

2010 年版

# 10 大脅威

『あぶり出される組織の弱点！』



**IPA**<sup>®</sup>

独立行政法人 情報処理推進機構  
セキュリティセンター

2010 年 3 月

本書は、次の URL からダウンロードできます。

2010 年版

10 大脅威 『あぶり出される組織の弱点！』

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

## 目次

---

2010年版 10大脅威.....	3
はじめに.....	3
第1章 2009年における組織へのビジネスインパクト.....	4
1.1 大手企業でも相次ぐガンブラー.....	4
1.1.1 ガンブラーの脅威とリスク.....	4
1.1.2 ビジネスインパクト.....	5
証券会社や金融機関等の場合.....	5
製造業等の場合.....	5
1.1.3 事前対策・事後対応.....	5
1.2 内部犯罪による情報窃取事件.....	6
1.2.1 内部犯罪の脅威とリスク.....	6
1.2.2 ビジネスインパクト.....	7
製造業(車や医薬品等)の場合.....	7
1.2.3 事前対策・事後対応.....	7
第2章 10大脅威.....	8
【1位】変化を続けるウェブサイト改ざんの手口.....	8
【2位】アップデートしていないクライアントソフト.....	10
【3位】悪質なウイルスやボットの多目的化.....	12
【4位】対策をしていないサーバ製品の脆弱性.....	14
【5位】あわせて事後対応を！情報漏えい事故.....	16
【6位】被害に気づけない標的型攻撃.....	18
【7位】深刻なDDoS攻撃.....	20
【8位】正規のアカウントを悪用される脅威.....	22
【9位】クラウド・コンピューティングのセキュリティ問題.....	24
【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.....	26
第3章 対策.....	28
3.1 体制の整備・ルール作成.....	28
3.2 安全な運用のための企画・設計.....	29
3.3 安全な運用のための契約.....	29

3.4 サーバシステムへの対策 .....	30
3.5 クライアントシステムへの対策 .....	30
3.6 アカウント情報の管理・運用 .....	30
3.7 セキュア・プログラミング .....	31
3.8 体制・ルール・システム等の点検 .....	31
3.9 体制・ルール・システム等の見直し .....	31
【付録 1】 10 大脅威関係表 .....	32
【付録 2】 10 大脅威関連図 .....	33
【付録 3】 参考資料 .....	34
執筆協力者 .....	35

# 2010年版 10大脅威

## 『あぶり出される組織の弱点！』

### はじめに

2009年にはガンブラー(Gumblar)によるウェブサイト改ざん・ウイルス感染等をはじめとした様々なセキュリティ事故・事件が発生した。特にガンブラーは、自組織だけではなく業務委託先も含めたセキュリティ対策を考えなければならなくなった例と言える。この委託先も含めたセキュリティ対策は新しい考え方ではない。組織としては、従来から必要とされてきた対策を再認識して対策を進めたい。対策はやみくもに行うのではなく、「脅威」が組織に対してどのような「リスク」を生じ、さらに組織へどのような「ビジネスインパクト」を及ぼすかを判断したうえで適切な、コストとのバランスを考慮した対策をすることが望ましい。

本書における「脅威」とは、自組織へ何らかの損害を与える事象である。「リスク」とは、その「脅威」によって自組織にもたらされる損害や危険に遭う可能性である。「ビジネスインパクト」と

は、「リスク」が自組織のビジネスやサービス継続に及ぼす影響の度合いである。

組織は対策を進める際に、事業の継続管理の考えに従って、脅威が自組織に及ぼすビジネスインパクトを分析・評価し、適切な対策をしていく必要がある。事業継続にとって重要な情報やシステムに対して、多重の対策を施したい。対策には、セキュリティ事故・事件の発生を低減して事業継続できるようにする「事前対策」と、事故が起き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2つを考える必要がある。

本書の第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する。第2章の10大脅威では、それぞれの脅威についての解説とその影響を踏まえ、第3章では考えられる対策を紹介している。

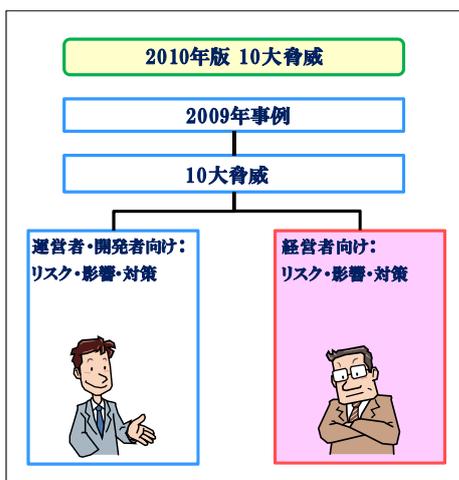


図1. 2010年版10大脅威対象

表1. 2010年版 10大脅威

順位	10大脅威
1位	変化を続けるウェブサイト改ざんの手口
2位	アップデートしていないクライアントソフト
3位	悪質なウイルスやボットの多目的化
4位	対策をしていないサーバ製品の脆弱性
5位	あわせて事後対応を！情報漏えい事件
6位	被害に気づけない標的型攻撃
7位	深刻なDDoS攻撃
8位	正規のアカウントを悪用される脅威
9位	クラウド・コンピューティングのセキュリティ問題
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

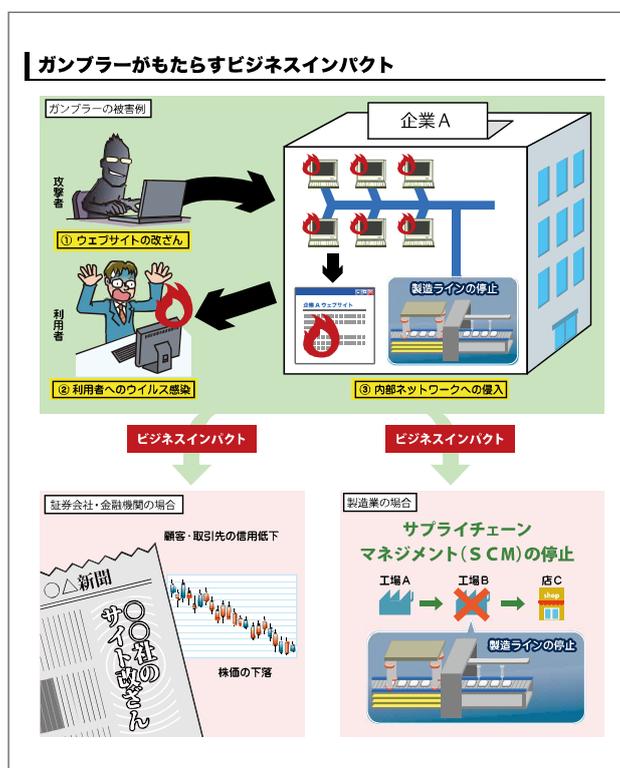
# 第1章 2009年における組織へのビジネスインパクト

本章では、2009年に実際に起きたセキュリティ事故・事件に基づき、いくつかの組織にとって考えられるリスクを明確にし、ビジネスインパクトを分析・評価し、組織としての問題点と対策を考察する。事業継続の管理におけるインパクト分析の視点で対策をとることを提起している。

本章では、「金融機関」や「製造業」を例にそれぞれのビジネスインパクトを分析した。

なお、本章は「事業継続計画(BCP)策定ガイドライン」(編:経済産業省)を参考に記載している。

## 1.1 大手企業でも相次ぐランブラー



### 1.1.1 ランブラーの脅威とリスク

ランブラーと呼ばれるウイルス感染の手口は一般紙やテレビ番組等でも報道された。これらの報道は、「有名企業や公共機関のウェブサイトが改ざんされ、そのサイトを閲覧した利用者がウイルスに感染した可能性がある」というものだ。公共交通機関や大手のカード会社等が含まれている。

ランブラーでは、次のような3つの脅威とそれぞれのリスクが挙げられる。

- ① 自組織のウェブサイトが改ざんされる脅威:  
自組織のウェブサイトが、ウイルスを頒布するサイトへ改ざんされる脅威の結果、自組織のサイトに訪れた利用者に対して攻撃者になってしまう。結果として、セキュリティ対策が不十分な組織であると見られてしまうリスクが考えられる。
- ② 利用者から情報が窃取される脅威:  
改ざんされたウェブサイトを閲覧した利用者がウイルスに感染した場合、その利

用者の個人情報等が盗まれてしまう脅威がある。その結果、組織の信頼が低下するリスクが考えられる。

③ 自組織内のネットワークを攻撃される脅威:

自組織内のネットワークを攻撃される脅威がある。その結果、攻撃者による自組織内の重要な情報の窃取や、ネットワークや重要なシステムを利用停止に陥らせる攻撃をされるリスクが考えられる。このリスクは、2010年3月時点で実際の被害は報告されていないが、発生しうるリスクである。

### 1.1.2 ビジネスインパクト

#### 証券会社や金融機関等の場合

証券会社や金融機関等の場合、1.1.1の①と②の脅威・リスクに対して、次のようなビジネスインパクトがある。

まず、利用者がウェブサイト上で株式等の売買をしていて、誤った情報で被害を受けてしまうと、その企業の信頼は低下してしまう。

次に、利用者の個人情報や金銭情報が窃取されてしまうことにより、損害賠償や組織に対する信頼の低下が起きてしまう。

利用者の財産に大きな被害を及ぼすような事態に陥れば、被害を受けた利用者の信頼低下だけに留まらず、顧客全体の信頼低下につながってしまう。そして、それが報道されるとステークホルダの信頼も低下して、売り上げの低下や株価の下落を招く可能性がある。

ウェブサイトにおける売り上げの依存度が高い場合、事業継続が困難となってしまう。

#### 製造業等の場合

精密機械等を製造する会社の場合、特に1.1.1の③の脅威・リスクに対して次のようなビジネスインパクトが考えられる。

このような会社では、製造ライン等でコンピュ

ータを使用している。また、商品の耐久テストや実験等でもコンピュータを使用している。商品の開発に関わる設計図もコンピュータ上に保存している。このような用途で使用されるコンピュータは通常、インターネットに直接接続していることは考えにくい。しかし、ガンブラー等でダウンロードされたウイルスが、社内ネットワークや外部記憶媒体を通して、会社の重要な情報を窃取や、コンピュータをサービス停止状態に陥れるような攻撃を行う可能性がある。

製造ラインを攻撃され、停止してしまうと商品の出荷が停止してしまうため、サプライチェーンに影響を与えてしまう。関連企業に損害を与えてしまい、その補償等を行わなければならない事態に陥る可能性がある。

また、設計図等の窃取が行われてしまうと、この情報を用いて、競合他社から安価な商品が販売され、価格競争で負けてしまうような事態に陥る可能性がある。

#### 1.1.3 事前対策・事後対応

対策は、事業継続の観点から行う必要がある。例えば、次のような事前対策と事後対応を組み込みたい。

事前対策として、組織にとって特に重要な情報やシステムが何かを洗い出し、それらをどのように守るのか、ルールと体制を整備しなければならない。ガンブラーでは、自組織だけでなく、ウェブサイトの運営委託先までも含めてIDやパスワードが窃取されてしまったことが大きな原因である。したがって、委託先等の関係組織に対するセキュリティ対策も考慮すべきであることを念頭に置きたい。

重要な情報やシステムに対しては、アクセスできる担当者を限定する必要がある。これには、担当者以外が重要なシステムが動作している部屋へ入室することの禁止や、担当者自身に

も外部メディアを持ち込ませない等の物理的な防御もある。また、担当者をネットワークを通じてアクセスさせないシステム上の防御もある。

更に、ガンブラーの被害に遭わないための事前対策では、重要な情報やシステムの関係者の使用 PC において、クライアントソフトウェアやウイルス対策ソフトの定義ファイルのアップデートを定期的実施するルールを盛り込まなければならない。これは組織内だけに留まらず、委託先を含めた関係組織全てに該当する。

次に、事後対応も「事業継続計画(BCP)策定ガイドライン」等を参考に考える必要がある。例えば事後対応は、「BCP 発動」、「原因調査」、「顧客対応等のリスクコミュニケーション」、「再発防止策の実施」という順序で行う。

「BCP 発動」で担当者による情報の一元化を図り、情報の管理を徹底する。

「原因調査」では、漏えいした項目、量等も

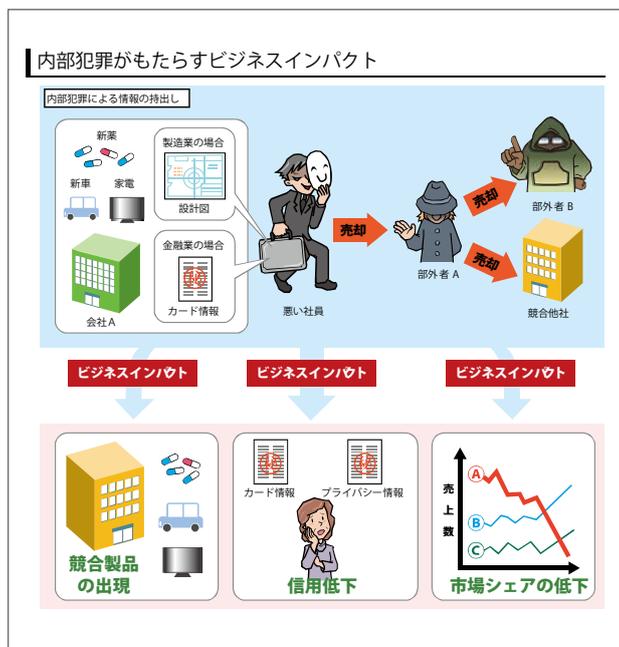
分析する。これには外部の専門調査機関を利用する手法もある。

「リスクコミュニケーション」は、顧客、潜在顧客、株主、関係省庁等の関係者において必要な情報が何かを把握し、情報をタイムリーに提供することである。提供方法は事実関係の公表、記者会見、窓口の設置等の手段がある。

リスクコミュニケーションは、事業継続において大事な観点である。関係者に必要な情報を適切に公表しないことは、関係者から信頼を得られなくなり、今後の事業継続において大きな影響を及ぼす。また、リスクコミュニケーションでは、「再発防止策」も公表の対象である。継続的な情報開示によって、対策の進捗状況を明らかにすることで、信頼を回復していきたい。

被害を最小限に留め、真摯な対応を取ることでビジネスチャンスの拡大につながることも考えられる。

## 1.2 内部犯罪による情報窃取事件



### 1.2.1 内部犯罪の脅威とリスク

某大手企業で情報窃取が発生し、その被害

額が約 70 億円である、と試算したニュースが 2009 年 9 月に流れた。社員が不正に顧客情報

を持ち出し、それを外部へ売却したという事件に対する当該企業による被害額の試算だ。

この事件は、犯人の逮捕にまで至り、CD を持ち出したという窃盗及び他人の ID を使用したという不正アクセス行為の禁止等に関する法律違反の罪となった。

このような内部犯罪による情報窃取の脅威は、外部からの攻撃による情報窃取の脅威に比べて重要な情報を窃取される可能性が高い。上記のような例では、犯人は重要な情報(または機密情報)にアクセスする権限を持っていたため、情報を容易に盗める状態であったからだ。内部犯罪では、故意に情報を盗んでいるため、その情報が悪用される可能性が非常に高い。

顧客情報や機密情報等が窃取されてしまい、悪用されると組織の信頼失墜だけでなく、競争力が低下する等のリスクが考えられる。このリスクによって、直接的な金銭的損失や対応時間が掛かってしまい、コストがかかってしまうビジネスインパクトへ発展する。

### 1.2.2 ビジネスインパクト

#### 製造業(車や医薬品等)の場合

内部犯罪により商品図面や製薬成分等の情報が窃取され、他組織に転売されてしまい、悪用されるというようなビジネスインパクトがある。

たとえば、競合他社に安価で同様の商品を出されてしまい、結果的に価格競争に負けてしまうという事態が考えられる。その結果、自社製品が売れなくなり、事業継続に深刻な影響を及ぼしてしまう。

また、複数の企業での共同開発の情報や委託された開発に関する情報であれば、提携企業、顧客に対しても損害を与えることになる。これによって、窃取された情報に関する補償だけでなく、提携企業、顧客からの信用の失墜も考えられる。その場合、今後の事業継続を困

難にする事態に陥る。

### 1.2.3 事前対策・事後対応

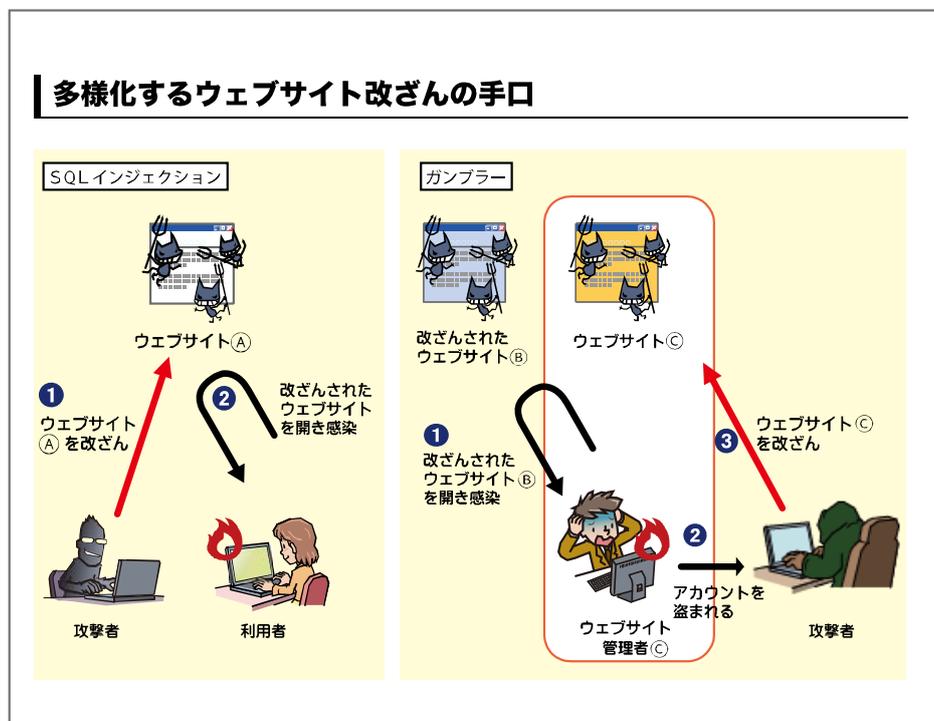
一般紙をはじめとするメディアで取り上げられている内部犯罪の事件では、不正経理や私文書(公文書)偽造等、様々なことが取り上げられている。経営者は、これらの問題と同様に、情報窃取に関しても対策しなければならない。ここでは内部犯罪による情報窃取について述べる。

事前対策には、IPA の「情報セキュリティ教本」等を参考に総合的な対策を行いたい。例えば、アクセス制御である。重要な情報に対してアクセス制御を行っておきたい。重要な情報が保存されているシステムがある部屋へのアクセスを生体認証付の入退室管理にして制限する等の「物理的な側面」と、社員が PC からアクセスできることをシステム上の権限チェックにより制限する「システムの側面」での双方でのアクセス制御が必要だ。重要な情報へアクセスして作業をする際は、二重チェックする等のルールを適用することも有効になる。このようなアクセス制御をすることで、社員を監視していることを示すことにより、社員が不正に持ち出すことに対する抑止効果が生まれる。

また、事後対応も重要である。事業継続における影響を最小限に留めることを考えておきたい。事後対応は、1.1.3 と同様の対策が必要である。内部犯罪のように重要な情報を盗まれてしまうような事態では、特に顧客や提携企業、警察、関係省庁等の関係者に対するリスクコミュニケーションが重要である。継続的な情報開示によって、対策の進捗状況を明らかにすることで、信頼を回復していきたい。このようにして、事業継続における影響を最小限に留めたい。

## 第2章 10大脅威

### 【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る。このような脅威をもたらす攻撃に新しい手口が現れた。「第1章 1.1のガンブラー」だ。

#### 脅威

近年のウェブサイトを経由した攻撃では、一定の信用を獲得しているウェブサイトが改ざんされ、加害者となってしまうことが多い。ガンブラー以前には、SQL インジェクション攻撃によって同様の脅威をもたらされた。SQL インジェクション攻撃に対して脆弱なウェブサイトが攻撃を受けると、データベース内の情報を改ざんされ、ウイルスを頒布するサイトへ誘導するウェブサイトとして利用され、利用者へウイルスをダウンロードさせてしまう。2009年もSQL インジェクション攻撃は確認されており、引き続き注意が必要である。

2009年に流行した攻撃トピックの一つであるガンブラーは、ウェブサイトを改ざんする手口がSQL インジェクションと異なる。SQL インジェクションではデータベースが狙われたが、ガンブラーはデータベースとは無関係で、多くの場合、ガンブラーはウェブサイトの更新に使用するFTP(File Transfer Protocol)等のアカウントの認証情報を盗み改ざんする。FTPアカウントでのウェブサイトの更新は多くのウェブサイトで行われているため、ガンブラーの被害は数多くのサイトが確認されている。このガンブラーの被害は次のような流れで生じる。

1. ウェブサイトAの更新担当者が、改ざんされたウェブサイトBにアクセスする。
2. 改ざんされたウェブサイトBが、ウイルスを頒布するウェブサイトCへのアクセスを誘導する。

3. ウェブサイト A の更新担当者は、ウェブサイト C から、ウイルスをダウンロードさせられ、実行させられる。
4. ウィルスによって、ウェブサイト A の更新に使用する FTP のアカウント等が漏えいする(攻撃者へ送られる)。
5. 盗んだ FTP のアカウントが悪用され、ウェブサイト A が改ざんされる。

以降、別のウェブサイト D の更新担当者がウェブサイト A にアクセスすると、同様にウェブサイト D が改ざんされる。このような手口で、ガンブラーによる被害は連鎖的に増える仕組みになっている。

### 2009 年の事例・統計

ここでは、SQL インジェクション攻撃とガンブラーの事例や統計について述べる。

国内における SQL インジェクション攻撃は、2008 年末から 2009 年初頭にかけて多く観測されたという国内セキュリティベンダのレポートがある。その後、同レポートでは観測数が減少し、

2007 年の水準に戻ったとしている。

ガンブラーの被害は、2010 年 2 月時点で企業等が公表しているだけで数十件の例がある。しかし、セキュリティベンダ各社のレポートでは、日本でも数千件、海外を含めると数万件以上の被害があったとしている。

### 影響

ガンブラーは、大手企業のウェブサイトが改ざんされたこともあり、新聞等でも大きく取り上げられた。これによって、ウェブサイトを運営する各組織で、対応を迫られる事態となっている。

また、ウェブサイトを運用する会社から FTP のアカウントが漏えいするケースも散見された。このため、ウェブサイトの運用を外部に委託している場合には、委託先のセキュリティ対策も考慮する必要が生じている。

2009 年は、数多くのウェブサイトが改ざんされた。自組織のウェブサイト、およびサイト利用者が被害を受けまいよう、運用方法を見直す必要がある。

## 第3章:対策

「3.1体制の整備・ルールの作成(P28)」・「3.2安全な運用のための企画・設計(P29)」・「3.3安全な運用のための契約(P29)」

「3.8体制・ルール・システム等の点検(P31)」・「3.9体制・ルール・システム等の見直し(P31)」

SQLインジェクション:

「3.4サーバシステムへの対策(P30)」・「3.7セキュア・プログラミング(P31)」

ガンブラー:

「3.5クライアントシステムへの対策(P30)」・「3.6アカウント情報の管理・運用(P30)」

## 関連資料

IPA: “ガンブラー” の手口を知り、対策をしましょう

<http://www.ipa.go.jp/security/txt/2010/02outline.html#5>

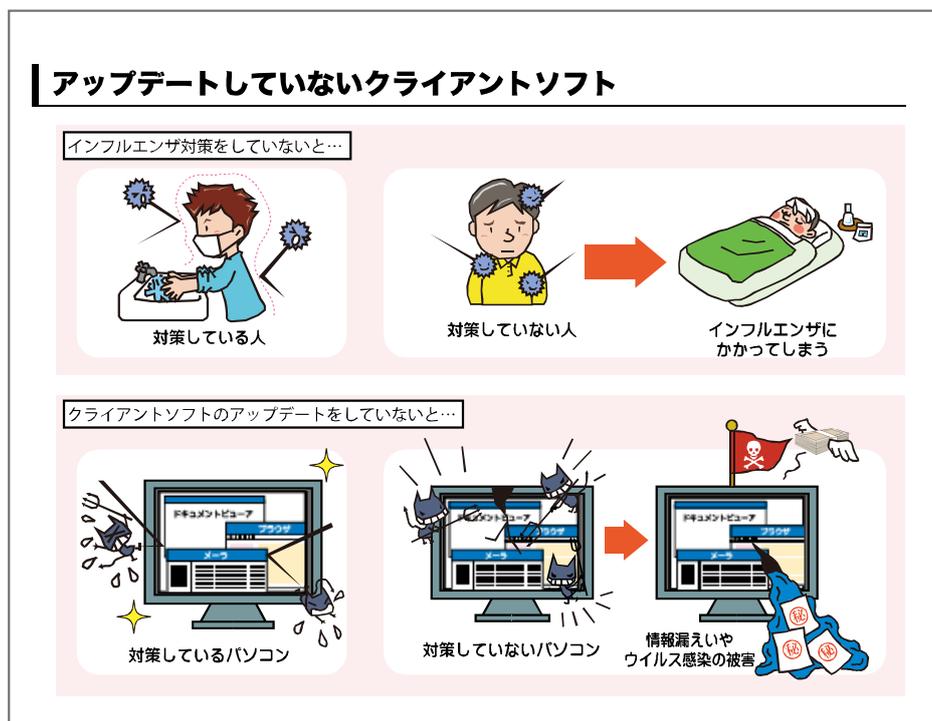
So-net: 「ガンブラー」「サイト改ざん」めぐる基本のQ&A ～ 何が起きている? 対策は?

[http://www.so-net.ne.jp/security/news/newsttopics\\_201001.html](http://www.so-net.ne.jp/security/news/newsttopics_201001.html)

LAC: SQLインジェクション攻撃検知数(2009年5月まで)

<http://www.lac.co.jp/info/alert/alert20090609.html>

## 【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た。しかし、悪用された脆弱性の中には開発者が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だ。

### 脅威

コンピュータ上では様々なソフトウェアが動作している。OS(Operating System)や OS に付随するソフトウェア、購入してインストールするソフトウェア、フリーソフトウェア等だ。これらのソフトウェアに、脆弱性が見つかる場合がある。

ソフトウェアの脆弱性は、見つかりと攻撃に悪用されることがある。そのため、ソフトウェアの利用者は、脆弱性を修正したバージョンへアップデートしなくてはならない。

「第 1 章 1.1 のガンブラー」等では、クライアント PC で利用されるソフトウェアの脆弱性が突かれている。それらの脆弱性の多くは、既に開

発者が修正したバージョンを提供しているソフトウェアである。したがって、ソフトウェアをアップデートすることが有効な対策になる。

最近の OS やソフトウェアには、自動的なアップデート機能が備わっていることがある。OS や OS に付随するソフトウェアは、専用のアップデート機能によって一括でアップデートできるものが多い。その他のソフトウェアも、アップデート機能がある場合、アップデートを促す通知をしている。広く普及しているソフトウェアには、このようなアップデート機能があることが多い。

しかし、クライアント PC の利用者は、ソフトウェアをアップデートせず、古いまま使い続けることも少なくない。

昨今、クライアント PC の脆弱性が攻撃に悪用されているため、ソフトウェアのアップデートはより切実な問題になったと言える。

### 2009 年の事例・統計

IPA は「2009 年度 情報セキュリティの脅威に対する意識調査」の中で、アップデートをしない(セキュリティパッチを適用しない)理由について調査した。

調査結果では、セキュリティパッチを適用しない理由として、「セキュリティパッチの更新方法が分からない(42.5%)」が最上位に挙げられた。これは、OS やソフトウェアベンダが提供している自動的なアップデート機能が、利用者に理解されていないものと思われる。

また、「手間がかかる」という理由も上位にある。これは、作業を中断することの兼ね合いと考えられる。この他にも、「更新するメリットがわからない」、「セキュリティパッチを更新する必要性を感じない」という理由も挙げられている。このように、アップデートの必要性が、ソフトウェア利用者に理解されていない現実が明らかになっている。

また、2009 年 8 月頃の海外企業の調査では、調査対象の 250 万人のうち、79.5%が脆弱なバージョンの Adobe Flash を利用しており、さらに

83.5%が脆弱なバージョンの Acrobat や Adobe Reader を使っていることが示された。

このような背景があるため、Adobe 社の製品の脆弱性を狙うウイルスが増加傾向である。これは Adobe 社の製品が普及していることから、多くの利用者へウイルスを感染させるために狙われていると考えられる。

### 影響

多くのクライアント PC がアップデートされないという現実から、今後もクライアント PC をターゲットとした攻撃が続くと予想される。したがって、ランサムウェアのような攻撃が今後も十分に起こりうる。特にクライアント PC は社内のネットワークを通して重要なシステムに対して接続できるような環境にある場合がある。社内の他の PC へのウイルス感染や重要なシステムに対する DDoS 攻撃(参照:7 位深刻な DDoS 攻撃)、重要な情報の窃取等の被害を受けることが考えられる。そのため、利用者によるアップデートの徹底が望まれる。そのため、第 3 章 3.5(クライアントシステムの対策)等を参考に対策を行いたい。

## 第3章:対策

「3.1体制の整備・ルールの作成(P28)」・「3.2安全な運用のための企画・設計(P29)」・「3.3安全な運用のための契約(P29)」

「3.5クライアントシステムへの対策(P30)」

「3.8体制・ルール・システム等の点検(P31)」・「3.9体制・ルール・システム等の見直し(P31)」

## 関連資料

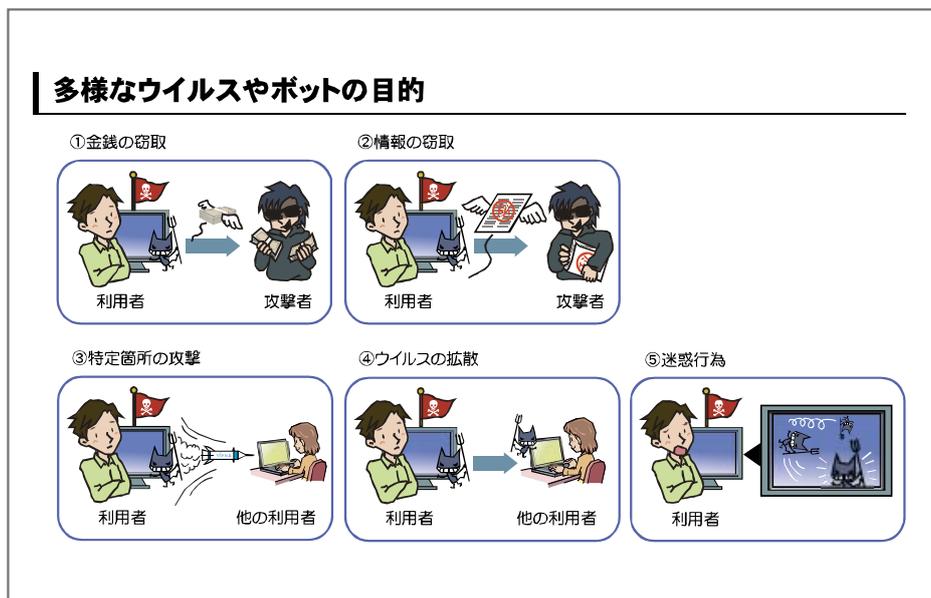
IPA: 「2009年度 情報セキュリティの脅威に対する意識調査」報告書を公開

<http://www.ipa.go.jp/security/fy21/reports/ishiki/index.html>

ZDNet Japan: ウェブユーザーの約8割が、脆弱性のあるバージョンのFlash・Acrobatを利用

<http://japan.zdnet.com/sp/feature/07zeroday/story/0,3800083088,20399036,00.htm>

### 【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ある。ウイルスには多様な目的がある。また、2009年にはウイルスの亜種が爆発的に増加した。

#### 脅威

昨今のウイルスには、「感染してしまったことに気づかせない」という特徴を持つことが多い。これは、利用者のPCを悪用するためだ。攻撃者は利用者のPCにウイルスを感染させることで、利用者のPCを様々な目的で悪用する。攻撃者の主だった目的を推測し、次に挙げる。

#### ① 金銭の窃取

攻撃者の一番の目的は、利用者からの金銭の窃取であろう。“偽セキュリティ対策ソフト”がこの目的の代表と言える。偽セキュリティ対策ソフトは、利用者に対して、「あなたのパソコンはウイルスに感染している！そのウイルスを削除したければ、有償版のセキュリティ対策ソフトを購入する必要があります」と通知し、利用者をだまして意味のないソフトを購入させたり、カード情報等を盗んだりする。攻撃者は利用者の

不安を煽ることで、金銭を窃取していく。

#### ② 情報の窃取

「金銭の窃取」に続く攻撃者の目的は、利用者のPCに保存されている情報の窃取だ。ウイルスによって、オンラインバンキングやアカウント情報等の重要な情報を盗んでいく。攻撃者はこれらの重要な情報が盗み、オンラインバンキングに登録している個人情報や盗んだアカウントを使った不正アクセス等を行う。

#### ③ 特定箇所への攻撃

金銭や情報の窃取といった攻撃者を潤わせる目的とは別に、特定箇所への攻撃を目的とするものも考えられる。ウイルスに感染した利用者のPCに一斉に命令することで、特定箇所をサービス不能状態に陥らせるDDoS攻撃やSQLインジェクション攻撃を仕掛ける。また攻撃者には、攻撃を仕掛けることができる感染PC群を悪意ある人に貸し出すレンタルサービスを運営するといった意図もある。

#### ④ ウイルスの拡散

過去のウイルスの性質から多くの PC にウイルスを感染させたいという、攻撃者の目的が読み取れる。金銭や情報の窃取、特定個所への攻撃を行うにしろ、ウイルス作成者はウイルスに感染させる PC が 1 台では不十分だと考える。その PC でセキュリティ対策をされてしまえば、攻撃者の目的は達成されない。そのため、多くの PC にウイルスを感染させる必要がある。

#### ⑤ 迷惑行為

利用者の PC にウイルスを感染させることで、利用者を困らせる、世間を騒がせるというような迷惑行為が目的となることもある。例えば、画面を真っ黒に染めて利用者を驚かせるウイルスが存在する。悪質なものになると、PC を使用不可能な状態にしてしまうウイルスや、PC に保存されている情報をインターネットに公開してしまう暴露ウイルスというウイルスも存在する。

ウイルスは、このような攻撃者の目的を達成するため、様々な経路から利用者の PC に感染

しようと試みる。

#### 2009 年の事例・統計

ウイルス対策ソフトベンダのレポートによると、ウイルスの種類は爆発的な増加をみせている。同レポートでは、2007 年には約 13 万 3 千のウイルスを確認している。これが 2009 年になると約 160 万のウイルスに及んでいる。10 倍以上の数値だ。(2008 年は約 90 万)

ウイルスが増加した背景には、簡易にウイルスを作成できるツールが存在することが言える。これらのツールでは、ウイルス対策ソフトに検知されないウイルスを作成する機能が盛り込まれていると推測される。

#### 影響

組織内部の 1 台の PC がウイルスに感染してしまうことで、いつの間にか組織内部にウイルスが蔓延し、システムが停止してしまう事態が考えられる。実際に 1 台の PC がウイルスに感染したことで、1,000 台以上の PC に感染が拡大し、業務運用に支障が出た事例がある。電力・水道のような重要インフラに該当する組織でウイルス感染が広がった場合、その影響は非常に大きいと言える。

### 第3章:対策

「3.1体制の整備・ルール作成(P28)」・「3.2安全な運用のための企画・設計(P29)」・「3.3安全な運用のための契約(P29)」

「3.5クライアントシステムへの対策(P30)」

「3.8体制・ルール・システム等の点検(P31)」・「3.9体制・ルール・システム等の見直し(P31)」

### 関連資料

G DATA Software: 1年間の新種マルウェア、史上最大数160万へ

<http://gdata.co.jp/press/archives/2010/02/1160.htm>

IPA: コンピュータウイルス・不正アクセスの届出状況[12月分および2009年年間]について

<http://www.ipa.go.jp/security/txt/2010/01outline.html>

## 【4位】対策をしていないサーバ製品の脆弱性



サーバ製品(ウェブアプリケーションやミドルウェア等)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る。

### 脅威

ウェブサーバやウェブアプリケーションに代表されるサーバ製品に脆弱性があると、攻撃者にその脆弱性を悪用される恐れがある。過去の例では、2003年頃のウイルス(ワーム)蔓延は、サーバ製品の脆弱性が悪用されることで引き起こされた。2009年はSQLインジェクション等によるウェブサイト改ざんが度々報道された。現在もサーバ製品には、適切な脆弱性対策を行う必要がある。

サーバ製品のなかでも、特にウェブサイトのように外部に対して公開する運用の場合、注意が必要である。

ウェブサイトは、ウェブサーバ、動的なコンテンツ(ユーザや入力値に基づいてサイトを構成するコンテンツ)を提供するウェブアプリケーション、ミドルウェア(Perl, PHP 等)で構成される。ウェブサイトを運用している場合、これら全てのソフトウェアに対する脆弱性を考慮しなければならない。

サーバ製品の脆弱性対策が重要であるが、開発者が脆弱性を修正したサーバ製品を公開しても、アップデートされていないサーバ製品が散見される。サーバ製品をアップデートしない理由は大きく2つ考えられる。

- ① 特定のサービスが動作しなくなる可能性を恐れてアップデートできない
- ② サーバ製品のアップデートの必要性を理解していない

脆弱性を放置することで生じるリスクを理解し、脆弱性を修正する以外の回避策を講じている場合は問題ない。回避策は、例えば「脆弱性を悪用した攻撃を防御するためにIPS(Intrusion Prevention System)を導入している」等が挙げられる。回避策を講じていれば、リスクが顕在化することが軽減できる。サーバ製品の管理者は、このことを理解した上で、脆弱性を修正する、または回避策を講じる等の適切な脆弱性対策を行うことが重要だ。

### 2009年の事例・統計

2009年にIPAから、届出件数の多かった複数の製品を使用するウェブサイト運営者に対して、「古いバージョンを使用しているサイトへの注意喚起」を発信した。この注意喚起から、脆弱性対策をきちんと実施できていないサーバ製品が多いことが分かる。「ウェブサイトで利用されているDNSサーバの既知の脆弱性への注意喚起」を発した時点で、DNSキャッシュポイズニング対策を実施していないウェブサイトの届出を1,307件受理していた。

また、「EC-CUBEの古いバージョンを利用しているウェブサイトへの注意喚起」を発した時

点で、IPAは「EC-CUBE」の既知の脆弱性が修正されていないウェブサイトの届出を49件受理していた。「EC-CUBE」に関する届出は、当該製品のクロスサイト・スクリプティングの脆弱性に関するものであった。だが、当該製品にはSQLインジェクションの脆弱性も発見されており、早い脆弱性対策が望まれる。

このように脆弱性が修正されていないサーバ製品が存在している事実が浮かび上がった。

### 影響

サーバ製品の脆弱性を悪用されることで、不特定多数の利用者が被害を受ける可能性がある。サーバ製品に保存されている情報が改ざんされる等の恐れがある。結果、サーバ製品の利用者の情報窃取や利用者へのウイルス感染といった被害が生じる。

サーバ製品の脆弱性が悪用された場合、被害を受けるのはサーバ製品だけではなく、その製品の利用者にも及ぶ。これは、ランブラーによる被害からも分かる。

サーバ製品の管理者は、被害が利用者にも及ぶことを十分に認識して、サーバ製品の適切な脆弱性対策を行わなければならない。

## 第3章：対策

「3.1体制の整備・ルール作成(P28)」・「3.2安全な運用のための企画・設計(P29)」・「3.3安全な運用のための契約(P29)」

「3.4サーバシステムへの対策(P30)」

「3.8体制・ルール・システム等の点検(P31)」・「3.9体制・ルール・システム等の見直し(P31)」

## 関連資料

IPA: 「EC-CUBE」の古いバージョンを利用しているウェブサイトへの注意喚起

[http://www.ipa.go.jp/security/vuln/documents/2009/200907\\_ec-cube.html](http://www.ipa.go.jp/security/vuln/documents/2009/200907_ec-cube.html)

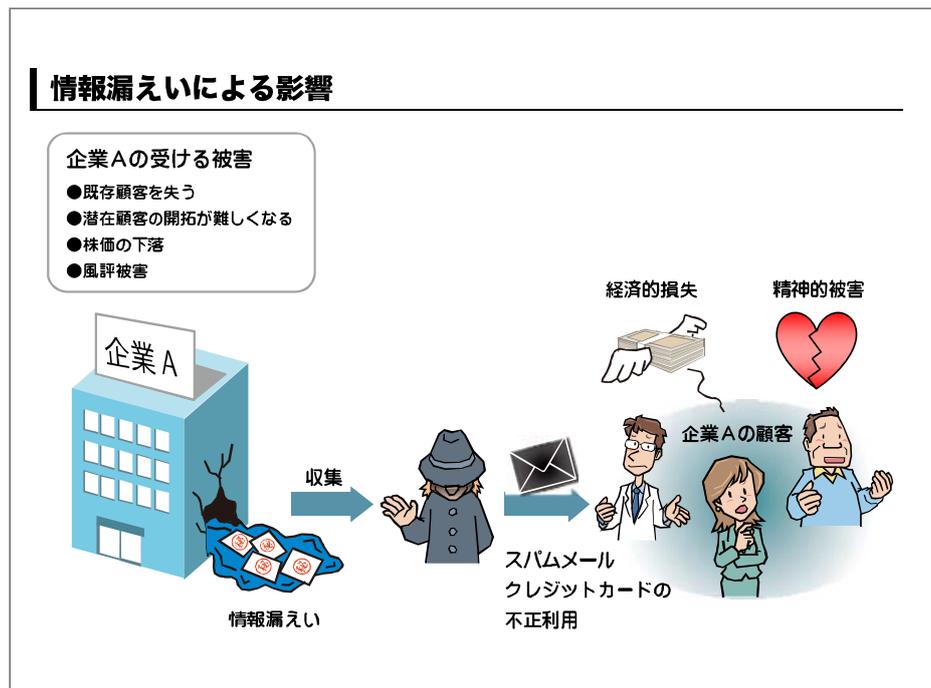
IPA: 「OpenSSL」の古いバージョンを利用しているウェブサイトへの注意喚起

[http://www.ipa.go.jp/security/vuln/documents/2009/200909\\_openssl.html](http://www.ipa.go.jp/security/vuln/documents/2009/200909_openssl.html)

ITMedia: WordPressの旧版を狙うワーム出現、最新版に更新を

<http://www.itmedia.co.jp/enterprise/articles/0909/08/news027.html>

## 【5位】あわせて事後対応を！情報漏えい事故



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

### 脅威

情報漏えいの原因には、例えば SQL インジェクション攻撃、ウイルス感染、第1章1.2のような内部犯罪、メールの誤送信や記憶媒体の紛失等の内部の人間による過失等が挙げられる。過失による漏えいは、情報漏えいの原因の中で最も多いものである。過失によって発生する情報漏えいは、例えばメールの誤送信や記憶媒体の紛失については、メール配送前の確認ルールや、記憶媒体の持ち出しルールといった、技術・運用面で対策を行っていたとしても、情報漏えい事故がルール違反等によって生じている場合も含めると、技術・運用面だけで完全に対策することは難しい。

そのため、重要な情報をメールで配送する場合は送信前に上長の承認(送信先、内容確認)を必須化したり、持ち出される記憶媒体を暗号化できる製品に制限し、記憶媒体の暗号

化を必須化する等の、二次予防策を用意することが有効である。

また、上述のような情報漏えい事故は、社員・職員の情報セキュリティに対する意識低下にも起因するため、定期的な情報セキュリティ教育活動を行い、セキュリティ意識の向上を図ることも有効である。

### 2009年の事例・統計

2009年に限らないが、内部から発生する事件が多い。あるISPの調査によると、2008年6月から2009年5月の期間内における情報漏えい事故は1,583件あった。このうちの18.3%の291件が紛失や盗難によるものだ。この紛失や盗難の対象は、ノートパソコンやUSB等の外部記憶媒体であった。

当該調査では、組織内からの持ち出しは禁止というルールを作成しても、締め切りに追われている等の事情によって「持ち出さざるをえない背景がある」と分析している。

調査結果が示すように、ルールを作成してい

てもそれが実情に則していなければ有名無実化してしまう恐れがある。したがって、ルールは業務と照らし合わせて適用可能かを事前に検討しておく必要がある。

他にも、業務委託先業者が、個人情報を持ち出すという事件があった。このような被害への対策は、自組織だけでなく、委託先も考慮に入れる必要がある。システムの構築やテスト等を「全て委託先任せ」にしてしまうことで、委託先が情報漏えいを起こすケースもあるためだ。どのような契約に基づいて情報をやり取りするのかが明確にしておかなければならない。

### 影響

企業が保存している個人情報で、漏えいしてはならない情報は大きく分けて2種類考えられる(関連資料:BPnet)。まずは、クレジットカードのカード番号や暗証番号等のような、「経済的損失」を伴う情報である。経済的損失が発生するような個人情報は、悪用されることが想定される。

もう一つは、健康診断結果や病歴のような、誰かに見られてしまうことで、「精神的な苦痛」を伴う情報である。また、これら2つの情報を兼ねた情報もある。例えば、資産や残高、所得等

は、漏えいすることで「経済的損失」と「精神的な苦痛」の双方を伴う。精神的苦痛を伴う個人情報も、漏えいそのものが問題であり、悪人がいなくても問題になる。

利用者にとっては、情報漏えいしたことによって、経済的損失と精神的な苦痛による被害がある。この利用者の被害は、結果的に組織の損害という影響に発展する。

まず、直接被害を受けた利用者に対して契約違反になり、訴訟等での損失に発展する可能性がある。そして、直接被害を受けた利用者(既存の顧客)を失ってしまうという損害に発展する。これは、利用者が受けた被害によって組織への信頼が失われてしまった結果によるものだ。次に、一般に報道されることで、ステークホルダからの信頼を失ってしまう結果によるものがある。

また、事故が発生した後の事後対応も重要だ。情報漏えいを起こしてしまった後、素早く適切な対応を取ることによって、適切にセキュリティ対策を行っている組織としてブランドイメージを高め、逆に信頼を上げるケースもある。このような対応を組織としては目指したい。

### 第3章:対策

「3.1体制の整備・ルールの作成(P28)」・「3.2安全な運用のための企画・設計(P29)」・「3.3安全な運用のための契約(P29)」  
「3.8体制・ルール・システム等の点検(P31)」・「3.9体制・ルール・システム等の見直し(P31)」

### 関連資料

BPnet: 社員情報の収集はどこまで許されるか (2)～社員情報はセンシティブ情報の塊～

<http://www.nikkeibp.co.jp/sj/2/column/c/19/index.html>

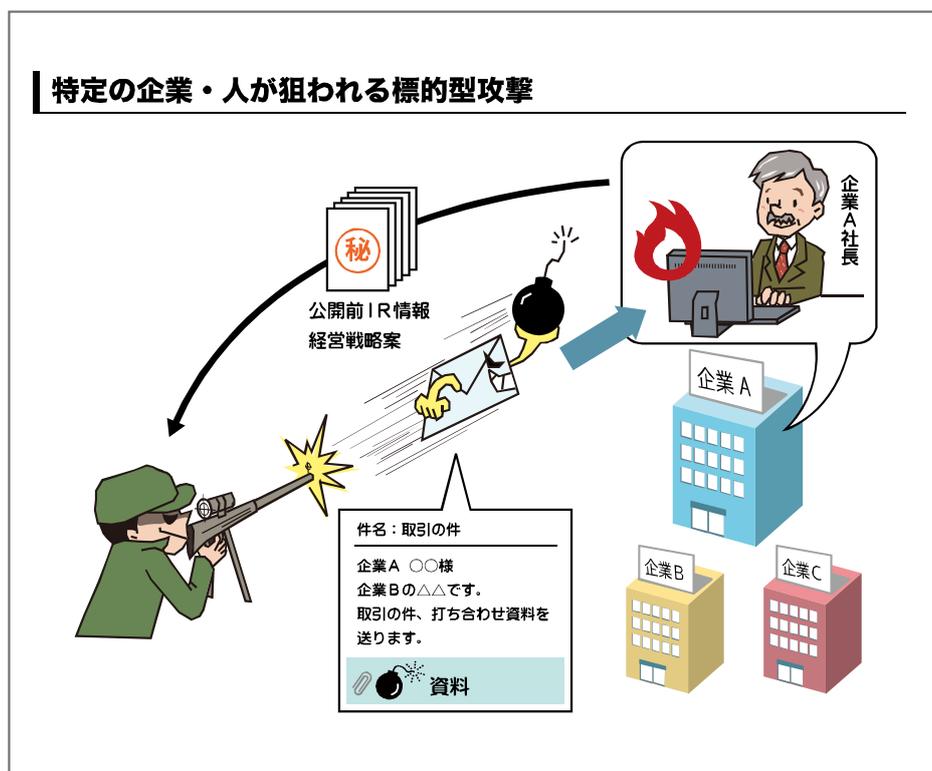
So-net: PC、USBメモリ、携帯電話紛失！～恐怖の「情報流出」を防ぐには

[http://www.so-net.ne.jp/security/news/newsttopics\\_200907.html](http://www.so-net.ne.jp/security/news/newsttopics_200907.html)

SecurityNext: 個人情報漏洩事件一覧

[http://www.security-next.com/cat\\_cat25.html](http://www.security-next.com/cat_cat25.html)

## 【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、ウイルスを送りつける手口を標的型攻撃という。

### 脅威

標的型攻撃は2005年頃より問題視されるようになった。当時US-CERTやJPCERT/CCから発表されたウイルスによる被害<sup>1</sup>が該当する。その後、このように限定的に攻撃される手口が存在することが広まり、研究されるようになった。

知人や取引先からのメールを閲覧することは自然なことだ。文面に怪しい要素がなければ、ウイルスが添付されているようなことがあるとは考えないだろう。ただし、それは本当に相手が知人であり、本当に取引先企業である場合だ。標的型攻撃の特徴には、添付されているウイルスが通常使用するファイルと見分けがつかないことが挙げられる。このウイルスはソフトウェア

の脆弱性を悪用していることが多い。そのため、通常のファイルと見分けがつかない形で送付されている。また、ファイルを開いた後にも何らかの文書が表示されるため、添付されているファイルがウイルスであると気がつかない。このように標的型攻撃は、攻撃にあったかどうか分からないような仕組みを幾重にも取り込んでいる。

ソフトウェアの脆弱性を悪用したウイルスは、ソフトウェアを適切にアップデートすることで防げる。しかし、中にはまだベンダが修正していない脆弱性を悪用する、いわゆるゼロデイ攻撃を行う場合があるところが更に恐ろしいところだ。

標的型攻撃に狙われる対象は、企業の経営層等の重要な情報を持っているような人物であるケースがあり、経営に関わる機微な情報を盗まれてしまうリスクが考えられる。

標的型攻撃は限定的に行われ、攻撃であるかどうかの判別も難しい。このような攻撃に対し

<sup>1</sup> <http://www.jpccert.or.jp/wr/2005/wr052701.txt>

ても他の対策と同様に、まずは基本的な対策であるソフトウェアのアップデートを行っておきたい。また、自分が攻撃を受けたと判明した場合は、セキュリティ関連の事業者等に相談して、他の人が攻撃を受けないように情報共有することが重要である。

### 2009年の事例・統計

2009年にJPCERT/CCより、「ITセキュリティ予防接種調査報告書」が公表された。これは、標的型攻撃を疑似的に体験するもので、幅広い業種を対象に約2,600人の被験者に行った調査結果である。この調査では、標的型攻撃を模したメールを被験者へ送付している。

調査結果では、年齢、性別、職種等の属性に関係なく、標的型攻撃の被害にあう恐れがあることが示された。しかしながら、1回目の全体のメールの開封率が45.4%だったのに対して、2回目の14.0%と減少傾向がみられる。これは標的型攻撃を体験的に学習したことによる効果であると考えられる。

また、セキュリティベンダのレポートによると、観測した標的型攻撃は2009年1月から5月までに663件あった。この内、Adobe社の提供するAdobe Reader/Acrobatの脆弱性を狙ったウイルスが添付されていることが、前年の比率と

比べると多くなっていると述べている。Adobe Reader/Acrobatの脆弱性以外には、マイクロソフト社のWord, Excel, PowerPointの脆弱性が狙われている。2008年(1,968件)と対比すると、マイクロソフト社の製品が約72%から約51%まで減少しているのに対し、Adobe社の製品は約29%から約49%まで上昇している。これに対して同レポートでは、Adobe社の製品に対する脆弱性が見つかりやすいためであるとしている。

### 影響

標的型攻撃は、企業の経営層等の重要な情報を持っている人をターゲットにした攻撃の事例が報告されている。企業の経営層が所有している情報は、より重要であることが想定される。そのため、企業の戦略情報や経営企画案のような情報が漏えいしてしまうことで、企業の事業継続において深刻な影響を与える可能性もある。もちろん、これは企業の経営層だけに限らず、機密情報を保持またはアクセス可能な全ての社員に言えることである。したがって、企業の関係者が常に注意して行動できるように、日頃から情報セキュリティの教育・研修を継続的に実施することが重要である。したがって、企業の全ての人が注意しておかなければならない脅威である。

### 第3章:対策

- 「3.1体制の整備・ルール作成(P28)」・「3.2安全な運用のための企画・設計(P29)」・「3.3安全な運用のための契約(P29)」
- 「3.5クライアントシステムへの対策(P30)」
- 「3.8体制・ルール・システム等の点検(P31)」・「3.9体制・ルール・システム等の見直し(P31)」

### 関連資料

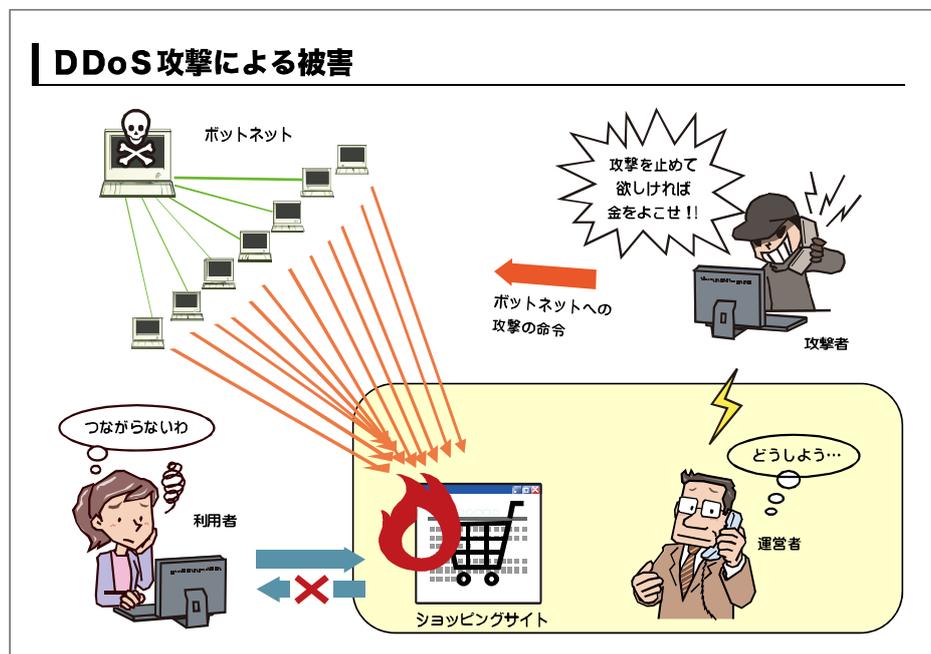
JPCERT/CC: ITセキュリティ予防接種調査報告書

<http://www.jpccert.or.jp/research/index.html#inoculation>

ITPro: 2009年は「PDFウイルス」を使う標的型攻撃が最多、およそ半数に

<http://itpro.nikkeibp.co.jp/article/NEWS/20090507/329641/>

## 【7位】深刻なDDoS攻撃



DDoS(Distributed Denial of Service)攻撃は、DoS 攻撃(サーバやルータ等の機能を麻痺状態にさせる攻撃)の一種である。

### 脅威

DoS 攻撃は、主に2つの種類に分けられる。

- ① サーバやルータの脆弱性を突いて引き起こす攻撃
- ② サーバやネットワーク回線における性能の限界を超えた大量のリクエストを送付する攻撃

DDoS 攻撃は、「分散型サービス運用妨害攻撃」とも呼び、主に②の手法を使用する。そして、DDoS 攻撃では、該当するサーバへの攻撃が分散された大量のコンピュータから行われる。

②の攻撃には、HTTP リクエストを大量に送付する方法等が挙げられる。また、攻撃にはさほど難しくないものもある。特にHTTPリクエストを大量に送付する攻撃は、サーバに対してアクセスを集中させるだけで行える。

1 箇所からの DoS 攻撃の場合、その箇所から

のアクセスを遮断することで対処が可能だ。しかし、DDoS 攻撃のように大量のコンピュータから攻撃された場合、サービスを提供しつつ、アクセス制御による対処を行うことは難しい。

HTTPリクエストを送付する攻撃は、さほど難しくない攻撃である。そのため、もし組織に恨みがあるような人間が多くの人に呼び掛けて賛同者が多く出しまえば、それだけで攻撃が発生する可能性がある。これは、多くの人が一斉にアクセスすると変わらない現象である。更に、それらの人に攻撃用のツールを配布すれば簡易に攻撃が可能となり、被害が拡大してしまう。

DDoS 攻撃を行う目的は大きく3つある。

- (1) 国家の重要なシステムをサービス不能状態にさせ、社会を混乱させるもの
- (2) サービス運営者への恨みによるもの
- (3) DDoS 攻撃の解消を売り物にするための詐欺や脅迫を目的とするもの

(3)の目的では、攻撃者はボット等を使用してDDoS 攻撃を仕掛け、サービス運用妨害状態

にする。攻撃者はそこにサービス業者を装って金銭を取ろうとする。

他にもボットによって攻撃が行われる場合もある。ボットは、世界中に点在するのが現状である。そのため、攻撃者は多くの DDoS 攻撃拠点を持っていると言える。

### 2009 年の事例・統計

2009 年の 7 月に米国の政府機関のウェブサイト、韓国の公的機関、民間企業等が DDoS 攻撃を受けたというニュースが流れた。この攻撃では、ボットに感染した PC が攻撃に悪用された。この攻撃に悪用されたボットの感染台数は、世界中に 13 万台以上にも上っていた。

この攻撃に悪用されたボットの感染は、利用者にとって防ぎにくいものだった。感染はあるウェブサービスを改ざんされたことに端を発している。この改ざんにより、ウェブサービスで提供しているアップデートプログラムをボットにさしてしまった。アップデートプログラム自身は当該ウェブサイトより提供されているものであるため、利用者は疑いなく実行するため感染した。

また、この攻撃において各ボットの役割が分担されていたということが特徴として挙げられる。

これは、一つのボットを解析しても攻撃の全体像がつかめないことを意味する。また、一つのボットからの攻撃の通信も通常の通信と変わらないものであった。そのため、これが攻撃であるのか、それとも通常の通信であるのかも判別しづらいものであった。

また、国内においては、ASP(Application Service Provider)事業者のレンタルサーバに対して攻撃が行われた事例がある。なお、当該事業者は攻撃を受けた後、詳細な対応方法を説明した障害報告を発表している。このような事後対応は、利用者との信頼関係を損なわないために重要な対応である。

### 影響

稼働しておかなければ事業継続に関わってしまうようなシステムへ DDoS 攻撃を受けた場合、インパクトが大きい。金融機関やショッピングサイト等において、取引機会を損失することによる経済損失等が考えられる。

また、前述した DNS サーバに対する DDoS のように、自社管轄外のネットワーク資源が攻撃された場合であっても、利用している場合はサービスが提供できなくなる場合がある。

## 第3章:対策

「3.1体制の整備・ルール作成(P28)」・「3.2安全な運用のための企画・設計(P29)」・「3.3安全な運用のための契約(P29)」  
「3.8体制・ルール・システム等の点検(P31)」・「3.9体制・ルール・システム等の見直し(P31)」

## 関連資料

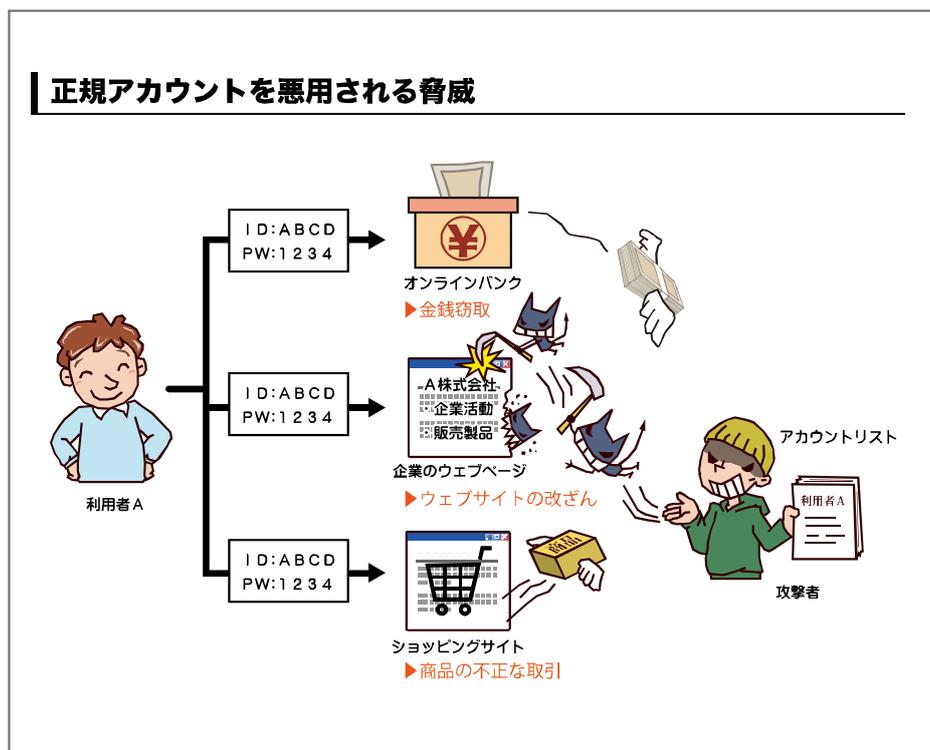
Impress: 米・韓サイトのDDoS攻撃に用いられたボット感染PC、日本にも存在

[http://internet.watch.impress.co.jp/docs/news/20090710\\_301397.html](http://internet.watch.impress.co.jp/docs/news/20090710_301397.html)

ZDNet Japan: DDoS攻撃の価格は1時間あたり1300円～2万円--G Data、地下経済を調査

<http://japan.zdnet.com/news/sec/story/0,2000056194,20402570,00.htm>

## 【8位】 正規のアカウントを悪用される脅威



オンラインバンキング等のインターネットサービスや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)がアカウントである。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る。

### 脅威

アカウント情報の中でもパスワードは、本来自分しか知らない情報であり、他人に知られないようにしなければならない。パスワードを他人に知られてしまうと、他人が自分になりすましてシステムを操作することが可能になる。

アカウント情報を悪用されることによる被害には、次のようなものがある。

- 管理するウェブサイトを改ざんされる。
- オンラインバンキングやネットショッピングで、不正に取引が行われる。
- SNS(Social Network Service)等のサービスにおいて、友人になりすまして詐欺行為が行われる。

このような正規のアカウントを悪用される要因としては次のようなものが挙げられる。

- 安易なパスワードを利用している：  
「abcde」や「password」、「ユーザ ID と同じ文字」のような安易なパスワードを利用している事例が多いというレポートがある。安易なパスワードの使用により、簡単に暴かれてしまいアカウント情報を悪用される可能性がある。
- アカウント(ID・パスワード)を使いまわしている：  
複数のインターネットサービスで同じアカウントを使用していると、一つのインターネットサービスでアカウント情報が漏えいしてしまえば、他のインターネットサービスで悪用されてしまう危険性がある。
- パスワードを机の上等の安易な場所に表示させている：  
重要なシステムのユーザ ID とパスワー

ドは、それを操作する必要のある人間だけが知っておくべき情報である。机の上に誰でも分かるようにメモを置いている、PC のデスクトップ上にパスワードを表示させている等の要因がある。

- 不要なアカウントを残したままである：  
退職者のアカウント等、既に不要になったアカウントを残してしまっている場合がある。退職者等のアカウント情報を悪用して、内部システムにアクセスされるような事態がある。

### 2009 年の事例・統計

2009 年に、正規のアカウントを悪用した事件で最も目立ったものはガンブラーによるウェブサイトの改ざんだ。また、過去に、複数のウェブサービス上でアカウントを使いまわしているため、ウェブサービスの個人の情報を書き換えられる、不正な取引に悪用されるといったニュースが散見された。2009 年に発表されたセキュリティベンダの調査によると、利用者の 3 割はパスワードを使いまわしているという。

アカウントの悪用は日本だけに限らず、海外でも起こっており、SNS のアカウントを盗み、そのアカウントの友人に対して詐欺行為を行うと

いう手口があった。

また、国内においては、退職者のアカウントを残してしまったがために、恨みのある退職者にウェブサイトが改ざんされたというニュースがあった。これは、アカウントの運用を見逃しがちになるということに起因している。

### 影響

正規のアカウントを悪用されることは、そのシステムを不正に操作される、情報を窃取される等の被害を受ける可能性がある。正規のアカウントを悪用されてしまうと、システムではそれが悪用であるのか、正規の利用であるのか判断できない。したがって被害にあった場合、気づくのが遅れてしまう。

現状の ID とパスワードでの認証では、利用者や管理者が複数のサービスやシステムでそれぞれのアカウントを持つ必要がある。しかし、全てのアカウント情報を覚えきれないという事情がある。ID とパスワード以外の認証方法として、生体情報やワンタイムパスワードを利用するものもある。ハードウェアの導入の際には生体情報等の第二認証を考慮に入れるのも一つの手段である。

### 第3章:対策

- 「3.1体制の整備・ルールの作成(P28)」・「3.2安全な運用のための企画・設計(P29)」・「3.3安全な運用のための契約(P29)」
- 「3.6アカウント情報の管理・運用(P30)」
- 「3.8体制・ルール・システム等の点検(P31)」・「3.9体制・ルール・システム等の見直し(P31)」

### 関連資料

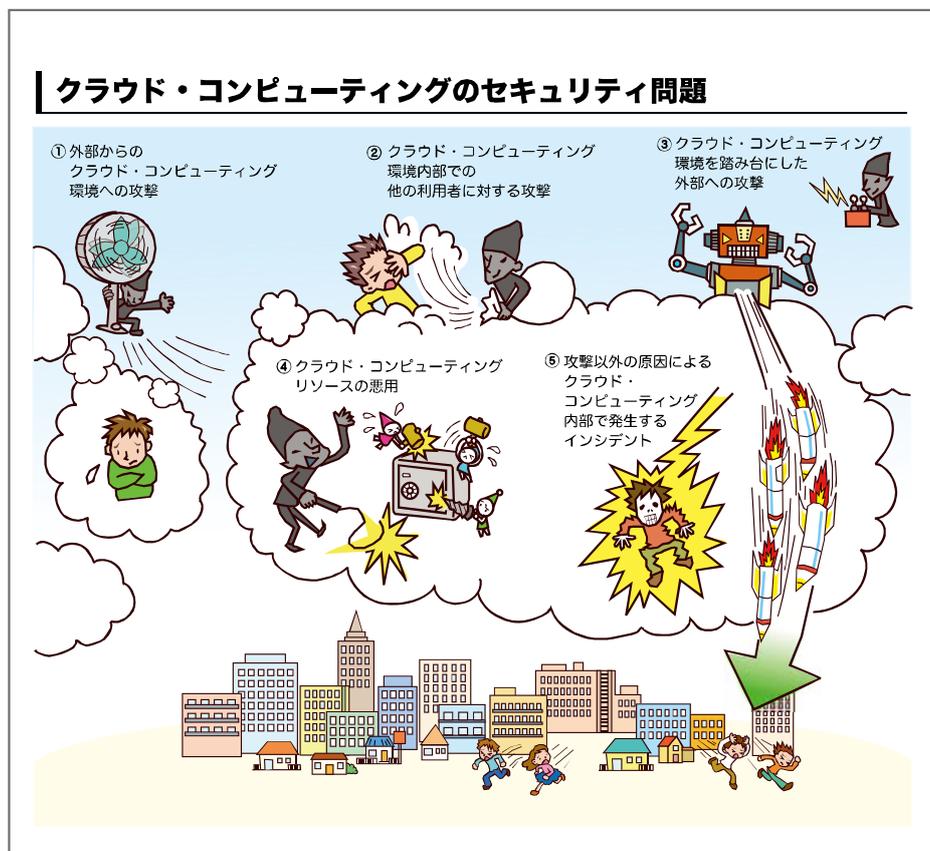
ITMedia: ネット利用者の3割はパスワードを使い回し——Sophos調査

<http://www.itmedia.co.jp/enterprise/articles/0903/12/news028.html>

ITMedia: 最も安易なパスワードは？ 流出情報の分析結果を発表

<http://www.itmedia.co.jp/news/articles/1001/22/news025.html>

## 【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る。

### 脅威

米国の国立標準技術研究所(NIST)では、クラウドを「最小限の管理労力で迅速に利用開始あるいは利用解除できる構成変更可能なコンピュータからなる、共有資源に対して簡便かつ要求に即応できるネットワークアクセスを可能にするモデル」と定義している。クラウドで提供するサービスは、次の3つがある。

- a. SaaS(Software as a Service):電子メール、グループウェア等のソフトウェアのサービス
- b. PaaS(Platform as a Service):仮想化されたアプリケーションサーバやデータベース等

- c. IaaS(Infrastructure as a Service):仮想化サーバや共有ディスク等
- クラウドには、次のようなセキュリティの問題点が指摘されている。

- ① 外部からクラウド環境への攻撃:  
クラウド環境自身が攻撃対象となる。従来のように自社でサーバを用意してサービスを提供している場合と異なり、データがクラウド環境上で一極集中している。そのため、攻撃が成功した際の影響が大きくなる可能性がある。
- ② クラウド環境内部での他の利用者に対する攻撃:  
クラウド環境では他の利用者と利用環境を共有する。同じクラウド環境に攻撃者がいる可能性がある。この環境を悪用され、攻撃者がクラウド環境を攻撃すること

で、他のクラウド利用者が攻撃を受けると  
いう事態が想定される。例えば、仮想化技  
術の脆弱性等を悪用されて、クラウド環境  
を通して攻撃されることが想定される。

③ クラウド環境を踏み台にした外部への攻  
撃

クラウド環境を攻撃の道具として悪用さ  
れる懸念がある。第三者に対して DoS そ  
の他の攻撃が仕掛けられる可能性がある。  
また、攻撃者が善意のクラウド利用者の環  
境にマルウェアを埋め込む等、クラウド外  
のシステム等に攻撃が仕掛けられることも  
考えられる。

④ クラウドのリソースの悪用

クラウド環境が攻撃のためのリソースと  
して悪用され、暗号解析やパスワード解析  
に利用される懸念がある。クラウド事業者  
側は、この利用方法が正規の利用か不正  
利用かを見分けづらく、検知や防止が困  
難である。

⑤ 攻撃以外の原因によりクラウド内部で発生  
するインシデント

クラウド環境は、データセンター等での  
停電や、ソフトウェアやハードウェアの不  
具合によってサービスが停止し、クラウドの  
利用者がサービスを利用できなくなる懸

念がある。

2009 年の事例・統計

2009 年に、既にクラウドに関連する事件、事  
故が発生している。

海外で展開している大手のクラウド・コンピ  
ューティング・サービスでは、外部から DDoS 攻撃  
に遭った①のような事例がある。この事例では、  
サービスの利用者が「トラブルが発生している  
のではないかと」、クラウド事業者にお問い合わせ  
を行っても、クラウド事業者でも攻撃を検知でき  
ていなかったため、復旧に時間を要してしまっ  
た。これは、攻撃や事故等への対応がクラウド  
事業者側へ依存してしまっている例と言える。

影響

従来のように自社でサーバを用意してサービ  
スを提供している場合、サービスにインシデント  
が発生した際や、脆弱性の存在が判明した際、  
自社で障害の対応や原因の特定が可能である。

一方、クラウド環境においては、クラウド事業  
者が対応する場合も想定される。仮にクラウド  
事業者の脆弱性やインシデントに対する認識  
が不足している場合、クラウドの利用者に十分  
な情報提供が行われず、結果として問題の解  
決に適切な対処が行えないといった事態が想  
定される。

第3章:対策

「3.1体制の整備・ルール作成(P28)」・「3.2安全な運用のための企画・設計(P29)」・「3.3安全な運用のための契約(P29)」  
「3.8体制・ルール・システム等の点検(P31)」・「3.9体制・ルール・システム等の見直し(P31)」

関連資料

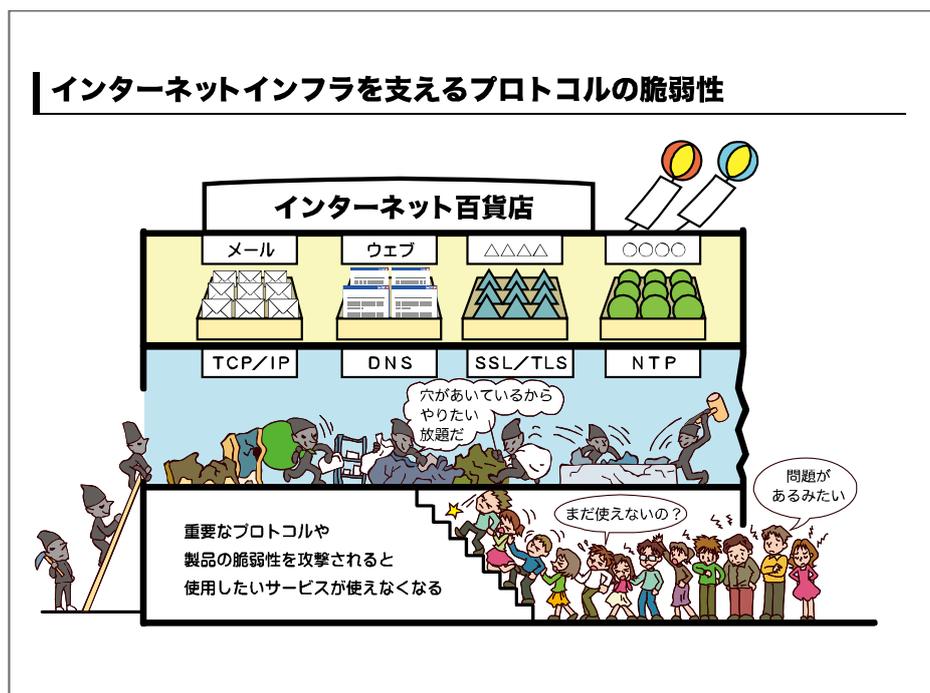
Impress: セキュリティにクラウドの闇、Amazon EC2悪用の総当たり攻撃も

[http://internet.watch.impress.co.jp/docs/news/20091208\\_334134.html](http://internet.watch.impress.co.jp/docs/news/20091208_334134.html)

ITPro: 「攻撃元は『ボットネット』から『クラウド』へ」、ラックが警告

<http://itpro.nikkeibp.co.jp/article/NEWS/20091209/341795/>

## 【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にインターネット接続するための機能が備えられている。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る。

### 脅威

インターネットインフラを支えるための技術や製品には、情報の伝達のためにネットワーク同士を接続するためのプロトコルであるIP(Internet Protocol)や、IP アドレスとドメイン名を結びつけるためのDNS(Domain Name System)等がある。他にも、WWW(World Wide Web)を実現するHTTP やメールを実現するためのSMTP(Simple Mail Transfer Protocol)、POP3 (Post Office Protocol)、ネットワークに接続されている機器の示す時刻を正しい時刻へ同期するためのNTP(Network Time Protocol)等がある。また、通信の経路を伝達するルーティング技術、通信を暗号化するSSL/TLS(Secure Sockets Layer/Transport Layer Security)等はインターネット上で幅広く

使用されている。

これらを実現するプロトコルやプロトコルを実装している製品における脆弱性のリスクは深刻である。仮に、その脆弱性を攻撃されてしまえば、インターネットに重大な影響がある。例えば、DNSのプロトコルにDoSの脆弱性が存在する場合、その脆弱性に対する攻撃が世界中で行われることで、最悪インターネットが麻痺してしまうような事態まで考えられる。また、通信を暗号化するプロトコルに脆弱性が存在することで、暗号を解読される恐れがあり、暗号通信の信頼性が揺らいでしまう。これにより、安心したインターネットの利用が妨げられてしまう。

このような重要なシステムは、動作し続けることが重要視されるため、アップデートをしづらいという事情がある。そのため、定期的なアップデートの計画や、可能であれば回避策の準備等を行っておく必要がある。

### 2009年の事例・統計

2009年に公開されたソフトウェア製品の脆弱

性のうち、インターネットインフラを支える製品に関わるような脆弱性も幾つか存在する。ここでは、特に注目した四つの問題を次に挙げる。(関連資料参照)

まずは、ISC(Internet Systems Consortium)が提供する DNS サーバソフトウェアである BIND(Berkeley Internet Name Domain)におけるサービス運用妨害(DoS)の脆弱性だ。これは、特殊なパケットを BIND が受信することで、BIND が停止状態になってしまう問題である。

次は、TCP/IP におけるサービス運用妨害(DoS)の脆弱性だ。この問題は、特殊なパケットを送付されることでシステムが通信を受け付けなくなる状態にされる。2009 年になり、各ベンダで本問題への対応がなされてきた。

3 つ目は、SSL/TLS の脆弱性で、攻撃者に通信を仲介される攻撃(第三者中継による攻撃)を防止できないという問題があった。これは、プロトコルそのものの脆弱性で、当該プロトコルを使用している製品全てに影響がある。2010 年にそのプロトコルの技術仕様である RFC が改

訂されている。

4 つ目は NTP の脆弱性だ。NTP には複数の脆弱性が公開され、修正されている。これは、特殊なパケットを受信することでサービス運用妨害(DoS)状態になるものと、システムを乗っ取られる危険性のあるバッファオーバーフローの脆弱性があった。

### 影響

本脅威の影響を受けるのは、インターネットを利用する全ての人々である。そのため、特にインターネットに接続するための機器の開発者にとっては、この問題による影響は大きい。

開発者はこのような脆弱性が発見された場合、修正しなければならない。場合によっては、プロトコルからの修正も必要になる場合もある。

機器の利用者では、ISP(Internet Service Provider)事業者やホスティングサービスを手掛けている事業者等、機器を多数扱っている事業者が深刻だ。これらの事業者は、サービスを受けている顧客、関係者等に影響を及ぼす可能性があり、問題となる。

## 第3章:対策

「3.1体制の整備・ルールの作成(P28)」・「3.2安全な運用のための企画・設計(P29)」・「3.3安全な運用のための契約(P29)」

「3.4サーバシステムへの対策(P30)」

「3.8体制・ルール・システム等の点検(P31)」・「3.9体制・ルール・システム等の見直し(P31)」

## 関連資料

JVN: ISC BIND 9 におけるサービス運用妨害 (DoS) の脆弱性

<http://jvn.jp/cert/JVNVU725188/>

JVN: 複数の SSL VPN (Web VPN) 製品においてウェブブラウザのセキュリティが迂回される問題

<http://jvn.jp/cert/JVNVU261869/>

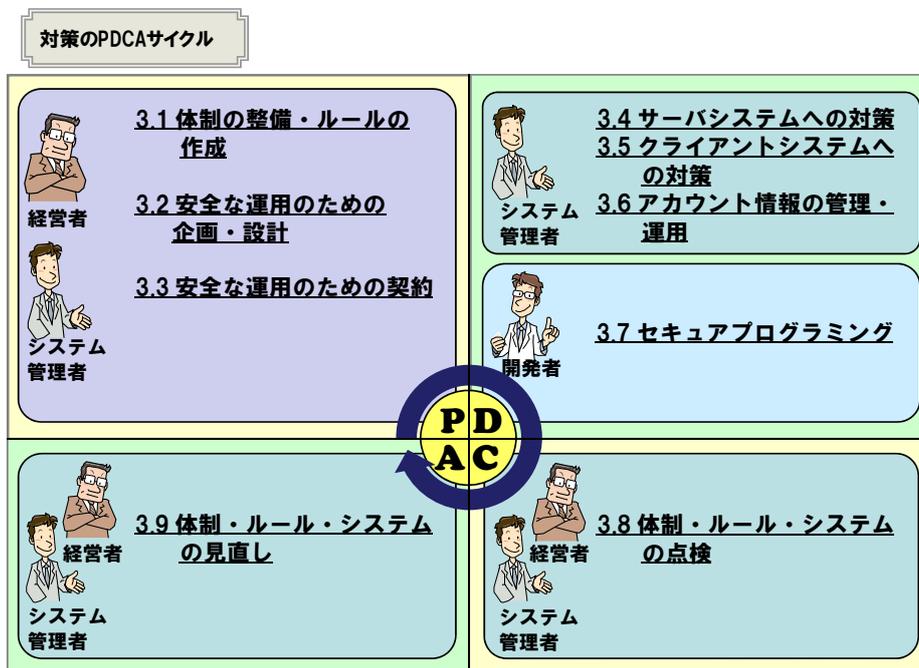
JVN: NTP におけるサービス運用妨害 (DoS) の脆弱性

<http://jvn.jp/cert/JVNVU568372/>

JPCERT/CC:複数製品の TCP プロトコルの脆弱性に関する注意喚起

<http://www.jpCERT.or.jp/at/2009/at090019.txt>

## 第3章 対策



セキュリティ対策は、経営課題として組織に組み込まれることが当たり前になっている。

本章では、主に第2章で取り上げた脅威への対策を記載している。セキュリティ対策は、様々な書籍等で紹介されており、組織に対して必要かつ十分なセキュリティレベルを確保するためには、これらの書籍等を参考にして取り組む必要がある。

本章は、上図のようにPDCAサイクルと関係者を位置づけている。関係者は、それぞれのサイクルで対策を実施する必要がある。

### 3.1 体制の整備・ルールの作成

[担当:経営者・システム管理者]

経営者が組織のセキュリティ対策として最初に行うべき点は、組織内にセキュリティマネジメントのサイクルを確立させることである。セキュリティマネジメントサイクルを確立することにより、組織のセキュリティレベルの維持・向上に関わる指針を示す。次に、事業継続に影響する事件、事故が発生した場合に必要な緊急時対応

計画や事業継続計画を整備することである。例えば、事業継続計画は、セキュリティ事件・事故等の際に中核となる事業や早期復旧を可能とするため、どの様に対応するべきかを決めた計画である。また、整備した事業継続計画に基づき、組織内で教育、訓練を行い、事業継続をマネジメントすることで、重要な事業を継続することが可能となる。

本節では、「事前対策」と「事後対応」に分けて記載している。事前対策や事後対応は、経営者が作成を指示し、その指示に基づいてシステム管理者がルールや体制の案を作成する。経営者はその案の妥当性を判断し、実施の宣言を行う。

#### <事前対策>

組織にセキュリティマネジメントサイクルを確立するには、まず、組織内に情報セキュリティ対策を推進する体制を確立し、組織のセキュリティ対策の目的、原則を定める(基本方針)。この基本方針には、3.2と3.3の対策も含まれる。

その後、組織内で守るべき情報資産を特定し、これに対してどのようなリスクがあるか分析を行い、具体的な対策事項を立案する(対策基準)。対策事項について、具体的な実施手順(マニュアル)を策定し、経営者が責任を持って組織内に周知を行い遵守させることが必要である。

事業継続計画を整備する際には、まず組織の事業継続において重要な情報や、重要なシステムを洗い出さなければならない。次に、洗い出した情報の関係者は誰か、関係者はどのような事故・事件の影響を受けるのかを洗い出す必要がある。

ここで洗い出した情報を基に、誰がどのような体制・ルールを用いて対策を実施するか、事業継続に基づいて影響度を分析し、対処方法を検討する。対処方法は、IPAの「情報セキュリティマネジメントとPDCAサイクル」における「リスクへの対応」のように、「リスクの低減(セキュリティ事故・事件が発生する可能性を低下させる策を講じる)」、「リスクの保有(セキュリティ事故・事件が発生する可能性を受容する)」、「リスクの回避(セキュリティ事故・事件が発生する要素を取り除く)」、「リスクの移転(セキュリティ事故・事件が発生した場合でもその損失を充当する)」のいずれかを検討する。

#### <事後対応>

事後対応においては、「BCP発動」、「原因調査」、「顧客対応等のリスクコミュニケーション」、「再発防止策の実施」について考えなければならない。

事故や事件が発生した場合、どのような基準で「BCP発動」をするのかを決めておく必要がある。また、「BCP発動」した際には、どのような体制で事故や事件に対応するのかも決めておく必要がある。

体制に基づいて、「原因調査」と「再発防止

策」の策定を実施する。仮に、これらの対応で外部の専門調査機関を利用する場合、どの組織に依頼するのかを決めておくことも検討する必要がある。

「顧客対応等のリスクコミュニケーション」は、予め関係者の特定や、想定される事故においてどのような対応を行うかを検討する。

リスクコミュニケーションでは、関係者に必要な情報を適切に公表・説明できる対応を検討する必要がある。

### 3.2 安全な運用のための企画・設計

[担当:システム管理者]

安全にシステムを運用するためには、あらゆるケースを想定し、企画・設計を実施することが重要である。システム及び情報資産を安全に運用するために、組織としてどこまで対策を実施するのか、要求するセキュリティレベルはどこまでかを検討し、自社で運用するか、外部の業者に委託するのかどうかを判断する。

システム運用のための企画・設計は、経済産業省の「情報セキュリティ管理基準」等を参考に行うことが望ましい。例えば、次のような管理策について考慮する必要がある。

- ① 資産の分類及び管理
- ② 人的資源のセキュリティ
- ③ 物理的及び環境的セキュリティ
- ④ 通信及び運用管理
- ⑤ アクセス制御
- ⑥ 情報システムの取得、開発及び保守
- ⑦ 情報セキュリティインシデントの管理
- ⑧ 事業継続管理
- ⑨ 法律面や監査面からの適合性

### 3.3 安全な運用のための契約

[担当:経営者・システム管理者]

この対策は、外部に業務を委託する場合において、委託先で適切なセキュリティレベルが

確保されることを目的としている。

組織が業務を進めていくにあたり、システムの管理、運用等の自組織の特定の業務を外部の業者に委託する事がある。また、組織においてはサプライチェーン等において、業務提携をする場合も考えられる。

委託先や提携先のセキュリティ対策が不十分であった結果、委託元の情報システムに対して、事業継続上の影響を与える可能性がある。これを防ぐためには、組織として、契約関連の規程、運用ルール及び契約書(業務委託契約)、委託先選定基準、秘密保持契約、個人情報に関する取扱等について、セキュリティ対策という観点から見直しを図る必要がある。また、見直した結果、適切に規程及びルールが運用されているかについて、定期的に監査部門による委託先のチェックを行わなければならない。

### 3.4 サーバシステムへの対策

[担当:システム管理者]

この対策の目的は、サーバ製品に対する攻撃や、その二次被害を防止することである。サーバ製品は、脆弱性対策としてアップデートが必要である。しかし、サーバ製品はクライアント製品と違い、重要なシステムほどアップデートが困難になりがちである。なぜならば、アップデートの影響でサービスが停止する可能性が大きいからだ。しかし、脆弱性が存在するサーバ製品を使い続けても、攻撃されるリスクが残る。

解決策は、アップデート計画や回避策を用意し、計画的に実行することである。まず、アップデートをテストする環境を用意し、予めテストを行った後に、本番環境をアップデートするという手順が基本となる。

アップデートによるサービスへの影響を回避できない場合、IDS/IPS や WAF 等で攻撃を検

知/防御する仕組みを導入して、回避策を取る必要がある。IDS/IPS や WAF の運用には、専門的なノウハウが必要になる上に専門知識の収集が不可欠であるためコストとリスクのバランスを鑑みつつ、セキュリティ会社の監視サービスを利用することも検討するとよいだろう。セキュリティ会社の監視サービスによって、自社で運用するより高い安全性を達成することが期待できる。

### 3.5 クライアントシステムへの対策

[担当:システム管理者]

この対策の目的は、クライアントソフトに対する攻撃や、その二次被害を防止することである。攻撃によってウイルス感染が起きた場合は二次被害が広がりやすいため、特に注意したい。

解決策は、OS やクライアントソフトを常に最新版にアップデートすることだ。OS については、OS 自身の自動アップデート機能でアップデートすることができる。クライアントソフトについては、自動アップデート機能が利用できない場合もあるが、IPA で提供している「MyJVN バージョンチェッカ」を使用することで、いくつかの製品について確認することが可能である。

ただし、ソフトウェアを最新版にしても、ゼロデイ攻撃は防げない。ゼロデイ攻撃に対しては、ウイルス対策ソフトを導入すること、ウイルス対策ソフトの定義ファイルを最新に保つことで対応できる場合がある。また、実行ファイルのふるまいを検知してウイルスと判定するような対策ソフトを導入することにも効果があるだろう。この対策の目的はウイルス感染や感染による二次被害を減らすことである。

### 3.6 アカウント情報の管理・運用

[担当:システム管理者]

この対策の目的は、アカウントの盗用を防ぐことである。それにはアカウントの適切な管理と

運用が必要で、具体的には以下のような対策が挙げられる。

#### ＜サーバ設定上の対策＞

サーバ設定上の対策は次の2つである。

- ・ 不要なアカウントを削除または無効化する。
- ・ サーバに対して外部からアクセスできる場所を限定する。

#### ＜利用者教育＞

システム管理者はアカウントの利用者に次の3点について適切に教育する必要がある。

- ・ 個々のアカウントに、それぞれ異なるパスワードを割り当てる。
- ・ パスワード等の認証情報は、利用者本人だけがわかる場所に保管する。
- ・ パスワードを使用する場合、十分な長さと同様複雑さを確保する。

### 3.7 セキュア・プログラミング

[担当:開発者]

この対策は、ウェブサイトやソフトウェアに対する攻撃を防止することである。

ウェブサイトを構築する場合、IPA が公開している「安全なウェブサイトの作り方」や「セキュア・プログラミング講座」等を参考に、ウェブサイトの安全性向上に取り組む必要がある。

また、セキュア・プログラミングは、ソフトウェア製品や組み込み製品でも同様に必要である。開発者は、脆弱性対策の漏れが生じることや新しい脆弱性が発見される場合に備えておく必要がある。脆弱性を修正したバージョンを提供する際、利用者が簡易にアップデートできるような機能をソフトウェア製品に組み込みたい。

### 3.8 体制・ルール・システム等の点検

[担当:経営者・システム管理者]

この対策の目的は、組織に導入されている

セキュリティマネジメントサイクルが適切に運用、遵守されているかを確認し、情報システムに対して導入されているセキュリティ対策が有効に機能しているかを評価することで、リスクを再評価することである。評価・点検を実施した後は、3.9の見直し、改善へ繋げる必要がある。

組織に導入され、運用されているセキュリティマネジメントサイクル及び情報セキュリティ対策が、組織のセキュリティレベルの維持のために有効に機能しているか、隠れた脆弱性が潜んでいないか等について、評価、点検を行い、リスクを顕在化させる必要がある。

情報セキュリティ対策の評価には、「自己点検」、「情報セキュリティ対策ベンチマーク」、「情報セキュリティ監査」等がある。第三者の認証を受けるのは、その一つの方法である。

### 3.9 体制・ルール・システム等の見直し

[担当:経営者・システム管理者]

この対策の目的は、3.8の評価、点検によって再評価したリスクについて、対策の見直しと改善を行うことにより、組織のセキュリティレベルを維持・向上させることである。組織のセキュリティ対策の評価、点検結果に基づいて体制やルールが適切であるかを見直す必要がある。

評価、点検によって再確認されたリスクへの対処は、まずリスク分析を行う。リスクへの対処として「リスクの低減」、「リスクの保有」、「リスクの回避」、「リスクの移転」等があるが、組織においてどの対処が適切であるかを決定する。

また、現在とられている対処が適切であるかという点についても見直す事が重要である。

見直しによって、変化するセキュリティの情勢の中で形骸化している対策や見逃していたセキュリティ対策を実施することが期待できる。

## 【付録 1】 10 大脅威関係表

付表 1 は、10 大脅威における対策が必要な主な対象者を表す。2009 年は、ガンブラーに関連する脅威が多い。今年、新規に取り上げられた脅威としては、「アップデートしていないクライアントソフト」や「対策をしていないサーバ製品の脆弱性」等がある。また、昨年の 10 大脅威より順位が上がったものとして、「変化を続けるウェブサイト改ざんの手口」や「悪質なウイルスやボットの目的」等がある。

付表 1. 10 大脅威 対策が必要な対象者と総合順位

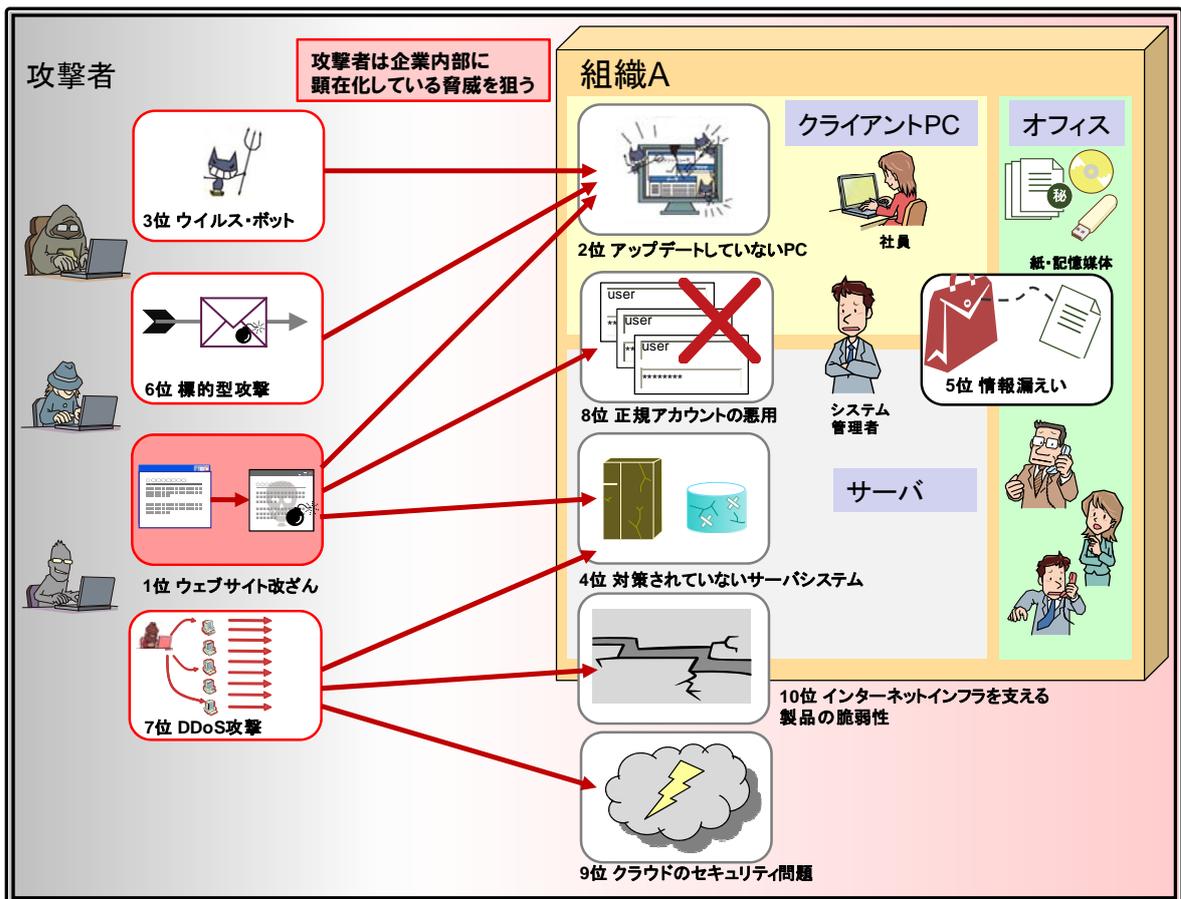
10 大脅威		対策が必要な主な対象者			2009 年度 順位 [白書 2009]	2008 年度 順位 [白書 2008]
		経営者	システム 管理者	開発者		
1 位 ↑	変化を続けるウェブサイト改ざんの手口	○	◎	◎	2 位	5 位
2 位 ↑	アップデートしていないクライアントソフト	○	◎		—	4 位
3 位 ↑	悪質なウイルスやボットの目的	○	◎		4 位	6 位
4 位 ↑	対策をしていないサーバ製品の脆弱性	○	◎		—	—
5 位	あわせて事後対応を！情報漏えい事件	◎	◎		5 位	3 位
6 位	被害に気づけない標的型攻撃	◎	◎		3 位	4 位
7 位	深刻な DDoS 攻撃	○	◎		—	—
8 位 ↑	正規のアカウントを悪用される脅威	○	◎		10 位	—
9 位 ↑	クラウド・コンピューティングのセキュリティ	◎	◎		—	—
10 位	インターネットインフラを支える製品の脆弱性	○	◎		—	—

◎:特に対策が必要な対象者    ○:対策を考慮する必要がある対象者    ↑:昨年より順位が上がったもの

## 【付録 2】 10 大脅威関連図

付図 1 は、10 大脅威の関連図を示したものである。攻撃者が使用してくる手口の脅威としては「1 位 変化を続けるウェブサイト改ざんの手口」、「3 位 悪質なウイルスやボットの目的」、「6 位 被害に気づけない標的型攻撃」、「7 位 深刻な DDOS 攻撃」がある。組織に顕在化している脅威で攻撃者に狙われるものとしては、「2 位 アップデートしていないクライアントソフト」、「4 位 対策をしていないサーバ製品の脆弱性」、「8 位 正規のアカウントを悪用される脅威」、「9 位 クラウド・コンピューティングのセキュリティ」、「10 位 インターネットインフラを支える製品の脆弱性」としている。また、組織に顕在化している脅威で、攻撃者如何に関わらず発生するものとしては「5 位 あわせて事後対応を！情報漏えい事件」がある。

図中の矢印は、「攻撃者」が、「組織」で顕在化しているそれぞれの脅威を狙っていることを示す。なお、これは 10 大脅威の関係を網羅したものではなく、また 10 大脅威以外の脅威については触れていない。



付図 1. 10 大脅威の主要な関係

## 【付録 3】 参考資料

- (参考資料 1) 事業継続計画策定ガイドライン  
[http://www.meti.go.jp/policy/netsecurity/downloadfiles/6\\_bcpguide.pdf](http://www.meti.go.jp/policy/netsecurity/downloadfiles/6_bcpguide.pdf)
- (参考資料 2) 情報セキュリティ管理基準  
[http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS\\_Audit\\_Annex01.pdf](http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex01.pdf)
- (参考資料 3) 情報セキュリティマネジメントと PDCA サイクル  
<http://www.ipa.go.jp/security/manager/protect/pdca/index.html>
- (参考資料 4) 重要インフラ情報システム信頼性研究会報告書、2009 年 4 月  
<http://sec.ipa.go.jp/reports/20090409.html>
- (参考資料 5) 2009 年度 情報セキュリティの脅威に対する意識調査、2009 年 11 月  
<http://www.ipa.go.jp/security/fy21/reports/ishiki/index.html>
- (参考資料 6) 情報漏えい発生時の対応ポイント集、2007 年 9 月  
<http://www.ipa.go.jp/security/awareness/johorouei/>
- (参考資料 7) 5 分でできる！情報セキュリティポイント学習、2009 年 10 月  
[http://www.ipa.go.jp/security/vuln/5mins\\_point/index.html](http://www.ipa.go.jp/security/vuln/5mins_point/index.html)
- (参考資料 8) 「脆弱性を利用した新たな脅威の監視・分析による調査」、2009 年 7 月  
<http://www.ipa.go.jp/security/vuln/report/newthreat200902.html>
- (参考資料 9) ソーシャル・エンジニアリングを巧みに利用した攻撃の分析と対策、2009 年 2 月  
<http://www.ipa.go.jp/security/vuln/report/newthreat200902.html>
- (参考資料 10) 「クラウド・コンピューティング社会の基盤に関する研究会」報告書、2010 年 3 月  
<http://www.ipa.go.jp/about/research/2009cloud/index.html>
- (参考資料 11) 知っていますか？脆弱性(ぜいじゃくせい)、2007 年 7 月  
[http://www.ipa.go.jp/security/vuln/vuln\\_contents/](http://www.ipa.go.jp/security/vuln/vuln_contents/)
- (参考資料 12) 安全なウェブサイト運営入門、2008 年 6 月  
<http://www.ipa.go.jp/security/vuln/7incidents/>
- (参考資料 13) 脆弱性対策情報ポータルサイト JVN  
<http://jvn.jp/>
- (参考資料 14) 脆弱性対策情報データベース JVN iPedia  
<http://jvndb.jvn.jp/>
- (参考資料 15) 脆弱性対策情報収集ツール MyJVN、MyJVN バージョンチェッカ  
<http://jvndb.jvn.jp/apis/myjvn/>
- (参考資料 16) SQL インジェクション検出ツール iLogScanner、2008 年 11 月  
<http://www.ipa.go.jp/security/vuln/iLogScanner/index.html>
- (参考資料 17) Web Application Firewall 読本、2010 年 2 月  
<http://www.ipa.go.jp/security/vuln/waf.html>
- (参考資料 18) セキュア・プログラミング講座  
<http://www.ipa.go.jp/security/awareness/vendor/programmingv2/>
- (参考資料 19) 安全なウェブサイトの作り方 改訂第 4 版、2010 年 1 月  
別冊：安全な SQL の呼び出し方、2010 年 3 月  
<http://www.ipa.go.jp/security/vuln/websecurity.html>
- (参考資料 20) TCP/IP に係る既知の脆弱性に関する調査報告書・検証ツール、2009 年 1 月  
[http://www.ipa.go.jp/security/vuln/vuln\\_TCPIP.html](http://www.ipa.go.jp/security/vuln/vuln_TCPIP.html)  
[http://www.ipa.go.jp/security/vuln/vuln\\_TCPIP\\_Check.html](http://www.ipa.go.jp/security/vuln/vuln_TCPIP_Check.html)
- (参考資料 21) SIP に係る既知の脆弱性に関する調査報告書・検証ツール、2009 年 4 月  
[http://www.ipa.go.jp/security/vuln/vuln\\_SIP.html](http://www.ipa.go.jp/security/vuln/vuln_SIP.html)  
[http://www.ipa.go.jp/security/vuln/vuln\\_SIP\\_Check.html](http://www.ipa.go.jp/security/vuln/vuln_SIP_Check.html)

執筆協力者

10 大脅威執筆研究会 構成メンバー

氏名	所属	氏名	所属
渡部 章	(株)アーケン	高橋 紀子	(社)JPCERT コーディネーションセンター(JPCERT/CC)
石田 淳一	(株)アールジェイ	林 薫	(株)シマンテック
加藤 雅彦	(株)アイアイジェイ テクノロジー	大野 雅子	(株)スマートバリュー
根岸 征史	(株)アイアイジェイ テクノロジー	星澤 裕二	(株)セキュアブレイン
高橋 康敏	(株)アイアイジェイ テクノロジー	神菌 雅紀	(株)セキュアブレイン
齋藤 衛	(株)インターネットイニシアティブ	正木 健介	セコムトラストシステムズ(株)
徳丸 浩	HASH コンサルティング(株)	澤永 敏郎	ソースネクスト(株)
三輪 信雄	S&J コンサルティング(株)	青谷 征夫	ソースネクスト(株)
小林 克巳	NRI セキュアテクノロジーズ(株)	百瀬 昌幸	(財)地方自治情報センター(LASDEC)
西尾 秀一	(株)NTT データ	木村 道弘	(株)電子商取引安全技術研究所(社)
池田 和生	(株)NTT データ	小橋 一夫	電子情報技術産業協会(JEITA)
入宮 貞一	(株)NTT データ	渡辺 淳	(株)デンソーウェーブ
井上 克至	(株)NTT データ	吉松 健三	(株)東芝
前田 典彦	(株)Kaspersky Labs Japan	小島 健司	東芝ソリューション(株)
岸本 博之	(財)金融情報システムセンター(FISC)	小屋 晋吾	トレンドマイクロ(株)
林 弘毅	経済産業省	岡谷 貢	内閣官房情報セキュリティセンター
清水 友晴	経済産業省	鍋島 学	内閣官房情報セキュリティセンター
秋貞 幸雄	経済産業省	須川 賢洋	新潟大学
鈴木 啓紹	(社)コンピュータソフトウェア協会(CSAJ)	徳田 敏文	日本アイ・ピー・エム(株)
福森 大喜	(株)サイバーディフェンス研究所	井上 博文	日本アイ・ピー・エム(株)
名和 利男	(株)サイバーディフェンス研究所	谷川 哲司	日本電気(株)
高木 浩光	(独)産業技術総合研究所	宇都宮 和顕	日本電気(株)
大岩 寛	(独)産業技術総合研究所	秋山 卓司	(社)日本電子認証協議会(JCAF)
宮地 利雄	(社)JPCERT コーディネーションセンター(JPCERT/CC)	長島 雅夫	日本電信電話(株)
伊藤 友里恵	(社)JPCERT コーディネーションセンター(JPCERT/CC)	杉浦 芳樹	日本電信電話(株)
宮崎 清隆	(社)JPCERT コーディネーションセンター(JPCERT/CC)	安部 哲哉	日本電信電話(株)
古田 洋久	(社)JPCERT コーディネーションセンター(JPCERT/CC)	住本 順一	日本電信電話(株)
		やすだ なお	特定非営利活動法人日本ネットワークセキュリティ協会(JNSA)
		榎本 司	日本ヒューレット・パッカード(株)
		西垣 直美	日本ヒューレット・パッカード(株)

氏名	所属	氏名	所属
佐藤 直之	日本ベリサイン(株)	村瀬 一郎	(株)三菱総合研究所
杉岡 弘毅	(株)ネクストジェン	川口 修司	(株)三菱総合研究所
山田 陽介	ネットエージェント(株)	村野 正泰	(株)三菱総合研究所
高橋 潤哉	(株)ネットセキュリティ総合研究所	藤井 誠司	三菱電機(株)
水越 一郎	東日本電信電話(株)	青木 歩	(株)ユービーセキュア
太田 良典	(株)ビジネス・アーキテクツ	志田 智	(株)ユビテック
吉野 友人	(株)ビジネス・アーキテクツ	福本 佳成	楽天(株)
本川 祐治	(株)日立情報システムズ	岩井 博樹	(株)ラック
田山 晴康	(株)日立製作所	山崎 圭吾	(株)ラック
寺田 真敏	(株)日立製作所	柳澤 伸幸	(株)ラック
梅木 久志	(株)日立製作所	川口 洋	(株)ラック
藤原 将志	(株)日立製作所	伊藤 耕介	(株)ラック
鵜飼 裕司	(株)フォティーンフォティ技術研 究所	若居 和直	(株)ラック
金居 良治	(株)フォティーンフォティ技術研 究所	中田 邦彦	(株)ルネサス テクノロジ
森 玄理	富士通(株)	矢島 秀浩	
富士原 裕文	富士通(株)	小森 聡	
木村 秀年	富士通(株)	小松 文子	
草間 正	富士通(株)	杉浦 昌	
望月 大光	(株)富士通ソフトウェアテクノロジ ーズ	小門 寿明	
佐藤 友治	(株)ブロードバンドセキュリティ	木邑 実	
許 先明	(株)ブロードバンドセキュリティ	加賀谷 伸一郎	
藤田 耕作	放送大学大学院	花村 憲一	
高橋 正和	マイクロソフト(株)	宮本 一弘	
加藤 義宏	マカフィー(株)	小林 偉昭	
国分 裕	三井物産セキュアディレクション (株)	金野 千里	
後藤 久	三井物産セキュアディレクション (株)	山岸 正	
寺田 健	三井物産セキュアディレクション (株)	中野 学	
		渡辺 貴仁	
		大森 雅司	
		園田 道夫	
		杉山 賢	
		勝海 直人	
		永安 佑希允	
		相馬 基邦	
		大谷 槇吾	
		谷口 隼祐	

※独立行政法人情報処理推進機構の職員（執筆当時）については所属組織名を省略しました。

著作・制作 独立行政法人情報処理推進機構(IPA)

編集責任 小林 偉昭 山岸 正

執筆協力者 10 大脅威執筆者会

執筆者 相馬 基邦

2010 年版

## 10 大脅威 『あぶりだされる組織の弱点！』

---

2010 年 3 月 31 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 16 階

<http://www.ipa.go.jp/>

# 情報セキュリティに関する届出について

IPA セキュリティセンターでは、経済産業省の告示に基づき、コンピュータウイルス・不正アクセス・脆弱性関連情報に関する発見・被害の届出を受け付けています。

ウェブフォームやメールで届出ができます。詳しくは下記のサイトを御覧ください。

URL: <http://www.ipa.go.jp/security/todoke/>

## コンピュータウイルス情報

コンピュータウイルスを発見、またはコンピュータウイルスに感染した場合に届け出てください。

## 不正アクセス情報

ネットワーク(インターネット、LAN、WAN、パソコン通信など)に接続されたコンピュータへの不正アクセスによる被害を受けた場合に届け出てください。

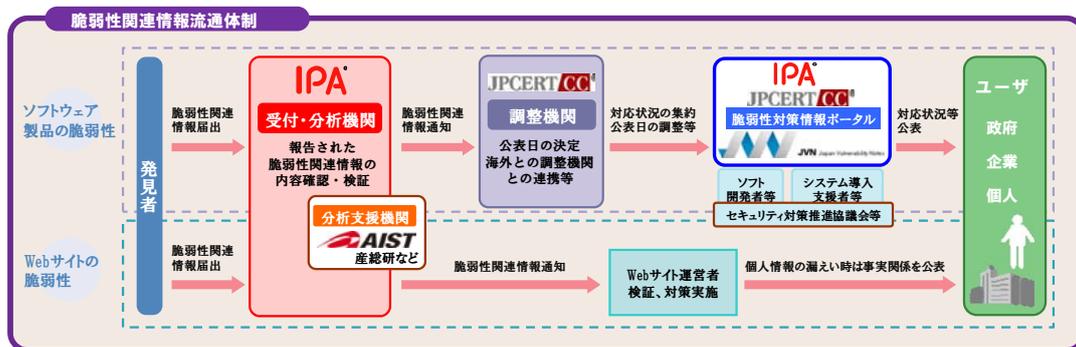
## ソフトウェア製品脆弱性関連情報

OSやブラウザ等のクライアント上のソフトウェア、ウェブサーバ等のサーバ上のソフトウェア、プリンタやICカード等のソフトウェアを組み込んだハードウェア等に対する脆弱性を発見した場合に届け出てください。

## ウェブアプリケーション脆弱性関連情報

インターネットのウェブサイトなどで、公衆に向けて提供するそのサイト固有のサービスを構成するシステムに対する脆弱性を発見した場合に届け出てください。

## 脆弱性関連情報流通の基本枠組み「情報セキュリティ早期警戒パートナーシップ」



※IPA: 独立行政法人 情報処理推進機構、JPCERT/CC: 有限責任中間法人 JPCERT コーディネーションセンター、産総研: 独立行政法人 産業技術総合研究所

# IPA<sup>®</sup>

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16階

<http://www.ipa.go.jp>

セキュリティセンター

TEL: 03-5978-7527 FAX 03-5978-7518

<http://www.ipa.go.jp/security/>