



# 発見者の方へ

## (ソフトウェア製品やウェブアプリケーションの脆弱性を発見した方)

脆弱性を発見された際はIPAへの届出を検討してください\*2。届け出された脆弱性が、ソフトウェア製品の場合はJPCERT/CCから製品開発者へ、ウェブアプリケーションの場合はIPAからウェブサイト運営者へ連絡し、対策を促します。

### 【発見者の対応】

#### 脆弱性の発見

- 脆弱性関連情報を発見・取得する際には法令に触れることがないように注意が必要です。
- 脆弱性関連情報は、無関係な第三者に漏れないよう適切に管理することが望まれます。

#### IPAへの届出

- 届出様式(フォーマット)に従い、必要な情報を記入の上、IPAへお届けください。
- 届出の際、発見者の連絡先および発見者情報の取扱いについて記載してください。発見者が希望しない場合、発見者情報は第三者に開示されません。
- IPAから受理または不受理の連絡があります。

### 【他の関係者の対応】

- 製品開発者やウェブサイト運営者との情報交換をIPAやJPCERT/CCが仲介します\*3。
- 製品開発者やウェブサイト運営者において脆弱性の検証を進めます\*4。
- 検証が済み確認された脆弱性については、製品開発者やウェブサイト運営者が対策方法を検討します。
- ソフトウェア製品の脆弱性の場合、JVNで公表し利用者へ脆弱性対策情報を周知します。JVNで公表した際は、その旨をIPAから発見者へ通知します。
- ウェブアプリケーションの脆弱性の場合、ウェブサイト運営者から修正した旨の通知を受ければ、その旨をIPAから発見者へ通知します。
- IPAは、脆弱性関連情報を下表の期間、第三者に漏れないよう適切に管理することを発見者に依頼します(情報非開示依頼)。

双方が了解すれば、発見者が、製品開発者やウェブサイト運営者と直接情報交換することも可能です。

発見者は、取扱の進捗状況についてIPAにお問合せいただくことができます。その際、IPAから開示された情報をみだりに第三者に開示しないようにしてください。

ソフトウェア製品の脆弱性の場合、起算日\*5から1年以上経過した届出については、発見者はIPAに対し、情報非開示依頼の取り下げを求めることができます。

ソフトウェア製品の脆弱性	届出 ~ JVN*6公表の期間
ウェブアプリケーションの脆弱性	届出 ~ 修正の期間

\*2) 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制約されません。

\*3) 届出を受理した後に、IPAから発見者へ問い合わせることがあります。

\*4) 既知の脆弱性であった等の理由で取扱いを中止する場合には、IPAから発見者にその旨を連絡します。

\*5) 当該脆弱性関連情報についてJPCERT/CCが製品開発者への連絡を最初に試みた日。

\*6) IPAおよびJPCERT/CCが共同運営する脆弱性対策情報ポータルサイト (<https://jvn.jp/>)

# 製品開発者の方へ

## (ソフトウェア製品の脆弱性について連絡を受けた方)

製品開発者\*7は、自社のソフトウェア製品の脆弱性を通知された場合、その内容を検証すること、さらに当該脆弱性が存在した場合には、利用者へ対策方法を周知することが望まれます。また、JPCERT/CCから脆弱性関連情報に係わる技術的事項および進捗状況について問合せを受けた場合には、ご協力ください。

### 【製品開発者の対応】

#### 窓口の設置

- 脆弱性情報に関する情報交換を行なうための窓口を設置し、JPCERT/CCに連絡してください。
- 窓口の変更があれば速やかにJPCERT/CCにご連絡ください。

### 【IPA・JPCERT/CCの対応】

- JPCERT/CCが製品開発者リストに登録します。
- IPAが受付けたソフトウェア製品の脆弱性関連情報は、JPCERT/CCから該当する製品開発者へ連絡します。

#### 脆弱性の検証

- 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、脆弱性検証を行って、その結果をJPCERT/CCにご報告ください。
- 脆弱性関連情報は第三者に漏えいしないよう適切に管理してください。

#### 公表日程の調整

#### 対策の作成

- 検証の結果、脆弱性が存在することを確認した場合には、対策方法の作成や外部機関との調整に要する期間、当該脆弱性情報流出に係わるリスクを考慮しつつ、脆弱性情報の公表に関するスケジュール\*9)についてJPCERT/CCとご相談ください。
- 製品開発者は、脆弱性情報の公表日までに対応状況をJPCERT/CCに連絡するとともに、対策方法を作成するよう努めてください。

#### 一般への公表

- 製品開発者は、脆弱性情報の公表日以降、対策方法を製品利用者に周知してください。

製品開発者への連絡が不能な場合\*8、連絡をとるためにその製品開発者名等を公表することがあります。それでも連絡が取れない場合、公表判定委員会での審議を経て、当該脆弱性を公表することがあります。

IPA、JPCERT/CCを介し、発見者の了承を得て、発見者と直接情報交換をすることも可能です。

製品開発者がすべての製品利用者に脆弱性対策情報を通知する場合、公表をとりやめることがあるので、その旨をJPCERT/CCにご連絡ください。

製品利用者に生じるリスクを低減できると判断した場合、製品開発者は、JPCERT/CCと調整した上で、製品利用者に脆弱性検証の結果や対応状況を公表前に通知することができます。

\*7) ソフトウェアを開発した企業または個人。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等）を含みます。

\*8) 製品開発者の連絡先が不明か適切な連絡手段が存在しない、連絡先が分かっても全く応答がないか調整を行うのに必要な情報が得られない等、製品開発者と適切な連絡が取れないケースを指します。

\*9) 公表日は脆弱性の起算日から45日を目安としますが、さらに時間がかかる場合はJPCERT/CCとご相談ください。なお、起算日から1年間以上経過した届出について、発見者はIPAに情報非開示依頼の取り下げを求め、当該脆弱性情報を公表する可能性があります。

# ウェブサイト運営者の方へ

## (ウェブアプリケーションの脆弱性について連絡を受けた方)

ウェブサイト運営者は、自組織のウェブアプリケーションに脆弱性が存在する可能性について通知された場合、その内容を検証すること、さらに当該脆弱性が存在した場合には、影響の大きさを考慮した上で修正することが望めます。また、IPAから脆弱性関連情報に係わる技術的事項および進捗状況について問合せを受けた場合には、ご協力ください。

【ウェブサイト運営者の対応】

### 問合せ先の 開示

- ウェブページに関する問合せ先をウェブ上に明示してください。

【IPAの対応】

- IPAが受付けた脆弱性関連情報は、IPAから該当するウェブサイト運営者へ連絡します。

【ウェブサイト運営者の対応】

### 脆弱性の 検証

- ウェブサイト運営者は、IPAから脆弱性関連情報を受け取ったら、当該脆弱性の内容を検証し、その影響を把握してください。
- 当該脆弱性関連情報に関して検証した結果をIPAにご連絡ください。
- 脆弱性関連情報は第三者に漏えいしないよう適切に管理<sup>\*10</sup>してください。

IPAを介し、発見者の了承を得て、発見者と直接情報交換をすることも可能です。

### 脆弱性の 修正

- 脆弱性が存在することを確認した場合には、その影響を考慮して修正してください<sup>\*11</sup>。
- 当該脆弱性関連情報を修正した場合、その旨をIPAに連絡してください。この連絡は、IPAから脆弱性関連情報の通知を受けてから、3ヶ月以内を目処としてください。

\*10) ウェブサイトの構築を委託した事業者、およびウェブサイトの運用を委託している事業者には、秘密保持契約を締結した上で脆弱性関連情報を連絡することを推奨します。

\*11) 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、脆弱性の修正後に情報の公表を検討してください。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。

#### 本資料に関するお問い合わせ先

独立行政法人情報処理推進機構(略称:IPA) 技術本部 セキュリティセンター

〒113-6591 東京都文京区本駒込二丁目28番8号 文京グリーンコートセンターオフィス16階

<https://www.ipa.go.jp/security/> TEL: 03-5978-7527 FAX: 03-5978-7518

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

〒101-0054 東京都千代田区神田錦町3-17 廣瀬ビル11階

<https://www.jpccert.or.jp/> TEL: 03-3518-4600 FAX: 03-3518-4602