JPCERT/CC
脆弱性関連情報取扱いガイドライン

Ver 2.0

有限責任中間法人JPCERTコーディネーションセンター

はじめに

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。米国 CERT/CC が扱った脆弱性情報の件数は 2006 年に約 8,000、2007 年も 7,200 を数えるなど，高い値で推移しています。また、情報機器やソフトウエア製品のグローバル化に伴い、脆弱性情報が発見された場合には、その影響を受ける製品の利用者と製品開発者が、国境を越えて存在することも珍しくはありません。このため、JPCERT/CC は、脆弱性関連情報を安全かつ適切に取り扱うことを目的として、米国 CERT/CC、英国 NISCC（現 CPNI）とパートナーシップを締結し、一般公開日までの調整を行う協力関係を国際的に構築してきました。

一方、JPCERT/CC は、独立行政法人情報処理推進機構（IPA）と共同で、国内の指針や公的なガイドラインの整備を進めてきました。

JPCERT/CC 脆弱性関連情報取扱いガイドラインは、JPCERT/CC の脆弱性関連情報の取扱い実績と、「ソフトウエア等脆弱性関連情報取扱基準」及び「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」を前提として、製品開発者の方々に、脆弱性関連情報の取扱いに関してお願いをすることを目的としたものです。具体的には、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記述しています。脆弱性関連情報を扱う際の参考に本文書をご利用ください。

有限責任中間法人 JPCERT コーディネーションセンター
代表理事　歌代和正

覚えていただきたい事項

脆弱性情報ハンドリング

脆弱性情報ハンドリングとは、脆弱性関連情報を必要に応じて適切に開示することで、脆弱性情報の悪用、または障害を引き起こす危険性を最小限に食い止めるためのプロセスです。JPCERT/CC は、このプロセスの調整役(コーディネーター)として、影響のある製品を持つ製品開発者に脆弱性情報の連絡、対応を依頼します。

規約への合意と規約の遵守

JPCERT/CC の脆弱性情報ハンドリングの枠組みにご協力頂ける場合、JPCERT/CC が用意する「JPCERT コーディネーションセンター製品開発者リスト登録規約」に合意して頂く必要があります。製品開発者の皆様には、本枠組みへのご参加と共に、上記規約を遵守して頂きますようお願いします。

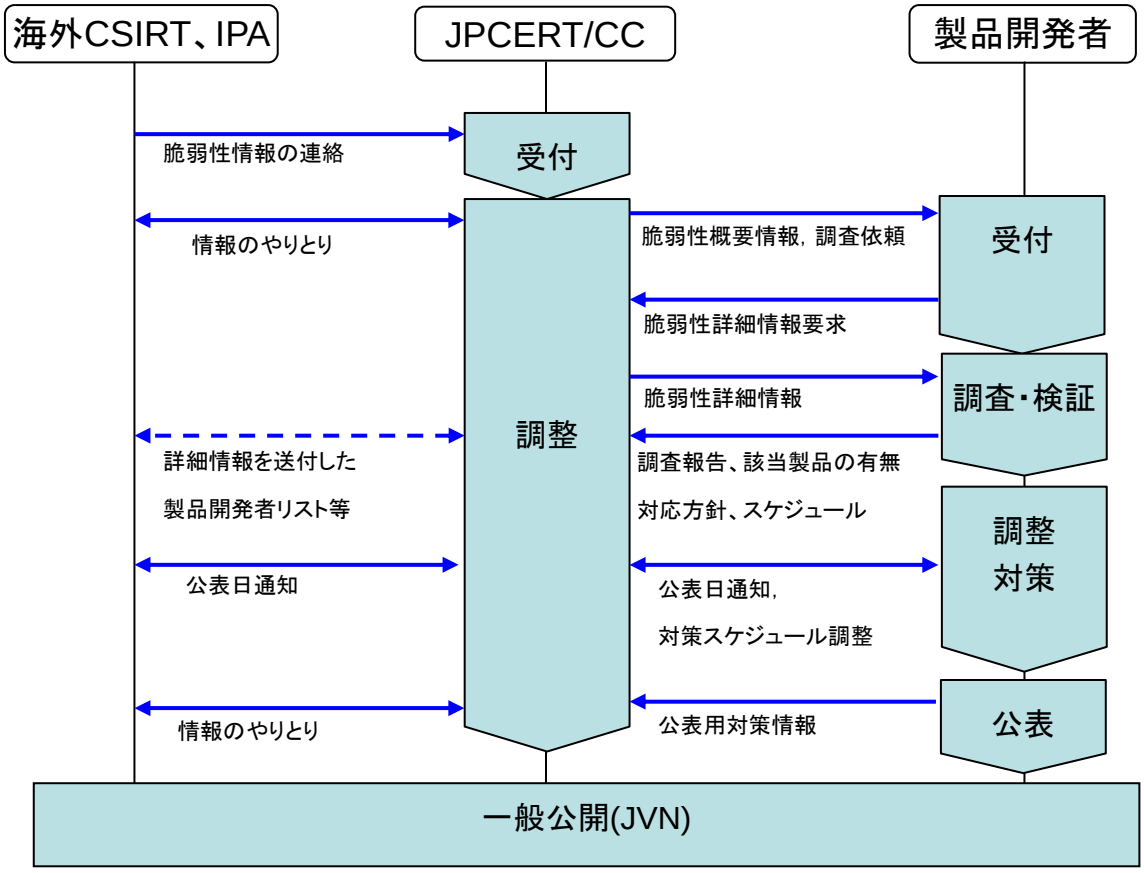
公表日一致の原則

一般公表前の脆弱性関連情報をハンドリングする場合、脆弱性関連情報が、対策方法が整わない時点で、一般にまたは悪意のある第三者に漏れると、悪意のあるコード(攻撃コード)が開発され、流通し、システムの脆弱性への攻撃が始まる可能性があります。結果としてシステムに危険が及ぶ事態を招く可能性があります。特に、複数の製品が影響を受ける脆弱性の場合には、関係者間で一定の足並みをそろえることが重要です。

また、関係者間で調整した一般公表日を待たずに、単独で情報を公表することは、他の製品の利用者を危険にさらす可能性があります。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)、当該開発者が今後の脆弱性関連情報のハンドリングから外されるだけでなく、最悪のケースでは日本全体として公表前の脆弱性関連情報をコーディネーションできなくなることも考えられます。

脆弱性情報ハンドリングプロセスの概要

脆弱性情報ハンドリングの概要は、下図の通りです。



次ページ以降で、脆弱性情報ハンドリングの詳細を示します。

脆弱性情報ハンドリングプロセスの詳細説明

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「ソフトウエア等脆弱性関連情報取扱基準」に基づき、脆弱性関連情報の取扱いを行なうため組織内体制を整備してください。以下の例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「ソフトウエア等脆弱性関連情報取扱基準」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. 暗号化通信の準備（PGP でのやりとりの準備）
f. 連絡窓口の JPCERT/CC 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社団法人電子情報技術産業協会（JEITA)、社団法人情報サービス産業協会（JISA）が公開しているガイドラインもご覧ください。

■窓口登録について

製品開発者は JPCERT/CC に製品脆弱性対策管理者の連絡窓口情報を登録してください。登録種別には以下の２種類があります。

- 一般登録：登録者が JPCERT/CC から受け取る脆弱性関連情報について、特に制限を設けない
- 個別登録：登録者が JPCERT/CC から受け取る脆弱性関連情報は、それが一般公開前のものである場合、登録者が開発した製品に固有のもので、他の製品開発者との調整作業が生じないものに原則として限定される

それぞれの登録手順は以下の通りです。

《 一般登録 》

1) 製品開発者が所定の様式により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：http://www.jpcert.or.jp/form/poc.txt ）
2) JPCERT/CC から、登録手続きに必要な書類を受け取る
3) 製品開発者が登録手続きのための必要書類を作成する
4) 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
5) JPCERT/CC 製品開発者リストに登録される

上記 3)の登録に必要な書類は、以下のとおりです。
- JPCERT/CC 製品開発者リスト登録規約への合意
- JPCERT/CC からの連絡時に暗号化を行うための公開鍵（PGP）
- 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

また、上記 4)のミーティングは、以下の内容を想定しております。
- 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、脆弱性取扱に関する組織内体制の説明

《 個別登録 》
製品開発者が、脆弱性情報ハンドリングへの協力および登録についての同意とともに個別登録の意思の表明を、連絡窓口およびその責任者（製品脆弱性対策管理者）に関する以下の情報とともに、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、メールアドレス
- PGP 公開鍵、または郵便物が到達可能な住所氏名

■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、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ごろから管理しておくことをお奨めします。

■登録後に

JPCERT/CC では、製品開発者リストへ登録した製品開発者の方にお集まりいただき、脆弱性情報ハンドリング業務や技術情報に関する定例連絡会を定期的に開催します。製品脆弱性対策管理者の方には、可能な限りこの定例連絡会に参加して頂き、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

■脆弱性関連情報の発生に際して

JPCERT/CC が、IPA や海外の CSIRT からの連絡を受けるなど、脆弱性関連情報発生時には、製品脆弱性対策管理者へ、「脆弱性の概要情報」を通知します。

2-1. 脆弱性概要情報とは

脆弱性概要情報とは、脆弱性関連情報について、技術的な詳細を含まない概要情報です。始めに脆弱性概要情報を通知し、脆弱性の詳細情報を必要とする製品開発者を特定し、情報が漏えいする可能性を低減するためです。脆弱性概要情報の例としては、以下のようなものが考えられます

・〇〇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？

また、脆弱性概要情報を通知する際は、脆弱性関連情報の識別番号を記載します。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、そ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、その内容をもとに、自組織の開発製品のなか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された場合、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。

３．調査・検証：脆弱性詳細情報の取り扱いと製品の調査

■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全ての製品開発者は、脆弱性情報の公表時に製品開発者名と共にその対応状況が公表される場合があります。

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り扱いに際して

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策定するかどうかについて検討してください。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、以下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・検証時に以下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、情報の一般公表日までは第三者に漏えい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、他社・他組織のソフトウエア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の設定に際して

冒頭の「覚えて頂きたい事項」にて記述した通り、脆弱性情報には一般公表日が設定されます。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、一般公表日の決定の際には、JPCERT/CC が脆弱性関連情報の取扱いを開始した日時から起算して 45 日以内を目安とします。ただし公表日時は以下の点も考慮して検討し、場合により 45 日を超えることもあります。

●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係わるリスク

4-2. 公表日時の変更

決定された一般公表日に関して、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。JPCERT/CC では他の製品開発者との調整の上、公表日の変更を検討します。

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までに、脆弱性関連情報に係わる対応状況を JPCERT/CC に連絡すると共に、脆弱性関連情報に係わる対策情報を作成するよう努めてください。

4-4. 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コミュニケーションは、原則として全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。

4-5. 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。重要インフラ事業者には、情報通信、金融、航空、鉄道、電力、ガス、医療、水道、物流の各事業者が含まれます。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、この限りではありません。

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(ワークアラウンド)や修正方法(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、対策方法の作成と公表、情報の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、製品の利用者等に危険が及ぶ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)
http://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することが推奨されます。

独立行政法人情報処理推進機構（IPA）
「ソフトウェア製品開発者による脆弱性対策情報の公表マニュアル」
http://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。その際には以下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：6-3 を参照のこと)

6-3. JPCERT/CC における公表情報の作成と公表

JPCERT/CC は、事前に設定された一般公表日時に、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のは以下の情報が含まれます

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全ての製品開発者をリストとして公表します。この際、各製品開発者の状況を以下のような表現で記載します。

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
不明	脆弱性への対応状況の連絡がない場合

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は、次ページのようなイメージになります。

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へのリンクになる）

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	不明		
□□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 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。

株式会社〇〇 の脆弱性 JVN00XX-XXXY への対応

脆弱性識別番号
脆弱性タイトル
ステータス：該当製品あり

製品開発者からのコメント：
株式会社〇〇では本件に関して以下の URL にて情報を公開しています
http://marumaru.example.co.jp/vul/1234567/index.html

更新履歴
□年□月□日

6-4. 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、脆弱性情報一般公表日以降であっても、それを製品等の利用者に周知してください。

その他

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。

●情報漏洩の防止について

以下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

●関係組織への情報の取り扱いについて（情報の二次配布）

製品への脆弱性の影響調査等をおこなうにあたり、関係会社および外注先など（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。原則として脆弱性関連情報の開示は JPCERT/CC から直接、関係組織に対しておこないます。具体的には、以下の手順となります。

■以下、情報の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望む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だけを伝え、JPCERT/CC に直接連絡するように伝える

■以下、関係組織担当者と 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取る

●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 に連絡してください。

●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（マスコミなど）による情報のリークが発生した場合、一般公表の日時が早まる可能性があります。

●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わる問い合わせ先

有限責任中間法人 JPCERT コーディネーションセンター
E-Mail ： office@jpcert.or.jp
電話番号:03-3518-4600 (9:00-18:00)
FAX 番号:03-3518-4602

付録：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) ： http://www.jpcert.or.jp/

- 脆弱性情報コーディネーション概要

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

- JPCERT/CC 製品開発者リスト登録申請様式

  http://www.jpcert.or.jp/form/poc.txt

- Japan Vulnerability Notes (JVN)

  http://jvn.jp/

■ 経済産業省 ： http://www.meti.go.jp

- 脆弱性関連情報取扱体制

  http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html

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

- 情報セキュリティ：脆弱性対策

  http://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

  http://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

  http://www.ipa.go.jp/security/fy15/reports/vuln_law/index.html

- ソフトウェア製品開発者による脆弱性対策情報の公表マニュアル

  http://www.ipa.go.jp/security/ciadr/vuln_announce_manual.pdf

■ その他(日本語)

- 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

■ その他(英語)

- CERT Coordination Center (CERT/CC)

  http://www.cert.org/

- United States Computer Emergency Readiness Team(US-CERT)

  http://www.us-cert.gov/

- US-CERT Vulnerability Note Database

  http://www.kb.cert.org/vuls/

- Centre for the Protection of National infrastructure (CPNI)

  http://www.cpni.gov.uk/

更新履歴

2004-8-25	Ver1.0　初版
2004-10-13	Ver1.1　付録記載の URL 情報を更新
2008-4-21	Ver.2.0