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
付録 5 抜粋編

※目次

2008 年 4 月

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 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

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

過去にリリースした製品に脆弱性が存在することを知りながら、脆弱性対策情報を公表せず、被害が生ず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。製品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。

しかしながら、製品開発者によっては、このような情報公開を経験した前例がないことなどが原因となって、不十分な情報公開や、不適切な方法での情報提供が行われる場合があり、利用者に必要な情報が届かない事態が生じているのが現状です。

本資料は、必要としている利用者に必要な情報が的確に届けられることを目標として、製品開発者が行うべき脆弱性対策情報の望ましい公表の手順について、一つの方針を示すものです。

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、製品開発者は、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。製品開発者が、十分な説明なしに修正プログラムの提供のみを行った場合、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) 脅威

脆弱性情報が公表された際、それによりもたらされる危険が小さければ対策しないで済ませ、重大な危険がある場合のみ対策するという判断をする利用者が存在します。したがって、その脆弱性の修正プログラムを適用しなかった場合にもたらされ得る具体的な脅威がどのようなものかについて、公表することが求められます。

(4) 回避策

修正プログラムを適用できない場合に、攻撃を受けない、もしくは受けても被害が発生しないための回避策が存在するならば、その手段に関する情報が求められます。製品開発者が修正プログラムだけ提供して脆弱性の詳細を公表しなかった場合、回避策が不明となり、修正プログラムを適用できない利用者が不利益を被ることがあります。回避策が存在する場合には、製品開発者がその方法を適切に公表するべきです。

(5) 他に公表されている脆弱性関連情報

製品開発者が公表する脆弱性対策情報以外にも、深刻さや緊急性を測るための参考情報があるならば、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。

3. 脆弱性対策情報の公表項目と公表例

製品開発者がウェブサイト上で脆弱性対策情報を公表する際に示すべき情報の項目を列挙し、望ましい公表と、望ましくない公表の例を示します。

3.1. 脆弱性対策情報の公表項目

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

以下、一般的に考えられている脆弱性対策情報の望ましい公開の手順を、情報の項目ごとに区切って示します。

3.1.1. タイトル

製品の名称で検索して情報に辿り着く利用者のために、ページタイトルに製品名を記載します。また、過去および将来において同じ製品に複数の脆弱性が生ずる場合があることから、それらを区別可能なように、タイトルに脆弱性名称を記し、脆弱性情報のシリアル番号等を含めます。また、検索サイトなど外部サイトから直接に当該ページへ誘導される場合に備えて、そのページが脆弱性対策情報についての記述であることを明示します。

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、内容を簡潔にまとめた概要を冒頭に示します。

3.1.3. 該当製品の確認方法

脆弱性のある製品のバージョン情報と、利用者が使用している製品のバージョン情報を確認する方法を説明します。

3.1.4. 脆弱性の説明

利用者が同じ製品に存在した他の脆弱性と混同するなどの混乱が生じないよう、脆弱性の名称やその原因箇所などを記載して、その脆弱性の存在を説明します。

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生じ得る被害の内容、危険の度合い、攻撃が成功する可能性の大きさ等、脆弱性の深刻度を評価するために必要な情報を記載します。

3.1.6. 対策方法

対策を施した製品のインストール方法やバージョンアップ方法、修正プログラムの適用方法を記載します。

3.1.7. 回避策

修正プログラムを適用しないままで、製品の利用方法を制限することや、運用を工夫すること等によって被害を防止できる場合には、その方法を回避策として記載します。

3.1.8. 関連情報

製品開発者による情報以外に、その脆弱性について公表されている情報がある場合には、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。

3.1.9. 謝辞

製品開発者によっては、脆弱性発見者への謝辞を記載することがあります。

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、更新日を示すとともに、更新内容の説明を記載します。

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、問い合わせ先を明記します。

3.1.12. 脆弱性対策情報の公表例

脆弱性対策情報の望ましい公表の例は、使用者等の情報提供の対象者を特定できない場合に、製品開発者が使用者に告知する例とし、参考文献「消費者生活製品のリコールハンドブック」を参考に作成しています。

- **望ましい公表の例**

☆☆☆☆株式会社 > セキュリティ脆弱性情報 > ○○○○製品

IPASA2007-001: ○○○○製品における××××の脆弱性

公開日 2007 年 1 月 4 日
最終更新日 2007 年 1 月 9 日

■概要

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

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

■該当製品の確認方法

影響を受ける製品は以下の製品です。

製品名称 ○○○○
該当バージョン
1.5.4 (Windows XP SP2 版) 以前の全てのバージョン
1.5.4 (Linux 版) 以前の全てのバージョン

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

バージョン表示ウィンドウの図 (省略)

■脆弱性の説明

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。

■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。

・IPASA2007-001 技術詳細情報

■対策方法

〇〇〇〇バージョン 1.0.0 より前の製品を利用されているお客様は、一度製品をアンインストールしてから対策版製品をインストールしてください。〇〇〇〇1.0.0 以降の製品を利用されているお客様は、修正プログラムをインストールしてください。

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

対象製品名称 〇〇〇〇

修正プログラムのダウンロード

1.5.5 patch.zip (WindowsXP SP2 版) 2007.1.4

1.5.5 patch.tgz (Linux 版) 2007.1.4

・ 修正プログラムによって置き換えられる設定ファイル

xxxxx.cfg、yyyyy.dif

■回避策

この脆弱性は、次に示す手順で影響を緩和できる場合があります。

・ 回避策

〇〇〇で使用する管理用ポート番号宛ての通信を信頼できる IP アドレスのみに限定するよう、IP フィルタリング機能またはルータ等にてフィルタリング設定を行うことで、影響を緩和することができます。

■関連情報

JVN#12345678 〇〇〇〇製品における××××の脆弱性

■謝辞

□□□の□□□氏よりこの問題をご報告いただき(略)

■更新履歴

2007.01.4 この脆弱性情報ページを公開しました。

2007.01.9 脆弱性がもたらす脅威に、権限の低い設定のアカウントで利用している場合についての技術詳細情報を追加しました。

■連絡先

脆弱性連絡窓口

電話 :03-xxxxx-xxxx (平日 10:00 - 17:00)

メール:example@example.co.jp

- **望ましくない公表の例(1)**

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

望ましくない理由

- 脆弱性対策を目的とした告知であることが不明確で、利用者に分かりません。
- 日頃から送付している宣伝メッセージと間違われかねない形式で書かれているため、脆弱性対策情報であることに気づけません。
- どのような危険が差し迫っているか、詳細が不明確なため、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の判断ができません。

- **望ましくない公表の例(2)**

> **○○○○リリースノート**
>
> 2007.1.4　　バージョン 1.5.5
>
> ・メール送信機能に任意のヘッダの編集機能を追加
>
> ・ファイルアップロード機能で長いファイル名を指定したときにバッファオーバーフローが生ずる不具合を修正
>
> ・そのほかの細かなバグの修正
>
> 2006.11.28　バージョン 1.5.4
>
> ・ファイルアップロード機能を追加
>
> ・・・・・・・

望ましくない理由

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

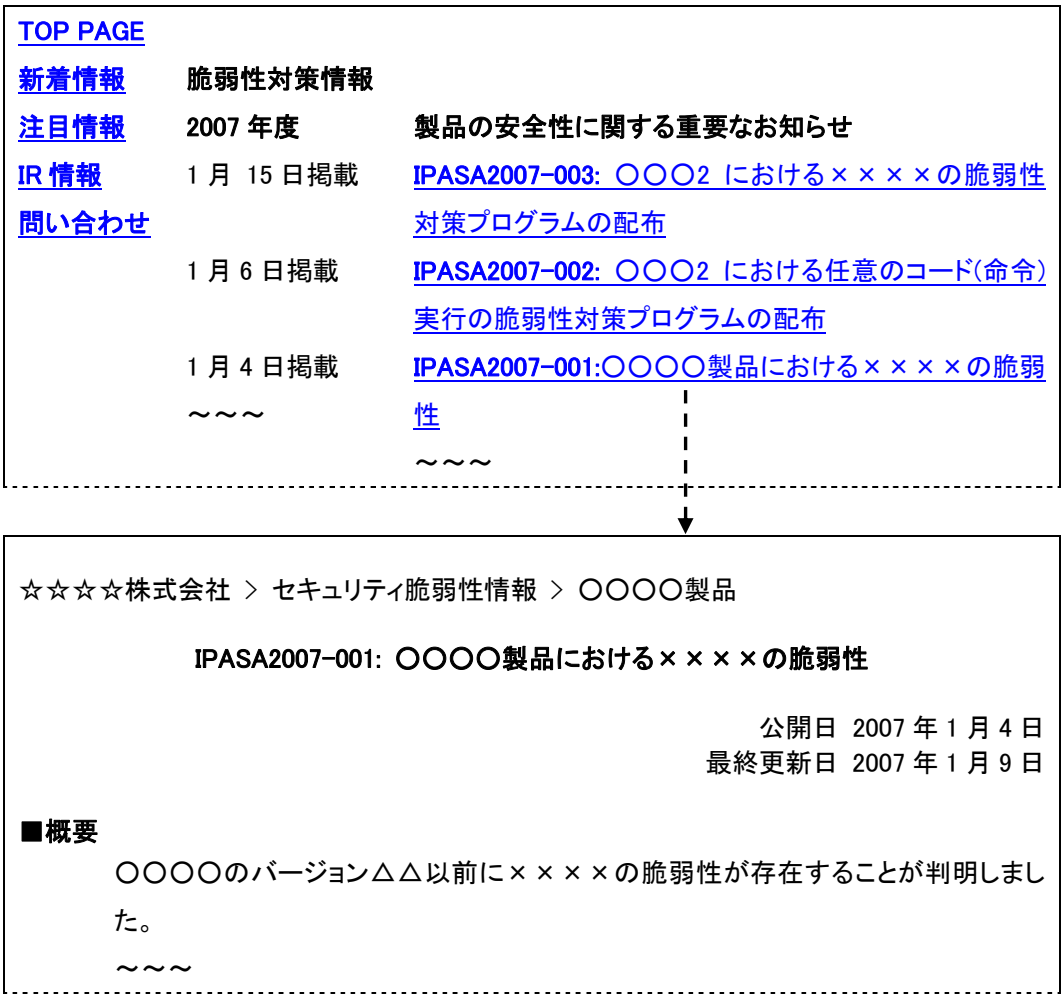
4. 脆弱性対策情報への誘導方法

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

脆弱性対策情報への誘導する際に望ましい構成

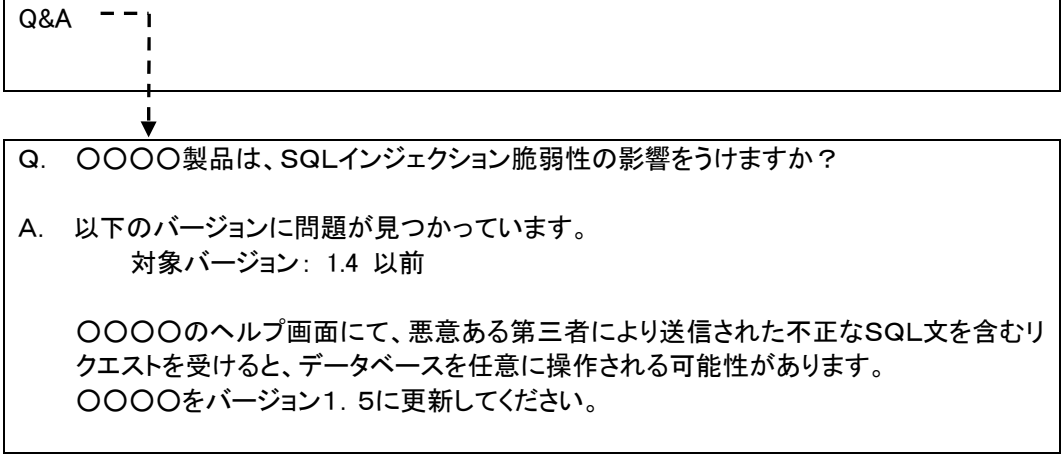
- ウェブサイトの階層が深くなったり、表示される情報が複雑化したりすると、利用者は脆弱性対策情報にたどり着きにくくなります。したがって、ウェブサイトのトップページから脆弱性対策情報にリンクで誘導する際は、階層が深くならないような工夫が必要です。
- 誘導する際のリンクの名称は、タイトルと同様にします。
- リンクで脆弱性対策情報に誘導する際は、3.1.10 と同様に更新日時を記載します。

- **望ましい誘導方法の例**



- **望ましくない誘導方法の例**

TOP PAGE
サービス
ニュース
2002 年 2003 年 2004 年 2005 年 2006 年 2007 年
ソリューション
新着情報
IR 情報
弊社からのお知らせ
Q&A



望ましくない理由

- Q&A などの他の情報に脆弱性情報が混在しています。
- FAQ に脆弱性対策情報が掲載されているため、この情報が脆弱性対策情報であることが分かりません。
- 脆弱性対策情報を探している利用者がここにその情報があることを予想できません。
- いつ掲載された脆弱性対策情報か利用者が分かりません。

5. 参考文献

消費生活用製品のリコールハンドブック，製品安全研究会，2002.5
P.47 参考2 社告の例 望ましい社告の例
http://www.meti.go.jp/policy/consumer/seian/contents/recall/handbook.pdf

・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「ソフトウエア等脆弱性関連情報取扱基準」が制定され、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。

本資料は、このガイドライン（2008 年 4 月 4 日改訂版）の付録 5 を全文抜粋したものです。主にソフトウエア製品開発者による活用を想定しており、ソフトウエア製品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。

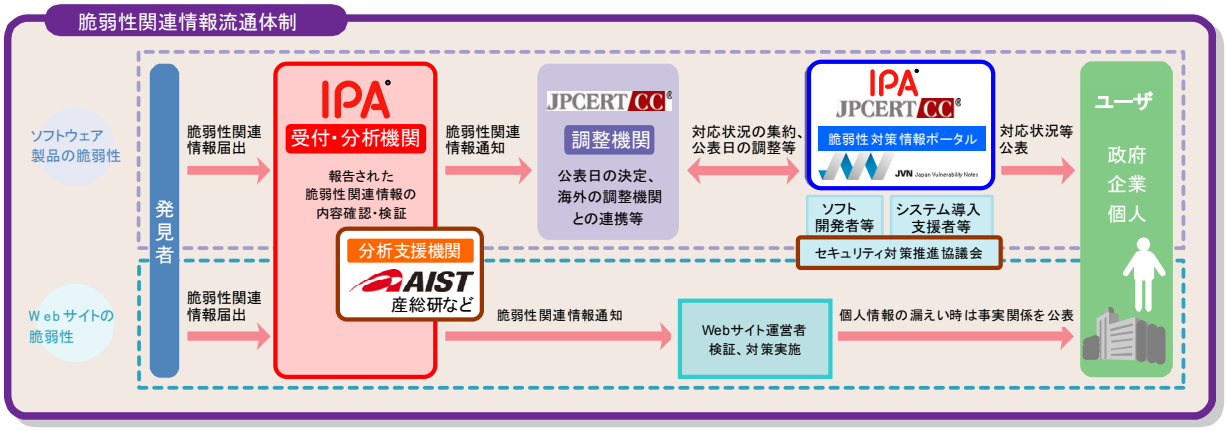
関係者の方々は、脆弱性関連情報の公表に際し、利用者が必要とする情報を的確に示すため、本資料を参考にご対応くださいますようお願い申し上げます。

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。

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

http://www.jpcert.or.jp/vh/#guideline

・脆弱性関連情報流通の基本枠組み「情報セキュリティ早期警戒パートナーシップ」



※JPCERT/CC：有限責任中間法人 JPCERT コーディネーションセンター、産総研：独立行政法人　産業技術総合研究所

・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

http://www.ipa.go.jp/security/　TEL: 03-5978-7527　FAX: 03-5978-7518

有限責任中間法人　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

http://www.jpcert.or.jp/　TEL : 03-3518-4600　FAX : 03-3518-4602

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　付録 5 抜粋編 －

［発　　行］　２００７年　５月３０日　第１版

２００８年　４月　４日　第３版

［編　著　者］　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］　独立行政法人　情報処理推進機構