製品開発ベンダー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

第1.0版

2004年12月

(社)日本パーソナルコンピュータソフトウェア協会
Japan Personal Computer Software Association

1. はじめに

セキュリティ上の「**脆弱性**」とは、**ソフトウェア製品**において、コンピュータ・ウイルスやコンピュータ不正アクセス等の攻撃により、その機能や性能を損なう原因となりうる安全性上の問題箇所である。ネットワーク攻撃に利用される可能性があるという点において、通常の不具合と区別される。

我が国においては、e-Japan戦略Ⅱの中で「安全・安心な利用環境の整備」を新しいIT社会基盤の整備に向けた重要課題の一つに揚げ、コンピュータやネットワークのセキュリティ向上に向けた総合的な取組みが進められている。こうした環境にあって、コンピュータ・ウイルスやコンピュータ不正アクセス等によって不特定多数の者に対して引き起こされる被害を予防し、もって高度情報通信ネットワークの安全性の確保に資するための施策の一つとして、経済産業省告示「ソフトウェア等**脆弱性関連情報**取扱基準」が2004年7月7日に公示され、翌日8日から施行された。この告示および、告示を受けて7月8日に発表された「**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」では、発見された脆弱性関連情報の国内における受付から公表までの体制と手順を定めるとともに、情報ネットワーク機器やソフトウェア・メーカ等の**製品開発ベンダー**に、**脆弱性情報**または脆弱性関連情報を受け取り、適切に管理するとともに自社製品に対する調査の実施や対策の作成を行い、調整されたタイミングで公表することを求めている。製品に含まれる脆弱性に対する迅速かつ適切な対応が、高度情報通信ネットワークの基盤製品を開発し提供する製品開発ベンダーの社会的な責務であると位置づけられるようになったのである。

本書は、情報システムを構成するソフトウェア製品の製品開発ベンダーが「情報セキュリティ早期警戒パートナーシップ」に賛同し、提供製品に係わる脆弱性への対応を率先かつ協調して進めるために必要な社内体制と業務手順を整備するためのガイドラインである。

以下の第2章では、上述の告示と同日付けの指定告示で脆弱性関連情報の**受付機関**として指定された **IPA** (独立行政法人情報処理推進機構)や、**調整機関**として指定された **JPCERT/CC** (有限責任中間法人JPCERTコーディネーションセンター)を含む、脆弱性関連情報に関する我が国の体制の全体像を述べる。第3章では、ベンダーにおいてまったく新たに脆弱性対応を始める場合に焦点を絞って、社内体制や手順を作るためのアプローチやJPCERT/CCへの登録手続き等を述べる。第4章では脆弱性対応のための社内体制の構築にあたってのガイドラインを、第5章では社内対応手順を定めるにあたってのガイドラインを述べる。

なお、本書で記述した内容は、社団法人日本パーソナルコンピュータソフトウェア協会(JPSA)会員企業の事業の実態を忖度し、それにできるだけマッチする形を意識して、基本的な取組の枠組みを記述している。その際、会員企業で参考になるような具体策や期待される対策に及ぶ記述に対しては、「望ましい」とか「考えられる」といった示唆的記述となるよう留意した。

会員企業が実際に体制を構築するに際しては、更に個別的に疑問や困難に直面することが想定される。そのような場合には、JPSA もしくは JPCERT/CC、IPA 等へ遠慮なく相談していただき、「情報セキュリティ早期警戒パートナーシップ」ならびに本ガイドラインの趣旨にそった体制を早期に構築されるよう期待したい。

本書の作成には、JPSA内に専任の研究会を組織し、会員企業十数社の代表を中心に外部権威者を招き、検討・執筆活動を行った。本書の執筆に際しては、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)共同チームによりまとめられ2004年10月に公表された同名のガイドライン「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」を参考にさせていただき、その記述に沿って編集させていただいた。研究会の活動をかくも効率的に遂行することができたのも、ひとえに同ガイドラインを検討のベースとして快く活用させていただいたことに負う所が大である。ここに両協会ならびに同ガイドライン作成に当られた方々のご努力に敬意を表すると共に、そのご好意に対して厚く感謝の意を表したい。

また、本書の文中において太文字で表記される単語の定義については巻末P33～34 <<<付録>>>用語集に記載がある。

本ガイドラインの前提となっている文書一覧を次に掲げ参考とする。

経済産業省 : 告示第235号「ソフトウェア等脆弱性関連情報取扱基準」、2004年7月7日、
http://www.meti.go.jp/policy/netsecurity/downloadfiles/vulhandlingG.pdf

経済産業省 : 告示第236号、2004年7月7日

独立行政法人 情報処理推進機構(IPA)
有限責任中間法人 JPCERT コーディネーションセンター(JPCERT/CC)
社団法人 電子情報技術産業協会(JEITA)
社団法人 日本パーソナルコンピュータソフトウェア協会(JPSA)、
社団法人 情報サービス産業協会(JISA)、
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(JNSA)

- : 「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」、2004年7月8日
http://www.ipa.go.jp/security/ciadr/partnership_guide.pdf

JPCERT/CC : 脆弱性関連情報取扱ガイドライン、2004年8月25日、
http://www.jpcert.or.jp/vh/guideline.pdf

2. 国内の脆弱性関連情報取扱体制と製品開発ベンダーの責務

ソフトウェア等の脆弱性は、ソフトウェアの設計･開発段階に内包される潜在的な問題であり、近年、コンピュータ不正アクセスやコンピュータ･ウイルス等の攻撃に悪用されるケースが増加している。脆弱性をめぐる情報には次のような種類がある。脆弱性関連情報は、脆弱性そのものについての情報や、脆弱性を悪用した**攻撃方法**、あるいは脆弱性の**検証方法**についての情報である。**対策方法**は、脆弱性によって生じる被害を回避するための**回避方法**、または、脆弱性を取り除くための**修正方法**に関する情報であり、通常は製品開発ベンダーが作成する。**対応状況**は、製品開発ベンダーの声明として作成される、調査や対策状況の提供状況についての情報である。

本来、関係者内で適切に共有され対策が策定されるべき脆弱性の情報が、適切に扱われずに放置されたり、対策がない段階で暴露されることにより、大きな被害をもたらす危険性がある。**米国CERT/CC** で扱っている脆弱性関連情報の件数は、2002年に4,000件を超えた。脆弱性の発見からそれを悪用した攻撃コード(ワームなど)が出現して被害を及ぼすまでの時間が著しく短くなってきており、いかに迅速に脆弱性を除去するかが喫緊の課題となっている。しかも、脆弱性関連情報が発見された場合、その影響が大きいと判断される製品を開発している製品開発ベンダーは、国境を越えて存在している。

このため、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、各国**CSIRT** (Computer Security Incident Response Team) が調整機関となり、公表までの調整を行う協力関係が国際的に構築されつつある。発見された脆弱性が複数の製品に関係する場合、関係者間で足並みを揃えることが重要である。関係者間で調整された公表日を待たずに、単独で情報を公表することは、他の製品利用者を危険にさらす可能性があり、その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、日本全体として公表前の脆弱性関連情報を受けることができなくなる最悪のケースも考えられる。

我が国においては、脆弱性への対応の全体的な枠組みが存在しなかったため、脆弱性の公表に関する調整が不十分であるとともに、ソフトウェア等の脆弱性に関する発見･分析･対策策定を海外に依存しており、また、日本市場に固有のソフトウェアに関しては脆弱性の届出とフォローアップ体制が皆無に等しかったことが問題であった。この問題に対し政府の「情報セキュリティ総合戦略」（2003年10月発表）の提言に沿って、2004年7月に経済産業省から「ソフトウェア等脆弱性関連情報取扱基準」が告示され、また関係団体連名による「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」が発表され、脆弱性への業界の取り組みをより円滑かつ効果的に進めるための脆弱性関連情報取扱体制が構築されるに至った。

IPAおよびJPCERT/CCが、それぞれ受付機関および調整機関として、この脆弱性関連情報取扱体制の基盤部分を提供している。この枠組みの中で、製品開発ベンダーはJPCERT/CCと調整連携しながら、脆弱性関連情報を適切に取り扱いつつ、対策に係る方針を策定し、この方針に従って対策方法を策定し公表する。IPAは、コンピュータ･ウイルス、コンピュータ不正アクセスの受付機関として実績を有しており、本脆弱性関連情報取扱体制においても受付機関の役割を担う。また、IPAは脆弱性分析の機能を備え、届出のあった脆弱性関連情報について再現性の確認･調査等を行い、結果をJPCERT/CCおよびJPCERT/CCを介して製品開発ベンダーに提供する。その脆弱性関連情報が、国民の日常生活に必要不可欠なサービスを提供するための基盤となる設備に重大な影響を与えるおそれがある場合には、IPAは調整機関および当該製品開発ベンダーと協議の上、政府機関等に脆弱性および対策方法をあらかじめ通知する。

JPCERT/CCは、米国**CERT/CC**、英国**NISCC** それぞれとパートナーシップを締結し、日本国内の製品開発ベンダーが公表前の脆弱性関連情報を入手し、対応できるように調整の実績を有しており、脆弱性関連情報取扱体制において調整機関の役割を担う。

脆弱性関連情報の取り扱いの概要は次の通りである。

（1）製品の脆弱性に関する**発見者**からの届出受付は IPA が行う。IPA は届出情報の一次受付と再現性検証・調査、統計データ化などを行い、調整機関（JPCERT/CC）へ通知する。

（2）JPCERT/CC は、IPA や海外のセキュリティ対応組織（CSIRT）から受けた脆弱性関連情報を、関係すると考えられる製品開発ベンダーに通知し、脆弱性情報の公表スケジュールなどを調整する機能を担う。海外に影響を与えることが予想される場合には、海外 CSIRT へ連絡を行う。

（3）IPA と JPCERT/CC は、製品開発ベンダーの脆弱性対応状況と策定した**対策情報**の公表を共同して行う。IPA は定期的に脆弱性関連情報の届出状況などを公表する。

国内の脆弱性関連情報取扱体制を図2-1、役割分担を表2-1、関係者間の脆弱性関連情報交換プロセスを図2-2に示す。

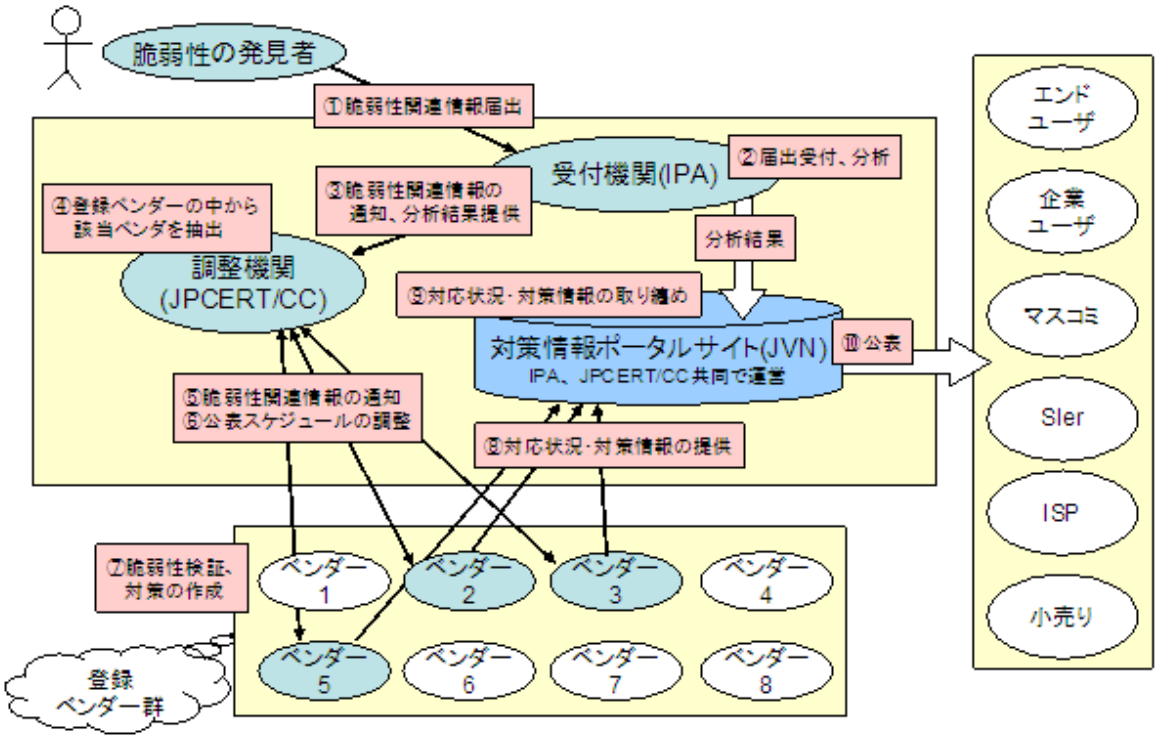

図 2-1 国内の脆弱性関連情報取扱体制

表2-1 国内のソフトウェア等の脆弱性関連情報取扱役割分担

対象	発見者からの届出	海外CSIRTからの連絡
受付	●IPA ･一次受付 ･スクリーニング、受理／不受理通知 ･JPCERT/CCへの通知 ･統計情報集計	
調整	●JPCERT/CC ･連絡すべき製品開発ベンダーの特定、連絡 ･脆弱性情報、対応状況の公表日の調整とスケジュール管理 ･IPAの分析結果を当該製品開発ベンダーに提供 ･海外に影響を与えることが予想される場合には、海外CSIRTに連絡 ●当該製品開発ベンダー ･脆弱性情報の公表日に関しJPCERT/CCと相談	●JPCERT/CC ･海外CSIRTから脆弱性関連情報受信 ･連絡すべき製品開発ベンダーの特定、連絡 ･脆弱性情報公表スケジュールの管理 ･IPAの分析結果を当該製品開発ベンダーに提供 ･影響有無等を情報管理元CSIRTへ報告
検証・対策作成	●当該製品開発ベンダー ･製品への影響調査、脆弱性検証を行い、結果を報告 ･対策（ワークアラウンド、パッチ、ver-up等）を作成 ●IPA ･脆弱性分析（再現性検証、影響範囲の分析、リスク分析、脆弱性検証ツールの作成等）	
公表	●当該製品開発ベンダー ･脆弱性情報の公表日までに対応状況を連絡 ･対策を作成した場合、利用者に周知 ●IPA、JPCERT/CC ･製品開発ベンダーの脆弱性検証結果と対応状況を公表し、DB登録 ･IPAが統計情報の集計と公表	●当該製品開発ベンダー ･脆弱性情報の公表日までに対応状況を連絡 ･対策を作成した場合、利用者に周知 ●IPA、JPCERT/CC ･製品開発ベンダーの脆弱性検証結果と対応状況を公表し、DB登録 ･JPCERT/CCが海外CSIRTへ対応状況を送付
情報利用	●製品開発ベンダー ･JPCERT/CCから脆弱性関連情報の提供を受け、自社製品への影響調査、脆弱性検証を行い、結果を報告 ･機密保持が前提 ●政府機関等 ･IPAから公表前の対策方法や準備要請情報の提供を受けて対処 ●システム構築者/運営者/ISP(Telecom-ISAC Japan) ･公表後の対策方法を受けてユーザーに対策実施 ･JNSA等の活動と連携 ･IPA、JPCERT/CC共同運営の公表情報を活用	

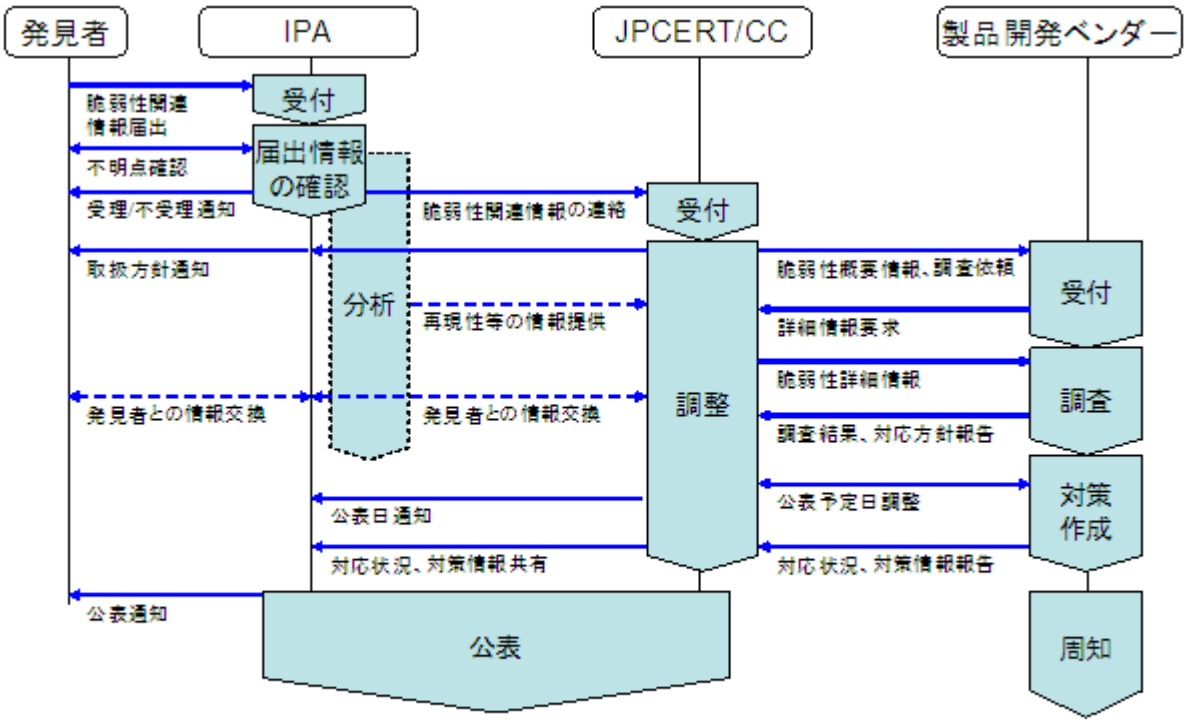

図2-2 関係者間の脆弱性関連情報交換プロセス

この枠組みにおける製品開発ベンダーに求められる事項を以下に列挙する。

- 調整機関と連絡をとるための窓口を設置し、調整機関に通知する。
- 調整機関から通知された脆弱性関連情報に関して、脆弱性検証を行い、その結果を調整機関に報告する。
- 通知された脆弱性が他社のソフトウェア製品に含まれることが推定される場合には、そのことを調整機関に報告する。
- 脆弱性情報公表日までの間、この脆弱性関連情報を第三者に漏洩しないよう適切に管理する。
- 脆弱性関連情報公表日までに、対応状況を受付機関および調整機関に報告するとともに、対策方法を作成するよう努める。
- 対策方法を作成した場合、受付機関および調整機関に報告し、脆弱性情報の公表日以降、自らもそれを利用者に周知する。
- 自ら開発等を行ったソフトウェア製品に影響が限られる脆弱性関連情報を発見または取得した場合は、対策方法を作成し、この脆弱性関連情報および対策方法を受付機関および調整機関に通知する。
- 影響範囲が自社のソフトウェア製品に限らない脆弱性関連情報を発見若しくは取得した場合、受付機関に届出る。

この枠組みは法律の後ろ盾のない官庁告示に基づいているため、製品開発ベンダーにとっては、法的な強制力をともなった義務ではなく、この枠組みに参加することにより何らかの免責や法的な保護が得られるわけでもない。しかし、製品の脆弱性に対する迅速な対応により、自社製品の脆弱性がネットワーク社会全体と顧客に及ぼすリスクを軽減し、顧客に安心を与えることで自社製品への満足度を高めるために活用する枠組みと考えるべきである。

なお、IPA報告書「情報システム等の脆弱性情報の取り扱いにおける法律面の調査」(http://www.ipa.go.jp/security/fy15/reports/vuln_law/documents/vuln_law_2004.pdf；2004年6月)にまとめられた法律専門家による検討報告も参考にしてほしい。

3. 脆弱性関連情報取扱体制の立ち上げ

本章では、製品開発ベンダーが新たに「情報セキュリティ早期警戒パートナーシップ」に参加する場合に必要となる社内体制の立ち上げの要点について述べる。

3.1 全社的な体制づくり

「情報セキュリティ早期警戒パートナーシップ」への参加は自社製品の脆弱性への対応を社会的な責務として迅速且つ適切に遂行することを内外に宣言することになるので、体制づくりにはすべての主要な関係者の理解と賛同を得ておく必要がある。

脆弱性への対応はその性質上、非定常な業務遂行を余儀なくされるので、迅速な対応を全社で足並みを揃えて遂行する体制が必要となる。また、脆弱性関連情報は漏洩して悪用されれば情報ネットワーク社会を危機に陥れかねないので、機密性を厳に保持できるような枠組み作りが重要である。さらに、出荷されて顧客の下で稼動中の製品に対する対策実施を考えると、調査や対策の作成にあたる開発部門はもとより、**顧客窓口部門**など複数組織にわたる調整や協力も必要である。

⑴ 経営層から責任を持つ者の了解を取り付ける

脆弱性への対応に関して、企業としての最終的な判断や意思決定を行う権限を持つ責任者を定める。この責任者は取締役等経営責任をとれるレベルから選任することが望ましい。この責任者から、脆弱性対応に関するベンダーとしての社会的な責務や社内での取扱体制と手順について理解と了解を取り付けておくことが重要である。

⑵ 対象となる製品とその責任部署を確認する

脆弱性対応の対象となる汎用性を有する製品を確認し、各対象製品について、脆弱性調査や対策の作成の責任を負っている部門と担当者を明確にする。脆弱性関連情報の流通は、漏洩の可能性をできるだけ減らすために、対象製品を持つ部門や担当者に止める必要がある。

なお、対象製品の開発に密接に関係する**関連会社**等がある場合は、調整機関であるJPCERT/CCに関連会社等の名称を通知して、それらを自社の体制に含めることができる。

(3**)ベンダーCSIRT**を決めてJPCERT/CCに登録する

ベンダーCSIRT (シーサート : Computer Security Incident Response Team) は、脆弱性対応において中心的な役割を担う組織である。

JPCERT/CCなど社外の機関や個人に対しては、製品開発ベンダーを代表して脆弱性関連情報をやり取りする窓口 (**POC** : Point of Contact と呼ばれる) として機能し、社内に対しては、脆弱性関連情報への対応活動に関する司令塔として、個々の脆弱性について情報を分析し、大枠としての対応方針を決め、関連部門への展開と集約をはかる組織である。

ベンダーCSIRTのメンバーには、情報ネットワーク・セキュリティに関するの技術的な知識と、全社横断的な製品ラインアップの理解が求められる。ベンダーCSIRTの立ち上げは、セキュリティの専門家が集まった部門を母体として設置するアプローチ、または横断的な品質管理関連の部門を母体として設置するアプローチのいずれかが一般的である。

前者のアプローチをとった場合には、個々の製品開発部門での対応活動推進のために品質担当部門などが既に持っている仕組みの利用を検討するのが賢明である。

対象製品の種類が限られている場合には、ベンダーCSIRTは兼務者による運用や、複数部門にまたがった仮想組織として設置するアプローチも可能である。

⑷ 脆弱性関連情報が漏洩しないような施策 (体制、仕組み、ルール) 作り

脆弱性関連情報の機密保持のための体制とポリシーを定め、社内の関係者に通知する。脆弱性関連情報は漏洩の可能性をできるだけ減らすために、流通範囲を調査や対策の作成に必要十分な部門に止めなければならない。また、社内の関連部門で安全に脆弱性関連情報を共有するために、アクセス認証機能付きの情報データベースなど、必要なリソースを確保する必要がある。

3.2 製品開発部門の体制確立と対応ルール作り

個々の製品に関する脆弱性の有無や影響の度合いの調査、対策の作成といった実作業は、個々の製品の開発担当部門毎に業務プロセスの一環として組み込むことが望ましい。しかも、脆弱性関連情報は社外から突発的に入ってくるため、通常業務との優先度調整で判断に迷うこともありうる。あらかじめ各製品開発部門では次のような準備を整えておく必要がある。

①全社のポリシーや方針に整合し、かつ開発製品の市場を勘案して、部門としての脆弱性への対応方針を決める。その中では、脆弱性を一般の不具合と同列に扱うのか、最優先課題として対応するのか、報告のマイルストーンなどを明らかにしておく必要がある。

②製品開発部門としての責任者を定め、ベンダーCSIRTとの情報流通経路を確立する。

③部門が保守対象品として保有している製品及びそのバージョンのリストを作成する。

④調査結果と対策(暫定回避策やパッチや改版を含む)方針がまとまった後における、通知・公表や顧客サポートのための手順と体制を定めておく。

⑤社外から導入した製品・技術等についても、脆弱性に係わる調査が必要になる場合に備えて、問い合わせの手順を確認しておくことが望ましい。また、ライセンス契約の際には、脆弱性への対応を明文化して盛り込んでおくことが望ましい。

3.3 その他の部門の体制確立と対応ルール作り

ベンダーCSIRTや開発担当部門の他に、円滑で一貫した脆弱性への対応を実現するために、次のような関連部門の積極的な関与や協力のための枠組みも順次整備することが望ましい。

(1) 企業ウェブ・サイトの運用部門

特に量販されるインターネット関連製品の場合には、脆弱性情報等の通知手段として企業ウェブ・サイトからの情報発信が重要であるので、企業ウェブ・サイト運用部門の了解を得て、ウェブ・サイト上における脆弱性情報の提供方法や掲載手順を定める。

(2) 顧客窓口部門

脆弱性情報等が公表された後における、顧客からの問い合わせに対して、適切な回答ができるよう、営業窓口やコールセンターなどの顧客窓口部門の協力を得て対応ルールを作る。

(3) 広報部門

脆弱性情報等が公表された後、マスコミからの問い合わせやコメントを求められる場合があるので、タイムリーに適切な回答ができるよう、広報部門との連携をはかる枠組みを作る。

4. 脆弱性関連情報取扱体制の整備

脆弱性関連情報を社外から受け付け、製品の脆弱性問題を調査し、顧客へ対策情報を展開する一連の作業を適切且つ迅速に遂行するためには、脆弱性関連情報の流通を統制しながら、社内外の関連部署が協調し問題解決に当たる新たな社内体制が必要となる。

社内体制は最初から新たな組織体系を作っても良いが、最小限の機能を持つ「ベンダーCSIRT」を立ち上げ、既存の社内組織の枠組みを利用した連携体制を作り、対象範囲や規模の拡大に伴って、独立した組織を検討していく方が賢明である。

連携に必要と思われる組織機能には以下のものがあり、企業の規模や形態によって、同一の組織が複数の機能を担っていることもある。

①ベンダーCSIRT	脆弱性対応全般の推進･集約を担う司令塔および対外窓口
②推進･管理組織	脆弱性対応の推進･管理･統制（一般的には品質管理部門が向いている）
③製品開発部門	脆弱性問題の調査･対策
④顧客窓口部門	顧客への対応状況の通知、問い合わせ受け付け
⑤広報部門	社外への脆弱性対応状況の周知･公表

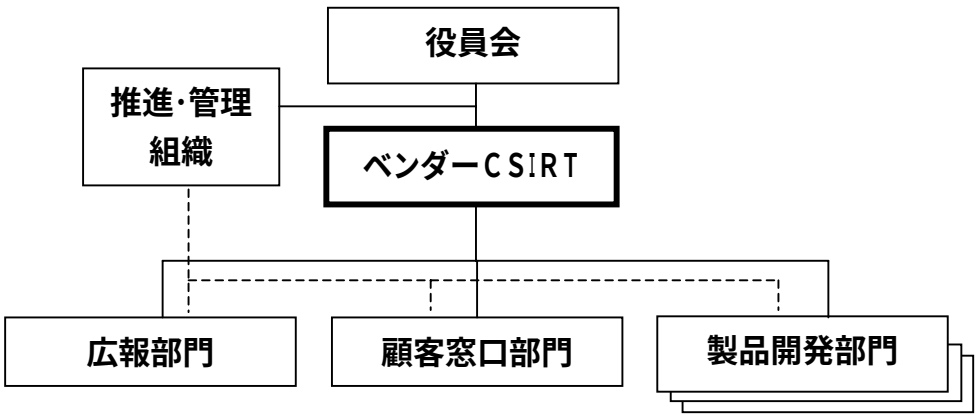

図4-1脆弱性対応のための社内体制(例)

4.1 ベンダーCSIRT

ベンダーCSIRTは、脆弱性対応において中心的な役割を担う必須組織である。社外に対してはJPCERT/CCなどの機関や個人に対して製品開発ベンダーを代表して脆弱性関連情報をやり取りする窓口 (POC) として機能し、社内に対しては、脆弱性関連情報への対応活動に関する司令塔として、個々の脆弱性について情報を分析し、大枠としての対応方針を決め、関連部門への展開と集約をはかる。また、社内外に対して脆弱性関連情報の流通に関するコントロールを行う。

具体的には、次のようなアクションアイテムを実施する責任を負うことになる。

① 大枠としての対応方針に従いスケジュールを決めて対策計画を立案する。
② 対策計画に基づき期日を決めて製品開発部門に影響調査を実施させる。
③ 対策計画に基づき期日を決めて製品開発部門に対処（パッチ作成など）させる。
④ 公表に向けて公表記事(**ベンダー声明**等：5.4参照)を作成させ、内容の確認を行う。
⑤ 公表後の顧客対応方針を明確にさせる。
⑥ 情報の公表後のフォロー活動として、適宜顧客への対応状況の確認を行う。

4.1.1　ベンダーCSIRTの位置づけの明確化と周知

ベンダーCSIRTが全社を代表する脆弱性関連情報取扱組織として機能するために、組織の役割と業務内容を明らかにして、関連部門の協力を取り付けて、組織としての認知度を高める必要がある。

一般に、社外から通知・通報を受ける窓口は、広報部門、コールセンター部門、営業部門等、多数考えられる。個々の製品ごとに窓口が異なることもあり、製品毎、部署毎にバラバラの対応となってしまう可能性がある。また、異なった製品分野の複数の事業部門が存在する場合や、関連会社を束ねているような会社の場合には、個々の製品の情報をどこの事業所、関連会社、窓口へ通知するべきか判り難いことが多い。そこで、全社を代表する統一的な窓口を設置する必要がある。

こうした状況を踏まえ、ベンダーCSIRTを全社体制として定着させるには下記の手順に従うとよい。

①組織形態の如何にかかわらず、ベンダーCSIRTを組織として認知させ、その機能と役割を認識させる。

②会社の窓口部門（広報部門、コールセンター部門、営業部門 等）に製品の脆弱性に関する情報を受け付けた場合にはベンダーCSIRTへ通報するように周知する。

③製品の脆弱性関連情報の調整機関との対応は、セキュリティ問題や脆弱性に関する知識を持ったベンダーCSIRTが行うことを周知徹底する。

④複数事業部門や関連会社がある場合には、各事業部門または関連会社に事業部門CSIRTや代表者を設置し、ベンダーCSIRTとの情報交換を行い、各事業部門や関連会社等の個々の窓口で受け付けた製品の脆弱性関連情報もベンダーCSIRTと情報共有できる仕組みを作る。

4.1.2　ベンダーCSIRTに必要な人材

通報される製品の脆弱性関連情報は、プロトコルや特定の機能・実装に関わるもの、システム設定や特殊条件によるもの等、多岐に渡り、幅広い知識を必要とする。内容によっては、問題に至るメカニズムや問題個所の特定等を調整機関または発見者と協力して行なわなければならないこともあり、問題内容の共有や問題解明へ導くための調整機関との対話も、ベンダーCSIRTが行うことが必要となる。

また、セキュリティ問題は様々な利用環境・利用形態で発生する可能性があり、その脅威度合や緊急性も様々であり、更には、影響の及ぶ範囲が複数の製品・部門にまたがる可能性がある。このような状況の中で調査を円滑かつ洩れなく進めるために、脆弱性とその脅威の度合ならびに影響の及ぶ範囲とその度合を調査するための調査方法、確認手段、解説等を、調整機関等から可能な範囲で入手・作成して、製品開発部門へ渡すことが望ましい。

脆弱性のメカニズムや実装が自社製品に含まれているか、実際に影響があるかを判断するために、自社の製品全てを対象として、すべての製品開発部門に調査を行わせた場合、膨大な時間と労力を要してしまう。この労力を減らすには、製品の構造や実装を理解している専門家による調査対象製品の選定が必要である。

上記の対応を行うためには、ベンダーCSIRTには下記のメンバーが参画することが必要となる。

①情報を分析し、脅威の影響度合いや調査方法をまとめるセキュリティ専門家
製品開発部門の専門家との兼任でもよいが、調整機関との対話が必要な場合があるので、ネットワークの脅威と脆弱性に関するセキュリティ知識を有していることが求められる。

②分析結果や調査方法に基づいて、影響の可能性がある製品を特定する製品開発部門の専門家
すべての製品を熟知した専門家がいるケースは少ないので、製品分野毎に代表者を決め、その代表者が担当範囲内の製品を取りまとめる形態が一般的である。会社の規模によっては、部門毎の協力者を配置して、チームを構成する形態もある。

③ベンダーCSIRT活動をフォローアップし、適宜報告を行う品質保証部門
通知された問題への対応が行われていることを監視し、その重要度や影響度合いに応じて、製品開発部門等対策立案に携わる部門への督励、経営幹部への報告やリスク管理部門への通知を行う。

4.1.3 調整機関であるJPCERT/CCとの連携と登録

ベンダーCSIRTは、調整機関であるJPCERT/CCとの間で脆弱性関連情報に関する相互の連絡を行う必要がある。そのための窓口(POC)を設置し、事前にJPCERT/CCへ届け出て登録しておく。さらに、脆弱性関連情報を適切に管理するために、JPCERT/CCが定める規約 (JPCERT/CC **製品開発者**リスト登録規約) に則って、情報を適切に管理することが求められる。

⑴ JPCERT/CCとの連絡

POCは、JPCERT/CCのカウンターパートとして、以下の役割を担う。なお、JPCERT/CCが公表している「JPCERT/CC脆弱性関連情報取扱ガイドライン」も合わせて参照すること。

①窓口情報の登録・更新
- 窓口情報の管理、更新
- JPCERT/CCが提示する、テクノロジ・キーワード・リストの該当項目の更新

②脆弱性関連情報に関するJPCERT/CCからの連絡
- JPCERT/CCからの脆弱性関連情報の受け取り
- 脆弱性関連情報のアップデート(公表日時の変更など)
- その他、JPCERT/CCからの連絡

③JPCERT/CCへの連絡
- 脆弱性に該当する製品の有無
- 社内の全体的なスケジュール
  (調査開始から、対策情報の作成、公表情報の作成まで)
- 公表情報の内容

④脆弱性への対応方針等の協議
- 第三者への情報転送に関する協議
- 対応方針に関する協議
- 公表の方法に関する協議
- その他、相互に必要と認める協議(発見者へ開示する情報に関する協議など)

⑤定例会への参加
- JPCERT/CCが開催する定例会への参加

⑵ POCの設置とその要求条件

JPCERT/CCからの脆弱性関連情報の通知を受け、また関連する情報の授受を行うために、専用のPOCを設置する。POCは以下の条件を満たす必要がある。

①常設とする。ベンダーCSIRTの機能そのものは脆弱性関連情報を受け取る都度編成する方法も考えられるが、窓口機能は常に設置する。

②電子メールは24時間・週7日受信可能とする。電子メールやFAXが受信可能であれば、夜間や休日には常に人員を配置する必要は無い。JPCERT/CCからの一次連絡は原則として電子メールによって行われるが、営業時間帯には電話などにより連絡が入る場合がある。

③脆弱性関連情報の通知を受信した場合、可能な限り速やかに応答できる体制とする。遅くとも翌営業日中には応答できるようにするのが望ましい。

応対する担当者は、以下のような人物を想定する。

- 脆弱性関連情報について技術用語を理解することが可能な者
- 脆弱性関連情報の機密性について理解し、取り扱いに十分な注意が払える者
- 自社製品について速やかに対応状況が把握できる者

すなわち、受付のためのオペレータではなく、脆弱性関連情報に対して責任を持って取り扱うことが可能な者をPOC担当者とする。

④公表直前には相互に連絡する場合があることを考慮した体制とする。場合によっては、休日の連絡が必要になることがある。

⑶ POCの登録と登録情報の更新

POCの準備が完了した後、速やかにJPCERT/CCへ届け出る。POCの届出を受けたJPCERT/CCでは、POCを登録し、第三者に漏洩しないように適切に管理する。届け出る項目はJPCERT/CCが定める。

電子メール等を用いる場合の暗号については、原則としてJPCERT/CCが定める方法を用いる。また、本人確認についても、JPCERT/CCが定める方法を用いる。

POCの登録情報を更新する場合は、JPCERT/CCが指定するフォーマットによって更新後の情報を記述し、JPCERT/CCに通告する。担当者の変更を行う場合は、原則として更新前の担当者から連絡を行う。

登録変更の確認のため、JPCERT/CCから電話による確認が行われる場合がある。JPCERT/CCが交代の真偽について確認できた時点で、登録情報の更新が行われる。

⑷ JPCERT/CC 製品開発者リスト登録規約への同意

「情報セキュリティ早期警戒パートナーシップ」の主な目的は、脆弱性関連情報の不用意な流通の制限と、公表のタイミングをそろえることにある。そのため、JPCERT/CCでは、「製品開発者リスト登録規約」を定めている。

①規約の目的

規約は、製品開発ベンダーとJPCERT/CCとの間で脆弱性関連情報を適切に管理するために定める。

②規約の内容

規約はJPCERT/CCが提示し、個々の製品開発ベンダーが同意する。JPCERT/CCは調整等を目的として様々な製品開発ベンダーと情報を交換するため、規約には秘密保持に関する項目を含む。調整機関と製品開発ベンダーとの間で協議の上、第三者に最低限の情報を開示できる内容になっている。また、JPCERT/CCが製品開発ベンダーに対して情報の提供を強制するものではない。したがって、製品開発ベンダーが不利益を被るような情報を提供することを求めることはなく、提供した情報を相互に適切に扱うための規約である。

製品開発ベンダー各社は、JPCERT/CCが提示する規約に同意し、脆弱性の発生に際しては相互に協議の上、個々の脆弱性関連情報の取り扱いを決める必要がある。

4.1.4 ベンダーCSIRTの運営

ベンダーCSIRTの活動は非定期であるため、受付がいつでも可能であり、構成メンバーが特定されていれば、必要に応じて、問題発生時・情報受付時にのみ速やかに編成される形態でも良い。しかし、脆弱性問題の通知や対応要請がいつ発生するかは予測できず、また緊急の対応が求められる場合もあるため、ベンダーCSIRTは、少なくとも電子メールに関しては、24時間・週7日、受付が可能であることが求められる。

4.1.5　情報共有の枠組み

製品の脆弱性関連情報は、その対応が決まっていない（対策の提供や公表が行われていない）段階で、社内・顧客を含む第三者へ情報を流通させてはならない。すなわち、社内の者であっても、限定した最小限の関係者にのみ情報を提供しなければならない。情報が漏洩してしまった場合、その脆弱性関連情報を悪用した攻撃、妨害等が発生する可能性があり、顧客でのセキュリティ侵害へ繋がる恐れがある。また脆弱性関連情報には、特定のプロトコルや実装を行っている製品の多くで発生する問題も数多く含まれており、自社製品だけでなく他社製品への影響も想定され、漏洩による影響は計り知れない。

しかし、その一方で製品の調査・対策のためには、多くの製品の開発担当者、関連会社員や協力会社員まで情報を流通させる必要があり、情報の共有と漏洩防止・流通管理の両方を満たす必要がある。

情報を管理しつつ流通させていくために、あらかじめ会社としての下記のような枠組みを作成しておくことが必要である。

①脆弱性関連情報の流通・参照に関する管理規則を作成し、情報参照の必要性がある関係者すべてに周知徹底する。
②参照および利用時のアクセスコントロールを行う。
③情報のコピー、転送、抜き取り、印刷等を制限する。
④漏洩元を特定する仕掛け、監査による管理状況把握の仕組みを作る。

これらの措置を実現するためには一般に、認証、アクセス制限、暗号、改ざん防止、ログの作成と管理等の手段を組み合わせて適宜配置することが有効である。

また、社員や派遣社員、関係会社や協力会社等において脆弱性関連情報に直接触れる立場の者に対しては、次のような点も考慮しておくことが望ましい。

①雇用契約、就業規則、派遣契約、関係会社や協力会社との業務委託契約や請負契約が守秘義務や情報流通に関するコントロールの規定を盛り込んでいるかを見直し、確認する。
②関係会社、協力会社に対して、事前に情報セキュリティ早期警戒パートナーシップへの参画を促すとともに、本ガイドラインの遵守を求め、JPCERT/CC の定める「製品開発者リスト登録規約」の理解を徹底しておく。

4.1.6　ベンダー間協調

通報された脆弱性によっては、自社製品だけでなく、他社製品への影響が想定・確認される場合がある。こうした場合には調整機関に対して、その影響の及ぶ範囲と内容を報告する。

また、複数の会社の製品に影響がある場合には、調整機関等により公表時期の調整が行われることがあるため、自社の対応状況との調整や、顧客への対応開始時期や公表日時の社内調整を行うことが必要となる。自社での対策が完成したからといって、顧客への対応や対策の流通を勝手に行ってはならない。

4.1.7　発見者とのコミュニケーションにおける留意事項

情報セキュリティ早期警戒パートナーシップの枠組みにおいては、脆弱性の発見者は受付期間に届け出、製品開発ベンダーとの連絡調整は調整機関が行うことを想定し、枠組みの原則としている。しかしながら、まれに発見者が直接製品開発ベンダーにそのベンダーの製品の脆弱性情報を通報してくることがありうる。

そのような場合にも、発見者・通報者の個人情報の取り扱い、他ベンダーとの関係、脆弱性情報のユーザーへの流通、場合によっては海外とのコーディネーション等、専門機関に扱いを委ねるべき要素が

多いので、必ず調整機関への通知を行うものとする。この場合、通報者にその旨を説明して理解してもらうこと、その後の調整は原則として受付機関を通じて行うことも了解してもらうことが肝要である。

万が一、発見者・通報者がベンダーとの直接のコミュニケーションを要求する場合には、調整機関との連携とアドバイスを確保しつつ、以下のような点に留意して良好なコミュニケーションを維持するよう注意が必要となる。

①通知を受けた旨を返答する。
②調査状況や対応方針等を適宜報告する。
③セキュリティ問題として扱わない場合には、発見者の理解を得られる形での対応方針を説明する。
④状況の変化により対応方針や時期が変更になる場合も、報告を行う。
⑤対応が完了し、顧客への通知、対策提供が行われる場合には、その内容と謝辞を報告する。

4.2 全社的な推進・管理組織

推進・管理組織は脆弱性対応に関する全社的司令塔であるベンダーCSIRTを社内的にサポートし、製品開発部門、顧客窓口部門、広報部門等を連携させてベンダーCSIRTの指令が徹底するよう調整と推進を行う。推進のための機能としては、取り扱い手続きを提示し、ベンダーCSIRT体制に関する意思決定を行い、対応状況を監視し、必要に応じて脆弱性に関する技術を育成する役割を担う。

脆弱性対応の推進・管理は製品の品質問題への対応と類似するので、社内の品質管理部門に新しいミッションを持たせることで実現することができる。また、ベンダーCSIRTが自分でこの機能を担ってもよい。

推進・管理機能を担う体制の在り方には、会社によりバリエーションがあるが、本書では、便宜上「推進・管理組織」と表記する。

4.2.1 全社的な体制の構築と維持

全社的な体制を構築するにはトップダウン方式で、以下のような手順で実施すると良い。

①最初にベンダーCSIRT体制とそこへの権限委譲について、経営責任を持つ者の了解と決定を取り付ける。これは必須項目である。
②各役割組織の代表者を集め、全社を通した対応手順を決める。その時に、草の根的に先行活動してきた部門の意見を聞く事が、後の活動をやりやすくする。
③全社を通した対応手順で、脆弱性対応ができる事を確認して、ルール化する。
ルールの中には、作業の優先度を明確にしておく事が重要である。また、脆弱性関連情報の漏洩防止のルールも必要である。
④各関連部門の責任者を決めて、ルールに従って活動する。

また、この体制を運用・維持して行くには、以下の事項も考慮する必要がある

- 情報入手～影響調査～対応決定～対処～公表～顧客対応までの一連の流れを、監視・督促する。
- 対応決定のために、責任者と判断基準を明確化する。また適宜見直しを行う。
- 経営責任を持つ者への報告・承認ルートを確立しておく。
- ルールの説明、脆弱性による影響、脆弱性と対策方法の説明などのために、教育機能を用意・整備する。

4.2.2 対応推進のための権限

脆弱性への対応は、情報入手～影響調査～対応決定～対処～公表～顧客対応までの一連の流れである。そのため推進・管理組織には、ベンダーCSIRTが社内で活動するに際して、関連部門に対しその指示に従わせる指令を、側面から発せられる権限が必要である。

4.2.3　教育･育成

脆弱性への対応は、素早くかつ機密情報管理下で行わなければならず、ルールを決めただけではうまく行かない。関係者に手順／ルールを説明し、脆弱性に関する対応に必要な技術を教育することが必要である。

対応に必要な技術はセキュアなソフトウェア製品を開発するための技術との共通点があるため、IPAのセキュリティセンター(http://www.ipa.go.jp/security/index.html)に掲載されている教材やスキルマップなどを参考にするとよい。

4.3　製品開発部門

製品開発部門は、実際に脆弱性に対応する部門である。

4.3.1　製品開発部門の定義

製品開発部門は、実際にソフトウェア製品を開発しているか、他社から提供されたソフトウェア製品またはソフトウェア部品を自社製品、または自社製品の一部として提供している部門である。

4.3.2　製品開発部門の役割

製品開発部門は以下の役割を担う。

①脆弱性対応の対象となる自部門の製品を確認し、ベンダーCSIRTに通知する。

②ベンダーCSIRTを経由して入手した脆弱性関連情報に対し、自部門の対象製品が影響を受けるか否か調査し、結果をベンダーCSIRTに報告する。

③脆弱性に影響される時は、回避方法、修正方法を検討し、ベンダーCSIRTに回避方法と修正のスケジュールを提示する。スケジュールの作成に当っては、必要に応じベンダーCSIRTを通じて品質担当、顧客窓口部門、広報部門とも協議する。

④スケジュールに従って修正を作成し、ベンダーCSIRTに通知する。必要に応じ品質担当、顧客窓口部門、広報部門にもベンダーCSIRTを通じて通知する。

⑤上記③④の活動に対する問い合わせ対応を行う。

⑥顧客などから単なる不具合として報告された問題事項についても、脆弱性に関する問題が含まれている場合もあるため、脆弱性関連情報としての取り扱い手順に乗せるためのレビューの機会を業務手順の中に組み込んでおくことも必要である。

4.3.3　製品開発部門内の体制

製品開発部門内には以下の担当者が必要である。なお、すべての担当者に対し、公表前の脆弱性関連情報については守秘義務があるので、情報管理方法を確認しておく必要がある。

⑴ 製品開発部門のとりまとめ責任者

製品開発部門のとりまとめ責任者は、ベンダーCSIRTが顧客窓口部門、広報部門と連携し、脆弱性の影響調査、影響がある時の修正提供･広報作業の取りまとめを行う際の、製品開発部門全体の責任者としてベンダーCSIRTに協力する。なお、製品開発部門が大きい場合は、必要に応じて複数のサブ部門とりまとめ責任者を任命すると良い。

製品開発部門のとりまとめ責任者は、調査対象製品を確認し、調査作業ならびに対策（回避方法、修正方法）作成作業の進捗を管理しなければならない。

⑵ 各製品の調査責任者

各製品の調査責任者は、製品開発部門のとりまとめ責任者を経由して取得した脆弱性関連情報に対し、担当製品の影響の有無を回答しなければならない。調査責任者は、必要に応じてベンダーCSIRTに**詳細情報**を要求する事ができる。また、担当製品が他社から提供される製品／部品を含む場合は、製品提供元の会社に対し影響調査を依頼しなければならない。ただし、製品提供元が調整機関に予め届出ている関連会社でない場合は、ベンダーCSIRTを窓口として、調整機関を通じて調査を依頼しなければならない(5.2.1(3)参照)。

⑶ 各製品の調査／修正者（開発／保守担当）

各製品における脆弱性の影響調査や、影響がある場合の修正作成は、製品開発担当者または保守担当者が行う。調査者および修正者は、通常他の作業も実施しているので、全社の推進・管理組織またはベンダーCSIRTで決めた作業の優先度のルールおよび修正のスケジュールに従って行動する。

4.4　顧客窓口部門

製品の顧客は、狭義では製品を購入・利用している個人または企業（エンドユーザー）を意味するが、その製品を販売している販売会社や小売店、システムに組み込んでエンドユーザーに提供しているシステムインテグレータ(SI)等も重要な顧客である。同時にこれら販売会社や小売店、SI等も購入顧客を有しているため、エンドユーザーへの情報伝達には、これらのチャネルに依存し、それをうまく活用する必要がある。従って、顧客窓口部門には、エンドユーザー対応部門（直販営業、直販SE、保守・サポート、顧客サービス　等の部門）と、チャネル対応部門　（OEM先、パートナー会社、販売会社、小売店、量販店、システムインテグレータ　等に対して営業、SE、保守・サポートを提供する部門）がある。

製品の脆弱性に関する対応状況や対策情報を、購入・利用しているすべての顧客へ通知するためには、このエンドユーザー対応部門とチャネル対応部門の両方の顧客窓口部門と協調していく必要がある。また、顧客窓口部門はこのように多岐に渡る可能性があり、そのすべてが同じ情報を同じ理解度で認識し、同じコントロールの下で対応する必要があるので、脆弱性関連情報の取り扱いの考え方とルールを徹底しておく必要がある。

4.4.1　顧客への通知

製品脆弱性への対応状況や対策情報を購入・利用顧客へ通知するためには、顧客への連絡手段が必要であり、購入・利用顧客の情報を保持している顧客窓口部門を通して行うのが一般的である。脆弱性関連情報は、対策情報や対策提供の準備が不十分な状態で公知となる場合には、社会に多大な影響を及ぼす怖れがあるので、ベンダーCSIRTは、顧客窓口部門の十分な理解と協力を得ることが重要である。

購入・利用顧客への連絡先が全数把握できない場合、顧客窓口部門のみならず、広報やマーケティング部門を通じて、不特定多数へ周知することを検討する必要がある。

複数の会社の製品に影響がある脆弱性問題の場合には、他社と協調した対応が必要であり、調整機関や発見者と調整した公表日時以前に情報を通知してはならない。

対応状況や対策情報を、公表日以降速やかに顧客へ通知するためには、その通知内容を顧客窓口部門（エンドユーザー対応部門およびチャネル対応部門）へ充分な準備期間を用意して展開する必要がある。このため、スケジュールの策定に際しては、この準備期間をうまく反映するように留意する必要がある。

対応状況や対策情報は顧客へ通知または公表する情報であるが、公表日時までは関係者以外へは流通してはならない。また当該情報を先行利用する行為（営業行為、誘導行為等）も行ってはならない。

①顧客窓口部門は対象となる製品の購入・利用顧客をリストアップして、通知・公表日時までに通知の準備を行なう。

②製品分野・問題内容・顧客状況により、メール、文書、口頭等の適切な通知手段を選択して、通知・公表日時以降速やかに通知する。

4.4.2　問い合わせ対応

製品の脆弱性に関する対応状況や対策情報を顧客へ通知、または情報を公表した場合、顧客窓口部門へは、その内容に関する問い合わせや、対策の実施や実装等に関する支援要請や対応費用等についての相談が入ってくることが予想される。また、製品分野によっては、自社に直接問い合わせが入ってくるだけでなく、自社のチャネル先（OEM先、パートナー会社、販売会社、小売店、量販店、システムインテグレータ 等）へも問い合わせが発生する場合がある。

顧客からの問い合わせ等への対応を円滑にかつ迅速に行うためには、下記の取組が必要である。

①顧客窓口部門の代表者が通知・公表内容の決定に参画することが望ましい。
製品分野や問題内容によっては、通知・公表内容や通知先の選定が必要であり、事前に準備すべき内容が異なってくると想定される。

②製品開発部門は、通知または公表する内容、想定される問い合わせとその模範回答、想定外の問い合わせに対する回答の要請先（エスカレーション先）を決定し、対象となる顧客窓口全部門へ事前に通告しておく。

③顧客窓口部門へ事前通告する情報には通知・公表日時を明記し、指定日時までは、顧客窓口部門は、その情報を社内を含む第三者へ開示してはならない。またその情報を利用した営業行為をしてはならない。

④顧客窓口部門は、製品開発部門からの情報を、通知・公表日時以降、OEM先や販売会社等、顧客からの問い合わせを受ける可能性のあるチャネル先へ速やかに送付する。特にOEM先における影響が大きいと想定される場合には、事前にOEM先での対策を講ずることも考慮する必要があり、調整機関とよく事前相談の上対応すべきである。

⑤広く一般消費者に行き渡るような製品の場合には、コールセンター等の顧客サポート部門に問い合わせが殺到する可能性がある。そのような事態が想定される場合には、あらかじめ電話回線の確保や対応要員の増強・確保、サポート窓口対応マニュアルの整備、二次サポート体制の確保等、十分な準備を整えることが重要である。

自社製品の対策作成が完了していない状態で公的機関やメディア等で報告・公表された脆弱性に関して、自社製品への影響問い合わせを受ける場合がある。こうした場合に、個別の部門で対応状況や予定を回答してしまった場合、個別対応を余儀なくされる場合が生じる。

こうした問い合わせを受けた場合には、社内での対応状況を知っている場合でも、ベンダーCSIRTへ報告し、ベンダーCSIRTの指示の下に対応しなければならない。

4.5　広報部門

製品の脆弱性問題を不特定多数へ通知する場合には、広報部門と連携して、製品の脆弱性を通知するのに適切な手段（ウェブ・サイト、電子メール、報道メディア等）を採用する。

ウェブ・サイト等を利用する場合には、当該製品の情報として常に参照される場所へ掲載する、あるいは自社製品の脆弱性対応状況をまとめた専用ページを作成し、常にそこに掲載する等が望ましい。対策情報をウェブ・サイトからダウンロード提供できることが望ましいが、ウェブ・サイトへの掲載および不特定多数へのダウンロード提供に関しては輸出管理上の問題等が発生することにも注意しなければならない。

影響の大きな問題に関しては、報道メディア等で取り扱われる場合もあり、広報部門による取材への対応が必要な場合がある。自社製品の対応については、ベンダーCSIRTと調整して取材に対応することが必要である。

5. 脆弱性関連情報取扱手順の整備

本章では、製品開発ベンダーにおける脆弱性対応の各段階を時間的な経過を追って順に述べ、脆弱性関連情報を適切に取り扱うための手順整備のガイドラインを示す。JPCERT/CCでは脆弱性情報の公表日程の設定の目安を取り扱い開始後45日としており、状況によっては更に早い時期に公表される場合もあるので、製品開発ベンダーは、脆弱性情報を受け取った場合には時間を無駄にすることなく迅速に行動しなければならない。なお、本章で述べる手順を実施する主体は、特に指定がない限り、第4章で定義した各部門が各々引き受けるものとする。

5.1 脆弱性関連情報の受付

以下に述べる脆弱性関連情報の受付に関する対応手順全体の流れの概略を図 5-1 に示す。

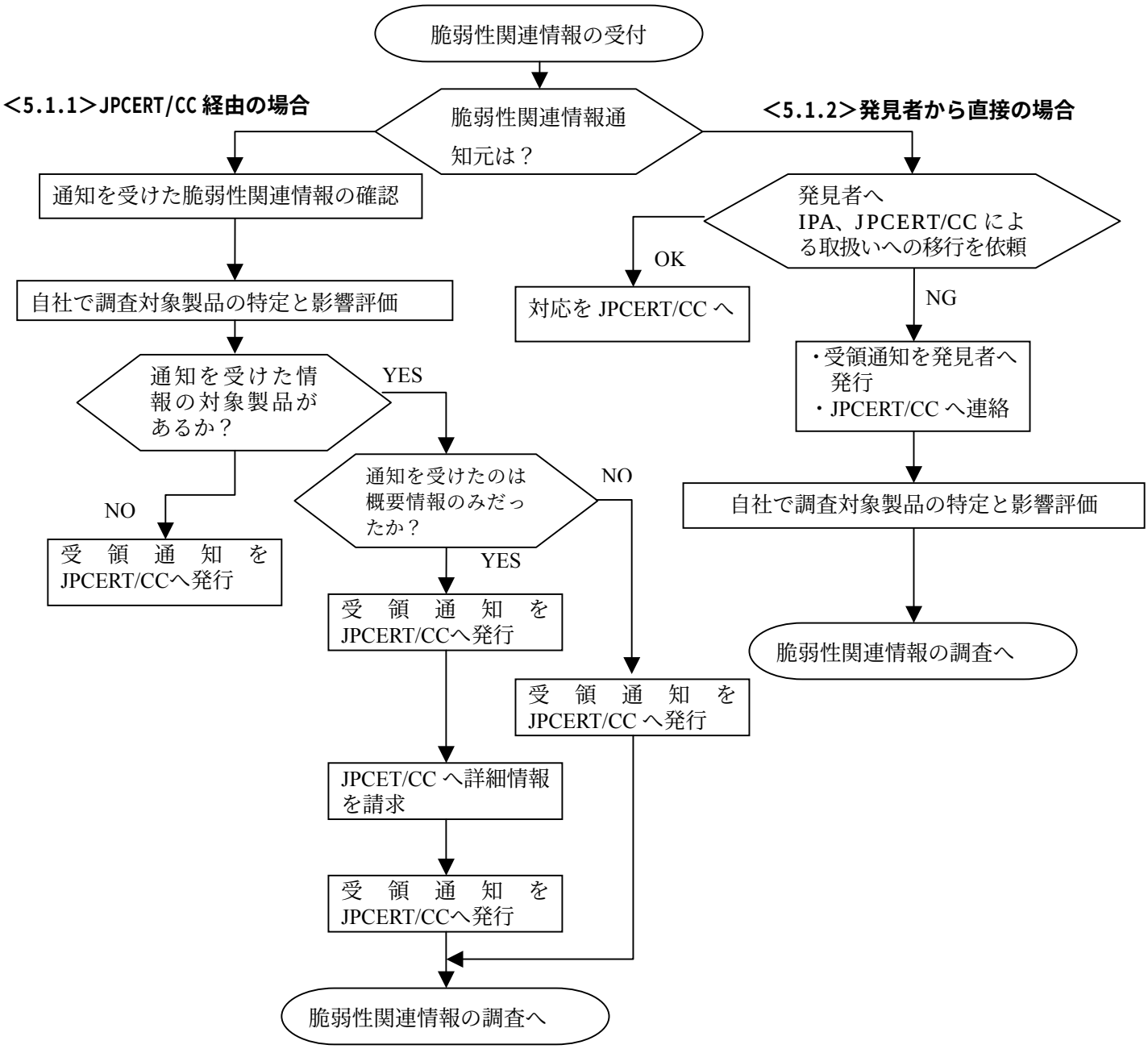

図 5-1. 製品開発ベンダーからみた脆弱性関連情報の受付の概略手順

脆弱性関連情報を特定するために、2種類の識別子、すなわち「**ベンダートラッキング番号(Tracking Number: TN)**」と「**脆弱性情報識別番号**(Vulnerability Number: VN)」とが用いられるので、混同することなく使い分ける必要がある。「ベンダートラッキング番号」は、JPCERT/CCから製品開発ベンダーごとに送付される脆弱性番号に付与された「JPCERT#番号」の形式をもつ識別子である。JPCERT/CCと当該ベンダー間の情報交換においてのみ利用され、第三者にとっては無意味である。「脆弱性情報識別番号」は、脆弱性関連情報の受付機関により付与された識別子で、「JPCERT-IPA#番号」(IPAの場合)や「VU#番号」(CERT/CCの場合)などの形式をもつ識別子であり、グローバルに通用する。第三者への問い合わせなどに際しては脆弱性情報識別番号を使わなければならない。なお、米国CERT/CCでは同時に発見されたものであっても一つ一つ脆弱性を識別して番号を付与しているため、米国CERT/CCが受け付けた脆弱性関連情報の中には、複数の脆弱性情報識別番号をもつものもある。

5.1.1　JPCERT/CCを通じて脆弱性関連情報の通知を受けた場合

JPCERT/CCからの脆弱性関連情報の通知は、ほとんどの場合メールを利用して行われる。情報のやり取りを確実に行うために、メールでは表題や本文の初めの部分で脆弱性のベンダートラッキング番号を明示した上で内容を記述する。

JPCERT/CCからの脆弱性関連情報の通知は、最初から詳細情報を添えてなされる場合と、まず**概要情報**だけが送られてくる場合とがある。

いずれの場合にも直ちに脆弱性関連情報の通知を受け取った旨の返事(**受領通知**)を返す。受領通知は、速やかに（遅くとも翌営業日中に）発行するよう努める。

⑴ 通知を受けた脆弱性関連情報の確認

通知された脆弱性関連情報の内容を確認する。

JPCERT/CCからの脆弱性関連情報（概要情報）通知の例：

プロトコルXの実現に関する脆弱性がABCから報告されています。実装製品がありますか？
詳細情報が必要ですか？

上の例におけるABCの部分は、日本国内で報告された情報の場合にはIPA、それ以外の場合には米国CERT/CCや英国NISCCのような海外の脆弱性関連情報取扱機関である。

IPAに脆弱性関連情報を通知した発見者の名前は製品開発ベンダーには通知されないが、調査などで追加情報を求めるために製品開発ベンダーが希望し、発見者もこれに同意していた場合には、交換されるすべての情報の写しをJPCERT/CCに提供することを条件に、直接の情報交換を選ぶことができる。

⑵ 調査対象製品の特定と影響評価

製品開発部門に対し、脆弱性関連情報（概要情報）に関連する調査対象製品の特定と影響評価を指示する。

⑶ 受領通知の発行

開発部門での該当製品特定作業が完了する目処を勘案して、当面の対応方針を決め、それに即した受領通知をJPCERT/CCに発行する。

すぐに該当製品を特定できないが、製品の特定作業を開始する場合の受領通知の例：

概要情報を受けました。製品の特定を始めます。詳細情報が必要な場合すぐ連絡します。

該当製品が特定された場合の受領通知の例：

概要情報を受けました。影響のありそうな製品がありますので、詳細情報を送ってください。

該当製品が無い場合の受領通知の例:
　概要情報を受けました。影響のありそうな製品はありません。詳細情報は必要ありません。

⑷ 通知された詳細情報の確認

詳細情報の送付を依頼した場合には、機微な情報なので、詳細情報を受け取りしたい、受領通知を返す。詳細情報の内容を確認し、関連部門に必要な情報を提示し調査を指示する。

JPCERT/CCからの脆弱性関連情報（詳細情報）の例-1
　脆弱性につながる不具合を再現させる条件を送付します。期待されるアクションは…です。

JPCERT/CCからの脆弱性関連情報（詳細情報）の例-2
　モジュールXの脆弱性を修正するためのパッチを送付します。期待されるアクションは…です。

JPCERT/CCからの脆弱性関連情報（詳細情報）の例-3
　脆弱性を検証する**テスト・スイート**を送付します。期待されるアクションは…です。

5.1.2　発見者から直接に脆弱性関連情報の通知を受けた場合

発見者がIPAを介さず直接に製品開発ベンダーに脆弱性関連情報を通知してきた場合には、顧客である発見者との対話が感情的な行き違いなどから円滑に進まなくなる可能性もあり、また他のベンダーや海外との連携が必要となる場合もあるためるため、情報セキュリティ早期警戒パートナーシップの枠組みによる取扱に移行するよう求め、理解を得るようにする。万一に発見者が自社との直接接触の継続を主張する場合には、別途調整機関に報告するとともに、以下の手順に沿って誠実に対応を進めるようにする。

⑴ 通知された脆弱性関連情報の確認

通知された脆弱性関連情報の内容を確認する。通知の中に明示されていなかった場合には、次の事項を関連情報として発見者に問い合わせる。

① 脆弱性関連情報を既にIPAや他の製品開発ベンダーなどに通知したかどうか。
② 脆弱性関連情報を公表する意思とその時期。
③ 製品開発ベンダーが対策を含めた脆弱性対応状況を公表する際の謝辞における発見者名の記載方法についての希望。

⑵ 受領通知の発行

脆弱性関連情報の通知を受け取った旨の返事(受領通知)を返す。受領通知は、速やかに（遅くとも翌営業日中に）発行するよう努める。受領通知の発行が遅れ、発見者から受領通知に対する督促を受けた場合は、発行遅れの理由や状況などを添えて速やかに受領通知を出す。

通知された内容が、脆弱性なのか単なる不具合なのかも慎重に吟味する必要がある。脆弱性でないと判断した場合には、その旨を発見者に伝えるとともに通常の不具合に対する対応をとる。

⑶ 調査対象製品の特定と影響評価

製品開発部門に対し、脆弱性関連情報に対応する調査対象製品の特定と影響評価を指示する。

なお、その後の対応においても、再現性の確認や対策提供時期の決定などの大きな動きを発見者に伝えておくことが望ましい。また、発見者が脆弱性関連情報の公表を希望する場合には、その時期や方法、発見者の個人情報の開示方法と内容等について、慎重にかつ適時に対応することが必要である。そのためにも、適宜調整機関と調整し、アドバイスを得ることが望ましい。

5.2　脆弱性関連情報の調査

脆弱性関連情報の調査では、それらの「再現試験」とそれに続く「脆弱性評価」を行う。JPCERT/CCから通知される脆弱性関連情報は、技術を特定した脆弱性関連情報である場合と、製品を特定した脆弱性関連情報である場合とがある。発見者が製品開発ベンダーに直接に脆弱性関連情報を通知する場合のほとんどは、製品を特定した脆弱性関連情報であると想定される。以下では、技術を特定した脆弱性関連情報と、製品を特定した脆弱性関連情報の場合に分けて対応手順を述べる。

5.2.1　技術を特定した脆弱性関連情報の通知を受けた場合

技術を特定した脆弱性関連情報は、「プロトコルXの多くの実現にZの脆弱性がある」あるいは「広く利用されているコードYにZの脆弱性が発見された」といった表現で通知される。この場合には、自社のどの製品が該当しうるかを判断して調査範囲を定め、それに含まれる各製品の調査を進める。

⑴ 調査対象製品の範囲を特定する

通知されている脆弱性関連情報で特定されている技術が利用されている可能性があるかどうかという視点に基づいて調査すべき製品の範囲を特定する。

⑵ 個々の製品について脆弱性の有無を調査する

調査対象として特定された個々の製品に関して、脆弱性関連情報に照らして製品に含まれる脆弱性の有無を判定する。 判定は、1) 再現シナリオに基づいた試験の実施またはコード・レビュー、 2) プログラム・コードの由来の調査、または、3) テスト・スイートによる試験結果、などの方法により行う。

なお、テスト・スイートは、そのまま攻撃用ツールとして悪意ある者に悪用され、あるいは攻撃用ツール開発のヒントを与えうる。テスト・スイートを入手または開発した場合には、その後の管理には特に注意を払わなければならない。

⑶ 他社から導入したモジュールが関連する場合の調査方法

上述の製品についての脆弱性の有無の調査において、関連するモジュールが他社からの導入品を組み込んだものであり、提供元に調査を依頼しなければならない場合がありうる。脆弱性関連情報の機密管理のために、調査依頼は脆弱性情報識別番号のみを提示して問い合わせ、脆弱性関連情報そのものを提供してはならない。脆弱性情報識別番号を入手していない場合には調整機関(JPCERT/CC)に問い合わせて確認する。モジュールの提供元が脆弱性関連情報を得ていない場合には、状況をJPCERT/CCに伝え調整を依頼することができる。

なお、調査内容の報告などにおいて、提供元との間で結んでいる機密保持義務により第三者への開示や報告が許されない場合もありうる。こうした兼合いにも配慮する必要がある。

5.2.2　製品を特定した脆弱性関連情報の通知を受けた場合

⑴ 脆弱性を通知された製品を確認する

脆弱性を通知された製品名や版番号などを確認する。

さらに、その製品について既に存在が分かっている脆弱性の中に、通知された脆弱性と同じものがないかどうかを調べる。同じものが見つかり、対策の作成が完了している場合には、JPCERT/CCまたは発見者にそれを連絡し、対応を終結する。同じものが見つかっても、対策の作成が完了していなかった場合には、対策作成予定の前倒しなどの必要性と可能性を検討する。

⑵ 指摘された脆弱性につながる現象の再現を試みる

通知された脆弱性関連情報に基づき、指摘された脆弱性につながる現象の再現を試みる。再現を確認できた場合には、JPCERT/CCまたは発見者にその旨を報告する。

通知された情報をもとに現象の再現を試みたものの再現できなかった場合には、その旨を調整機関または発見者に伝え、補足情報の提供を依頼することも検討すべきである。この場合の補足情報とは、脆弱性のさらに詳細な説明、脆弱性が発生する環境や設定条件、関与が考えられる他のソフトウェアなどの情報である。

⑶ 不具合の原因と発現する条件を特定する

再現できた脆弱性の原因を特定する。その結果に基づいて、当該製品と同様の機能構成を持つ製品や共通するコードを利用して開発された製品について、同様の脆弱性が存在しないかどうかを確認する。

⑷ 脆弱性の影響範囲が自社製品に限定されるかどうかを判定する

脆弱性の原因箇所が自社製品に固有のコードにあるかどうかを調べる。社外から導入したコードに原因がある場合には、他の製品開発ベンダーの製品にも共通の脆弱性が存在する可能性が高いと推定されるので、JPCERT/CCを通じて、ないし直接に提供先の製品開発ベンダーにその旨を報告する。この場合には、対策を含む脆弱性対応状況の公表時期が再調整される可能性がある。

また、社外に提供している自社コードに原因がある場合には、必要に応じてJPCERT/CCを通じて、または直接提供先の製品開発ベンダーにその旨を報告し、できる限り、情報セキュリティ早期警戒パートナーシップの枠組みを活用して対処するようにする。

5.3 対策の作成

調査により脆弱性が確認された場合、製品開発ベンダーはサポートしている製品に対し、脆弱性のリスクを削除または低減する対策を以下のステップに従って作成する。

5.3.1 対策方法の検討

製品開発ベンダーは、回避方法、修正方法、対策を公表する目標期日などを含む対策計画を作りJPCERT/CCに通知する。対策計画を通知することは、JPCERT/CCによる公表時期の調整の基礎データとなる。通知を怠った場合には、自社製品に関する固有事情が配慮されないまま公表日が設定されるリスクが増すことに留意する必要がある。

対策計画の策定にあたって配慮すべき点は次のとおりである。

⑴ 暫定的な対策の検討

①リスク下にあるシステムの数とリスクの切迫度、対策可能な時期、当該対策を適用する難しさなどを考慮した上で、必要ならば暫定対策を提案することが望ましい。

②暫定対策には、その効果と制約を明示する。

⑵ 複数の版/複数言語/複数製品への対応

①複数の版や、複数の言語対応版や、複数の製品が同じ脆弱性の影響を受ける場合には、すべての版や製品に対する対策を同時に提供できることが望ましい。

②対策の提供を妥当な時間内に行う(JPCERT/CCの目安は45日後)ために、すべての版や製品に対する対策の同時リリースが困難と判断した場合には、リスクに応じて対策提供開始時期の優先順位付けを行うとともに、暫定的な回避策を提供するなど、対策の提供が遅れる製品に対するリスクを回避軽減するよう努める。

⑶ 対策公表の目標期日の設定

対策を公表する期日の設定においては、JPCERT/CCによる取扱い開始から起算し45日後の目安、当該脆弱性が引き起こすリスク、対策作成の難しさ、対策の品質を保証するのに必要なテストのための時間、対策の円滑な実施を保証するのに必要な準備などを考慮する。計画は、作業進捗や状況の変化を反映し、通知後も随時変更できる。複数の製品開発ベンダーからの計画に基づいて、JPCERT/CCが対策公表期日を調整し指定した場合には、それに対応する必要がある。また、情報のコントロールに関する不測の事態や他製品ベンダーの事情によっては、急遽予定が変更される可能性がある。JPCERT/CCまたは製品開発ベンダーは、対策公表の期日について調整が必要と判断した場合には随時協議をおこなう。

5.3.2 対策方法の開発

対策計画に従って対策方法の開発を行う。対策方法には次のような類型のものが考えられる。

⑴ 修正による対策方法

①パッチまたは修正版を用意する。
②他の機能や性能強化を含んだ改版を用意し、その上で脆弱性を除去する。

⑵ 回避による対策方法

①設定時のパラメータ変更を指示する。
②運用環境を変更する。 (例えば、他の機器やソフトによるパケット・フィルタリングの導入など)
③運用条件を変更する 。(例えば、監視下で運用し異常検出時に再起動するなど)
④制限事項として明示する。

製品開発ベンダー側で修正による対策方法の開発にかかる時間や、利用者側で運用中の製品に適用するまでに要する時間・コストや難しさなどを配慮し、回避による対策方法を先行して提供したり、異なった複数のタイプの対策方法を同時に提供すべき場合もある。

5.3.3 対策の確認

対策公表前に、最大限の合理的な努力をもって対策の妥当性を確認する。

①対策の有効性、対策によって引き起こされる副作用、互換性の問題、その他の制限について検証して妥当性を確認し、検証結果を明確に文書化する。
②改版の提供が必要な場合には、関連・前提製品のバージョン等との組み合わせのチェックも必要となる。同時に、改版の提供媒体の選択、提供流通経路の選択、有償無償の判断、エンドユーザーへの改版情報伝達の徹底と更新促進の工夫等の検討も必要である。
③ウェブ・サイト等からのダウンロード提供の場合には通知のみで済むが、対策情報の提供形態が、個別のファイル送付や媒体提供や改版への切り替え等になる場合には、顧客窓口部門に顧客と折衝の上で個別対応をしてもらう必要がある。顧客窓口部門と連携して、顧客へ送付する媒体の種別や数量、送付先等をリストアップして対策情報を遅滞なく送付できるようにすることが求められる。
④もし発見者が対策を確認することを望む場合には、それを出来る限り支援することが望ましい。

5.4　対策の通知と公表

公表すべき脆弱性対応状況には次の3種類がある。

①対応状況とベンダー声明

対応状況とベンダー声明は、公表を前提としてJPCERT/CCに送られる。脆弱性をもつ製品の有無や対応状況の概略および製品開発ベンダーが自身のウェブ･サイトを通じて提供する関連情報のURLなどを記述する。その形式はJPCERT/CC脆弱性関連情報取扱ガイドラインで指定されている。これは他の製品開発ベンダーの対応状況と併せて一覧できるよう編集され、IPAとJPCERT/CCが共同で運用しているウェブ･サイト **JVN** (JP Vendor Status Notes)で公表される。

JVN上での公開は、原則として脆弱性情報識別番号をインデックスとして公表される。ただし、米国CERT/CCが**US-CERT** Technical Cyber Security Alertとして公表する場合など、海外CSIRTが受け付けた脆弱性関連情報で影響の大きなものに対しては, 当該CSIRTの判断により特別な識別子が割り当てられることがある。この場合にはJVN上でも、脆弱性情報識別番号の代わりに、同じ特別な識別子がインデックスとして用いられる。

②企業ウェブ･サイトで公表する自社製品に関する脆弱性の概要等とそれへの対応状況

企業ウェブ･サイト上の、トップページ等利用者が比較的アクセスしやすい階層に、自社製品の脆弱性に関する情報を掲載する。更に、そこから容易にアクセスできる場所に、脆弱性ごとの概要説明やJVN等の公的な情報へのリンクを載せるようにする。製品が多岐にわたる場合は、上位階層のページをポータルサイトのように構成することが望ましい。

③その他のメディアにより通知･公表する対策情報

上記以外のメディアを通じて通知･公表される情報。通知対象者や通知メディアの特性を考慮して作成する。

いずれの情報も、会社としての正式な公表情報として扱われるため、社内の情報公表手続きに従って、承認された情報を公表しなければならない。

これらを含む公表される脆弱性情報等の相互関係を図5-2に示し、作成や公表に関連する手順を以下に述べる。

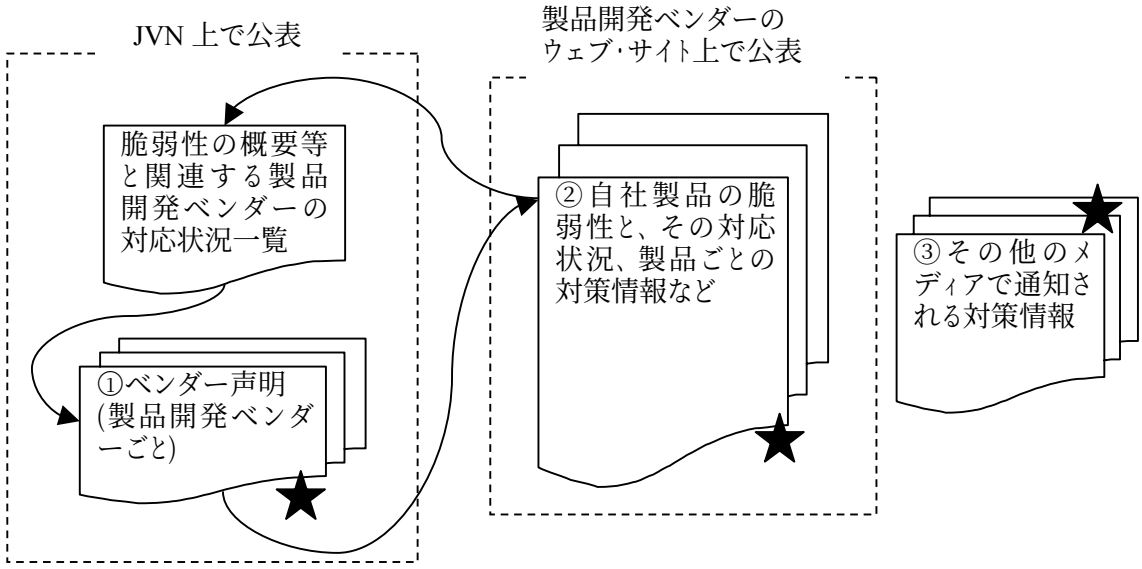

図 5-2. 公表される脆弱性情報や対策情報の関係
(★印の情報は製品開発ベンダーが用意する)

5.4.1　JPCERT/CCから公表予定の脆弱性情報の骨格の受領

脆弱性対応状況の公表予定日まで1週間ほどになると、JPCERT/CCから関連する製品開発ベンダーに、公表情報の骨格部分の草案と、公表情報が掲載される予定のURLを添えて、対応状況とベンダー声明の提供を求める電子メールが配布される。特定の製品のみに関連する脆弱性では多くの場合、JPCERT/CCによる公表情報の作成に製品開発ベンダーの協力が望まれる。

受け取った公表情報の骨格草案を精査し、製品開発ベンダーが準備すべき通知や公表情報の作成を次項で述べるように進める。この時点で可能ならば、情報を公表する予定URLを決める。

5.4.2　JPCERT/CCへの対応状況に関するベンダー声明の連絡

脆弱性対応状況とベンダー声明を作成し、脆弱性情報の公表予定日に間に合うようJPCERT/CCへ連絡する。対策が公表予定日に間に合わない場合でも、連絡をおこなわなければならない。連絡を怠った場合には、JVN上で「不明」と表示され一般利用者の心証を損なう可能性があるので注意が必要である。また、連絡の際には、暗号化などを施すことにより情報の機密性を保たなければならい。

対応状況（ステータス）は次のいずれかから選ぶ:

- 該当製品あり　(脆弱性に該当する製品がある場合)
- 該当製品なし　(脆弱性に該当する製品がない場合)
- 該当製品あり：調査中 (脆弱性に該当する製品が1つ以上あり、継続して調査中の場合)
- 該当製品なし：調査中 (脆弱性に該当する製品は見つかっていないが、継続して調査中の場合)

次に連絡内容の一例を示す。「提供情報」として記述する内容は製品開発ベンダーごとに用意されたページに掲載される。

JPCERT/CCに連絡するベンダー声明の連絡例-1:

弊社における対応状況(JVN公表用)を次のとおりご連絡いたします:
ベンダートラッキング番号 : JPCERT#12345678
脆弱性情報識別番号 : JPCERT-IPA#A1B2C3D4
会社名:　　○○株式会社
ステータス:　該当製品あり
提供情報:　本脆弱性情報に関しては、以下の URL にて対策を公開しています
http://www.example.co.jp/vuls/12345/22222.html

JPCERT/CCに連絡するベンダー声明の連絡例-2:

弊社における対応状況(JVN公表用)を次のとおりご連絡いたします:
ベンダートラッキング番号: JPCERT#87654321
脆弱性情報識別番号 : JPCERT-IPA#F8C2C1G3
会社名:　　○○株式会社
ステータス:　該当製品なし
提供情報:　本脆弱性に該当する○○株式会社の製品はありません

5.4.3　企業ウェブ・サイトなどから直接に公表する対策情報の準備

企業ウェブ・サイトなどから製品開発ベンダーが直接に公表するための脆弱性対応状況を準備する。次の例を参考にするなどして、製品ユーザーや対策実施者にとってできるだけわかりやすいものとするよう努める。

企業ウェブ･サイト上の脆弱性ポータル･サイトでの対応状況の公表例:

脆弱性情報識別番号: JPCERT-IPA #F88C2C13　プロトコルZZZの実現の脆弱性
(JVNへのリンク)
概要:
プロトコルZZZの一部の実現にバッファ･オーバフローの脆弱性がある
想定される影響:
リモートから第三者にDoS攻撃されうる
最悪の場合には任意のコードを実行される可能性もある
各製品の該非:
* 製品ABC: 脆弱性がある
詳細情報: <URL-1>
* 製品DEF: 脆弱性はない
* 製品GHI: 脆弱性がある
詳細情報: <URL-2>
* その他の製品については鋭意調査中です
謝辞: 本脆弱性を発見し通報された日本太郎氏に心から感謝申し上げます
公表期日:　　xxxx年tt月t日
最新更新期日: xxxx年uu月u日

脆弱性の概要や想定される影響の記述にあたっては、情報を悪用して攻撃に利用されることがないように過度に情報を開示しないことと、脆弱性によるリスクを製品の利用者が的確に把握するために必要な情報を十分に提供することとのバランスに留意しなければならない。

製品ごとの対応状況の公表例:

タイトル: JPCERT-IPA #F88C2C13 プロトコルZZZの実現に脆弱性
(JVNへのリンク)
概要:
プロトコルZZZの一部の実現にバッファ･オーバフローの脆弱性がある
想定される影響:
リモートから第三者にDoS攻撃されうる
最悪の場合には任意のコードを実行される可能性もある
製品ABC: 脆弱性がある
影響を受ける範囲: 版MM.nnnよりも以前の版が脆弱
対策: ftp-1で提供しているパッチが必要
詳細情報: <URL-1>
製品DEF: 脆弱性はない
詳細情報: <URL-2>
製品GHI: 脆弱性がある
影響を受ける範囲: MM.nnn以前の版が脆弱
対策: xxxx年vv月頃にパッチを提供予定
暫定対策: オプションをオフに設定する
詳細情報:問い合わせ先
その他の製品に関する調査状況
関連情報: プロトコルZZZの実現に脆弱性
http://jvn.jp/xxxx/index.html
謝辞: 本脆弱性を発見し通報された日本太郎氏に心から感謝申し上げます
更新履歴:　xxxx年tt月t日　新規
xxxx年uu月u日　製品DEFに関する情報を追記

公表の1週間ほど前になり、公表情報の準備が済んだら、公表後の問い合わせに混乱なく対応できるよう、顧客窓口部門などの代表者の参画を求め、必要に応じてQ&A集や顧客個別情報を用意するなどして準備を整える。

5.4.4　企業ウェブ・サイト上などでの脆弱性対応状況の公表

JVN上で対応する脆弱性対応状況が公表されたことを確認した後に速やかに(あるいは協議の上決定された日時に)製品開発ベンダーからも前項において準備した情報の公表を開始する。

5.4.5　発見者への報告

JPCERT/CC経由でなく発見者から直接に通知を受けていた場合や、調査の過程などで発見者と直接の情報交換をした経緯がある場合は、発見者に脆弱性情報の公表を謝意とともに伝える。対策の提供まで済んでいる場合には、この連絡をもって一連の対話を終結させる。

5.4.6　その後の更新

公表後も調査や対策作成の進捗に応じて、JPCERT/CCに連絡した対応状況や企業ウェブ・サイト上で直接に公表している情報を最新版に随時更新する必要がある。特に公表時点で、調査中の製品が含まれていた場合や暫定的な回避策しか提供できていない場合は、本対策の作成が対象製品の全てについて完了するまで継続フォローする必要がある。

脆弱性情報の通知と公表に際して注意すべき点を以下に列挙する。

①公表日一致の原則

複数のシステムに影響を与える脆弱性の場合には、脆弱性が悪用されて社会全体の混乱を招くリスクを下げるために、公表にあたって関係者が足並みを揃えることが重要である。これは公表日一致の原則とも呼ばれる。関係者が足並みを揃えるための調整は日本国内においてはJPCERT/CCによりより行われる。公表日は不測の事態の発生などにより急遽変更される可能性もあるので、状況把握に努めなければならない。

製品開発ベンダーは公表日を厳守し、公表日より前に情報が漏れないように厳重に管理する必要がある。万一、何らかの事故で脆弱性関連情報が第三者に漏洩したことが疑われる場合には、直ちにJPCERT/CCに通報しなければならない。

②通知、公表手段の検討

製品開発ベンダーは、製品の市場特性、当該脆弱性が及ぼす影響の範囲や大きさに応じ、どのような手段でセキュリティ対策情報および対策手段の通知、公表を行うかについて事前に検討、準備をしておく必要がある。その際、ユーザー環境にも十分配慮した手段を検討する必要がある（例：ナローバンドユーザーへの大容量パッチの配信手段など）。

通知、公表先としては以下のような連絡先が考えられる。

⑷　製品ユーザー
⑸　製品を利用したシステム、ネットワークの構築・運用者（自社内を含む）
⑹　製品の販売店、量販店
⑺　業界団体
⑻　情報セキュリティに関する民間団体
⑼　政府機関など

また、通知、公表の手段としては以下のようなものが考えられる。

- ウェブ･サイトへの掲載
- ダイレクトメール（電子メール、郵便）、FAX等による個別通知
- 製品の販売店、量販店を通じた周知（CD-Rの配布などを含む）
- メディア（新聞、雑誌、テレビ等）による周知など

③問い合わせ窓口の準備

対策情報の公表後には当該脆弱性情報に関してユーザーからの問い合わせが考えられる。問い合わせ窓口の設置や対応方法などを事前に検討しておく。場合によっては、製品の販売店等とも連携する必要がある。

6. まとめ

このガイドラインでは、まず情報セキュリティ早期警戒パートナーシップとその背景から説き起こし、次いで、顧客と社会に対する責務を果たすために、インターネット関連製品を提供する製品開発ベンダーがその枠組みに参加して、脆弱性情報に適切に対応するために整備すべき社内体制と対応手順についての要件を述べた。特に強調したいポイントは以下の3項目である。

①脆弱性関連情報に関する取り扱いの枠組みを理解し、全社的な組織体制と手順を確立して、その周知と理解を徹底させ、経営者権限によって推進、運営しなければならない。

②全社横断的取り組み体制の下、社内関連部門の協力と協調を得て、迅速かつ的確に対策を推進しなければならない。

③脆弱性の対策情報は調整されたタイミングで公表し、先行して公表してはならない。独断による情報の公表は多大なる影響を及ぼし、国内ばかりでなく全世界的な規模での被害を発生させる場合もある。情報管理を徹底し、情報の漏洩を防ぎ、調整機関(JPCERT/CC)との連携によって円滑に必要な情報を公表しなければならない。

なお、本ガイドラインのカバーする範囲ではないが、脆弱性を克服した安全快適な情報ネットワーク社会の実現のためには、この「情報セキュリティ早期警戒パートナーシップ」の枠組みだけでなく、

①脆弱性を作り込まない開発手法の開発とそのための研究や教育

②広くエンドユーザーに脆弱性情報を行き渡らせ、市場に出回っている製品の末端にまで対策の実施を徹底させるための、迅速で効率的で実効性のある体制の構築と整備

③製品の脆弱性の是正のために、対策の手間やコストの負担問題を含めて、顧客の理解と協力を得ること

④これらを通じて、脆弱性への取組が製品ベンダー・販売店・SI 業者・エンドユーザーの枠を超えて広がり共有されていくこと

が必要であり、そのための社会的コンセンサス作りに、産・官・学がそれぞれの立場から、かつ協力し合って取り組みを深めていくことが必要ではなかろうか。

情報ネットワークの発展と浸透は経済社会に多大の利便と効果をもたらしているが、同時にソフトウェアの脆弱性とそれを攻撃対象とする行為による社会的経済的打撃の脅威も高まっている。我々ソフトウェアベンダーにとって、脆弱性を極力排除した製品を提供することは共通の責務であるが、万一リリース後の製品に脆弱性が存在する場合には、迅速にその是正策を講じる社会的責任がある。そのために、本ガイドラインに沿って、JPSA 会員企業をはじめとしてできるだけ多くのソフトウェアベンダーが脆弱性問題への対応体制を確立し、「情報セキュリティ早期警戒パートナーシップ」の枠組みに加わっていただきたい。そして、エンドユーザー、販売店、SI 業者、IPA や JPCERT/CC 等の運営機関、JPSA、その他の業界団体、更には脆弱性の研究者・発見者をも含めた信頼の輪を育みつつ、このパートナーシップの枠組みを発展させ成長させるために積極的役割を担っていただきたい。そのために必要な、各社における社内体制の整備と対応手順の確立の一助として、本ガイドラインがお役に立てれば幸いである。

<<<付録>>>用語集

(ABC、あいうえお順)

用語	解説
CERT/CC	CERT Coordination Center　読み：サートシーシー 米国のCSIRT。 1988年11月の Morris ワーム事件をきっかけに米国カーネギーメロン大学の Software Engineering Institute (SEI) に作られた世界で最初のCSIRT。
CSIRT	Computer Security Incident Response Team コンピュータセキュリティに関するインシデント（攻撃等の事案）が発生したときにその対応について支援調整を行う組織
IPA	Information-technology Promotion Agency, Japan; 独立行政法人 情報処理推進機構 経済産業省告示第236号において受付機関に指定されている <http://www.ipa.go.jp/>
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center; 読み：ジェイピーサートシーシー 有限責任中間法人JPCERTコーディネーションセンター 経済産業省告示第236号において調整機関に指定されている
JVN	脆弱性情報の一般への公表を行うウェブサイトであり、製品開発ベンダーの脆弱性対応状況や対策情報がJPCERT/CCを通してこのサイトに表される JP Vendor Status Notes (JVN)　<http://jvn.jp/>
NISCC	National Infrastructure Security Co-ordination Center　読み：ナイシー 英国の内務省内に組織されている、政府系CSIRT。
POC	Point Of Contact; 社外からベンダーを見た時の脆弱性関連情報に関する総合窓口 ベンダーCSIRTが社外に対して提供する主要な機能
US-CERT	United States Computer Emergency Readiness Team　読み：ユーエスサート 米国の国土安全保障省内に組織されている、政府系CSIRT。
受付機関	発見者が脆弱性関連情報を届出るための機関 経済産業省告示第236号によりIPA(独立行政法人情報処理推進機構)と指定されている。
回避方法	脆弱性自体を修正することなく、脆弱性が原因となって生じる被害を回避するための方法 脆弱なサービス機能の停止や攻撃経路の遮断など
概要情報	脆弱性関連情報のうち、技術的な詳細を含まない情報 情報漏洩の可能性を低減するため、製品開発ベンダーに該当する可能性がある製品の有無を照会するためにJPCERT/CCから送られる
関連会社	JPCERT/CC 製品開発者リスト登録規約に基づいて登録した製品開発ベンダーにおいて、社内の開発部門と同等に位置づけられる自社以外の会社 これらの会社の名称はJPCERT/CCへの製品開発者リスト登録時に明示する
検証方法	脆弱性が存在することを調べる方法
攻撃方法	脆弱性を悪用するプログラム、コマンドまたはデータおよびそれらの使用方法
顧客窓口部門	製品について顧客からの問い合わせに対応する部門（お客様総合窓口、コールセンターなど）を指す 製品について個々の顧客に直接アプローチし、対策の実施にあたる部門（顧客ＳＥ、保守部門等）は含まない
修正方法	脆弱性を修正する方法 （ソフトウェアのパッチや改版など）
受領通知	発見者またはJPCERT/CCからの脆弱性関連情報の報告を受領したことを、製品開発ベンダーが発見者またはJPCERT/CCに送る通知
詳細情報	脆弱性関連情報で、脆弱性の検証方法や検証ツールや攻撃コードなどの、技術的な詳細を含む情報 (製品に脆弱性があるか否かを調査するために利用する)

情報セキュリティ早期警戒パートナーシップ	経済産業省告示第235号および第236号を踏まえ、IPAが受付機関、JPCERT/CCが調整機関という役割を担い、発見者や製品開発ベンダーやウェブ･サイト運営者と協力しながら、脆弱性関連情報について発見から公表までを円滑に進めるための枠組み
脆弱性	ソフトウェアやこれを組み込んだハードウェアにおいて、コンピュータ･ウイルスやコンピュータ不正アクセス等の攻撃により、その機能や性能を損なう原因となりうる安全性上の問題箇所
脆弱性関連情報	脆弱性に関連する情報であって、脆弱性または、検証方法または、攻撃方法のいずれかに該当するもの
脆弱性情報	脆弱性の性質および特徴を示す情報
脆弱性情報識別番号	脆弱性関連情報を識別するユニークな識別子 (Vulnerability Number: VN) 脆弱性関連情報を直接には渡すことなく、対応状況を他のベンダーに問い合せるためにも利用できる 国内で発見されIPAが受け付けたものは「JPCERT-IPA#番号」、米国CERT/CCが取り扱っているものは「VU#番号」のような形式で採番される
製品開発者	経済産業省告示第235号の中で、本ガイドラインにおける製品開発ベンダーを意味する用語として用いられている ソフトウェアを開発した者、または、ソフトウェア製品の開発、加工、輸入または販売に関する形態その他の事情からみて、当該ソフトウェアの実質的な開発者と認められる者
製品開発ベンダー	ソフトウェアを開発した者、または、ソフトウェア製品の開発、加工、輸入または販売に関する形態その他の事情からみて、当該ソフトウェアの実質的な開発者と認められる者
ソフトウェア製品	ソフトウェア又はそれを組み込んだハードウェアであって、汎用性を有する製品
対応状況	JPCERT/CCから脆弱性関連情報の通知を受けた製品開発ベンダーが報告する対策方法、取り組みの状況などを含む情報 製品開発ベンダーの公式見解としてJVN (JP Vendor Status Notes)上で公表される
対策情報	製品開発者が脆弱性対策の状況または結果を利用者に伝えるための情報
対策方法	対策方法は、脆弱性から生ずる問題を回避するまたは解決を図る方法のことであり、回避方法と修正方法から成る 本ガイドラインで、「対策方法」との記述がある場合、「回避方法または修正方法」の意味となる
調整機関	脆弱性関連情報に関して、製品開発ベンダーへの連絡および公表等にかかわる調整を行う機関 経済産業省告示第236号によりJPCERT/CC(有限責任中間法人JPCERTコーディネーションセンター)と指定されている
テスト･スイート	多くの場合テスト用プログラムとテスト用データの対から構成された、一群の試験シナリオまたは試験項目
発見者	脆弱性関連情報を発見または取得した者
ベンダーCSIRT	ソフトウェアベンダー内で、外部のCSIRT(JPCERT/CC等)との窓口役を果たしつつ、 自社製品の脆弱性への対応活動を統括し推進する司令塔的機能と責務を担う組織
ベンダー声明	脆弱性関連情報に該当する製品の有無や対応状況の概略および製品開発ベンダーが自身のウェブを通じて提供する関連情報のURLなどを記述した公表を前提とした声明文
ベンダートラッキング番号	JPCERT/CCから製品開発ベンダーごとに送付される脆弱性情報に付与された番号 (Tracking Number: TN) , 「JPCERT#番号」の形式で採番される 脆弱性情報識別番号とは異なるので注意を要する

「製品開発ベンダー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第 1.0 版」

脆弱性関連情報企業内取扱ガイドライン研究会
発行　平成 16 年 12 月

発行者　　社団法人　日本パーソナルコンピュータソフトウェア協会
〒100-0014　東京都千代田区永田町 2-4-2　秀和溜池ビル 4 階
TEL：03-5157-0780　　FAX：03-5157-0781
URL：http://www.jpsa.or.jp