JPCERT CC®

JPCERT/CC
脆弱性関連情報取扱いガイドライン

Ver 6.1

一般社団法人JPCERTコーディネーションセンター

2019年7月8日

JPCERT CC®

はじめに

「JPCERT/CC 脆弱性関連情報取扱いガイドライン」（以下、「本ガイドライン」という。）は、経済産業省告示「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」および IPA と JPCERT/CC による「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」に対応して、製品開発者の方々に、脆弱性関連情報の取扱いに関する事項をお知らせすることを目的として作成したものです。

JPCERT/CC は、1996 年の設立以来、海外の関連機関との連携の下、脆弱性に関連する情報を取り扱って参りました。具体的には、脆弱性関連情報[1]を安全かつ適切に取り扱うことを目的として、米国 CERT/CC、フィンランド NCSC-FI（旧 CERT-FI）およびオランダ NCSC-NL と連携し、一般公表日時までの調整を国際的に行う協力関係を構築してきました。また、国内においては、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」（平成 16 年 7 月 7 日官報公示）に基づき、「情報セキュリティ早期警戒パートナーシップ」における調整機関としての役割を果たしてきました。
この基準は、経済産業省告示「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 2 月 8 日官報公示）に引き継がれています。

本ガイドラインは、JPCERT/CC が製品開発者の連絡窓口である製品脆弱性対策管理者の方に期待する役割を中心に、脆弱性関連情報の受領から公表に至るまでのプロセスについて詳細に記述しています。「情報セキュリティ早期警戒パートナーシップ」の趣旨をご理解の上、脆弱性関連情報を扱う際の参考として、ご活用いただきますよう、お願い申し上げます。

一般社団法人 JPCERT コーディネーションセンター
代表理事　菊池 浩明

[1] 脆弱性に関する情報であって、経済産業省告示 19 号では、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、指令又はデータ及びそれらの使用方法）のいずれかに該当するものと定義されている

本ガイドラインにおける基本的な事項

脆弱性情報ハンドリング

脆弱性情報ハンドリングとは、発見者から届け出られた未知の脆弱性関連情報を、製品開発者に開示し、対策情報とともに一般に公表する一連のプロセスのこと。

規約への合意と規約の遵守

JPCERT/CC による脆弱性情報ハンドリングにご協力いただける製品開発者は、JPCERT/CC 製品開発者リスト登録規約に合意し、同リストに登録していただく必要があります。詳細は、「1. 組織内体制の構築と窓口の登録」をご参照ください。

公表日一致の原則

一般公表前の脆弱性関連情報をハンドリングする場合、脆弱性への対策方法が整わない時点で、脆弱性関連情報が一般に公表される、または悪意のある第三者に漏洩すると、悪意のあるコード（攻撃コード）が開発され、流通し、脆弱性の影響を受けるシステムに対する攻撃が始まる可能性があります。結果として製品利用者に被害が及ぶ事態を招く可能性があります。このため脆弱性関連情報は必ずその対策情報とともに公表されなければなりません。

また、複数の製品が影響を受ける脆弱性の場合には、情報の公表に当たって、関係者間で一定の足並みをそろえることが重要です。関係者間で調整した一般公表日時を待たずに、単独で情報を公表することは、同じ脆弱性の影響を受ける他の製品の利用者を危険にさらす可能性があります。

特に、海外機関との国際的な調整案件においては、情報開示の時期を誤った場合（一般公表日前に単独での情報公開を行った場合）、海外機関によって当該開発者を今後の脆弱性関連情報のハンドリング対象から外す措置が取られることがあります。

JPCERT CC®

目次

1. 組織内体制の構築と窓口の登録

■組織内体制の構築

製品開発者は、経済産業省告示「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」に基づき、脆弱性関連情報の取扱いを行うため組織内体制を整備してください。次の手順を参考にしてください。（※URL 等は付録参照）

a. 経済産業省告示「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」の確認
b. 「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」の確認
c. 組織内体制の構築、担当者（製品脆弱性対策管理者）の決定、情報取扱いルールの作成など
d. 製品脆弱性対策管理者が JPCERT/CC との連絡や外部からの情報を受け付けるための連絡窓口（専用のメールアドレス、電話番号等）の設置
e. 連絡窓口の JPCERT/CC 製品開発者リストへの登録

また、製品開発者の組織内体制の構築に関しては一般社団法人電子情報技術産業協会（JEITA）、一般社団法人コンピュータソフトウェア協会（CSAJ）が公開しているガイドラインもご覧ください。

製品開発者における脆弱性の取扱いと開示に関わるプロセスは、国際標準化されており、それぞれ次の国際標準として文書化されています。ビジネスをグローバルに展開する企業においては、これら国際標準との整合性もご勘案ください。

- ISO/IEC 30111 - Vulnerability handling processes (脆弱性取扱い手順)
- ISO/IEC 29147 - Vulnerability disclosure (脆弱性開示)

1-1. 窓口登録について

製品開発者は製品脆弱性対策管理者の連絡窓口情報を JPCERT/CC 製品開発者リストへ登録してください。登録種別には次の２種類があります。

- 一般登録：登録者は、自らが開発した製品固有の脆弱性関連情報に限らず、製品に関係する可能性のある脆弱性関連情報を受け取り、調査を行うことができる
- 個別登録：登録者は、原則として、自らが開発した製品に固有の脆弱性関連情報だけを受け取り、調査を行うことができる

それぞれの登録手順は次のとおりです。

《 一般登録 》

1) 所定の様式に従い製品脆弱性対策管理者の情報を JPCERT/CC に提出する （登録様式：https://www.jpcert.or.jp/form/poc.txt ）
2) JPCERT/CC から登録手続きに必要な様式を受け取り、必要書類を作成する
3) JPCERT/CC が設定して行われる製品開発者（製品脆弱性対策管理者）との間のミーティングにおいて、開発製品などについて説明し、必要書類を提出する
4) JPCERT/CC 製品開発者リストに登録される

登録に必要な提出物は、次のとおりです。

- JPCERT/CC 製品開発者リスト登録規約への合意
- JPCERT/CC が提示するテクノロジーキーワードリストへの回答
- PGP 公開鍵（必須ではない）

また、上記 3)のミーティングは、次の内容を想定しています。

- JPCERT/CC による脆弱性情報ハンドリングの説明
- 製品開発者による、製品開発者の組織概要説明
- 製品開発者による、主な製品の説明
- 製品開発者による、脆弱性取扱いに関する組織内体制の説明

《 個別登録 》

製品開発者は、脆弱性情報ハンドリングへの協力の同意と、個別登録の意思表明を、連絡窓口およびその責任者（製品脆弱性対策管理者）に関する次の情報とともに、電子メール等により JPCERT/CC に連絡する

- 製品脆弱性対策管理者の氏名
- 連絡可能なメールアドレス、または郵便物が到達可能な住所氏名
- PGP 公開鍵（必須ではない）

なお、製品開発者が発見者からの直接届出を受け付けることを希望する場合、JPCERT/CC は当該製品開発者の脆弱性受付窓口の情報を JVN に掲載します。

1-2. 日常的対応に関して

JPCERT/CC から受け取った脆弱性関連情報に基づき調査を行う際、使用している部品製品に脆弱性がある場合に、該当製品の特定が困難な作業となる場合があります。製品毎のソフトウエア構成を日頃から管理しておくことをお勧めします。

1-3. 登録後に

JPCERT/CC では、製品開発者リストへ登録いただいた製品脆弱性対策管理者の方向けの連絡会を開催しています。脆弱性情報ハンドリングに関する技術情報や業務内容をご紹介しておりますので、製品脆弱性対策管理者の方は、可能な限りこの連絡会に参加していただき、ご意見などをお聞かせ下さい。

2. 受付：脆弱性概要情報の取扱い

■脆弱性関連情報の受付に際して

JPCERT/CC が、新たな脆弱性関連情報について IPA や海外の CSIRT 等から連絡を受けた際には、製品脆弱性対策管理者へ連絡を行います。

脆弱性に該当する製品開発者を特定するため、JPCERT/CC は、テクノロジーキーワードリスト等を利用して該当すると思われる製品開発者を推定し、その製品開発者に対し「脆弱性概要情報」を通知し、製品開発者からの請求に基づいて「脆弱性詳細情報」を提供します。

ただし、該当する製品開発者が明らかである場合には、JPCERT/CC は「脆弱性概要情報」の通知を省略し、その製品脆弱性対策管理者に「脆弱性詳細情報」を通知します。

「脆弱性概要情報」については下記を、「脆弱性詳細情報」については 3 項をご参照ください。

2-1. 脆弱性概要情報とは

「脆弱性概要情報」は、技術的な詳細を含まない脆弱性の概要に関する情報です。情報が漏洩する可能性を低減しつつ、脆弱性詳細情報を必要とする製品開発者を特定することを目的として通知します。

「脆弱性概要情報」の例としては、次のようなものが考えられます。

- ○○の実装を用いた製品がありますか？
- ××の技術に関する脆弱性情報が報告されています。該当製品はありますか？
- □□に関する検証ツールが提供されています。使用する必要はありますか？

通知される「脆弱性概要情報」には、脆弱性識別番号が記載されます。脆弱性関連情報について製品開発者が JPCERT/CC へ問い合わせる際は、この識別番号を示してください。

2-2. 脆弱性概要情報の取扱いに際して

製品脆弱性対策管理者は、「脆弱性概要情報」を受け取った際は、その内容を元に、自組織の開発製品の中に脆弱性に該当する可能性のある製品があるかどうかを判断してください。脆弱性に該当する可能性のある製品があると判断した場合、JPCERT/CC に「脆弱性詳細情報」を請求してください。また、脆弱性に該当する製品がないと判断した場合は、JPCERT/CC にその旨を連絡してください。

2-3. 窓口が未登録の製品開発者への連絡・通知について

製品開発者リストに未登録の者が開発する製品について脆弱性関連情報が発生した際には、JPCERT/CC は当該製品開発者に対し、製品開発者リストへの登録（個別登録）の要請を行い、登録が完了した後に脆弱性関連情報を開示します。

なお、上記の目的で製品開発者に対し登録を要請するにあたり、以下に該当する場合は「連絡がとれない」ものと判断し、７項に示す手順にしたがって取り扱うことがあります。

- 製品開発者が不明な場合
- 製品開発者への連絡手段が存在しない場合
- 製品開発者への連絡手段のうち有効なすべての方法により、連絡を開始した日（以下「起算日」という）から一定の期間、一定の回数連絡を試みても、製品開発者からの応答がない場合

この時、JPCERT/CC が行う連絡手段とは、代表連絡先や、脆弱性関連情報に該当する製品のウェブ・ページ等インターネット上に記載された連絡先情報による、電子メールや郵便、電話、FAX、バグ管理システム、掲示板、ソーシャル・ネットワーキング・サービス等を使った方法を指します。

3. 調査・検証：脆弱性詳細情報の取扱いと製品の調査

■脆弱性詳細情報の受取りに際して

JPCERT/CC は、「脆弱性詳細情報」を請求した製品開発者に対して、詳細情報を開示します。製品開発者はその情報を元に、開発製品について調査してください。また、「脆弱性詳細情報」を受け取ったすべての製品開発者は、脆弱性情報の公表時に製品開発者名とともにその対応状況等が公表される場合があります。公表される対応状況の詳細は、6 項を参照してください。

3-1. 脆弱性詳細情報とは

「脆弱性詳細情報」とは、脆弱性関連情報のうち技術的な詳細を含む情報で、実際に脆弱性に該当する製品があるかどうかを調べるための情報です。例えば、脆弱性の検証方法や検証ツール、攻撃コードなどがこれにあたります。

3-2. 脆弱性詳細情報の取扱いに際して

「脆弱性詳細情報」を受け取った後は、その情報を元に脆弱性に該当する可能性があると判断した製品について、調査・検証してください。脆弱性に該当する製品があった場合、その製品に関して対策方法等を検討してください。また、「脆弱性詳細情報」は機密情報として慎重な取扱いをお願いします。

3-3. 脆弱性調査・検証結果の報告

「脆弱性詳細情報」に基づいた調査・検証後、その結果を JPCERT/CC に報告してください。この際、次の点についてご連絡ください。

- ●脆弱性該当製品の有無
- ●該当製品がある場合、回避方法や修正方法の作成・提供方針
- ●該当製品がある場合、対応スケジュール（回避方法の策定スケジュールや修正方法の策定スケジュールなど）
- ●製品開発者としての公表情報の作成・提供方針

3-4. 脆弱性調査・検証における注意点

製品開発者は、脆弱性の調査・検証時に次の点に留意してください。

- ●脆弱性関連情報を、組織内の必要最小限の関係者にのみ開示する
- ●脆弱性関連情報を、情報の一般公表日時までは第三者に漏洩しないように管理する
- ●脆弱性関連情報で示される脆弱性が、他の製品開発者が開発する製品に含まれることが推定される場合には、JPCERT/CC にその旨を連絡する

4. 調整：公表日時の決定

■脆弱性情報の一般公表日時の設定に際して

冒頭の「本ガイドラインにおける基本的な事項」にて記述したとおり、脆弱性情報には一般公表日時が設定されます。製品開発者は、対策情報なども含む脆弱性関連情報の公表に関して、一般公表日時を遵守してください。

4-1. JPCERT/CC における公表日時の決定

脆弱性情報の一般公表日時は、製品開発者と JPCERT/CC が協議の上決定します。特に、複数の製品開発者が関係する脆弱性情報の場合には、JPCERT/CC が製品開発者間のスケジュール調整を主導的に行います。また、決定した一般公表日時は JPCERT/CC より各製品開発者と関係機関に連絡します。

JPCERT/CC では、一般公表日時の決定の際には、JPCERT/CC が製品開発者に脆弱性関連情報を通知した日時から起算して 45 日以内を目安とします。ただし、公表日時は次の点も考慮して検討し、この目安を前後することがあります。

- ●製品開発者が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
- ●脆弱性情報の流出に伴うリスク
- ●脆弱性が悪用されるリスク、脆弱性を悪用したインシデントの発生状況

4-2. 一般公表日時決定後の対応

決定された一般公表日時に関して、作業進捗等の理由で見直しが必要となった場合には、すみやかに JPCERT/CC に連絡してください。複数の製品開発者が関係する脆弱性の場合には、JPCERT/CC では他の製品開発者との調整の上、一般公表日時の変更等を検討します。

また、次の場合においては、一般への公表を取りやめることがあります。

- ●通知を行った製品開発者から既知[2]の脆弱性情報であるとの連絡を受けた場合
- ●通知を行った製品開発者から脆弱性による影響が無い[3]との連絡を受けた場合
- ●製品開発者がすべての製品利用者に脆弱性情報と対策情報を通知する場合[4]（システム構築事業者[5]を介して通知するケースを含む）

---

2 製品開発者が脆弱性情報を既に公式 Web サイト等で公表している場合

3 複数の製品開発者が関係する脆弱性の場合には、脆弱性による影響が無い場合でもベンダ情報を公表します。詳細は、6-4 項を参照して下さい

4 製品開発者が脆弱性に該当する製品の利用者をすべて把握していることが前提となります

5 ソフトウエア製品を入手し、それを使ってシステムを構築し、利用者に提供する企業または個人のこと。システムの保守、運用のサービスを提供することもあります

4-3. 脆弱性情報の公表に際して

脆弱性情報の一般公表日時までに、脆弱性関連情報に係わる対策情報[6]を作成するよう努めてください。また、脆弱性関連情報に係わる対応状況を JPCERT/CC に適宜連絡してください。

4-4. 重要インフラ事業者等に対する優先的な情報の提供

JPCERT/CCは、届出がなされた脆弱性関連情報に関して、重要インフラ等に対し特に影響が大きいと推察される場合、IPAおよび製品開発者と協議の上、決定された一般公表日時より前に、脆弱性関連情報と対策方法を、政府・行政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。優先的な情報提供の対象となる重要インフラ事業者は、内閣サイバーセキュリティセンター（NISC）の最新の「重要インフラの情報セキュリティ対策に係る行動計画」で定める重要インフラ事業者等です。

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、情報提供は行いません。

優先的な情報の提供を受ける重要インフラ事業者等を含む顧客サポートを円滑に行うために、6-3項にある方法により、製品開発者は、一般公表に先立って、製品の顧客に対策方法などを個別に通知することができます。詳しくは6-3項を参照ください。

4-5. 脆弱性情報公表までの注意事項

JPCERT/CC と製品開発者との間の連絡は、原則として製品脆弱性対策管理者を通して行います。製品脆弱性対策管理者には組織内の関係部署との調整をお願いします。

製品開発者に開示された脆弱性情報の発見者は、IPA および JPCERT/CC による一般公表までの間、脆弱性情報を第三者に漏えいしないよう適切に管理することを早期警戒パートナーシップガイドラインによって求められています（発見者に対する情報非開示依頼、以下「情報非開示依頼」という）。これに対して発見者は、起算日から１年以上経過した届出については、情報非開示依頼の取り下げを求めることができます。また１年に満たない場合であっても、発見者が止むを得ず脆弱性関連情報を開示する場合がありますので、製品脆弱性対策管理者は予めご留意ください。

製品開発者から脆弱性調査・検証結果等についての報告がなく、JPCERT/CC からの連絡への応答もないまま起算日から一定の期間が経過した場合、「連絡がとれない」ものと判断し、７項に示す手順にしたがって取り扱うことがあります。JPCERT/CC は原則として製品開発者リスト登録時に指定された連絡窓口情報を用いて連絡をおこないますので、製品

6 対策情報の作成に関しては、5 項を参照して下さい

開発者は、登録情報に変更があった場合はすみやかに JPCERT/CC へご連絡ください。

4-6. 海外調整機関が主導する脆弱性情報ハンドリングにおける公表日時の決定

JPCERT/CC が取り扱う脆弱性情報には、CERT/CC など海外の調整機関からの連絡を受けて、日本国内やアジア圏での調整に協力するものもあります。そのような場合、脆弱性情報の一般公表日時は、主導する海外調整機関によって決定されます。

5. 対策：対策情報の作成

■対策情報の作成に際して

脆弱性調査・検証の結果、脆弱性に該当する製品が見つかった場合は、一般公表日時までに対策方法の作成や、公表する情報の作成などの対応をお願いします。

5-1. 対策方法の作成

脆弱性に該当する製品について、回避方法（代替製品への切換えや利用中止を含むワークアラウンド）や修正方法（アップデートやパッチ等）の作成をお願いします。併せて、脆弱性公表の際に一般への公表が可能な情報があれば、公表する情報の準備もお願いします。さらに、脆弱性情報の公表後も、引き続き必要な情報の更新・周知をお願いします。

5-2. 対策情報の作成における注意点

脆弱性情報の一般公表の際に対策方法が存在しない場合でも、公表しなければ製品利用者が自らリスク管理できる機会を失して被害が発生する可能性が考えられます。修正方法（パッチ等）の作成が困難な場合には、回避方法（ワークアラウンド）のみでも作成してください。この場合修正方法（パッチ等）の作成に関しては製品開発者の判断に委ねられますが、可能な限り作成をお願いします。

6. 公表：対策情報の連絡と公表

■脆弱性情報の公表に際して

脆弱性情報の一般への公表は、全世界で関係する機関が同時に行う場合があります。JPCERT/CC が脆弱性情報を公表する場合には、以下のウェブサイトを通じて情報を公表します。なお、このウェブサイトは IPA と共同で運営しています。

Japan Vulnerability Notes (JVN)
https://jvn.jp/

6-1. 製品開発者における公表情報の作成

製品開発者は、脆弱性情報に関して公表可能な情報がある場合には、一般公表日時までに公表情報の作成をお願いします。公表する内容については以下の文書に指針が示されていますので、これに沿って作成してください。

独立行政法人情報処理推進機構（IPA）
「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」
https://www.ipa.go.jp/security/ciadr/vuln_announce_manual.pdf

6-2. JPCERT/CC への対応状況の連絡

製品開発者は、自社の対応状況について JPCERT/CC に連絡してください。その際には次の項目を含めてください。JPCERT/CC ではこれらの情報を元に、JVN に掲載する一般公表情報を作成します。

1. JPCERT/CC が発行した識別番号
2. 製品開発者名称（組織名）
3. 製品の該当状況（以下 1～4 より選択）
   1) 該当製品あり
   2) 該当製品あり：調査中
   3) 該当製品なし
   4) 該当製品なし：調査中
4. 公表情報に記載するフリーフォーマットの文章
   （URL や説明文など　※注：6-4 を参照のこと）

6-3. 一般公表前の顧客への個別通知

一般公表に先立って、直接または間接的に製品の顧客に対策方法などを個別に通知することにより、社会的な混乱を生じるリスクを低減できると見込まれる場合には、その旨を

JPCERT/CC に連絡して下さい。
JPCERT/CC が了承し、かつ、本通知に関与する者が、脆弱性情報と対策方法について、第三者に漏えいしない様に適切に管理することを担保出来ている場合、製品開発者から直接あるいはシステム構築事業者を介して、製品利用者に脆弱性検証の結果や対応状況を一般公表前に通知することが出来ます。

6-4. JPCERT/CC における公表情報の作成と公表

JPCERT/CC は、事前に設定された公表日時に、JVN を通じて脆弱性情報を一般に公表します。この際に公表される情報には以下が含まれます。

1) 脆弱性情報の概要
2) 脆弱性情報の影響範囲
3) 脆弱性情報に対する製品開発者の対応状況
4) 各製品開発者固有の情報

上記 3)の製品開発者の対応状況においては、「脆弱性詳細情報」を通知した製品開発者の対応状況を「ベンダ情報」として公表します。この際、複数の製品開発者が関係する脆弱性情報の場合には、各製品開発者の状況を次のような表現で掲載します。

表現方法	内容
該当製品あり	脆弱性該当製品がある場合
該当製品あり：調査中	脆弱性該当製品があり継続して調査を行っている場合
該当製品なし	脆弱性該当製品がない場合
該当製品なし：調査中	脆弱性該当製品は見つかっていないが、継続して調査を行っている場合
脆弱性情報提供済み（デフォルト表示 [7]）	「脆弱性詳細情報」を請求・取得した場合

また、上記 4)の製品開発者固有の情報においては、6-2-4 において JPCERT/CC に通知された情報を記載します。これらの情報の公表内容のイメージを[図 1]、[図 2]に示します。

6-5. 脆弱性情報の一般公表後の対応

脆弱性情報に関する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。また、対策方法を作成した場合は、脆弱性情報の一般公表日時以降であっても、それを製品の利用者に周知してください。

[7]「脆弱性詳細情報を請求し入手したすべての製品開発者のデフォルトの表示は「脆弱性情報提供済み」となります。製品開発者自身により、任意のタイミングでその他の表現に修正できます

JVN00XX-XXXY ○○に関する脆弱性

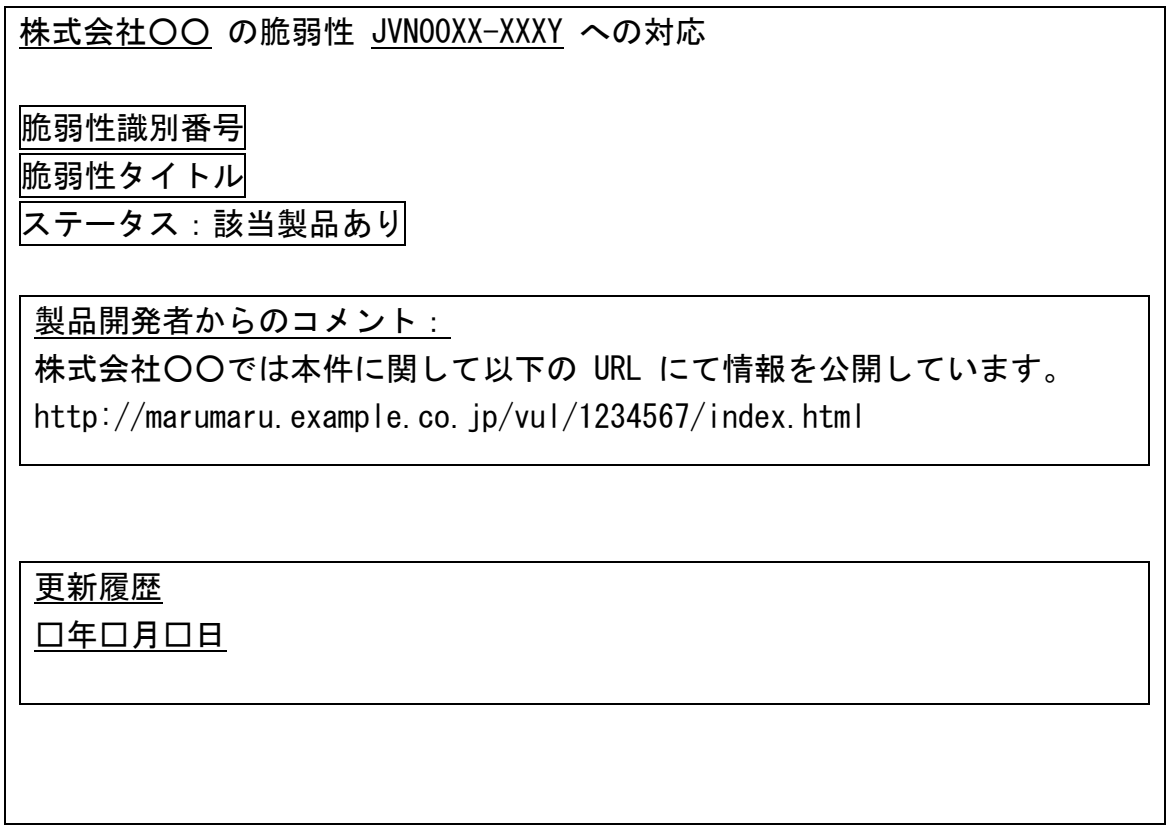
概要
（省略）
影響を受けるシステム
（省略）
詳細情報
（省略）
想定される影響
（省略）
対策方法
（省略）
ベンダ情報

ベンダ	ステータス	ベンダからのコメント	ベンダの告知ページ
株式会社○○	該当製品あり		
××ソリューション	該当製品なし		
△△情報システム	脆弱性情報提供済み		
□□情報産業株式会社	該当製品なし：調査中		
☆☆☆ Systems	該当製品あり：調査中		

参考情報
（省略）
JPCERT/CC からの補足情報
（省略）
JPCERT/CC による脆弱性分析結果
（省略）
謝辞
（省略）
関連文書
（省略）
更新履歴
（省略）

[図 1：JVN で公表する脆弱性情報の例]

「ステータス欄」の記載内容は各製品開発者情報（図 2）へのリンクになります。



[図 2：図 1 において、ステータス欄をクリックした際に表示される画面]

「製品開発者からのコメント」のフィールドには 6-2-4.の内容が記載されます。

7. 製品開発者との調整ができない場合の取扱い

IPA および JPCERT/CC は、製品開発者の連絡先がわからない、または連絡先はわかるが応答が無いなど、公表に向けて製品開発者との合意を形成することが困難であると判断した場合には、製品開発者名や製品情報などを JVN で公表することがあります。

7-1. 連絡不能開発者一覧での公表

2-3 項または 4-5 項に示す状況により製品開発者と連絡がとれない場合、JPCERT/CC は、製品開発者名を JVN にて公表し、当該製品開発者からの連絡を呼びかけます。それでも連絡がとれない場合には、3 ヶ月程度の猶予期間を置いた後、対象製品（製品名およびバージョン）を公表し、広く一般に情報提供を呼びかけます。

製品開発者名が JVN で公表されるイメージを[図 3]、対象製品の公表イメージを[図 4-1]及び[図 4-2] に示します。

7-2. 製品開発者との調整ができない場合の取扱い

7-1 項に示す手順による呼びかけにもかかわらず、さらに一定の期間、製品開発者との連絡がとれない場合、JPCERT/CC および IPA は、公表に向けた製品開発者との合意形成が困難であると判断し、連絡期限を追記して対象製品の公表情報を更新します。

その後、さらに製品開発者と連絡がとれない状況が続いた場合には、製品利用者自身にその対象製品を継続使用することで生じるリスクを自ら管理する機会を提供するため、第三者委員で構成される公表判定委員会での公表判断の審議を経た上で、製品開発者名とともに脆弱性情報などを JVN で公表することがあります。

公表判定委員会による公表判断のための審議を受ける場合、JPCERT/CC は、当該脆弱性情報の製品開発者連絡窓口情報や調整状況を示す情報など、公表判断に必要とされる情報を、公表判定委員会を組織する受付機関の求めに応じて提供します。

連絡期限を追記して更新した対象製品の公表イメージを[図 5-1]及び[図 5-2]に示します。公表判定委員会を経た脆弱性情報が JVN で公表されるイメージを[図 6]に示します。

JPCERT CC®

開発者情報　公開調査

概要

IPA（独立行政法人 情報処理推進機構）および JPCERT コーディネーションセンターでは、情報セキュリティ早期警戒パートナーシップに基づいて届出られたソフトウエア製品の製品開発者、またはその関係者からのご連絡を求めています。

調査対象

情報セキュリティ早期警戒パートナーシップに基づいて届けられたソフトウエア製品で、インターネット等から入手し得る情報では連絡がとれない、以下の一覧に掲載されている製品開発者、またはその関係者が調査対象です。

連絡先

Subject に問い合わせ番号を明記し jvn@jvn.jp 宛に、ご連絡ください。

連絡不能開発者一覧

問合せ番号	開発者名	関連情報	一覧追加日	製品情報	備考
DID#AAAAA	AAA		11/12/16		
DID#BBBBB	BBB		11/12/16		
DID#CCCCC	-		11/12/16		製品 C の開発者
DID#DDDDD	-	http://ddd	11/09/29	11/12/16(開示)	
DID#EEEEE	EEE	http://eee	11/09/29	11/12/16(開示)	

[図 3：JVN で製品開発者名を公表し連絡を呼びかける例]

（項目説明）問合せ番号　：掲載内容詳細の問合せ用番号
開発者名　：連絡不能開発者名またはハンドル名
関連情報　：開発者または製品情報へのリンク等
一覧追加日　：連絡不能開発者一覧に掲載した日付
製品情報　：対象製品情報開示日付と製品情報へのリンク
備考　：補足情報等

【対象が企業の場合】

XXXXX の製品開発者に関する情報

製品名ｘｘｘ、バージョン xxxx の作者、または著作権を有している製品開発者の方、または販売代理店等、本製品に関係する方は下記の宛先までご連絡をお願いします。
連絡先： jvn@jvn.jp
公開日：yyyy 年 mm 月 dd 日

[図 4-1：JVN で製品情報を公表し連絡を呼びかける例]

【対象が非企業（コミュニティを含む）の場合】

XXXXX の製品開発者に関する情報

製品名ｘｘｘ、バージョン xxxx の作者、または著作権を有している製品開発者の方、または製品開発者との連絡方法をご存じの方は下記の宛先までご連絡をお願いします。また、同製品の派生・関連製品のコミュニティに所属する製品開発者の方で、修正版の提供が可能な方からのご連絡もお待ちしています。
連絡先： jvn@jvn.jp
公開日：yyyy 年 mm 月 dd 日

[図 4-2：JVN で製品情報を公表し連絡を呼びかける例]

【対象が企業の場合】

XXXXX の製品開発者に関する情報

製品名ｘｘｘ、バージョン xxxx の作者、または著作権を有している製品開発者の方、または販売代理店等、本製品に関係する方は下記の宛先までご連絡をお願いします。
本件に関するご連絡は、yyyy 年 mm 月 dd 日まで受け付けます。
連絡先： jvn@jvn.jp
公開日：yyyy 年 mm 月 dd 日
更新日：yyyy 年 mm 月 dd 日（連絡期限追記）
なお、yyyy 年 mm 月 dd 日までにご連絡をいただけなかった場合は、製品開発者と連絡がとれないため調整不能と判断し、「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「Ⅳ. ソフトウエア製品に係る脆弱性関連情報取扱」および付録 8、9 及び 11 の記載に準じて取り扱います。

[図 5-1：JVN で公表した製品情報に連絡期限を追記した例]

【対象が非企業（コミュニティを含む）の場合】

XXXXX の製品開発者に関する情報

製品名ｘｘｘ、バージョン xxxx の作者、または著作権を有している製品開発者の方、または製品開発者との連絡方法をご存じの方は下記の宛先までご連絡をお願いします。また、同製品の派生・関連製品のコミュニティに所属する製品開発者の方で、修正版の提供が可能な方からのご連絡もお待ちしています。
本件に関するご連絡は、yyyy 年 mm 月 dd 日まで受け付けます。
連絡先： jvn@jvn.jp
公開日：yyyy 年 mm 月 dd 日
更新日：yyyy 年 mm 月 dd 日（連絡期限追記）
なお、yyyy 年 mm 月 dd 日までにご連絡をいただけなかった場合は、製品開発者と連絡がとれないため調整不能と判断し、「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「Ⅳ. ソフトウエア製品に係る脆弱性関連情報取扱」および付録 8、9 及び 11 の記載に準じて取り扱います。

[図 5-2：JVN で公表した製品情報に連絡期限を追記した例]

JVN00XX-XXXY ○○に関する脆弱性

概要

（省略）

ベンダ情報、製品情報

○○○○株式会社　　製品 A ver*.*

詳細情報

（省略）

想定される影響

（省略）

対策方法

（省略）

ベンダの見解

なし

JPCERT/CC からの補足情報

公表に至る経緯は以下のとおりです。

YYYY/MM/DD：「連絡不能開発者一覧」に「補足情報」の掲載を行う

YYYY/MM/DD：「連絡不能開発者一覧」に「補足情報」を掲載後、期限内に製品開発者から応答なし

YYYY/MM/DD：本情報を「JVN」にて公表

JPCERT/CC による脆弱性分析結果

YYYY.MM.DD における脆弱性分析結果(CVSS Base Metrics)

（省略）

検証情報

IPA および、JPCERT/CC にて、届出されたバッファオーバーフローの脆弱性について再現検証を行った結果、○○の環境において、ファイル名のレジスタ値（EIP）が書き換わることを確認しました。なお、△△の環境においては、製品 A が異常終了することのみを確認しました。それぞれにおいて、シェルコードの実行までは確認していません。また、Vx.x においても同様となることを確認しました。

更新履歴

（省略）

[図 6：JVN で公表する脆弱性情報の例]

製品開発者と連絡がとれない案件において、製品の利用者自身によるリスク管理を促すことを目的として公表する場合の例です。

8. 脆弱性情報ハンドリングにおける注意事項

脆弱性ハンドリング全体を通して注意すべき事項を以下に示します。

8-1. 情報漏洩の防止について

次の事項に関する情報の漏洩に関して留意し、関連情報の管理の徹底をお願いします。

- 脆弱性関連情報
- 一般公表日時（日付、時間など）
- 脆弱性に関する製品の対策情報

8-2. 関係組織への情報の取扱いについて（情報の二次配布）

製品への脆弱性の影響調査等を行うにあたり、外部の開発委託先や協力会社など（以下、関係組織）との脆弱性関連情報の共有が必要な場合には JPCERT/CC に連絡してください。関係組織に対する脆弱性関連情報の開示は、原則として JPCERT/CC から直接行います。具体的には、次の手順となります。

1.関係組織との情報共有を望む製品開発者と JPCERT/CC とのやりとり

1) 製品開発者は、脆弱性関連情報の共有を必要とする関係組織に関する以下の項目を JPCERT/CC へ送付する
   a. 組織名、又は会社名
   b. 担当者名
   c. 担当者の連絡先情報（メールアドレス、電話番号）
2) 製品開発者は、関係組織の担当者に、脆弱性関連情報に個別に割り当てられた「識別番号」のみを伝え、あわせて、関係組織の担当者から JPCERT/CC に直接連絡し脆弱性識別番号に対応する脆弱性関連情報を請求するように伝える

2.製品開発者から連絡を受けた関係組織の担当者と JPCERT/CC とのやりとり

1) 関係組織の担当者は、JPCERT/CC に電話もしくはメールで連絡し「識別番号」に対応する脆弱性関連情報を請求する（この際、JPCERT/CC では上記識別番号を使って認証します）
2) 関係組織は、JPCERT/CC との必要な手続き（連絡窓口情報の登録）を経て、脆弱性関連情報を受けとる

なお、製品開発者が自社のグループ企業に対して脆弱性情報を共有する場合、および、協力会社等から派遣され自社に常駐する者などに対して脆弱性情報を共有する場合においては、製品開発者が実質的に監督することができ情報管理責任を負うことができることを条件に、上記の手順を経ずにそれらの者に対して脆弱性情報を共有することができます。

8-3. 製品開発者間の相互の連絡について

脆弱性関連情報およびそれに係わる作業に関して、製品開発者間の相互の連絡が必要な場合は、JPCERT/CC に相談してください。

8-4. JPCERT/CC における脆弱性関連情報の取扱いについて

JPCERT/CC は、届出がなされた脆弱性関連情報に関して、次の場合においては、秘密保持契約を締結したうえで、海外の調整機関または IPA を含む外部機関に連絡したり、分析を依頼したりすることがあります。

- ●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
- ●脆弱性関連情報の詳細な分析が必要な場合

また、JPCERT/CC は、届出がなされた脆弱性の社会的影響度を勘案し、影響度の大きな案件の処理を優先し、影響度の低い案件の処理を簡易にすることがあります（例：脆弱性関連情報を開発者に通知することをもって調整を終了するなど）。

8-5. JPCERT/CC による例外的な対応

関係者による情報漏洩や、関係者以外（マスメディアなど）による情報のリークが発生した場合や、脆弱性の悪用や脆弱性によるインシデントの発生等がみられた場合、一般公表の日時が早まる可能性があります。

8-6. JPCERT/CC への連絡に際して

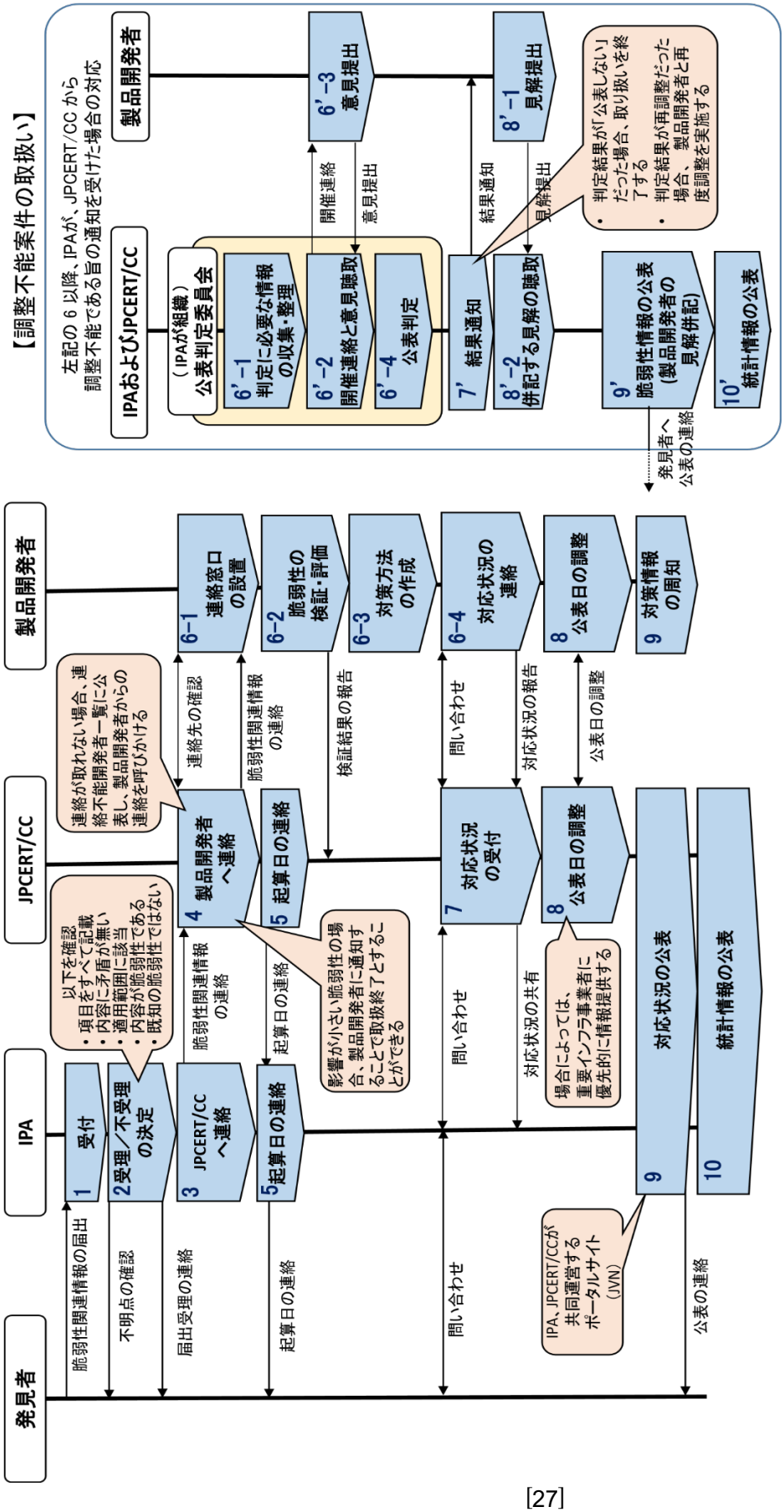
JPCERT/CC へ連絡する場合には、必要に応じてメッセージに暗号化を施した上で連絡してください。

脆弱性情報ハンドリングに係る問い合わせ先

一般社団法人 JPCERT コーディネーションセンター
早期警戒グループ

E-Mail : vultures@jpcert.or.jp
電話番号:03-6271-8901 (9:00-18:00)
FAX 番号:03-6271-8908

付録 A. 脆弱性情報ハンドリングプロセスの概要図



付録 B. 関連情報サイト一覧

■ JPCERT コーディネーションセンター(JPCERT/CC) ： https://www.jpcert.or.jp/

- 脆弱性対策情報
  https://www.jpcert.or.jp/vh/top.html
- 製品開発者登録
  https://www.jpcert.or.jp/vh/register.html
- Japan Vulnerability Notes (JVN)
  https://jvn.jp/

■ 経済産業省 ： https://www.meti.go.jp/

- 脆弱性関連情報取扱体制
  https://www.meti.go.jp/policy/netsecurity/vulhandlingG.html
- 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２月８日改正）
  https://www.meti.go.jp/policy/netsecurity/vul_notification.pdf

■ 情報処理推進機構(IPA) ： https://www.ipa.go.jp/

- 情報セキュリティ：脆弱性対策
  https://www.ipa.go.jp/security/vuln/
- 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/ciadr/partnership_guide.html
- 情報システム等の脆弱性情報の取扱いにおける法律面の調査
  https://www.ipa.go.jp/security/fy15/reports/vuln_law/index.html
- 脆弱性情報に係る調整不能案件の公表に関する基礎調査報告書
  https://www.ipa.go.jp/files/000014255.pdf
- 脆弱性情報に係る調整不能案件の公表のあり方に関する調査報告書
  https://www.ipa.go.jp/files/000014256.pdf
- 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
  https://www.ipa.go.jp/security/ciadr/vuln_announce_manual.pdf

■ その他(日本語)

- JEITA（一般社団法人 電子情報技術産業協会）
  製品開発ベンダーにおける脆弱性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
  http://it.jeita.or.jp/infosys/info/0407JEITA-guideline/index.html
- CSAJ（一般社団法人コンピュータソフトウェア協会）
  製品開発ベンダーにおける脆弱性関連情報取り扱いに関する体制と手順整備のためのガイドライン
  https://www.csaj.jp/activity/advocacy/20041203_security.pdf

■ その他(英語)

- CERT Coordination Center (CERT/CC)
  https://www.sei.cmu.edu/about/divisions/cert/index.cfm
- The Cybersecurity and Infrastructure Security Agency (CISA)（旧 US-CERT）
  http://www.us-cert.gov/
- The Cybersecurity and Infrastructure Security Agency (CISA)（旧 ICS-CERT）
  https://ics-cert.us-cert.gov/
- CERT/CC Vulnerability Notes Database
  https://www.kb.cert.org/vuls/
- The National Cyber Security Centre Netherlands (NCSC-NL)
  https://english.ncsc.nl/
- The National Cyber Security Centre Finland (NCSC-FI)
  https://www.kyberturvallisuuskeskus.fi/en

更新履歴：

2004-08-25　Ver1.0　初版
2004-10-13　Ver1.1　付録記載の URL 情報を更新
2008-04-21　Ver.2.0
2009-07-10　Ver.3.0
2011-03-31　Ver.4.0
2014-05-30　Ver.5.0
2017-06-22　Ver.6.0　影響度が低い脆弱性を簡易に取り扱う考え方を導入
2019-07-08　Ver.6.1