会計事務所向けセキュリティ研修会

NTTデータ先端技術株式会社

INDEX

本資料の構成

- **税理士としてご活躍されている先生方のセキュリティに関する視点として4つを挙げることができますが、このうち①～③までを本日の資料の対象としています。**
- **税理士先生は顧問先企業の第一の相談役であることも多いと思いますので、顧問先企業にとっても有用と思われる情報を記載しています。是非ご活用ください。**

ロケーション	視点	本資料で関連する章
税理士、税理士事務所内	①顧問先から預かった情報を守る	1章、2章、3章
	②自分の情報（営業秘密等）を守る	1章、2章、3章
顧問先	③企業の相談役、専門家として、顧問先にセキュリティを提案する	2章、3章
	④顧問先にセキュリティ投資関連税制の利用を提案する	対象外

直面するリスクとセキュリティ

①顧問先から預かった情報を守るという視点

様々なリスクの中の一つとしてのセキュリティリスク

- 税理士業務に関わるリスクについて調べました。
- 参考にした記事は、2004年の記事ですが、訴訟リスクとして、様々なリスクがあり、その中に「守秘義務違反」としての情報漏えいが挙げられている事が分かります。

＜委任契約に基づく訴訟リスク＞

・スポット関与事案と専門家責任
・顧問契約と専門家責任
・節税スキームの実行に伴う責任
・契約が終了した関与先に対する責任
・隣接専門家との提携と税理士の責任
・社員税理士・補助税理士・職員に対する責任

＜商法関連の訴訟リスク＞

・監査役の責任
・議事録作成に関する責任

＜税理士法関連の訴訟リスク＞

・守秘義務違反
・関与先の粉飾決算
・関与先の脱税

＜労働法関連の訴訟リスク＞

・事業主としての職員に対する責任

参考文献:「今そこにある危機　税理士業務に伴う訴訟リスク」2004.4『税理』株式会社ぎょうせい

税理士に求められる責任

- 税理士法、個人情報保護法等から見たインパクトを記載しました。
- 税理士に求められる高い職業倫理を反映した結果、「①顧問先から預かった情報を守る」ための厳しい守秘義務が課せられているのであろうと推測されます。

秘密を守る義務
（税理士法38）

税理士の使用人等の秘密を守る義務
（税理士法54）

＋

税理士業務委託契約に基づく民法上、
契約上の守秘義務

＋

個人情報保護法

【違反した場合】

- 税理士業務の禁止、1年以内の税理士業務の停止又は戒告
  （税理士法46）
- 刑事罰として懲役2年以下又は100万円以下の罰金
  （税理士法38,59①二）

これらは税理士事務所又は税理士法人の職員が漏らした場合も同様
（税理士法54,59①二）

＋

- 民事上　契約上の責任、悪質な場合は不法行為責任を負う
  （民法415,709）
- 過失の場合は、刑事罰は適用されないが、懲戒処分の対象にはなり得、顧客に対する民事上の責任は生じる。

＋

- プライバシー侵害を理由とする責任を追及される可能性
- 個人情報保護法に基づく罰則

＋

- 信頼の失墜

参考文献:「守秘義務違反」　砦 真希　『税理』2004.4 株式会社ぎょうせい

【参考】実際に情報セキュリティ事故は発生しているのか？

- 退職した職員が顧客の法人情報を持ち出し、転職先にその内容を流出させ、不正に使用して顧客から問い合わせがあった。このため被害法人に詫び状を送付するなどの事故対応費用が発生した。

- 顧客の未公表の出店計画が記載されたメールを、事務所の職員が誤ってライバル企業に転送し流出させた。その結果、顧客が事業計画の変更を余儀なくされ、先行して行っていた設備投資について顧客から損害賠償請求を受けた。

- 外部からの不正アクセスにより、メーリングリストに登録していた個人情報が漏えいしたことが報道で明らかになった。このため、お詫び状作成費用や謝罪のために支出する見舞い品の購入費用が発生した。

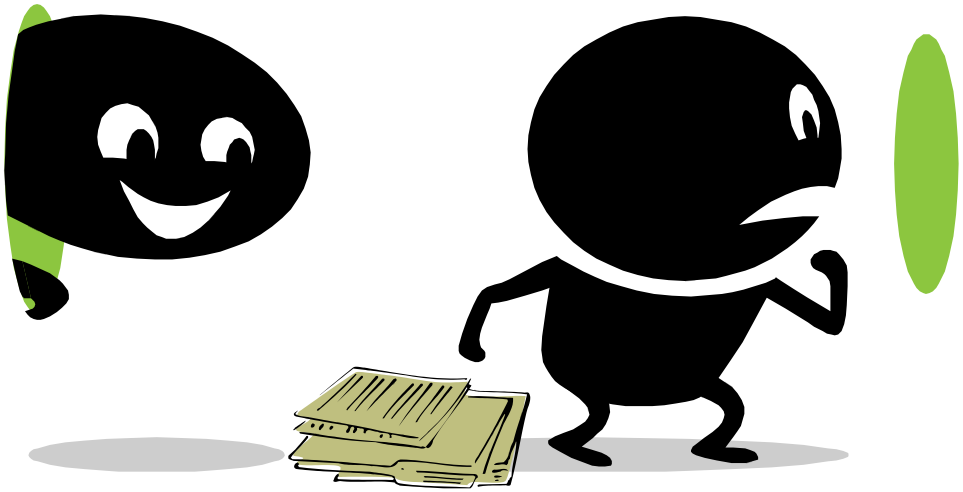
- 顧客名簿のデータベース化を委託した外部業者が情報を流出させたことにより、顧客の一部がプライバシーの侵害を理由に損害賠償を請求した。

出典：「税理士職業賠償責任保険 情報漏えい担保特約 パンフレット」株式会社日税連保険サービス

②自分の情報（営業秘密等）を守るという視点

- 「①顧問先から預かった情報を守る」、という視点以外に、「②自分の情報（営業秘密等）を守る」という視点についても検討しておく必要があります。
- 例えば、会計事務所の職員が退職する際に、顧問先名簿、顧問先料金表を持ち出し、顧問先に営業をかける、他の会計事務所に情報を渡す、などが想定されます。

- このようなケースの際に、営業秘密の要件である秘密管理性が無いとして、損害賠償請求などが認められなかった事案もあります。（会計事務所顧客名簿事件平成１１年９月１４日　大阪地裁）



【参考】会計事務所顧客名簿事件平成11年9月14日　大阪地裁

争点となった営業秘密:「顧問先名簿」「顧問料金表」「フロッピー」

■被告Aが原告に在職していた当時、原告は、顧問契約者一覧表記載の顧問先と顧問契約を締結していた。本件顧問先は、被告設立後、被告と顧問契約を締結し、原告との顧問契約を解約した。

■そこで、原告は、被告会社に対し、被告会社はAから開示された原告情報を使用し本件顧問先と顧問契約を締結したが、それは、不正競争防止法2条1項8号に該当するとして、主位的に右使用に基づく本件顧問先との顧問契約業務の差止めを求めるとともに、予備的に被告が本件顧問先と顧問契約を締結したことにより原告が被った損害の賠償を求めた。

秘密管理性:認められず

■顧問先名簿を、Aを含む従業員との関係で客観的に認識できる程度に、対外的に漏出しないように管理していたとは認められない。

■顧問料金表は、施錠されて保管されていたものの、それは原告の保有する経理文書の管理方法として一般的であって、原告が、顧問料金表を、Aを含む従業員との関係で客観的に認識できる程度に、対外的に漏出しないように管理していたとは認められない。フロッピーを、各従業員の机の上の無施錠の保管箱に入れて保管させていたことが認められ、フロッピーに秘密と表示していたとか、従業員にフロッピーは秘密とするよう指導していたとか、フロッピーにアクセスできる人的制限、時間的制限が課せられていたとかなど、然るべき事情は、認められない。

参考資料:平成一〇年(ワ)第一四〇三号　不正競争防止法に基づく差止請求事件
「営業秘密管理指針」2011.12 経済産業省

営業秘密とは何か

■ **「営業秘密」とは、①秘密として管理されていること、②有用な情報であること、③公然と知られていないことの三要件を満たす技術上、営業上の情報とされています。**

①秘密管理性

秘密管理性が認められるためには、その情報を客観的に秘密として管理していると認識できる状態にあることが必要。
具体的な要件は以下の二つ。

a.情報にアクセスできる者を特定すること、

b.情報にアクセスした者が、それを秘密であると認識できること

→例えば、情報に「秘密」などのラベルを貼り付ける。
情報を見ることのできる人を制限する（限られた職員さんにしか開示しない）。 などの管理が必要。

②有用性

有用性が認められるためには、その情報が客観的に有用であることが必要。
この有用性とは、競争優位性の源泉となる場合を含め、そもそも当該情報が事業活動に使用されたり、
又は使用されることによって費用の節約、経営効率の改善等に役立ったりするものであることを意味する。

③非公知性

「非公知性」が認められるためには、当該情報が刊行物に記載されていないなど、保有者の管理下以外では
一般に入手できないことが必要。

参考資料:「営業秘密管理指針」2011.12 経済産業省

営業秘密管理指針

■ **営業秘密の管理のあり方として、組織的管理（セキュリティマネジメント）が求められています。**

■ **「営業秘密の要件を満たす」、そして、「営業秘密を管理する」ということは、セキュリティを守ることそのものであり、セキュリティを守ることによって、情報と自分自身を守ることにつながるといえます。**

～営業秘密管理指針より～

- 営業秘密の管理に当たっては、「物理的管理」、「技術的管理」、「人的管理」等の具体的な管理方法により、秘密情報をその他の情報と区分し、権限に基づきアクセスした者がそれを秘密であると認識して取り扱うために必要な措置を講じるとともに、権限のない者がアクセスすることができないような措置を講じることが必要である。

- また、具体的な管理方法による管理を適切に機能させるために「組織的管理」をすることが重要である。

【参考】個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン

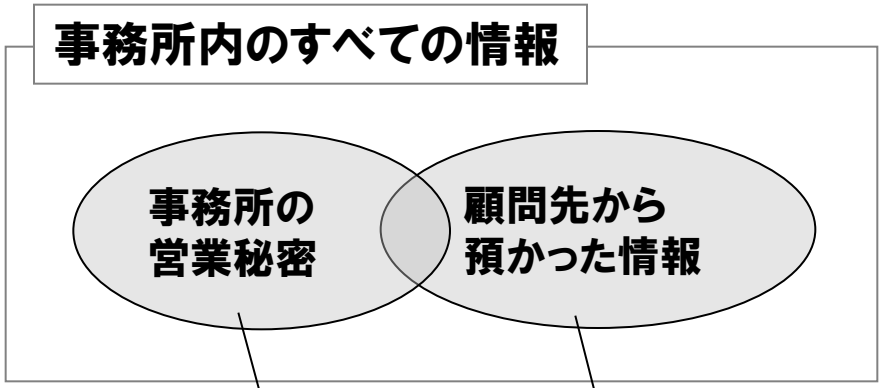
・個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。（法第20条）

・個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のため、組織的、人的、物理的及び技術的な安全管理措置を講じなければならない

参考資料：「営業秘密管理指針」2011.12 経済産業省
「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」2009.10 経済産業省

本章のまとめ

- 本章では、法律を中心に①顧問先から預かった情報を守る、②自分の情報（営業秘密等）を守るという視点について説明しました。
- 事務所内の営業秘密、顧問先から預かった情報以外にも守らなければならない情報はあると思いますが、いずれにしてもセキュリティの取り組みは行うべきだといえます。



①顧問先から預かった情報を守るという視点

税理士法上の守秘義務
＋税理士業務委託契約に基づく民法上、契約上の守秘義務
＋個人情報保護法上の責任

②自分の情報（営業秘密等）を守るという視点

不正競争防止法および営業秘密管理指針

情報セキュリティのリスクの考え方

■人体の急所って、調べたことありますか？

きゅうしょ【急所】

そこに打撃を受けると生命にかかわる場所をいう。
眉間（みけん）など全身に40ヵ所内外あり，それらの多くは東洋医学でいう
経穴(つぼ)※に一致し，皮下の浅いところを大血管が通過していたり，
骨の薄いところや，自律神経が集中していたりして，打撃によって外傷性ショック
を起こしやすい場所となっている。
なお，武道などでは，生命にはかかわらなくても，そこへの攻撃によって，
その人の行動を封じることができる場所をも急所とよぶことが多い。

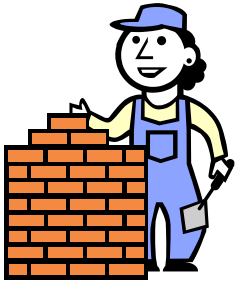
・天倒（てんとう）（頭頂部）
・烏兎（うと）（みけん）
・霞（かすみ）（こめかみ）
・人中（じんちゆう）（鼻下）
・水月（すいげつ）（みぞおち）
・明星（みようじよう）（下腹部）
・電光（でんこう）（右ひばら）
・月影（げつえい）（左ひばら）
・釣鐘（つりがね）（睾丸）
・ひざ関節　など

（出典：世界大百科事典 第2版）

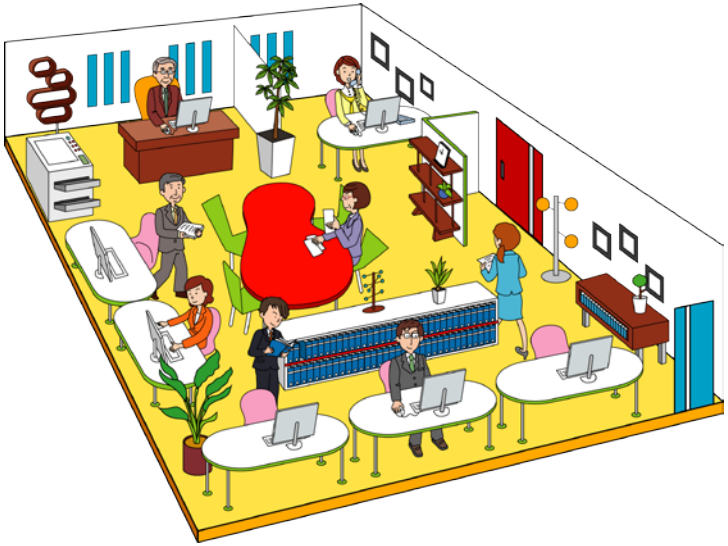
※経穴(つぼ)については、2006年に経穴部位国際標準化公式会議で361穴が国際標準として標準化されました。

本章のはじめに

- だからといって、皆が常に鎧を着て歩いているわけではありません。
- しかし、特定の作業を行う際には、体を保護する目的で作業服、防護服等を着て、安全靴を履いて、ヘルメットを被って作業に当たります。
- つまり、行う作業に伴う危険性によって、守る場所と対策を変えているのです。



会計事務所、顧問先の急所とは？



- セキュリティも同じと考えることができると思います。

- 取り扱う情報の重要性、社会的なインパクト、業務の方法等によって、守るべきものとセキュリティ対策は変わります。
- 国家の安全保障に関わる業務を行う企業と一般の企業ではセキュリティ対策が変わるのが当然といえます。

- 「セキュリティには際限が無い」、「どこまで対策をすればよいのか分からない」といった言葉をよく耳にします。まさにその通りで、明確な答えはありません。
- 今回の資料では、対策ではなく、急所（リスク）を把握するための方法を記載しています。
- なぜならば、**リスクの把握は、リスクマネジメントの最初のプロセスで、かつ、最も大切なプロセス**であるからです。

急所（リスク）を洗い出す際の考え方

① 省庁、関連団体の資料、ガイドライン等を参照する

リスクとリスク対応に関する基準を把握する

独立行政法人 情報処理推進機構から「中小企業の情報セキュリティ対策ガイドライン」が公開されている。
その他、各省庁からも基準、ガイドラインが多数公開されているため、自社に近いものを参照することが望ましい。

② 最新動向をチェックする（新しいリスクがないか）

セキュリティリスクは変化する

企業を取り巻く環境は日々変化している。情報漏えいやウイルス感染といったセキュリティリスクを取り巻く状況も次々と変化しており、セキュリティ対策を随時見直すとともに必要な対策を継続的に講じていかなければならない。

③ 事故事例をチェックする（同じ事象が会計事務所で起きないか）

失敗する方法があれば、誰かはその方法でやる

業務上のプロセスで、同じような事故が起きないかという視点で事故事例をチェックする。

①省庁、関連団体の資料、ガイドライン等を参照する

- 省庁、関連団体から出されている資料、ガイドライン等は多岐にわたります。
- 信頼性のある情報ですので、確認することをお奨めします。

特に経済産業省と、情報処理推進機構(IPA)の情報をチェックすることをお奨めします。

経済産業省　情報セキュリティ対策ポータル：
http://www.meti.go.jp/policy/netsecurity/index.html

IPA 独立行政法人 情報処理推進機構：
https://www.ipa.go.jp/

経済産業省ホームページ:http://www.meti.go.jp/policy/netsecurity/links.htm

②最新動向をチェックする（新しいリスクがないか）

情報セキュリティの変遷

- 2001年から2012年までの情報セキュリティの変遷を記載しました。
- セキュリティリスクが時代とともに変化していることが分かります。

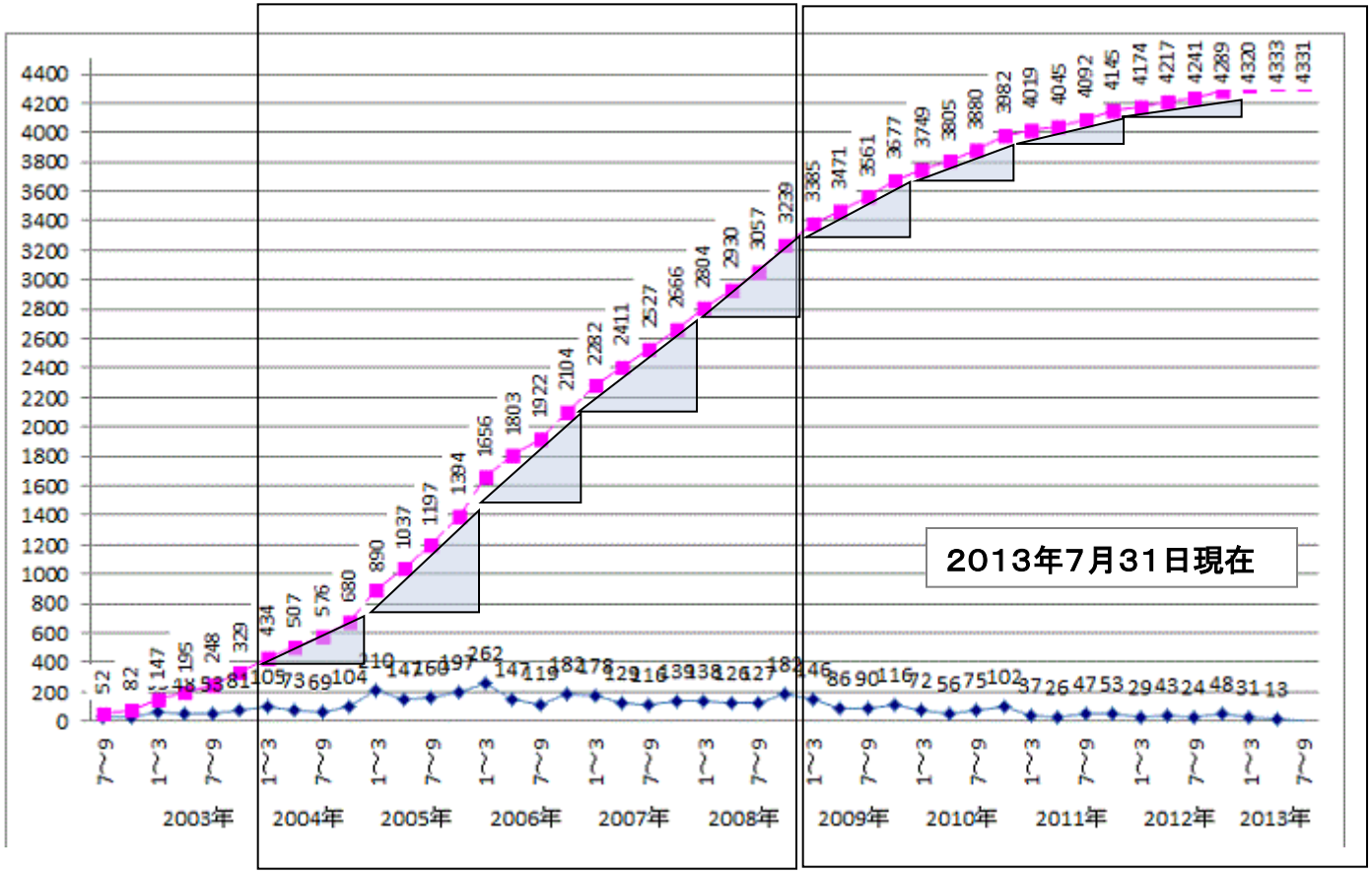
	2001-2003	2004-2008	2009-2012
時代背景	ネットワークウィルスの全盛	内部統制・コンプライアンス	脅威のグローバル化
IT環境	コミュニケーション手段の確立	e-コマースの加速	経済・生活基盤に成長
セキュリティの意味合い	サーバやPCの保護	企業・組織の社会的責任	危機管理・国家安全保障
攻撃者	攻撃者1人	金銭を目的とした攻撃者出現	・ハクティビストの顕在化※ ・諜報的集団（国家）の顕在化
攻撃傾向	ネットワーク上の攻撃	人をだます攻撃の登場	攻撃対象の拡大
攻撃対象	PC、サーバ	人、情報サービス	スマートデバイス、重要インフラ
対策の方向	セキュリティ製品中心の対策	マネジメント体制の確立	・官民・国際連携の強化 ・セキュリティ人材育成強化
法律	・不正アクセス禁止法施行（2000） ・電子署名法施行（2001）	・個人情報保護法　全面施行（2005） ・e-文書法施行（2005） ・日本版SOX法施行（2008）	・不正競争防止法改正（2010） ・刑法改正（ウィルス作成罪施行）（2011） ・不正アクセス禁止法改正（2012）
主な事件	Nimda、Code Red流行	・Winny,Share等での情報漏洩 ・不正アクセスによる情報漏洩 ・スパイウェアによる不正送金	・米韓にDdos攻撃 ・政府機関を狙ったサイバー攻撃 ・金融機関を狙った攻撃

※サイバー犯罪に関する用語で、社会的・政治的な主張を目的としたハッキング活動（ハクティビズム）を行う者のこと

出典：「「2013年度版　10大脅威」」2013.3 独立行政法人情報処理推進機構

【参考】ISMS認証取得組織数推移

- ISO27001認証の取得組織数の増加率が低くなっています。
- 大企業を中心とした初期の導入から、中小企業への導入にシフトし、マネジメントシステムの構築がひと段落したと考えられます。



出典:「認証取得組織数推移、認証機関別・県別認証取得組織数」　一般財団法人日本情報経済社会推進協会(JIPDEC)

急所：セキュリティ10大脅威

- セキュリティ10大脅威として、セキュリティの専門家が考える急所（リスク）を記載します。
- 2013年度版の10大脅威は、クライアントソフトの脆弱性を突いた攻撃が1位に挙げられています。

順位	脅威	影響		
		国家	企業	ユーザ
1	クライアントソフトの脆弱性を突いた攻撃		○	○
2	標的型諜報攻撃	○	○	
3	スマートデバイスを狙った悪意あるアプリの横行		○	○
4	ウィルスを使った遠隔操作		○	○
5	金銭窃取を目的としたウィルスの横行			○
6	予期せぬ業務停止		○	
7	ウェブサイトを狙った攻撃		○	○
8	パスワード流出の脅威		○	○
9	内部犯行		○	
10	フィッシング詐欺			○

出典：「「2013年度版　10大脅威」」2013.3 独立行政法人情報処理推進機構

10大脅威の変遷

- 10大脅威の変遷から、以前から存在していたリスクと新たなリスクが記載されていることが分かります。
- 次からのページで、特に「クライアントソフトの脆弱性をついた攻撃」と、「ウェブサイトを狙った攻撃」について補足します。

2008	2009	2010	2011	2012	2013	脅威
8	–	2	3	4	1	クライアントソフトの脆弱性を突いた攻撃
4	3	6	8	1	2	標的型諜報攻撃
–	–	–	4	6	3	スマートデバイスを狙った悪意あるアプリの横行
–	–	–	–	–	4	ウィルスを使った遠隔操作
–	–	3	–	–	5	金銭窃取を目的としたウィルスの横行
–	–	–	–	2	6	予期せぬ業務停止
2	2	1	2	5	7	ウェブサイトを狙った攻撃
–	–	8	–	9	8	パスワード流出の脅威
3	5	5	1	8	9	内部犯行
7	–	–	–	–	10	フィッシング詐欺

出典：「「2013年度版　10大脅威」」2013.3 独立行政法人情報処理推進機構

クライアントソフトの脆弱性を突いた攻撃

クライアントソフトの脆弱性を突いた攻撃

- 「攻撃されたことはない。」と考えていませんか？

今後の明確に分かっている脅威

- WindowsXP、Office2003のサポートが終了し、脆弱性を修正するプログラムが提供されなくなります。
- 4月以降に脆弱性が公開されたら、前頁のようにその脆弱性を狙って、攻撃が急増するでしょう。

Windows XPの脆弱性の数

- 2013年3月末時点でインターネットにアクセスする際のPCの約3割がMicrosoft Windows XPであるという調査結果もあります。
- WindowsXPの既知の脆弱性は、脆弱性の深刻度レベルIII(危険)が71%、レベルII(警告)が26%、レベルI(注意)が3%となっています。
- 97%がレベルII以上であり、攻撃に用いられた場合には重要なサービスを停止させられる、といった問題が発生する可能性が高くなります。

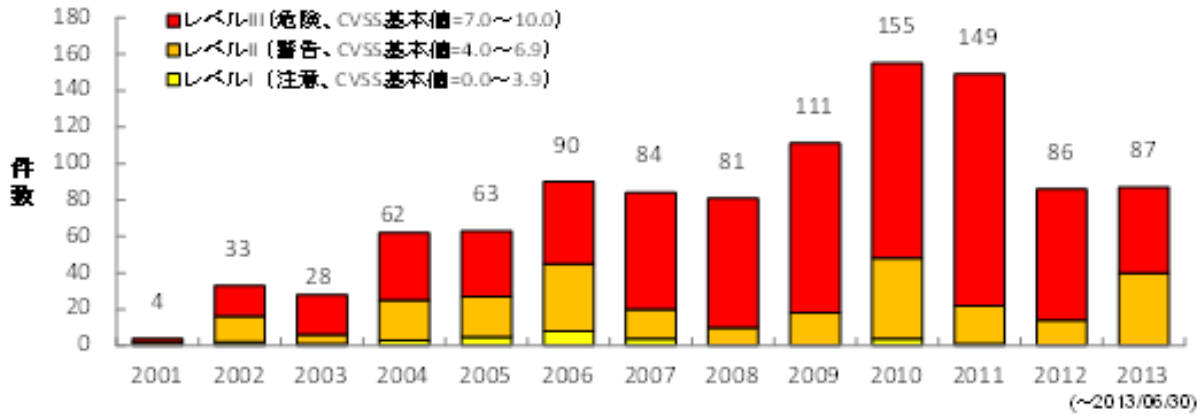


図1-3. Microsoft Windows XP 脆弱性対策情報の年別の深刻度割合

出典:「脆弱性対策情報データベースJVN iPediaの登録状況 2013年第1四半期(4月～6月)」2013.7 独立行政法人情報処理推進機構

脆弱性を狙われるクライアントソフトとは？

- Adobe Reader、Adobe Flash Player、Oracle Java (JRE) ,Micorosoft Officeといったクライアントソフトの脆弱性が悪用されやすい傾向にあります。
- クライアントソフトの脆弱性が攻撃に悪用される背景として以下が挙げられます。
  - 攻撃のターゲットになるユーザが多い
  - ファイルやウェブサイトを閲覧するといった操作が、ユーザがPCを利用する上で欠かせない操作であるため、攻撃の成功率が高くなる

参考文献:「「2013年度版　10大脅威」」2013.3 独立行政法人情報処理推進機構

クライアントソフトの脆弱性はどれぐらいの数存在するのか

NTT DATA

- 一般的に利用されるクライアントソフトの脆弱性の数の推移と脆弱性情報の深刻度割合を記載しました。
- Internet Explorar、電子申告で利用しているJavaの脆弱性が多いことが分かります。

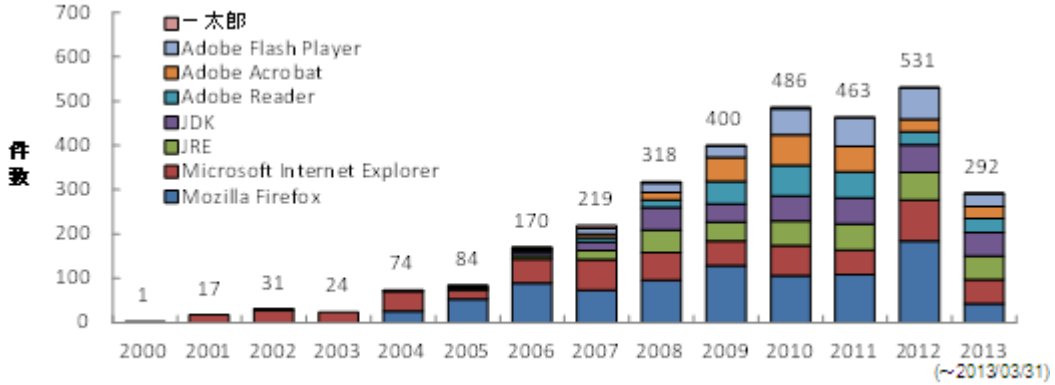


図2-1-1. PCで広く利用されているソフトウェアの脆弱性対策情報の登録件数の年別推移

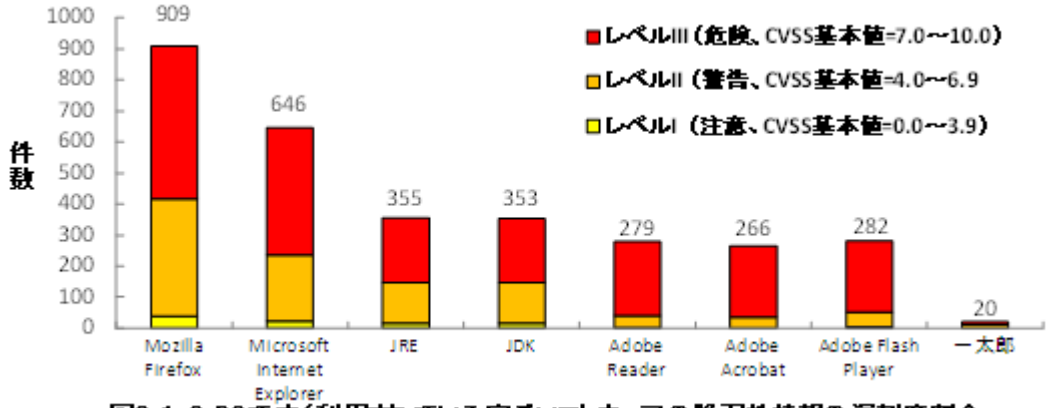


図2-1-2 PCで広く利用されている定番ソフトウェアの脆弱性情報の深刻度割合

・IPAでは、多くの利用者が影響を受けるセキュリティ対策情報を対象に、「重要なセキュリティ情報」として、セキュリティ上の問題と対策についての情報発信を行っています。

・2013年1月からの3ヶ月間では、既に攻撃が行われている等の「緊急」レベルの情報が8件、攻撃の情報は確認されていないが今後攻撃が行われる可能性がある「注意」レベルの情報が9件、計17件が公開されています。これは、2012年第4四半期（10月～12月）の発信件数が4件であったことと比較をすると4倍以上に急増しています。

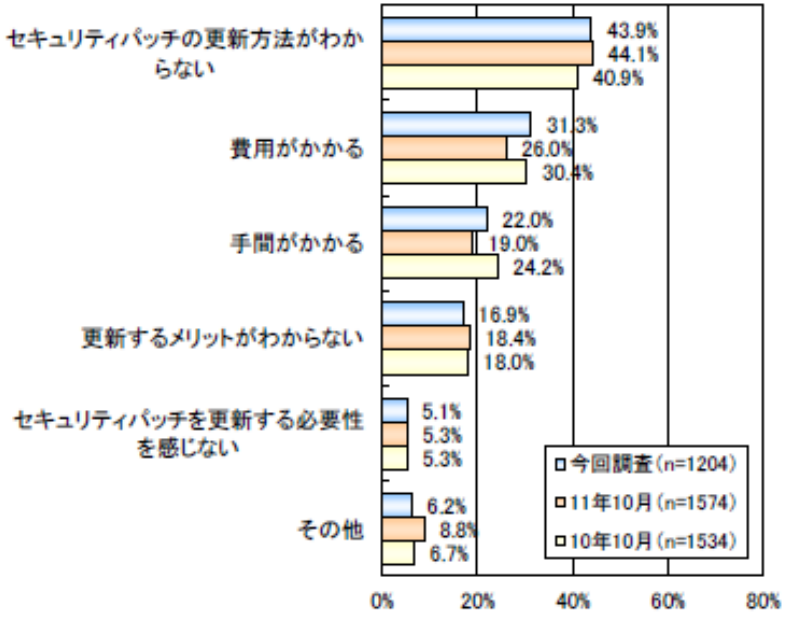
出典：「脆弱性対策情報データベースJVN iPediaの登録状況　2013年第1四半期（1月～3月）」2013.4 独立行政法人情報処理推進機構

パッチを実際に適用している人はどの程度いるのか

- 2012年度情報セキュリティの脅威に対する意識調査によると、セキュリティパッチを適用しないで使い続けることについては、約8割が問題ありと認識していますが、更新を実施しているのは6割という調査結果です。
- 更新をしない理由は、更新方法が分からないという理由が最も多く挙げられています。

セキュリティパッチの更新を実施しない理由

セキュリティパッチの更新を実施しない人ベース



マイクロソフト社以外のソフトウェアは、WindowsUpdateでは更新できないので、ソフトウェア毎に更新を実施してください。

出典:「2012年度情報セキュリティの脅威に対する意識調査 報告書」2012.12 独立行政法人情報処理推進機構

【参考】MyJVN バージョンチェッカー

■ IPAでは、使用しているソフトウェアのバージョンが最新であるか否か、容易に確認できる“MyJVNバージョンチェッカ”を公開していますので、脆弱性の有無を確認することができます。

脆弱性対策情報共有フレームワーク MyJVN:http://jvndb.jvn.jp/apis/myjvn/

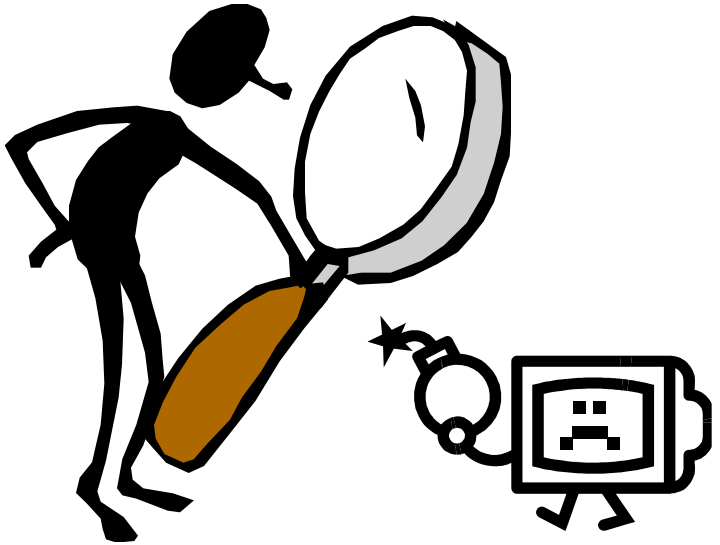
ウェブサイトを狙った攻撃

Webサイト、ネットワークの対策は大丈夫ですか？

NTT DATA

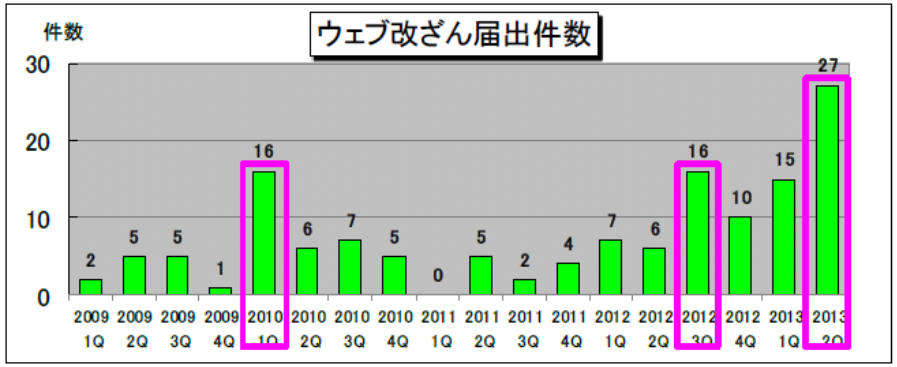
知彼知己、百戦不殆。

彼を知り己を知れば百戦殆うからず。

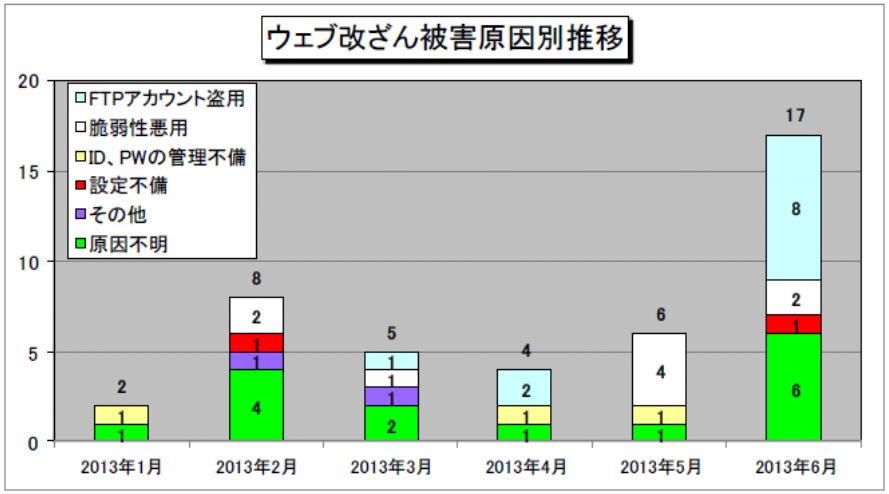


ウェブ改ざんの被害件数

- 2013年第2四半期（2013年4月～6月）では、『ウェブ改ざん』の被害の届出が27件ありました。
- ウェブサイトが改ざんされた主な原因として、「ウェブサーバーの脆弱性への攻撃」「ウェブサイト管理用パソコンがウイルスに感染することによるFTPパスワード漏えい」「サイト管理用FTPパスワードを容易に推測できてしまうよう不適切に設定」などが挙げられています。



ウェブ改ざん届出件数の推移

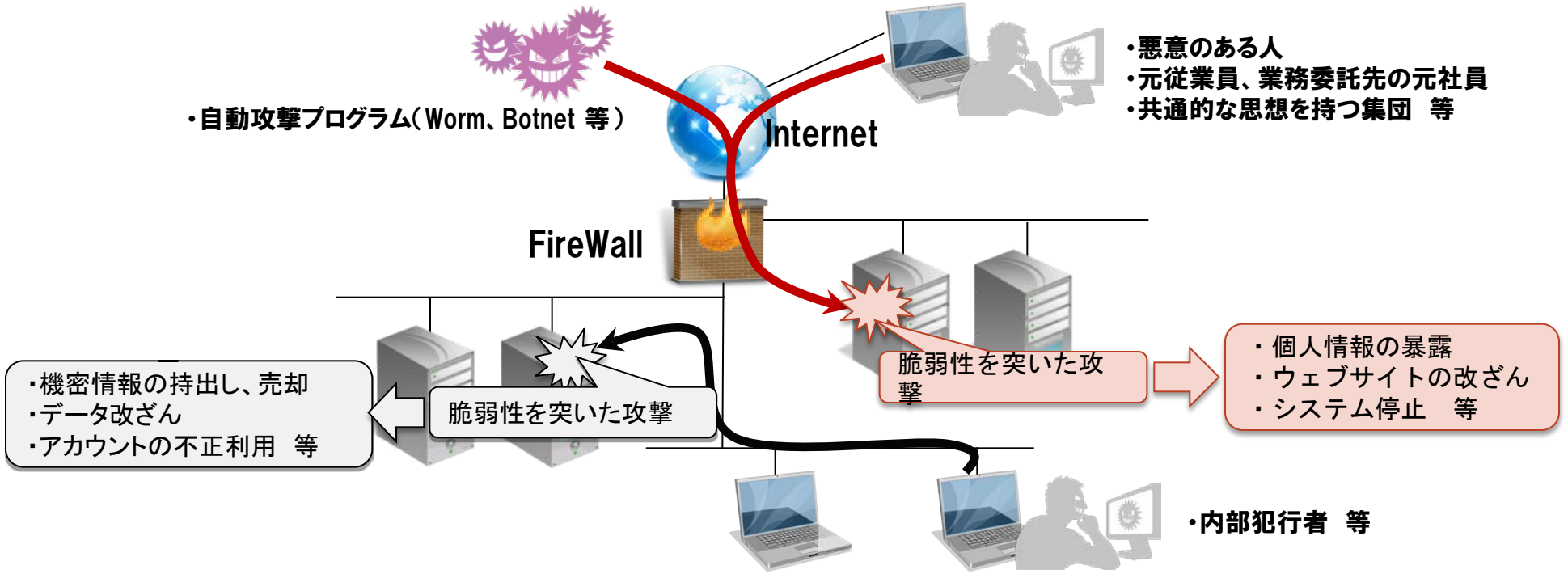


ウェブ改ざん被害原因別の推移

出典：「コンピュータウイルス・不正アクセス届出状況および相談受付状況[2013年第2四半期(4月～6月)]」2013.7独立行政法人情報処理推進機構
「「止まらないウェブ改ざん！」～ウェブサイトの管理の再検討を！～」2013.7独立行政法人情報処理推進機構

セキュリティ対策が不十分な場合

- 十分な対策が行われていない情報システムは、様々なメディアで報道されているように侵入、改ざん、情報漏えい等の様々な被害を受けます。
- 被害が顧客にまで及んだ場合、社会的信用を失い、大きな損失を被ります。



セキュリティ対策について

- セキュリティ対策は一つの企業、組織、担当、システム等において、複数の視点で見る必要があります。
- 技術的、専門的な知見が必要な箇所については、専門家の活用をお勧めします。

・Webアプリケーション診断

開発されたWebアプリケーションを実機へのアクセスにより診断

・ネットワーク診断

ネットワークシステム（ネットワーク機器、サーバ）を　実機へのアクセスにより診断

・セキュリティ監査

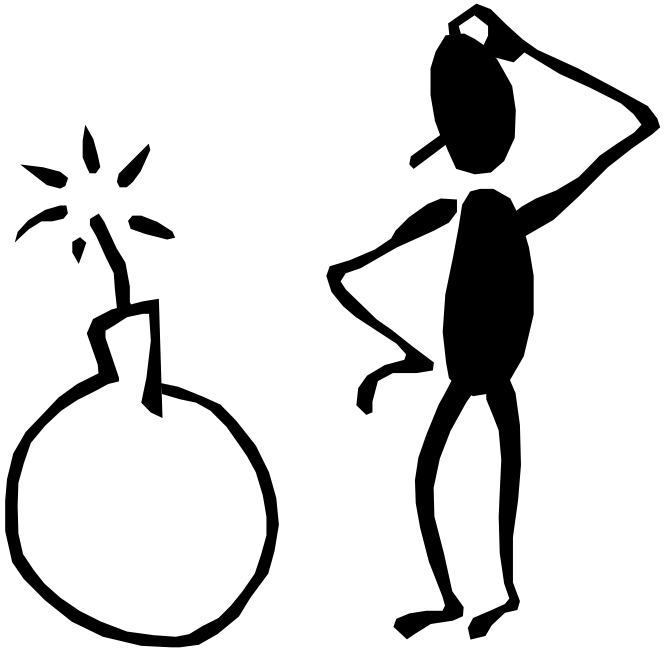
情報システムに関わる物理的環境、人的環境、技術的環境の運用・管理状況を文書確認、ヒアリング、現場確認等により監査

③事故事例をチェックする（同じ事象が起きないか）

事故の原因を急所(リスク)として考える。

If there is any way to do it wrong, he will.

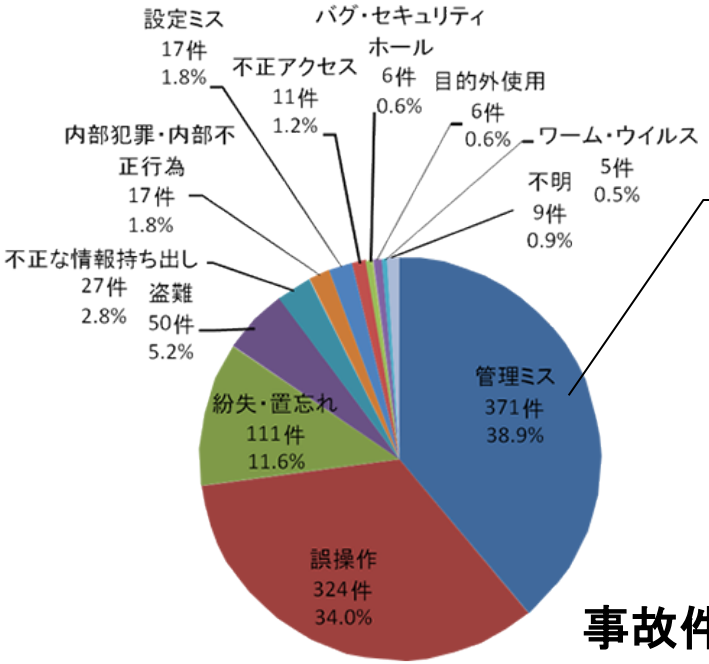
失敗する方法があれば、誰かはその方法でやる
(マーフィーの法則)



個人情報漏えいインシデントの原因

- 個人情報漏えいインシデントの発生原因はヒューマンエラーがほとんどです。
- 2012年度上半期速報版では、**誤操作、管理ミス、紛失・置忘れで、約85%**を占めています。
- つまり、誤操作、管理ミス、紛失・置忘れが発生するプロセスが急所だと考えることができます。

2012年上半期



マネジメントシステムの浸透、セキュリティ意識の向上によって、管理されている状況があるから、「管理ミス」という原因が出てくる点に注意してください。

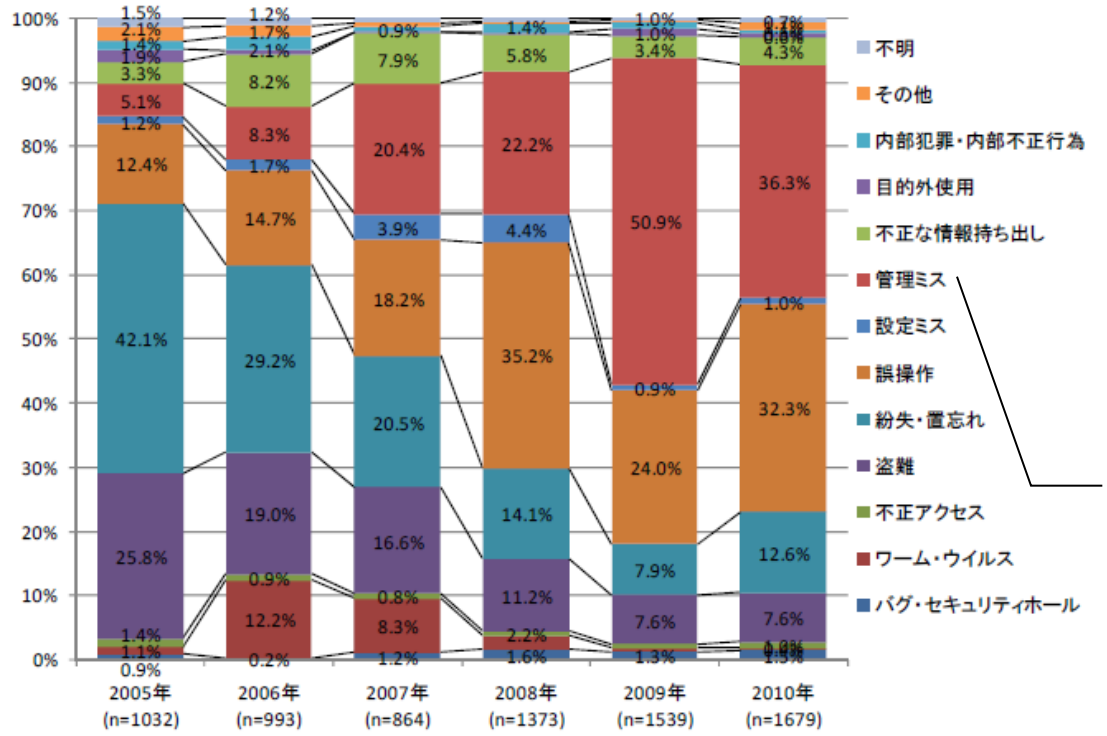
管理ミスの区分は、とは、ルールが整備されていない、もしくはルールは存在しているものの遵守されていないことによるインシデント。

事故件数：954件

出典：「2012年 情報セキュリティインシデントに関する調査報告書 上半期速報版」2013.4 NPO日本ネットワークセキュリティ協会

【参考】漏えい原因の経年変化

■ 10大脅威は変わっても、インシデントの発生原因はヒューマンエラーが多い。



漏えい原因比率の経年変化（件数）

以前は、管理ミスが少なく盗難が多い。

→管理ミスと盗難、紛失・置忘れがトレードしている可能性。（管理する仕組み、意識が浸透しているから、逆に、管理ミスという結果を検出することが可能）

出典：「2011年 情報セキュリティインシデントに関する調査報告書」2012.12 NPO日本ネットワークセキュリティ協会

本章のまとめ

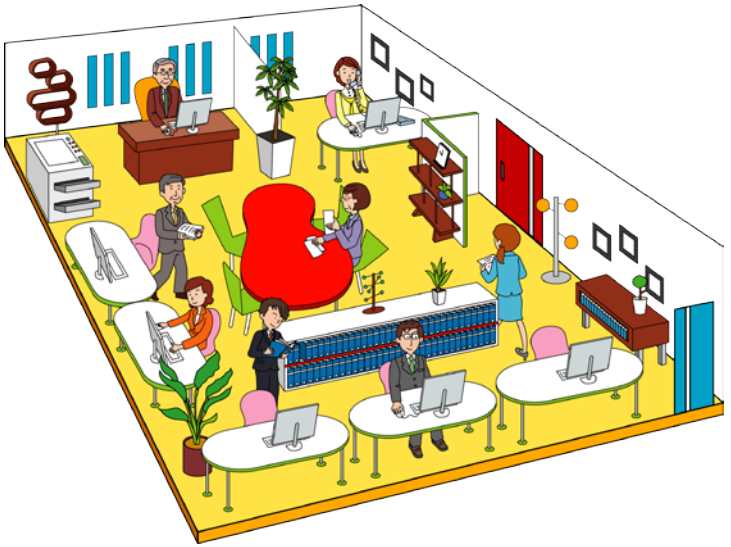
- 本章では会計事務所、顧問先の急所(リスク)に対する考え方について、説明しました。
- このアプローチは、①顧問先から預かった情報を守る、②自分の情報(営業秘密等)を守る、③企業の相談役、専門家として、顧問先にセキュリティを提案する、という3つの視点全てで有効です。
- なお、セキュリティリスクは変化しますので、できるだけ最新の情報を取得するようにしてください。

■急所(リスク)を洗い出す際の考え方

① **省庁、関連団体の資料、ガイドライン等を参照する**
リスクとリスク対応に関する基準を把握する

② **最新動向をチェックする(新しいリスクがないか)**
セキュリティリスクは変化する

③ **事故事例をチェックする(同じ事象が起きないか)**
失敗する方法があれば、誰かはその方法でやる



情報セキュリティの今後

業界を取り巻く代表的な3つの流れ

① マイナンバー制の開始

→2013年5月「マイナンバー」制度の関連法が国会で成立。

開始に伴って情報保護という観点からの懸念が議論されている。

国家管理への懸念、個人情報の追跡・突合に対する懸念、財産その他の被害への懸念などが挙げられ、マイナンバーが給付または還付措置と結びつくことによる「なりすまし」の広がりは、特に警戒すべきとされる。

今後税理士が法人、個人のマイナンバーの情報を預かることになった際、リスクが大きい。

参考文献:「「マイナンバー制度」の概要と課題」2013.7『税研』公益財団法人日本税務研究センター

② e-文書化の更なる進展

→今後、さらに文書の電子化が浸透する。

現状はあまり進展していないが、課題もある程度明確になっている。

電子帳簿は27%(国税庁調査では123千件)が実施しているが、書類のスキャナ保存まで実施している件数は0.05%以下。

スキャナ保存に対応する上での課題として、実施企業の35%が電子化の要件が厳しい、31%が税務署への申請・受付が簡単ではない、29%が電子帳簿保存法に完全対応したシステムが必要、と回答。

参考文献:「市場規模・ユーザ動向・e-文書法対応調査報告」2013.1『月刊IM』日本画像情報マネジメント協会

③ 技術の進展による端末小型化、クラウド化、低価格化

→技術の進歩とセキュリティリスクは表裏一体である。

スタイル変革の可能性

■ e-文書化の更なる進展、技術の進展によって、望むと望まざるにかかわらず、業務スタイルが変わってくるのではないでしょうか。

- インターネットにつながった端末しか必要ではなくなる（OSも、データも端末に入れなくて良くなる）
- 事務所内でサーバ機器、データを持たなくて良くなる
- すべて電子文書で申告が可能になる。
- 固定の事務所で業務を行うことが必要ではなくなる。

・
・
・

など

もうすでにこのスタイルをとっている方もいるようです。

参考文献:「【コラム】会計士、税理士のオフィスが無くなる時代」2013.2 カイケイ・ネット
「【コラム】会計士、税理士、弁護士…チームワークの時代」2013.3 カイケイ・ネット

さらに求められるセキュリティ

■ **技術の進歩とセキュリティリスクは表裏一体。必ず、新たなセキュリティリスクが発生する。**

- 電子的なデータが集積された場合は、紙での管理よりもさらに漏えいした場合の影響が大きい
- これまで以上の本人認証、人に応じた権限の付与の対策が必要
- 事務所、個人単位でのセキュリティ維持が困難になる
- 情報が漏えいすることを前提とした対策（暗号化、分散化）が必要となる
- 法的にも内容の改ざんが無いことを確保することが求められる
- など

完全なセキュリティは実在するのか？

The only truly secure computer is one buried in concrete, with the power turned off and the network cable cut.

本当に安全なコンピュータは、電源をオフにし、ネットワーク ケーブルを切断した状態で、コンクリートの中に埋められたコンピュータだけである

Scott Culp,10 Immutable Laws of Security Administration,Microsoft Tech net

セキュリティのためにビジネスを犠牲にしないように

- **セキュリティとは危険を回避することではなく、リスクを管理すること**です。
- **安全であっても、会社のビジネスに対して何の役にも立たないセキュリティは有害であるともいえます。**
- **有用なシステム、ネットワークのセキュリティは、決して完全ではありませんので、常にそのことを念頭に入れて、ビジネスのダイナミズムを失わないようにセキュリティの計画を策定してください。**

■ビジネス上の要求がセキュリティと対立することがあります

セキュリティは、それ自体が最終目標ではなく、あくまでもビジネスを支援する活動です。考えられる危険を挙げ、それをできる限りの範囲で軽減してください。

■ネットワークセキュリティは侵害されます

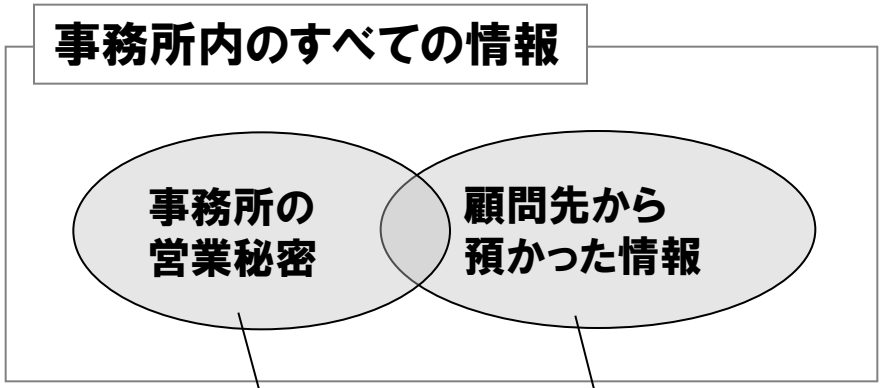
その原因は人間の攻撃かも、不可抗力かもしれませんが、ネットワークは何らかの形で侵害されます。侵害はちょっとした問題で済むかもしれないし、深刻な被害となるかもしれません。

侵害を検出し、調査し、回復させるために、不測の事態に対応できる計画を作成してください。

参考文献:「Scott Culp,10 Immutable Laws of Security Administration 」2000.11 Microsoft Tech net

まとめ

- 本章では、法律を中心に①顧問先から預かった情報を守る、②自分の情報（営業秘密等）を守るという視点について説明しました。
- 事務所内の営業秘密、顧問先から預かった情報以外にも守らなければならない情報はあると思いますが、いずれにしてもセキュリティの取り組みは行うべきだといえます。



①顧問先から預かった情報を守るという視点

税理士法上の守秘義務
＋税理士業務委託契約に基づく民法上、契約上の守秘義務
＋個人情報保護法上の責任

②自分の情報（営業秘密等）を守るという視点

不正競争防止法および営業秘密管理指針

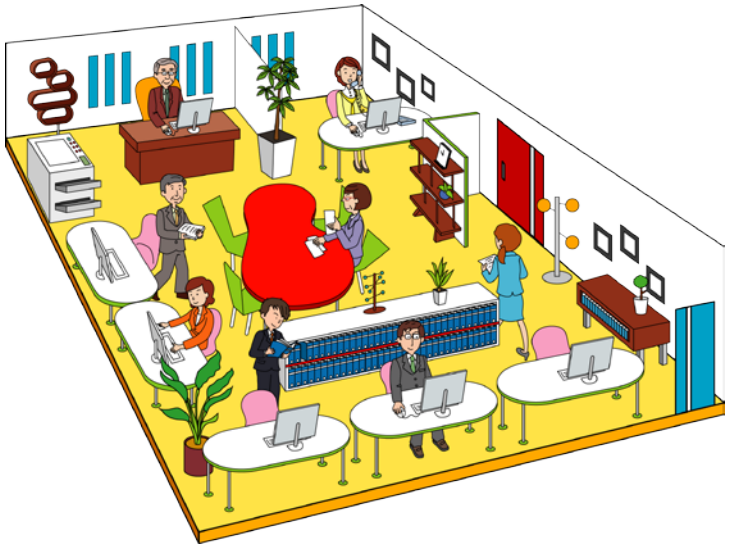
- 本章では会計事務所、顧問先の急所(リスク)に対する考え方について、説明しました。
- このアプローチは、①顧問先から預かった情報を守る、②自分の情報(営業秘密等)を守る、③企業の相談役、専門家として、顧問先にセキュリティを提案する、という3つの視点全てで有効です。
- なお、セキュリティリスクは変化しますので、できるだけ最新の情報を取得するようにしてください。

■急所（リスク）を洗い出す際の考え方

① 省庁、関連団体の資料、ガイドライン等を参照する
リスクとリスク対応に関する基準を把握する

② 最新動向をチェックする(新しいリスクがないか)
セキュリティリスクは変化する

③ 事故事例をチェックする(同じ事象が起きないか)
失敗する方法があれば、誰かはその方法でやる



- 本章では、業界を取り巻く流れと、情報セキュリティについて記載しました。
- セキュリティとは危険を回避することではなく、リスクを管理することです。
- 安全であっても、会社のビジネスに対して何の役にも立たないセキュリティは有害であるともいえます。
- 有用なシステム、ネットワークのセキュリティは、決して完全ではありませんので、常にそのことを念頭に入れて、ビジネスのダイナミズムを失わないようにセキュリティの計画を策定してください。

■ビジネス上の要求がセキュリティと対立することがあります

セキュリティは、それ自体が最終目標ではなく、あくまでもビジネスを支援する活動です。考えられる危険を挙げ、それをできる限りの範囲で軽減してください。

■ネットワークセキュリティは侵害されます

その原因は人間の攻撃かも、不可抗力かもしれませんが、ネットワークは何らかの形で侵害されます。侵害はちょっとした問題で済むかもしれないし、深刻な被害となるかもしれません。

侵害を検出し、調査し、回復させるために、不測の事態に対応できる計画を作成してください。

参考文献：「Scott Culp,10 Immutable Laws of Security Administration 」2000.11 Microsoft Tech net

全体を通じて

- 本日は、本資料を通じて①顧問先から預かった情報を守る、②自分の情報（営業秘密等）を守る、③企業の相談役、専門家として、顧問先にセキュリティを提案する、という3つの視点を説明しました。
- 特に今後、税理士先生が企業の相談役として税務面以外でも重要な役割を担うことになると思いますので、本資料の中で顧問先企業にとって有用と感じられる情報があれば提供してください。

ロケーション	視点	本資料で関連する章
税理士、税理士事務所内	①顧問先から預かった情報を守る	1章、2章、3章
	②自分の情報（営業秘密等）を守る	1章、2章、3章
顧問先	③企業の相談役、専門家として、顧問先にセキュリティを提案する	2章、3章
	④セキュリティ投資の関連税制の利用を提案する	対象外

終わりに

- 本資料では、急所(リスク)を洗い出す際の考え方について記載しましたが、絞り込み方、優先順位の考え方まで踏み込んでいません。
- さらに詳細を聞きたい場合は、

「NTTデータ先端技術　セキュリティ事業部」

までお問い合わせください。

エヌ・ティ・ティ・データ先端技術株式会社
（NTT DATA INTELLILINK CORPORATION）
03-5843-6800（代表）
information@intellilink.co.jp

ご清聴いただきまして、ありがとうございました。

参考文献

記載方法:「タイトル」，著者名，出版年.月，『雑誌名』，出版者

- 「今そこにある危機　税理士業務に伴う訴訟リスク」2004.4『税理』株式会社ぎょうせい
- 「守秘義務違反」　告 真希　『税理』2004.4 株式会社ぎょうせい
- 「顧客情報・個人情報の漏えい」阿部 隆幸 2006.12『税理』株式会社ぎょうせい
- 「法人税実務 社内情報セキュリティの確保策とその税務」鈴木 涼介 2006.7『税理』株式会社ぎょうせい
- 「個人情報の保護と内部統制」松嶋 隆弘 2007.5,2007.6『税理』株式会社ぎょうせい
- 「「マイナンバー制度」の概要と課題」2013.7『税研 』公益財団法人日本税務研究センター
- 「税理士職業賠償責任保険 情報漏えい担保特約 パンフレット」株式会社日税連保険サービス
- 「平成一〇年(ワ)第一四〇三号　不正競争防止法に基づく差止請求事件」
- 「市場規模・ユーザ動向・e-文書法対応調査報告」2013.1『月刊IM 』日本画像情報マネジメント協会
- 「営業秘密管理指針」2011.12 経済産業省
- 「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」2009.10 経済産業省
- 「「2013年度版　10大脅威」」2013.3 独立行政法人情報処理推進機構
- 「2012年度情報セキュリティの脅威に対する意識調査 報告書」2012.12 独立行政法人情報処理推進機構
- 「2011年度情報セキュリティ事象被害状況調査」2012.12 独立行政法人情報処理推進機構
- 「脆弱性対策情報データベースJVN iPediaの登録状況　2013年第1四半期（1月～3月）」2013.4 独立行政法人情報処理推進機構
- 「脆弱性対策情報データベースJVN iPediaの登録状況　2013年第2四半期（4月～6月）」2013.7 独立行政法人情報処理推進機構
- 「コンピュータウイルス・不正アクセス届出状況および相談受付状況[2013年第2四半期(4月～6月)]」2013.7独立行政法人情報処理推進機構
- 「「 止まらないウェブ改ざん！ 」～ウェブサイトの管理の再検討を！～」2013.7独立行政法人情報処理推進機構
- 「2012年 情報セキュリティインシデントに関する調査報告書 上半期速報版」2013.4 NPO日本ネットワークセキュリティ協会
- 「2011年 情報セキュリティインシデントに関する調査報告書」2012.12 NPO日本ネットワークセキュリティ協会
- 「認証取得組織数推移、認証機関別・県別認証取得組織数」　2013.7 一般財団法人日本情報経済社会推進協会(JIPDEC)
- 「【コラム】会計士、税理士のオフィスが無くなる時代」2013.2 カイケイ・ネット
- 「【コラム】会計士、税理士、弁護士…チームワークの時代」2013.3 カイケイ・ネット
- 「Scott Culp,10 Immutable Laws of Security Administration 」2000.11 Microsoft Tech net

NTT DATA

Global IT Innovator