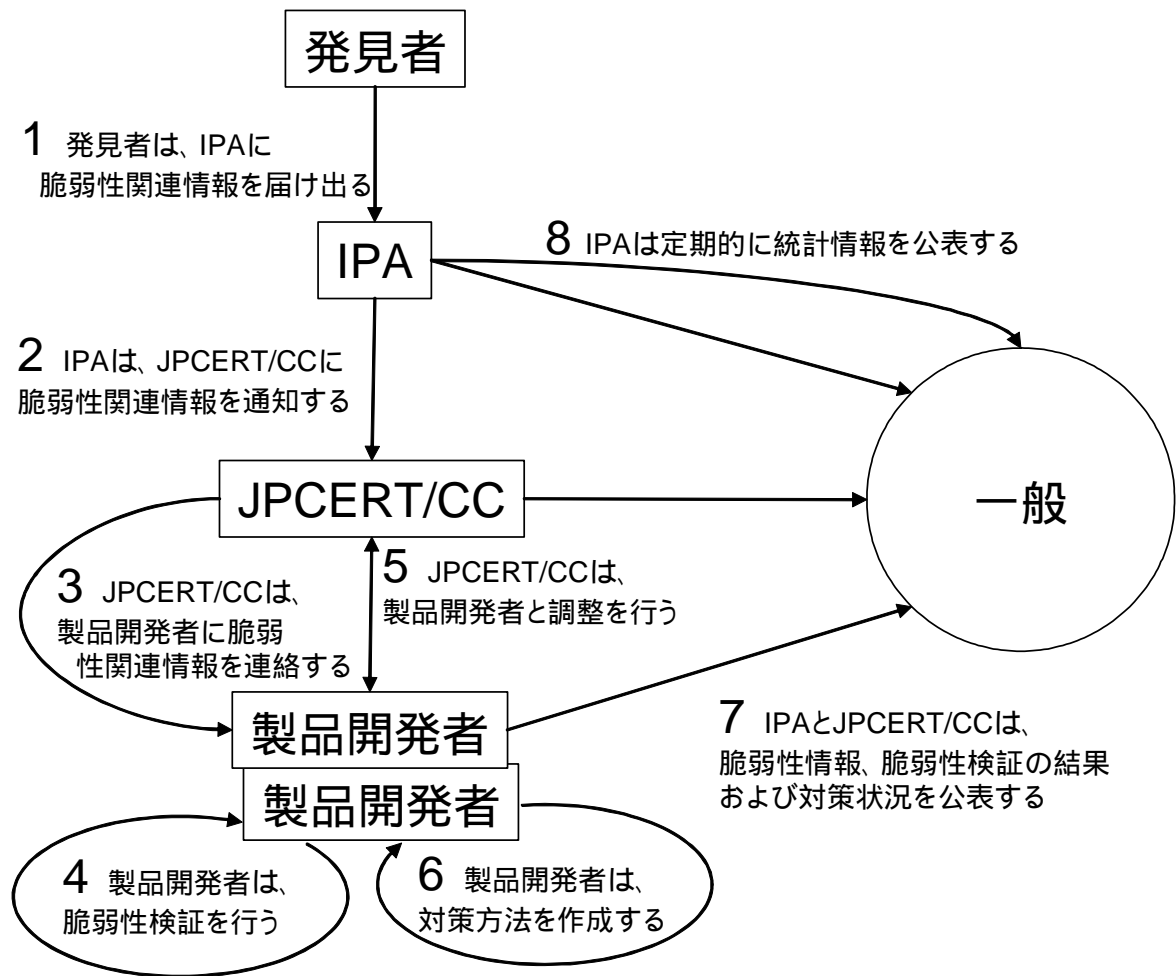


図1 ソフトウェア製品に係る脆弱性関連情報取扱の概要

- 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 に通知する
- 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通知する
- 4) 製品開発者は、脆弱性検証を行い、その結果を JPCERT/CC に報告する
- 5) JPCERT/CC と製品開発者は、脆弱性情報の公表に関するスケジュール調整し

決定する

- 6) 製品開発者は、脆弱性情報の公表日までに対策方法を作成するよう努める
- 7) IPA および JPCERT/CC は、脆弱性情報と、3)にて JPCERT/CC から連絡した全ての製品開発者の脆弱性検証の結果および対応状況を公表する
- 8) IPA は、統計情報を少なくとも一年に一度は公表する

## 2. 発見者の対応

### 1) 発見者の範囲

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類似の脆弱性があると推定されるものを発見・取得した場合、発見者としての対応が推奨されます。

### 2) 脆弱性関連情報の発見・取得

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

### 3) 脆弱性関連情報の届出

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

### 4) 脆弱性関連情報の管理および開示

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

### 5) 届け出る情報の内容

発見者は、届け出る情報の中で以下の点を明示してください（詳細は、<http://www.ipa.go.jp/security/vuln/> を参照してください）。

- ・発見者の氏名・連絡先
- ・脆弱性関連情報に関連する製品の具体的な名称

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

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

発見者が望む場合、IPA および JPCERT/CC は、脆弱性情報と製品開発者毎の脆弱性検証の結果および対応状況を公表する際に発見者名を付記するとともに、製品開発者に対しても、対策方法の公表時に発見者名を付記することを推奨します。

#### 6) 製品開発者との直接の情報交換

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

#### 7) 届出後の対応

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

### 3 . IPA および JPCERT/CC の対応

#### (1) IPA

##### 1) 脆弱性関連情報の受付

脆弱性関連情報の受付に関し、詳細は以下の URL を御参照ください。

<http://www.ipa.go.jp/security/vuln/>

受付は 24 時間ですが、作業は原則営業日となります。

##### 2) 届出の受理

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

- (ア) 原則として、上記 2 . 5) の項目が十分に記述されていること
- (イ) 匿名の届出でないこと（発見者への連絡が可能であることを確認できること）
- (ウ) 脆弱性関連情報であること（一般のバグ情報ではないこと）

(エ) 既に報告されている脆弱性関連情報ではないこと

なお、IPA は、これらの条件により、届出の受理または不受理を判断し、その理由とともに発見者に連絡します。なお、届出の受理を発見者にした日時が IPA および JPCERT/CC が脆弱性関連情報の取り扱いを開始した日時となります（(2) 3) 一般への公表日の決定 参照）。

3) 違法な手段で入手された脆弱性関連情報への対応

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

4) JPCERT/CC への連絡

IPA は、上記 2)、3)における対応の是非の判断の結果、対応することが妥当との判断を下した脆弱性関連情報について、速やかに JPCERT/CC に通知します。

5) 脆弱性関連情報の取り扱い

IPA は、脆弱性関連情報に関して、それに関する脆弱性情報が一般に公表されるまでの間は、発見者・JPCERT/CC・当該製品開発者以外の第三者に提供しないように適切に管理します。ただし、脆弱性が再現する状況を特定できない等止むを得ない理由がある場合、IPA は、守秘契約を結んだ上で、外部機関に脆弱性関連情報に関する技術的分析を依頼することがあります。

6) 発見者に係わる情報の取り扱い

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

7) 脆弱性関連情報の受理後の対応

IPA は、JPCERT/CC に通知した脆弱性関連情報に関して、JPCERT/CC から既知の脆弱性であるまたは脆弱性ではない等の理由により脆弱性情報の公表の中止の連絡を受けた場合、発見者に連絡するとともに、処理を取りやめることがあります。

8) 発見者との情報交換

IPA は、届出を受理した後、発見者に問い合わせをすることがあります。また、発見者から問い合わせがあった場合、JPCERT/CC と相談の上、適切な情報の開

示を行います。なお、発見者との情報交換に際しては、第三者に情報が漏洩しないよう留意します。

#### 9) 対応状況の受付

IPA は、JPCERT/CC を介して連絡した脆弱性関連情報に係わる製品開発者の対応状況を、JPCERT/CC と共有します。

#### 10) 優先的な情報提供

IPA は、届出がなされた脆弱性関連情報に関して、重要インフラに対し特に影響が大きいと推察される場合、JPCERT/CC および製品開発者と協議の上、脆弱性情報の一般公表より前に、脆弱性関連情報と対策方法を、政府機関や重要インフラ事業者等に対して優先的に提供することがあります。この際、発見者に対して、その旨を通知します。重要インフラ事業者には、情報通信、金融、航空、鉄道、電力、ガス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。

#### 11) 一般への情報の公表

IPA および JPCERT/CC は、一般に対し、脆弱性情報と JPCERT/CC から連絡した全ての製品開発者の脆弱性検証の結果と対応状況をインターネット上で公表します。さらに、一旦公表した後、製品開発者から新たな対応状況を受け取った場合、その都度公表します。なお、脆弱性検証の結果の報告および対応状況の報告がない場合、IPA および JPCERT/CC は、その旨を、製品開発者名とともにインターネット上で公表することがあります。

一般への情報の公表に際しては、IPA は、発見者にその旨を通知します。

#### 12) 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、届出件数の時間的推移等が含まれます。

### (2) JPCERT/CC

#### 1) 製品開発者リストの整備

JPCERT/CC は、製品開発者に対して脆弱性関連情報を連絡するために、日頃よ

り製品開発者リストの整備に努めます。この製品開発者リストには、製品開発者毎に、製品の情報、社名、窓口等を登録します。

## 2) 製品開発者への連絡

JPCERT/CC は、届け出られた脆弱性関連情報の IPA からの通知を受け、製品開発者リストの活用や脆弱性関連情報を分析することにより、速やかに製品開発者を特定し、必要に応じて製品開発者リストに当該製品開発者を追加した上で、その製品開発者に連絡を行います。その際に、各製品開発者に対して、脆弱性検証を行い、その結果を報告することを求めます。

## 3) 一般への公表日の決定

JPCERT/CC は、製品開発者から脆弱性検証の結果を受け取り、製品開発者と相談した上で、脆弱性情報と製品開発者の対応状況の公表日を決定し、IPA および関係する製品開発者に通知します。公表日は、JPCERT/CC および IPA が脆弱性関連情報の取り扱いを開始した日時（(1) 2）参照）から起算して、45 日後を目安とします。ただし、公表日の決定に際しては、以下の点も考慮します。

- ・ 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
- ・ 脆弱性情報流出に係わるリスク

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

## 4) 公表日決定後の対応

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

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

- ・ 通知を行ったすべての製品開発者から既知の脆弱性情報であるとの連絡を受けた場合
- ・ 通知を行ったすべての製品開発者から脆弱性による影響がないとの連絡を受けた場合

## 5) JPCERT/CC における脆弱性関連情報の取り扱い

JPCERT/CC は、脆弱性情報を一般に公表するまでは、第三者に漏洩しないように管理します。ただし、海外製品であり外国企業の日本法人や総代理店が無い場合、海外に大きな影響を与える脆弱性関連情報の場合、および脆弱性関連情報の詳細な分析が必要な場合などは、秘密保持契約を締結した上で、海外の調整機関または IPA を含む外部機関に連絡や分析を依頼することがあります。

#### 6) 対応状況の受付

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

#### 7) 一般への情報の公表

JPCERT/CC および IPA は、一般に対し脆弱性情報と JPCERT/CC から連絡した全ての製品開発者の脆弱性検証の結果と対応状況をインターネット上で公表します。さらに、一旦公表した後、製品開発者から新たな対応状況を受け取った場合、その都度公表します。なお、脆弱性検証の結果の報告および対応状況の報告がない場合、JPCERT/CC および IPA は、その旨を、製品開発者名とともにインターネット上で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な論点は、付録 2 に示します。

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

#### 1) 窓口の設置

製品開発者は、JPCERT/CC との間で脆弱性関連情報に関する情報交換を行うための窓口を設置し、あらかじめ JPCERT/CC に連絡してください。この窓口が、JPCERT/CC の製品開発者リストに登録されることとなります。

#### 2) 脆弱性検証の実施

製品開発者は、JPCERT/CC から脆弱性関連情報を受け取ったら、ソフトウェア製品への影響を調査し、脆弱性検証を行い、その結果を JPCERT/CC に報告し

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

### 3) 脆弱性情報の一般への公表日の調整

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

### 4) 発見者との直接の情報交換

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

### 5) 問い合わせへの対応

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

### 6) 対応状況の連絡と対策方法の作成

製品開発者は、脆弱性情報の一般の公表日までに、脆弱性関連情報に係わる対応状況を JPCERT/CC に連絡するとともに、脆弱性関連情報に係わる対策方法を作成するよう努めてください。JPCERT/CC に対する対応状況の報告をもって、IPA にも報告したとみなされます。また、対応状況が変わった場合、その都度、JPCERT/CC に最新の情報を連絡してください。

### 7) 対策方法の周知

製品開発者は、対策方法を作成した場合、脆弱性情報一般公表日以降、それを利用者に周知してください。

### 8) 製品開発者内の情報の管理

製品開発者は、上記 2) で作成した脆弱性情報の一般公表スケジュールおよび脆弱性関連情報を、脆弱性情報を一般に公表する日まで第三者に漏洩しないように管理してください。

## 5 . その他

1) 製品開発者自身による脆弱性関連情報の発見・取得

製品開発者は、自社のソフトウェア製品についての脆弱性関連情報であつて、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、JPCERT/CC に連絡することができます。この連絡をもって、IPA および JPCERT/CC に連絡したこととみなされます。

2) IPA および JPCERT/CC による普及支援

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

## ウェブアプリケーションに係る脆弱性関連情報取扱

### 1. 概要

ウェブアプリケーションに係る脆弱性関連情報取扱概要は、図2の通りです。

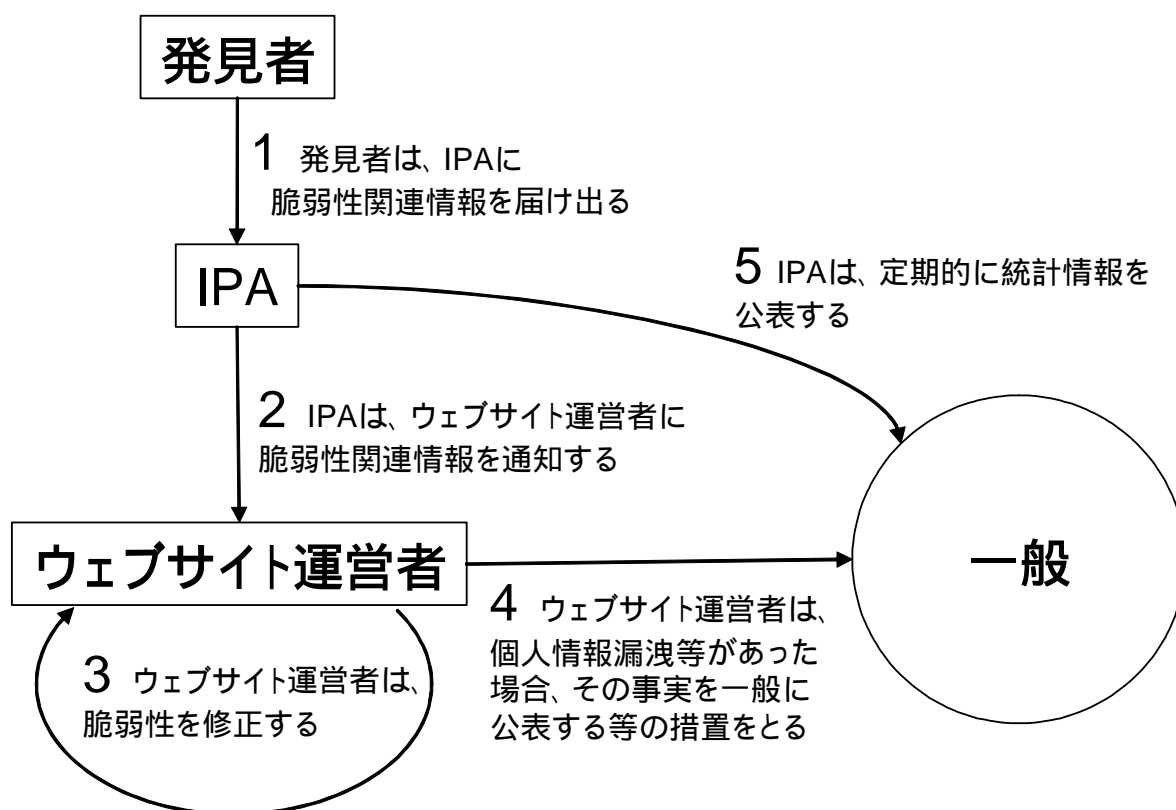


図2 ウェブアプリケーションに係る脆弱性関連情報取扱概要

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

## 2. 発見者の対応

### 1) 脆弱性関連情報の発見・取得

脆弱性関連情報の発見・取得に際しては、関連法令に触れることが無いように留意してください。法的な論点に関しては、付録 1 を参照してください。

### 2) 脆弱性関連情報の届出

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

### 3) 脆弱性関連情報の管理および開示

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

### 4) 届け出る情報の内容

発見者は、届け出る情報の中で以下の点を明示してください（詳細は、<http://www.ipa.go.jp/security/vuln/> を参照してください）。

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

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

### 5) ウェブサイト運営者との直接の情報交換

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

### 6) 届出後の対応

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

### 3 . IPA の対応

#### 1) 脆弱性関連情報の受付

脆弱性関連情報の受付に関し、詳細は以下の URL を御参照ください。

<http://www.ipa.go.jp/security/vuln/>

受付は 24 時間ですが、作業は原則営業日となります。

#### 2) 届出の受理

IPA は、上記 2 . 4) の項目が十分に記述されていると判断した時、その時点で届出を受理し、発見者に連絡します。

#### 3) 違法な手段で入手された脆弱性関連情報への対応

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

#### 4) ウェブサイト運営者への連絡

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

#### 5) 脆弱性関連情報への対応続行の判断

IPA は、以下の条件のいずれかと合致した場合、処理を取りやめるとともに発見者に連絡します。

(ア) IPA が脆弱性関連情報でないと確認した場合

(イ) IPA が既に報告されている脆弱性関連情報であると確認した場合

(ウ) ウェブサイト運営者から脆弱性関連情報でないと連絡があった場合

(エ) ウェブサイト運営者から既知の脆弱性関連情報であると連絡があった場合

#### 6) ウェブサイト運営者への連絡

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

#### 7) 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ることがあります。また、発見者から問い合わせがあった場合、ウェブサイト運営者と相談の上、適切な情報の開示を行います。

#### 8) 脆弱性関連情報の管理

IPA は、脆弱性関連情報に関して、発見者・ウェブサイト運営者以外の第三者に提供しないように適切に管理します。ただし、脆弱性が再現する状況を特定できない等止むを得ない理由により IPA が外部機関に脆弱性関連情報に関する技術的分析を依頼する場合、IPA は守秘契約を結びます。

#### 9) 発見者の個人情報の管理

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

#### 10)脆弱性の修正の通知

IPA は、ウェブサイト運営者から脆弱性を修正した旨の通知を受けた場合、それを速やかに発見者に通知します。

#### 11)統計情報の集計と公表

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

### 4 . ウェブサイト運営者

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

ウェブサイト運営者における法的な論点は、付録3に示します。

以下で、ウェブサイト運営者が対応すべき事項を説明します。

#### 1) 脆弱性関連情報への対処

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

#### 2) 問い合わせへの対応

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

#### 3) 発見者との直接の情報交換

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

#### 4) ウェブサイト運営者内での情報の管理

ウェブサイト運営者は、脆弱性が修正されるまでの間は、脆弱性関連情報を第三者に漏洩しないように管理してください。ただし、ウェブサイト運営者が脆弱性修正を依頼した外部機関、およびウェブサイトの管理を委託している外部機関には、秘密保持契約を締結した上で脆弱性関連情報を連絡することがあります。

#### 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ください。

- ・ 個人情報漏洩の概要
- ・ 漏洩したと推察される期間

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

## 付録1 発見者が心得ておくべき法的な論点

発見者が心得ておくべき法的な問題に関する法律専門家の見解を述べます。脆弱性発見と脆弱性関連情報の管理に関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 通常国会にて改正された電波法に触れる可能性があります。

#### (2) 不正アクセス禁止法に抵触しないと推察される行為の例

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

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

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

- 3) アクセス制御による制限を免れる目的ではなく、通常の高い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。
- (2) 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。
- (3) もっともその対策方法の選択については、種々の考慮が必要になります。

この対策方法の選択に際しては、以下の点を論点として意識する必要があります。

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

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

- 1) ウェブサイト運営者と、ユーザとの間においては、そのウェブアプリケーションの利用に際して、一定の契約関係にはいると考えられます。そして、ユーザが、そのサイトに一定の個人情報などをゆだねる場合には、ウェブサイト運営者は、そのサイトの利用契約に付随した義務として一定レベルのセキュリティ維持を果たすべき義務を負担していると考えられます。
- 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。

2004年7月8日  
独立行政法人 情報処理推進機構

## ソフトウェア等脆弱性関連情報に関する届出の受付開始について

独立行政法人 情報処理推進機構（略称 IPA、理事長：藤原 武平太）は、2004年7月8日より、ソフトウェア等の脆弱性関連情報に関する届出の受付を開始します。

IPA は、昨年 11 月から、「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 中央大学教授）を開催し、ソフトウェア等の脆弱性に関する情報を必要な機関間で流通させるとともに、有効な対策方法を迅速かつ正確にユーザに供給することを目的として、脆弱性の発見から、対策の策定・公表に至るまでの関連情報の取扱いのあり方について検討を行いました。この検討結果を、去る 4 月に研究会報告書として公表するとともに、経済産業省に対して提言しました。

これを踏まえ、7月7日、経済産業省は、告示で、脆弱性関連情報が発見された場合にそれらをどのように取り扱うべきかを示した「ソフトウェア等脆弱性関連情報取扱基準」を制定するとともに、脆弱性関連情報の届出の受付機関として IPA、脆弱性関連情報に関して製品開発者への連絡及び公表に関わる調整機関として有限責任中間法人 JPCERT コーディネーションセンター（JPCERT/CC）を指定しました。

また、上記告示を受けて、IPA、JPCERT/CC、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）、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）及び特定非営利活動法人 日本ネットワークセキュリティ協会（JNSA）では、本日、脆弱性関連情報の流通に関わる関係者、関係業界としての指針「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」を連名で公表しました（7月8日付プレスリリース「情報セキュリティ早期警戒パートナーシップガイドラインの公表について」ご参照）。

IPA は、上記告示の施行に伴い、本日より脆弱性関連情報の届出の受付を開始します。

### 1. 届出を受け付ける脆弱性関連情報について

IPA は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わる情報の届出を受け付けます。脆弱性関連情報の取扱いについては、ホームページで詳細を掲載していますので、そこから届出様式、届出様式記入の手引きなどを参照してください。

届出は、当初、電子メールで受け付けます。届出に際しては、ネットワーク経路における盗聴などにより、未対策の脆弱性情報が漏洩することを防ぐため、PGP 暗号鍵による暗号化を施した上で、下記アドレス宛に届出をお願いします。また、ウェブによる届出システムを今秋運用開始する予定です。

脆弱性関連情報取扱いホームページ	<a href="http://www.ipa.go.jp/security/vuln/index.html">http://www.ipa.go.jp/security/vuln/index.html</a>
届出メールアドレス	<a href="mailto:vuln-info@ipa.go.jp">vuln-info@ipa.go.jp</a>
PGP 暗号鍵	<a href="http://www.ipa.go.jp/security/pgp/index.html">http://www.ipa.go.jp/security/pgp/index.html</a>

- ソフトウェア製品の脆弱性関連情報について

OS やブラウザ等のクライアント上のソフトウェア、データベース管理ソフトウェアやウェブサーバ等のサーバ上のソフトウェア、ソフトウェアを組み込んだハードウェア等において、セキュリティ上の問題箇所を発見した場合に届け出てください。主な届出内容は、以下の通りです。

項目	内容
届出者情報	氏名、連絡先、届出者情報の取扱い（調整機関あるいは製品開発者へ知らせても良いかどうか、対策公表時の掲載希望の有無）など
脆弱性関連情報	脆弱性を発見したソフトウェアの名称、動作環境、脆弱性の再現手順、発生し得る脅威、回避策など
他組織への届出状況	IPA に届出を行う前に、IPA 以外の組織へ届出を行ったかどうか
今後の連絡について	最終的な修正の報告を希望するか、連絡時に暗号化を希望するか、など

- ウェブアプリケーションの脆弱性関連情報について

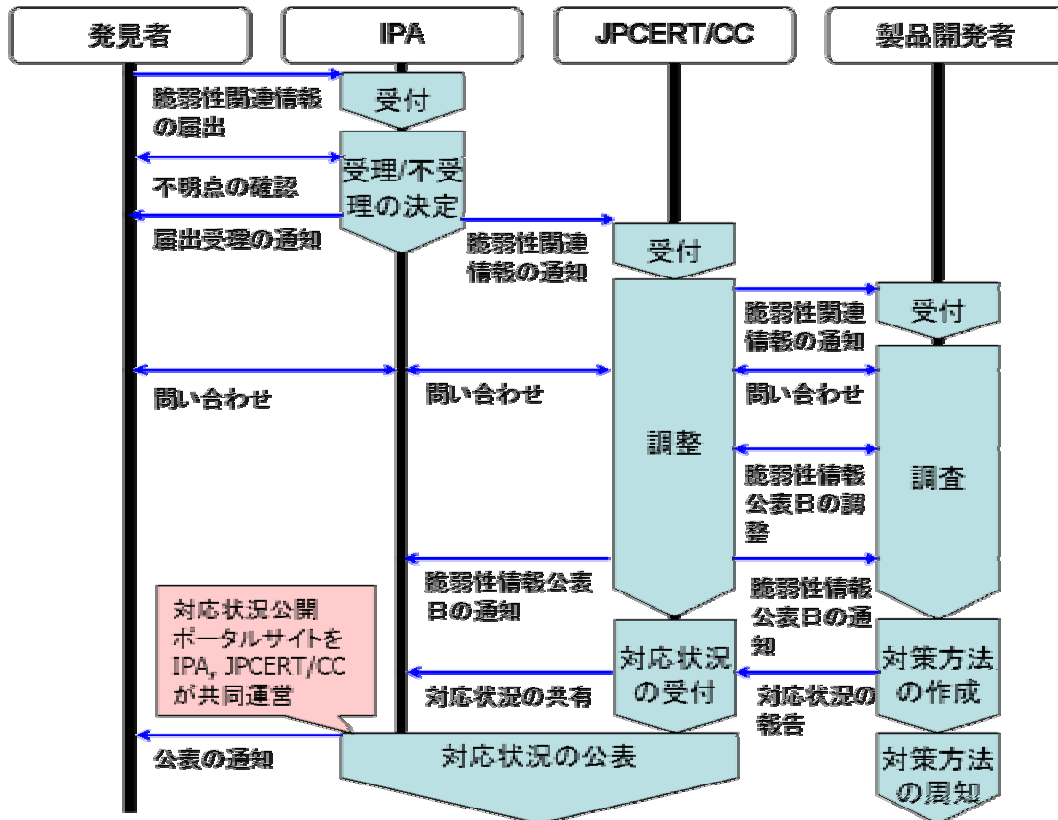
インターネットのウェブサイトなどで、公衆に向けて提供するそのサイト固有のサービスを構成するシステムにおいて、セキュリティ上の問題箇所を発見した場合に届け出てください。主な届出内容は、以下の通りです。

項目	内容
届出者情報	氏名、連絡先、届出者情報の取扱い（ウェブサイト運営者へ知らせても良いかどうか）など
脆弱性関連情報	脆弱性を発見したウェブサイトの URL、どのような脆弱性か、どのような状況で脆弱性を発見したか、など
他組織への届出状況	IPA に届出を行う前に、IPA 以外の組織へ届出を行ったかどうか
今後の連絡について	最終的な修正の報告を希望するか、連絡時に暗号化を希望するか、など

## 2. 届出後の脆弱性関連情報の取扱いプロセスについて

届け出られた脆弱性関連情報のうち、ソフトウェア製品に関する脆弱性関連情報については、IPA が内容を確認した上で、JPCERT/CC に通知します。ウェブアプリケーションの脆弱性関連情報については、IPA から直接ウェブサイト運営者に通知します。

ソフトウェア製品の脆弱性関連情報の取扱いプロセス



届出の受付

発見者からの届出を受け付けます。

届出情報の確認

記入項目に不備がないこと、既知の脆弱性情報ではないことなどを確認し、発見者への確認が必要な場合は連絡します。

届出受理の通知

の結果を踏まえ、届け出られた情報を受理するかどうかを判断します。受理する場合は、IPA から発見者へ届出を受理した旨をメールにて通知します。

JPCERT/CC への脆弱性関連情報の通知

脆弱性関連情報を、JPCERT/CC に通知します。脆弱性関連情報は、JPCERT/CC から製品開発者に通知します。

脆弱性に関する問い合わせ

製品開発者が脆弱性の存在有無を確認する際に、発見者の了解がある場合には、問い合わせをさせていただくことがあります。

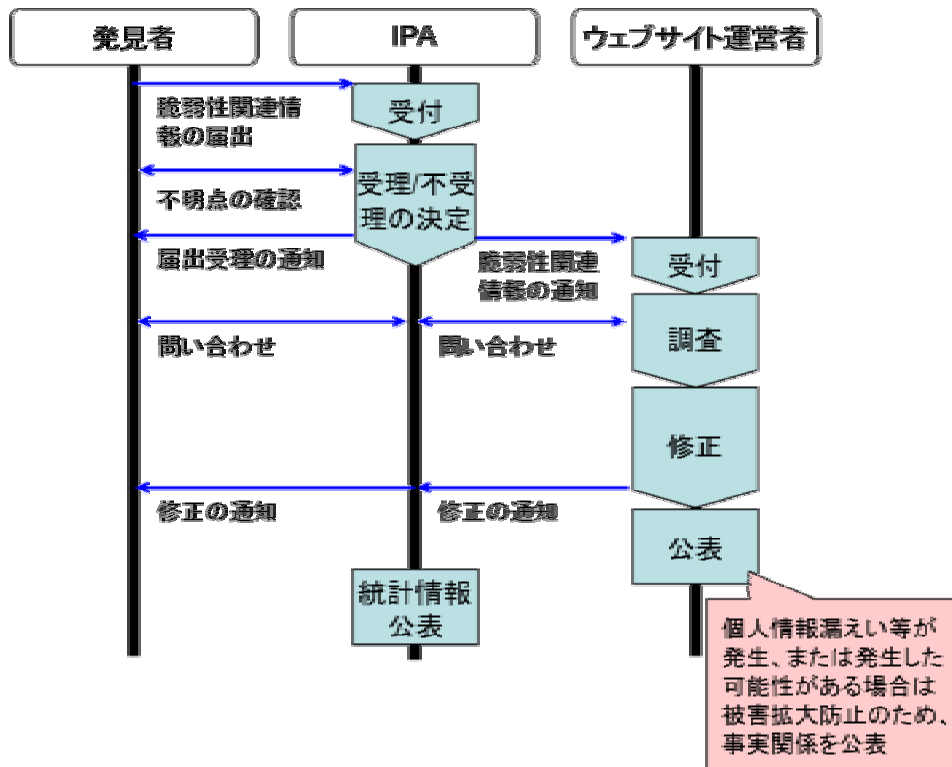
脆弱性情報公表日の受理

JPCERT/CC を通じ、製品開発者から脆弱性情報公表日の通知を受けます。

対応状況（脆弱性検証の結果および対策方法、取り組みの状況等）の公表

届け出られた脆弱性に対する製品開発者の対応状況を JPCERT/CC と共同運営するポータルサイト(JVN)にて公表します。また、公表に際しては、発見者にその旨通知します。

・ ウェブアプリケーションの脆弱性関連情報の場合



届出の受付

発見者からの届出を受け付けます。

届出情報の確認

記入項目に不備がないことを確認し、発見者への確認が必要な場合は連絡します。

届出受理の通知

の結果を踏まえ、届け出られた情報を受理するかどうかを判断します。受理する場合は、IPA から発見者へ届出を受理した旨をメールにて通知します。

ウェブサイト運営者への通知

ウェブサイト運営者の連絡先を調査し、脆弱性情報を通知します。連絡先が見つからない場合や、返信がない場合などは、取扱を終了することがあります。

修正に関する問合せ

ウェブサイト運営者に対し、修正に関する問い合わせを行います。ウェブサイト運営者が脆弱性の有無を確認する際、発見者への質問の仲介や確認作業に対する協力を行います。

修正通知の受理

ウェブサイト運営者から脆弱性の修正の通知を受理します。また、修正について、発見者に通知します。

統計情報の公表

届出情報を集計し、統計情報をウェブサイトにて公表します。

### 3. 届け出られた情報の取扱いについて

届け出られた情報については、情報の漏洩や紛失、誤用などのないよう、厳格に取扱います。

- ・ 発見者情報について  
製品開発者及びウェブサイト運営者と発見者との間で、脆弱性に関する詳細な情報のやり取りが発生することを考慮し、届出の際に発見者の連絡先情報の記入をお願いしています。発見者情報は、機密情報として取り扱い、脆弱性関連情報の取扱い終了後に削除します。
- ・ 脆弱性関連情報について  
脆弱性関連情報は、調整機関、開発者およびウェブサイト運営者との間で適切に取り扱い、脆弱性情報の公表前は、機密情報として取り扱います。脆弱性情報の公表後においても、脆弱性の詳細な情報や攻撃方法などの情報については、一般に広く公表する必要がない情報であるため、引き続き機密情報として取り扱います。

#### 情報の取扱いにおける基本方針

情報の種類	脆弱性情報公表前	脆弱性情報公表後
発見者情報	機密	機密 <sup>1</sup>
脆弱性情報	機密	公表
対応状況	機密	公表
攻撃方法	機密	機密

<sup>1</sup> ソフトウェア製品の脆弱性については、発見者の希望がある場合、対応状況とともに発見者名を公表します

### 4. その他

「脆弱性関連情報取り扱い説明会」の開催について

IPA と JPCERT/CC は、以下の日程で東京、福岡、大阪、名古屋、札幌にて、本基準の中心的な存在である、製品開発者の皆様にご参加いただく説明会を開催します。関係者各位の積極的なご参加をお願いいたします。

- 東 京: 2004年7月20日(火) 13:00-17:00, 都市センターホテル オリオン
- 福 岡: 2004年7月26日(月) 13:00-17:00, ホテルクリオコート博多
- 大 阪: 2004年7月27日(火) 13:00-17:00, 天満研修センター
- 名古屋: 2004年7月28日(水) 13:00-17:00, ホテルキャッスルプラザ
- 札 幌: 2004年7月30日(金) 13:00-17:00, アートホテルズ札幌

#### お問い合わせ先:

独立行政法人 情報処理推進機構 セキュリティセンター  
福澤、田原

TEL: 03-5978-7508 FAX: 03-5978-7518

E-mail: [isec-info@ipa.go.jp](mailto:isec-info@ipa.go.jp)

URL: <http://www.ipa.go.jp/security/>

## 「情報セキュリティ早期警戒パートナーシップ」の運用を開始

～ 調整機関として JPCERT/CC を指定 ～

2004年7月8日

有限責任中間法人 JPCERT コーディネーションセンター

<http://www.jpCERT.or.jp/>

有限責任中間法人 JPCERT コーディネーションセンター（東京都千代田区、代表・歌代和正、以下 JPCERT/CC）は、2004年7月8日に経済産業省より公示された「ソフトウェア等脆弱性関連情報取扱基準」において、日本国内の脆弱性関連情報流通のための調整機関として指定されました。

JPCERT/CC は従来より、海外調整機関（米国 CERT/CC、英国 NISCC など）との国際連携の枠組みにおいて、日本国内の脆弱性関連情報の流通、調整活動を行って参りました。今後も JPCERT/CC は日本国内の公的な枠組みの中で、引き続きその役目を担うこととなります。

また、上記基準をふまえ、独立行政法人情報処理推進機構（IPA）、JPCERT/CC、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）、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）、特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）では、脆弱性関連情報の流通に関わる関係者、関係業界としての指針「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」を連名で公表しました。

### 1. 調整機関としての役割

本枠組は、一般公表前の脆弱性関連情報を必要に応じて開示することで、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とどめることを目的としています。JPCERT/CC は、本枠組の調整機関として、一般公表前に脆弱性関連情報を製品開発者に連絡し、対応（パッチ、ワークアラウンドなどの作成）を依頼します。同時に、製品開発者に加えて海外の関係機関とも連携し、脆弱性関連情報を全世界で同時に公表するために、一般公表日を調整します。

### 2. 今後の予定

## 1) 製品開発者リストへの登録申請の受付開始

JPCERT/CC は、本枠組みに参加する製品開発者リストの策定を開始します。

登録手順は、以下の通りです。

- (1) 窓口 (POC: Point of Contact) 登録のための仮登録申請  
様式: <http://www.jpcert.or.jp/form/poc.txt>  
(注: すでにこの様式をご提出いただいている製品開発者の方には、  
JPCERT/CC からご連絡します。)
- (2) JPCERT/CC から、POC 本登録に必要な書類を提示する
- (3) 製品開発者に POC 本登録のための必要書類を作成し提出していただく
- (4) JPCERT/CC と製品開発者のミーティングを行う
- (5) 規約に同意いただき、登録する

上記 (3) の POC 登録申請においては、以下の情報が必要となります。

- ・会社の登記簿謄本
- ・会社概要(会社の紹介、パンフレットなど)
- ・サポート中の製品リスト
- ・窓口の連絡先
- ・窓口の責任者
- ・規約への同意書
- ・暗号化の公開鍵

## 2) JP Vendor Status Notes (JVN) の運用開始

7月8日より、製品開発者の対応状況を掲載するサイト (JVN) の本運用を開始します。詳細は以下の URL をご覧ください。

JVN  
<http://jvn.jp/>

JVN は、日本国内の製品開発者の脆弱性への対応状況を公表するサイトとして、JPCERT/CC と IPA が共同で運営します。JVN に掲載される脆弱性情報には、JPCERT/CC の製品開発者リストに登録している日本国内の製品開発者の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) が含まれます。

### 3) 「脆弱性関連情報取り扱い説明会」開催

JPCERT/CC と IPA は製品開発者の方を対象に、本枠組みに関する説明会を行います。日程等は以下の通りです。関係者各位の積極的なご参加をお願いいたします。

「脆弱性関連情報取り扱い説明会」

<http://www.jpccert.or.jp/workshop0407.txt>

東 京：2004年7月20日(火) 13:00-17:00，都市センターホテル オリオン

福 岡：2004年7月26日(月) 13:00-17:00，ホテルクリオコート博多

大 阪：2004年7月27日(火) 13:00-17:00，天満研修センター

名古屋：2004年7月28日(水) 13:00-17:00，ホテルキャッスルプラザ

札 幌：2004年7月30日(金) 13:00-17:00，アートホテルズ札幌

今日のインターネットは、日々新たなワームやウィルスが出現し、安定した運用が阻害される可能性が否定できません。このような状況において、ソフトウェア等における脆弱性関連情報を適切、かつ安全に流通させ、脆弱性に関する対策情報を広く一般に広めることで、より安全なインターネットの運用に繋がるものと JPCERT/CC では考えております。

本枠組みの円滑な運用のため、関係各位皆様のご協力をお願い致します。

以上

[参考資料]

JPCERT/CC

<http://www.jpccert.or.jp/>

独立行政法人 情報処理推進機構 (IPA)

脆弱性関連情報の取扱い

<http://www.ipa.go.jp/security/vuln/>

経済産業省

<http://www.meti.go.jp/>

本件に関する問い合わせ先:

有限責任中間法人 JPCERT コーディネーションセンター

担当: 伊藤、鎌田 (office@jpcert.or.jp)

電話番号: 03-3518-4600