2010年版 10大脅威 『あぶり出される組織の弱点！』

独立行政法人 情報処理推進機構（IPA）
セキュリティセンター 情報セキュリティ技術ラボラトリー

独立行政法人情報処理推進機構（IPA）は、情報セキュリティ関連の動向、被害状況、対策状況、制度の動向などを分析し、その結果をとりまとめてさまざまな形で情報発信している。本稿では、2010年3月31日に公開された「2010年版 10大脅威」の内容を紹介する。

1 はじめに

2009年にはガンブラー（Gumblar）[注]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。

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。

2 ガンブラーによるビジネスインパクト考察

ガンブラーでは、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。（図1参照）

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。

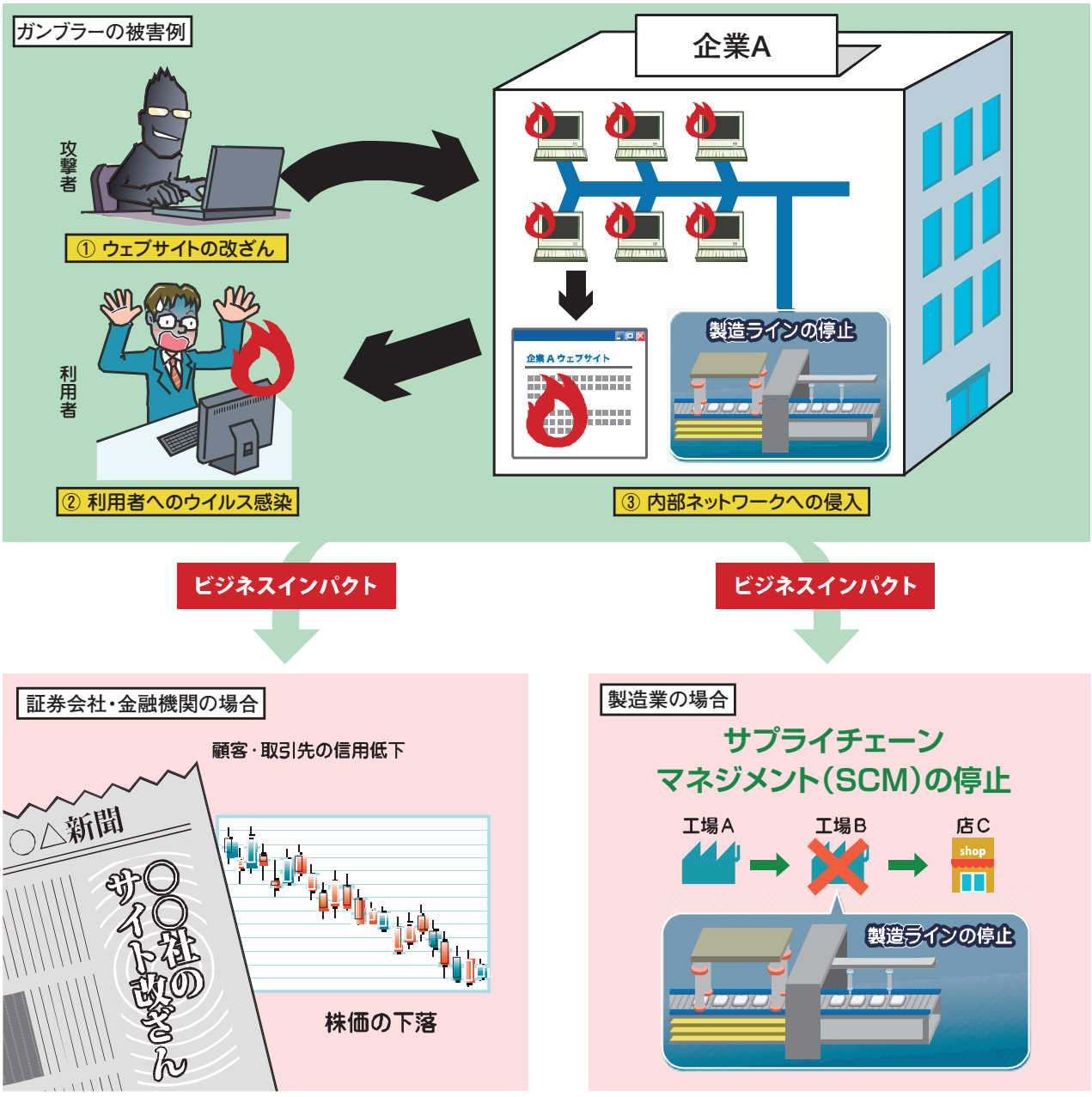
③ 自組織内のネットワークを攻撃される脅威

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）証券会社や金融機関等の場合

ガンブラーと呼ばれるウイルス感染の手口は一

図1　ガンブラーがもたらすビジネスインパクト



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。

証券会社や金融機関等の場合、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。

(2) 製造業等の場合

精密機械等を製造する会社の場合、特に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。

3 ガンブラーの事前対策・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に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。

4 内部犯罪による情報窃取事件のビジネスインパクト考察

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。**（図2参照）**

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。

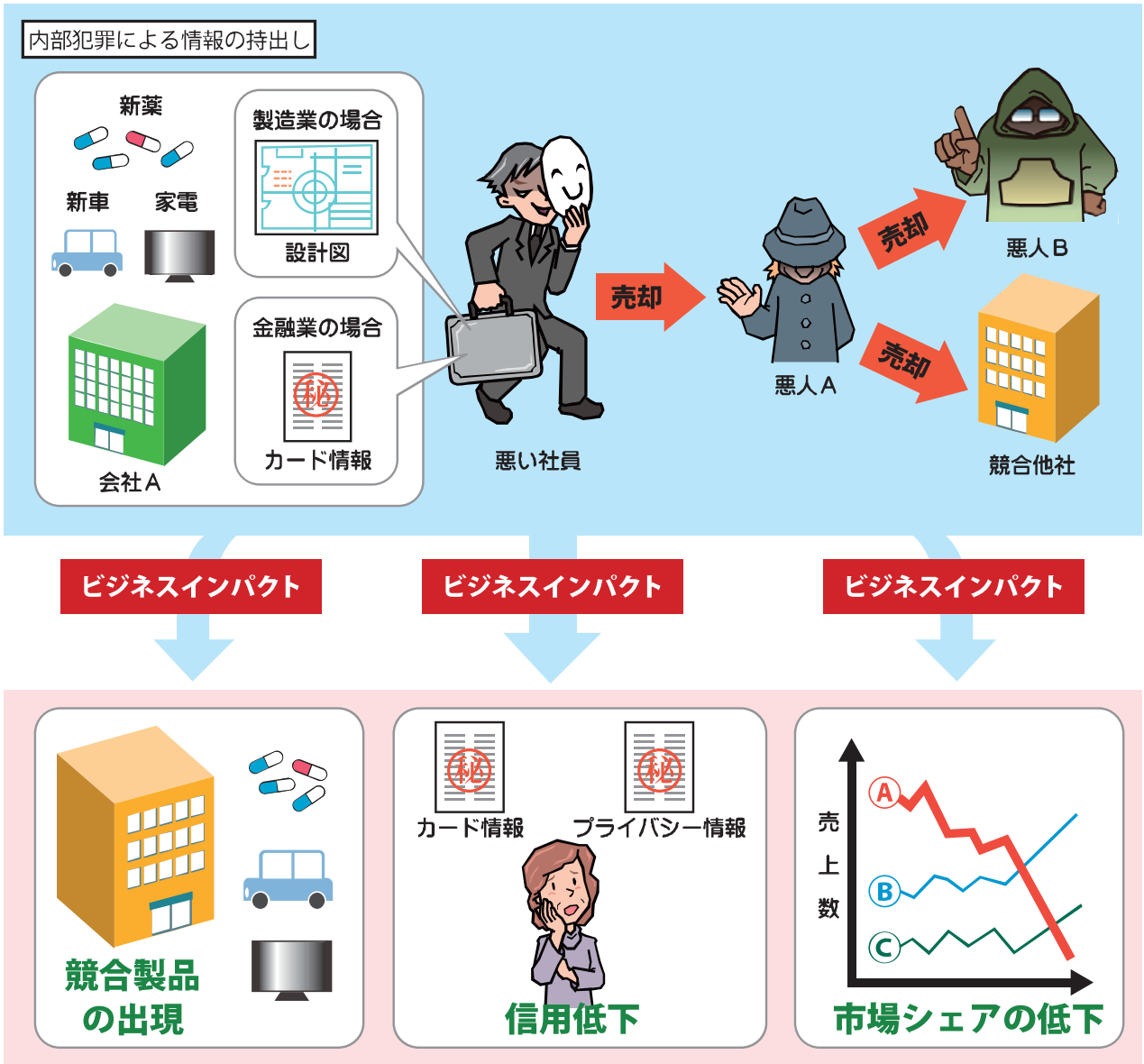
また、複数の企業での共同開発の情報や委託された開発に関する情報であれば、提携企業、顧客に対しても損害を与えることになる。これによって、窃取された情報に関する補償だけではなく、提携企業、顧客からの信用の失墜も考えられる。その場合、今後の事業継続を困難にする事態に陥る。

5 内部犯罪における事前対策・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

図2　内部犯罪がもたらすビジネスインパクト



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「システム的な側面」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、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。

6 10大脅威

2010年10大脅威を挙げる。10大脅威の各脅威についても、組織に対するビジネスインパクトを考えて、対策を講じる必要がある。**（図3参照）**

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。「2のガンブラー」だ。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がもたらされた。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。

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修正済みのものが多く、利用者側のアップデートが徹底されていれば、被害を減らせたはずである。

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。

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。2009年にはウイルスの亜種が爆発的に増加した。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。（2008年は約90万）

4位　対策をしていないサーバ製品の脆弱性

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

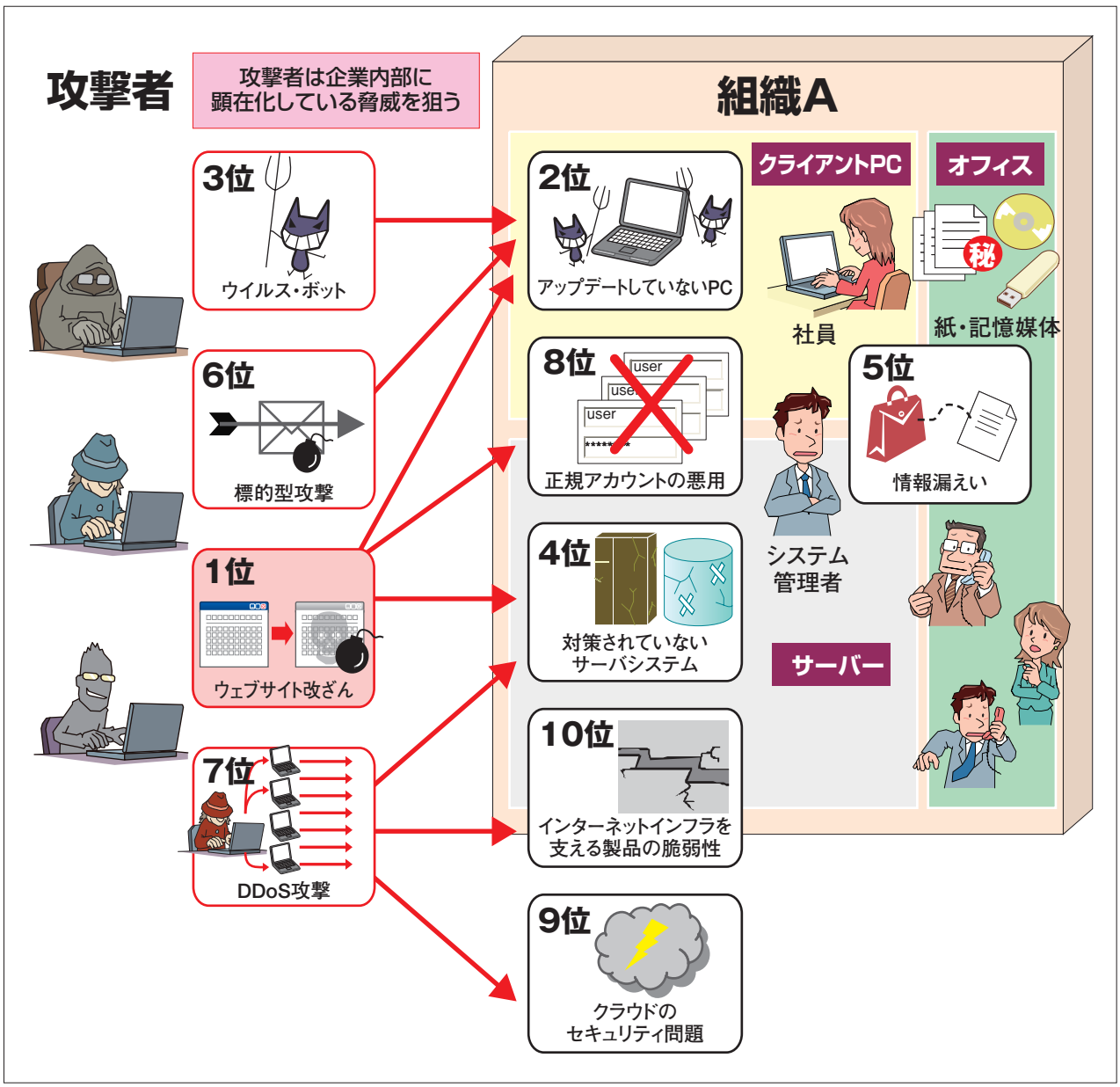
ウェブサーバやウェブアプリケーションに代表されるサーバ製品に脆弱性があると、攻撃者にその脆弱性を悪用される恐れがある。2009年はSQLインジェクション等によるウェブサイト改ざんが度々報道された。サーバ製品には、適切な脆弱性対策を行う必要がある。

5位　あわせて事後対応を！情報漏えい事件

情報漏えいには様々な原因がある。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、4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。

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

図3　10大脅威の関連図



コンやUSB等の外部記憶媒体であった。

6位　被害に気づけない標的型攻撃

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

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。

7位　深刻なDDoS攻撃

DDoS（Distributed Denial of Service）攻撃は、

DoS攻撃（サーバやルータなどの機能を麻痺状態にさせる）の一種である。

2009年7月に米国・韓国が攻撃を受けたニュースが流れた。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。

8位　正規のアカウントを悪用される脅威

コンピュータに対して自分であることを証明する情報（ユーザIDとパスワード等）がアカウントである。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。

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。

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。

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
②クラウド環境内部での他の利用者に対する攻撃
③クラウド環境を踏み台にした外部への攻撃
④クラウドのリソースの悪用
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

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。

10位　インターネットインフラを支えるプロトコルの脆弱性

多くのコンピュータでインターネットに接続するための機能が備えられている。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。

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。

7 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。

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。

対策の詳細については、『2010年版 10大脅威』の第3章を参照して欲しい。

【注】
ガンブラー（Gumblar）：多数のパソコンにウイルスを感染させようとする攻撃手法の一種を指す俗称。「ウェブサイト改ざん」と「ウェブ感染型ウイルス」を組み合わせ、改ざんされたサイトの閲覧者にウイルス感染させる。FTPアカウント情報を盗んでウェブサイト改ざんするのがガンブラーの特徴。当初、改ざんサイトを閲覧したユーザーが「gumblar.cn」ドメインのサイトにジャンプさせられてウイルス感染していたのが、名前の由来。