IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2010 年 3 月 31 日
独立行政法人情報処理推進機構

「2010 年版 10 大脅威 あぶり出される組織の弱点！」を公開

IPA（独立行政法人情報処理推進機構、理事長：西垣 浩司）は、2009 年の 1 年間（1 月～12 月）の IPA への届出情報や一般に報道された情報を基に、「2010 年版 10 大脅威 あぶり出される組織の弱点！」をまとめ、2010 年 3 月 31 日（水）から IPA のウェブサイトで公開しました。
URL：http://www.ipa.go.jp/security/vuln/10threats2010.html

本資料は、IPA に届出のあったコンピュータウイルス、不正アクセスおよび脆弱性に関する情報や、インターネット等で一般に報道された情報を基に、「情報セキュリティ早期警戒パートナーシップ[1]」に参画する関係者のほか、情報セキュリティ分野における研究者、実務担当者など 120 名から構成される「10 大脅威執筆者会（別紙参照）」でまとめたものです。2005 年から毎年公開しており、今年で 6 回目となります。

2009 年には、「ガンブラー（Gumblar）」と呼ばれる手口（攻撃手法）をはじめとした、様々な情報ネットワーク関連の事件・事故が発生しました。特に「ガンブラー」事件（図 1）では、ウェブサイトの運営委託先からウェブサイト更新用のユーザ ID やパスワードが盗まれた事例もあり、自組織だけではなく業務委託先も含めた総合的なセキュリティ対策の必要性が浮き彫りになりました。このような取組が従来から必要であった事実を認識し、自組織のセキュリティ対策を進める必要があります。

また、某大手企業で情報窃取が発生し、その被害額が約 70 億円に上ると試算した報道がある等、「内部犯罪」による事故も発生しました。内部犯罪による情報窃取という脅威は、外部からの攻撃による脅威に比べて、重要な情報を窃取される可能性が高まります（図 2）。重要な情報に対しては、システム的なアクセス制御等に加え、物理的な入退室管理等も重要になります。

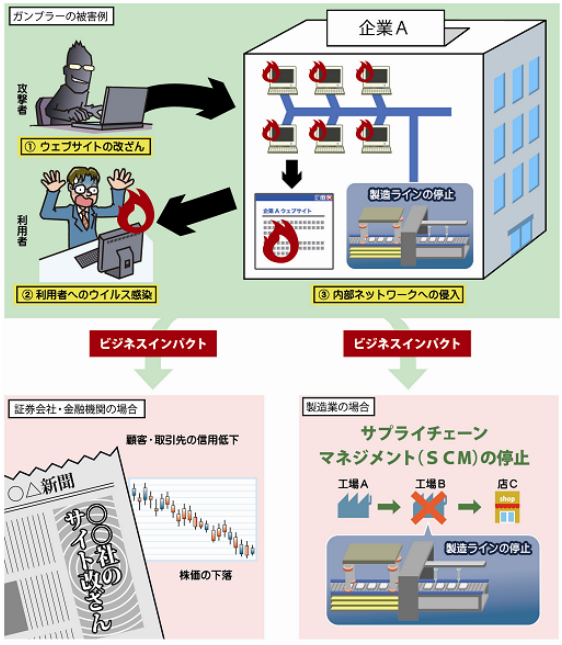

図 1. ガンブラーがもたらすビジネスインパクト

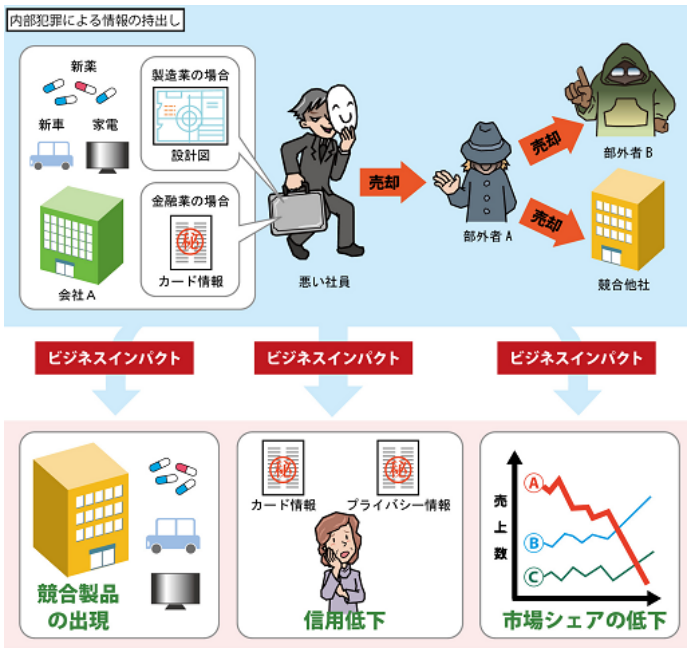

図 2. 内部犯罪がもたらすビジネスインパクト

[1] 経済産業省告示に基づき、2004 年 7 月より開始したものです。ソフトウェア製品及びウェブアプリケーション（ウェブサイト）に関する脆弱性関連情報を円滑に流通し、対策の普及を図るため、公的ルールに基づく官民の連携体制の基本枠組みです。

これらのセキュリティ対策を進める際には、脅威が自組織に及ぼすビジネスインパクトを分析[2]し、適切な対策をしていく必要があります。また、セキュリティ対策は、事件・事故の発生の抑制や被害を最小限に抑え事業継続を実現する「事前対策」の観点と、事故が発生したとしても被害を最小限に抑え、早期復旧を実現する「事後対応」の二つの観点も忘れずに考える必要があります。

本資料の第 1 章では、2009 年に実際にあった脅威を例に、組織にとってのビジネスインパクトを考察しています。第 2 章では、安全なインターネットの利用における脅威を、2009 年に「印象が強かったもの」「社会的影響が大きいもの」などの観点からまとめた 10 大脅威について解説しています。第 3 章では、経営者・システム管理者・開発者の立場から、10 大脅威に対する事前対策・事後対応を紹介しています。

本資料は、2010 年上期発刊予定の「情報セキュリティ白書 2010」の第 2 部とする予定です。近年の情報セキュリティを取り巻く状況の理解や、今後の対策の参考になることを期待します。次の URL よりダウンロードの上、参照下さい。

http://www.ipa.go.jp/security/vuln/10threats2010.html

【2010 年版 10 大脅威　あぶり出される組織の弱点！】

第 1 位　変化を続けるウェブサイト改ざんの手口

ウェブサイトを閲覧しただけで、利用者がウイルスに感染することがあります。このような脅威をもたらす攻撃に新しい手口が現れました。

第 2 位　アップデートしていないクライアントソフト

2009 年も、ソフトウェアの脆弱性が攻撃に悪用されました。しかし、悪用された脆弱性の中には修正済みのものが多く、利用者側のアップデートが徹底されていれば、被害を減らせたはずです。

第 3 位　悪質なウイルスやボットの多目的化

ウイルスやボット（以降、ウイルス）は利用者にとって身近な脅威です。ウイルスには多様な目的があります。また、2009 年にはウイルスの亜種が爆発的に増加しました。

第 4 位　対策をしていないサーバ製品の脆弱性

サーバ製品の脆弱性対策を行わずに運用しているウェブサイト等の存在が明らかになっています。

第 5 位　あわせて事後対応を！情報漏えい事件

情報漏えいには様々な原因がある。また、漏えいした情報の種類によって被害は異なります。

第 6 位　被害に気づけない標的型攻撃

メールの送付元を知人や取引先企業になりすまして、ウイルスを送付する手口があります。このようなソーシャル・エンジニアリングによって、ウイルスに感染させる攻撃を標的型攻撃といいます。

第 7 位　深刻な DDoS 攻撃

DDoS（Distributed Denial of Service）攻撃は、DoS 攻撃（サーバやルータなどの機能を麻痺状態にさせる）の一種です。2009 年 7 月に米国・韓国が攻撃を受けたニュースが流れました。

第 8 位　正規のアカウントを悪用される脅威

コンピュータに対して自分であることを証明する情報（ユーザ ID とパスワード等）がアカウントです。アカウントの不適切な運用によって、事件に発展する例が多発しています。

[2] ビジネスインパクト分析で、起こり得るリスク・脅威を網羅的に洗い出し、それらリスクに対して、組織における重要な事業・業務（基幹事業・業務）・プロセス、それに関連するリソースを特定し、事業継続に及ぼす影響の分析を行います。

第 9 位　クラウド・コンピューティングのセキュリティ問題

クラウド・コンピューティング（クラウド）が普及するにつれ、クラウドにおけるセキュリティの問題も指摘されてきています。

第 10 位　インターネットインフラを支えるプロトコルの脆弱性

多くのコンピュータでインターネットに接続するための機能が備えられています。これらの機能に脆弱性が発見され、攻撃された場合、インターネットに大きな被害が生じる可能性があります。

【参考】

（1）情報セキュリティ白書 2009 第 2 部 10 大脅威 攻撃手法の『多様化』が進む
http://www.ipa.go.jp/security/vuln/10threats2009.html

（2）情報セキュリティ白書 2008 第 2 部 10 大脅威 ますます進む『見えない化』
http://www.ipa.go.jp/security/vuln/20080527_10threats.html

（3）情報セキュリティ白書 2007 年版 10 大脅威「脅威の“見えない化”が加速する！」
http://www.ipa.go.jp/security/vuln/20070309_ISwhitepaper.html

（4）情報セキュリティ白書 2006 年版 10 大脅威「加速する経済事件化」と今後の対策
http://www.ipa.go.jp/security/vuln/20060322_ISwhitepaper.html

（5）コンピュータ・セキュリティ ～2004 年の傾向と今後の対策～
http://www.ipa.go.jp/security/vuln/20050331_trend2004.html

■ 本件に関するお問い合わせ先
IPA セキュリティセンター　山岸／相馬
Tel: 03-5978-7527　Fax: 03-5978-7518　E-mail: vuln-inq@ipa.go.jp
■ 報道関係からのお問い合わせ先
IPA 戦略企画部広報グループ　横山／大海
Tel: 03-5978-7503　Fax: 03-5978-7510　E-mail: pr-inq@ipa.go.jp

別紙

10 大脅威執筆者会 構成メンバー

氏名	所属	氏名	所属
渡部 章	(株)アークン	谷川 哲司	日本電気(株)
石田 淳一	(株)アールジェイ	宇都宮 和顕	日本電気(株)
加藤 雅彦	(株)アイアイジェイ テクノロジー	秋山 卓司	(社)日本電子認証協議会(JCAF)
根岸 征史	(株)アイアイジェイ テクノロジー	長島 雅夫	日本電信電話(株)
高橋 康敏	(株)アイアイジェイ テクノロジー	杉浦 芳樹	日本電信電話(株)
齋藤 衛	(株)インターネットイニシアティブ	安部 哲哉	日本電信電話(株)
徳丸 浩	HASH コンサルティング(株)	住本 順一	日本電信電話(株)
三輪 信雄	S&J コンサルティング(株)	やすだ なお	特定非営利活動法人日本ネットワーク
小林 克巳	NRI セキュアテクノロジーズ(株)		セキュリティ協会(JNSA)
西尾 秀一	(株)NTT データ	榎本 司	日本ヒューレット・パッカード(株)
池田 和生	(株)NTT データ	西垣 直美	日本ヒューレット・パッカード(株)
入宮 貞一	(株)NTT データ	佐藤 直之	日本ベリサイン(株)
井上 克至	(株)NTT データ	杉岡 弘毅	(株)ネクストジェン
前田 典彦	(株)Kaspersky Labs Japan	山田 陽介	ネットエージェント(株)
岸本 博之	(財)金融情報システムセンター(FISC)	高橋 潤哉	(株)ネットセキュリティ総合研究所
林 弘毅	経済産業省	水越 一郎	東日本電信電話(株)
清水 友晴	経済産業省	太田 良典	(株)ビジネス・アーキテクツ
秋貞 幸雄	経済産業省	吉野 友人	(株)ビジネス・アーキテクツ
鈴木 啓紹	(社)コンピュータソフトウェア協会(CSAJ)	本川 祐治	(株)日立情報システムズ
福森 大喜	(株)サイバーディフェンス研究所	田山 晴康	(株)日立製作所
名和 利男	(株)サイバーディフェンス研究所	寺田 真敏	(株)日立製作所
高木 浩光	(独)産業技術総合研究所	梅木 久志	(株)日立製作所
大岩 寛	(独)産業技術総合研究所	藤原 将志	(株)日立製作所
宮地 利雄	(社)JPCERT コーディネーションセンター	鵜飼 裕司	(株)フォティーンフォティ技術研究所
	(JPCERT/CC)	金居 良治	(株)フォティーンフォティ技術研究所
伊藤 友里恵	(社)JPCERT コーディネーションセンター	森 玄理	富士通(株)
	(JPCERT/CC)	冨士原 裕文	富士通(株)
宮崎 清隆	(社)JPCERT コーディネーションセンター	木村 秀年	富士通(株)
	(JPCERT/CC)	草間 正	富士通(株)
古田 洋久	(社)JPCERT コーディネーションセンター	望月 大光	(株)富士通ソフトウェアテクノロジーズ
	(JPCERT/CC)	佐藤 友治	(株)ブロードバンドセキュリティ
高橋 紀子	(社)JPCERT コーディネーションセンター	許 先明	(株)ブロードバンドセキュリティ
	(JPCERT/CC)	藤田 耕作	放送大学大学院
林 薫	(株)シマンテック	高橋 正和	マイクロソフト(株)
大野 雅子	(株)スマートバリュー	加藤 義宏	マカフィー(株)
星澤 裕二	(株)セキュアブレイン	国分 裕	三井物産セキュアディレクション(株)
神薗 雅紀	(株)セキュアブレイン	後藤 久	三井物産セキュアディレクション(株)
正木 健介	セコムトラストシステムズ(株)	寺田 健	三井物産セキュアディレクション(株)
澤永 敏郎	ソースネクスト(株)	村瀬 一郎	(株)三菱総合研究所
青谷 征夫	ソースネクスト(株)	川口 修司	(株)三菱総合研究所
百瀬 昌幸	(財)地方自治情報センター(LASDEC)	村野 正泰	(株)三菱総合研究所
木村 道弘	(株)電子商取引安全技術研究所	藤井 誠司	三菱電機(株)
小橋 一夫	(社)電子情報技術産業協会(JEITA)	青木 歩	(株)ユービーセキュア
渡辺 淳	(株)デンソーウェーブ	志田 智	(株)ユビテック
吉松 健三	(株)東芝	福本 佳成	楽天(株)
小島 健司	東芝ソリューション(株)	岩井 博樹	(株)ラック
小屋 晋吾	トレンドマイクロ(株)	山崎 圭吾	(株)ラック
岡谷 貢	内閣官房情報セキュリティセンター	柳澤 伸幸	(株)ラック
鍋島 学	内閣官房情報セキュリティセンター	川口 洋	(株)ラック
須川 賢洋	新潟大学	伊藤 耕介	(株)ラック
徳田 敏文	日本アイ・ビー・エム(株)	若居 和直	(株)ラック
井上 博文	日本アイ・ビー・エム(株)	中田 邦彦	(株)ルネサス テクノロジ

※IPA セキュリティセンターからは 22 名参加しました(記載省略)