情報セキュリティ

10大脅威 2015

～ 被害に遭わないために実施すべき対策は？ ～

IPA 独立行政法人情報処理推進機構
セキュリティセンター

2015年3月

このページは空白です。

目次

はじめに

本書「情報セキュリティ 10 大脅威 2015」は、情報セキュリティ専門家を中心に構成する「10 大脅威執筆者会」約 100 名の協力により、2014 年に発生したセキュリティ事故や攻撃の状況等から脅威を選出し、投票により順位付けした 10 の脅威を解説した資料である。さらに、実施すべき基本的な対策や、今後注目すべき課題や懸念についても解説している。

各脅威が自組織や自分自身にどう影響するか認識しながら本書を読み進めることで、様々な脅威と対策を網羅的に把握できる。

本書が、読者自身のセキュリティ対策への取組みと、各企業・組織の研修やセキュリティ教育等に活用されることによるセキュリティ対策の普及の一助となることを期待する。

【本書の概要】

- 基本的な情報セキュリティ対策の重要性

注目される脅威は毎年変わるが、情報セキュリティの目的や基本的な対策に大きな変わりは無い。情報セキュリティの目的は、「情報資産の保護」と情報システムの「安定稼動」と「安心・安全な利用」であり、企業・組織においては「情報漏えい」と「業務停止」を防ぐことが重要である。基本的な対策として、「ソフトウェアの更新」、「ウイルス対策ソフト（セキュリティソフト）の導入」、「パスワードの適切な管理」等を自発的かつ継続的に行い、被害の防止に努める必要がある。

- 2014 年の脅威の動向

2013 年に引き続き 2014 年もサイバー攻撃・犯罪の金銭被害が拡大した。インターネットバンキングの総被害額は昨年の約 14 億円から 2 倍を超える約 29 億円となり、法人の被害額が急増したことが、総被害額急増の要因の 1 つに挙げられる。

また、2014 年は運用管理における情報セキュリティの重要性を再認識する事案が多かった。2014 年 7 月、通信教育大手企業から 3,504 万件の個人情報が名簿販売業者に流出する内部不正事件が発覚し、内部不正対策の重要性に注目が集まった。また、2014 年 4 月には、Apache Struts、OpenSSL、Internet Explorer の脆弱性が立て続けに報告され、脆弱性を悪用した攻撃への懸念から、システム管理者やユーザーは待った無しの対応を迫られた。状況把握から対策実施までの対応の速さが求められる時代になっている。

- 企業・組織における課題

標的型攻撃、内部不正、脆弱性を狙った攻撃等の脅威や問題が噴出する中、それらに日々迅速に対処していくための人材の確保と体制作りが企業・組織の課題となっている。その課題に対し、緊急事態に対応できる体制 CSIRT（Computer Security Incident Response Team：シーサート）を構築し、他組織と情報交換を行いながらセキュリティを強化していくことが重要となっている。

1章. 情報セキュリティ対策の基本

1 章　情報セキュリティ対策の基本

SNS に代表される様々なインターネットサービスの普及、スマートフォンの利用によるライフスタイルの変化に伴い、我々を取り巻く情報セキュリティの脅威も多様化している。情報や金銭の窃取を狙った攻撃、国を越えた攻撃による被害等、具体的な脅威は攻撃者が誰で何を目的にしているかによって異なるが、「情報セキュリティの目的」と「対策の基本」は、長年変化が無いと言っても過言ではない。

情報セキュリティの目的は、「情報資産の保護」と情報システムの「安定稼動」と「安心・安全な利用」である。個人においては、金銭被害や個人情報漏えいの被害に遭わないこと、企業・組織においては、保持する重要なデータを漏えいさせないこと、情報システムを利用する業務を停止させないこと等がそれぞれの目的として挙げられる。

情報セキュリティ対策の基本を図 1.1 に示す。これらを実施していれば多くの事例で被害を受けずに済むと言える、まさに基本中の基本の対策である。本書の 1 章として「情報セキュリティ対策の基本」を次ページ以降で解説する。

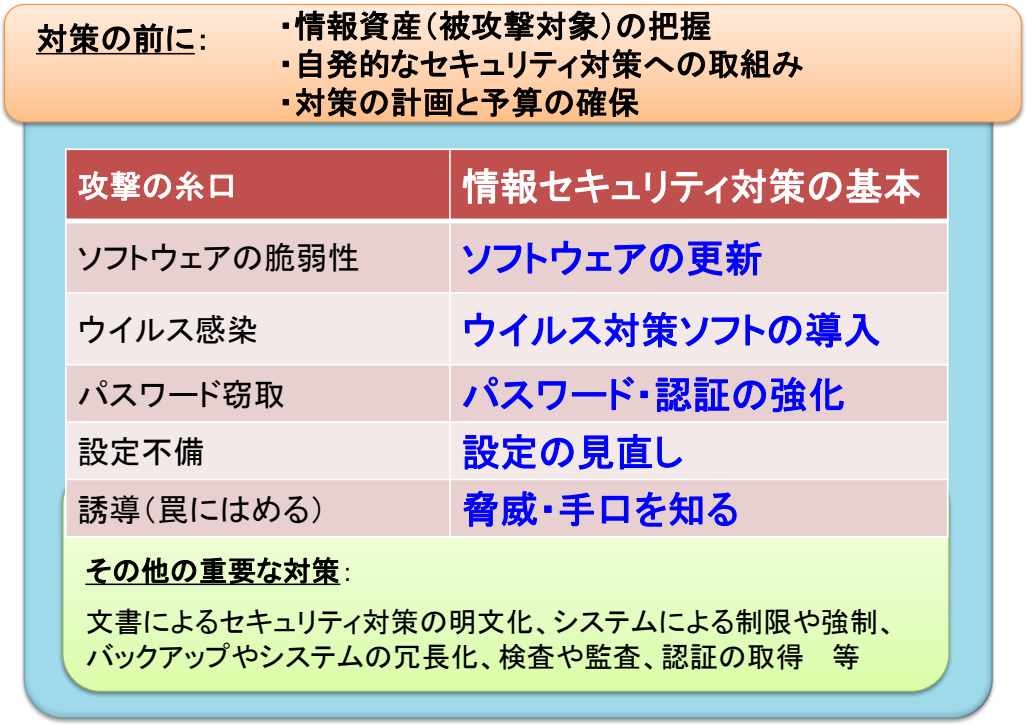
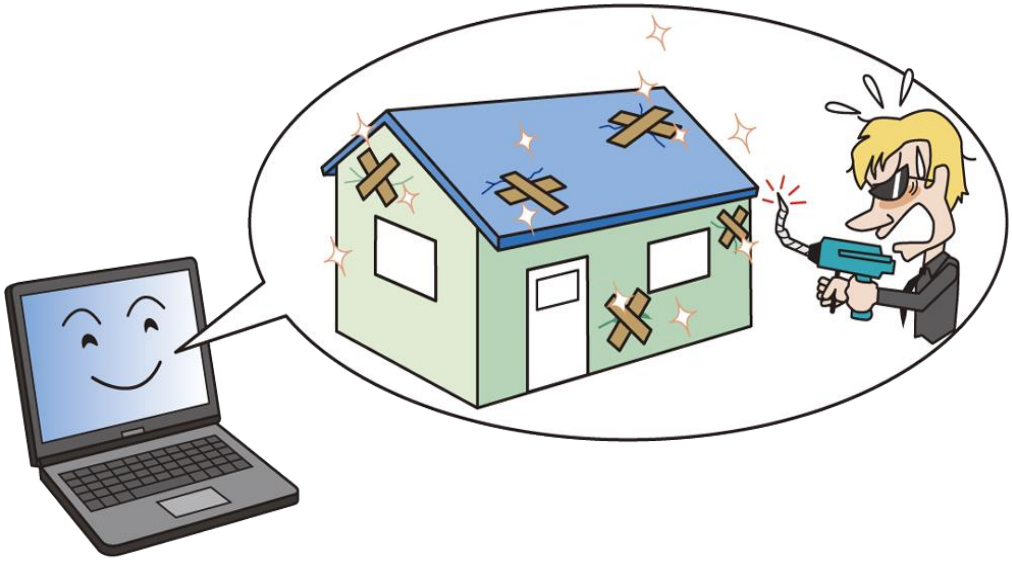


図 1.1　情報セキュリティ対策の基本

1.1. ソフトウェアの更新



ソフトウェアにセキュリティ上の欠陥である脆弱性（セキュリティホール）が発見されると、ソフトウェア開発者は修正プログラム（パッチ）を提供する。利用者はパッチを適用してソフトウェアの更新を行うことで、脆弱性を解消できる。

◆　ソフトウェアの更新は必要不可欠

ウイルスの感染や侵入等の攻撃に脆弱性が悪用される。攻撃を防御するためには、ソフトウェアを更新して脆弱性を根本的に解消することが最善の対策となる。

パソコンだけではなくブロードバンドルーター等のネットワーク対応機器に対してもソフトウェアを更新する必要がある。

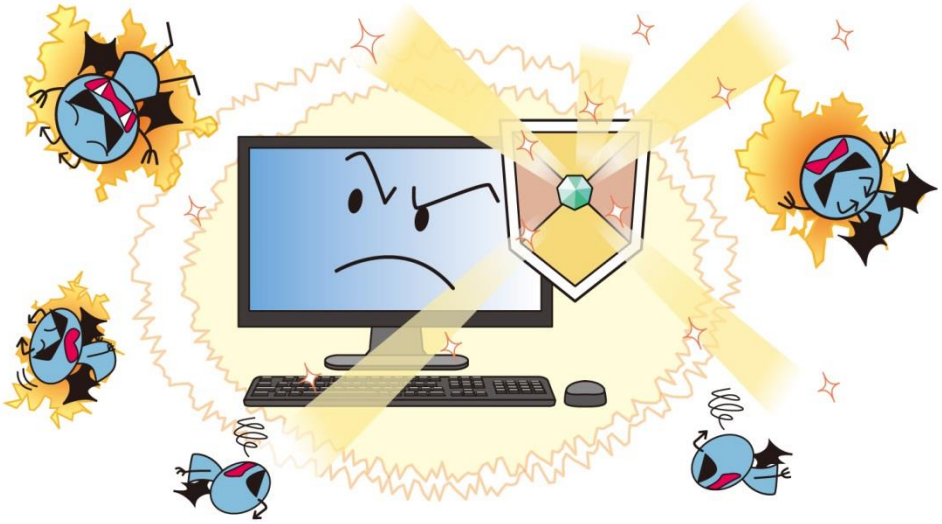
◆　パソコン利用者に求められる対応

多くの攻撃者は、インターネットやメールを閲覧するパソコン内の Internet Explorer を含む Microsoft 製品、Adobe Flash Player、Adobe Reader、Oracle JAVA(JRE)等の脆弱性を標的にしている。そのため、これらの製品の更新（アップデート）が提供され次第、速やかに更新して脆弱性を解消する必要がある。自動のソフトウェア更新や更新チェックを行う機能を動作させるために定期的にパソコンやソフトウェアを再起動すること、画面上に更新の通知があれば必ず更新を実施することを習慣化すると良い。IPA[1] が提供している MyJVN バージョンチェッカ[2] 等のツールを利用して、利用するソフトウェアが最新であるか定期的に確認することも有効な対策の 1 つである。

◆　企業・組織に求められる対応

利用するソフトウェアやネットワーク対応機器について、製品名とバージョン情報を把握しておき、製品開発者のウェブサイトで公開される脆弱性対策情報や IPA が公開する「重要なセキュリティ情報」[3] 等から脆弱性の情報を随時収集する。収集した情報に利用する製品があれば、重要度等に応じて関係先（組織内や顧客等）への周知やソフトウェアの更新の実施等の対応を行う。システムの規模が大きい場合は、一部で検証を行った上で対応を判断する。脆弱性への対応を迅速に行うためには、脆弱性対応の担当者を明確する等、企業・組織内の体制を構築しておくことが望ましい。

1.2. ウイルス対策ソフトの導入



パソコンやスマートフォン等の乗っ取りや金銭被害に遭わないためには、利用する端末をウイルス感染から守る必要がある。ウイルス対策ソフトを導入することで、既知のウイルスの感染を未然に防ぐことができる。

◆　既知のウイルスの感染を防ぐ

ウイルス感染による被害が後を絶たない。ウイルス対策ソフト開発企業は、日々新しいウイルスを解析し、パターンファイルを更新して配信している。これにより、ウイルス対策ソフトで膨大な種類のウイルスを検知できる。既知のウイルスの感染を未然に防止するために、ウイルス対策ソフトの導入は必要不可欠な対策となっている。

◆　ウイルス感染の経路

ウイルスの感染経路は様々であり、主な感染経路は以下の通りである。

- ウェブサイトの閲覧（改ざんされたサイト、アダルトサイト、不正な広告等）
- ファイルを開く（メールの添付ファイル、ネットで公開されているファイル）
- ソフトウェアのインストール（悪意のあるソフトウェアと知らずにインストール）

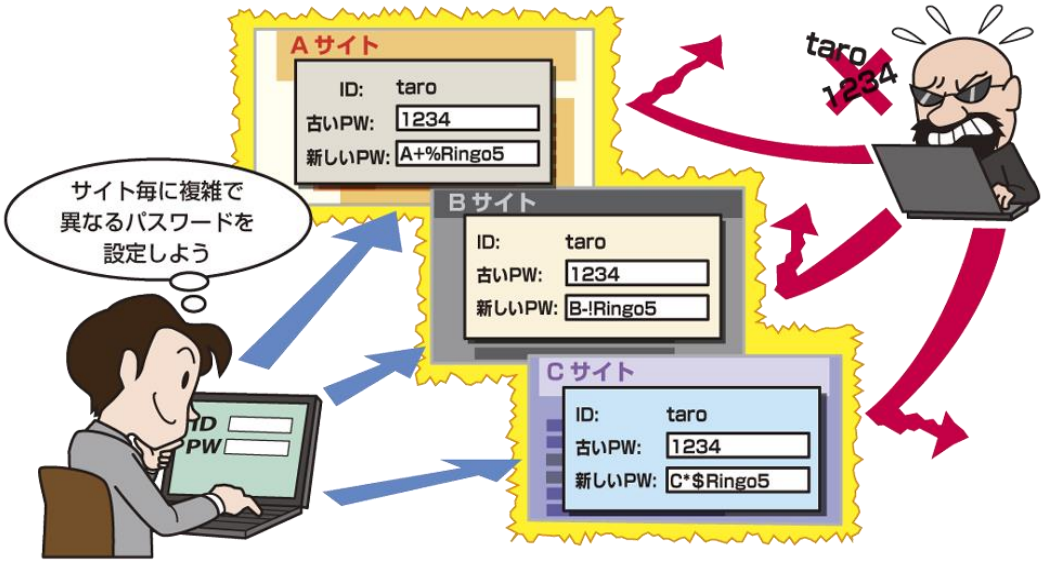
◆　ウイルス対策ソフトによる検知の限界

従来のウイルス対策ソフトが用いるパターンマッチングは既知のウイルスの検知に強い。しかしながら、ウイルス対策ソフトの多くは未知のウイルスを検知できない。近年は、未知のウイルスに対抗するため、ウイルスの振る舞い等を研究し、検知手法に取り入れているウイルス対策ソフトもある。

◆　ウイルス対策ソフトへの過信は禁物

ウイルス作成者は、新しい巧妙な手口を日々模索しており、ウイルス対策ソフトの検知から逃れるウイルスも多くなっている。ウイルス対策ソフトだけですべてのウイルス感染から防御できるわけではない。ウイルス対策ソフトの検知能力を過信せずに１章で説明する他の対策も併せて行い、情報システムを多層（多段）で防御していく必要がある。

1.3. パスワードの適切な管理と認証の強化



パスワードは設定した文字列を利用者本人だけが知っていることを前提とした認証方式であり、パスワードは第三者に知られてはならない。推測されにくいパスワードを設定し、かつパスワードを使い回さないことが不正ログインの防止に有効である。

◆ **短く推測されやすいパスワードは危険**

短いパスワードを設定している場合、パスワードを総当たりでログイン試行され、不正にログインされてしまう。また、パスワードに誕生日や名前、使われやすい文字列を設定している場合、パスワードを推測されて、不正にログインされてしまう。

◆ **サービス毎に異なるパスワードを設定**

ID とパスワードを複数のウェブサービスで使い回している場合、十分な文字数で推測困難なパスワードを設定していたとしても、どこか 1 つのサービスから漏えいした ID とパスワードを用いた「パスワードリスト攻撃」による不正ログインを防ぐことができない。この攻撃の被害に遭わないためには、サービス毎に異なるパスワードを設定しておく必要がある。[4]

◆ **適切なパスワードの作成・管理**

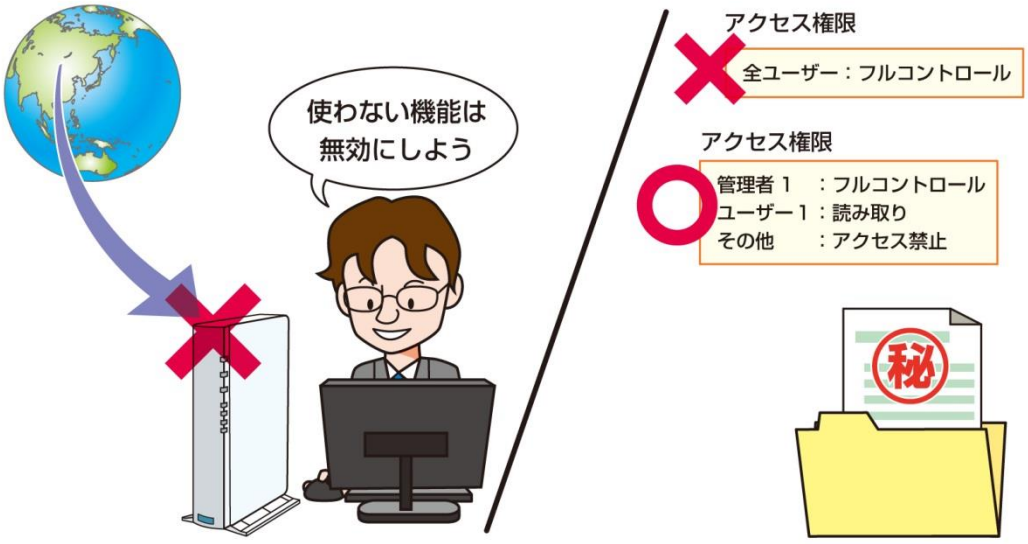
パスワードは、8 文字以上の文字列でアルファベットの小文字や大文字、数字や記号を組み合せる等の作成方法と、どのように記憶や記録をするかの管理方法が重要である。[5]

各々が自分に合ったパスワードの作成方法と管理方法を考えるのが一番だが、例えば、記憶できる文字列を決め、その文字列にサービス毎に 3 桁や 4 桁の異なる数字や記号を付け足すことで、異なるパスワードを作成できる。そして、作成したパスワードの文字列から、サービス毎の差分（記憶できない部分）だけ電子ファイルや手帳等に記録すると管理しやすい。また、パスワード管理ツールの利用も選択肢の一つと言える。[6]

◆ **認証の強化**

サービスによっては、PIN コードやワンタイムパスワード、電子証明書等を用いた多要素認証が提供されている。不正利用による金銭被害が懸念されるサービスでは、多要素認証方式を活用し、より安全にサービスを利用することが望ましい。[7] [8]

1.4. 設定の見直し



ソフトウェアのインストール直後およびサーバーやネットワーク対応機器等の購入時点では、不要な機能が有効になっている製品や機能へのアクセス制限が設定されていない製品がある。情報漏えいや乗っ取り等の被害を防止するため、利用開始時の設定確認や定期的な設定の見直しを行う必要がある。

◆　利用開始時に設定を確認する

利用しない機能や不要な設定は無効にする。また、セキュリティを強化する機能や設定は有効にする。必要性が分からない場合は、マニュアルやインターネット上の情報を確認して、必要か不要か判断する。

特に、ブロードバンドルーターや、複合機、ウェブカメラ等のネットワーク対応機器の各種機能の設定、例えばユーザー認証の有効化設定やファイル共有設定等を、必要に応じて適切な設定に変更する。[9] また、パソコンに初期インストールされているソフトウェアについても不要と判断できるものはアンインストールしておくことで、リスクを低減できる。

◆　アクセス制限や権限を設定する

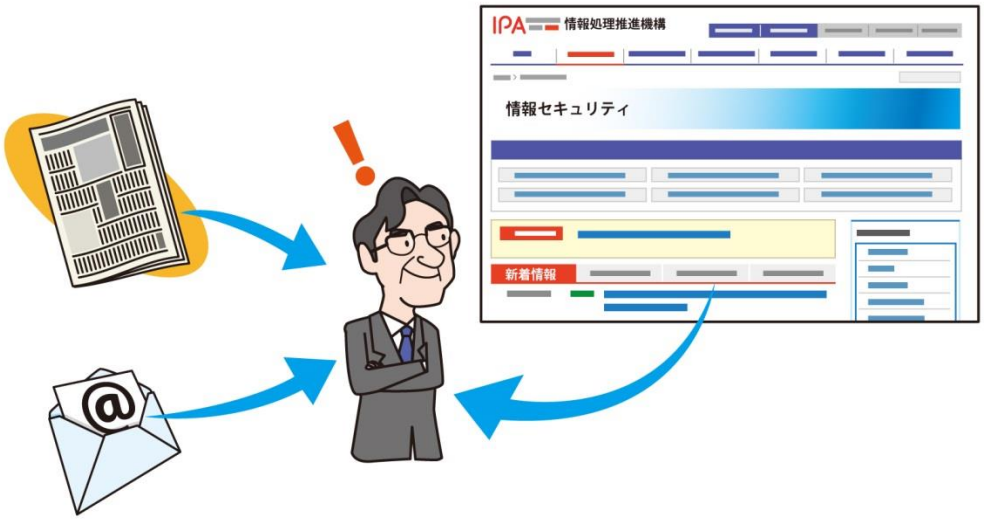
初期状態においてアクセス制限されておらず、管理機能やデータを誰でも利用できるように設定されているソフトウェアや機器が存在する。攻撃者に、機密情報を閲覧される、設定変更される等の被害を防止するためには、利用開始前にアクセス制限機能を有効にし、利用者毎のユーザーアカウントの作成とアクセス権限の付与を適切に行う必要がある。

特に、重要なファイルが保存されているフォルダのアクセス権限は、全アカウントが閲覧や削除ができる設定（フルコントロール）にせずに、特定のアカウントのみがアクセスできるように設定する。

◆　設定の見直しを実施する

企業・組織の場合、職員の退職時には速やかにユーザーアカウントを抹消する。また、職員の部署異動時には、アカウントに付与したアクセス権限を見直す必要がある。

1.5. 脅威や手口を知る



振り込め詐欺等の代表的な犯罪の手口を事前に知っておくことで被害に遭いづらくなる。情報セキュリティにおいても、脅威や対策を把握しておくことは被害の予防につながる。

◆ 情報技術(IT)の犯罪への悪用

パソコンやインターネット等の IT は、様々な分野に活用され生活に欠かせないものになっている。しかし、IT は犯罪にも悪用されていることを忘れてはならない。年々、犯行手口は巧妙化している。

◆ 言葉巧みに画面をクリックさせる手口

脆弱性を突く等の高度な技術が攻撃に悪用されている一方で、メールやウェブサイトを使って言葉巧みに誘導して画面をクリックさせる手口も存在する。例えば、会費無料と謳っておきながら突然高額な請求画面を表示するワンクリック請求[10][11]と呼ばれる手口や、有用なソフトと偽ってウイルス等をインストールさせる手口[12][13]等がある。これらのように人を巧みに誘導する手口を知っておくことで、犯罪者の仕掛けた罠に気付き、被害を未然に防ぐことができる。

◆ 自発的な情報収集を

報道、製品・サービスの提供者やセキュリティ関連機関の注意喚起等の情報源から、セキュリティに関する脅威を知ることができる。IPA が公表する「今月の呼びかけ」[14]、官公庁やセキュリティ企業が公表するレポートを参照することで、最新の脅威の動向と手口や対策等の情報を得られる。こうした情報を定期的に収集する習慣を付けることが重要である。また、毎年 3 月に発行される本書「情報セキュリティ 10 大脅威」[15]では、昨今の脅威の動向や今後注意すべき脅威等の情報を入手できる。

◆ 万一の時も冷静に

請求画面が表示されても絶対に振り込んではいけない。また、偽ウイルス対策ソフトのインストール画面等の確認画面が突然表示された場合も安易にボタンをクリックしてはいけない。上司等の身近な人やセキュリティ対策部門に報告し、相談することも必要である。他にも、IPA(技術面の相談)[16]、消費者庁(契約に関する相談)[17]、警察庁(違法行為の取り締まり)[18][19]等の支援機関の窓口に相談できる。

1.6. その他の重要な対策

前節までに解説した対策の他にも、企業・組織において情報システムやデータ等の情報資産を守るために効果があり、実施すべき対策がある。本節では、その対策の例を示す。

◆　情報資産の把握

企業・組織は、適切にセキュリティ対策を行うために、情報資産を把握しなければならない。重要なデータ、社内システムや業務用パソコン等の情報資産の存在はもちろん、脆弱性への対応のために利用しているソフトウェアはバージョン番号まで把握する。また、適切な移行計画のために、ソフトウェアのサポートの終了時期についても把握する。

◆　文書によるセキュリティ対策の明文化

セキュリティポリシー、就業規則、秘密保持契約等の文書や書類で、実施すべきセキュリティ対策や禁止事項に抵触した場合の罰則を明確にする。文書により明示化することは、従業員・職員の内部不正に対する「心のブレーキ」となる。また、システム開発や運用を外部に委託する場合にも、セキュリティ対策の実施を誓約する文書を取り交わすことで、委託先でのセキュリティ事故を抑制できる。

◆　システムによる制限や強制

Active Directory の活用や LAN スイッチ等のネットワーク機器の設定によるネットワーク分離等、既存の機器に適切な設定を施すことも有効な対策の 1 つとなる。

また、セキュリティ製品の導入によって、攻撃の緩和・検知、従業員・職員の行動制限、対策実施の強制等が可能となる。以下にセキュリティ製品の例を挙げる。

- ファイアウォール
- 認証付きプロキシサーバー
- ウェブフィルタリング
- メールフィルタリング
- 侵入検知システム
- ネットワーク検疫　等 [20]

◆　バックアップやシステムの冗長化

予期せぬ攻撃や障害により、データ消失やシステムダウンに見舞われる可能性がある。重要なデータはバックアップを行い、停止が許容されないシステムは、冗長構成にしておくことが重要である。

◆　検査や監査、セキュリティ認証の取得

システムの運用開始前に検査を行い、脆弱性の対処漏れや設定ミス等セキュリティ上の問題が無いか確認することも、重要なシステムやデータを守るためには必要なプロセスである。

運用中も定期的または随時監査して対策の実施有無や有効性を確認する。プライバシーマークや ISO/IEC27001 等のセキュリティ認証を継続的に取得することで、セキュリティポリシーや社内ルール等が遵守され、有効に機能しているかを評価でき、継続的な改善につながる。また、認証の取得によって顧客等の対外的な信頼を得ることも期待できる。

◆　対策には計画と予算が必要

企業・組織は重要な情報資産を把握し、重要度に応じて継続的に予算を確保して段階的かつ計画的に対策を行う必要がある。また、突発的なセキュリティ事故の対応費用についても予算化しておく必要がある。

1章.情報セキュリティ対策の基本：参考資料

1. IPAトップページ
https://www.ipa.go.jp/
2. IPA：MyJVNバージョンチェッカ
http://jvndb.jvn.jp/apis/myjvn/vccheck.html
3. IPA：重要なセキュリティ情報一覧
https://www.ipa.go.jp/security/announce/alert.html
4. IPA：2013年8月の呼びかけ「 全てのインターネットサービスで異なるパスワードを！ 」
https://www.ipa.go.jp/security/txt/2013/08outline.html
5. IPA：チョコっとプラスパスワード
https://www.ipa.go.jp/chocotto/pw.html
6. IPA：パスワードリスト攻撃による不正ログイン防止に向けた呼びかけ
https://www.ipa.go.jp/about/press/20140917.html
7. IPA：2013年9月の呼びかけ「 インターネットバンキング利用時の勘所を理解しましょう！ 」
https://www.ipa.go.jp/security/txt/2013/09outline.html
8. IPA：2014年8月の呼びかけ「 法人向けインターネットバンキングの不正送金対策、しっかりできていますか？ 」
https://www.ipa.go.jp/security/txt/2014/08outline.html
9. IPAテクニカルウォッチ「増加するインターネット接続機器の不適切な情報公開とその対策」
https://www.ipa.go.jp/about/technicalwatch/20140227.html
10. IPA：2013年5月の呼びかけ「 スマホにおける新たなワンクリック請求の手口に気をつけよう！ 」
https://www.ipa.go.jp/security/txt/2013/05outline.html
11. IPA：2014年6月の呼びかけ「 登録完了画面が現れても、あわてないで！ 」
https://www.ipa.go.jp/security/txt/2014/06outline.html
12. IPA：2013年4月の呼びかけ「 どうして偽セキュリティ対策ソフトがインストールされるの？ 」
https://www.ipa.go.jp/security/txt/2013/04outline.html
13. IPA：2015年2月の呼びかけ「 その警告表示はソフトウェア購入へ誘導されるかも知れません 」
https://www.ipa.go.jp/security/txt/2015/02outline.html
14. IPA：今月の呼びかけページ
https://www.ipa.go.jp/security/personal/yobikake/
15. IPA：情報セキュリティ10大脅威 2015
https://www.ipa.go.jp/security/vuln/10threats2015.html
16. IPA：情報セキュリティ安心相談窓口
https://www.ipa.go.jp/security/anshin/
17. 国民生活センター：全国の消費生活センター等
http://www.kokusen.go.jp/map/index.html
18. 警察庁：窓口・手続き案内
http://www.npa.go.jp/annai/index.htm
19. 警察庁：都道府県警察本部のサイバー犯罪相談窓口等一覧
http://www.npa.go.jp/cyber/soudan.htm
20. JNSA：ソリューションガイド
http://www.jnsa.org/JNSASolutionGuide/IndexAction.do

付録：情報セキュリティ船中八策

江戸時代に坂本龍馬がまとめたと言われる「船中八策」にあやかり、１章で解説した情報セキュリティの基本的な対策からさらに８つを厳選した「情報セキュリティ船中八策」を以下に示す。

情報セキュリティ船中八策

一、ソフトウェアの更新
～ 善は急げ ～

二、ウイルス対策ソフトの導入
～ 予防は治療に勝る ～

三、パスワードの適切な管理
～ 敵に塩を送ることのなきように ～

四、認証の強化
～ 念には念を入れよ ～

五、設定の見直し
～ 転ばぬ先の杖 ～

六、脅威・手口を知る
～ 彼を知り己を知れば百戦殆からず ～

七、クリック前に確認
～ 石橋を叩いて渡る ～

八、バックアップ
～ 備えあれば憂いなし ～

2章. 情報セキュリティ10 大脅威 2015

2 章　情報セキュリティ 10 大脅威　2015

2014 年において社会的影響が大きかったセキュリティ上の脅威について、「10 大脅威執筆者会」の投票結果に基づき、表 2.1 の通り順位付けした。

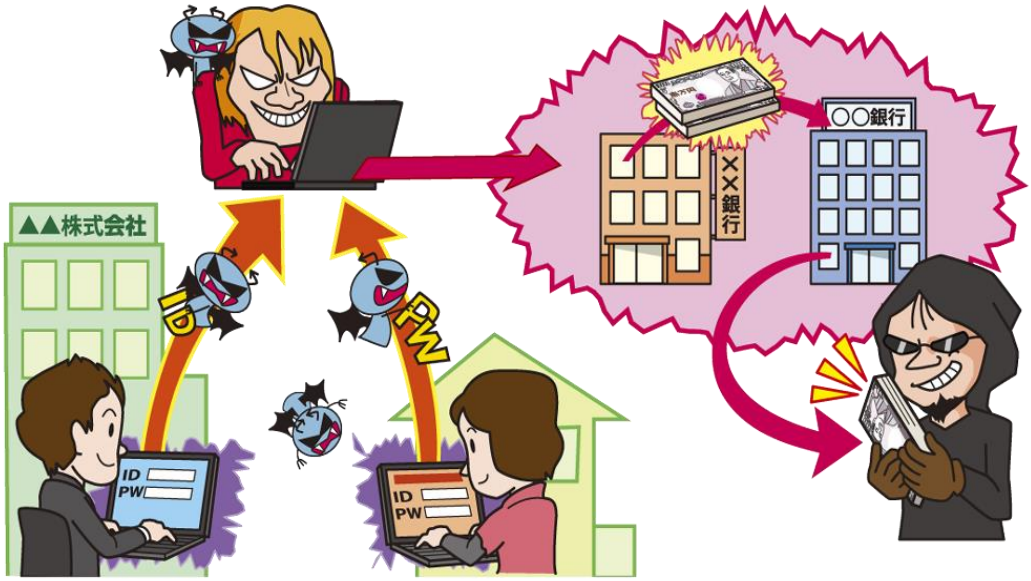
本章では、それぞれの脅威について解説する。

表 2.1：情報セキュリティ 10 大脅威 2015

順位	タイトル
1	**インターネットバンキングやクレジットカード情報の不正利用** ～個人口座だけではなく法人口座もターゲットに～
2	**内部不正による情報漏えい** ～内部不正が事業に多大な悪影響を及ぼす～
3	**標的型攻撃による諜報活動** ～標的組織への侵入手口が巧妙化～
4	**ウェブサービスへの不正ログイン** ～利用者は適切なパスワード管理を～
5	**ウェブサービスからの顧客情報の窃取** ～脆弱性や設定の不備を突かれ顧客情報が盗まれる～
6	**ハッカー集団によるサイバーテロ** ～破壊活動や内部情報の暴露を目的としたサイバー攻撃～
7	**ウェブサイトの改ざん** ～知らぬ間に、ウイルス感染サイトに仕立てられる～
8	**インターネット基盤技術を悪用した攻撃** ～インターネット事業者は厳重な警戒を～
9	**脆弱性公表に伴う攻撃** ～求められる迅速な脆弱性対策～
10	**悪意のあるスマートフォンアプリ** ～アプリのインストールで友人に被害が及ぶことも～

1位　インターネットバンキングやクレジットカード情報の不正利用

～個人口座だけではなく法人口座もターゲットに～



ウイルスやフィッシング詐欺により、インターネットバンキングの認証情報やクレジットカード情報が窃取され、利用者本人になりすました攻撃者による不正送金や不正利用が行われた。2014年は、個人口座だけでなく法人口座からの不正送金被害が急増した。

＜主な攻撃者＞

犯罪グループ

＜主な被害者＞

・インターネットバンキング利用者(法人含む)、クレジットカード利用者
・銀行、カード運営会社

＜脅威と影響＞

インターネットバンキングやインターネットを介したクレジットカードの利用が広く普及するのに伴い、これらの不正利用を目的とする攻撃も増加している。攻撃者がウイルスやフィッシング詐欺によって窃取したIDとパスワードやクレジットカード情報を不正利用することで、金銭的な被害が生じる。

2014 年は日本をターゲットにした不正送金ウイルスが横行し、個人口座だけでなく法人口座にも被害が拡大した。ネット銀行、大手銀行から地方銀行や信用金庫まで幅広く狙われている。また、レジ等で使用されるPOS(販売時点情報管理)システムをウイルス感染させクレジットカード情報を窃取する事件が発生している。海外ではその被害が年々増加しており、国内でも今後被害が拡大する可能性がある。

＜攻撃手口＞

◆　ウイルス感染

悪意のあるウェブサイトを閲覧する等によってパソコンがウイルスに感染する。そのパソコンで利用者が入力したIDとパスワードや口座番号等の情報が攻撃者に窃取される。攻撃者は窃取した情報を使用して、正規

の利用者になりすましてインターネットバンキングにログインし、不正送金を行う。

また、ウイルスがブラウザとサーバーとの通信を傍受して不正送金を行う MITB（Man In The Browser）攻撃と呼ばれる手口も確認されている。

◆ **フィッシング詐欺**

攻撃者は、実在する銀行やクレジットカード会社、オンラインゲーム運営会社等を装ったメールを送信する。被害者は、実在する企業・組織からのメールと思い込み、メールに記載されているリンクから偽のサイトに誘導され、認証情報やクレジットカード情報を入力してしまう。攻撃者は、その情報を悪用して不正ログインや不正送金を行い、金銭を窃取する。

＜事例と傾向＞

◆ **不正送金被害が急増**

警察庁によると、2014 年のインターネットバンキングに関わる不正送金の被害額は 29 億 1,000 万円となり、2013 年の 14 億 600 万円に対し、被害額が約 2 倍に急増した。特に法人口座の被害額は、2013 年の 9,800 万円から 2014 年には 10 億 8,800 万円と約 11 倍に増加している。[I]

◆ **法人口座を狙ったウイルス**

法人向けのインターネットバンキングの認証を強化するために、銀行が発行する電子証明書を使える場合がある。電子証明書は正当な利用者であることを保証する役割を担っている。しかし、ウイルスが電子証明書と秘密鍵を窃取し、攻撃者が正当な利用者になりすまして不正送金する手口が確認された。[II]

◆ **大手銀行を装ったフィッシング詐欺**

2014 年は大手銀行を装ったフィッシング詐欺が横行した。三菱東京 UFJ 銀行を装ったフィッシング詐欺では、偽メールで「個人情報漏えい事件が発生した」と顧客を不安にさせ、偽のログイン画面へ巧妙に誘導した。また、偽のログイン画面であるにも関わらず「偽画面にご注意！」と表示して顧客を信頼させるように巧妙に作り込まれていた。[III]

＜主な対策・対応＞

銀行・カード運営会社向け

- 利用者への事例や手口の情報提供
- 二要素認証等の強い認証方式の提供

利用者向け

- ソフトウェアの更新
- ウイルス対策ソフトの導入
- 事例や手口を知る
- 二要素認証等の強い認証方式の利用

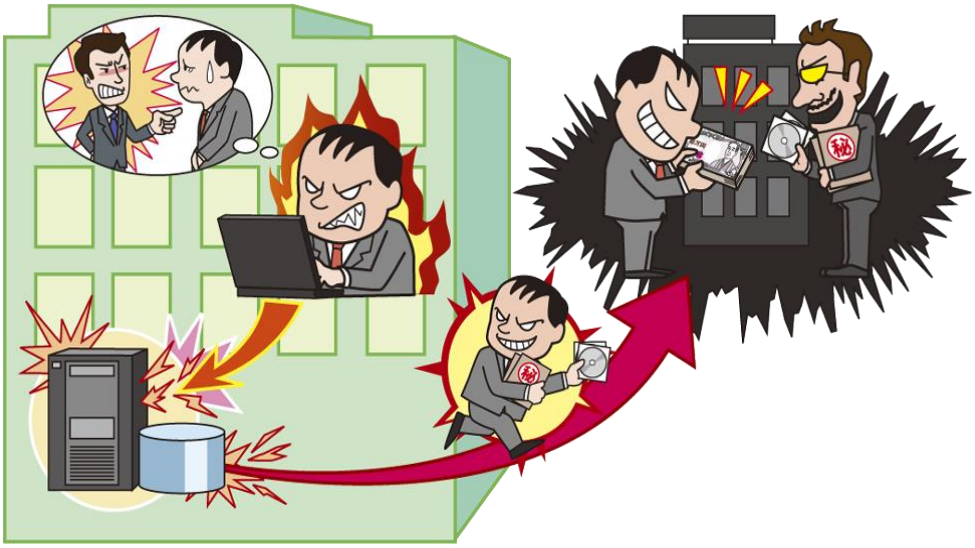
インターネットバンキングやクレジットカードの利用者は、利用している銀行やカード会社のホームページからフィッシング詐欺の事例等を知り、騙されないよう心がけることが重要である。また、銀行によってはインターネットバンキング専用のウイルス対策ソフトや二要素認証等が提供されているため、それらを利用することで安全性が高まる。

参考資料

I. 警察庁：平成26年中のインターネットバンキングに係る不正送金事犯の発生状況等について
http://www.npa.go.jp/cyber/pdf/H270212_banking.pdf
II. IPA：2014年8月の呼びかけ「 法人向けインターネットバンキングの不正送金対策、しっかりできていますか？ 」
https://www.ipa.go.jp/security/txt/2014/08outline.html
III.「偽画面にご注意！」、三菱東京UFJ銀行をかたるフィッシング
http://itpro.nikkeibp.co.jp/article/NEWS/20140610/562867/

2位　内部不正による情報漏えい

～内部不正が事業に多大な悪影響を及ぼす～



企業の従業員が内部情報を窃取し、第三者に販売した事件が社会的な問題となった。内部の人間が悪意を持つと、その人間がアクセスできる範囲で自由に情報を窃取できるため、情報の重要度に応じたアクセス権限の設定や退職者のアクセス権の抹消等、厳重な管理と監視を継続的に行う必要がある。

＜主な攻撃者＞

・企業、組織関係者

＜主な被害者＞

・企業、組織

・顧客

＜脅威と影響＞

組織内部の職員が悪意を持ち、与えられた権限を用いて内部情報を取得し、名簿業者に販売したり、私的に利用したりする事件が度々発生する。

内部不正は正規の権限を持つ人間が実行するため、ポリシー等に基づいた制約だけでは犯行を防ぐことが難しい。正規のアクセス権限を持つ職員であれば、容易に内部情報を持ち出せるためである。

顧客情報や製品情報の漏えいを引き起こした企業・組織には、賠償や、信用失墜による株価下落、競争力の低下等、事業に多大な悪影響を及ぼすことが考えられる。

＜発生要因＞

内部不正が発生する要因として、以下の動機、機会、正当化の３つが挙げられる。

- **動機**

仕事へのプレッシャーや、不当な解雇や社内の人事評価の低さ等の処遇面の不満、借金による生活苦等が、内部不正を行わせる動機となる。また、システム操作の記録と監視をしていない場合、発覚しないという思い込みが不正行為を助長する。監視していることを周知することは動機の抑止になる。

- **機会**

アクセス制限の未設定や、異動者や退職

者のアクセス権限を抹消していない等、重要な内部情報にアクセスできる人間が必要以上に多い場合、悪意を持つ人間に犯行の機会を与えてしまう。

利便性の観点から 1 つの管理者アカウントを複数の職員で共有して使用している場合も、共有する全員が必要以上の権限を持ってしまう。この場合、誰が操作を行ったのかを特定できない問題も伴う。

- **正当化**

一時的に情報を借りるだけなら犯罪にはならないという自分勝手な理由や不満への報復心で、自らを納得させ、犯行に及ぶ。

＜事例と傾向＞

◆ **内部犯行による膨大な個人情報漏えい**

2014 年 7 月、通信教育大手のベネッセコーポレーションは、システムを保守管理する委託先企業の社員が、顧客の個人情報を不正に持ち出し、約 3,504 万件分を名簿業者に販売していたと公表した。この事件は、当該企業に提供した個人情報を使ったダイレクトメールが届いた等の顧客からの問い合わせにより発覚した。情報が漏えいした顧客への補償として総額 200 億円を準備したことを発表した。[I]

◆ **海外への技術情報の漏えい**

東芝と業務提携していた半導体メーカーのサンディスクの社員が、東芝の研究データを不正に持ち出し、転職先の韓国の半導体大手 SK ハイニックスに流出させた。2014 年 12 月、SK ハイニックスが東芝に約 330 億円の損害賠償を支払うことで企業間の和解が成立した。[II]

＜主な対策・対応＞

経営者層

- 就業規則およびポリシーの整備
- 職員や委託先への秘密保持誓約の徹底
- 対策を推進できる体制の構築

セキュリティ担当部署

- セキュリティ教育の実施

システム管理者

- 情報資産の把握と重要度による分類
- アカウントや権限の管理（設定・抹消）
- システム操作の記録と監視
- 入退室の監視や持ち込み物等の確認

従業員・職員

- セキュリティ教育の受講

経営者層が対策について責任を持ち、組織の保持している情報資産を重要度等で分類し、積極的に対策を推進する体制を構築することが対策のポイントとなる。また、社員・職員一人ひとりに耳を傾け、業務や職場に対する不満を低減する方法を提供することも重要な対策となる。

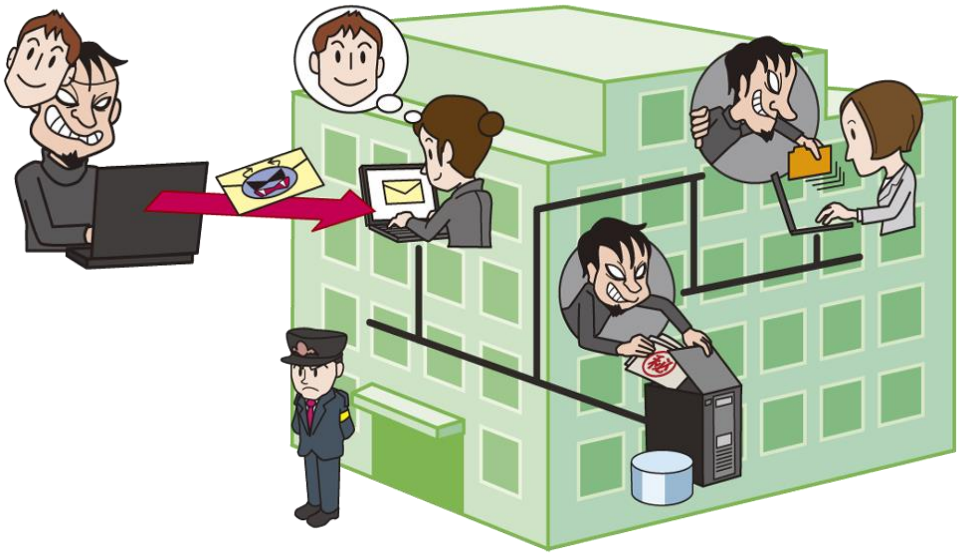
これらの対策は網羅的に行う必要がある。IPA が公開している「組織における内部不正防止ガイドライン」のチェックリストを用いることで、現状の対策を見直すことができる。[III]

参考資料

I. ベネッセコーポレーション：事故の経緯
http://www.benesse.co.jp/customer/bcinfo/01.html
II. 東芝、SKハイニックスから和解金330億円　提携拡大
http://www.nikkei.com/article/DGXLASDZ19I08_Z11C14A2MM8000/
III. IPA：組織における内部不正防止ガイドライン
https://www.ipa.go.jp/security/fy24/reports/insider/

3位　標的型攻撃による諜報活動

～標的組織への侵入手口が巧妙化～



ウイルスに感染させたパソコンを外部から遠隔操作して、内部情報を窃取する標的型攻撃による被害が政府機関や民間企業で後を絶たない。2014 年は、さらに巧妙化した手口が確認され、取引先や関連会社を踏み台にして目的の組織を狙う等の傾向が見られた。

＜主な攻撃者＞

・諜報員、産業スパイ

＜主な被害者＞

・企業・組織

＜脅威と影響＞

知財情報や顧客情報は企業・組織の事業の根幹となる重要な情報であり、競合する企業・組織の手に渡れば、事業に多大な影響を及ぼす可能性がある。

重要情報を窃取しようとする国家的な諜報活動や産業スパイ活動は、古くから存在するが、現在では標的型攻撃と呼ばれる IT を活用した手法により、インターネットとウイルスを用いて遠隔から隠密裏に諜報活動が行われている。

標的型攻撃は、メールやウェブサイト、外部媒体等によって標的企業・組織のパソコンにウイルスを感染させ、組織内部に潜入する。その後、ウイルス感染したパソコンを遠隔操作して組織内部の情報を探索し、情報を外部に送信する。

2014 年、地方公共団体や政府機関の下部組織、大手企業の関連会社等のセキュリティ対策が不十分な企業・組織を探して踏み台とし、複数企業を経由して最終的にターゲットの組織を狙う傾向が顕在化している。

＜攻撃手口＞

多くの場合、標的型攻撃は複数の攻撃手法を組み合わせ、以下の攻撃シナリオに沿って遂行される。

(1)　計画立案
(2)　攻撃準備（標的組織の調査）
(3)　初期潜入（ウイルス感染）
(4)　基盤構築（感染拡大）

(5)　内部侵入・調査（文書の探索）
(6)　目的遂行（外部へのデータ送信）
(7)　再侵入

この中の「(3)初期潜入」では、ウイルスが含まれるファイルをメールに添付し、不特定多数に送付する「ばらまき型」、標的とメールのやり取りを行った後にウイルスが含まれるファイルを送付する「やり取り型」、ウェブサイトを閲覧することでウイルスに感染させる「水飲み場型」等、様々な手口が確認されている。[I]

＜事例と傾向＞

◆　やり取り型攻撃を国内 5 組織で確認

IPA は、2014 年 8 月から 10 月にかけ、少なくとも国内 5 つの組織に対して、やり取り型攻撃の発生を確認した。ある事例では、攻撃者は最初に、セミナーについて問い合わせしたいと相談を持ちかけ、相談の了承を得てから、ウイルス入りの質問書を送付していた。やり取り型攻撃は、業務として問い合わせに対応せざるを得ない立場（窓口業務等）を巧妙に悪用した手口である。[I]

◆　一太郎のゼロデイの脆弱性を悪用

2014 年 11 月、日本語文書作成ソフト「一太郎」の脆弱性を悪用してウイルスに感染させる手口が確認された。ウイルス感染に悪用されたのは、修正プログラム（パッチ）が公開される前の、いわゆるゼロデイの脆弱性であった。[II]

＜主な対策・対応＞

経営者層

- 問題に迅速に対応できる体制の構築

セキュリティ担当部署

- セキュリティ教育の実施

システム管理者

- システム設計対策
- アクセス制限
- ネットワークの監視

従業員・職員

- セキュリティ教育の受講

標的型攻撃は、脆弱性対策やウイルス対策等の基本的な対策を巧妙にすり抜けて組織内部に侵入する。そのため、組織内部に侵入されることを前提に、機密情報を内部で「多層防御」できる環境を構築する。具体的には、情報システム全体に目を向け、ネットワークの分離や、機密情報には適切にアクセス権限を付与する等の対策が必要不可欠となる。対策の詳細については IPA の「『高度標的型攻撃』対策に向けたシステム設計ガイド」[III]や「標的型攻撃メールの例と見分け方」[IV]が参考になる。

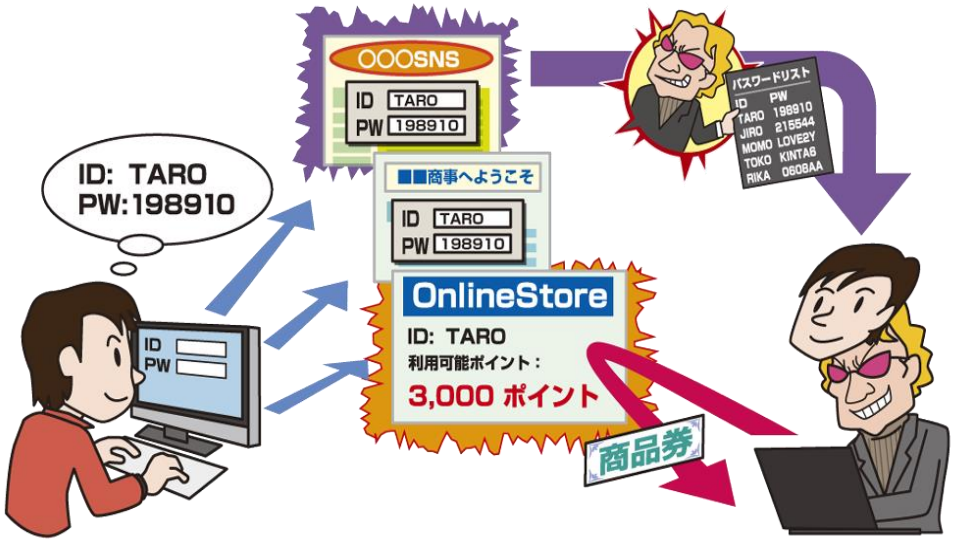
なお、IPA では、標的型攻撃に関する「標的型サイバー攻撃の特別相談窓口」で相談を受け付けている。[V]

参考資料

I. IPA：組織外部向け窓口部門の方へ：「やり取り型」攻撃に対する注意喚起 ～ 国内5組織で再び攻撃を確認 ～
https://www.ipa.go.jp/security/topics/alert20141121.html
II. 「一太郎」の脆弱性、日本を狙うゼロデイ攻撃で使用
http://www.nikkei.com/article/DGXMZO79698680U4A111C1000000/
III. IPA：「高度標的型攻撃」対策に向けたシステム設計ガイド
https://www.ipa.go.jp/security/vuln/newattack.html
IV. IPAテクニカルウォッチ「標的型攻撃メールの例と見分け方」
https://www.ipa.go.jp/security/technicalwatch/20150109.html
V. IPA標的型サイバー攻撃の特別相談窓口
https://www.ipa.go.jp/security/tokubetsu/

4位　ウェブサービスへの不正ログイン

～利用者は適切なパスワード管理を～



攻撃者に ID とパスワードを知られることで不正ログインの被害に遭う。2014 年も、脆弱なウェブサービスから窃取した ID とパスワードを悪用して、別のサービスに不正にログインされる被害が多発した。ID とパスワードを複数のサービスで使い回している利用者が被害に遭っている。

＜主な攻撃者＞

・犯罪グループ

＜主な被害者＞

・ウェブサービス利用者

＜脅威と影響＞

会員登録が必要なウェブサービスにおいて、ID とパスワードによる認証方式が標準的な認証手段として採用されている。パスワードは自分のみが知っていることを前提とした認証であるため、第三者にパスワードを知られてはならない。

しかし、パスワードに、連続した英数字、password 等のよく使われる英単語、自分の名前等、安易な文字列を設定している場合、攻撃者に推測される可能性が高くなる。[I]

また、複数のウェブサービスで同じパスワードを使い回している場合、特定のウェブサービスから ID とパスワードが漏えいすることで、他のウェブサービスの ID とパスワードも攻撃者に知られてしまう。パスワードを使い回す理由は「パスワードを忘れてしまう」ためが最も多い。多数のウェブサービスを利用していることも、パスワードの使い回しの背景にある。[II]

攻撃者にウェブサービスへ不正にログインされると、提供しているサービスを悪用されるため、個人情報の漏えいや金銭被害等、不正利用による様々な被害が発生する。例えば、ショッピングサイトに不正ログインされた場合、登録住所を見られたり、勝手に注文されたり、貯まっているポイントを窃取されたりする等の被害を受ける可能性がある。

＜攻撃手口＞

◆　**パスワード推測**

誕生日や名前、電話番号の一部等、使われやすい文字列をパスワードとして入力し、ログインを試みる方法である。利用者はパスワードを忘れないよう身近な文字列を使う可能性があるため、攻撃者は攻撃対象の個人情報を元にログインを試行する場合もある。

◆ **ウイルス感染**

パソコンやスマートフォンに感染するウイルスが、端末内部に記録している ID とパスワードを外部に送信してしまう。また、キーロガーと呼ばれるウイルスに感染した場合、キーボード入力した ID とパスワードが攻撃者に送信される場合もある。

◆ **パスワードリスト攻撃**

脆弱なウェブサイト等から窃取した ID とパスワードのリストを使い、他のウェブサイトに不正アクセスを仕掛ける方法である。利用者側で強固なパスワードを設定していても、パスワードを使い回している限り、パスワードリスト攻撃の被害を防ぐことはできない。

＜事例と傾向＞

◆ **SNS サービス LINE への不正ログイン**

2014 年 6 月、LINE に不正ログインし、不正ログインしたユーザーの友人にプリペイドカードを購入させる事件が相次ぎ、社会的な問題となった。他社サービスのログイン情報を用いて不正ログインしたと運営会社は推測している。[III]

◆ **JAL、ANA への不正ログイン**

2014 年 2 月に JAL、3 月に ANA のマイレージサービスが不正ログインされ、個人情報の漏えいやポイントが不正利用される被害が発生した。当時は、パスワードに 4 桁または 6 桁の数字しか登録できない問題を抱えていた。覚えやすい数字を設定している利用者が狙われたと考えられている。[IV]

＜主な対策・対応＞

ウェブサービス利用者

- 推測されにくいパスワードを設定
- パスワードを使い回さない
- 二要素認証等の強い認証方式の利用

サービス提供者

- 安全なウェブサービスの提供
- 複雑なパスワード設定を要求（少ない文字数の拒否、記号の使用の確認等）
- 二要素認証等の強い認証方式の提供

利用者は、パスワードの適切な管理方法を知り、実践することが重要となる。[II]

ウェブサービス提供者は、安全なウェブサービスを提供するのはもちろんのこと、同一ホストからの連続ログイン試行の拒否等のシステム的な対策を講じることで、被害を緩和できる。万が一、認証情報が漏洩したとしても悪用されないために、登録された利用者パスワードはハッシュ等で暗号化して保存することも求められる。[V]

参考資料

I. 「安易なパスワード」ランキングの最新版、首位が交代
http://www.itmedia.co.jp/news/articles/1401/21/news045.html
II. IPA：パスワードリスト攻撃による不正ログイン防止に向けた呼びかけ
https://www.ipa.go.jp/about/press/20140917.html
III. LINE：他社サービスと同じパスワードを設定している皆様へパスワード変更のお願い
http://official-blog.line.me/ja/archives/1004331596.html
IV. 危なすぎる数字だけのパスワード、JALとANAがユーザー認証を強化
http://itpro.nikkeibp.co.jp/atcl/column/14/346926/090100042/
V. IPA：安全なウェブサイトの作り方
https://www.ipa.go.jp/security/vuln/websecurity.html

5位　ウェブサービスからの顧客情報の窃取

～脆弱性や設定の不備を突かれ顧客情報が盗まれる～

ウェブサービスから氏名や住所等の顧客情報を窃取される事件が頻発した。窃取された情報に ID やパスワード、クレジットカード情報が含まれる場合、不正ログインや金銭被害が発生する等、影響は広範囲に及ぶ可能性もある。

＜主な攻撃者＞

・犯罪グループ

＜主な被害者＞

・ウェブサービス運営者

・ウェブサービス利用者

＜脅威と影響＞

近年、ウェブサービスは無くてはならない存在になっている。ショッピングサイトやインターネットバンキング等、生活を便利にするサービスが広く普及してきた。しかし、ウェブサービスは様々なソフトウェアから構成されており、セキュリティ上の問題が内在しやすい。また、インターネットに公開しているため、攻撃者の標的になりやすい。

脆弱性や設定の不備等セキュリティ上の問題がウェブサービスに内在する場合、顧客情報が窃取され、その情報を元に顧客に被害が及ぶ可能性がある。例えば、顧客のクレジットカード情報を窃取された場合、不正に使われ、顧客が金銭被害を受ける可能性がある。また、住所氏名、電話番号、メールアドレスを悪用され、執拗なセールスや詐欺、スパムメールやフィッシングサイトへの誘導を受けると、さらなる被害に発展する可能性がある。

＜攻撃手口＞

◆　ウェブアプリケーションの脆弱性を悪用

ウェブサービスを構築する際にセキュリティを充分に考慮していない場合、脆弱性を作り込む可能性がある。特に、SQL インジェクションやディレクトリ・トラバーサルの脆弱性は、個人情報窃取等に悪用される危険性がある。

◆　**ソフトウェア製品の脆弱性を悪用**

広く一般に普及しているソフトウェア製品の脆弱性は、攻撃に多用されている。そのため、脆弱性を放置しているウェブサイトは攻撃者の標的になりやすい。ウェブサービスで使用する OS やミドルウェア、コンテンツ管理システム（CMS）およびそのプラグイン等の脆弱性が悪用されて顧客情報を外部に送信されてしまう。システムを改変されることで情報を窃取される場合もある。

◆　**リモートによる運用管理の悪用**

FTP、SSH 等の管理用サービスを使用して遠隔から運用管理している場合、ID とパスワードの推測や、ウイルスを使って窃取された ID とパスワードを用いて管理用サービスに侵入されることがある。

＜事例と傾向＞

◆　**SQL インジェクションを狙った攻撃**

2014 年上半期にウェブアプリケーションファイアウォール（WAF）で最も検知された攻撃は、「SQL インジェクション」の脆弱性を狙った攻撃であったとシマンテックが発表している。[I]

ショッピングサイト「クルチアーニ C」および「クルチアーニ」でクレジットカード情報 22,544 件が漏えいする事件が発生した。原因は、攻撃者に SQL インジェクションの脆弱性を悪用され、WordPress のアカウント情報が窃取されたためと公表している。[II]

◆　**OpenSSL の脆弱性を狙った攻撃**

OpenSSL の Heartbleed の脆弱性を狙った攻撃により三菱 UFJ ニコスの 894 人分の顧客情報が流出した。この脆弱性の対策情報の公表日（4 月 7 日）から不正アクセスを検知した日（4 月 11 日）まで約 4 日という短期間で攻撃が行われた。[III]

＜主な対策・対応＞

ウェブサービス運営者

- 安全なウェブサービスの構築
- ソフトウェアの更新

ウェブサービスの構築時においてセキュリティの要件定義を行い、セキュリティを担保した設計と開発を進める。必要であれば要件定義書はサンプルを参考にできる。[IV] [V]

また、利用中のソフトウェア製品の修正プログラム（パッチ）情報を定期的に確認し、適宜パッチを適用することが重要である。[VI]

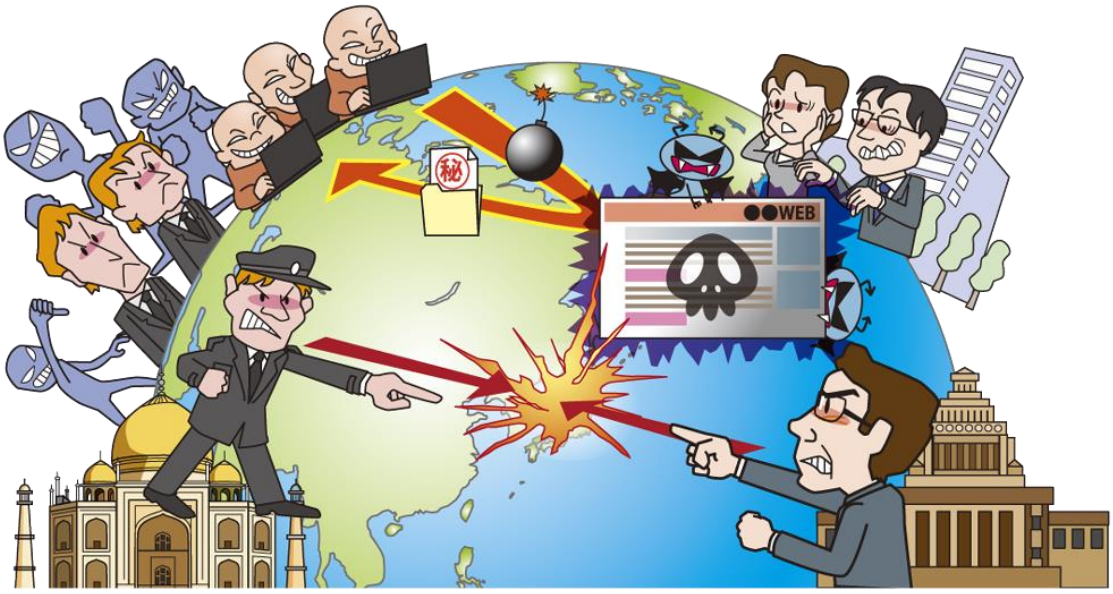
運用上、パッチ適用までに時間を要する場合、WAF や侵入防止システム（IPS）は、脆弱性に対応したシグネチャで攻撃を緩和できるため、導入による効果が期待できる。

参考資料

I. シマンテックがWeb攻撃の傾向を解説、最多の攻撃はSQLインジェクション
http://www.atmarkit.co.jp/ait/articles/1409/29/news104.html
II. ファッション通販2サイトでクレジットカード情報流出
http://japan.cnet.com/news/service/35056527/
III. 国内でもOpenSSL「心臓出血」が悪用、三菱UFJニコスから894人の情報流出か
http://itpro.nikkeibp.co.jp/article/NEWS/20140421/551884/
IV. OWASP Japan：Web システム／Web アプリケーションセキュリティ要件書
https://www.owasp.org/images/8/88/Web_application_security_requirements.pdf
V. 地方自治情報センター：地方公共団体における情報システムセキュリティ要求仕様モデルプラン（Webアプリケーション）
https://www.j-lis.go.jp/lasdec-archive/cms/12,28369,84.html
VI. IPA：サーバソフトウェアが最新版に更新されにくい現状および対策
https://www.ipa.go.jp/about/technicalwatch/20140425.html

6位　ハッカー集団によるサイバーテロ

～破壊活動や内部情報の暴露を目的としたサイバー攻撃～



2014 年、アメリカの映像メディア企業が攻撃を受けて情報漏えいやサービス停止等の被害に遭い、韓国の原発管理会社では内部文書が漏えいし公開される事件が発生した。犯行グループが声明文や窃取した情報を公表したことで社会的に大きなインパクトを与えた。

＜主な攻撃者＞

・ハッカー集団

＜主な被害者＞

・企業・組織

＜脅威と影響＞

高い技術を持つ攻撃者が、特定の民間企業や政府機関にダメージを与えることを目的として、システムに侵入し、重要な情報（機密情報、顧客情報等）の窃取やシステム破壊等を行う反社会的な事件が頻発している。

このような行為は、隠密裏に情報を窃取することを目的とした「標的型攻撃による諜報活動」とは異なり、攻撃者が犯行声明や窃取したデータ等を公表する場合が多く、攻撃を受けた事実が公表されることにより、思想や主義の主張、政治的な動機、報復、信用の失墜やビジネス機会を損失させることが目的に挙げられる。

過去に大きな話題となった事例の１つに、2013 年に韓国の金融機関ネットワークや報道機関のシステムがサイバー攻撃により破壊され業務停止に陥った事件がある。

＜攻撃手口＞

事件後に具体的な手口が明かされることが少ないため、各事件の手口の詳細は不明であるが、一般的な攻撃の手口として以下の３つが考えられる。

◆　ウイルスを悪用

メールの添付ファイルやウェブ　サイト等を介して、組織内部のパソコンをウイルスに感染させる。そのパソコンを外部から遠隔操

作することで内部への侵入を果たす。

◆ **ソフトウェアの脆弱性を悪用**

ウェブサーバー等のインターネットからアクセス可能なシステムで利用されているソフトウェアの脆弱性を悪用し、システムに侵入する。

◆ **パソコンやサーバーを踏み台に悪用**

ウイルスに感染させたパソコン等を踏み台にして大量の通信を発生させる DDoS 攻撃により、標的のウェブサーバーやネットワークに負荷をかけてサービス不能にする。

＜事例と傾向＞

◆ **米国企業へのサイバー攻撃**

2014 年 11 月、北朝鮮を舞台にした映画の公開直前に、アメリカの映像メディア企業 SONY Pictures Entertainment（SPE）への攻撃があった。報道によると、SPE から機密情報や顧客情報、映像コンテンツ等が流出し、システム停止の被害に遭ったとされている。米国政府は、この事件を北朝鮮によるサイバー攻撃であるとして、北朝鮮を「テロ支援国家」への再指定を検討していると公表した。[I] しかし、北朝鮮の攻撃への関与を示す根拠が SPE や米国政府から公表されておらず、内部犯行説等、様々な憶測を呼んでいる。

◆ **韓国の原発管理会社の内部文書流出**

2014 年 12 月、韓国の原子力発電所管理会社「韓国水力原子力」が攻撃を受け、内部文書が流出し、原子炉の設計図等を含む文書がインターネットで公開された。[II]

◆ **オンラインゲームサービスへのサービス妨害**

2014 年 8 月と 12 月、Xbox Live や PlayStation Network 等のオンラインゲームサービスに対し、ハッカー集団が DDoS 攻撃を行い、サービスへの断続的な接続障害が発生した。これに対し、ハッカー集団「Lizard Squad」が、犯行を認める声明を発表した。[III]

＜主な対策・対応＞

経営者

- リスクマネジメント体制の構築

セキュリティ担当部署

- セキュリティ教育の実施

システム管理者

- 安全なシステム設計 [IV]
- アクセス権限管理・アクセス制御
- データ保護・暗号化
- バックアップ

従業員・職員

- セキュリティ教育の受講

復旧のためのデータバックアップやシステムの冗長化と共に、インシデント（セキュリティ事故・事件）発生を想定した対応手順書の作成や訓練を行うことも重要である。

参考資料

I. 米国が北朝鮮「テロ支援国家」再指定検討、ソニーサイバー攻撃で
http://jp.reuters.com/article/topNews/idJPKBN0JZ0RC20141221
II. 韓国の原発情報が流出、北朝鮮関与の可能性も
http://www.itmedia.co.jp/enterprise/articles/1412/25/news061.html
III. ソニーのPSNなどで障害--DDoS攻撃の犯行声明
http://japan.cnet.com/news/service/35052792/
IV. IPA：「高度標的型攻撃」対策に向けたシステム設計ガイド
https://www.ipa.go.jp/security/vuln/newattack.html

7位　ウェブサイトの改ざん

～知らぬ間に、ウイルス感染サイトに仕立てられる～

閲覧するだけでウイルスに感染するように企業・組織のウェブサイトが改ざんされる事例が多く発生した。ウェブサイトを改ざんされることにより、復旧までのサービス停止による自社・自組織の被害だけでなく、ウェブサイト閲覧者にも被害が及ぶこともある。

＜主な攻撃者＞

・犯罪グループ

＜主な被害者＞

・ウェブサイト運営者

・ウェブサイト閲覧者

＜脅威と影響＞

かつては、主義主張を掲げる内容に書き換えられるウェブサイト改ざんが多く、見た目で改ざんされたことが判断できた。

しかし、近年多発しているウェブ改ざんでは、閲覧者のパソコンをウイルスに感染させるための細工が見た目では分からないようにサイトに埋め込まれる。ウェブサイトを改ざんされた運営者は、被害者となる一方で、結果としてウイルス感染に加担したことになり、社会的な信用失墜も招くことになる。

また、適切に管理されていないウェブサイトが改ざんされた場合、誰もそれに気付くことなく放置されていることも少なくない。

＜攻撃手口＞

◆　ソフトウェア製品の脆弱性を悪用

広く一般に普及しているソフトウェア製品の脆弱性を悪用してウェブサイトの改ざんを行う。システム構築時にインストールしたままで放置している等、古いバージョンのまま運用されているウェブサイトが狙われる。インターネット上の多数のウェブサイトを効率よく改ざんするために攻撃を自動化するツールも存在する。OS・ミドルウェア等のソフトウェアが狙われていたが、近年は WordPress、Joomla!等に代表されるコンテンツ管理システム（CMS）やそのプラグインの脆弱性が悪用される傾向にある。

◆　**ウェブアプリケーションの脆弱性を悪用**

ウェブサービスに利用するウェブアプリケーションの独自開発や、業務形態に合わせたパッケージソフトウェアのカスタマイズの際に、SQL インジェクションやディレクトリ・トラバーサル等の脆弱性を作り込んでしまう場合があり、攻撃者はその脆弱性を悪用して改ざんを行う。

◆　**リモート管理用サービスへの侵入**

遠隔から運用するために FTP、SSH 等の管理用サービスを使用しているウェブサイトが多く存在する。攻撃者は、ウイルス等を使って窃取したウェブサイト管理用アカウントの認証情報を悪用して、管理用サービスからウェブサイトに侵入する。また、CMS の管理画面から侵入する事例もある。

＜事例と傾向＞

◆　**2014 年も CMS が標的に**

日本で開発された無償の CMS である Web Diary Professional（WDP）の脆弱性を悪用して改ざんされたサイトを 2014 年 1 月から 3 月までの 3 か月間で 2,800 件以上確認したとカスペルスキーが報告した。改ざんされたサイトにはバックドアやスパムメール送信ツール等が設置されており、攻撃の踏み台に悪用されていた可能性が高い。[I]

◆　**外部サービスのセキュリティ侵害**

CDN（Content Delivery Network、コンテンツデリバリーネットワーク）と呼ばれる、企業の代理でコンテンツを配布するサービスが侵害され、複数のコンテンツが改ざんされた。改ざんされたコンテンツは、コンテンツを閲覧したパソコンがウイルスに感染する仕掛けが施されており、それらの中には、パソコンの周辺機器企業が提供していた修正プログラム（パッチ）も含まれていた。[II]

＜主な対策・対応＞

ウェブサイト運営者

- サーバーソフトウェアの更新
- サーバーソフトウェアの設定の見直し
- ウェブアプリケーションの脆弱性対策
- アカウント・パスワードの管理

ウェブサイト運営者は、ウェブサイトで利用しているソフトウェアの製品名やバージョンを把握し、利用製品の脆弱性対策情報はタイムリーに収集する。収集した脆弱性対策情報から影響有無を判断し、迅速に対策することが求められる。もし、ウェブサイトの管理者が不在等で対策ができない場合は、ウェブサイトの閉鎖を検討する。[III] また、ウェブサイト開発においては、ウェブアプリケーションの脆弱性を作り込まないように開発・構築、検査することが求められる。[IV]

ウェブサイト閲覧者は、定期的なソフトウェアの更新やウイルス対策ソフトの導入によって、ウイルス感染を予防することができる。

参考資料

I. 日本独自のブログ作成ツールが攻撃者の標的に！
http://blog.kaspersky.co.jp/obsolete-japanese-cms-targeted-by-criminals/
II. HISやバッファローのウイルス感染は、CDNetworksの改ざん被害が関与
http://itpro.nikkeibp.co.jp/article/NEWS/20140603/561262/?ST=security
III. IPA：管理できていないウェブサイトは閉鎖の検討を
https://www.ipa.go.jp/security/ciadr/vul/20140619-oldcms.html
IV. IPA：安全なウェブサイトの作り方
https://www.ipa.go.jp/security/vuln/websecurity.html

8位　インターネット基盤技術を悪用した攻撃

～インターネット事業者は厳重な警戒を～

インターネット上の様々なサービスは、DNS や電子証明書等の基盤技術に対する信頼の上に成り立っている。2014 年は、これらの技術を悪用してウイルス感染サイトへ誘導する等の攻撃が発生した。この攻撃は、利用者側では検知して対応することが難しいため、インターネット提供側である事業者の対策が強く求められる。

＜主な攻撃者＞

・犯罪グループ

＜主な被害者＞

・インターネット事業者（登録事業者、ISP 等）
・インターネット利用者

＜脅威と影響＞

インターネット上の様々なサービスは、インターネット黎明期より存在する多くのインターネットの基盤技術に対する信頼の上に成り立っている。しかし、近年では、DNS 等のインターネットの基盤技術を悪用したなりすましや DDoS 攻撃、不正に入手した電子証明書を悪用したなりすまし等、インターネット基盤技術への信頼を揺るがす新しい手口も編み出されている。

＜攻撃手口＞

◆　なりすまし

登録事業者をだましたり、登録事業者のシステムの脆弱性を悪用したりすることで、DNS 登録情報や BGP（インターネット上で経路情報をやり取りするためのプロトコル）の通信経路の変更が行われたり、電子証明書を不正に発行されることがある。これらの攻撃により、ウイルス感染サイトへの誘導や、通信経路での盗聴により重要な個人情報が窃取される危険性がある。

◆　DDoS 攻撃（リフレクター攻撃）

ウイルスに感染させたパソコン（ボット）や、ブロードバンドルーター等のオープンリゾルバ設定を悪用し、大量の通信を発生させてネットワークを麻痺させる攻撃も頻発している。これらの攻撃は、踏み台となった利用者

から攻撃の通信が発生するため、インターネットサービス提供者側からは攻撃の通信と通常の通信を区別することが難しい。

＜事例と傾向＞

◆ **ドメイン名ハイジャックによる登録情報の書き換え**

2014 年、国内の企業・組織が使用している複数の「.com」ドメインに対し登録情報の不正書き換えによるドメイン名ハイジャックが行われた。この攻撃により悪意のあるサイトに誘導されたパソコンがウイルスに感染した。この事例を受け、2014 年 11 月に日本レジストリサービス（JPRS）等が注意喚起を行った。[I]

◆ **不正な SSL 証明書の悪用によるサイバー攻撃のおそれ**

2014 年 7 月 11 日、インド国立情報工学センターより SSL 証明書が不正に発行され、この不適切な証明書により、なりすまし、フィッシング、中間者攻撃（暗号通信間に介入し、通信内容の盗聴や、情報を改ざんする攻撃）へ悪用されるおそれがあるとして、Microsoft は Windows 上で不正な証明書を無効化するための修正プログラムを提供した。[II]

◆ **DNS 水責め攻撃**

2014 年初頭に、攻撃対象の DNS サーバーに対して存在しないランダムなサブドメインの問い合わせを大量に行い、過負荷にさせる DDoS 攻撃が世界的に観測された。この攻撃により、2014 年 6 月から 7 月にかけて、国内の複数のインターネットサービスプロバイダ（ISP）の DNS サーバーが過負荷となり、応答遅延や無応答状態に陥った。[III]

＜主な対策・対応＞

インターネット基盤技術を悪用した攻撃に、利用者が気づくのは困難である。そのため、インターネットサービス事業者の対策が強く求められる。

事業者側において、以下の対策を継続的に行う必要がある。

インターネット事業者、ドメインや電子証明書等を使用する企業・組織等

● 運用やサービスの監視強化

・登録変更申請内容の真偽の確認強化

・定期的な登録情報の確認

・利用機器やソフトウェアの適切な設定

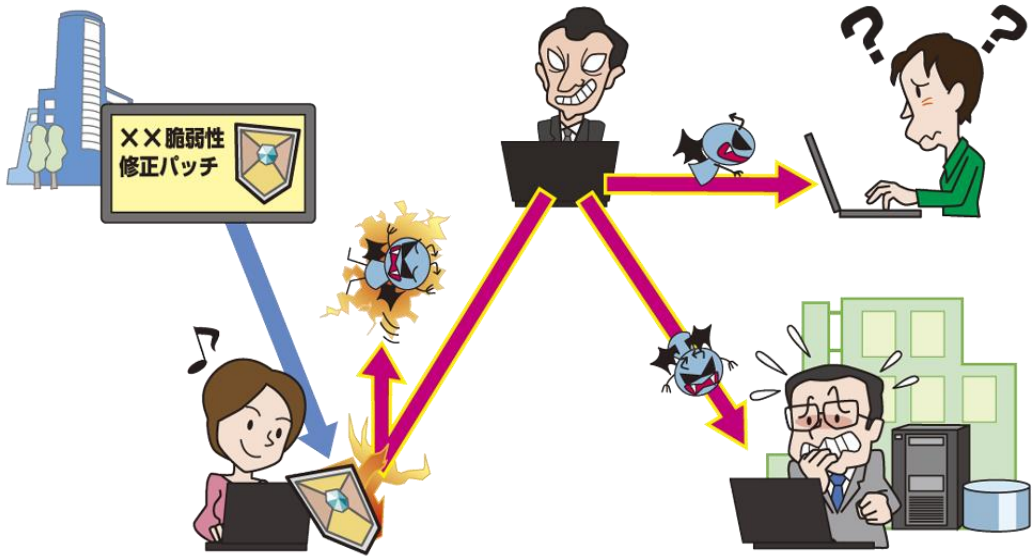
特に、申請内容の真偽の確認強化やサービスの監視強化が重要である。登録情報変更や発行等の手続きを行う際のメール通知や、DNS のレジストリロック（特別なロック解除手続き後のみ登録情報を変更できる機能）等の容易に変更できなくする仕組みを利用することも有効な対策となる。[I] また、ボットやオープンリゾルバを悪用した DDoS 攻撃の踏み台にされないために、インターネット利用者もウイルス対策やルーターの設定等を実施することが望ましい。

参考資料

I. 日本レジストリサービス（JPRS）：（緊急）登録情報の不正書き換えによるドメイン名ハイジャックとその対策について
http://jprs.jp/tech/security/2014-11-05-unauthorized-update-of-registration-information.html
II. マイクロソフト セキュリティ アドバイザリ 2982792 不適切に発行されたデジタル証明書により、なりすましが行われる
https://technet.microsoft.com/ja-jp/library/security/2982792.aspx
III. “未熟なDNS”をDDoSで拷問、「DNS水責め攻撃」が原因らしき実害が日本でも
http://internet.watch.impress.co.jp/docs/event/20141125_677364.html

9位　脆弱性公表に伴う攻撃

～求められる迅速な脆弱性対策～



2014 年は Apache Struts、OpenSSL、bash 等、広く利用されているソフトウェアの脆弱性対策情報の公表が相次ぎ、それらの脆弱性に対する攻撃が発生した。システム管理者や一般ユーザーは、製品の利用状況や攻撃発生の有無等、脆弱性の影響度に応じて迅速に対策する必要がある。

＜主な攻撃者＞

・犯罪グループ

＜主な被害者＞

・ソフトウェア利用者（システム管理者、一般ユーザー、ソフトウェア開発者）

＜脅威と影響＞

ソフトウェアの脆弱性対策情報は、利用者にとって、ある日突然公表される場合が多い。利用者は、公表された情報から影響度を確認し、ソフトウェアの更新等適切な対応を実施する必要がある。

しかし、組織の基幹システムのような重要なシステムになればなるほど、影響範囲が大きく、充分な検証や関係者との調整が必要となり、対策に時間が掛かる。その間に未対策のまま攻撃者に狙われた場合、脆弱性を悪用され、攻撃者の意図するプログラムの実行や権限の奪取、情報窃取等が行われる可能性がある。

＜要因＞

(1)　脆弱性対策情報の公表

一般的に、ソフトウェア開発者は脆弱性対策情報の公表と同時に、修正プログラム（パッチ）を提供する。多くの攻撃者もこのタイミングでソフトウェアの脆弱性を知ることになる。攻撃者はパッチから脆弱性を解析し、脆弱性を悪用したサーバーへの通信（攻撃パケットの送信）や、ウイルス感染させるファイルの作成と配布を実施する。

(2)　脆弱性の放置

脆弱性対策情報が公表されたにも関わらず、公表に気が付かない場合や、対策の実

施が遅れた場合等、対策を実施しないことが、被害を受ける最大の要因となっている。また、オープンソースソフトウェア等を組み込んでいる製品の開発者が、組み込んでいるソフトウェアの脆弱性対策情報に気づかずに脆弱性を放置してしまう場合もある。

＜事例と傾向＞

◆ サーバーソフトウェアの脆弱性

2014 年は、OpenSSL の Heartbleed、bash の ShellShock 等、脆弱性に名前を付けて大々的に公表され注目を集めた。また、Apache Struts 2 の脆弱性（CVE-2014-0094）の修正が不十分であることが発覚し、システム管理者は対応に追われた。[I] [II] [III]

◆ クライアントソフトウェアの脆弱性

Microsoft は 2014 年 4 月、Internet Explorer（IE）にゼロデイの脆弱性（修正プログラムが提供されていないがすでに悪用されている脆弱性）の存在を公表した。一部の報道機関が「米国土安全保障省が IE を使わないよう警告」と大きく報じたため、修正プログラムが提供されるまでの数日間、ユーザーの不安を招いた。[IV]

◆ ソフトウェアのサポート終了の問題

様々な理由でシステムの移行が進まず、サポートの終了した古いソフトウェアを使い続けている利用者は少なくない。サポートが終了した製品には、製品開発者からパッチ等の対策が提供されないため、影響度の高い脆弱性が見つかった場合の対応が容易ではなく、対応が遅れてしまい被害が発生するおそれがある。Apache Struts1 の脆弱性（CVE-2014-0114）が 2014 年 4 月に発覚した際には、利用者自身がソースコードからパッチを作成する等、高度な対応を求められた。

＜主な対策・対応＞

経営者層

- 迅速な対応に向けた体制の整備 [V]

ソフトウェア利用者

- 管理しているシステムの把握
- 定期的な脆弱性対策情報の収集
- ソフトウェアの更新

システム管理者等のソフトウェア利用者は、公表される脆弱性や攻撃に備えて、継続的に情報を収集して対処することが求められている。また、新しい情報だけでなく、修正が不十分である可能性も想定し、追加の情報が無いか継続的に確認する必要がある。

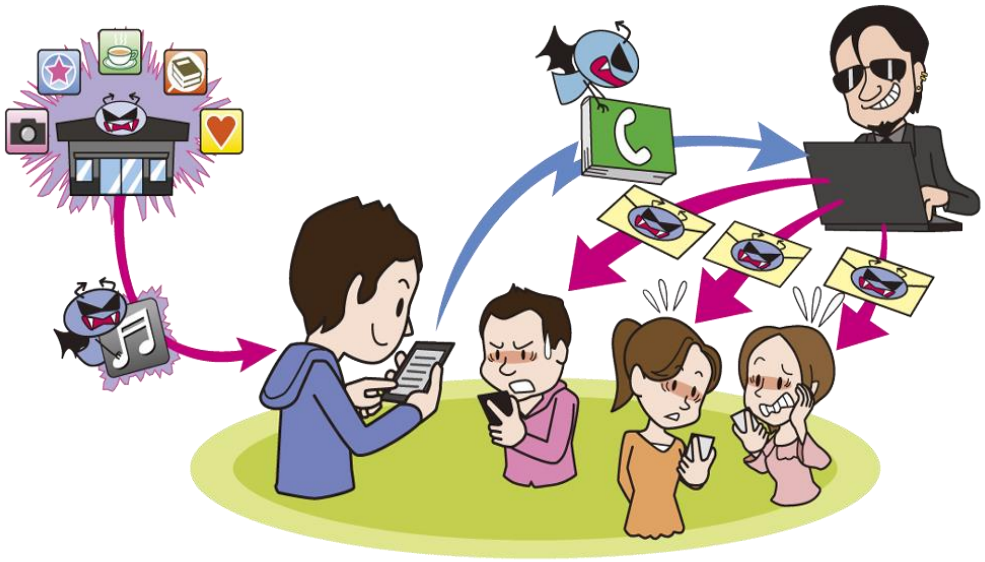
問題が発生した際の対応体制（CSIRT）を組織内に構築しておくと、迅速な対応が可能になる。また、サーバーソフトウェアの更新が間に合わない場合や適用できない状況でも、WAF や IPS を導入し、攻撃に対応したシグネチャを用いることで、攻撃を緩和できる。

参考資料

I. IPA：OpenSSL の脆弱性対策について
https://www.ipa.go.jp/security/ciadr/vul/20140408-openssl.html
II. IPA：bash の脆弱性対策について
https://www.ipa.go.jp/security/ciadr/vul/20140926-bash.html
III. IPA：Apache Struts2 の脆弱性対策について
https://www.ipa.go.jp/security/ciadr/vul/20140417-struts.html
IV. Internet Explorer に解放済みメモリ使用（use-after-free）の脆弱性
http://jvndb.jvn.jp/ja/contents/2014/JVNDB-2014-002260.html
V. JPCERT/CC：企業における情報セキュリティ緊急対応体制 ～組織内 CSIRT の必要性～
https://www.ipa.go.jp/files/000039115.pdf

10位　悪意のあるスマートフォンアプリ

～アプリのインストールで友人に被害が及ぶことも～



便利な機能があるように見せかけた悪意あるスマートフォンアプリにより、端末内の電話帳等の個人情報を知らない間に窃取されてしまう。窃取された情報がスパムメールや詐欺に悪用され、友人や知人にまで被害が及ぶ場合もある。

＜主な攻撃者＞

・犯罪グループ

＜主な被害者＞

・スマートフォン利用者

・スマートフォン利用者の友人・知人

＜脅威と影響＞

スマートフォン向けの多種多様な魅力あるアプリが公開されている。利用者は自由に好みのアプリをインストールできる。

一方で、利用者に害をもたらす悪意のあるアプリも数多く公開されている。悪意のあるアプリは、そのアプリの用途には必要の無いと思われる GPS 等スマートフォンの機能や電話帳等のデータへのアクセス権限を要求する。

悪意のあるアプリがもたらす主な被害を以下に示す。

- 端末情報・電話帳・写真・メール内容等の個人情報の窃取
- スマートフォンの機能（カメラやマイク、GPS）を悪用した盗撮・盗聴・追跡等
- 窃取した情報を悪用した、スパムメール等による二次的被害

＜攻撃手口＞

スマートフォン利用者に悪意のあるアプリをインストールさせるために、攻撃者が利用者を欺く典型的な手口は以下の４つである。

- **偽物のアプリを公開して誘導**

公式・サードパーティやその他のマーケットに、人気のある有料アプリ等の偽アプリを無料で公開し、本物と同じ紹介画像を掲載して本物と思わせてインストールさせる。また、

電池が長持ちする等、便利な機能と偽って利用者を欺くアプリも存在する。

- **利用者の心理に付け込む**

ウェブサイトやメールを使って、ウイルスの駆除やアダルト動画が再生できる等の案内を表示し、悪意のあるアプリをインストールさせようとする。

- **後から悪意のあるアプリへ豹変**

インストールの時点では悪意のある機能は持っていないが、アップデート後に悪意のある機能が追加されるアプリも存在する。

- **別のアプリを勝手にインストール**

勝手に別のアプリをインストールするAndroidアプリも存在する。インストール時に通常表示される確認画面を出さずに、悪意のあるアプリをインストールさせてしまう。[II]

＜事例と傾向＞

◆ **人気の Android アプリの偽物アプリ**

Android の公式ストアである Google Play に掲載されている無料の人気アプリ 50 本のうち 40 本の偽アプリが、非公式のダウンロードサイト上で確認されたとトレンドマイクロが報告している。これらの偽物のアプリは本物のアプリを不正に改ざんしたもので、同社が確認した偽物のアプリの内半数以上が、利用者に危険を及ぼす悪意のあるアプリであるとしている。[III]

◆ **性的脅迫を目的としたアプリ**

SNS で知り合った人物からビデオチャットアプリをインストールするように持ちかけられ、そのアプリで交換した動画を使って脅迫される事例が確認された。ビデオチャットアプリは電話帳情報を窃取する機能を有していたとみられている。[IV]

＜主な対策・対応＞

スマートフォン利用者

- 信頼できるアプリかどうかを確認

アプリに対する利用者レビューの確認や、アプリ名や開発者名でインターネット検索した結果を確認することで、信頼できるアプリか判断する。

- アクセス権限の確認

Android アプリのインストール前には、アプリで使用する端末の機能や使用するデータへのアクセス権限の確認画面が表示される。また、アップデート時にもアクセス権限の追加があれば確認画面が表示される場合がある。確認画面の内容を見て、アプリが要求する権限は本当に必要かよく考え、不安であれば承認せずインストールしない。

- OS やアプリは最新版を利用

OS やアプリの脆弱性を、ウイルス等に悪用され、被害が発生する可能性があるため、OS やアプリは最新版に更新する。

- ウイルス対策ソフトの導入

ウイルス対策ソフトによる、ブロックや警告が、利用者が脅威に気づく手助けになる。

参考資料

I. IPA：2014年5月の呼びかけ「あなたのスマートフォン、のぞかれていませんか？」
https://www.ipa.go.jp/security/txt/2014/05outline.html
II. Google Playからアプリ自動インストールを行う危険な国内向けAndroidアプリ
http://blogs.mcafee.jp/mcafeeblog/2014/03/1395.html
III.「リパックアプリ」：正規アプリになりすまし、利用者に被害を与える攻撃手法
http://blog.trendmicro.co.jp/archives/9571
IV. IPA：2014年12月の呼びかけ「個人間でやりとりする写真や動画もネットに公開しているという認識を！」
https://www.ipa.go.jp/security/txt/2014/12outline.html

その他の 10 大脅威候補

10 位までに選出されなかったものの、2014 年に社会へインパクトを与えた脅威や以前から継続して問題となっている脅威として、10 大脅威の候補を簡単に説明する。

11位.　ウイルスを使った詐欺・恐喝

ランサムウェアというパソコンをロックして身代金を要求するウイルスを用いた手口や、ウイルススキャンが始まったような画面を表示して有償版のソフトウェアの購入を促す手口が増加している。被害は個人にとどまらず、企業・組織にまで及んでいる。

- 日本を狙った複数の“ランサムウェア”が活動中、ファイルを人質に身代金要求
  http://internet.watch.impress.co.jp/docs/news/20141216_680615.html
- 2015年2月の呼びかけ「 その警告表示はソフトウェア購入へ誘導されるかも知れません 」
  https://www.ipa.go.jp/security/txt/2015/02outline.html

12位.　サービス妨害

攻撃によりサービスの提供が妨害される事例が後を絶たない。ウイルスに感染したパソコンで構成されるボットネットを利用し DDoS 攻撃を行う手法は古くからあり、DDoS を実施するために有料でボットネットの貸し出す DDoS 攻撃代行サービスも登場している。2014 年には、日本の高校生がその DDoS サービスを利用して有名ゲーム機のサービス基盤を攻撃する事件が発生した。

- 高校生でも企業サイトを落とせる時代に、「DDoS攻撃サービス」の脅威
  http://itpro.nikkeibp.co.jp/atcl/column/14/346926/092200062/
- 100Gbps超のDDoS攻撃頻発、大規模化の様相に
  http://www.itmedia.co.jp/enterprise/articles/1410/24/news053.html

13位.　無線 LAN の無断使用・盗聴

適切なセキュリティ設定がされていない無線 LAN アクセスポイントを第三者によって無断使用され、犯罪行為の踏み台等に悪用される事例が問題となっている。また、公衆無線 LAN サービスによっては、その通信内容が容易に盗聴できることが確認されており、個人情報が漏えいする可能性がある。

- 無線LAN＜危険回避＞対策のしおり
  https://www.ipa.go.jp/security/keihatsu/announce20140320_1.html
- 無線LANのメール丸見え　成田・関西・神戸の3空港
  http://www.nikkei.com/article/DGXLASDG2600E_W4A820C1CR0000/

14位.　ネット上の誹謗・中傷・いじめ

掲示板への誹謗中傷の書き込みや SNS 上で行われるいじめ行為も社会的な問題となっている。元恋人の性的な画像や動画等をインターネット上に投稿すると脅迫する行為「リベンジポルノ」も問題視されており、2014 年には「私事性的画像記録の提供被害防止法（リベンジポルノ防止法）」が成立した。

- 特徴は「さらし型」 高校生によるネットいじめの実態
  http://benesse.jp/news/kyouiku/trend/20141112120011.html
- リベンジポルノ防止法が成立
  http://www.itmedia.co.jp/news/articles/1411/19/news104.html

15位.　悪意のあるアプリを使った遠隔操作

遠隔操作されて脅迫文を掲示板に投稿させられたパソコンの所有者が誤認逮捕された事件や、パソコンにインストールしたソフトウェアを用いて盗撮を行う等、犯罪行為や私的な意図で遠隔操作が可能なソフトウェアが悪用されている。

- 片山被告を勾留へ　PC遠隔操作事件　関与すべて認める
  http://www.asahi.com/articles/ASG5N3D1PG5NUTIL003.html
- 2014年11月の呼びかけ「 遠隔操作ソフトは利用目的を理解してインストールを！ 」
  https://www.ipa.go.jp/security/txt/2014/11outline.html

16位.　利用者情報の不適切な取り扱いによる信用失墜

利用者情報の不適切な取扱いによって、サービスを提供している企業・組織の信用が失墜する。メールの誤送信により利用者情報（メールアドレス等）が漏えいする事例は後を絶たない。また、利用者の同意を得ていることが不明瞭であることや、同意を得ずに利用者の情報を得るソフトウェアの存在も批判の的になっている。

- メール誤送信に関するお詫びとお知らせ
  http://www.olc.co.jp/news/olcgroup/20141223.pdf
- JR東、Suicaデータ社外提供は「利用者への配慮が不足していた」有識者会議の中間報告を公表
  http://www.itmedia.co.jp/news/articles/1403/20/news096.html

17位.　不適切な情報公開

Twitter 等の SNS やブログへの不適切な写真の投稿が相次ぎ問題となっている。遊び半分で投稿した内容が、本人の知らない間にインターネット上で一気に話題となり、社会的な注目を受ける事例が多数存在する。従業員・職員が軽率に投稿した場合、企業・組織が損失を受けてしまう。

- ハサミの天ぷらをツイッター投稿　鯖江の「はま寿司」アルバイト
  http://www.fukuishimbun.co.jp/localnews/society/54612.html
- 無銭飲食をTwitterで自慢　武蔵野大、学生を処分
  http://www.itmedia.co.jp/news/articles/1406/18/news042.html

18位.　不正請求詐欺

アダルトサイトや出会い系サイトの正当な契約のように見せかけ、サービス利用料を不正に請求されるワンクリック請求の被害は、パソコンだけではなくスマートフォン利用者にも増加している。不正請求の手口は年々巧妙化している。

- スマホのワンクリ詐欺が増加、登録完了画面に慌てない！
  http://ascii.jp/elem/000/000/900/900096/
- スマホ向けアダルト詐欺…高額請求と脅しの手口
  http://www.yomiuri.co.jp/it/security/goshinjyutsu/20140704-OYT8T50234.html

19位.　過失や災害による情報漏えいやサービス停止

顧客情報や機密情報を保存したパソコン等の紛失や盗難の事例が後を絶たない。また、非公開にしておくべき情報が単純な設定ミスにより一般に公開される事例も発生している。企業・組織はこのような不測の事態に備えておかなければならない。

- グーグル、誤って空港の見取り図などを公開状態に--修正し謝罪
  http://japan.cnet.com/news/business/35046482/
- 防衛機種試験データ記録用ハードディスク紛失について
  http://www.mhi.co.jp/notice/notice_20140924.html

このページは空白です。

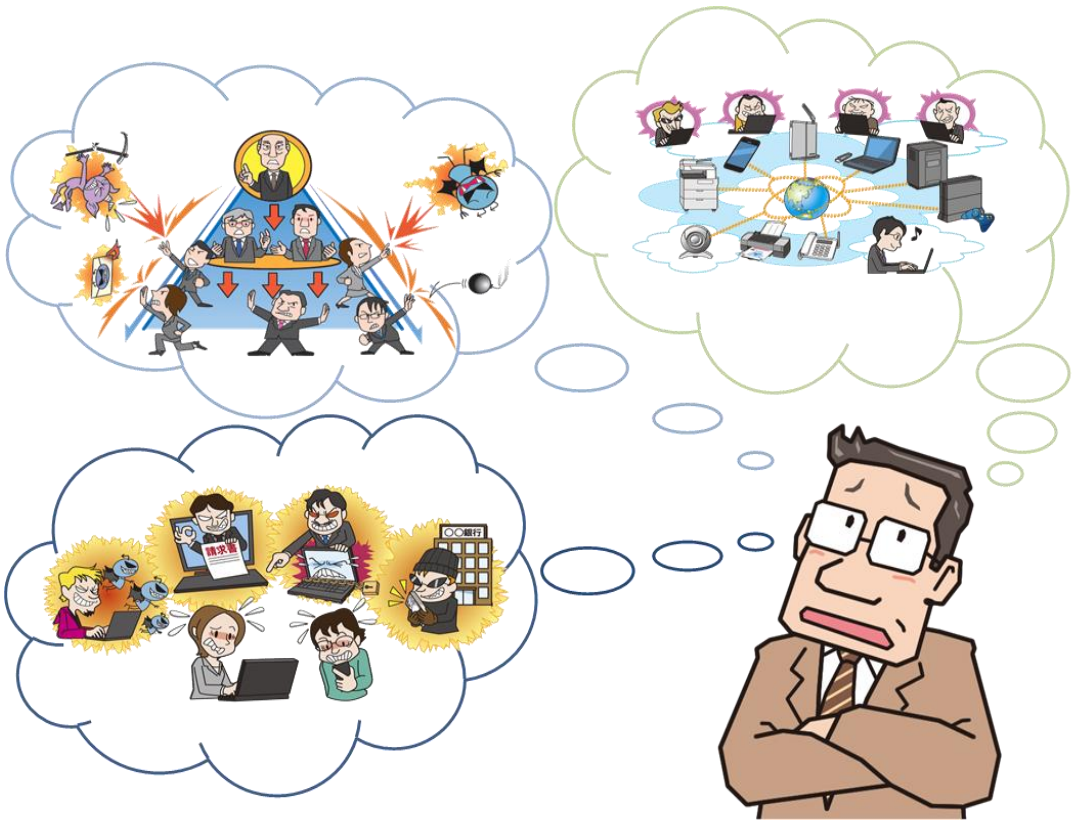
3章. 注目すべき課題や懸念

3 章 注目すべき課題や懸念

本章では、解決すべき課題や、問題視されている脅威や今後大きな脅威となると考えられる懸念について解説する。

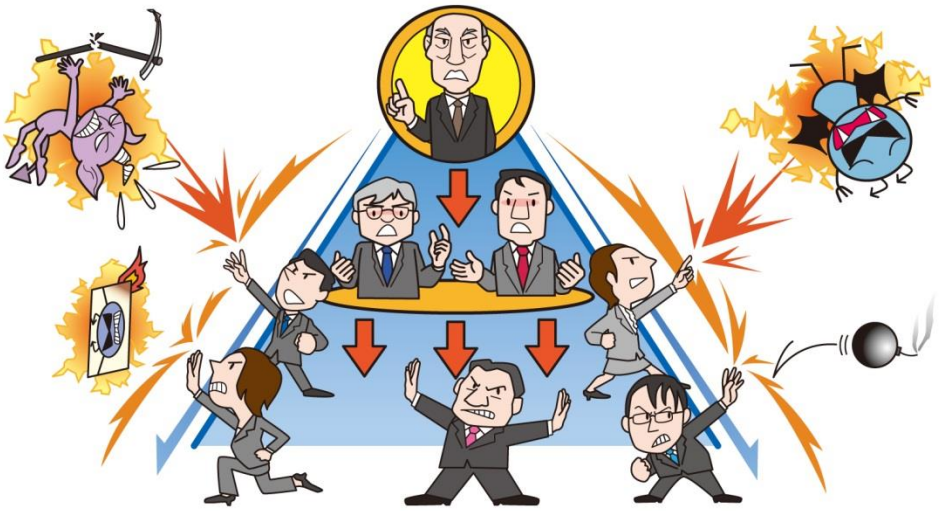
表 3.1：注目すべき課題や懸念

番号	タイトル
1	迅速に対応できる体制の構築 ～脆弱性対策情報の公表や事件発生に対応可能な体制作り～
2	ネットワーク対応機器の増加 ～モノのインターネット（IoT）にもセキュリティ対策を～
3	拡大するネット犯罪の被害 ～巧妙化するウイルスやネット詐欺による金銭被害～



3.1. 迅速に対応できる体制の構築

～脆弱性対策情報の公表や事件発生に対応できる体制作り～



今や企業・組織の活動や社会インフラは、IT に大きく依存しており、情報セキュリティの脅威も多様化している。各企業・組織は、重要な情報資産を保護するために必要な予算を計上しながら対策を進める必要がある。トップダウンでの対策実施、脆弱性や事故への迅速な対応のために、組織としての体制強化が求められる。

＜迅速な対応が求められる時代に＞

コンピュータやインターネットの普及によって、業務の効率や質の向上が図られた反面、情報資産を狙う様々な脅威が生まれた。この数年で諜報活動や犯罪での悪用が進み、脅威は多様化・複雑化していると言える。

企業・組織には、脅威により情報資産や金銭を失わず、かつ業務を停止させない対策を進める必要がある。そのために、突然公表される脆弱性対策情報への対応や、ウイルス感染被害の発生、内部不正の発覚、情報漏えい事故等、セキュリティインシデントへの迅速な対応が求められている。また、昨今、企業・組織から盗み出した情報を用いて別の企業・組織を狙うケースもあり、被害は一企業・組織だけで留まらない時代となっている。

＜迅速な対応が求められた事例＞

◆ 突然公表される脆弱性

2014 年は、Apache Struts や OpenSSL、bash 等の一般のサービスに広く使われているサーバーソフトウェアおよび、Internet Explorer や Adobe Flash Player 等のクライアントソフトウェアに深刻な脆弱性が見つかり、早急な対応が求められた。

企業・組織は、公表される脆弱性対策情報の迅速な収集、影響範囲の把握、対策実施の意思決定を行い、業者とも連携しながら対策を実施することが求められる。しかし、企業・組織によっては、脆弱性対策情報を収集できていない場合や、収集できていたとしても適切な対応が行われない場合があることが、現状の課題と言える。

◆ **内部不正**

2014 年 7 月、通信教育大手のベネッセコーポレーションにおいて、委託先企業の社員により約 3,504 万件の顧客情報が持ち出され、名簿業者に販売されてしまう事件が公表された。この件は顧客からの問い合わせにより発覚し、国内過去最悪の漏えい件数であったことから、大きく報道され、内部不正対策の必要性が再認識されるきっかけとなった。

＜迅速な対応に求められる対策＞

◆ **トップダウンによる対策の推進**

対策を網羅的かつ継続的に実施するためには、経営者層が対策の内容と実施について責任を持つことと、トップダウンで積極的に対策を推進できる体制を構築し、内部統制の PDCA サイクルを回すことがポイントとなる。[I]

◆ **予算を確保し継続的な対策実施**

セキュリティを確保した組織的な体制の構築と継続的な実施のためには、必要な予算を毎年計上し、適切な対策を選択していかなければならない。予算が少ない場合でも、情報資産毎に優先順位を付けて対策を実施することが重要となる。

◆ **企業・組織内に「CSIRT」設置**

脅威に対抗するために、CSIRT（Computer Security Incident Response Team：シーサート）を設置する企業・組織内が増えている。CSIRT とは各企業・組織ごとに設置する緊急対応チームであり、脆弱性対策情報や攻撃予兆情報の収集、対応方針の選定、問題が発生した場合の調査や対処等を行う。CSIRT を設置することで、セキュリティへの取り組みを対外的に示すこともできる。日本の CSIRT を持つ企業・組織の集まりである日本シーサート協議会は、攻撃の動向等について加盟組織間で情報交換を行っている。また、CSIRT スターターキット等、CSIRT の構築や維持の参考となる資料は、CSIRT を構築したい企業・組織が活用できる。[II]

◆ **運用フェーズも継続的な取り組みを**

ソフトウェアの修正プログラム（パッチ）を適用して脆弱性を解消すること、重要な顧客データに対してログ等を監査して内部不正に注意を払うことも、システムの運用フェーズで実施する重要な作業である。システムの導入時の要件の検討や、セキュリティ対策製品の導入等、上流フェーズでの一時的な実施だけではなく、運用フェーズにおいても継続的に取り組んでいく必要がある。また、定期的に現状の情報資産の重要性やリスクに応じて運用を改善する必要がある。

＜国家レベルで対応を強化＞

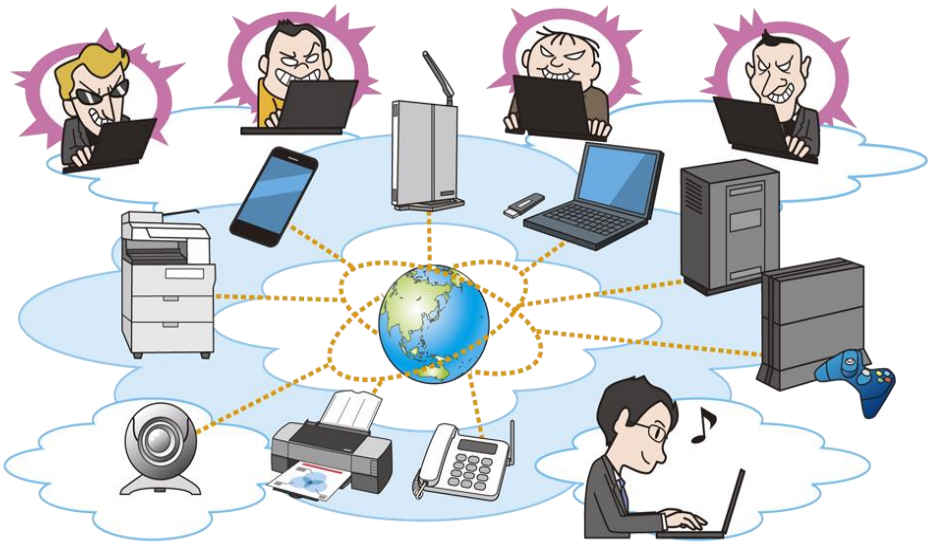
2014 年 11 月 6 日、サイバーセキュリティ基本法が成立した。[III] 法律には国が「被害から迅速に復旧できる強靭な体制を構築するための取組を積極的に推進する」との基本理念が明記されている。政府機関や地方公共団体、重要インフラ事業者はもちろんのこと、これらの組織から受託や受注する民間企業等をはじめ、国内の多くの企業・組織は、今後もさらなる情報セキュリティへの取組みが求められている。

参考資料

I. IPA：組織における内部不正防止ガイドライン
https://www.ipa.go.jp/security/fy24/reports/insider/
II. 日本シーサート協議会
http://www.nca.gr.jp/index.html
III. 内閣サイバーセキュリティセンター：サイバーセキュリティ基本法
http://www.nisc.go.jp/law/pdf/basicact.pdf

3.2. ネットワーク対応機器の増加

～モノのインターネット（IoT）にもセキュリティ対策を～



家庭にはネット家電、職場にはオフィス機器、工場には制御機器等、ネットワーク対応の機器が増えつつある。これらの機器はパソコンやスマートフォンから操作できる等、利便性が高い一方で、ネットワークを介して攻撃された場合、機器の乗っ取りやウイルス感染、情報漏えい等の懸念があり、これらの機器への攻撃が今後大きな脅威となる可能性がある。

＜モノのインターネット（IoT）＞

ネットワーク対応機器は、モノのインターネット（Internet of Things、IoT）と称され、注目を集めている。将来、センサー機器やウェアラブルデバイス等の IoT は爆発的に増加すると予想されている。その数は、調査会社ガートナーは 2009 年の 9 億台から、2020 年に 260 億台に達すると試算している。

＜ネットワーク対応機器の危険性＞

ネットワーク対応機器を LAN またはインターネットに接続することで、クラウドサービスやスマートフォンとの連携等、様々な恩恵を得られる半面、逆に攻撃者に悪用される危険性を伴う。特に、インターネットに機器を接続している場合、世界中の攻撃者から狙われる可能性がある。

また、ネットワーク対応の車載システムや医療機器が侵害された場合、人命が脅かされる可能性が危惧されている。

＜ネットワーク対応機器への攻撃＞

2014 年 2 月、Linksys は自社の無線 LAN ルーター製品への「The Moon」ウイルス感染を確認し、対処方法を公表した。ファームウェアをアップデートした上で、インターネットから遠隔管理する機能の無効化を推奨している。[I]

2014 年 9 月、Linux を搭載した機器に広く利用されているソフトウェア bash の脆弱性（Shellshock）が公表された。10 月にセキュリティ企業ファイア・アイが特定のネットワーク接続型のハードディスク機器（NAS）が Shellshock を悪用されて乗っ取られる攻撃を確認したと公表した。[II] 攻撃は TCP ポート 8080 番に対して行われ、12 月に警察庁が NAS を狙ったアクセスが増加していると警告

した。[III]

ネットワーク対応機器の多くは、Linux をベースとしたオペレーティングシステムを使用しており、ウェブサーバー機能を搭載している場合も多い。今後もネットワーク機器の Linux およびウェブサーバー部分が攻撃される傾向が継続すると考えられる。

＜ネットワーク対応機器の問題点＞

ネットワーク対応機器に対するセキュリティ上の懸念は新しいものではなくサーバーやパソコン等と類似している。攻撃を受ける主な要因として、以下の点が挙げられる。

- **セキュリティを充分考慮していない設計**

初期状態では認証無しに誰でも機能にアクセス可能である等、多くの機器は未だにセキュリティを考慮せず設計されている。初期状態で利用している機器が被害に遭うことが多い。

- **インターネットからアクセス可能な状態**

機器が直接インターネットに接続している場合に攻撃を受ける可能性を利用者が充分に認識できていないことが多い。

- **更新（アップデート）されない機器**

パソコンのソフトウェアとは異なり、更新のための修正プログラム（アップデート）が自動で配信されない機器が大多数を占める。製品開発者のウェブサイトで修正プログラムが提供されていることに気付かない場合や、工場等では安定稼動の継続を重視して修正プログラムを適用できない場合もある。また、脆弱性が存在するにも関わらず製品開発者からアップデートが提供されない機器もある。

- **管理者不在の機器**

サーバーやパソコン以外のオフィス機器は、ネットワークやシステムの管理者の管理対象外になっていることが多い。

＜機器への留意点・対策＞

ネットワーク対応機器もサーバーやパソコン等と同様に対策を実施する必要があると考え、製品開発者やシステム管理者、および利用者それぞれが以下を留意しなければならない。

- **製品開発者**

初期状態でセキュリティの高い設定にする。取り扱うデータに対してプライバシーの侵害や情報漏えい対策を行う。また、セキュリティの懸念があれば、利用者に対して注意喚起を行うと共に迅速に対策を講じる。

- **システム管理者**

ファイアウォールやブロードバンドルーター等の通信機器を用いて、ネットワークの境界を設け、インターネットからのアクセスを制限する。また、企業・組織においてはネットワーク接続機器にもセキュリティポリシーを定めて適用する。インターネット側から接続可能な機器が無いかを検査することも重要である。[IV]

- **利用者**

インターネットへの接続に関わらず、機器をネットワークに接続する際に、攻撃者からアクセスされる可能性を充分に認識し、適切に機器のセキュリティを設定して利用することが重要である。

参考資料

I. ルータ感染ワームは未解決の脆弱性を悪用、Linksysが対策を紹介
http://www.itmedia.co.jp/enterprise/articles/1402/18/news040.html
II. bashの脆弱性を抱えるNASへの攻撃、日本や韓国が標的に
http://www.itmedia.co.jp/enterprise/articles/1410/03/news109.html
III. 警察庁: Bash の脆弱性を標的としたアクセスの観測について
http://www.npa.go.jp/cyberpolice/topics/?seq=15063
IV. IPA:「増加するインターネット接続機器の不適切な情報公開とその対策」
https://www.ipa.go.jp/security/technicalwatch/20140227.html

3.3. 拡大するネット犯罪の被害

～巧妙化するウイルスやネット詐欺による金銭被害～

犯罪者や犯罪グループがITを悪用して金銭を窃取する事件が増加している。ウイルスを使ったインターネットバンキングからの不正送金、銀行等の偽のウェブサイトにログインさせようとするフィッシング詐欺、スマートフォン利用者を狙った不当な会費の請求等、年々手口が多様化し、被害金額が増大している。

＜犯罪者もITを利用＞

現在、コンピュータやスマートフォンおよびインターネット等のITは、生活に欠かすことのできない社会インフラとして広く普及している。しかしながら、IT は、一般利用者だけではなく犯罪者または犯罪グループにも同様に便利であることを忘れてはならない。犯罪者は、メールやウェブサイトを悪用して、ウイルスによるパスワード等の認証情報やクレジットカード情報の窃取や、払う必要の無い会費等金銭の不当請求により、利用者から金銭を奪う。

犯罪グループは、Facebook や LINE 等のソーシャルネットワークサービス（SNS）等、新しいサービスも巧みに悪用する。また、ソフトウェアの情報セキュリティ上の欠陥である脆弱性の悪用や、ウイルス対策ソフトの検知回避等、高度な研究を行いながら、新種のウイルスを開発していると考えられる。

＜金銭被害額の増加＞

2014 年は、インターネットバンキングに関わる不正送金被害が急増した。警察庁の調べによると、2014 年のインターネットバンキングに関わる不正送金の総被害額は 29 億 1,000 万円となり、2013 年の 14 億 600 万円に対し、被害額が約 2 倍に急増した。特に、法人口座の被害額は、2013 年の 9,800 万円から 2014 年には 10 億 8,800 万円と約 11 倍に増加しており、個人だけでなく法人も狙われていることが顕著に示されている。[1]

海外では利用者ではなく直接銀行から金銭を窃取する攻撃も確認されており、今後、

日本の銀行への攻撃が懸念されている。[II]

＜不正請求の手口＞

第 2 章の 1 位「インターネットバンキングやクレジットカード情報の不正利用」で解説しているウイルスによる不正送金やフィッシング詐欺以外にも、金銭を狙う手口は数多く存在する。パソコン等の画面上に請求画面を表示させる代表的な手口を以下に紹介する。

- **ワンクリック請求**

アダルトサイトの動画を閲覧するために、18 歳以上である等の利用規約の同意ボタンをクリックさせたり、動画閲覧用のソフトウェアと偽ってウイルスをインストールさせたりする等の手口により、利用者の画面に有料会員の会費の請求画面を表示させる。これだけでは金銭被害は発生しないが、請求に驚いた閲覧者が個人情報を入力してしまうと、詐欺グループから電話やメール等で執拗に会費を振り込むよう要求される。[III]

以前はパソコン利用者が標的になっていたが、IPA では 2011 年からスマートフォンの電話発信機能を狙ったワンクリック請求を確認しており、Android 利用者も iPhone 利用者もこの詐欺の標的となっている。[IV]

- **偽ウイルス対策ソフト**

インターネットの広告スペースを悪用し、あたかもウイルスに感染しているかのように偽の警告画面を表示し、その問題を解決するために 1 万円程度の有償製品の購入を迫る偽ウイルス対策ソフトと呼ばれるウイルスがある。正規のウイルス対策ソフトを連想させるソフト名や警告が表示されることでウイルス感染を恐れた一般利用者が、画面の案内に従って偽ウイルス対策ソフトを購入してしまう。

- **ランサムウェア**

感染するとパソコン画面のロックやファイルを暗号化し、解除するための身代金を要求するランサムウェアと呼ばれるウイルスが存在する。業務上必要なファイルや思い出の写真等、重要なデータにアクセスできなくなったパソコンの利用者は、やむを得ず金銭を支払ってしまう。

＜IT にも防犯が必要＞

空き巣や振り込め詐欺等と同様に、IT を悪用した詐欺に対しても、手口や事例を知ることが防犯対策となる。警察庁のサイト [V] や銀行のサイトまたは IPA のサイト [VI] には、上記の代表的な手口の対処方法や最新の手口が紹介されており、これらのサイトを参照して事前に手口を知ることで、被害を未然に防ぐことができる。

参考資料

I. 警察庁：平成26年中のインターネットバンキングに係る不正送金事犯の発生状況等について
http://www.npa.go.jp/newlyarrived/?seq=15339
II. カスペルスキー：今世紀最大規模の銀行強盗：10億ドルが盗まれる
http://blog.kaspersky.co.jp/billion-dollar-apt-carbanak/6879/
III. IPA：ワンクリック請求に関する相談急増！ パソコン利用者にとっての対策は、まずは手口を知ることから！
https://www.ipa.go.jp/security/topics/alert20080909.html
IV. IPA：2013年5月の呼びかけ「スマホにおける新たなワンクリック請求の手口に気をつけよう！」
https://www.ipa.go.jp/security/txt/2013/05outline.html
V. 警察庁：サイバー犯罪対策
http://www.npa.go.jp/cyber/
VI. IPA：情報セキュリティ 今月の呼びかけ
https://www.ipa.go.jp/security/personal/yobikake/

10 大脅威執筆者会

氏名	所属	氏名	所属
石田 淳一	(株)アールジェイ	神薗 雅紀	(株)セキュアブレイン
木村 道弘	(株)ECSEC Laboratory	星澤 裕二	(株)セキュアブレイン
佐藤 直之	(株)イノベーションプラス	平田 真由美	セキュリティ対策推進協議会(SPREAD)
齋藤 衛	(株)インターネットイニシアティブ	唐沢 勇輔	ソースネクスト(株)
高橋 康敏	(株)インターネットイニシアティブ	辻 伸弘	ソフトバンク・テクノロジー(株)
梨和 久雄	(株)インターネットイニシアティブ	永野 恵寿	地方公共団体情報システム機構
三輪 信雄	S&J(株)	百瀬 昌幸	地方公共団体情報システム機構
松本 隆	SCSK(株)	山崎 英人	(株)T マネー
大塚 淳平	NRI セキュアテクノロジーズ(株)	杉山 俊春	(株)ディー・エヌ・エー
小林 克巳	NRI セキュアテクノロジーズ(株)	森 槙悟	(株)ディー・エヌ・エー
正木 健介	NRI セキュアテクノロジーズ(株)	桑原 和也	デジタルアーツ(株)
中西 克彦	NEC ネクサソリューションズ(株)	岩井 博樹	デロイト トーマツ リスクサービス(株)
北河 拓士	NTT コムセキュリティ(株)	大浪 大介	(株) 東芝
東内 裕二	NTT コムセキュリティ(株)	田岡 聡	(株) 東芝
鴨田 浩明	(株)NTT データ	長尾 修一	東芝インフォメーションシステムズ(株)
西尾 秀一	(株)NTT データ	小島 健司	東芝ソリューション(株)
宮本 久仁男	(株)NTT データ	小屋 晋吾	トレンドマイクロ(株)
植草 祐則	NTTデータ先端技術(株)	大塚 祥央	内閣サイバーセキュリティセンター
佐久間 邦彦	NTTデータ先端技術(株)	佐々木 勇也	内閣サイバーセキュリティセンター
村上 純一	(株)FFRI	須川 賢洋	新潟大学
岡田 良太郎	OWASP Japan Chapter	田中 修司	日揮(株)
前田 典彦	(株)カスペルスキー	井上 博文	日本アイ・ビー・エム(株)
小林 偉昭	技術研究組合制御システムセキュリティセンター	徳田 敏文	日本アイ・ビー・エム(株)
		守屋 英一	日本アイ・ビー・エム(株)
小熊 慶一郎	(株)KBIZ	宇都宮 和顕	日本電気(株)
岡村 浩成	京セラコミュニケーションシステム(株)	谷川 哲司	日本電気(株)
小峰 広道	京セラコミュニケーションシステム(株)	住本 順一	日本電信電話(株)
佐藤 宏昭	京セラコミュニケーションシステム(株)	種茂 文之	日本電信電話(株)
谷合 通宏	(社)金融 ISAC	加藤 雅彦	NPO 日本ネットワークセキュリティ協会
秋山 卓司	クロストラスト(株)	やすだ なお	NPO 日本ネットワークセキュリティ協会
鈴木 啓紹	(社)コンピュータソフトウェア協会(CSAJ)	榎本 司	日本ヒューレット・パッカード(株)
名和 利男	(株)サイバーディフェンス研究所	大森 健史	日本ヒューレット・パッカード(株)
福森 大喜	(株)サイバーディフェンス研究所	加藤 義登	日本ヒューレット・パッカード(株)
楢原 盛史	シスコシステムズ合同会社	大村 友和	(株)ネクストジェン
宮崎 清隆	(社)JPCERT コーディネーションセンター(JPCERT/CC)	金 明寛	(株)ネクストジェン
		杉岡 弘毅	(株)ネクストジェン
宮地 利雄	(社)JPCERT コーディネーションセンター(JPCERT/CC)	七條 麻衣子	(公財)ハイパーネットワーク社会研究所
		徳丸 浩	HASH コンサルティング(株)
林 薫	(株)シマンテック	渡辺 久晃	パナソニック(株)
村上 大輔	(株)シマンテック	水越 一郎	東日本電信電話(株)
山内 正	(株)シマンテック	太田 良典	(株)ビジネス･アーキテクツ

氏名	所属	氏名	所属
大森 雅司	(株)日立システムズ	綿口 吉郎	(株)富士通研究所
折田 彰	(株)日立システムズ	山室 太平	(株)ベリサーブ
本川 祐治	(株)日立システムズ	清水 秀一郎	三井物産セキュアディレクション(株)
寺田 真敏	(株)日立製作所	川口 修司	(株)三菱総合研究所
藤原 将志	(株)日立製作所	村野 正泰	(株)三菱総合研究所
古賀 洋一郎	ビッグローブ(株)	冨張 伸宏	(株)ユービーセキュア
上村 理	ファイア・アイ(株)	志田 智	(株)ユビテック
服部 良平	ファイア・アイ(株)	福本 佳成	楽天(株)
山下 慶子	ファイア・アイ(株)	山崎 圭吾	(株)ラック
原田 弘和	富士通(株)	若居 和直	(株)ラック

IPA 協力者

伊藤 毅志　町田 昇　金野 千里　栗栖 正典　花村 憲一

渡辺 貴仁　板橋 博之　谷口 隼祐　加賀谷 伸一郎　小川 貴之

野澤 裕一　亀山 友彦

著作・制作　　独立行政法人情報処理推進機構（IPA）

編集責任　　土屋 正

イラスト制作　　株式会社 創樹

執筆協力者　　10 大脅威執筆者会

執筆者　　土屋 正　　中西 基裕　　関口 竜也
山下 勇太　　岡崎 圭輔　　篠原 崇弘

情報セキュリティ 10 大脅威 2015

～ 被害に遭わないために実施すべき対策は？ ～

2015 年 3 月 25 日　　第 1 刷発行

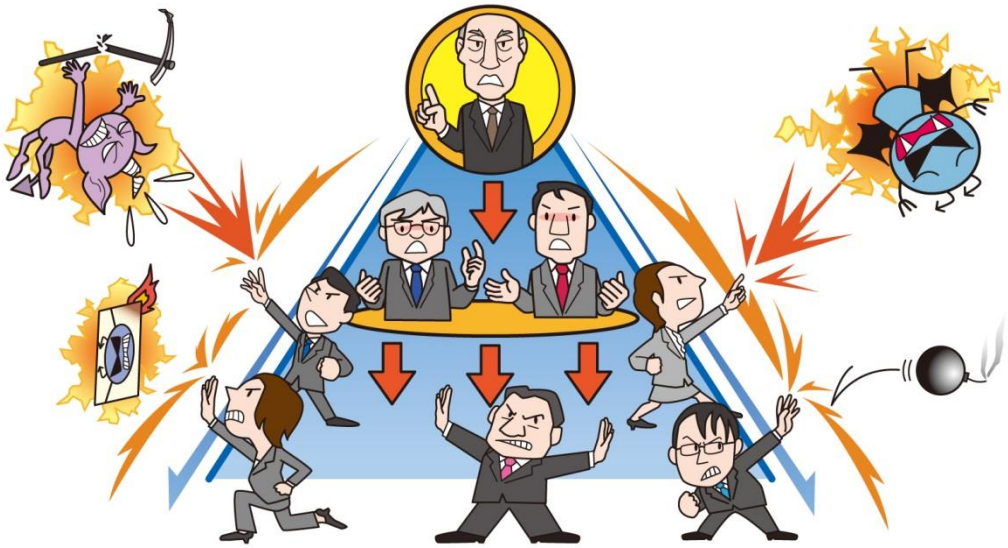
[事務局・発行]　　独立行政法人情報処理推進機構

〒113-6591

東京都文京区本駒込二丁目 28 番 8 号

文京グリーンコートセンターオフィス

https://www.ipa.go.jp/



IPA 独立行政法人**情報処理推進機構**
セキュリティセンター

〒113-6591
東京都文京区本駒込二丁目 28 番 8 号
文京グリーンコートセンターオフィス
TEL：03-5978-7527　FAX：03-5978-7518
https://www.ipa.go.jp/security/