ソフトウエア製品開発者による
脆弱性対策情報の公表マニュアル

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
別冊

※目次

2024 年 3 月

独立行政法人 情報処理推進機構
一般社団法人 JPCERT コーディネーションセンター
一般社団法人 電子情報技術産業協会
一般社団法人 ソフトウェア協会
一般社団法人 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

1. 本資料の目的

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

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

開発者によっては、このような情報の公開が未経験であることなどが原因となって、不十分な情報公開や、不適切な方法での情報提供が行われる場合があり、利用者に必要な情報が届かない事態が生じているのが現状です。

また、サポートが終了し脆弱性対策が行えない場合において、脆弱性が発見された際には、利用停止等の案内が必要です。脆弱性対策情報は、サポート提供の有無にかかわらず、利用者に提供されることが望まれます。

本資料は、脆弱性対策情報を必要としている利用者に情報が的確に届けられることを目的として、開発者がウェブサイト上で脆弱性情報を公表する際の一つの方針を示すものです。

2. 脆弱性対策について利用者が必要としている情報

脆弱性対策情報を利用者に提供するにあたり、開発者はどのような情報が利用者に必要とされているかを知っておくべきです。開発者が十分な説明なしに修正プログラムの提供のみを行った場合、利用者に不利益が生ずることがあります。以下に、修正プログラムの適用方法の情報のほかに、一般的に利用者が必要としていると考えられる情報の種類と、その理由を示します。

(1) 製品の名称およびバージョン

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

(2) 脆弱性対策情報の公表時期

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

(3) 脆弱性がもたらす脅威

脆弱性情報が公表された際、それによりもたらされる危険が小さければ対策は行わず、重大な危険がある場合のみ対策するという判断をする利用者が存在します。したがって、利用者がその脆弱性の修正プログラムを適用しなかった場合にもたらされる具体的な脅威（利用者にどの様な影響があるか）を記載する必要があります。

また「どのような脆弱性が存在しているのか」、「脆弱性により利用者がどのような影響を受けるのか」といった内容を評価できる共通の指標により、定量的な情報を補足します。

(4) 回避策

利用者の環境によっては、修正プログラムを適用できない場合も考えられるため、攻撃を受けない、もしくは受けても被害が発生しないための回避策が存在するならば、その手段に関する情報が求められます。また、開発者が修正プログラムを提供できない場合についても、回避策が存在する場合には、開発者がその方法を適切に公表するべきです。

(5) 他に公表されている脆弱性に関する参考情報

開発者が公表する脆弱性対策情報以外にも、深刻さや緊急性を測るための参考情報があるならば、利用者はそれもあわせて確認するものです。したがって、それらの情報を参考情報として示すことが求められます。深刻さや緊急性を測るための情報としては、既にその脆弱性が悪用されている可能性があることを示す情報などが含まれます。

3. 脆弱性対策情報の公表項目と公表例

開発者がウェブサイト上で脆弱性対策情報を公表する際に示すべき情報の項目を、「3.1.脆弱性対策情報の公表項目」に示します。

各項目の具体的な記載例については、「3.2.脆弱性対策情報の公表例」と「3.3.サポート終了製品の脆弱性公表例」にそれぞれ、望ましい公表と望ましくない公表の例を示します。

3.1. 脆弱性対策情報の公表項目

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

3.1.1. タイトル

検索サイトなどから製品の名称で検索して情報に辿り着く利用者のために、ページタイトルに以下の情報を含めるようにします。

・製品名： 対象製品の識別のため

・脆弱性名： 同じ製品に複数の脆弱性が生じた際の識別のため

・「脆弱性」という用語： 脆弱性対策情報のページであることを明示するため

3.1.2. 概要

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

特に、緊急の対応が必要な場合や、攻撃の発生が確認されている場合には、その旨を記載することを推奨します。

（例）「本脆弱性については、今後被害が拡大する可能性があるため、至急、修正プログラムを適用して下さい。」

（例）「本脆弱性を利用した攻撃の発生が既に確認されています。至急、修正プログラムを適用して下さい。」

3.1.3. 対象バージョンと確認方法

脆弱性のある製品のバージョン情報を記載します。あわせて、利用者が使用している製品のバージョン情報の確認方法も記載します。

3.1.4. 脆弱性の説明

脆弱性の名称やその原因箇所などを記載します。さらに、利用者が同じ製品に存在する他の脆弱性と混同するなどの混乱が生じないよう、「共通脆弱性タイプ一覧」（CWE）[1]を用いて、脆弱性の種類を特定し、「脆弱性タイプ」と「CWE 識別子」を示すことによりどの脆弱性かを明確にします。CWE は、脆弱性の種類を伝えるために広く利用されており、脆弱性の名称を「脆弱性タイプ」によって、また脆弱性の原因を「CWE 識別子」の番号によって、それぞれ体系的把握することか可能になります。

また、製品の設定や利用環境などの要因が含まれる脆弱性の場合には、補足説明を行います。「望ましい公表の例」では、「※その他の設定および条件」のように記載しています。

3.1.5. 脆弱性がもたらす脅威

脆弱性を悪用された場合に利用者に生じ得る被害の内容、危険の度合い、攻撃の実現性等、脆弱性の深刻度を評価できるように、想定される影響やその範囲を特定できる情報を記載します。

---

[1] 「共通脆弱性タイプ一覧 CWE 概説」https://www.ipa.go.jp/security/vuln/scap/cwe.html

攻撃手法を公開すると攻撃を誘発する危険性があるため、「望ましい公表の例」のように、利用者の対応を促すために必要となる情報を記載します。

脆弱性の脅威に関する深刻度を定量的に評価する方法として、「共通脆弱性評価システム CVSS[2]」があります。CVSS は、FIRST (Forum of Incident Response and Security Teams)が提供する評価方法で、情報システムに求められる 3 つのセキュリティ特性である『機密性(Confidentiality Impact)』、『完全性(Integrity Impact)』、『可用性(Availability Impact)』に対する影響を、ネットワークから攻撃可能かどうかといった基準で算出し、「CVSS 基本値スコア」を 0(低)～10.0(高)の数値で表します。IPA が公開している「CVSS 計算ソフトウエアの多国語版[3]」を利用することで、比較的容易に値を取得することができます。詳細な説明および、CVSS 値の算出方法については、「共通脆弱性評価システム CVSS v3 について(付録 1)」を参照してください。

3.1.6. 対策方法

この項目では、根本的な対策として、修正済み製品のダウンロードページやインストール方法、アップグレード方法、修正プログラムの適用方法を記載します。

3.1.7. 回避策

修正プログラムの適用が困難な場合において、製品の利用方法を制限することや、運用を工夫すること等によって被害を回避できる際には、その方法を記載します。

例えば、回避策として設定値の変更により影響を緩和する方法が考えられる場合、「望ましい公表の例」では、攻撃元の範囲を限定する緩和策を記載しています。

3.1.8. 関連情報

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

例えば、多数の脆弱性情報サイトと連携して、個別製品中の脆弱性対策情報を相互に参照したり、関連付けて共有するために「CVE 番号(CVE-ID) [4]」を取得し、当該情報へのリンクとして記載する方法があります。CVE は、MITRE[5]社が、ソフトウエアの脆弱性を対象として、提供している脆弱性情報データベースです。CVE-ID は、脆弱性情報を収集し採番した番号で、付与することで、各ベンダが個別に公表した脆弱性情報の問題が同じであることを確認したり、比較することが可能になるため、脆弱性検査ツールや脆弱性対策情報提供サービスで広く利用されています。CVE 番号を取得するには、MITRE 社より認定された CVE 番号登録機関

---

[2] 「共通脆弱性評価システム CVSS v3 概説」https://www.ipa.go.jp/security/vuln/scap/cvssv3.html
[3] 「CVSS 計算ソフトウエア多国語版」https://jvndb.jvn.jp/cvss/
[4] 「共通脆弱性識別子 CVE 概説」 https://www.ipa.go.jp/security/vuln/scap/cve.html
[5] 「MITRE」https://www.cve.org/

（CNA）への申請が必要です。日本では、「JPCERT/CC[6]」が CVE 番号取得の申請を受け付けているため、詳細については「JPCERT/CC」にお問い合わせください。

3.1.9. 謝辞

開発者によっては、脆弱性発見者への謝辞を記載することがあります。

3.1.10. 更新履歴

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

3.1.11. 連絡先

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

3.2. 脆弱性対策情報の公表例

- **望ましい公表の例**

☆☆☆☆株式会社 ＞ セキュリティ脆弱性情報 ＞ ○○○○製品

緊急

○○○○製品における×××の脆弱性

公開日 20XX 年 12 月 4 日
最終更新日 20XX 年 12 月 9 日

■概要

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

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

該当製品をご利用の場合、今後被害が拡大するおそれがあるため、至急、修正プログラムをインストールしてください。

（※既に攻撃が確認されている場合）
【重要】本脆弱性を利用した攻撃の発生が既に確認されています。至急、修正プログラムを適用して下さい。

■該当製品の確認方法

影響を受ける製品は以下の製品です。

[6] 「JPCERT/CC」https://www.cve.org/PartnerInformation/ListofPartners/partner/jpcert
（vuls@jpcert.or.jp）

製品名称　〇〇〇〇
該当バージョン
1.5.4 (Windows 版) 以前の全てのバージョン
1.5.4 (Linux 版) 以前の全てのバージョン

使用しているバージョン番号の確認方法は以下の通りです。
1, 〇〇〇〇を起動し、「ヘルプ」メニューから「バージョン情報」を選択する。
2. 現れたウィンドウの下記の部分が起動している〇〇〇〇のバージョン番号です。

バージョン表示ウィンドウの図 （省略）

■脆弱性の説明

〇〇〇〇製品は、ファイルの■■■■のために▽▽▽▽の機能を搭載しています。◎◎◎◎データの一部として提供され▲▲▲▲で配布された▽▽▽▽の機能に、×××××の脆弱性が存在するため、外部の第三者からインターネット越しに□□□□を実行される脆弱性が存在します。

※その他の設定および条件

▽▽▽▽の機能が搭載されていないバージョン 1.5.4 以前 (Windows 版) を利用している場合、または、この機能が無効化されている場合には、外部の第三者からインターネット越しに□□□□を実行されることはありません。

・CWE-20　不適切な入力確認

■脆弱性がもたらす脅威

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

・CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/BS9.8　緊急
・〇〇製品における技術詳細情報

■対策方法

バージョン 1.5.4.より前の製品を利用されているお客様は、一度製品をアンインストールしてから対策版製品をインストールしてください。バージョン 1.1 以降の製品を利用されているお客様は、修正プログラムをインストールしてください。

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

対象製品名称　〇〇〇〇
修正プログラムのダウンロード
1.5.5 patch.zip (Windows 版) 20XX.12.4
1.5.5 patch.tgz (Linux 版) 20XX.12.4

・ 修正プログラムによって置き換えられる設定ファイル
xxxxx.cfg、yyyyy.dif

■回避策

この脆弱性は、次の手順で影響を緩和できる場合があります。

〇〇〇〇で使用する管理用ポート番号宛ての通信を、信頼できる IP アドレスのみに限定するよう、ルータ等にてフィルタリング設定を行うことで、攻撃元の範囲を限定することができます。

■関連情報

CVE-20XX-12345678
JVN#12345678 ○○○○製品における×××××の脆弱性

■謝辞

□□□の□□□氏よりこの問題をご報告いただき（略）

■更新履歴

20XX.12.4　この脆弱性情報ページを公開しました。
20XX.12.9　脆弱性がもたらす脅威に、システム管理者の権限でコンピュータを任意に操作する際の技術詳細情報を追加しました。

■連絡先

本件に関するお問い合わせはこちら
脆弱性連絡窓口
電話　：03-xxxxx-xxxx（平日 10:00 - 17:00）
メール：example@example.co.jp

- **望ましくない公表の例(1)**

> ○○○○製品の更新について
>
> 平素は格別のご愛顧を賜り厚くお礼申し上げます。
>
> さて、この度弊社で開発しました○○○○に開発工程にて、ごく稀に△△△△機能にて動作が不安定になることがございます。
>
> この現象は限定された利用環境において発生するものです。しかし、万が一のため、ここに○○○○製品のアップデートプログラムの公表を連絡させていただくものです。
>
> 今後とも、お客様の身になって、品質の向上に努めてまいる所存ですので、本製品をご愛顧いただけますよう、お願いいたします。
>
> ■アップデートプログラム
>
> ○○○○1.5.5 (Windows 版)　　○○○1.5.5 (Linux 版)

望ましくない理由

- タイトルに、脆弱性対策を目的とした告知であることが記載されていないため、利用者に伝わりません。
- 日頃から送付している宣伝メッセージと誤解されかねない形式で書かれているため、利用者は脆弱性対策情報であることに気づけません。
- どのような危険が差し迫っているか、脆弱性がもたらす脅威が不明確なため、利用者は脆弱性対策を早急に行うべきか判断できません。
- アップデート方法について具体的な記述が無いため、対策方法が分かりません。
- 公表された時期が不明なため、利用者が既に対策済みの脆弱性情報かどうか判断ができません。
- 連絡先が記載されていないため、利用者は、疑問が生じた場合に、確認することができません。

- **望ましくない公表の例(2)**

> ○○○○リリースノート
>
> 20XX.12.4　バージョン 1.5.5
>
> ・メール送信機能に任意のヘッダの編集機能を追加
>
> ・ファイルアップロード機能で長いファイル名を指定したときにバッファオーバーフローが生じる不具合を修正
>
> ・そのほかの細かなバグの修正
>
> 20XX.11.28　バージョン 1.5.4
>
> ・ファイルアップロード機能を追加
>
> ・・・・・・・

望ましくない理由

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

3.3. サポート終了製品の脆弱性公表例

サポート終了製品の脆弱性情報を公表する際には、サポートが終了しているため本製品の使用を中止してもらうか、サポート中の上位バージョン製品などがある場合は、サポート中の製品にアップグレードしてもらうように記載します。

脆弱性情報を公表するタイミングで初めてサポート終了情報を公開することは、利用者が困惑することになるため、製品を販売する時点など早い段階で、サポート終了時期を含む製品のライフサイクルを明示しておくことが望まれます。

望ましい公表の例

☆☆☆☆株式会社 > セキュリティ脆弱性情報 > ○○○○製品

○○○○製品 における××××の脆弱性

公開日 20XX 年 7 月 11 日

■概要

○○○○ Linux 版は、Java のウェブアプリケーションを作成するためのソフトウェアフレームワークです。○○○○ には、xxxMode が有効になっている場合、××××の脆弱性が存在します。

○○○○ 2.3.20 以前の製品はサポートが終了しています。ご利用のユーザは、バージョン 3.0.1 以降の製品にアップグレードを行ってください。

■影響を受けるシステム

○○○○ 2.3.20 以前のバージョン

該当のバージョンは、20XX 年 4 月 5 日付けでサポート終了（EOL）しているため、修正モジュールの提供予定はありません。

■対象バージョンの認方法

1. 製品管理画面より、メイン画面右上の［設定アイコン］より[バージョン情報]をクリックします。

2. 「バージョン情報」画面で脆弱性のないバージョンかどうかを確認できます。
   - ・製品 ○○○○
   - ・バージョン 3.0.1
   - ・プラットフォーム Linux 版
   - ・シリアル番号

■脆弱性の説明

××××(CWE-nn)

■脆弱性がもたらす脅威

・ユーザのウェブブラウザ上で任意のスクリプトを実行される可能性があります。

・スクリプトが実行されると、ログイン状態を乗っ取られたり、偽の入力欄を表示されて利用者が入力した情報を窃取されるなどの被害に遭う可能性があります。

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/BS:6.1

■対策方法

最新版へアップグレードしてください。

※または、利用を中止してください。

■関連情報

対象製品の以下のサポートページより詳細をご確認ください。

・アドバイザリ

・ホワイトペーパー

・マニュアル

・サポート終了製品の情報提供

■謝辞

□□□の□□□氏よりこの問題をご報告いただき（略）

■更新履歴

20XX.7.11　この脆弱性情報ページを公開しました。

■連絡先

本件に関する連絡窓口

電話　：03-xxxxx-xxxx（平日 10:00 － 17:00）

メール：example@example.co.jp

望ましくない公表の例

> **〇〇〇2.3.20 (Linux 版) 以前の製品を利用されているお客様へ**
>
> この度、「利用者の関連コミュニティ」に、弊社一部製品において、脆弱性があるとの報告がございました。弊社環境において、事象の再現を確認しており、製品が参照しているライブラリに脆弱性がある場合に、問題の現象が発生いたします。
>
> 脆弱性のあるライブラリを利用している場合に影響があることから、〇〇〇2.3.20 (Linux 版) 以前の製品をご利用の場合には、サポートしているバージョン〇〇〇3.0.1 (Linux 版)以降へのアップグレードをご検討ください。

望ましくない理由

- 対象のバージョンがサポート終了製品であることが明確でないため対策の必要性の判断ができません。
- 脆弱性がもたらす被害の内容が記載されていないため、利用者が脆弱性の種類や影響を判断できません。
- 製品のアップデートモジュールへのリンクや手順書などの記載などの情報が不充分なため、利用者が必要な対策がすぐに実施できません。
- 連絡先が記載されていないため、利用者に疑問が生じた場合に、すぐに連絡がすることができません。

4. 脆弱性対策情報への誘導方法

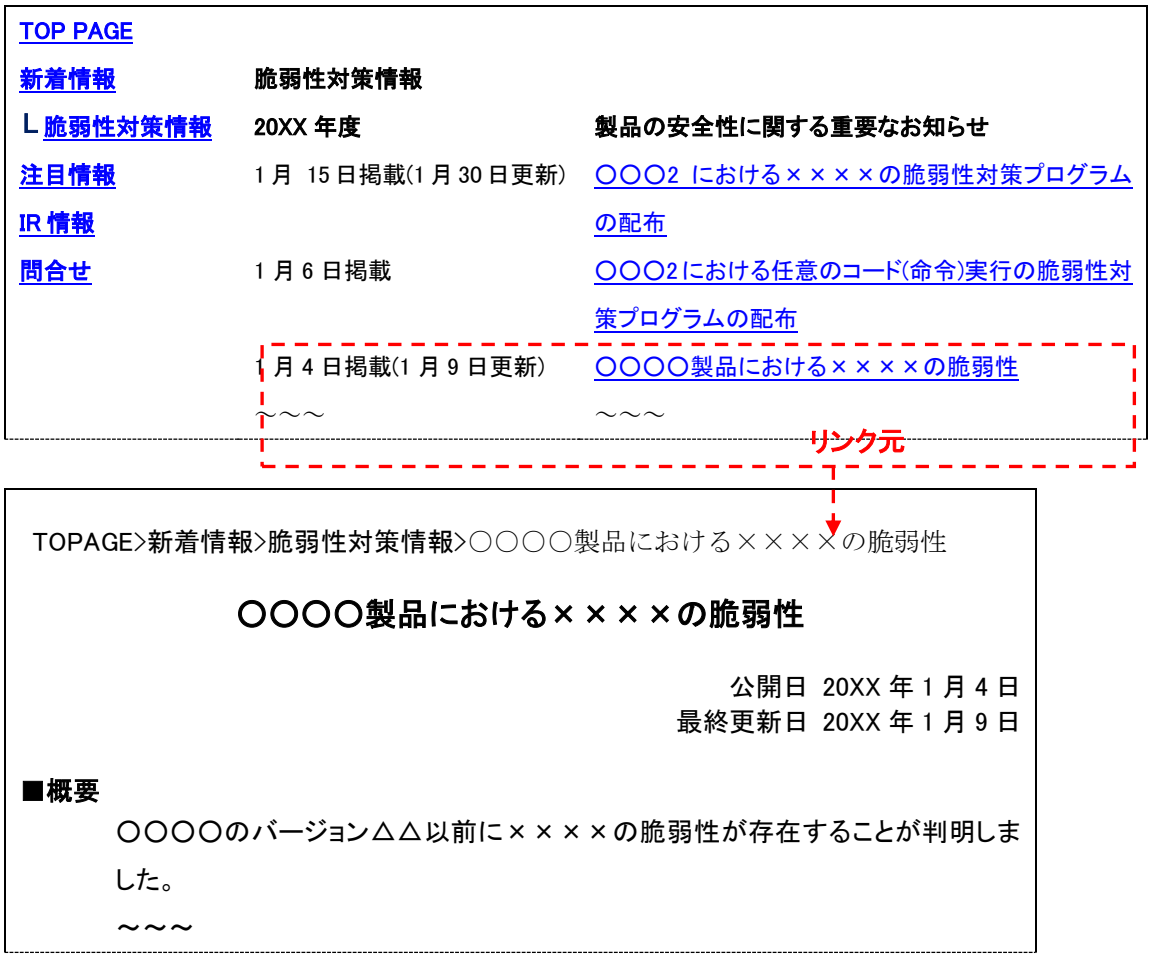
開発者がウェブサイトのトップページから脆弱性対策情報へ利用者を誘導する方法として望ましい例と、望ましくない例を示します。

- **望ましい誘導方法の例**

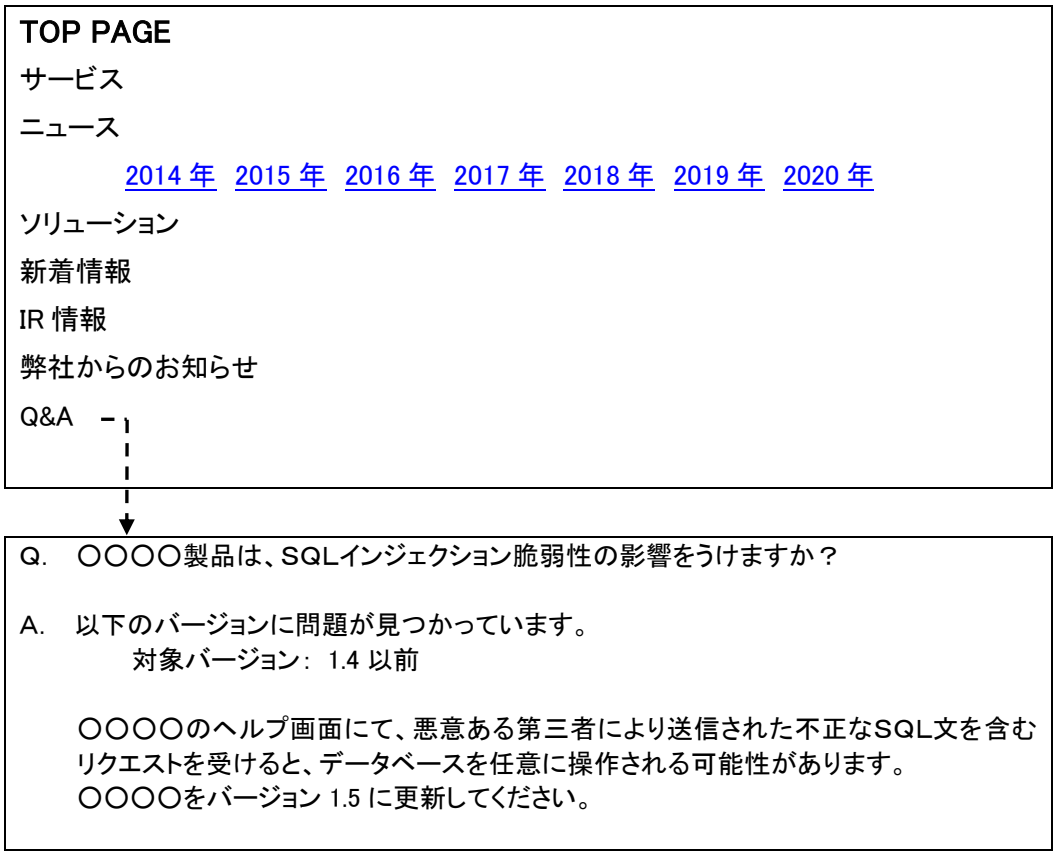
ウェブサイトの階層が深い場合や表示される情報が複雑な場合は、利用者は脆弱性対策情報にたどり着きにくくなります。したがって、以下のような工夫を行います。

・ 誘導するリンクの名称は、対策情報のタイトルと同じになるように記載します。

・ リンクで脆弱性対策情報に誘導する際は、リンク元にも更新日時を記載します。



- **望ましくない誘導方法の例**



望ましくない理由

- 一般的な Q&A に脆弱性対策情報が混在して記載されているため、利用者が脆弱性対策情報を発見できません。
- 脆弱性情報の項目がないため、利用者が脆弱性対策情報にたどり着けません。
- 更新日時が記載されていないため、利用者が既に確認し対応を行った脆弱性対策情報か分かりません。

5. 参照情報

脆弱性情報の公表にあたり取り扱いの体制や脆弱性公開ポリシー作りなどの準備が必要になる場合には、それぞれ、以下の情報をご参照ください。

- 脆弱性情報公表のための体制について
  「製品開発ベンダにおける脆弱性関連情報取扱に関する体制と手順整備のためのガイドライン」 P30
  http://it.jeita.or.jp/infosys/info/0407JEITA-guideline/guideline-v10.pdf

- 脆弱性公開ポリシー策定にあたって
  「ISO/IEC 29147」並びに各ベンダの動向をご確認ください。以下の情報が参考となります。
  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
  https://www.ipa.go.jp/security/guide/vuln/partnership_guide.html
  ・付録6 国際標準に準拠するための留意点
  ・付録7 本ガイドラインの別冊・関連資料一覧

「脆弱性対策情報の公表例」「脆弱性対策情報への誘導方法」の各例示作成については、以下の文献を参考に作成しました。

消費生活用製品のリコールハンドブック2016
https://www.meti.go.jp/product_safety/recall/handbook2016.pdf
「社告の基本掲載事項」P68

・本資料の位置付け

近年、日本国内においてソフトウエアやウェブアプリケーションの脆弱性が発見されることが増えており、これらの脆弱性を悪用した不正アクセス行為やコンピュータウイルスの増加により、企業活動が停止したり情報資産が滅失したり個人情報が漏洩したりといった、重大な被害が生じています。

そこで、脆弱性関連情報が発見された場合に、それらをどのように取り扱うべきかを示した経済産業省告示が制定されました。この告示をふまえ、関係者に推奨する行為をとりまとめた「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」が公表されています。

（参考）

「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」（平成 29 年経済産業省告示第 19 号）」

「受付機関及び調整機関を定める告示（平成 31 年経済産業省告示第 19 号）」

本資料は、このガイドラインの別冊資料であり、主にソフトウエア開発者による活用を想定しており、ソフトウエア開発者による脆弱性対策情報の望ましい公表手順について一つの方針を示しています。

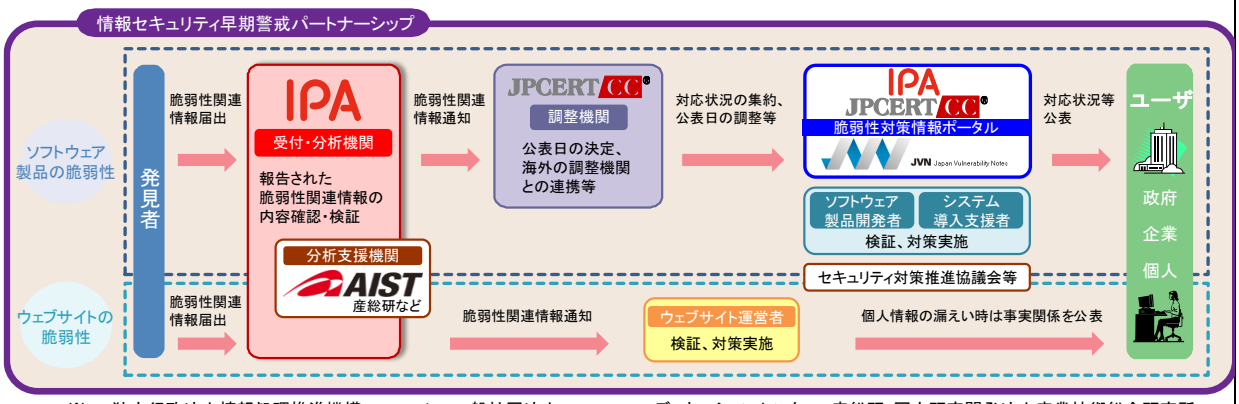
関係者の方々は、脆弱性関連情報の公表に際し、利用者が必要とする情報を的確に示すため、本資料を参考にご対応くださいますようお願い申し上げます。

本資料の配布に制限はありません。本資料は、次の URL からダウンロードできます。

https://www.ipa.go.jp/security/guide/vuln/partnership_guide.html

https://www.jpcert.or.jp/vh/index.html#link_japan

・「情報セキュリティ早期警戒パートナーシップ」



※IPA:独立行政法人情報処理推進機構, JPCERT/CC:一般社団法人　JPCERTコーディネーションセンター、産総研：国立研究開発法人産業技術総合研究所

・本資料に関するお問合わせ先

独立行政法人情報処理推進機構（略称：IPA）　セキュリティセンター

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

https://www.ipa.go.jp/security/　TEL: 03-5978-7527　FAX: 03-5978-7552

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

〒103-0023 東京都中央区日本橋本町 4-4-2 東山ビルディング 8 階

http://www.jpcert.or.jp/　　TEL：03 - 6271- 8901　FAX：03 - 6271- 8908

ソフトウエア製品開発者による脆弱性対策情報の公表マニュアル

― 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 別冊 ―

２００７年　５月３０日　第１版発行　　２０２０年　３月１８日　第５版発行

２００９年　７月　８日　第２版第３刷発行　　２０２４年　３月２７日　第６版発行

２０１５年　３月２６日　第３版発行

２０１７年　３月３０日　第４版発

［著作・制作］　情報システム等の脆弱性情報の取扱いに関する研究会

［事務局・発行］　独立行政法人情報処理推進機構