第6回JSSMセキュリティ公開討論会　　「情報セキュリティの日」制定記念セミナー

2011年情報セキュリティその事例と考察

ーサイバー攻撃、スマホ、内部犯罪、クラウドー

社団法人　情報セキュリティ相談センター　　事務局長
ACCS（社団法人　コンピュータソフトウェア著作権協会）技術顧問
金融ニュービジネス＆テクノロジー研究会　常任アドバイザー
JSSM「先端技術・情報犯罪とセキュリティ研究部会」主査
CFE（公認不正検査士）

萩原　栄幸

Mail:　jssm@hoshizora.jp

2012年2月18日

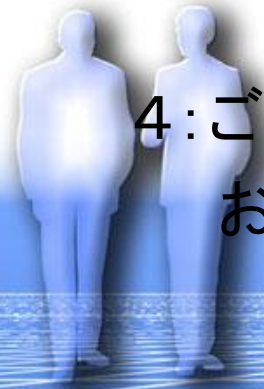
本資料の取り扱い

1：本資料はJSSMの正式見解を述べたものではありません。

2：本資料の全体もしくは一部のコピーや転載を行う場合は
必ず作成者に承認を得てください。無断転載は禁止です。
連絡先　萩原栄幸　mail:　jssm@hoshizora.jp

3：リンクや論文の根拠先としてURLを記載するなどの行為
はご自由に活用頂ければと存じます。

4：ご不明な点やご意見などございましたら上記連絡先まで
お願い致します。



最近のサイバー攻撃

昨年の11月15日朝日新聞朝刊3面記事に大きく「サイバー攻撃」が取り上げられ、講師のコメントが掲載されました。
翌月12月19日日本経済新聞夕刊3面記事に「サイバー攻撃」特集が掲載され、ここでもコメントが載りました。

その他、NHK、テレ朝、読売新聞、毎日新聞など取材攻勢がしばらく続き、仕事に差しさわりが出るくらいになりました。

サイバー犯罪はその昔、国会議員の中でもサイバーテロ防止の超党派会合にも呼ばれ、国民の意識が高まりましたが、その後一時廃れはじめたものの現在はホットな話題として注目を浴びています。

サイバー攻撃とは

意味・・・

脆弱性を悪用し、複数の既存攻撃を組み合わせ、ソーシャルエンジニアリングにより特定企業や個人をねらい、対応が難しく執拗な攻撃が出現してきている。この新しいサイバー攻撃は2010年の春頃から海外ではAPT(Advanced Persistent Threats)と呼ばれている。

IPAでは、システムへの潜入等の「共通攻撃手法」と情報窃取等の目標に応じた「個別攻撃手法」から構成される攻撃であると分析した。このように「共通攻撃手法」と「個別攻撃手法」を持った攻撃をIPAでは、『新しいタイプの攻撃』と呼ぶ。

IPA「新しいタイプの攻撃」レポートから抜粋

個人だから･･･零細企業だから･･･自宅だから･･･

サイバー攻撃は関係がない

これは大きな誤りです！！！

今後の企業防衛のありかた

大企業から中小零細企業までその情報セキュリティのあり方を
今一度、再検討すべきではないでしょうか？

例えば・・・今までは正当な利用者と欺いて侵入してきた犯罪者の
区別がつくことを考えてきた・・・そういう企業、団体が圧倒的に多かった
のではないでしょうか？

今後は正当なIDとパスワードでシステムに来た場合において
「本当に本人なのか？」
「本人であっても悪さをしない保証はない」
という観点で考えた場合、今までのセキュリティではまずいと思い
ませんか？

キーワード　「振る舞い防御」「多層防御」

今までの攻撃、例えば、それがガンブラー攻撃でも、キーロガーでも、スパイウェアでも、ショルダーハッキング（盗み見行為）でも、押し並べて「そこに戦術はあっても戦略がなかった」・・・だから

対応策も（どんな技術的な脆弱だとしても）ある意味、単純に対応出来た・・・でも、今後はあらゆる面で警戒し、それは技術的なものソフト、ハード、ネットワーク、人（メンタル、環境、金銭的なものを含めたトラブル要因）などを統合的に監視する必要がでてくる。

しかも一度、管理者権限などを盗み侵入に成功すると議員サーバーのようにこっそり、密かに身を隠し、深海の「あんこう」のごとく、情報が

目の前を通るとこっそりコピーして、こっそり送信していく・・・
これを何年も何年も繰り返していく・・・

こういう犯罪を防御するのは100%の対応策はない・・・
だから多層防御して全体の防衛を99．99%にするしかない。
（例えば7割の防御しか出来ない対応策（策としては劣悪レベル）
　を5層に重ねれば・・・数学上では99.8%の防御となる。通常なら
　1つの対応策で99%程度とすると5層なら99．99999999%となる）

そういう意味で今後のログ管理はその重要性は高まることは
あっても下がることはないと思われる。

しかも単一な管理ではなく、多層防御的な管理を目指すのは
極めて重要だと思う。

パスワードの考え方

中小企業でも最近はパスワード管理を相当重視しているようで
感心しています。でも、システムでガードするにはお金と人とシステム
の導入が必要なので、だいたいが紙（社則とか○○規定とかいう）
でのルールなのです。それでも形（成果物）しか見ないISMSとか
Pマークとかいう代物はセーフです（あっ！言い過ぎです！すみません）
・・・でもね・・・実際は・・・個人の方も極めて重要なことです・・・
多くのルール
8文字以上英字小文字大文字＋数字＋特殊文字を混在させ、意味の
ある単語（人名、地名、商品名など）は使わない、車の番号や電話番号
などの個人にとっての意味のある数字も使わないこと。過去更新した
パスワードは5回まで遡り同じものは使わない・・・などなど・・・
さて問題です。ここで仮にパスワード8文字として英字26種×2（大文字
と小文字）＋数字10種＋特殊文字を計算を簡単にするため8種とする
ならそのパスワードの種類は70の8乗（＝約576兆通り）となります。

以前、パスワードをクラックするスピードを計算した事があります。
パソコンのパスワードをクラックする途中でインターバルをとり、
その間のクラック回数を表示させました。すると約7年前のパソコン
でアバウトですがざっと100万回／秒程度でした。（実測値）
その時のパソコンのスペックを今のパソコンの処理能力で換算するなら
これもアバウトですが大よそ600万回～900万回です。
（昨年のレベルで購入出来る最高に近いスペックで）
仮に1000万回とします。すると8文字の平均クラック時間は（電卓を
お持ちなら簡単に計算できます）約0．9年かかります。これを例えば
3か月に1回変更するなら・・・まあ、OKなんでしょうか・・・

というのは「机上の空論」です。ここには犯罪者の目線がないからです。

人は様々、この世界で一番重要なのは「人」・・・重要とは
一番「やっかいなもの」という意味でもある。

・・・啓蒙活動は中小でも大企業でもNASAでも
重要です。特に中小にとってはお金をそれほどかけず効果
も大きい（100%の効果は無理だけど70%の効果なら期待！）
その啓蒙活動を「かたちだけ」行うと・・・ある中堅の上場企業に
て役員会や人事の了解のもとパスワードクラックを従業員
に対して実施・・・3分ももたない従業員が続出！！！
これではねえ・・・

内部犯罪調査で気が付くこと・・・犯人の目線で考えると・・・
パスワードの場合、現場で実際に泥水を漱ぎながら調査すると
一番多いケース・・・同僚（上司）のパスワードを盗む方法
横に座っていてとなりから覗き見、かっこよくいうならショルダーハッキング・・・でも8文字を追うのは相当大変なんです。そこで
割り切って最初の半分いやもっと少なくて3文字だけ追う・・・
これなら実際に行ってみると判りますが比較的簡単です。
・・・で判ったとします。
ではそこからクラックツールを仕掛けて試すと時間はどのくらいでしょうか全体の3／8が判ったので残りは5／8だから0．9年×5／8で約7カ月弱・・・もしこう計算したなら・・・おいおい！
ですね。実際計算すると判りますが何とカップラーメンの待ち時間である3分より更に短い時間である1分24秒が平均クラック時間！
机上での自称専門家にこういう発想は期待しないでください

内部犯罪抑止の側面支援でもっとも大事なこと･･･
メンタルケアってご存知ですか？実は4年前から金融セミナーでお伝えしています。
簡単にご説明致しましょう！！！
「善意の確信犯は要注意！」この本当の意味とは･･

システムで防御＋メンタルでの不正抑止
この両輪で大きな改善効果が生まれます！
多層防御の1つになるのです！

第二世代、第三世代のサイバー攻撃は様々な予測がたてられますが・・・振る舞い防御も重要な考えの1つである多層防御の1層になると思われます！

前頁に記載の人間の精神的な脆弱性を巧みに突いたサイバー攻撃も当然予測して対応を考えてください。
ログも単純に収集するだけのものでは時代遅れです！

なりすましの防御だけでなく正当な権限者のアクセス防御をどう実装していくのか・・・この考えを頭の片隅において下さい！

スマートフォンのセキュリティ

JSSEC（日本スマートフォンセキュリティフォーラム）の技術WGのメンバーとして・・・

世界ではじめて実証実験結果をKDDI研究所の竹森工学博士と纏めた結果をネットに公開しました
この記事を踏まえて解説致します。

2011年12月26日
萩原栄幸が斬る！ IT時事刻々：
Android OSから見たセキュリティ対策ソフトの制約
http://www.itmedia.co.jp/enterprise/articles/1112/26/news015.html

抜粋記事　Androidにおける不正プログラムの危険性

まず誤解を恐れずに言うと、Androidではその設計からウイルス感染はまず起こり得ないのだ。（注意：ウイルスとは、ファイルやインターネットなどを介在して自動的に拡散するものを指す。ここで悪性ソフト全般を指すマルウェアという用語がある。Androidにおいては利用者が明示的にインストールを行わないと、自らが独自に感染することが出来ない機構を持つ。もちろん、研究所でわざと実行環境を作成してのウイルス感染はできるが、一般にご利用のAndroidにおいてはまずあり得ない。あるのはマルウェアへの感染である。）

このマルウェアの感染経路には通常、以下の3つの種類が考えられる。

１：Android Marketなどのさまざまなアプリケーションストアからマルウェアをインストールする

２：メール添付マルウェアをインストールする

３：USB接続したPCからマルウェアをインストールする

これらの感染経路において、提供側の責任になる（1）のケースでは一部の悪質なMarketを除けばさまざまな取り組みが行われている。

例えばGoogleは、

開発者登録にクレジットカードが必要で、ある程度の身元保証を義務としており、金銭も徴収することでマルウェアの掲載頻度をなるべく少なくしている

抜粋記事　Androidにおける不正プログラムの危険性

ユーザーから指摘を受けた場合は、迅速にマルウェアを駆除するなどの事後対策を行っており、感染者を極力少なくしている

また、「au one Market」では信頼できるアプリケーション提供者であることの身元確認を行っている。アプリケーションを掲載する際に、セキュリティチェックを行う事前対策を持っている アプリケーションストアから駆除されれば、“横”への広がりはなくなり、ネットワーク上で生き残るPC向けウイルスに比べて、拡散期間が短い特徴がある。これは、PCにはないAndroidの安全な機構であり、これまで爆発的な感染が生じていない理由である。

抜粋記事　マルウェアが実際に感染する仕組み

Androidはよく知られているように、Linux OSをベースとしている。Linux OS上に利用したい機能や情報へのアクセスを承認するパーミッション可変型のサンドボックスを構築したOSがAndroidというわけだ。

サンドボックスとはWikipediaでは、「外部から受け取ったプログラムを保護された領域で動作させることによってシステムが不正に操作されるのを防ぐセキュリティモデルのこと」と説明されている。つまり、この領域でしか通常は実行できないこととなる。しかしAndroidの場合、アプリケーションが利用する機能や情報を利用者が承認する形を取っており、サンドボックスに穴を開けることができる。ある意味で「安全性」と「利便性」のトレードオフを利用者に委託した自己責任モデルである。

Androidにおける感染としては、「パーミッション悪用型」と「脆弱性攻撃型」の2つの形態が考えられる。この2つの解説をする前に、このパーミッションの利用実態を理解しておかねばならないだろう。

抜粋記事　驚くべきパーミッションの利用状況

KDDI研究所の調査によると、2011年8月に、Android Market上の無料アプリケーション980個のパーミッションの利用率を調査した結果が発表された。その中でアプリケーションの利用でどうにも不要と思われるパーミッションが多数発見されている。

2011年11月28日の読売新聞夕刊の社会面でも大きく取り上げられているが、電話帳の中身を読み取るもの11%、位置情報を読み取るもの27%、スマートフォンの電話番号やSIM情報を読み取るものは58%にも上っているのだ。また新聞には掲載されていないがスマートフォン起動時にアプリケーションを自動起動しているものも12.4%もあり、実に不気味な状況となっている。なぜ単純なゲームソフトにこういう機能が必要なのか――これらの趣旨に関する説明がないまま、画面に承認するかしないかの同意を求められて、OKボタンを押す仕組みとなっており、一度押せば全てが承認されたというような仕組みとなっている。

さらに重要なことは、そのパーミッションの機能の果たす役割や影響を、アプリケーション制作会社や制作者本人も意識していないという状況となっているのだ。彼らの中には、契約した広告会社のプログラムの特性を知らないままアプリケーション作成時に組み込むケースが多くみられ、アプリケーションの趣旨と表示されるパーミッションのギャップが生じてしまい、ユーザーに不審や不安を与えている実態がある。

専門家の素人化というのはちょっと言い過ぎかもしれないがそういう状況が今の現実なのだ。

抜粋記事　Androidの実行権限について

なるべく平易に説明するなら、Androidの実行権限には3種類ある。

１：一般権限……アプリケーション開発者が自己署名してMarketプレイスを通じて（一部不法Marketもあるようだが）配布されるアプリケーション。「Dalvik」サンドボックス内で動作し、利用者承認のパーミッションの機能を持つ。保存先は「/data/app」「/data/app-private」「SDカード」の3つ

２：システム権限（管理者権限と混同されがちだが異なる）……「/system」ディレクトリ配下にインストールされたアプリケーション、もしくは「SharedUserID='android.uid.system'」が設定されたアプリケーションに与えられる権限。Androidが持つ特別な操作を実現できるSignatureOrSystemパーミッションを利用できる

３：管理者権限……Androidの領域外でLinuxのroot権限が割り当てられたものでLinuxコマンドを利用できる。

これらの権限区分において「ウイルス対策ソフト」（正確にはマルウェア対策ソフト）がどこで動作しているかというと、調査した全てのソフトが「一般権限」であった。世界中の全てのソフトで調査をしたものではないが、有名なものは調べている。ここから、以下のような疑問を生じてしまうのである。

抜粋記事　マルウェア対策ソフトの限界

1.前述の一般権限での保存先の1つにある「/data/app-private」内は、一般権限ではコード自体をスキャンできない。スキャンできるのは「/data/app」もしくは「SDカード」だけである。それではこの領域（/data/app-private）への書き込みはどうすればいいか。この領域のアプリケーションを専門用語で「フォワードロックアプリ」というが、一番簡単な方法はAndroid Marketに投稿するときに「著作権管理フラグ」をオンにすればいい。これだけでコード検証型のスキャン対象から外れてしまうのである。

2.一般権限でマルウェアを駆除しようとするなら、PackageManagerにアンインストールを依頼して、利用者による手動操作を待つことになる。マルウェアがインストールされただけではまだ攻撃は行われない。起動して初めて攻撃が行われ、さまざまな影響を及ぼす結果をもたらす。だが、Androidにはアプリを自動起動させる仕組みが豊富にある。例えば「端末の起動」「SMS受信」「電話発呼」などである。実験ではインストールしてから自動起動されるまで約1秒のものも見つかった。この間に利用者は画面でアプリの削除要求をしなければいけない。実際に1秒以内でのユーザー操作は不可能であり、被害に遭ってからの事後の駆除となり意味がなくなる。

抜粋記事　マルウェア対策ソフトの限界

3.一般権限ではメモリダンプやリアルタイムでの通信モニタも使えず、他のアプリケーションの挙動を監視することは不可能だ。例えば、一般のWebブラウザを使った悪性Webサイトへの接続制限では、接続した後で悪性URLの場合にはWebブラウザを停止させる。これは、Logcatログを監視してアクセス履歴をチェックしているだけなので、実際問題としては接続して事件が発生してから停止させるため、その時は既に“後の祭り”なのである。

またインストールでのスキャンはその仕組み上、ウイルス対策ソフトはインストールが完了したブロードキャストを拾って検査するので、その時は既に「/data/app」やSDカードに展開済み。もし「/system/app」にインストールされてしまった場合には、一般権限では駆除できなくなる。そこからスキャンして何か意味があるのだろうか（もちろん、「/data」以下にインストールされたアプリが、継続的な情報漏えいや外部攻撃を行うものであれば、手動による駆除も意義は大きい）。

なお、アプリがインストールされる先のほとんどは、「/data」配下であることを述べておく。ここにインストールされるアプリは、アンインストール操作により、クリーンに駆除できる。PCの場合には、感染による影響が残ってしまうことが多いのに対して、Androidの安全機構の一つであると言える。

抜粋記事　かなり堅牢な“スッピン”のAndroid

Android自体は実は堅牢な仕組みである。その理由は、自動感染型ウイルスが存在しない。

スマートフォンを狙う不正プログラムやマルウェアが急増しているといわれており、これ自体は確かだが、絶対数からみると、マルウェアの数はPCに比べると極めて少ない。著者が独自で入手した情報は、10月時点ではその比率は「1600（PC）：1（スマートフォン）」だった。これには調査対象に亜種が含まれていない。亜種を含むと、その差は「約42000：1」となる。このように情報源によって数字が相当に異なるほど、スマートフォンのマルウェアの数は少ないということだ（けたが違いすぎるのである）。

全体的な傾向としては、スマートフォンはPCに近づいているが、まだまだスマートフォンのマルウェアに遭遇したユーザーは希少な存在である。実際にKDDI研究所が、会社や個人でスマートフォンのマルウェアに遭遇して、実際に被害を受けたかの問いかけでは実被害を訴えたユーザーはいなかった。今後はさらにその差は縮小するだろうが、PCと肩を並べるにはもう少し時間がかかりそうだと筆者は感じている。

抜粋記事　かなり堅牢な“スッピン”のAndroid

現実にAndroid Marketにマルウェアが掲載されることはほとんどなく、通信事業者の独自のMarketでも同様だ。それよりは、グレーなアプリケーション（見解の相違はあるが、例えば端末改造ツールやシャッター音の無いカメラなど）は今後も増加すると思われる。

セキュリティがほとんど考慮されないようなMarketプレイスでの感染事例が増加する可能性がある。Android向けウイルス対策ソフトにPCと同じレベルの防御力を期待している一部のユーザーが、対策ソフトをインストールすることで、逆に「危険なMarketプレイスに行っても安全」と思い込む場合を懸念している。本記事はこのユーザーへの注意喚起を主な目的にしている。

抜粋記事　マルウェア対策ソフトの意義をどう考える？

Androidのマルウェア対策ソフトに文字通りの機能を期待しても、それは“ないものねだり”となる。ただし保険として（偽対策ソフトを除けば）考えればないよりはいい。PCと違い、機能に限界があると理解した上で利用すべきだろう。過去に出現した手動起動型、もしくは時間をかけて自動起動するマルウェアには有効といった程度だと割り切るべきだ。筆者としては今より優秀な製品が登場することを期待したい。

特に有料ソフトであれば、ウイルス対策以外にもさまざまな機能を数多く搭載しているので、そちらを期待しての購入ならユーザーも納得できるだろう。「リモートロック」「リモート消去」「ログ管理」「盗難対策」「バックアップ機能」「データリカバリ対策」など、メーカーによって呼び方も機能も多種多様だ。

以上の点を踏まえてユーザーに知ってほしいのは、ウイルス対策ソフトの現状は“ないよりはまし”程度であるということ。それよりも、世間で評判になっている一部の悪質Marketは、セキュリティ管理がほとんどされていないので、絶対にアクセスしないことの方が遥かに有効な安全対策となる。また、「メールの添付ファイルに用心する」「怪しいサイトには行かない」といったPCでは常識の、危険だと思われる行為をスマートフォンでもしないことが重要である。スマートフォンを有効に利用していくという前向きの姿勢でぜひセキュリティ対策を心がけてほしい。

抜粋記事　マルウェア対策ソフトの意義をどう考える？

日本スマートフォンセキュリティフォーラム（JSSEC）でも「スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン」を提供している。手前みそで申し訳ないが、無料なのでぜひこのガイドも併せて活用していただきたい。

対策ソフトメーカーに対しては、「できること」「できないこと」をより明確に表現（技術者が不勉強な場合もあるが）していただきたい。一部製品の宣伝では「誇大広告ではないか？」と思われるケースも見受けられる。

抜粋記事　問題は山積み

Androidには、本稿で取り上げたウイルス対策ソフト以外にも検討課題が多い。無線LANやWi-Fiにおけるセキュリティ問題もあるが、筆者が非常に懸念しているのが「著作権管理」である。例えば、先日のJSSECの発表の場でSony Ericssonの方（米国在住）が「ゲームでテトリスを検索すると3000種類以上ものゲームが見つかる」と話しており、この中で「正規の著作権を保持したテトリスはどれか？」と問いに、筆者はまったく分からなかった。ほとんどが、本家のソースをコピーしたのではと疑われるものや、そっくりな機能を持ったアプリが無料ゲームとして提供されている。「いったい本家のアプリはどれ？」という状況で、これは有名なゲームに限った話ではない。

Androidの世界では、制作者自身が何カ月も苦心して作成したゲームや優良ツールが簡単に盗まれ、別名でMarketに出されるケースも多いと聞く。この現状をどう改善すべきなのか。そもそも本当にあなたが「正規の制作者」だと、どのように主張すればよいのか――デジタル認証といった技術論もさることながら、商流や物流、そして情流を鑑みるとまだまだ問題が山積されているのである。以前にも本コーナーで記したが、ソフトの購入とはモノを購入することではなく、使用する権利を購入するという事をどうやったら実効力のあるものにできるのだろうか。まだまだ道は長い。

内部犯罪：本当の怖さを知らない

情報漏洩事件が、モラル欠落企業が、多発しています。。。そして残念なことに一部の会社は目の前の面子や利益を優先させた結果、結局後々まで悔いを残す結果となっています。
なぜ、雪印があそこまで落ちたのか？
なぜ、浅田農産の会長夫妻が自殺にまで追い詰められていったのか？
なぜ、三菱ふそうが陰湿な隠しをしたのか？
なぜ、不二家があそこまで落ちてしまったのか？
なぜ、船場吉兆は・・・
なぜ、三笠フーズは・・・

その時になった時、どう対応すべきか？あなたの会社はその机上訓練ができていますか？前述の通り・・・
日本：そうならない為に防止策、予防策を考える！
欧米：そうなった時、被害を最小限に食い止める対応策を考える！

金融機関向け「情報セキュリティ管理者養成コース」を14年努めていて・・・雑感

１：１０年以上もの昔・・・ある地銀の頭取はこうお話されました・・・「うちの行員に悪さをしようとする人間は絶対にいない！」・・・私は記者の前には我慢しましたが・・・

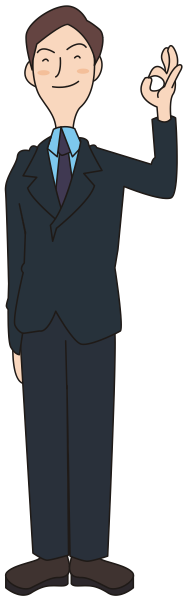
「おいおい！そんな事なぜあなたが判るのか？その言葉は絶対に「嘘」と確信します。」と・・・数年後、その通りになりました・・・

２：内部犯罪・・・これはご存知の通り、めったに表には出ません

しかし実体を知っている私は８年ほど前からセミナーにおいて「実際には内部犯罪が圧倒的に多いです。件数では控えめにみても７割以上ではないでしょうか・・・・・」

３：外部からのアタック、HPの改ざん、インターネットの各種のセキュリティ上の脆弱性、・・・・・これらも当然大事です。でも、日本人のカルチャーには馴染まないかも知れませんが、部下、同僚、上司、そして役員などありとあらゆるケースを想定した内部通報者制度の問題や内部統制上の問題、モラルの問題、コンプライアンス等の問題・・・いまや何をとっても軽視すべきものはありません。

米国の金融機関ではたった１人の若い行員の不正で銀行そのものが破綻になった例があるのをご存知でしょうか？



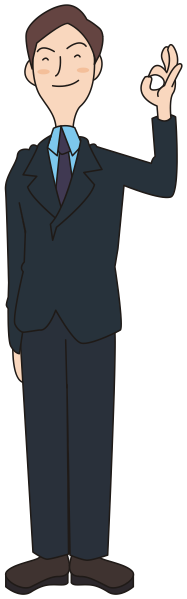
内部犯罪が企業を破滅させる可能性が高くなっています！

現実に、私共への相談も不正アクセスやHP改ざんなどより従業員の不正調査、犯人探しのご依頼など「内部不正」によると思われる方が圧倒的に多くなっています！

米国の調査会社によると退職した従業員の59%がデータの不正持ち出しに関与したという・・・

（2009年2月Ponemon Institute調査）

JNSAの統計数字を分析すると・・・



日本ネットワークセキュリティ協会（JNSA）が毎年発行している「情報セキュリティインシデントに関する調査報告書」（2011年8月24日改訂版）によれば、情報漏えい事件・事故のうち、「内部不正・内部犯罪」が原因となって発生したものは全体の0.5%を占めていました。「大したことはない」という方・・・実は、この報告書を別の視点から読み解くと、全く違う顔が浮かび上がるのです。
分類を「内部要因」「外部要因」の2つに別けます・・・すると

9割が「内部」……故意か過失かにかかわらず、漏えいの原因が企業の「内部」と「外部」のどちらにあるかで見ると、グレーな事案（双方に跨ると考えられるもの）を除いても、「内部」が9割近くを占めています。

1件当たりの漏えい人数は「内部」が多い……私の経験では特に「内部犯罪」が全体の7～8割近くを占めると考えています。

JNSA（NPO日本ネットワークセキュリティ協会）資料より

2010年　個人情報漏洩規模

・漏洩人数　5,579,316人
・漏洩件数　1，679件
・想定損害賠償総額　121,576,000,000
・1件あたりの平均漏洩人数　3,468人
・1件あたりの平均想定損害賠償額　75,560,000円
・1人あたりの平均想定損害賠償額　43,306円

（平均値は単純平均値ではありません。詳細はJNSA資料をご覧ください）
http://www.jnsa.org/result/incident/data/2010incident_survey_PIL_v1.4.pdf

ということは・・・
日本の人口は約127,692,000人だから約23人に1人が被害を被っている！

内部不正・内部犯罪とは？

会社や団体における「内部不正・内部犯罪」とは狭義においてはその関係者（従業員・役員・派遣社員など）もしくは関係者と位置付けられる人（従業員の家族など）が意識的に（主犯者、加担者、協力者などの関与した濃淡を問わない）不正行為、犯罪行為を行った事案を指す。
また、外部者と密接して共同で行為に及ぶ事案も含まれる事が慣例となっている。（例外もあり得る）

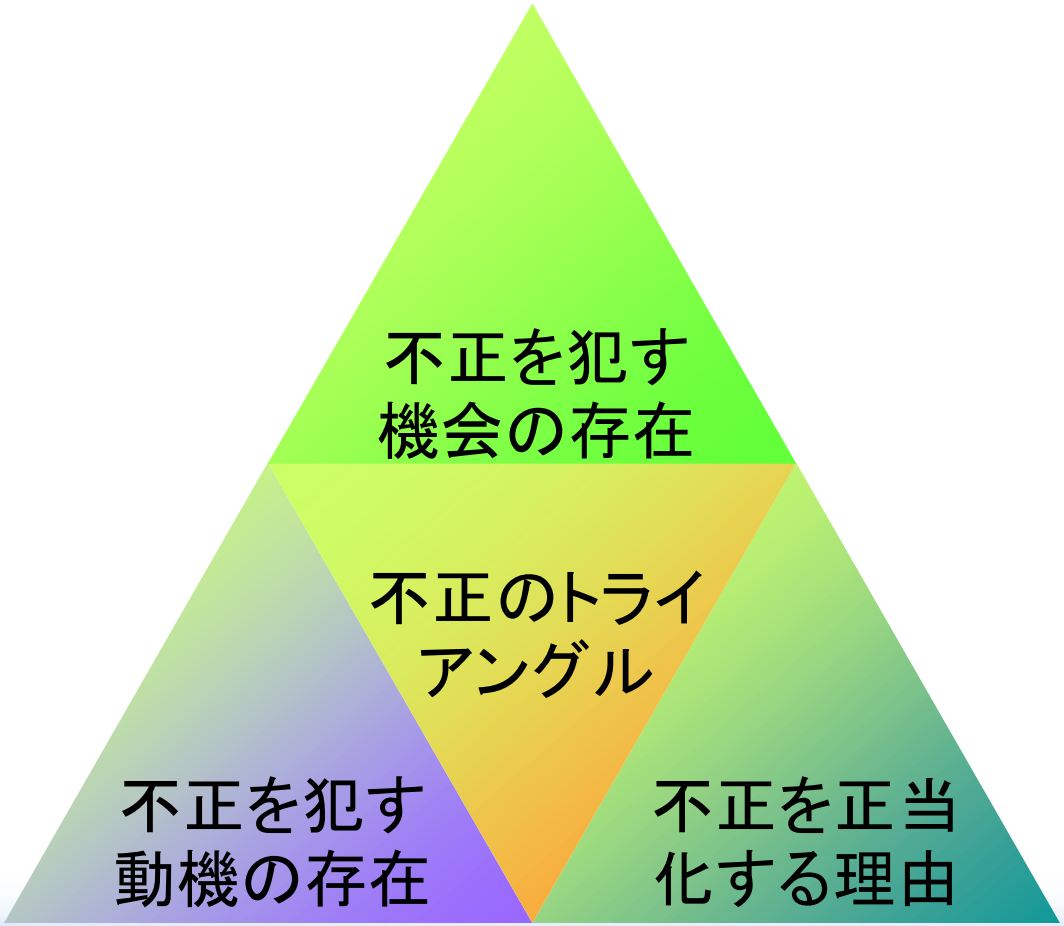
特徴は、
１：その殆どは表面化しない。関係者以外は厳秘情報とされ、
　緘口令を敷く場合も多い。
２：ただし、被害の程度はバラバラであり、軽微な事案から、会社
　自体が倒産する可能性を持つ深刻な事案まで様々である。
３：経営者の信頼を受けていた人、もしくは親族が被疑者である
　ケースも多いので調査をためらう中堅の管理職が多い。

不正のトライアングルとは？

不正が行われるには「動機」「機会」「正当化」の3つが
必ず存在する・・・犯罪学者クレッシーが提唱

「動機」・・・経済的理由、目標達成のプレッシャー　等
「機会」・・・全てお任せ状態、相互監視無し、検査がザル　等
「正当化」・・・経営側もしている、先輩も代々行ってきた、
こんなに頑張っているのに上司が不当な評価　等

逆にこれらの１つでもなくなれば犯罪は起きない！！！
（ただし、「動機」＋「機会」があると「正当化」は簡単に
乗り越えられる傾向が強い）


不正を犯す
機会の存在
不正のトライ
アングル
不正を犯す
動機の存在
不正を正当
化する理由

14コの内部不正に関する危険信号

あなたの会社、団体は大丈夫ですか？横領犯のProfileは過去20年変わっていません(ACFE第19回年次総会分科会より抜粋)

① 勤続年数が長い

② 次の理由により雇用主からは重宝されている

- 出勤時間が早い
- 夜遅くまで残業する
- 休日出勤もいとわない
- 仕事を家に持ち帰る
- 病欠以外は仕事を休まない
- 休暇を取ろうとしない
- IQが高い(頭がいい)

③ (しかし)同僚からは尊敬されていない

④ 地域や教会の活動に積極的に関与している

⑤ 単独で業務をこなしている

⑥ 家族は何も知らない
⑦ 横領した金は貯めずに費消する
⑧ 裕福な生活を送っている。その理由を遺産相続、借り入れ、配偶者の収入のためと説明する
⑨ 定期的な調査に抵抗感を示す
⑩ 自分の職場に人を近づけたがらない
⑪ 事業主に業務記録を見せたがらない
⑫ 次から次へと仕事(責任)を引き受けようとする
⑬ 犯人が予定外に職場にいない間に発覚しやすい
⑭ 小額の着服から始まり、徐々に大胆になりながら一定期間継続する

如何でしょうか？

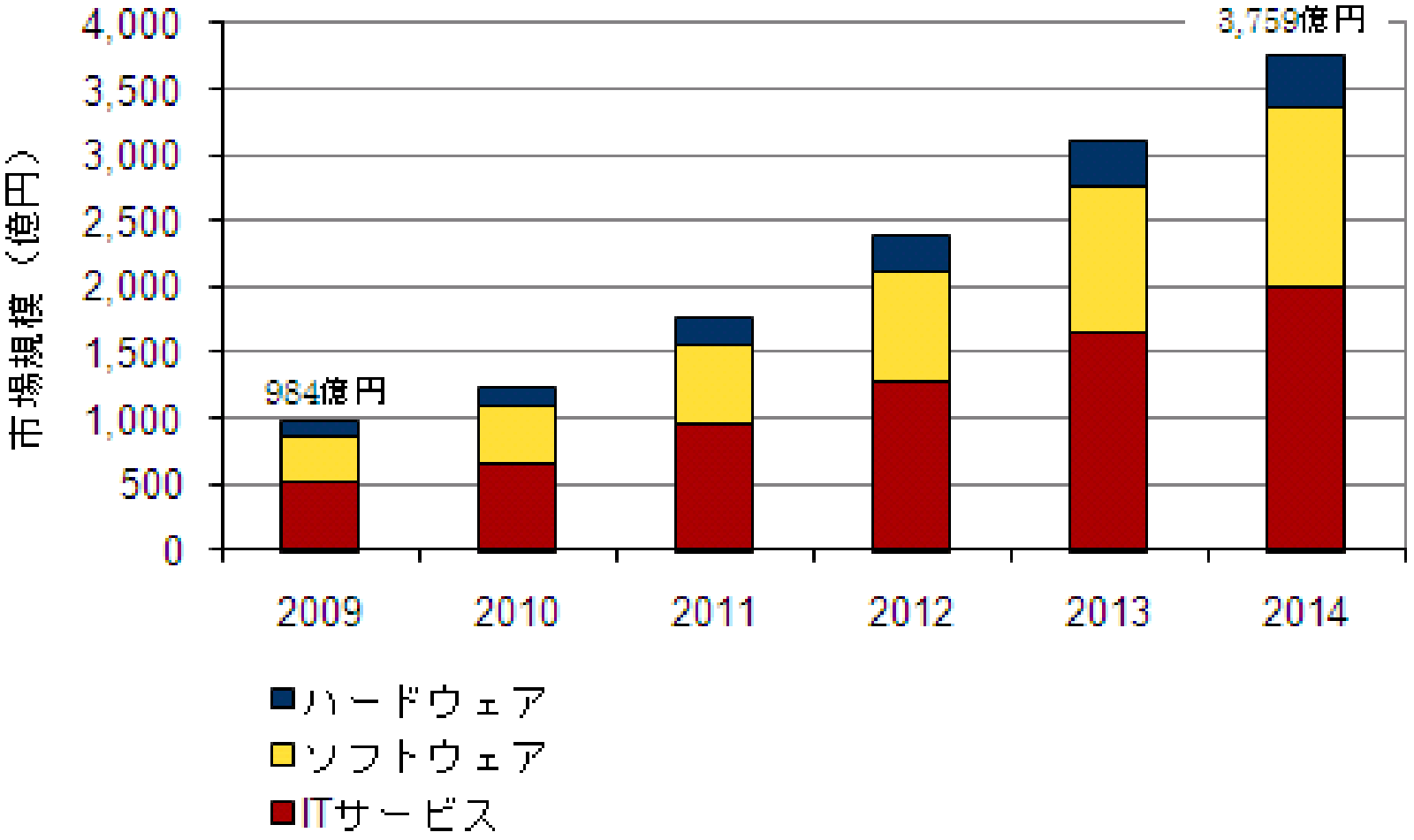
どこでもその様な方々がいらっしゃるのではありませんか？

ただし、念を押しますが、「だからといって不正をしている」ということではありません。不正をしていた方々の行動にこの様な兆候が統計学的に認められたということにすぎません。前述の14項目のように行動している人を疑うのは統計的に誤りです。不正した方々にこの様な兆候が顕著にあったに過ぎないという事です。くれぐれも誤解されない様にお願い致します。

クラウドについて

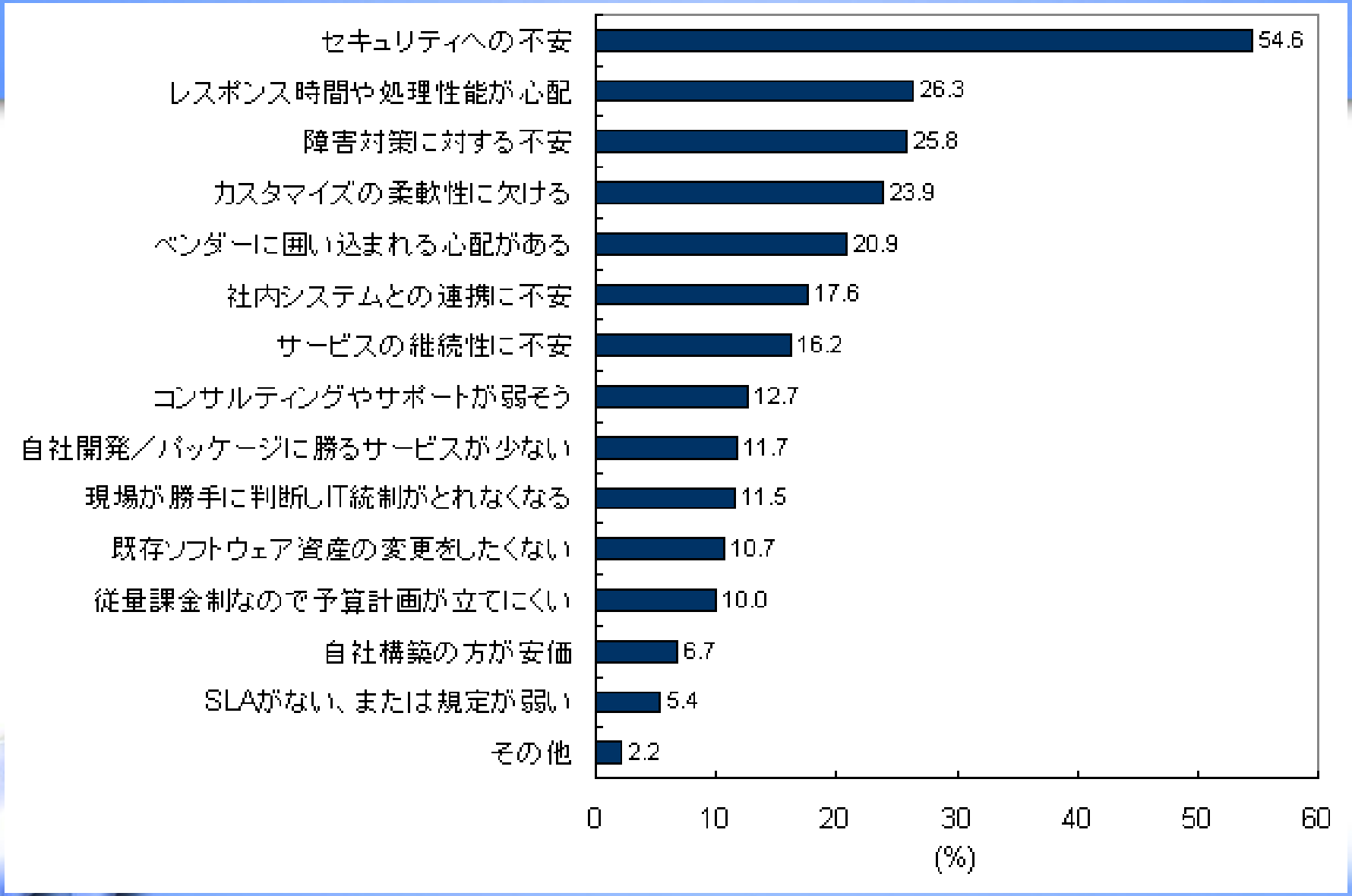
次ページのグラフは2010年9月2日にIDC　Japanが発表した国内プライベート・クラウドの市場予測である。このグラフからもお判りの通り、年成長率は30%を超え、国内IT市場においてもっとも期待が出来る市場の1つとしている。
詳細　http://www.idcjapan.co.jp/Press/Current/20100902Apr.html

これによれば2009年の規模は984億円であったが2014年には3,759億円にも成長するという。たった4年後に2,800億円も伸びる市場はまずない事を考えるならここが「宝の山」の1つになる事は想像に難くない。


市場規模（億円）
4,000
3,500
3,000
2,500
2,000
1,500
1,000
500
0
984億円
3,759億円
2009
2010
2011
2012
2013
2014
ハードウェア
ソフトウェア
ITサービス

また次ページのグラフは国内のパブリッククラウドのサービス阻害要因についてIDCJapanが調査を行った結果である。

結果はある意味予想通りであるが、ダントツで阻害要因と認識されているものが・・・**「セキュリティ」**である。


セキュリティへの不安 54.6
レスポンス時間や処理性能が心配 26.3
障害対策に対する不安 25.8
カスタマイズの柔軟性に欠ける 23.9
ベンダーに囲い込まれる心配がある 20.9
社内システムとの連携に不安 17.6
サービスの継続性に不安 16.2
コンサルティングやサポートが弱そう 12.7
自社開発／パッケージに勝るサービスが少ない 11.7
現場が勝手に判断しIT統制がとれなくなる 11.5
既存ソフトウェア資産の変更をしたくない 10.7
従量課金制なので予算計画が立てにくい 10.0
自社構築の方が安価 6.7
SLAがない、または規定が弱い 5.4
その他 2.2
0
10
20
30
40
50
60
(%)

クラウドとはいってもその様態は様々・・・
パブリック・クラウド
プライベート・クラウド
SaaS、PaaS、IaaS、DaaS　・・・・・

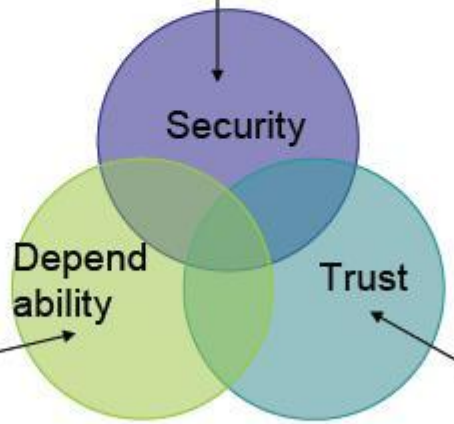
一般論として
ここのセキュリティを考える場合は契約業者の身元や業者の管理者
端末が汚染された場合の取り決めやテナント側からの攻撃の耐性
まで今までにないセキュリティチェックが必要不可欠となる。
クラウドのリソースアクセスはID＋パスワードしかないのだから・・・
学会でも研究発表がいくつかされている。

それでもクラウド化のスピードは加速していく

民間・・・明らかなコストダウン（しかも7割減、8割減が当たり前）
行政・・・震災以降の自治体クラウドの推進が急加速
（県庁や市役所自体が消失する危険性の具現化）

クラウドの安全・安心のための課題
＜ITリスク克服のために＞

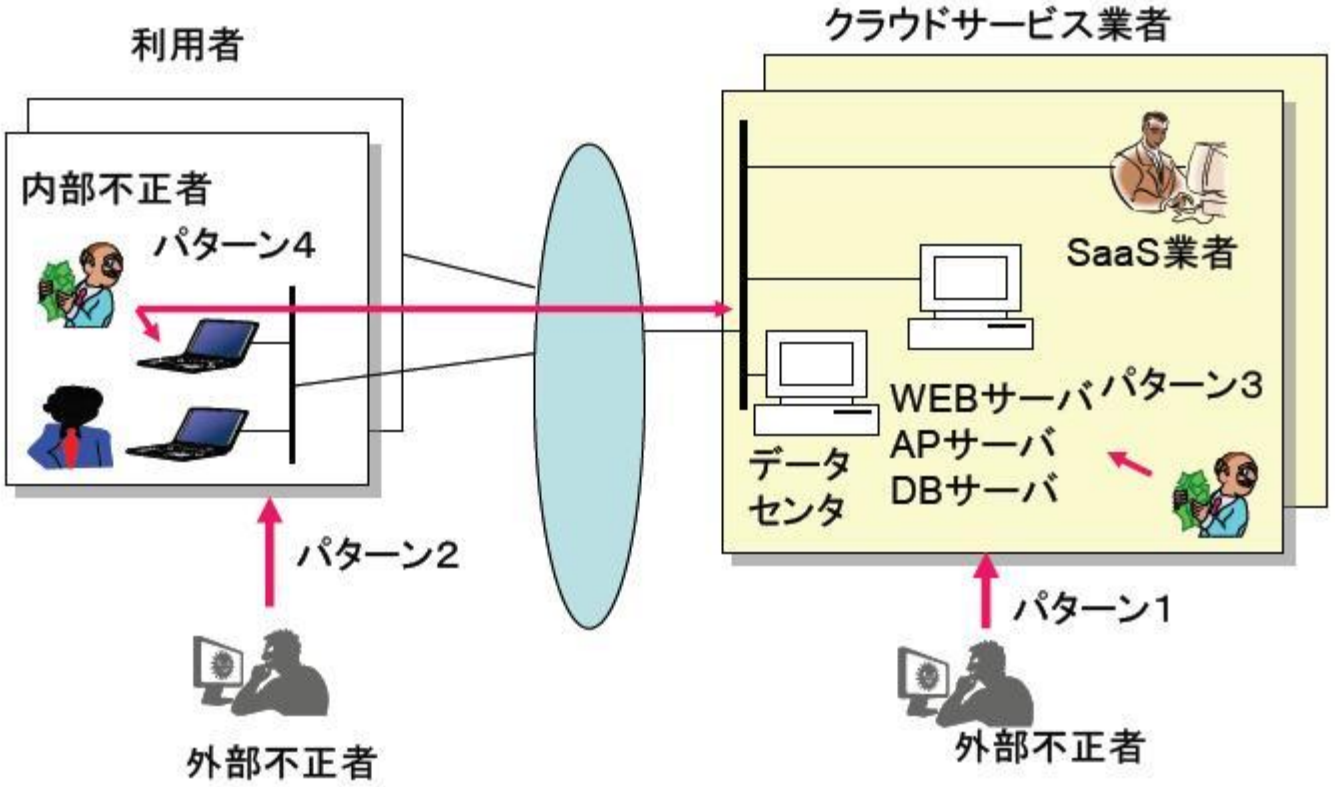
①外部や内部からの攻撃に対するセキュリティ対策
（a）クラウドへの攻撃 （b）利用者の装置への攻撃



②バグや故障・災害などへの対策
（a）システムの停止
（b）データの喪失
（c）誤処理

③サービス提供者へのトラストの確保対策
（a）将来にわたりサービスしてもらえるか
（b）データの目的外使用や不正処理をしていないか
（c）政府などによる検閲のある国で処理してないか
（d）障害や不正があったとき調査などに協力してもらえるか

セキュリティに対する攻撃パターン



【PR】講師略歴

旧通産省の情報処理技術者試験で最難関である「特種」に日本最年少で合格。早稲田大学システム科学研究所に通学後、プロジェクトリーダーとして多数のシステムを担当。
日本セキュリティ・マネジメント学会の「先端技術・情報犯罪とセキュリティ研究会」などで 講師経験を積み、各種のコンピュータ専門誌、金融専門誌等で情報セキュリティ、ウイルス、ハッキング・クラッキング、ネットワーク犯罪など多岐に渡り、独自の検証を踏まえ執筆や講演活動を行う。NHKやフジテレビにも出演し、活動範囲を広め、(社)コンピュータソフトウェア著作権協会や、金融アドバイザーとしても活躍。クラウドやスマートフォンでも各種セミナーなどを行い、2011年12月に世界で初めてAndroid OSのウイルス対策ソフトが現状のものではあまり役に立たないことを実証実験結果を解説し世界の注目を浴びた。
2008年6月まで22年間三菱東京UFJ銀行に勤務。
2010年に社団法人情報セキュリティ相談センターを立ち上げ、現事務局長。
現在、セミナーや講演会は年間30～40を消化し、コンサルタントとしても全国で活動中。

【著書】
「経営戦略としての個人情報保護と対策」(工業調査会、2002年8月、共著)
「名探偵ハギーの世界ーやさしい情報セキュリティの本」(日科技連出版、2004年6月)
「45分でわかる個人情報保護」(日経BP社、2005年4月,共著)
「個人情報はこうして盗まれる」(KKベストセラーズ、2005年5月)
「デジタル・フォレンジック事典」(日科技連出版、2006年12月、編集責任＋共著)
「バンキングシステム」Vol.35-No.2(2007年4月20日発行)
「金融機関における情報漏洩防止策～技術上。運用上のポイントを探る」
「NHK達人に学ぶ人間力アップ 」(日本文芸社、2007年10月発行、共著扱い)

ご清聴ありがとうございました！

メール　jssm@hoshizora.jp　　萩原栄幸

企業での講演やセミナーのご依頼は上記アドレスまでご連絡下さい！
情報セキュリティー般、コンプライアンス、情報漏えい、内部犯罪、
クラウド、スマートフォン、ハッキング・クラッキング、個人情報保護、
など豊富な実績（防衛省、海上保安庁、各種県警本部、市役所など）
一部上場企業様から、零細企業様まで業種業態規模を問いません。
新製品紹介や主催、共催での特別講演、基調講演でのご利用で売上が倍以上になった企業様も多数おります。
是非、ご検討頂ければ幸いです。全国、海外どこでも講演可能です。