

コンピュータ・セキュリティ問題に関する早期警戒体制の構築・拡充について
～「情報システム等の脆弱性関連情報の取扱いに関する研究会」報告書公表～

平成 16 年 4 月 6 日
経済産業省

1. 背景

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¹」を、2003年から「インターネット定点観測事業²」を実施し、ウイルスや不正アクセスの届出・公表などによるコンピュータ・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、昨年8月に発生した MS ブラスターのように、コンピュータウイルス等の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り、被害はますます拡大・深刻化しつつある。また、コンピュータウイルス等の性質も、単純なウイルスファイルを電子メールに添付させ広めるようなものから、MS ブラスターのように特定のソフトウェアがもつ問題箇所(以下「脆弱性^()」という)を直接攻撃するものへと発展しつつある(別紙1参照)。

()「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。

このため、経済産業省では、これまでのコンピュータ・セキュリティ問題の早期警戒体制を更に拡充・強化するため、昨年11月から、「コンピュータウイルス・不正アクセス届出事業」を行ってきた情報処理推進機構(IPA)に検討を委託、IPAにおいて、官民の関係有識者を一堂に集めて検討を行い、このたび、体制の骨格をまとめた報告を公表することとなった(メンバーリストは別紙2を参照)。

なお、この取り組みは、昨年10月に公表した「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))における、「脆弱性に対処するためのルールと体制の整備」の必要性に関する提言(別紙3参照)を受けたものである。

報告書本体は以下の URL から入手することが可能です。

http://www.meti.go.jp/policy/netsecurity/downloadfiles/Vulnera_Report.pdf

¹ 情報処理推進機構(IPA)において、1990年よりコンピュータウイルスの届出受付・分析及び実績の公表を実施。JPCERT コーディネーションセンター(JPCERT/CC)において、1996年より不正アクセスの相談窓口業務を実施。

² JPCERT/CCにおいて、2003年より、インターネット上に設置した複数のセンサーから得られる情報を解析し、ネットワーク・システム管理者向けに HP 上で公開する「インターネット定点観測事業」を実施。

2. 報告書のポイント

(1) コンピュータ・セキュリティ問題を巡る現状

コンピュータウイルスや不正アクセスによる攻撃は、単純なウイルスファイルを電子メールに添付させ広めるようなものから、MS ブラスターのように特定のソフトウェアの脆弱性を悪用したものへと発展しつつある。このため、ソフトウェア等の脆弱性が放置されれば、悪意の者によって危険な利用をされるおそれも高まっている。

しかし、ソフトウェア等の脆弱性への対策は、ソフトウェア製品開発者等の利益に直ちに結びつかず、また、自ら気づきにくい側面もあることから、事業者の自発的な改善がなかなか進んでいない。また、自発的に取り組んできた事業者にとっても、国内にこうした早期警戒体制がないため、米国の CERT/CC³や英国の UNIRAS⁴など海外の機関が提供する脆弱性関連情報の管理・流通体制を頼っているのが実情である。

(2) コンピュータ・セキュリティ早期警戒体制の枠組みの拡充

体制の枠組み(別紙4参照)

- ・ こうした現状を踏まえ、早期警戒体制の対象を、従来のコンピュータウイルス情報及び不正アクセス情報から、ソフトウェア製品(OS、データベース、プロトコルの実装等)及び Web サイトの脆弱性に拡大する。
- ・ 脆弱性情報については、一般のコンピュータ利用者やソフトウェアメーカなどが発見した情報が、悪意の者の手に渡る前に機密性を保持しつつ迅速に流通し、ソフトウェアメーカ等による対策の策定・公表につなげるよう、その処理の手順を別途定める。
- ・ 具体的には、発見者が安心して脆弱性に関する情報を届け出ることが出来る公的な窓口機関(受付機関)を設置するとともに、受付機関に届けられた脆弱性情報がどのソフトウェアやシステムに影響するものか確認しつつ、採るべき対策方法やその内容の公表時期をソフトウェアベンダ等関係者間で調整する機関(調整機関)を設置する。
- ・ 両機関の設置を前提に、「発見者からの通報」「受付機関での内容の確認」「調整機関での対応の調整」「ソフトウェア製品開発者等からユーザへの対策方法の公表」という、脆弱性関連情報の基本的な流れと作業手順を特定する。
- ・ なお、通知しても脆弱性の修正をしようとならない事業者のソフトウェア等に関しては、当該脆弱性の内容を適切な形で一般に公開することとする。このための手続きの詳細等については、今後更にソフトウェア業界等と調整を行うこととする。

「受付機関」及び「調整機関」

- ・ 受付機関については、これまでウイルスや不正アクセスによる被害届出業務等を通じ、コンピュータ・セキュリティ問題の早期警戒に実績を上げ、一般にも知名度の高い公的

³ Computer Emergency Response Team/Coordination Center の略。米国において情報セキュリティインシデントに対応するための技術的支援を行う組織。

⁴ Unified Incident Reporting and Alert Scheme の略。英国における情報セキュリティインシデントに対応するための技術的支援を行う組織。

機関として IPA が担当する。

- ・ 調整機関については、脆弱性関連情報に関する海外の関係機関(CERT/CC 等)との調整を行ってきた実績を有する JPCERT/CC が担当する。

この基本枠組みを規定する「公的ルール」の策定

- ・ 脆弱性関連情報に係る受付窓口の存在を広く知らせるとともに、本スキーム自体を悪意の者に利用される可能性を排除し、関係者が安心して本スキームに関与できるよう担保するため、本早期警戒体制の枠組みを規定する「公的ルール」の案を提示。

3. 期待される効果

(1) 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の促進

発見された脆弱性が迅速に伝えられる仕組みが整備され、対策を採らない事業者のソフトウェア等に関する脆弱性関連情報の公表スキームが担保されることで、ソフトウェア製品開発者及び Web サイト運営事業者等事業者の自覚と取り組みが促進される。

また、国内に脆弱性関連情報に関する仕組みが確立することで、米国 CERT/CC や英国 UNIRAS 等と直接交渉する必要がなくなり、より広い事業者の参加が期待できる。

(2) 脆弱性関連情報の放置・危険な公表を抑制

脆弱性が発見された場合の公的な「受付窓口」(IPA) が設置されることで、脆弱性関連情報が悪意を持つ者の手に渡ったり、ウイルス等の増加を招きかねない危険な公表が行われたりする事態を予防する。

(3) 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

脆弱性関連情報が迅速に流通する仕組みが担保されることにより、脆弱性の修正の遅れによる個人情報等の重要情報の流出や重要システムの停止の予防に寄与する。

4. 経済産業省としての今後の対応

本報告書の提言を受け、早期警戒体制の骨格をなす「脆弱性関連情報流通の基本枠組み」と関係者間の役割分担に関する「公的ルール」に関し、パブリックコメント等の手続きを踏まえつつ、経済産業省告示の形で本年6月中にも制定する。

また、告示の施行を受けて、早ければ本年7月にも、IPA 及び JPCERT/CC において、実際の脆弱性関連情報の取り扱いを開始する。

(本件に対する問い合わせ先)

経済産業省 商務情報政策局 情報セキュリティ政策室

URL <http://www.meti.go.jp/policy/netsecurity/index.html>

電話 03-3501-0397(直通)

電子メール it-security@meti.go.jp

担当: 山崎、川口、佐藤、加来

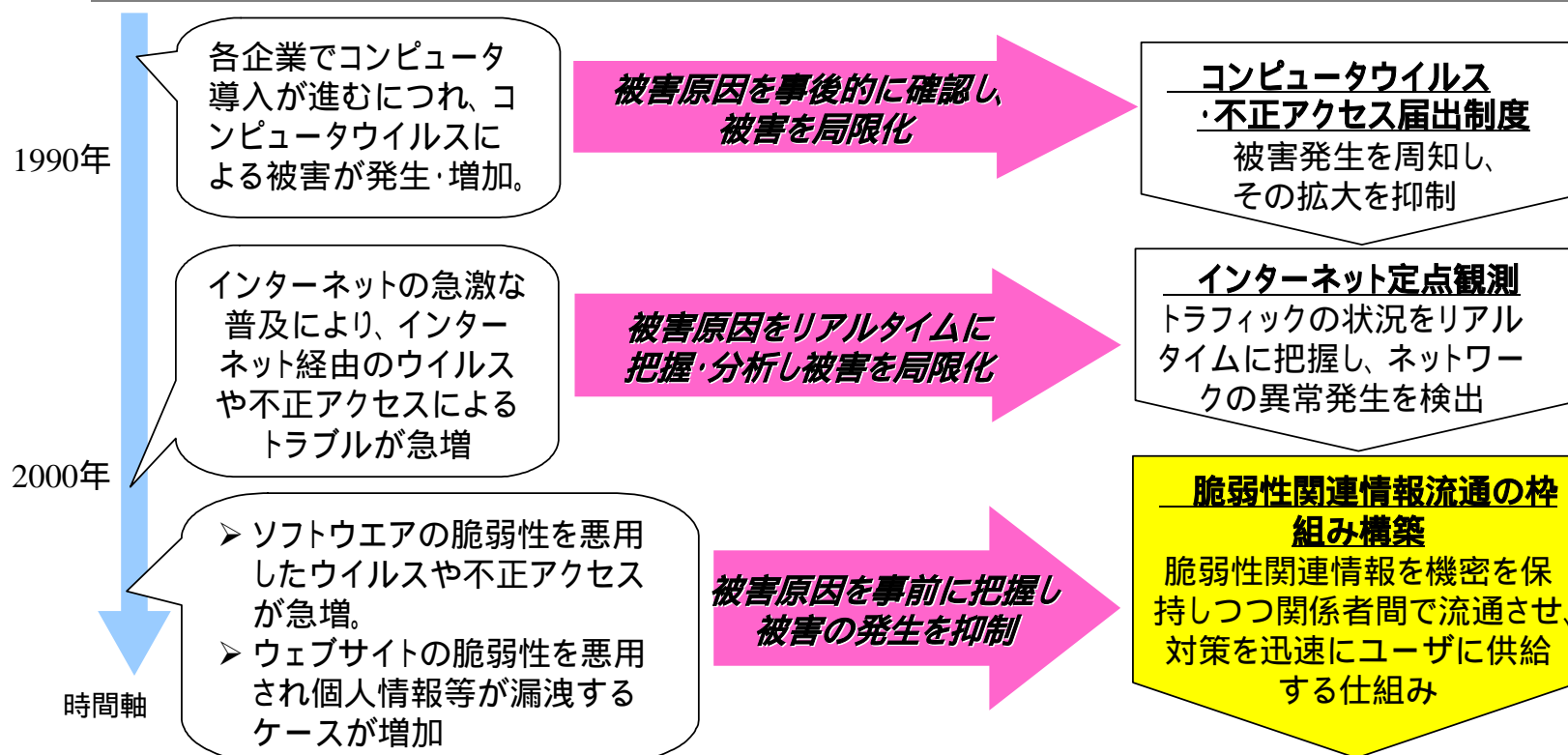
コンピュータ・セキュリティに係る早期警戒体制の変遷

- 経済産業省では、コンピュータウイルス・不正アクセスなどのコンピュータ・セキュリティ問題に関し、早期にトラブルを発見・公表することで、その被害を局限化するための仕組み作りに取り組んできた。

コンピュータウイルス・不正アクセス届出 (IPA 1990年~, JPCERT/CC 1996年~)

インターネット定点観測 (JPCERT/CC 2003年11月~)

脆弱性関連情報流通の枠組み構築 (IPA、JPCERT/CC 2004年(予定))



情報システム等の脆弱性情報の取扱いに関する研究会委員名簿

(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ーツ株式会社
	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
	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

「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年以内に実現する項目	・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処、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。

コンピュータ・セキュリティ早期警戒体制の枠組み

コンピュータウイルス及び不正アクセス等の問題の早期発見・公表に加え、ソフトウェア等の脆弱性に関する情報の流通/管理を含めた体制へと早期警戒体制の拡充・強化を図る。

