

2004年4月6日

独立行政法人 情報処理推進機構

## 「情報システム等の脆弱性情報の取扱いに関する研究会」報告書の公表について

独立行政法人 情報処理推進機構（略称：IPA、理事長：藤原 武平太）は、昨年11月から、「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）を開催し、ソフトウェア等の脆弱性に関する情報を必要な機関間で流通させるとともに、有効な対策方法を迅速かつ正確にユーザに供給することを目的として、脆弱性の発見から、対策の策定・公表に至るまでの関連情報の取扱いのあり方について検討してきました。

本年3月29日に、これまでの検討結果を報告書としてとりまとめましたので、ここに公表いたします。

### 1. 背景

近年、日本国内でも社会へのITの浸透が進み、同時にその基盤であるソフトウェア等に多くの脆弱性が発見されるようになってきています。これらの脆弱性が悪用される例も後を絶たず、その影響も深刻なものとなることが少なくありません。

一方、発見された脆弱性に関する情報をどのように取り扱うべきなのか、という国内の指針やガイドラインはこれまで存在しておらず、このことが報告の遅れや被害の拡大の一因となっていたことは否めません。昨年10月に公表された「情報セキュリティ総合戦略」（経済産業省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））においても、「脆弱性に対処するためのルールと体制の整備」が必要であることが提言されているところです（別紙1参照）。

このような社会的背景の下、IPAは、経済産業省からの要請により、昨年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、脆弱性に関する情報が発見された場合の届出・報告から、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扱いについて、議論を重ねて参りました。

### 2. 研究会の構成

本研究会には、中間法人 JPCERT コーディネーションセンター、独立行政法人産業技術総合研究所、NPO 日本ネットワークセキュリティ協会（JNSA）、ハードウェア/ソフトウェアメーカー、セキュリティベンダなど、約30機関・50人に参加いただき、さらに、脆弱性に関する情報の取扱いに関するルールについて検討をする「脆弱性情報取扱いガイドラインワーキンググループ」と脆弱性に関する情報を流通させる実際の体制を検討する「脆弱性情報流通ワーキンググループ」とを構成して検討を進めました（研究会委員及びワーキンググループメンバーについては、別紙2参照）。

### 3. 研究会報告書のポイント

本研究会報告書による提言のポイントは、以下のとおりです。

#### (1) 脆弱性に関する情報の届出窓口の整備

脆弱性関連情報の届出先を決め、それを国民に周知することで、脆弱性関連情報が放置されたり、暴露されたりすることを防ぐ効果が期待できる。また、発見者側の負担（製品開発者との交渉、脆弱性を立証するためのリスク）を軽減する効果も期待できる（受付機関は、発見者本人が望まない限り、発見者の氏名、連絡先等の情報を他には提供しない）。

IPA は、これまでもコンピュータウイルス、コンピュータ不正アクセスの届出先（受付機関）として実績を積んでおり、本件についても受付機関としての役割を担うのに適していることから、届出窓口は、IPA に設置する。

#### (2) 届け出られた脆弱性関連情報の分析、対策方法の策定、公表に関する処理手順の明確化、体制の整備

ソフトウェア製品の脆弱性の場合、一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、各製品開発者が対策を講じる期間及びそれを公表するタイミングを調整する必要がある。一方、ウェブアプリケーションの脆弱性については、他のサイトへの影響はほとんどないものと考えられるので、受付機関が受理した脆弱性関連情報を当該ウェブサイト運営者に直接通知する形での処理が可能である。このようにソフトウェア製品の脆弱性とウェブアプリケーションの脆弱性とは、情報の取扱いの流れが異なり得る。

また、機密性が要求される脆弱性そのものや攻撃方法に関する情報と、迅速に広く社会に提供していくことが期待される対策情報とは、その流通のさせ方は異ならざるを得ない。

さらに、システム構築支援事業者やインターネットアクセスプロバイダ、ユーザ等に対し脆弱性の対策方法の周知徹底を図るため、対策方法を集積・公表し、現状の脆弱性対策に係る主要な情報を入手できる環境を提供することが有用である。

機密性が要求される脆弱性や攻撃方法の情報の流通については、これまで実績のある JPCERT/CC が、製品開発者との協力関係を強化していく形で進めることが適当である。一方、対策方法の集積・開示については、独自の脆弱性分析機能を有し、公的性格の強い IPA が実施することが適当である。なお、IPA は、影響度分析、脆弱性検証ツールの作成等の分析を行い、JPCERT/CC、製品開発者を支援する。

以上を勘案すれば、脆弱性に関する情報の取扱いについて、次の図のような取扱い体制を構築することが適当である。



### (3) 各当事者に推奨される行動基準及び心得るべき法的問題

脆弱性に関する情報の発見者、受付機関（IPA）、調整機関（ソフトウェア製品については JPCERT/CC、ウェブアプリケーションについては IPA）、製品開発者及びウェブサイト運営者について、それぞれに推奨される行動基準、心得るべき法的問題を整理した（行動基準については報告書 26 ページ以降及び脆弱性関連情報等取扱基準、法的問題については報告書 35 ページ以降を参照）。

### (4) 以上のような枠組みを規定する「公的ルール」の必要性及びその内容についての提言

脆弱性関連情報の発見者に受付機関の存在を周知するとともに、関係者の適切な対応を促す目的を考慮すれば、政府が公的なルールを制定し、その目的や枠組みを広報するとともに、関連業界団体に対しても積極的に協力を呼びかけていくことが期待される。この「公的なルール」に盛り込むことが期待される内容を、「脆弱性関連情報等取扱基準」案としてとりまとめた。

また、公的なルールと連動する形で、受付機関や調整機関等の役割・機能を規定し、処理の流れを明確化するためのガイドラインを別途策定することが適当である。この「ガイドライン」として期待される内容を「脆弱性関連情報等取扱ガイドライン」案としてとりまとめた。

## 4. 今後の展開

今後は、今回とりまとめた報告書に基づき、脆弱性関連情報の取扱いルール及び流通体制を実装していくフェーズに入ることとなりますが、IPA としては、経済産業省における公的ルールの整備状況を支援しつつ、JPCERT/CC 及びソフトウェア・ハードウェアメーカー、セキュリティベンダ各社の協力も得ながら、本年 7 月から脆弱性に関する情報の届出の受付及び脆弱性分析機能の提供を開始できるよう、体制の充実を図って参ります。

#### 本件に関するお問い合わせ先

独立行政法人 情報処理推進機構 研究会事務局

電話：03-5978-7508 FAX：03-5978-7518 e-mail：[isec-itvac@ipa.go.jp](mailto:isec-itvac@ipa.go.jp)

#### 報道関係からのお問い合わせ先

独立行政法人 情報処理推進機構 戦略企画部広報グループ 高瀬 / 横山

TEL：03-5978-7503 FAX：03-5978-7510 e-mail：[pr@ipa.go.jp](mailto:pr@ipa.go.jp)

「情報セキュリティ総合戦略」関連部分抜粋

3.2.2. 企業・個人における新たな事前予防策

(1) 官民連携した脆弱性対応体制の整備

脆弱性に対処するためのルールと体制の整備

3年以内 to 実現する項目	・脆弱性に対処するためのルールと体制の整備
3年以内に着手し実行に移す項目	-

我が国では、情報システムの脆弱性やコンピュータウイルス、ワーム等の詳細を把握し対策を講じるための情報を収集し分析する体制が弱く、米 CERT/CC やウイルスワクチンソフトベンダなどの情報を基に危険性を判断しているのが現状である。そのため、国内を中心に使用されるソフトの脆弱性への対応や急速に広がるコンピュータウイルス感染の被害を食い止める緊急対応を行うことが難しい。

そこで、政府と IT 事業者が中心となって、情報システムの脆弱性情報を集積するためのルールを構築し、それを分析する体制を整備する。具体的には、

- 1) 不正アクセスやコンピュータウイルス感染等の被害通報の受付
- 2) ネットワークのトラフィック観測に基づく異常予測
- 3) 脆弱性の通知と公開に関する一連の手続きルールの明確化( IT 事業者や研究者等が発見した製品・システムの脆弱性の通報の受け付け、製造元もしくはサービス提供者の対応、一定期間後の公開等)
- 4) 脆弱性及びウイルス、ワーム等の危険性を検証・解析する体制
- 5) 脆弱性及びウイルス、ワーム等の危険性を警告・公表する体制

が必要である。

特に、電子政府の拡大に対応し、通報されたシステムの脆弱性やコンピュータウイルス、ワームの危険性について迅速に検証・解析する体制を、政府として整備することが重要である。中でも、オープンソースのツールや製造元が倒産した製品のように責任を負うべき事業者が明確でない場合の対応、ネットワーク全体に障害をもたらすような緊急性が高く社会的影響の大きい問題への対応等について、本体制の持つ役割は重要である。

【 委員構成 】( 順不同・敬称略 )

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
( 座長代理 )	山口 英	JPCERT/CC / 奈良先端科学技術大学院大学
( 顧問 )	今井 秀樹	東京大学
	村井 純	慶應義塾大学
	村岡 洋一	早稲田大学
( 委員 )	高橋 正和	インターネットセキュリティシステムズ株式会社
	林 簡	株式会社インフォセック
	西尾 秀一	株式会社 NTT データ
	岡野 直樹	サン・マイクロシステムズ株式会社
	大和 敏彦	シスコシステムズ株式会社
	勝見 勉	株式会社シマンテック
	松島 正明	新日鉄ソリューションズ株式会社
	松本 泰	セコム株式会社
	安田 直義	株式会社ディアイティ
	中尾 康二	Telecom-ISAC Japan/ KDDI 株式会社
	才所 敏明	東芝ソリューション株式会社
	小屋 晋吾	トレンドマイクロ株式会社
	石垣 良信	日本アイ・ピー・エム株式会社
	石井 孝治	日本コンピュータセキュリティリサーチ株式会社
	杉浦 昌	日本電気株式会社
	能地 將博	日本ネットワークアソシエイツ株式会社
	佐藤 慶浩	日本ヒューレット・パッカーード株式会社
	松本 直人	株式会社ネットアーク
	小林 偉昭	株式会社日立製作所
	塩崎 哲夫	富士通株式会社
	古川 勝也	マイクロソフト株式会社
	長瀬 正人	三菱商事株式会社
	近藤 誠治	三菱電機株式会社
	横地 裕	横河電機株式会社
	新井 悠	株式会社ラック
( オブザーバ )	岡谷 貢	防衛庁
	高橋 郁夫	高橋郁夫法律事務所
	中村 彰二郎	サン・マイクロシステムズ株式会社
	堀内 弘司	サン・マイクロシステムズ株式会社
	井上 隆文	サン・マイクロシステムズ株式会社
	星澤 裕二	株式会社シマンテック
	斉藤 克敏	トレンドマイクロ株式会社
	村上 清治	日本コンピュータセキュリティリサーチ株式会社
	谷川 哲司	日本電気株式会社
	岸田 明	富士通株式会社
	岡田 興	三菱電機株式会社

	小林 伸太郎	三菱電機株式会社
	西岡 秀司	三菱電機株式会社
	金山 卓矢	横河電機株式会社
	水越 一郎	JPCERT コーディネーションセンター (JPCERT/CC)
	伊藤 友里恵	JPCERT コーディネーションセンター (JPCERT/CC)
	武智 洋	NPO 日本ネットワークセキュリティ協会 (JNSA)
	印南 朋浩	経済産業省
	山崎 琢矢	経済産業省
	川口 修司	経済産業省
	加来 芳郎	経済産業省
	佐藤 貴幸	経済産業省
	田沼 均	独立行政法人産業技術総合研究所
	中村 章人	独立行政法人産業技術総合研究所
(幹事)	大林 正英	JPCERT コーディネーションセンター (JPCERT/CC)
	下村 正洋	NPO 日本ネットワークセキュリティ協会 (JNSA)
	川口 耕一	NPO ネットワークリスクマネジメント協会 (NRA)
	高木 浩光	独立行政法人産業技術総合研究所
	戸村 哲	独立行政法人産業技術総合研究所
(事務局)	早貸 淳子	独立行政法人情報処理推進機構
	日下 保裕	独立行政法人情報処理推進機構
	小門 寿明	独立行政法人情報処理推進機構
	福澤 淳二	独立行政法人情報処理推進機構
	笠井 行弘	独立行政法人情報処理推進機構
	井上 信吾	独立行政法人情報処理推進機構
	加藤 昌和	独立行政法人情報処理推進機構
	宮川 寧夫	独立行政法人情報処理推進機構
	園田 道夫	独立行政法人情報処理推進機構
	花村 憲一	独立行政法人情報処理推進機構
	田原 美緒	独立行政法人情報処理推進機構
	高坂 史彦	独立行政法人情報処理推進機構
	村瀬 一郎	株式会社三菱総合研究所
	牧野 京子	株式会社三菱総合研究所
	村野 正泰	株式会社三菱総合研究所

## 脆弱性情報取扱いガイドラインワーキンググループ

(メンバー)	高橋 郁夫	高橋郁夫法律事務所
	高橋 正和	インターネットセキュリティシステムズ株式会社
	林 簡	株式会社インフォセック
	勝見 勉	株式会社シマンテック
	安田 直義	株式会社ディアイティ
	斉藤 克敏	トレンドマイクロ株式会社
	杉浦 昌	日本電気株式会社
	佐藤 慶浩	日本ヒューレット・パカード株式会社
	松本 直人	株式会社ネットアーク
	藤田 耕作	株式会社日立製作所
	塩崎 哲夫	富士通株式会社

(オブザーバ)	古川 勝也	マイクロソフト株式会社
	小林 伸太郎	三菱電機株式会社
	金山 卓矢	横河電機株式会社
	武智 洋	横河電機株式会社
	岡谷 貢	防衛庁
	水越 一郎	JPCERT コーディネーションセンター (JPCERT/CC)
	伊藤 友里恵	JPCERT コーディネーションセンター (JPCERT/CC)
	山崎 琢矢	経済産業省
	川口 修司	経済産業省
	佐藤 貴幸	経済産業省
	加来 芳郎	経済産業省

## 脆弱性情報流通ワーキンググループ

(メンバー)	高橋 正和	インターネットセキュリティシステムズ株式会社	
	西尾 秀一	株式会社 NTT データ	
	岡野 直樹	サン・マイクロシステムズ株式会社	
	星澤 裕二	株式会社シマンテック	
	松本 泰	セコム株式会社	
	安田 直義	株式会社ディアイティ	
	中尾 康二	Telecom-ISAC Japan/KDDI 株式会社	
	才所 敏明	東芝ソリューション株式会社	
	小屋 晋吾	トレンドマイクロ株式会社	
	石井 孝治	日本コンピュータセキュリティリサーチ株式会社	
	村上 清治	日本コンピュータセキュリティリサーチ株式会社	
	谷川 哲司	日本電気株式会社	
	能地 將博	日本ネットワークアソシエイツ株式会社	
	松本 直人	株式会社ネットアーク	
	田中 和雄	株式会社日立製作所	
	岸田 明	富士通株式会社	
	古川 勝也	マイクロソフト株式会社	
	近藤 誠治	三菱電機株式会社	
	横地 裕	横河電機株式会社	
	新井 悠	株式会社ラック	
	(オブザーバ)	岡谷 貢	防衛庁
		水越 一郎	JPCERT コーディネーションセンター (JPCERT/CC)
		伊藤 友里恵	JPCERT コーディネーションセンター (JPCERT/CC)
		山崎 琢矢	経済産業省
		川口 修司	経済産業省
		佐藤 貴幸	経済産業省
		加来 芳郎	経済産業省
田沼 均		独立行政法人産業技術総合研究所	
中村 章人		独立行政法人産業技術総合研究所	