

製品開発者と連絡が不能な「連絡不能案件」の“脆弱性情報”<sup>(\*1)</sup> 公表に向けた運用を開始  
～「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」を改訂～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）および JPCERT/CC（一般社団法人 JPCERT コーディネーションセンター、代表理事：歌代 和正）は、脆弱性情報取扱における関係者の行動基準を示した「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」<sup>(\*2)</sup>（以後、ガイドライン）を改訂しました。これにより、発見された脆弱性の製品開発者と連絡がとれない案件を「連絡不能案件」として脆弱性情報を公表する運用を開始しました。

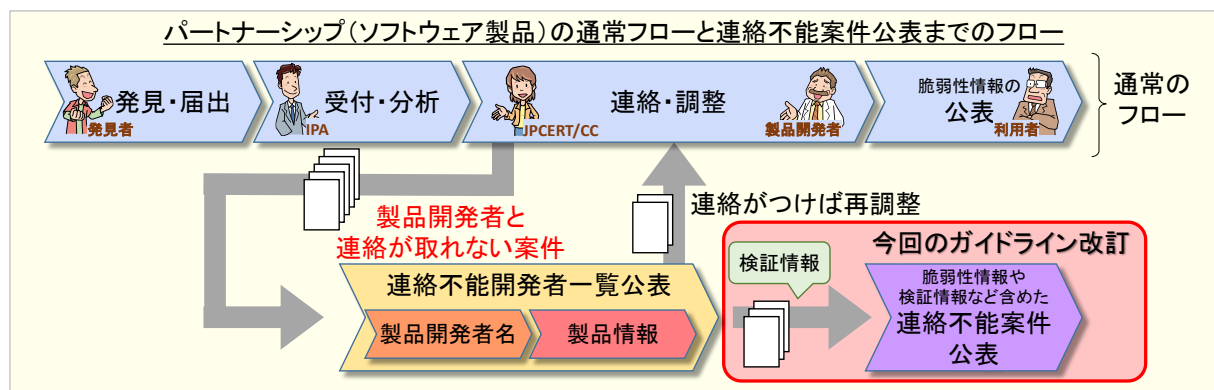
[http://www.ipa.go.jp/security/ciadr/partnership\\_guide.html](http://www.ipa.go.jp/security/ciadr/partnership_guide.html)

<https://www.jpccert.or.jp/press/2014.html>

ソフトウェアやウェブサイトの脆弱性を悪意ある者に利用された場合、標的型攻撃における組織への侵入の突破口に悪用されたり、インターネットバンキングの偽ログイン画面を表示させることで不正送金につながったりと、企業や個人の利便を損なうだけでなく、実害が生じる可能性があります。

そのため、脆弱性が発見された場合、悪用をされることのないよう、対策方法策定、およびその情報の公表までは、厳重に情報を秘匿するなど、適切な情報管理が必要です。

「ガイドライン」に基づく脆弱性取扱業務（ソフトウェア製品の届出）では、受付機関である IPA が発見者から未知の脆弱性の届出を受付けています。届出られた脆弱性は IPA で分析し、調整機関である JPCERT/CC へ連絡します。そして JPCERT/CC は脆弱性対策情報を利用者に提供するため、製品開発者への交渉を開始します。しかし、製品の開発者と連絡が取れない場合、このような交渉を始めることができません。



(\*1) 脆弱性情報には、脆弱性の内容、想定される影響、分析結果などの他、製品開発者の脆弱性検証の結果、その対応状況が含まれる。「連絡不能案件」ではこの脆弱性情報に加え、IPA、JPCERT/CC の検証情報が付加される。

(\*2) 2004年7月7日に経済産業省が「情報システム等脆弱性情報取扱基準」を告示し、これに基づく公的な制度として「情報セキュリティ早期警戒パートナーシップ」が確立。発見された脆弱性の扱いや対策情報の策定、これらの公表に至るまでの関係者の行動基準を「ガイドライン」として示している。脆弱性取扱業務は IPA、JPCERT/CC が中心に実施。

そこで、製品開発者と連絡がとれない脆弱性の届出を「連絡不能開発者一覧」として“製品開発者名”、“製品情報”を段階的にウェブサイトで公表し、広く第三者からの情報提供を求めるという運用を2011年9月から実施してきました。これまで取り扱ったソフトウェアの脆弱性1,788件のうち、製品開発者に連絡がとれなかったものは170件、「連絡不能開発者一覧」として2011年9月以降に公表したのは152件、情報公表により製品開発者と連絡がとれたのは21件でした。  
(2014年3月末時点)

この「連絡不能開発者一覧」の公表により開発者と連絡が取れたケースがある一方で、全く連絡がとれないものがまだ131件存在しています。これらは脆弱性の対策が一向に進まぬまま放置されていることを意味しており、その結果、製品利用者は脆弱性がある製品を使い続け、脆弱性による被害を受ける可能性を排除できないままとなっています。

このような状況を改善するには、「連絡不能案件」の“脆弱性情報”の公表<sup>(\*)</sup>が有効と考えられることから、経済産業省が改正した告示と連動した「ガイドライン」が改訂されました。これにより製品利用者は製品の利用を止めるという判断や、他の緩和策の実施により、脆弱性による被害回避が可能となります。

その他、今回の改訂では一部の脆弱性情報を一般公表に先立ち、利用者に提供する取組みについて、記載が加えられています。

たとえば制御システムのように、製品開発者が製品利用者を特定していても、ソフトウェアがシステム上どのように使われているかを、把握していない場合があります。そこで、事前にその影響度と対策を計ることを可能とするため、製品利用者に脆弱性情報を先に提供します。これにより、一般公開で初めて脆弱性情報を認知するよりも、対策に十分な時間を確保することができ、脅威をより確実に回避することが可能になると考えられます。

IPA、JPCERT/CCではこのたびのガイドライン改訂により開始される「連絡不能案件」の脆弱性情報公表で、悪意のある者からの攻撃に備え、利用者が公表情報をもとに適切な対応が進むことを期待しています。

■ 本件に関するお問い合わせ先 IPA 技術本部 セキュリティセンター 渡辺／板橋 Tel: 03-5978-7527 Fax: 03-5978-7518 E-mail: <a href="mailto:vuln-inq@ipa.go.jp">vuln-inq@ipa.go.jp</a> JPCERT/CC 情報流通対策グループ 古田 Tel: 03-3518-4600 Fax: 03-3518-4602 E-mail: <a href="mailto:office@jpcert.or.jp">office@jpcert.or.jp</a>	■ 報道関係からのお問い合わせ先 IPA 戦略企画部広報グループ 横山／白石 Tel: 03-5978-7503 Fax: 03-5978-7510 E-mail: <a href="mailto:pr-inq@ipa.go.jp">pr-inq@ipa.go.jp</a> JPCERT/CC 事業推進基盤グループ 広報 江田 Tel: 03-3518-4600 Fax: 03-3518-4602 E-mail: <a href="mailto:pr@jpcert.or.jp">pr@jpcert.or.jp</a>
---	---

(\*) ガイドラインの改訂により、「連絡不能開発者一覧」の公表などによっても製品開発者と連絡が取れない場合には、中立的な委員で構成した委員会での審議を経て、脆弱性情報を公表できることとなった。この場合、「調整不能」であったことを明示した上で、通常の調整を経た脆弱性と同様に脆弱性情報ポータル・サイト JVN に掲載する。