2. 脆弱性情報の取り扱いについて
—情報セキュリティ早期警戒パートナーシップの概要と運用の状況—

前（独）情報処理推進機構セキュリティセンター
早貸 淳子　j-hayaka@ipa.go.jp

情報システムの脆弱性をめぐる問題の状況

◆脆弱性関連情報の流通

2003年8月に発生したMS Blasterワームや2004年に発生したSasserワームに見られるような，ソフトウェアの「脆弱性」を悪用するコンピュータウイルスや不正アクセスによる攻撃は，いったん発生してしまうと，ユーザが対処可能なスピードをはるかに超える勢いで広がり，システムダウンなどの思わぬ被害の拡大を招くことになる．また，「脆弱性」のあるソフトウェアを利用しているコンピュータやWebサイトがその脆弱性を突く攻撃を受けると，顧客情報や企業秘密等の窃取に発展してしまう可能性がある．このようにソフトウェア等の「脆弱性」は，IT社会の安全性を脅かすインシデントの一因となっているといえる．

昨年の7月に運用を開始した「情報セキュリティ早期警戒パートナーシップ」は，情報システム等の脆弱性について，その発見から，対策方法の策定，公表に至るまでの過程に関与する関係者に期待される行動基準を示すことにより，脆弱性関連情報を適切に流通させ，より迅速な対策方法の提供・適用を促す産官連携の枠組みである．行政庁の告示に基づく公的な制度として運用されているという点では，国際的にも例を見ない独特の制度として評価できるものであるが，脆弱性情報の取り扱いは，国際的な連携により実施することが必要となるものであることから，国際的な運用実務とも整合するかたちで運用されている．

本稿は，情報システムの脆弱性に関する「情報セキュリティ早期警戒パートナーシップ」の策定に至るまでの経緯や制度の概要，現在までの運用の状況等について解説を試みるものである．

◆脆弱性とは

「脆弱性」という言葉は，その使用目的に応じ，さまざまな定義で用いられるが，情報セキュリティの分野においては，いわゆるセキュリティホールの意味で使われることが多く，本稿においても，「ソフトウェア等において，コンピュータ不正アクセス，コンピュータウイルス等の攻撃によりその機能や性能を損なう原因となり得る安全性上の問題個所（Webアプリケーションにあっては，Webサイト運営者がアクセス制御機能により保護すべき情報等に誰もがアクセスできるような，安全性が欠如している状態を含む）」の意で用いる．「コンピュータ不正アクセス，コンピュータウイルス等の攻撃によりその機能や性能を損なう原因となり得る…」とする部分は，他者からの攻撃により攻撃が顕在化する特徴を示すものであり，脆弱性が一般的なバグとは区別して取り扱われるべきものであることを確認するものである．

◆脆弱性に関する情報の取り扱い上の問題

脆弱性は，本来，設計・開発段階において発見，回避されるべきものであるが，現在のソフトウェア等の設計・開発の状況において完全に回避することは難しいとされており，ソフトウェア等の脆弱性が発見される都度，製品開発者☆1等が修正プログラム（パッチ）や被害の回避方法（ワークアラウンド）を提供し，ユーザがそれを適用することで問題の解決が図られるのが通常である．Webアプリケーションの脆弱性については，Webサイ

☆1　ソフトウェア製品を開発した企業もしくは個人．また，ソフトウェア製品の開発，加工，輸入または販売に関して当該ソフトウェア製品の実質的な開発者と認められる者．ソフトウェア製品の開発者が外国の会社である場合は，そのソフトウェア製品の国内での主たる販売を行っている会社．

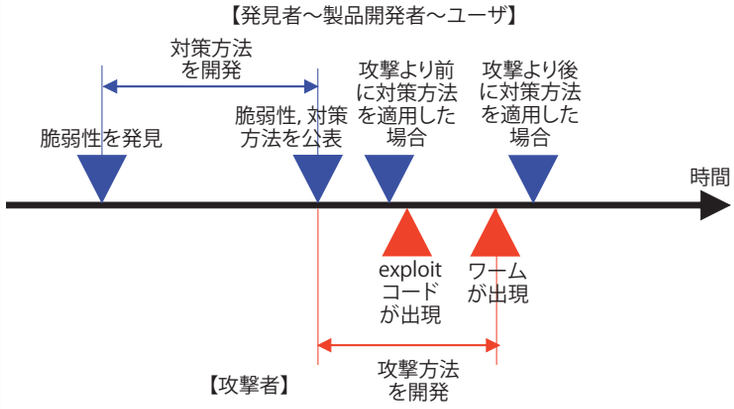


図 -1　脆弱性の発見から対策方法の適用までの流れ

トの運営者☆2が対策を自ら実施し，またはシステム構築受託者に依頼することで解決が図られる．

この，脆弱性の発見　→　製品開発者による対策方法（修正プログラムまたは回避方法をいう）の提供の流れが，悪意を持つ者に介入されることなく円滑に進めば，「脆弱性」を悪用する攻撃は生じないはずであるが，実際には，以下のような問題が発生する（図 -1 参照）．

① 発見された脆弱性に関する情報の暴露，流出

脆弱性に関する情報が，対策方法が提供される前に悪意を有する者に入手されてしまうと，対策方法が行き渡る前に exploit コード☆3やコンピュータウイルス等の攻撃方法☆4が出現するリスクを生むこととなり，脆弱性のあるソフトウェアを使用しているコンピュータ等が攻撃にさらされることとなる．このような事態は，たとえば，次のような場合に起こり得る．

- 発見者が，修正を促すためなどの目的で，脆弱性に関する情報を掲示板等に暴露してしまう．
- 発見者が，製品開発者やWebサイト運営者に脆弱性に関する情報を通知する負担（脆弱性を顕在化させるための条件設定や操作手順など詳細な説明が要求される，不正アクセス禁止法違反等発見の手段の適法性が問題とされるなど）を嫌い，発見した脆弱性に関する情報を放置してしまう．
- 発見者が脆弱性に関する情報を製品開発者等に通知しても，製品開発者またはWebサイト運営者がなんら対応をとらず，悪意を有する者がその脆弱性を察知，悪用してしまう．
- 発見された脆弱性が複数の種類の製品に影響を与えるものである場合に，一部の製品開発者が他の製品開発者に先んじて対策方法を公開してしまい，他の製品開発者の製品に関する対策方法の提供が間に合わないうちに，悪意を有する者が（対策方法を分析するなどにより）攻撃を開始してしまう．

② ユーザの対応が攻撃の開始に間に合わない（脆弱性の公表から攻撃方法の出現までの期間が短縮）

製品開発者が対策方法を提供しても，ユーザがそれを直ちに適用しなかった場合は，その脆弱性が悪意を有する者の攻撃にさらされることとなる．ユーザの対応が間に合わない原因としては，次のようなものが考えられる．

- ソフトウェアの脆弱性の公表からexploitコードやコンピュータウイルス等攻撃方法の出現までの期間が，急速に短くなってきている（たとえば，2003年2月に韓国のネットワークをダウンさせたSQL Slammerワームについては，脆弱性の対策方法の公表からワームの発生までに約半年の期間を要したが，2003年8月に発生したMS Blasterワームについては，脆弱性の対策方法が公表されてからわずか3週間強でワームが発生した）．
- ITが社会の隅々に行き渡った結果，さまざまなリテラシーレベルのユーザが存在するようになっており，これまでのような方法で製品開発者が対策方法を提供しても，十分に反応できないユーザ層が生じている．
- 他社製品を組み込む形での製品・システム開発が一般化しており，対策方法の適用の是非の判断に時間がかかる場合や対策の必要性にさえ気づかない場合が増えている．

☆2　そのWebサイトについて対外的に責任を有する事業者（個人の場合を含む）．依頼されてWebサイトの作成・運用を代行する事業者や第三者は含まない．
☆3　脆弱性を悪用するソフトウェアのソースコード．使い方によっては，脆弱性の検証に役立つこともある．
☆4　脆弱性を悪用してソフトウェアの動作に不具合を発生させるプログラムやコマンド，データおよびそれらの使い方．

◆脆弱性に関する情報の流通のあり方の検討

我が国においては，発見された脆弱性に関する情報を，発見者，製品開発者等の関係者がどのように取り扱うべきなのかという指針やガイドラインが存在しておらず，上記①のような問題にどう対処すべきかについてのルールが定まっていなかった．

また，上記②のような事情や，必要な者が必要なタイミングで脆弱性関連情報を入手できる仕組みが未整備であることから，製品開発者が対策方法を提供しても，ユーザレベルでの迅速な対策の適用につながりにくいとの問題もあった．

さらには，我が国では，特に汎用のソフトウェアにおいて国産製品の利用比率が高くないこともあり，脆弱性に関する研究が必ずしも活発でなく，脆弱性に関する情報の大半は海外に依存しているため，国産のソフトウェアの脆弱性検証は十分とはいえないとの問題もあった．

これらの問題に関し，2003 年 10 月に経済産業省が公表した「情報セキュリティ総合戦略」（産業構造審議会情報セキュリティ部会（部会長：寺島実郎（財）日本総合研究所理事長））は，「脆弱性に対処するためのルールと体制の整備」の必要性を提言している．

このような社会的要請の下，（独）情報処理推進機構（IPA）は，同年 11 月に「情報システム等の脆弱性情報の取扱いに関する研究会」（座長：土居範久中央大学教授）を設置し，JPCERT コーディネーションセンター（JPCERT/CC），（独）産業技術総合研究所（AIST），NPO 日本ネットワークセキュリティ協会（JNSA），ハード／ソフトウェアメーカ，セキュリティベンダなど，約 30 機関・50 人に参加いただき，脆弱性の発見から，通知（届出），評価・分析，適切な保護のもとでの情報流通，対策の策定，公表までの情報の取り扱いのあり方について，議論を重ね，2004 年 4 月にその検討結果を公表した（http://www.ipa.go.jp/security/fy15/reports/vuln_handling/index.html）．

この研究会における検討の成果は，その後のパブリックコメントの結果を踏まえた検討を経て，以下の告示およびガイドラインに結実し，「情報セキュリティ早期警戒パートナーシップ」として運用されることとなった．

① 平成 16 年経済産業省告示第 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 日制定，翌 8 日施行）：ソフトウェア製品または Web アプリケーションの脆弱性関連情報に関する基本的な処理の流れと，関係者（発見者，受付機関，調整機関，製品開発者，Web サイト運営者）に望まれる行動基準を規定（http://www.meti.go.jp/policy/netsecurity/downloadfiles/vulhandlingG.pdf）．

② 平成 16 年経済産業省告示第 236 号：ソフトウェア等脆弱性関連情報取扱基準における「受付機関」として IPA，「調整機関」として JPCERT/CC を指定．

③「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 日発表）：IPA，JPCERT/CC，（社）電子情報技術産業協会（JEITA），（社）情報サービス産業協会（JISA），（社）日本パーソナルコンピュータソフトウェア協会（JPSA）および NPO 日本ネットワークセキュリティ協会（JNSA）が，ソフトウェア等脆弱性関連情報取扱基準による枠組みに参画する関係者および関係業界としての指針を連名で発表．脆弱性関連情報に関する処理の流れや取り組む行動をより詳細に示すとともに，関係者が担う役割や推奨される事項を明示（図 -2）．また，法律専門家の見解をもとに発見者，製品開発者，Web サイト運営者等の関係者が留意すべき法的論点を整理（http://www.ipa.go.jp/security/ciadr/partnership_guide.pdf）．

④「製品開発ベンダ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（JEITA，JISA）」（2004 年 7 月 26 日概要版公表，2004 年 10 月 13 日本文公表）：JEITA と JISA が共同で公表．製品開発ベンダが，ソフトウェア等脆弱性関連情報取扱基準に基づいて，脆弱性関連情報取り扱いに関する社内体制や取扱手順を制定する際の最低要件とあるべき方向性を示す（http://it.jeita.or.jp/infosys/info/0407JEITA-guideline/index.html）．

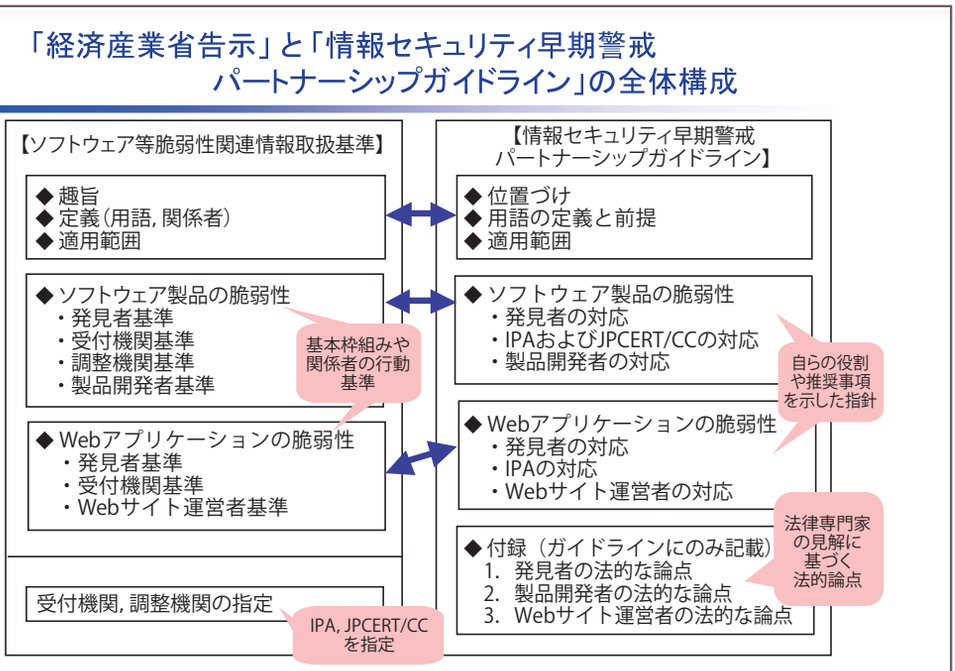
⑤「製品開発ベンダにおける脆弱性関連情報取扱に関する体制と手順整備のためのガイドライン（JPSA）」（2004 年 12 月 3 日公表）：パソコンソフトウェアベンダの事業の実態を考慮し，それにできるだけマッチする形を意識して，脆弱性関連情報に関する企業内においての取り扱いについて基本的な取り組みの枠組みを示す（http://www.jpsa.or.jp/info/04/20041203_security.html）．

情報セキュリティ早期警戒パートナーシップの概要

これらの告示やガイドラインに基づく「情報セキュリティ早期警戒パートナーシップ」の概要は，以下のとおりである．

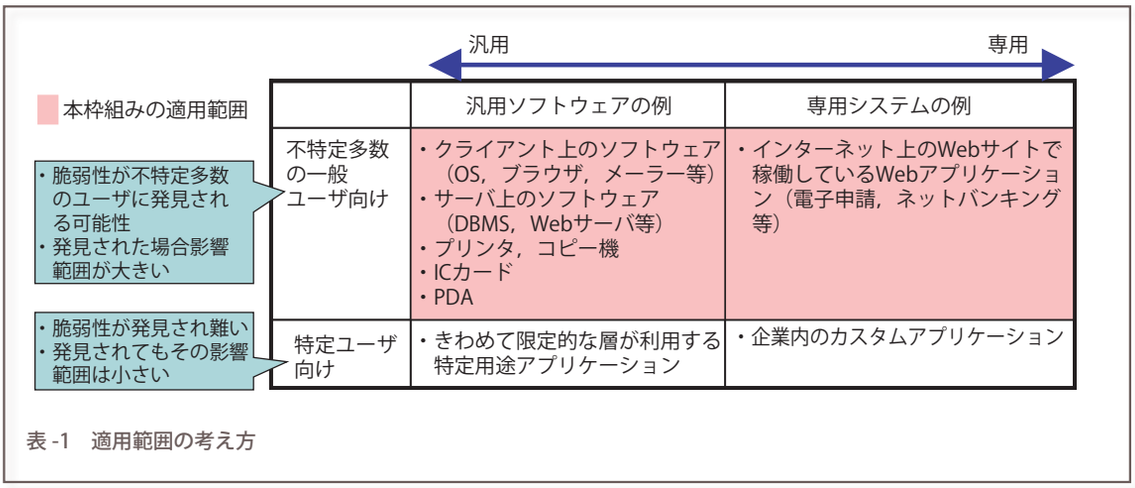
◆適用範囲

脆弱性が発見された場合の影響規模（不特定多数のユーザが影響を受けるか否か）の観点から，以下のもの



出典）「ソフトウェア等脆弱性関連情報取扱基準とガイドラインの概要説明」（脆弱性関連情報取り扱い説明会資料，経済産業省）より

図 -2　告示と早期警戒パートナーシップガイドラインの全体構成



	汎用ソフトウェアの例	専用システムの例
不特定多数の一般ユーザ向け	・クライアント上のソフトウェア（OS，ブラウザ，メーラー等） ・サーバ上のソフトウェア（DBMS，Webサーバ等） ・プリンタ，コピー機 ・ICカード ・PDA	・インターネット上のWebサイトで稼働しているWebアプリケーション（電子申請，ネットバンキング等）
特定ユーザ向け	・きわめて限定的な層が利用する特定用途アプリケーション	・企業内のカスタムアプリケーション

表 -1　適用範囲の考え方

を適用範囲としている☆5（表 -1）．

- 国内で利用されている汎用性を有するソフトウェア製品（市販のパッケージソフトウェアや共通に利用されるソフトウェア部品，組み込みソフトウェアを搭載したアプライアンス型のハードウェア等）および通信プロトコルや標準化されたフォーマットなどの仕様
- 国内においてアクセスされている Web サイトの Web アプリケーション

☆5　暗号アルゴリズムの脆弱性については，総務省および経済産業省により推進されている暗号技術評価プロジェクト「CRYPTREC」の活動において対応がなされていること，一般に理論的要素がきわめて強いことから，本枠組みでは積極的には扱わないこととしている．

◆取り扱う情報の種類と取り扱い方針

流通範囲を限定して慎重に取り扱うべき「脆弱性関連情報」（脆弱性，検証方法，攻撃方法）と，広く周知すべき「対策方法」（回避方法，修正方法）とでは，当然その取り扱いのルールが異なるべきであり，異なる方針で取り扱われる（表 -2）．

◆脆弱性関連情報の届出を受け付ける機関（受付機関）の設置：IPA を指定

脆弱性関連情報が放置されたり，不用意に暴露されたりすることを防ぐため，第三者機関が，脆弱性関連情報の届出を受け付け，発見者（または届出者）に代わって

情報の種類		内　容	取り扱い方針
脆弱性関連情報	脆弱性	ソフトウェア等において，コンピュータ不正アクセス，コンピュータウイルス等の攻撃によりその機能や性能を損なう原因となり得る安全性上の問題個所．Web アプリケーションにあっては，Web サイト運営者がアクセス制御機能により保護すべき情報等に誰もがアクセスできるような，安全性が欠如している状態を含む．	対策方法が公表されるまでは原則として公表しない．
	攻撃方法	脆弱性を悪用するプログラム，コマンド，データおよびそれらの使用方法．	公表しない．
	検証方法	脆弱性が存在することを調べるための方法	公表しない．
対策方法	回避方法	脆弱性を修正するのではないが，それが原因となって生じる被害を回避するための方法．ワークアラウンドと呼ばれる．	公表後迅速にユーザに流通させる．
	修正方法	脆弱性を修正する方法．	公表後迅速にユーザに流通させる．

表 -2　脆弱性関連情報の種類と取り扱い方針

製品開発者や Web サイト運営者への提供を行うこととした．これにより，脆弱性関連情報の通知に関する発見者の負担（脆弱性の立証や，発見方法の適法性が問題とされるリスク等）を軽減することが可能となる．

IPA は，すでに，経済産業省告示によりコンピュータウイルスおよび不正アクセスの届出受付機関に指定されているが，コンピュータウイルス，不正アクセス，脆弱性関連情報の間の境目が判然としない場合も少なくないため，ウイルス・不正アクセスと脆弱性関連情報とで届出受付機関が別になることは望ましくない．また，脆弱性に気づいた者が，脆弱性の存在を確認するために法令に違反する行為を行うことがないよう，脆弱性が存在する疑いがある段階での届出を受け付け，存否の確認は受付機関が行うこととしているため，自ら脆弱性の評価・検証をする能力を有する機関が受付機関となることが望ましいとの理由から，IPA が受付機関に指定された．

◆ソフトウェア製品の脆弱性の公表時期を調整する機関（調整機関）の設置：JPCERT/CC を指定

ソフトウェア製品の脆弱性の場合，1 つの脆弱性が複数の製品開発者の製品に影響する可能性があるため，脆弱性関連情報の提供を受けるべき製品開発者を特定し，各製品開発者の対策方法の策定の状況を把握して，一斉に公表を行うタイミングを調整する機関が必要となる．

JPCERT/CC は，米 CERT/CC や英 NISCC との関係を築き，それらから提供された脆弱性関連情報の国内流通について実績を積んでいることから，それを継続・発展させていくのが適当であり，また，国内で届け出られた脆弱性関連情報と外国からのコーディネーションに係る脆弱性関連情報とで調整者を別にすることは望ましくないことから，JPCERT/CC が調整機関に指定された．

なお，Web アプリケーションの脆弱性については，複数のサイト運営者間での調整が必要となることはないことから，脆弱性関連情報を受け付けた受付機関（IPA）が，直接，当該 Web サイト運営者に通知することとされた．

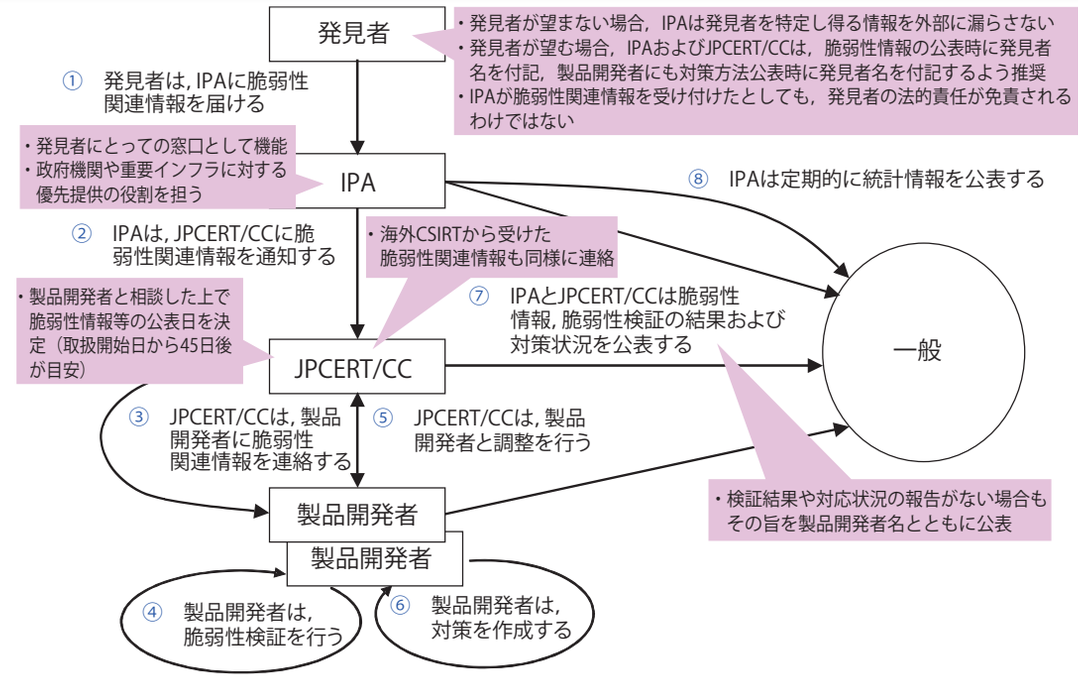
◆脆弱性関連情報の取り扱いに関する行動指針を提示

発見者に対しては，法令の遵守および対策方法が公表されるまでの間は第三者に脆弱性関連情報を漏洩しないよう協力を求め，製品開発者に対しては，調整機関との連絡窓口の登録，提供された脆弱性関連情報に関する迅速な検証，対策方法の一斉公表日の調整への協力を求め，Web サイト運営者に対しては，提供された脆弱性関連情報に関する迅速な検証・修正，個人情報の漏洩が発生した場合の適切な公表への協力を求めるなど，それぞれの関係者の行動指針を示すとともに，それぞれが留意すべき法的責任やこの枠組みに協力する意義に関する説明を行っている．

この場合における「発見者」とは，脆弱性を自ら発見者した者に限らず，情報が暴露されていることを知った者をも含むこととされており，また，「製品開発者」には，①ソフトウェア製品を開発した者（企業もしくは個人）のほか，②ソフトウェア製品の開発，加工，輸入または販売に関して当該ソフトウェア製品の実質的な開発者として認められる者（たとえば，外国の会社が開発したソフトウェア製品について，外国の開発元の代理として国内の子会社または販売代理店等の販売を行っている会社等，海外の開発元に対策方法の策定を働きかけることができる影響力を有する者）も該当するとの整理が行われている．

◆ソフトウェア製品に関する脆弱性関連情報の流通体制

関係者が上記行動基準に従って行動する場合，ソフトウェア製品に関する脆弱性関連情報は，図 -3 のように



出典）「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」，IPA, JPCERT/CC, JEITA, JPSA, JISA, JNSA（2004年7月8日）

図 -3　ソフトウェア製品の場合の脆弱性関連情報流通体制

取り扱われることとなる．

① 発見者から届出があった場合

脆弱性関連情報の届出は，PGP 暗号鍵により暗号化した電子メールまたは IPA の Web サイト上の Web 届出フォームへの入力により行うことができる（http://www.ipa.go.jp/security/vuln/report/index.html）．受付機関に届け出られた脆弱性関連情報は，本枠組みの取り扱い対象となるか否か，既知の脆弱性ではないか等の審査を経て調整機関に通知され，調整機関を介して当該脆弱性関連情報に関連すると予想される製品開発者に提供される．製品開発者はその影響を検証し，その結果をフィードバックするとともに，対策方法の策定についてのスケジュールを調整機関と相談する．製品開発者が作成した対策方法は，調整機関によって調整された公表日に一斉に公表される．

② 海外 CSIRT から脆弱性関連情報のコーディネーションを受けた場合

海外 CSIRT から通知された脆弱性関連情報は，調整機関から当該脆弱性関連情報の影響が予想される製品開発者に提供される．製品開発者はその影響を検証し，その結果をフィードバックするとともに，対策方法の策定についてのスケジュールを調整機関と相談する．製品開発者が作成した対策方法は，調整機関によって調整された公表日に一斉に公表される．

◆ Web アプリケーションに関する脆弱性関連情報の流通体制

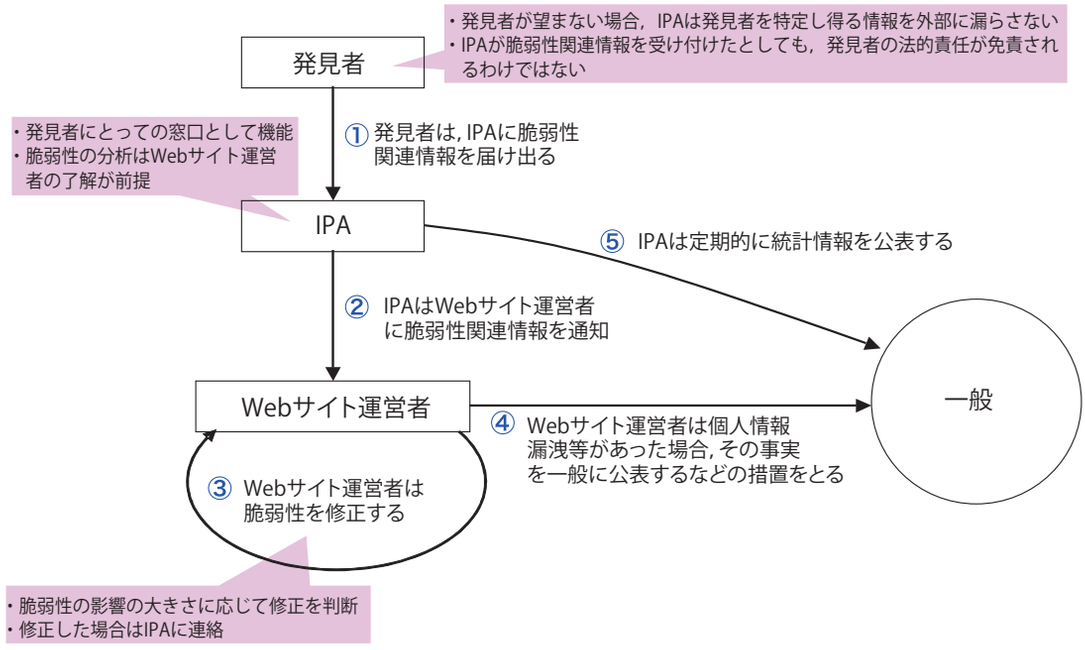
関係者が上記行動基準に従って行動する場合，Web アプリケーションに関する脆弱性関連情報は，図 -4 のように取り扱われることとなる．

脆弱性関連情報の届出は，PGP 暗号鍵により暗号化した電子メールまたは IPA の Web サイト上の Web 届出フォームへの入力により行うことができる（http://www.ipa.go.jp/security/vuln/report/index.html）．届け出られた脆弱性関連情報は，受付機関が確認の上，当該 Web サイト運営者に通知し，検証・修正を求める．受付機関は，Web サイト運営者の求めに応じ，届出に係る脆弱性が修正されたかどうかを検証する．

◆脆弱性関連情報，製品開発者の対応状況の公表

JPCERT/CC および IPA は，脆弱性情報ならびに JPCERT/CC から連絡したすべての製品開発者の脆弱性検証の結果と対応状況（脆弱性検証の結果の報告および対応状況の報告がない場合は，その旨），公表後に製品開発者から提供された追加情報をインターネット上で公表すべきこととされている．

これらの情報は，JPCERT/CC と IPA が共同で運営している「JP Vendor Status Notes（JVN）」において，米国 CERT/CC および英国 NISCC から調整のあった脆弱性関連情報とともに公表されている（http://jvn.jp/）．



出典）「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」，IPA, JPCERT/CC, JEITA, JPSA, JISA, JNSA（2004年7月8日）

図 -4　Web アプリケーションの場合の脆弱性関連情報流通体制

	2004 年 第 3 四半期	2004 年 第 4 四半期	2005 年 第 1 四半期	合計
ソフトウェア製品に関する届出	19	13	12	44
Web アプリケーションに関する届出	73	67	71	211
合　計	92	80	83	255

表 -3　脆弱性関連情報の期別届出件数の推移

運用の状況（2004 年 7 月から 2005 年 3 月まで）

◆届出状況に関する統計情報

受付機関である IPA は，脆弱性にかかわる実態を周知徹底し，危機意識の向上を図るため，受け付けた脆弱性関連情報に関する統計情報を定期的に公表すべきこととされており，現時点においては，IPA と JPCERT/CC が連名で，四半期ごとに統計情報を公表している．

2004 年 7 月 8 日の運用開始から 2005 年 3 月までの届出受付状況は，表 -3 のとおり，ソフトウェア製品に関する届出が累計で 44 件（うち脆弱性の公表に至ったものは，17 件），Web アプリケーションに関する届出が累計で 211 件（うち脆弱性の修正が完了したものは，90 件）となっている．

運用開始から 9 カ月弱の間の届出件数としては，順調な立ち上がりであろう．また，我が国で発見された脆弱性について，外国に向けてハンドリングを行う案件も増えており，国際的な貢献の実績も上がってきているところである．

ソフトウェア製品の脆弱性関連情報の届出の処理状況は，図 -5 のとおりであり，Web アプリケーションの脆弱性関連情報の届出の処理状況は，図 -6 のとおりとなっている．Web アプリケーションに関し，「取り扱い不能」とされているものが 29 件存在するが，これは，Web サイト運営者が本枠組みを認知しておらず，受付機関からの連絡に取り合わないなどの事情で，届出に係る脆弱性関連情報を Web サイト運営者に提供することができない状況にあるものなどの件数である．

ソフトウェア製品に関する届出の製品種類別の内訳は，図 -7 のとおりである．総数が少ないため，いまだ統計的な価値は十分ではないものと考えられるが，Web ブラウザ，アンチウイルスソフト，メールクライアントソフト，グループウェア等が他に比して多く，情報家電（HDD-DVD）や携帯機器も対象となっている．

届け出られた脆弱性の，種類別内訳は図 -8，脅威別内訳は図 -9 のとおりである．脆弱性の種類では「クロ

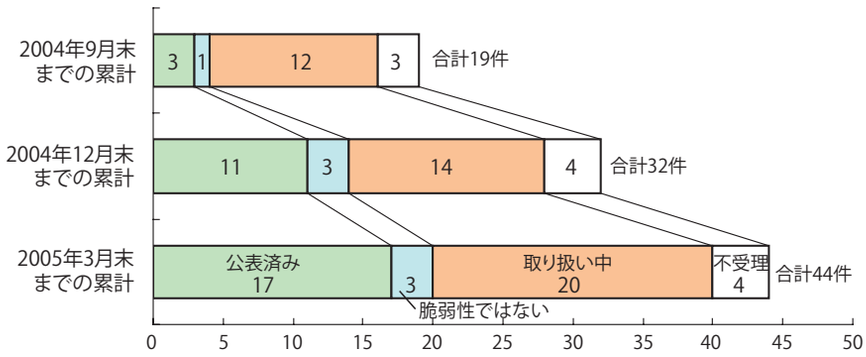


図 -5　ソフトウェア製品脆弱性関連情報の届出の処理状況

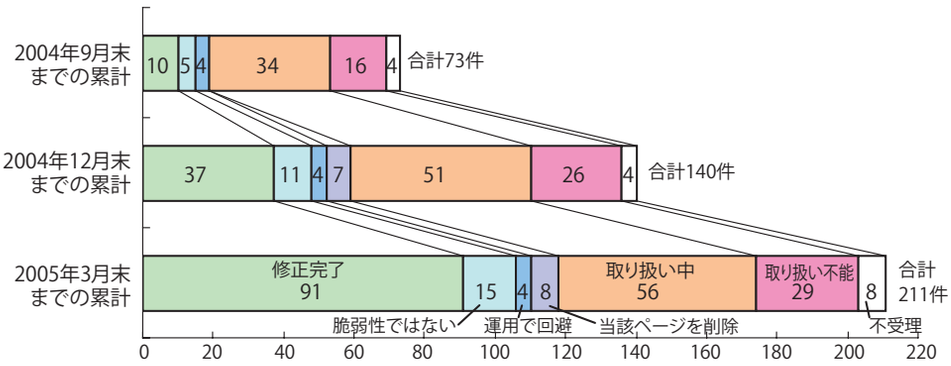


図 -6　Web アプリケーション脆弱性関連情報の届出の処理状況

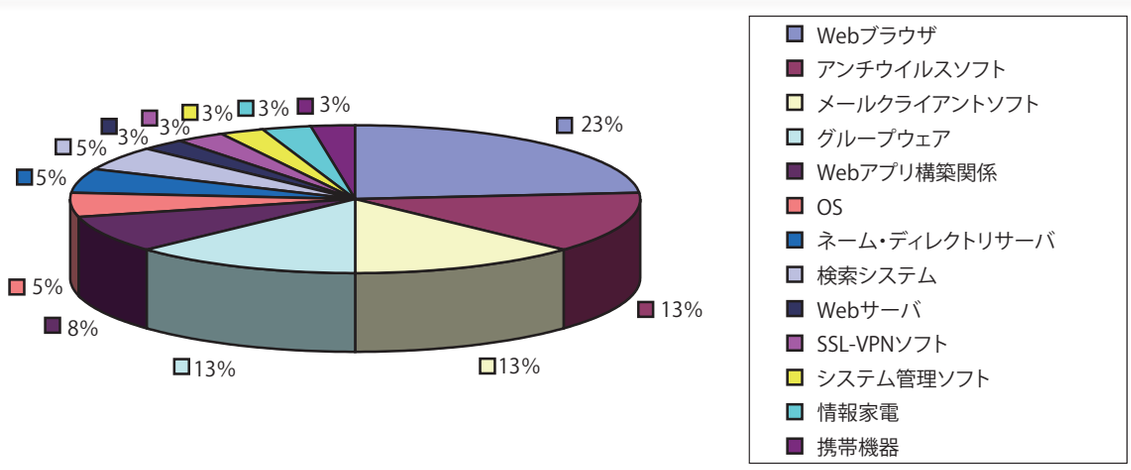


図 -7　ソフトウェア製品種類別の届出件数の内訳（届出開始から 2005 年 3 月末まで）

スサイト・スクリプティング」が最多であり，発見者が届出時に想定した脅威別でも，この脆弱性により起こり得る「Cookie 情報の漏洩」が最多となっている．なお，この脆弱性の分類については，各四半期ごとの届出状況に関する報告中の付表をご参照いただきたい（http://www.ipa.go.jp/security/vuln/report/documents/vuln2005q1.pdf）．

◆製品開発者リストへの登録状況

JPCERT/CC は，原則として，「製品開発者リスト」に登録されている製品開発者に対し，該当製品に関する脆弱性関連情報を提供し，一斉公表日の調整等を行うが，同リストに登録されている者のうち，42 社が社名を公表している（http://jvn.jp/nav/index.html）．このリストに載ることが，「脆弱性問題に前向きに取り組んでい

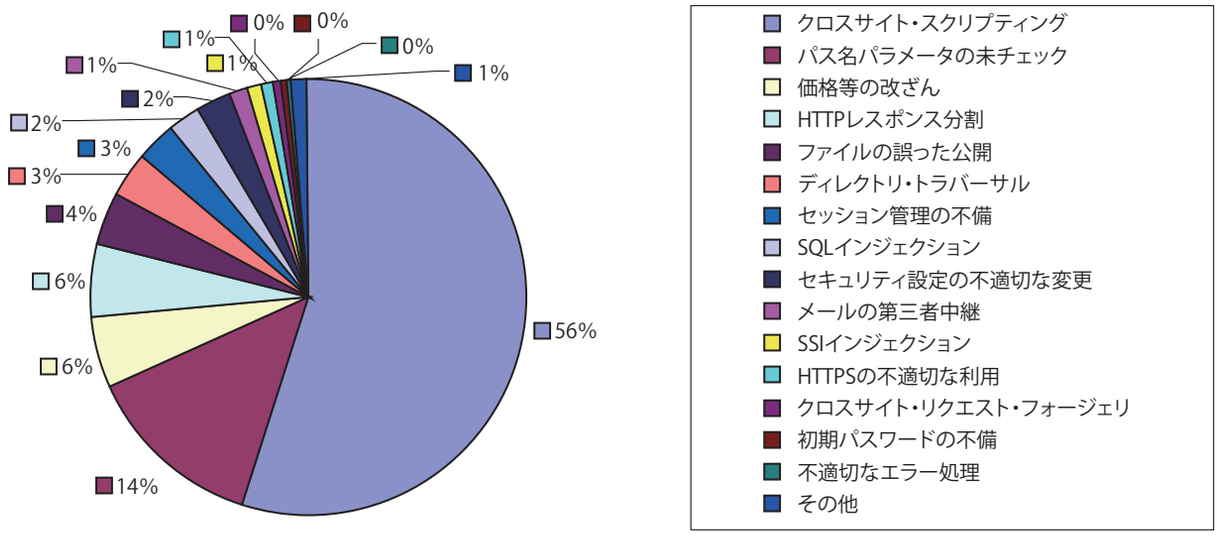


図 -8　Web アプリケーションの脆弱性種類別内訳（届出開始から 2005 年 3 月末まで）

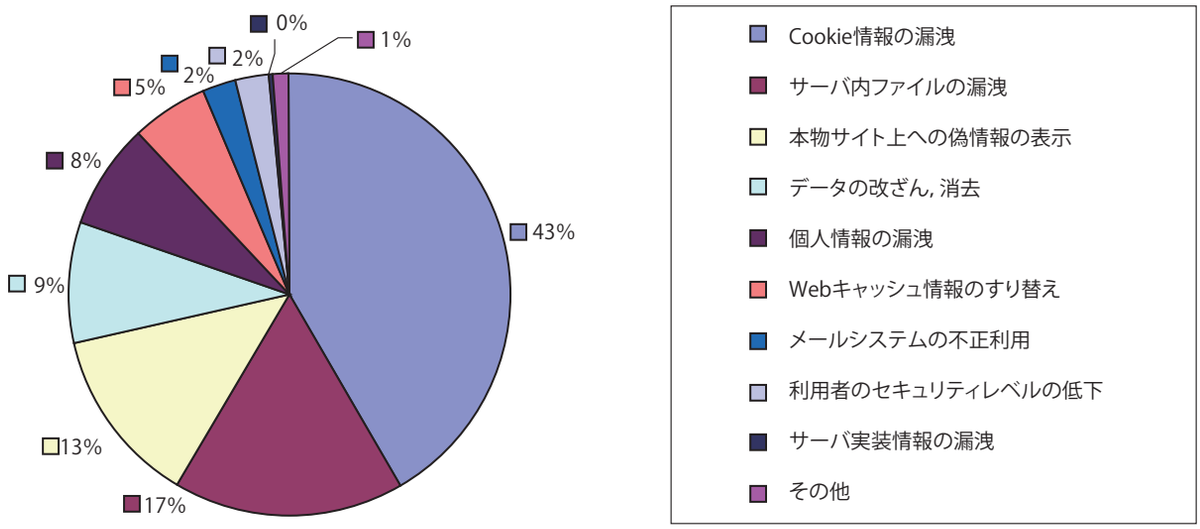


図 -9　Web アプリケーションの脆弱性脅威別内訳（届出開始から 2005 年 3 月末まで）

る企業」のステータスとして評価されるよう市場の意識の醸成を行っていくことで，この枠組みに参加する製品開発者を増加させ，情報の提供漏れが生じない体制を作っていくことが期待される．

運用の過程において顕在化した検討を要する事項

この 9 カ月間の「情報セキュリティ早期警戒パートナーシップ」の運用の過程において，当初深く意識されていなかった，以下のような問題が顕在化した．もとより，トライ・アンド・レビューを前提として，試行運用の位置づけで運用を開始した枠組みであり，運用を継続する中で，さまざまな改善点が生じるものと考えられるところ，関係者との意見交換等を通じて，より効果的な枠組みに発展させていくことが期待される．

◆情報家電・ネットワーク家電・オフィス関連機器

ソフトウェア製品の脆弱性には，純粋なソフトウェア製品のほかに，ソフトウェアを組み込んだハードウェアやプロトコルの実装にかかわる脆弱性が含まれており，いわゆるネットワーク家電に組み込まれているソフトウェアもこの枠組みの対象となり得る．これらの製品については，利用に際してユーザがセキュリティを意識していない場合が多く，また，対策（例：パッチの適用）の実施が技術的な観点から困難であったり，製造物責任法の適用の問題があったりして，情報システムと同様の

枠組みでは対処しきれない場面が多い．今後，この分野の開発者や製品流通の担当者等を交えて検討を進めることが必要となる．

◆製品開発者自身による自社製品に関する脆弱性の発見

現在の告示・ガイドラインによれば，製品開発者が，自社製品について，他社製品にも影響を及ぼし得る脆弱性関連情報を発見したときは，「発見者」としてその脆弱性関連情報を受付機関に届け出るよう奨励しているところであるが，いったん脆弱性として届け出てしまうと，一斉公表日までの間は，対策方法を自社製品の顧客に提供することができなくなってしまう．このような結果は，せっかく脆弱性を発見した製品開発者にとっては切ないものとなり，届出を躊躇させる要因ともなりかねないことから，取り扱いについて検討を行うことが必要となろう．

◆Webアプリケーションの脆弱性か，ソフトウェア製品の脆弱性か．

電子申請システムを利用するためのアプリケーションをダウンロードするためのインストーラーのような，Webアプリケーションとソフトウェア製品との境界事例や，Webアプリケーションの脆弱性として受け付け，手続きを開始したが，調査の過程で原因がソフトウェア製品の脆弱性にあることが判明した場合など，現在の手続きのみでは処理しきれない場面について，適切な運用手続きを検討をする必要がある．

◆その他

ソフトウェア製品の脆弱性については，調整機関が調整する公表日が対応期限の目安となるが，Webアプリケーションについては，対応する期限が定まっておらず，対応の状況が公表されるわけでもないため，サイト運営者の対応のスピードはまちまちで，脆弱性のあるWebサイトが放置されたままとなる可能性もある．このような事案に対応するため，Webアプリケーションに係る脆弱性関連情報の取り扱いについても，対応期間の目安の設定や脆弱性情報の公表を検討すべきであるとする意見がある．

また，製品開発者に提供される脆弱性情報について，緊急度や危険度等の情報の付加を求める声がある．

さらには，脆弱性関連情報と対応状況の公開に関し，①JVNにおける情報公開の内容が十分ではない，②JVNのリンク先（製品開発者のサイト等）における情報公開の内容について，製品開発者間で差があり過ぎるため，なんらかのガイドやモデルを提供すべきである，との意見がある．

今後の課題：ユーザへの迅速な対策情報の提供

現時点における「情報セキュリティ早期警戒パートナーシップ」は，製品開発者による対策方法の作成・公表までの行動基準を指針として示しているが，その対策方法をユーザに迅速かつ正確に伝える仕組みについては，まだ確立していない．個人ユーザに対する関係についてはセキュリティ対策推進協議会（SPREAD）☆6の活動状況を，重要インフラに対する関係については内閣官房情報セキュリティセンター（NISC）☆7や事業者間における合意形成の状況を見守りつつ，システムインテグレータや企業ユーザの意向も踏まえながら，検討を継続する必要がある．

参考文献

1）経済産業省のWebサイト「脆弱性情報取扱体制」のページ：http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html
2）(独)情報処理推進機構(IPA)のWebサイト　セキュリティセンター「脆弱性関連情報の取扱い」のページ：http://www.ipa.go.jp/security/vuln/index.html および「脆弱性関連情報に関する届出について」のページ：http://www.ipa.go.jp/security/vuln/report/index.html
3）JP Venders Status NotesのWebサイト：http://jvn.jp/
4）JPCERTコーディネーションセンターのWebサイト「脆弱性情報コーディネーション」のページ：http://www.jpcert.or.jp/vh/

（平成17年5月12日受付）

☆6 Security Promotion Realizing sEcurity meAsures Distribution：日本ネットワークセキュリティ協会，Telecom-ISACJapanを中心に，ハードウェア・ソフトウェアメーカ，インターネットサービスプロバイダ，システムインテグレータ，量販店，メディア，各種コミュニティや政府関連機関など，コンピュータ，インターネットに関係するさまざまな業界の団体と密接に連携することにより，公開された脆弱性情報や対策情報などのセキュリティ関連情報を「わかりやすく」「迅速に」「確実に」インターネット利用者に流通させる活動を行う（http://www.spread-j.org/）．

☆7 National Information Security Center (http://www.bits.go.jp/).