

平成16年10月18日

経済産業省

ソフトウェア等の脆弱性関連情報に関する届出状況の公表について

～制度スタート後、初の届出受付・処理状況の公表～

独立行政法人情報処理推進機構（IPA）及び有限責任中間法人JPCERTコーディネーションセンター（JPCERT/CC）は、「ソフトウェア等脆弱性関連情報取扱基準」（経済産業省告示）に基づき、脆弱性関連情報の届出受付・調整・公表を実施しているが、このたび7月8日の運用開始から9月末までの約3ヵ月間の状況を取りまとめた。

当該取りまとめ結果によれば、約3ヶ月間で90件を超える届出があったこと、日本で発見された脆弱性情報をもとに国際連携・対処を実施したこと、日本製の情報家電製品に脆弱性が発見されたことなどが明らかになっている。

経済産業省としては、引き続きIPA及びJPCERT/CCの活動を支援するとともに、普及啓発にも取り組み、「情報セキュリティ早期警戒パートナーシップ」¹の拡充・強化に努めてまいりたい。

1. 概要

コンピュータウイルス・不正アクセス等の攻撃は、ソフトウェア製品やウェブサイトに内在する安全性上の問題箇所（脆弱性）を悪用して行われることが多い。このため経済産業省は、脆弱性関連情報の届出受付・調整・公表に係る制度につき、本年7月7日に「ソフトウェア等脆弱性関連情報取扱基準」（経済産業省告示）を制定した。

当該基準に基づき脆弱性関連情報の受付機関を担当するIPA及び調整機関を担当するJPCERT/CCでは、本年7月8日の運用開始から9月末までの約3ヵ月間の脆弱性関連情報の届出受付、ソフトウェア等の製品開発者及びウェブサイト運営者との調整、並びに脆弱性に関する対策情報の公表等の状況を取りまとめた（別紙1参照）。

2. ポイント

約3ヵ月間で90件超の届出

受付機関であるIPAでは、本制度の運用開始から9月末までの約3ヶ月間で、計92

¹ 「ソフトウェア等脆弱性関連情報取扱基準」に基づく官民連携の枠組み全体を指す（別紙2参照）。

件（ソフトウェア製品：19件、ウェブアプリケーション：73件）の脆弱性関連情報の届出を受け付けた。運用開始当初にもかかわらずこれだけの件数に達したことは、我が国のソフトウェア等において対処すべき脆弱性の問題が多数存在することを示しており、本制度の強化は我が国IT社会の安全性向上において極めて重要と言える。

日本で発見された脆弱性情報をもとに国際連携・対処を実施

ソフトウェア製品の脆弱性に関する届出のうち3件については、製品開発者による対策策定が完了し、「対策情報」が公表された。このうちの1件は、海外も含めた複数の製品開発者に関係する脆弱性であったため、調整機関である JPCERT/CC が海外の調整機関を介して、製品開発者への通知や脆弱性情報の公表時期等に関する国際的な調整を行った。これは、本制度を通じて届け出られた脆弱性情報が日本から海外に発信された初めてのケースである。コンピュータウイルス・不正アクセス等の攻撃は国境を超えて行われることから、このような国際連携・対処を一層強化していくことが重要である。

日本製の情報家電製品にも脆弱性発見

インターネットに接続できる日本製家電製品（HDD&DVDビデオレコーダー）に脆弱性が発見され、その対策が公表された。このように、脆弱性の問題は、インターネットに接続可能な家電製品、事務機器、携帯電話等においても発生し得ることから、既に連携が進みつつあるコンピュータ等の分野²だけではなく、今後家電製品メーカー等との連携も進めていくことが重要である。

（本発表資料のお問い合わせ先）

商務情報政策局 情報セキュリティ政策室

担当者：川口、佐藤

電話：03-3501-0397（直通）

² 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）「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」（2004年10月13日）
<http://it.jeita.or.jp/infosys/info/0407JEITA-guideline/index.html>

ソフトウェア等の脆弱性関連情報に関する届出状況 [2004年第3四半期(7月～9月)]

独立行政法人 情報処理推進機構(略称:IPA)及び有限責任中間法人 JPCERT コーディネーションセンター(略称:JPCERT/CC)は、2004年第3四半期(7月～9月)の脆弱性関連情報届出状況を、以下のとおり、とりまとめました。

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」(平成16年経済産業省告示 第235号)に基づき、IPAは2004年7月8日より脆弱性関連情報の届出の受付を開始し、JPCERT/CCは日本国内の製品開発者などの関連組織との調整を行いました。ソフトウェア製品の脆弱性については、19件の届出のうち、3件について製品開発者による対策が完了し、公表されました。このうちの1件は、JPCERT/CCが海外CSIRT¹と連携し、海外の製品開発者も含めて調整をしたものです。ウェブアプリケーションの脆弱性については、73件の届出のうち、10件について修正が完了しました。

1. 届出件数

2004年7月8日から9月30日までのIPAへの脆弱性関連情報の届出件数は、総計92件(ソフトウェア製品に関するもの19件、ウェブアプリケーションに関するもの73件)でした。月別の届出状況を表1-1に示します。

表 1-1 脆弱性関連情報の月別の届出状況

	2004年 7月	2004年 8月	2004年 9月	合計
ソフトウェア製品に関する届出	7	7	5	19
ウェブアプリケーションに関する届出	17	36	20	73
合計	24	43	25	92

(1) ソフトウェア製品の脆弱性

ソフトウェア製品の脆弱性については、対策を終了し公表されたものが3件、製品開発者により脆弱性ではないと判断されたものが1件あります。また、告示で定める届出の対象に該当せず、取扱い対象外としたものが3件あります。この3件の内訳は、製品の仕様であり脆弱性ではないと判断されたものが2件、届出時に公知の情報だったものが1件となっています。

(2) ウェブアプリケーションの脆弱性

ウェブアプリケーションの脆弱性については、修正を完了したものが10件、脆弱性を運用で回避したものが4件、ウェブサイト運営者により脆弱性はないと判断されたものが5件あります。取扱い対象外としたものの内訳は、届出時に既に修正済みであったものが1件、日本国内からのアクセスを想定したウェブサイトでないものであったものが3件でした。このほか、16件が、ウェブサイト運営者と連絡が取れず、取扱いができない状態(取扱い不能)となっています。

¹ Computer Security Incident Response Team の略であり、コンピュータセキュリティに関するインシデント(事故)への対応や調整、サポートをするチームのことです。

届出の取扱い状況を図 1-1 に示します。

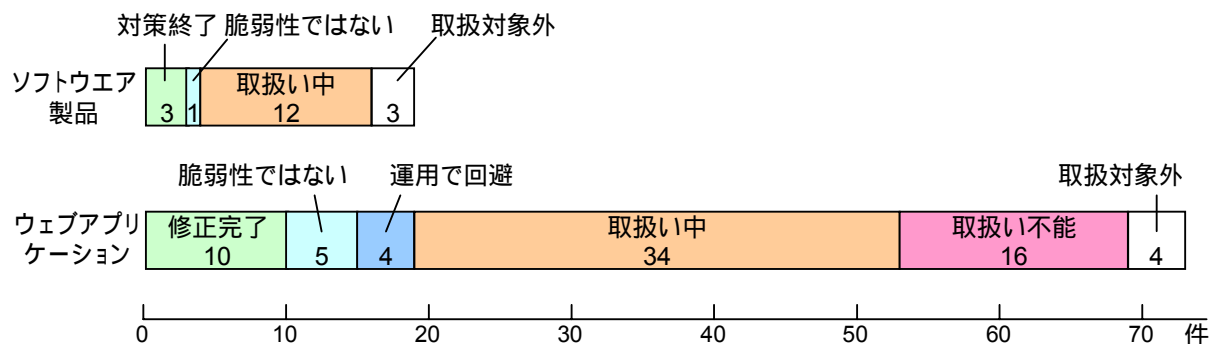


図 1-1 脆弱性関連情報の届出の取扱い状況

2. ソフトウェア製品の脆弱性関連情報の届出

JPCERT/CC が日本国内の製品開発者などの関連組織との調整を行ない、公表した脆弱性関連情報は 7 件です。このうち、IPA への届出により手続きを開始した脆弱性関連情報は 3 件であり、そのうちの 1 件である「SSL-VPN 製品における Cookie の脆弱性」については、海外 CSIRT とのパートナーシップに基づき、海外開発者も含めて調整しました。これは、企業内システムを社員が外出先からインターネット経由で利用できるようにする VPN (Virtual Private Network) を、従来よりも手軽に実現するものとして近年注目を浴びてきた「SSL-VPN」製品に対し、その使い方によっては、必ずしも VPN ほどの堅牢な安全性が確保されるとは限らないことが指摘されたものです。一部の製品には、一般的なウェブアプリケーションにみられる脆弱性と同種の欠陥を有するものがあり、パケット盗聴によるセッションハイジャック攻撃を許してしまうものがありました。

他の 4 件は、海外 CSIRT からの脆弱性情報について JPCERT/CC が日本国内の製品開発者との調整を行ったものです。

製品開発者の対応状況は、IPA と JPCERT/CC が共同運営している対策情報ポータルサイトである JP Vendor status Notes (JVN) において公開しています。(URL: <http://jvn.jp/>)

表 2-1 に、IPA に届出があり、対策が完了し公表した脆弱性を示します。

取扱い対象の届出 16 件のうち、複数の製品開発者のソフトウェア製品に影響がある脆弱性の届出は 2 件あり、これらは、JPCERT/CC が複数の製品開発者に対して調整を行いました。特定製品の脆弱性関連情報の届出は 14 件であり、アンチウイルスソフトやメールソフトなどのクライアント製品が多くありました。また、情報家電において、アクセス制御機能が適切に機能していない問題も 1 件ありました。特定製品の脆弱性の製品種類別の内訳を図 2-1 に示します。

表 2-1 対策が完了した届出

種類	脆弱性の概要	JVN 公表日
1 SSL-VPN 製品における Cookie の脆弱性	SSL-VPN 製品について、SSL のクライアント認証を使用せずに、ユーザ名とパスワードでログインするモードを使用している場合に、Cookie 情報が漏洩し、セッションハイジャックされる可能性があります。これは、複数製品に関わる脆弱性であり、海外製品開発者も含めて調整されました。	2004 年 9 月 30 日
2 desknet's の脆弱性	株式会社ネオジャパンのウェブグループウェアである desknet's に関して、ユーザが悪意のあるスクリプトを含んだ HTML メールやインフォメーション(掲示板に相当する機能)を参照した場合には、スクリプトが実行されます。結果として、Cookie 情報(設定によっては ID やパスワードを含む)の漏洩によるなりすましや個人情報の漏洩などが発生する可能性があります。	2004 年 9 月 24 日
3 ウィルスバスターコーポレートエディションの脆弱性	トレンドマイクロ株式会社の企業向け総合セキュリティ対策ソフトウェアであるウィルスバスターコーポレートエディションに関して、管理コンソールに問題があり、特定の URL を指定すると OPP.ini ファイル(Outbreak Prevent Policy の設定ファイル)を閲覧できます。	2004 年 9 月 3 日

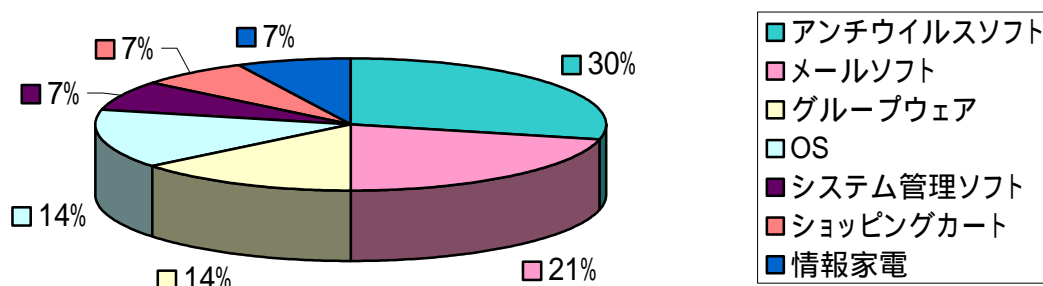


図 2-1 ソフトウェア製品種類別の届出内訳

3. ウェブアプリケーションの脆弱性関連情報の届出

ウェブアプリケーションについては、19 件の届出について取扱い終了しました。内訳としては、修正を完了したものが 10 件、脆弱性を運用で回避しているものが 4 件、ウェブサイト運営者により脆弱性が存在しないと判断されたものが 5 件です。修正や回避等により、最終的に脆弱性に対処したものは 19 件中 14 件ですが、取扱い中のものにも、修正完了の報告を受け IPA による修正確認中のものが 4 件あります。

修正された届出の脆弱性の種類別の修正件数および修正に要した日数を表 3-1 に示します。

表 3-1 脆弱性の種類別の修正件数および修正日数

脆弱性	件数	修正日数
クロスサイト・スクリプティング(第三者へのスクリプト実行)	9	平均 15 日
パス名パラメータの改ざん(フォーム入力値の改ざん)	3	当日、3 日、16 日
ファイルの誤った公開	1	21 日
SQL インジェクション(データベースへの不正な入力)	1	39 日

脆弱性の種類別内訳を図 3-1 に、想定される脅威別内訳を図 3-2 に示します。脆弱性の種類は、「クロスサイト・スクリプティング²」が最も多く、ユーザからの入力を十分にチェックしていないウェブサイトが多いことがわかります。次いで「パス名パラメータの未チェック」が多くなっていますが、これは、あるウェブアプリケーション部品が多くのウェブサイトで使用されていたことによります。

脆弱性から想定される脅威は、「サーバ情報の漏洩」が最も多く、次いで「Cookie³情報の漏洩」でした。利用者の識別に Cookie 情報が使われている場合には、Cookie 情報の漏洩により、なりすましや個人情報漏洩につながる可能性があります。アクセス制御の欠如や回避の脆弱性がある場合にも、個人情報を含むファイルがサーバ上にあれば、情報漏洩する可能性があります。実際に、修正が完了した 2 件のウェブサイトからも、個人情報漏洩する可能性があった、との報告がありました。

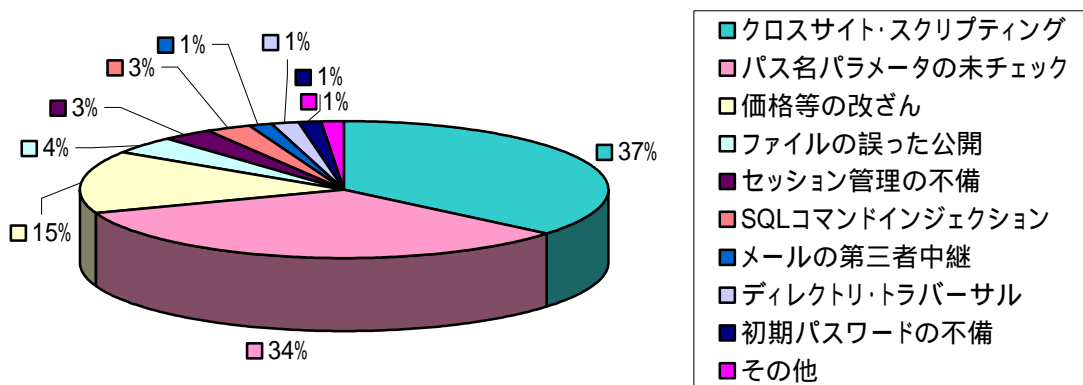


図 3-1 ウェブアプリケーションに関する脆弱性関連情報の届出の種類別内訳

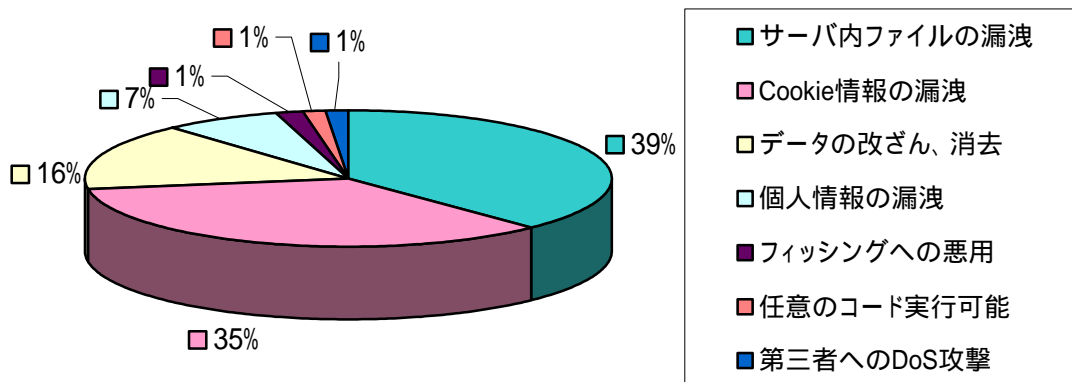


図 3-2 ウェブアプリケーションに関する脆弱性関連情報の届出の脅威別内訳

² 脆弱性の説明については付録を参照してください。

³ ウェブサーバが発行し、ウェブブラウザに預ける小さなテキストデータです。いったん Cookie を預かったウェブブラウザは、それを発行したウェブサーバのコンテンツにアクセスする際、預かった Cookie のデータをコンテンツの要求に必ず含めるようになります。

4. 皆様へのお願い

届出の受付開始から約3ヶ月が経過しましたが、脆弱性の修正をより強く促進していくために、関係者の皆様に、以下のとおり、ご協力をお願いします。

- ウェブサイト運営者の皆様へ

ウェブアプリケーションの作成時には、重要な情報はブラウザ側に送らない設計にし、入力フォーム等へのユーザからの入力に対しては、スクリプトや命令を含んでいないかどうかを十分にチェックしてください。

IPA からの連絡はウェブサイトに記載のある窓口に対して、電子メールまたは電話で行っています。本制度の趣旨をご理解のうえ、窓口の明確化および連絡があった場合のご協力をお願いします。IPA からの連絡について、本当に IPA からの連絡かどうか等の疑問を感じられた場合は、メール(vuln-inq@ipa.go.jp)もしくは電話(03-5978-7527)にて、ご連絡ください。

- 製品開発者の皆様へ

JPCERT/CC は、ソフトウェア製品の脆弱性関連情報について、整備している「製品開発者リスト」に基づき、一般公表日の調整等を行います。迅速な調整を進められるよう、「製品開発者リスト」への登録にご協力ください。(URL: <http://www.jpccert.or.jp/>)

- 脆弱性を発見された皆様へ

脆弱性を発見した場合は、匿名掲示板などに書き込むことは避け、この届出制度を利用してください。また、届出した情報は、その脆弱性に関する情報が悪意のある者に利用されることを避けるため、開発者等により対策情報が公表されるまで、公表しないよう、お願いします。

- 一般インターネットユーザの皆様へ

JVN や IPA、JPCERT/CC など、脆弱性情報や対策情報を公表しているウェブサイトを参照し、パッチの適用など、自発的なセキュリティ対策を日ごろから心がけてください。

■ お問い合わせ先

独立行政法人 情報処理推進機構 セキュリティセンター

Tel:03-5978-7527 Fax:03-5978-7518

E-mail: vuln-inq@ipa.go.jp

有限責任中間法人 JPCERTコーディネーションセンター

Tel:03-3518-4600

E-mail: office@jpccert.or.jp

付表 ウェブアプリケーション脆弱性の分類

脆弱性の種類	深刻度	説明	届出において 想定された脅威
ファイルの誤った公開	高	一般に公開すべきでないファイルが公開されており、自由に閲覧できる状態になっている	サーバ内ファイルの漏洩 個人情報の漏洩
パス名パラメータの未チェック	高	パス名(ファイル名)を指定する CGI パラメータに、ウェブサーバ上の任意のディレクトリのファイルを指定できてしまう	サーバ内ファイルの漏洩
ディレクトリ・トラバーサル	高	ウェブサーバ上のディレクトリのアクセス権を超えて、本来許可されている範囲外のディレクトリに相対的にアクセスできる	サーバ内ファイルの漏洩
セッション管理の不備	高	セッション管理用のパラメータにおいて、秘密情報が含まれておらず、容易に予測ができる	個人情報の漏洩 権限の無い者によるサービス利用
SQL コマンドインジェクション	高	入力フォームへ SQL コマンド(データベースへの命令)を入力し、実行させることができる	サーバ内ファイルの漏洩 データの改ざん、消去
クロスサイト・スクリプティング	中	悪意のあるスクリプトをウェブサイトへの入力中に記述し、第三者に対し悪意のある行為を仕掛けることができる	Cookie 情報の漏洩 本物サイト上への偽情報の表示
メールの第三者中継	低	他人のメールサーバを用いて、メールを送信することができる	第三者への DoS 攻撃 メール配送の遅延
初期パスワードの不備	低	認証に使用するために、管理者が発行したユーザ ID や初期パスワードが、単純であり推測が容易である	個人情報の漏洩
価格等の改ざん	低	ショッピングサイトにおいて、価格情報等が利用者側で改ざんできる	データの改ざん、消去

平成16年7月8日
経済産業省

「情報セキュリティ早期警戒パートナーシップ」の運用を開始

～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」、本日より施行～

経済産業省では、情報セキュリティ早期警戒体制の拡充・強化の一環として、ソフトウェア製品や Web サイト等に内在する安全性上の問題箇所（脆弱性）への対応を促進すべく、本日より上記経済産業省告示を施行し、関係機関にてソフトウェア等の脆弱性関連情報流通を図る「情報セキュリティ早期警戒パートナーシップ」の運用を開始した。

1. 概要

昨年8月に発生したMS ブラスターや本年5月に発生したサッサーなど、コンピュータウイルス・不正アクセス等の攻撃は、ソフトウェアの脆弱性（ ）を悪用することによってより高度化・効率化しており、被害拡大のスピードは、ユーザが対処可能なスピードを遙かに超える勢いで早まりつつある。

（ ）「脆弱性」とは、「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機能や性能を損なう原因となり得る、安全性上の問題箇所」と定義。

こうした状況に対処すべく、経済産業省では、情報セキュリティ問題の早期警戒体制の構築・拡大の一環として、昨年11月から独立行政法人情報処理推進機構（IPA）に委託し官民の関係有識者による研究会を開催した。本年4月に公表された研究会の提言¹に基づき、経済産業省や関係機関・団体において、以下の取り組みが進められてきた。

経済産業省では公的ルールの位置づけを検討し、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**」として7月7日に制定（官報掲載）し、本日から施行。

（別添1参照）

また、これに合わせて、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）、社団法人情報サービス産業協会（JISA）、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）、特定非営利法人日本ネットワークセキュリティ協会（JNSA）では、本枠組みに参画

¹ 「情報システム等の脆弱性情報の取扱いに関する研究会報告書」（<http://www.ipa.go.jp/about/press/20040406.html>）

する関係者及び関係業界としての指針「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」(以下「**パートナーシップガイドライン**」という。)を連名で発表(別添2参照)。また、IPA、JPCERT/CCでは、**脆弱性関連情報の取扱業務を本日から開始**(別添3,4参照)。

さらに、7月中旬に公表される予定である、ソフトウェア製品の開発者が脆弱性関連情報を扱う上での業務プロセスや社内体制等の在り方を示す「**(仮称)製品開発者向けガイドライン**」(JEITA及びJISA連名)、ソフトウェア製品開発者における脆弱性関連情報の窓口担当者が把握すべき作業事項を示す「**(仮称)窓口担当者向けマニュアル**」(JPCERT/CC)等を活用することにより、本制度の実効的な運用をめざす。

経済産業省では、こうした一連の取り組みを通じて、官民連携したソフトウェア等の脆弱性関連情報流通の枠組み ~ **情報セキュリティ早期警戒パートナーシップ** ~ の円滑な運用を促進し、高信頼性社会の実現をめざす所存である。

2. ポイント

(1) 早期警戒体制の枠組みの強化・拡充の一環として構築

経済産業省では、1990年から、「コンピュータウイルス・不正アクセス届出事業」を、2003年から「インターネット定点観測事業」を実施し、届出情報や観測データ等の分析・公表によって、被害の局限化を図る情報セキュリティ問題の早期警戒体制を整備してきた。

しかし、コンピュータウイルスや不正アクセスによる攻撃がソフトウェアの脆弱性を悪用したものと発展しつつあることから、早期警戒体制の対象をソフトウェア製品及びWebサイトの脆弱性に広げ、その対策を官民連携して促進することで、被害の発生そのものを未然に抑制することをめざすこととした。

(2) 告示において関係者に望まれる行動基準を規定

情報セキュリティ早期警戒パートナーシップを推進する手段として、経済産業省では経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」を制定した。本告示では、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している。また、告示では、受付機関としてIPA、調整機関としてJPCERT/CCを指定した。

(3) 自らの役割を宣言する「パートナーシップガイドライン」を関連機関・団体が連名で公表

「パートナーシップガイドライン」は、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」を踏まえ、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した指針である。IPA、JPCERT/CC、JEITA、JISA、JPSA、JNSA が連名で公表した。

(4) IPA、JPCERT/CC が脆弱性関連情報の取扱業務を開始

告示が本日(7月8日)より施行されたのを受けて、受付機関である IPA、調整機関である JPCERT/CC において脆弱性関連情報の取扱業務を本日から開始した。

(5) JEITA、JISA による製品開発者向けガイドライン等も公表予定

本枠組みに参画するソフトウェア製品の開発者においては、脆弱性関連情報の通知に伴い対策を策定する上で、社内の体制や手続き、情報管理ルール等を調整する必要が生じる。そこで、JEITA では、製品開発者の社内体制やルール等の在り方を検討する WG を設置、JISA メンバーを加え、検討を重ねている。7月中旬には検討成果を「(仮称)製品開発者向けガイドライン」としてとりまとめ、JEITA 及び JISA の連名で公表する予定である。

また、JPCERT/CC でも、製品開発者における脆弱性関連情報の窓口担当者が把握すべき作業事項を示す「(仮称)窓口担当者向けマニュアル」を策定中であり、7月中旬に公表する予定としている。

3 . 期待効果

上記の取り組みは、情報セキュリティ早期警戒パートナーシップの基盤強化とその円滑な立ち上げを促進するものである。情報セキュリティ早期警戒パートナーシップを本格運用することによって、以下の効果が期待される。

ソフトウェア製品開発者及び Web サイト運営者による脆弱性対策を促進

脆弱性関連情報の放置・危険な公表を抑制

個人情報等重要情報の流出や重要システムの停止を予防

4 . 今後の予定

情報セキュリティ早期警戒パートナーシップの実効的な運用のためには、発見者からの脆弱性関連情報の届出促進(取扱業務の周知)と、ソフトウェア製品開発者側の積極的な参画が不可欠である。このため、本事業に関する説明会(主催: IPA、JPCERT/CC)を7月中~下旬に全国5カ所にて開催し、関係者への啓発を促す予定である。(<http://www.ipa.go.jp/security/vuln/event/20040720.html>)

また、公表した脆弱性対策の情報をユーザに適切に活用してもらえよう、企業ユーザや個人ユーザの対策適用を促すしくみについても検討を進める。

さらに、本制度を一定期間運用した上で、関係者によるフォローアップを行い、実務的な問題点を洗い出し、本格的な運用に向けてさらなる改善を進めて参りたい。

(本発表資料のお問い合わせ先)

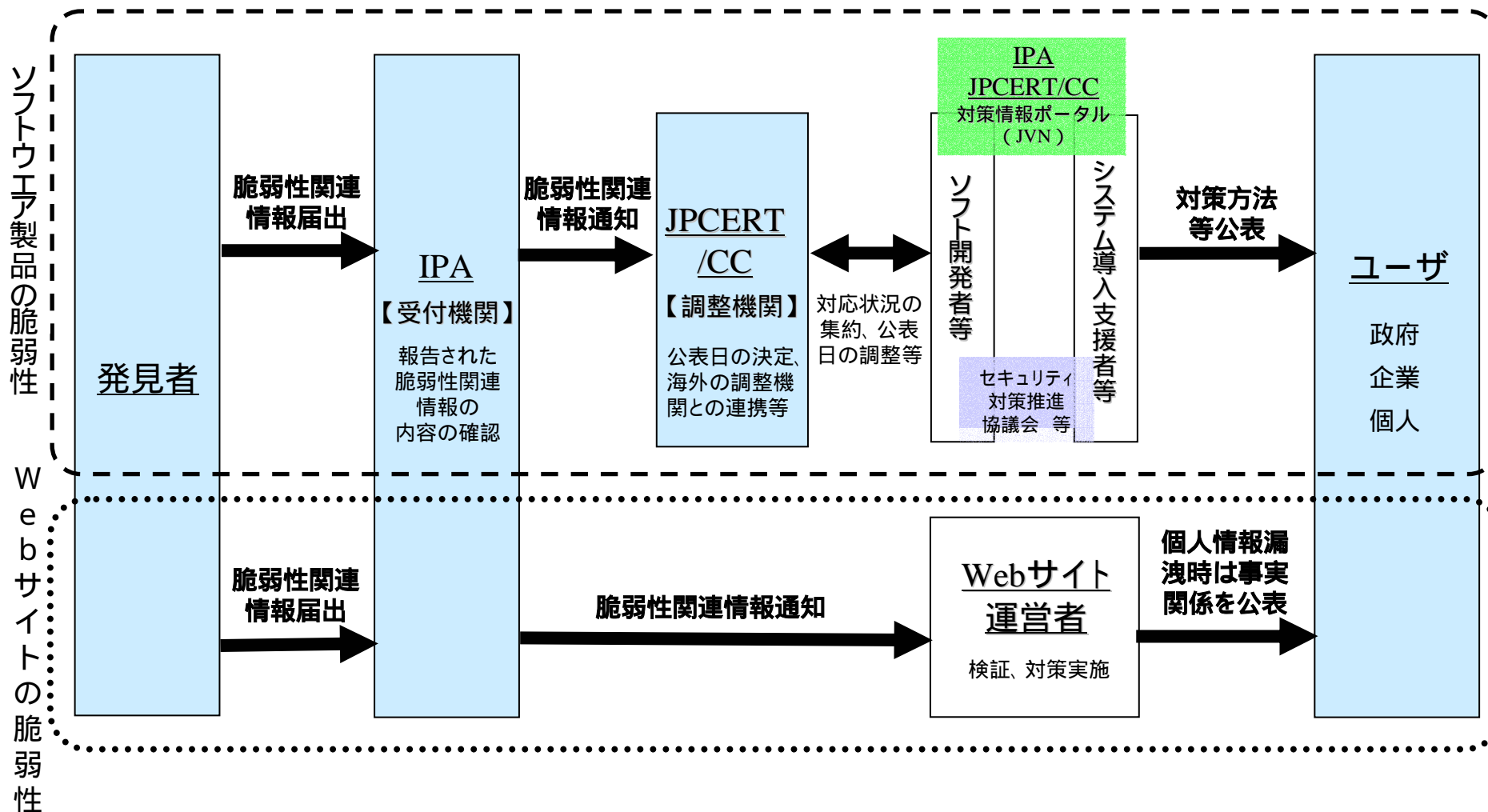
商務情報政策局 情報経済課 情報セキュリティ政策室

担当者：川口、佐藤

電話：03 - 3501 - 1511 (内線 3961)

03 - 3501 - 0397 (直通)

官民連携の体制で、ソフトウェア製品やWebアプリケーションの脆弱性関連情報の円滑な流通と対策の普及促進を図る。



業界側の参加促進

<7月中旬発表予定>

窓口担当者向けマニュアル

【JPCERT/CC】

製品開発者における脆弱性関連情報の窓口担当者が把握すべき作業事項

<7月中旬発表予定>

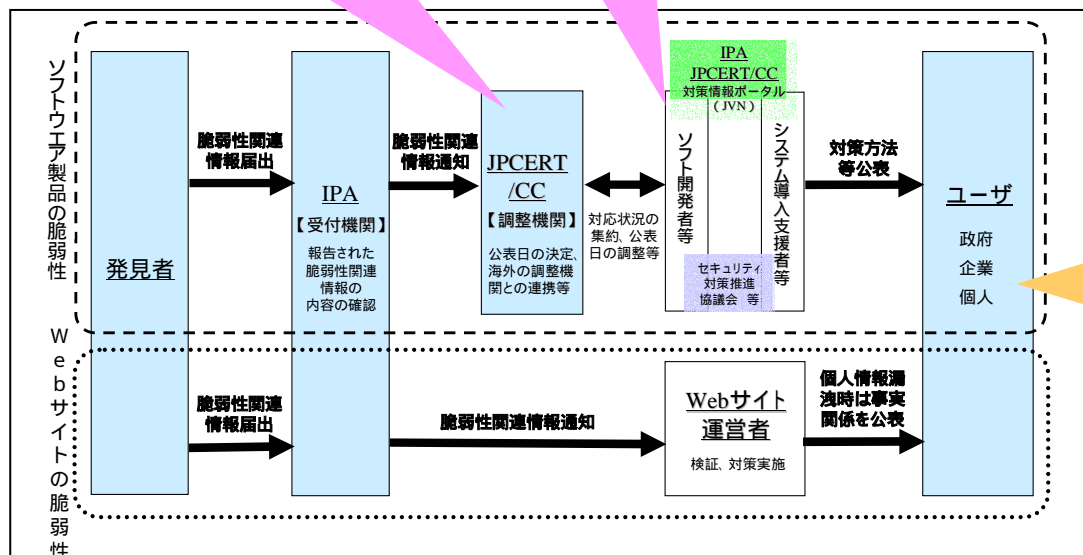
製品開発者ガイドライン

【JEITA, JISA】

脆弱性関連情報を扱う上で業務プロセスや社内体制等の在り方を提示

波及効果

他の業界団体版ガイドライン



ユーザ側の対策促進

ユーザ側から見た、脆弱性問題に関する改善方策の検討

官民連携した枠組みの支持

官

<7月7日制定>

ソフトウェア等脆弱性関連情報取扱基準

(経済産業省告示)

- 脆弱性関連情報の基本枠組みを規定
- 関係者に求められる役割を要請

民

<7月8日公表>

パートナーシップガイドライン

【IPA, JPCERT/CC, JEITA, JISA, JPSA, JNSA】

枠組みに参加する関係者及び関係業界が、自らの役割や推奨される事項を明示した指針