―富山茂賞受賞記念―
IT統制研究会/先端技術・情報犯罪とセキュリティ研究会
「クラウド時代のIT統制」

# 内部犯罪事例と対策

## ～クラウド・コンピューティングも例外ではない！～

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
NIS（ネット情報セキュリティ研究会）　相談役
CFE（公認不正検査士）

萩原　栄幸
Mail: jssm@hoshizora.jp

2010.12.11

# Ⅰ．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。

# JNSA（NPO日本ネットワークセキュリティ協会）資料より

2009年　個人情報漏洩規模

・漏洩人数　5,735,673人
・漏洩件数　1,539件
・想定損害賠償総額　389,411,440,000円

ということは・・・

・1件あたりの平均漏洩人数　3,934人
・1件あたりの平均想定損害賠償額　267,090,000円
・1人あたりの平均想定損害賠償額　49,961円

日本の人口は約127,692,000人だから約22人に1人が被害を被っている！

2009年漏洩原因比率

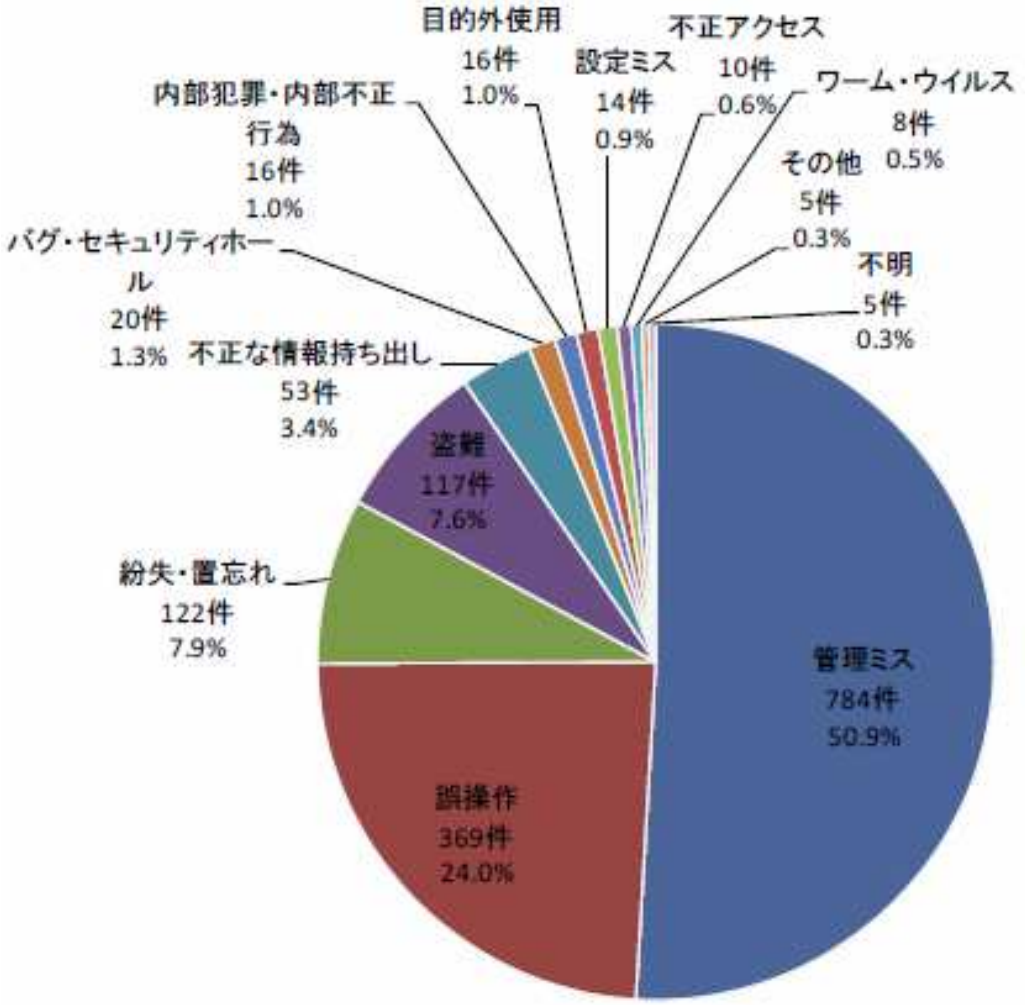



図 8：漏えい原因比率（件数）

## 2009年原因1件あたりの漏洩人数

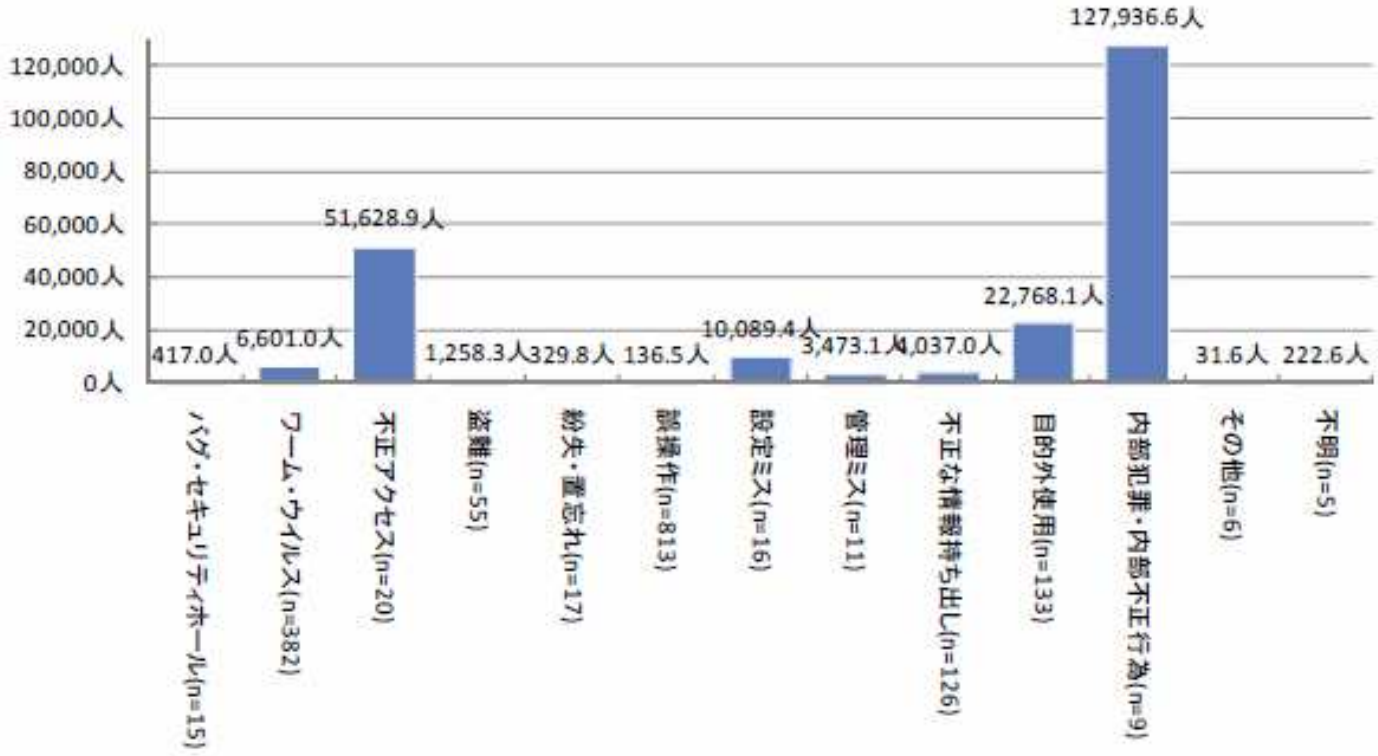
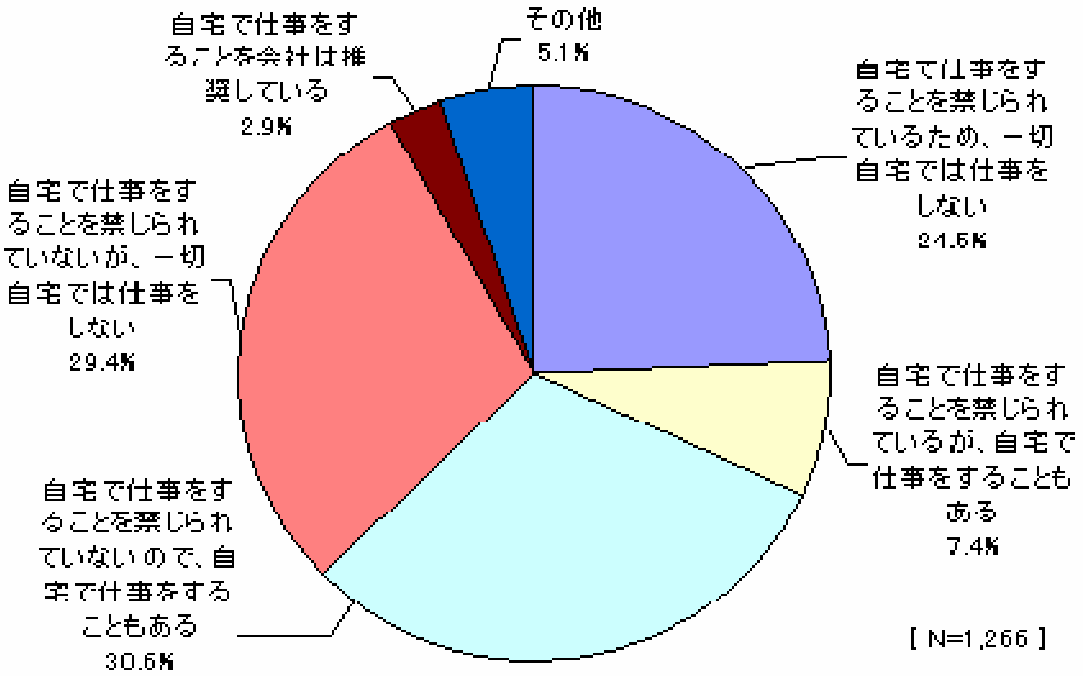



図 11：漏えい原因別の一件あたりの漏えい人数

自宅でパソコンを使った仕事の実施状況と企業ルールの遵守状況（NRIセキュアテクノロジーズ調べ）




あなたの会社では、自宅でパソコンを使って仕事をすることを禁じていますか。（回答は1つ）

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

いかがでしょうか？
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にはならない」。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マークするのではなく、マークした方々にこの様な兆候があればより不正に関与している可能性が高いという統計的な差異が認められたということです。くれぐれも誤解されない様にお願い致します。

## （その他）参考資料として・・・

１：公開資料によれば個人情報漏洩事件の要因分析の結果
（流出データ数を「外部者」「内部者」「不明」に分類すると）
**圧倒的に「内部者」の要因**である事が判った。
（http://www.itmedia.co.jp/enterprise/articles/0502/17/news001.html）

２：セキュリティベンダーのウェブルート・ソフトウェアは2007年10月29日、日本や米国、カナダ、フランス、ドイツ、英国の中小規模企業を対象に実施した、セキュリティに関する調査結果を発表した。それによると国内企業においては、ウイルスのような外部からの攻撃よりも、
**内部の人間によるデータ盗難や過失の方が深刻だと考えている**ことが明らかになった
（http://itpro.nikkeibp.co.jp/article/NEWS/20071030/285925/）

## （その他）参考資料として・・・

３：**退職した従業員の59%が会社のデータを盗み出し**ており、67%が新たな仕事を見つけるために会社の機密情報を利用した経験を持つ――米国の調査会社、Ponemon Instituteが2009年2月23日に発表したレポート「Jobs at Risk＝Data at Risk」で明らかになった。
（http://www.computerworld.jp/news/sec/136569.html）

４：仕事で「顧客情報を扱う」人は、約7割。しかしPCの電源状態について「トイレなどで**10分ほど席を外すとき」は4割近くが「何もしていない」と回答**。
（http://www.itmedia.co.jp/enterprise/articles/0811/04/news060.html）

＊なぜ、10分に拘るのか？実態はご存知ですか？10分いえ、
**3分あれば大概の事は出来てしまう**のです・・・

# Ⅱ．Cloud:クラウドの光と闇（リスク）

今や「クラウド」が大流行！！！！！

クラウドという言葉がでないとITや情報セキュリティの
DMが読まれない・・・という噂が・・・

内部犯罪（内部不正）もだんだんブレークしつつあるけど・・・

今年７月１０日（土）
経済産業省＋LACの最高執行役員の西本氏と萩原の３名
でセミナーを開催しましたがその時西本氏はクラウドについて
「平成の黒船来たる！」とご講演されておりました・・・

私も技術論としてはさほど目新しいものではないが、
ベクトルとしては相当な影響力をもって、様々な業種・業態の変革を
促す「カンフル剤」として効果を示す可能性が高いと感じています。

これを理解していないと
今後の仕事が根本的に変容していく現実を見逃してしまう事になって
しまう可能性があると考えています！！

最近某東証一部上場企業の「新・基幹システム」のお目付け役を
していますがコンサルタント会社、有名ベンダー共にクラウドの論理
すら知らない人が多いのにはびっくり！しています。
どうしてそうなっているのでしょうか・・・

クラウドの（なるべく眠くならない）技術論

キーワード（他にもたくさんありますがここを切り口にしたという意）

・Hadoop（HDFS/MapReduce/Key-valueストア/コンシステントハッシング）

・NoSQL（SQLを否定している訳じゃない。Not Only SQLという意味合いが強くなっているのが現状です）

そして具体例として

Twitter・・・これもクラウドを利用しています。

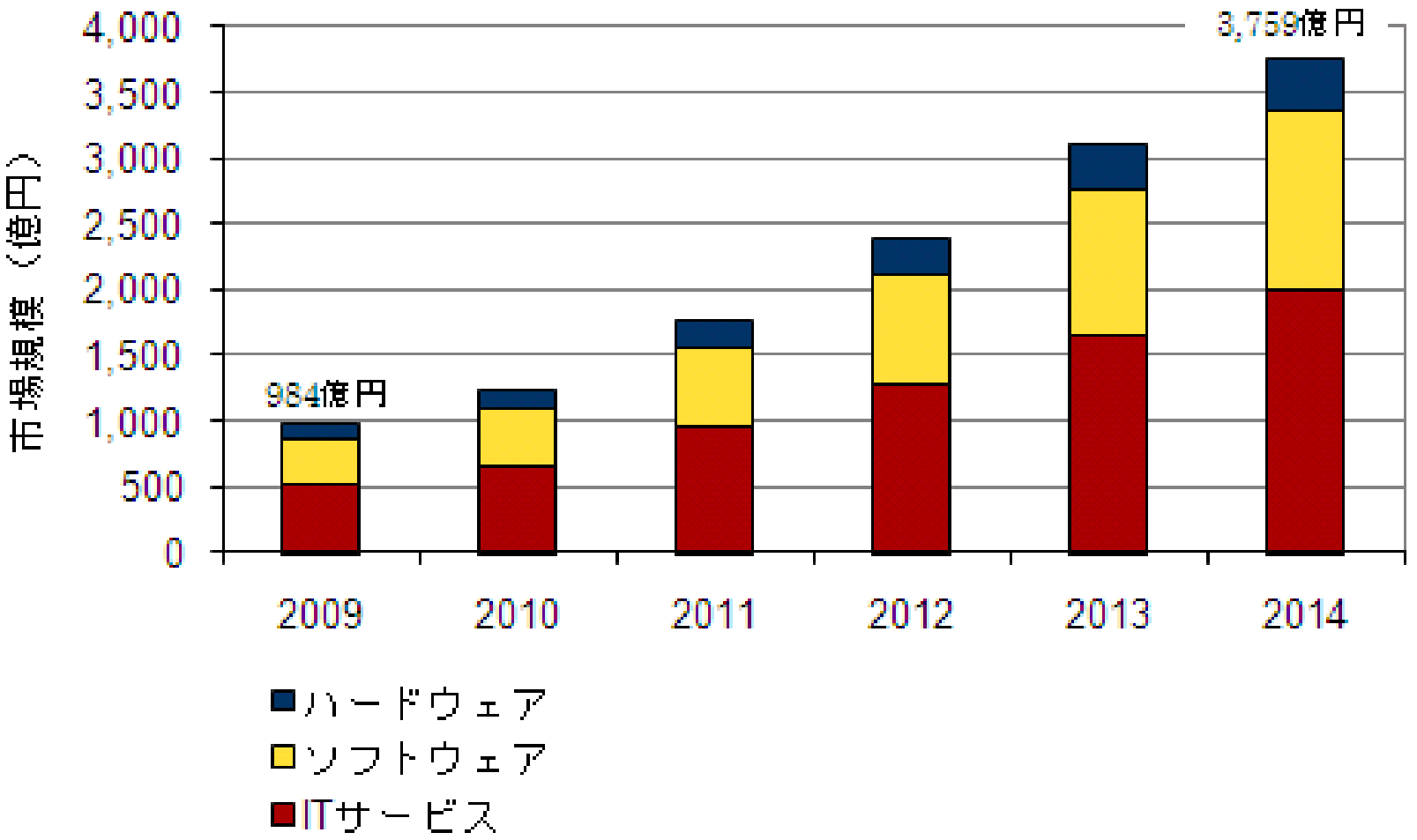
えっ？全く聞いた事もない単語が・・・技術者の悪い癖ですね・・・

お時間が許せば解説を簡単に行います。

技術的には（誤解を恐れずに言うなら）２点だけ覚えればいいかも？

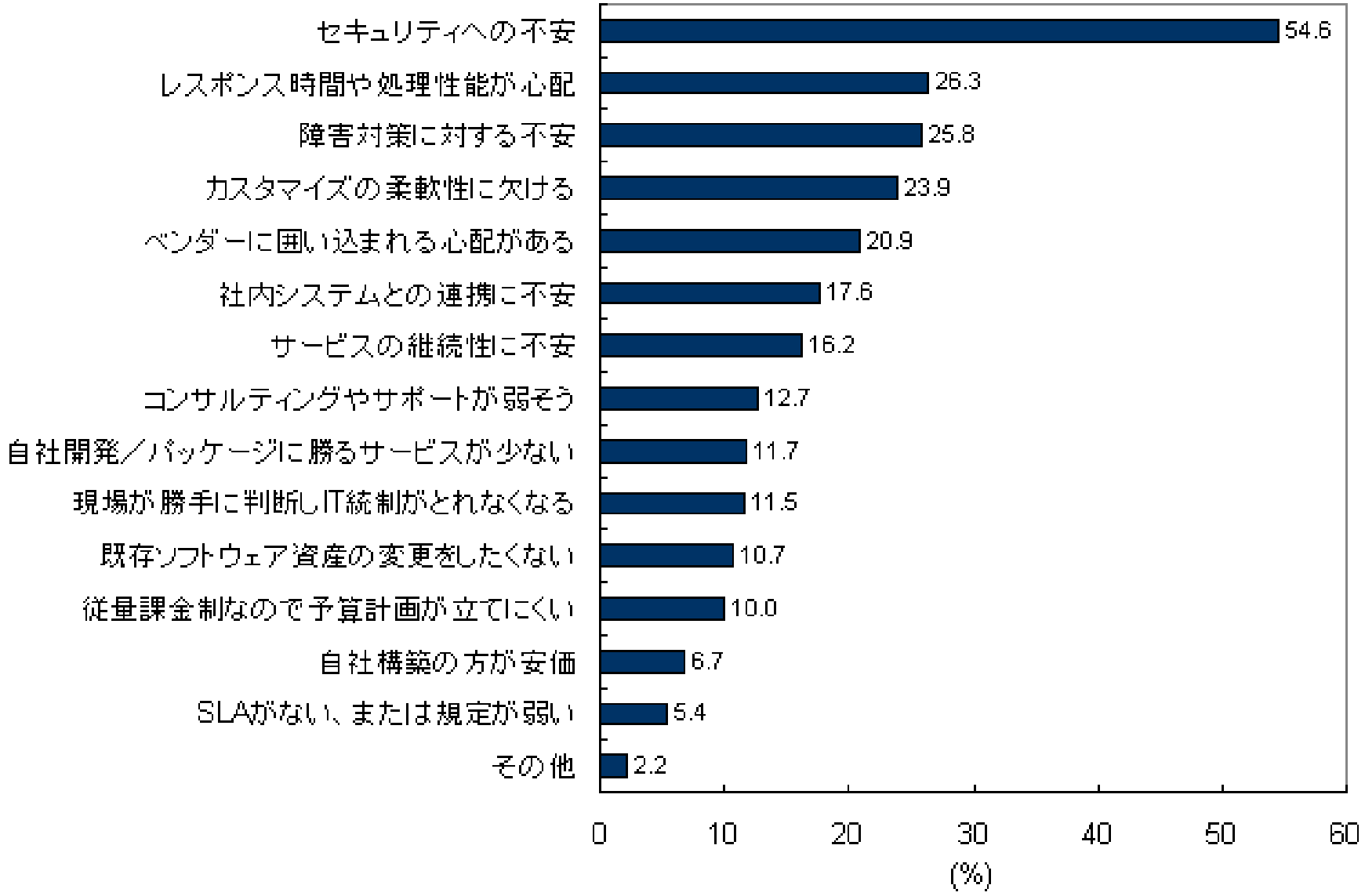
次ページのグラフは2010年9月2日にIDC Japanが発表した国内プライベート・クラウドの市場予測である。このグラフからもお判りの通り、年成長率は30%を超え、国内IT市場においてもっとも期待が出来る市場の1つとしている。
詳細
http://www.idcjapan.co.jp/Press/Current/20100902Apr.html

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。

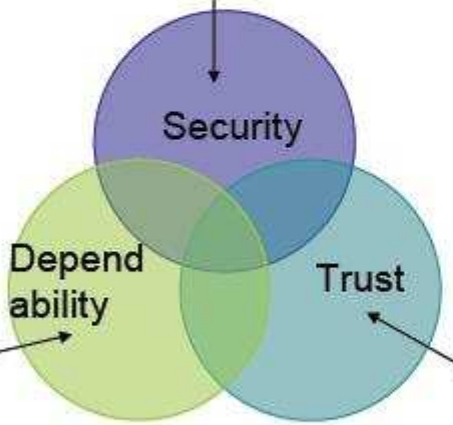
結果はある意味予想通りであるが、ダントツで阻害要因と認識されているものが・・・**「セキュリティ」**である。


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
(%)

# 第４回ITリスク学研究会 「クラウドとITリスク」抜粋

## 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

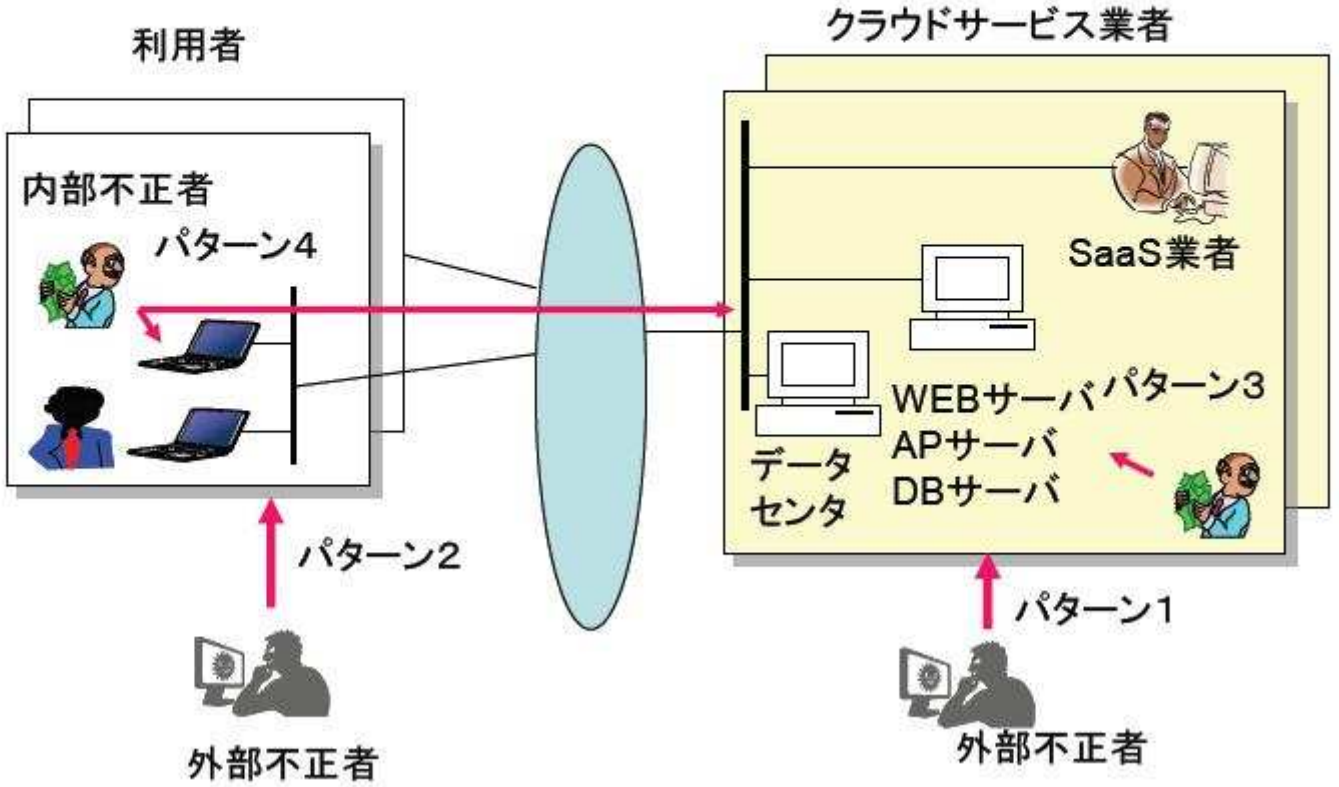



**②バグや故障・災害などへの対策**
（a）システムの停止
（b）データの喪失
（c）誤処理

**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

# 第４回ITリスク学研究会 「クラウドとITリスク」抜粋

## セキュリティに対する攻撃パターン



東京電機大学佐々木教授によれば
　クラウドにおけるセキュリティの攻撃パターンは次の４つ

１：クラウドサービス業者への外部からの攻撃
２：クラウドサービス業者への内部からの攻撃
３：利用者への外部からの攻撃
４：利用者への内部からの攻撃

それぞれの特徴を次頁に述べる

## （1）（2） クラウドサービス業者への攻撃

攻撃対象

WEBサーバー　APサーバー　DBサーバー　　など

主要対策

１：入退出管理・・・監視カメラなどの物理的対策

２：アクセス制御、暗号化、セキュリティ監視などの情報処理対策

３：セキュリティ管理、監査などの管理的対策

備考

１：一般企業と必要な対策は基本的に同じ

２：説明責任を果たすためログの収集などの対策は一般より強く
　　要求される

３：利用者側が出来る事は厳重なIDとパスワードの管理くらいか？

# （3）（4）利用者への攻撃

主要対策
１：セキュリティ監視（外部、内部共）
２：セキュリティ教育（内部犯罪対策）

利用者側のパソコンが１台もなくなる事はあり得ないものの
セキュリティ対応能力はどんどん落ちるのでここへの攻撃が
今後問題になりうる。

検疫ネットやセキュリティ監視、セキュリティ応急対応と組み合わせ
End－Endセキュリティサービスのクラウド化は大きなビジネス
チャンスになり得る。

こうした考えの中で利用者、クラウド業者ともに最も気がつかないものは佐々木先生の図でいくなら「パターン３」及び「パターン４」もしくはこれらが関与した複雑骨折の犯罪行為である。
（つまり内部犯罪者が主体で関与した場合のクラウドからの情報漏洩）
クラウドでの一番の問題点はIDとパスワードでの認証であると、友人たちと話していてもそこがどうしてもボトルネックとなる。技術論でNoSQLがどうのHadoopがどうのCassandraがどうのと話していた、自称クラウドを心底知っている男（自分だけそう話しているらしいが）がここの部分や内部犯罪防止との観点でクライアント様と打ち合わせをすると、何とも頼りない（と感じている）・・・
特に非偏在性やクラウド業者をどこまで信じていくのか・・・それはそれぞれの企業における経営者の判断にも遡る。極めて非技術的な問題なのである。しかも国境を越えたコンティンジェンシープランやリーガルチェックでの諸問題を考慮するなら、まだまだ問題が消化しきれていないと感じています。

# Ⅲ. 内部犯罪事例

ここから実際の古典的内部犯罪事例を紹介し、
最後にクラウドでの想定事例（一部実際の事例）を
ご紹介致したい。

# 例１：LAN上のメールをすべて収集していた女性

・食品加工会社の本社総務部
・30代の元SEの女性
・この女性は以前社内のシステム開発部にてシステム設計を担当していた人物。社内異動で4年前から総務部所属。そして周りは気がつかなかったが3年程前から同じ所属の課長と不倫関係に。だが1年前から別れ話が出ていた。しかし彼女は頑なに拒否をしていた・・・
事件は隣の同僚からの告発から始まった。実はある日彼女が真剣に画面を食い入る様に見ていた事に気がついた隣の同僚が何気なく画面を見ていたら、何とその画面は課長宛のメールだった。最初は勘違いと思っていたが、どうやら本当に課長宛のメールであると気がつき、会社の人事に


26

相談したものだった。状況を確認し、証拠を掴むためにしばらく静観した。その間に専門家に調査の依頼をしたのは言うまでもないだろう。

結果、彼女は昔の知識を悪用し、LAN上に流れるメールを無条件に全て自分のところに来るアングラツールを仕込んでおいたのが判明。
実はこの手のソフトは現在でも簡単に無料で手に入れる事ができる。
仕組みはこうである。
このソフトは同じLANにあるメールを宛先関係なくすべて取り込んでしまうものであり、通常の場合であればHUBと称される機器がメールのパケットをすべてのクライアントに流し、「これはあなた宛のメールですか？」と聞き、違っている場合なら「違います」とHUBに返答の上メールは破棄する。合っていれば「そうです」と返答しメールの内容をパソコンに取り込む。ところがこのソフトは無条件にメールを取り込んでしまうので結果的にLAN上に流れるすべてのメールを収集することになってしまうのである。


27

彼女は依願退職（本来の行為としては懲戒免職であるが動機が動機なのでなるべく穏便という計らいがあったと思われる）
また余談ではあるが課長もそれなりの処分を受ける事になった。
【予防策】これはどうすれば防げたのであろうか？男女の関係にまで突っ込んでどうこういうセミナーではない。飽くまで論理的という観点でお考えください。概ね次の内容となる。（本件の場合もこの中から出来るものを順次導入していった）

- 会社のパソコン内に許可されないソフトのインストール禁止（社内規定）
- またそれを有効にさせるための自己申告、クロス内部検査、検査部での強制検査、外部コンサルによる抜き打ちチェックなどの導入
- それと不正ソフトを巡回監視するためのエージェントソフトや専用の情報漏洩防止ソフトの導入
- ネット上でのダウンロードの監視
- スパイウェア検知ソフトの導入

まだまだ考えられるものもあるが原則はこれらの応用となる。


28

また、補足としてはHUBをインテリジェントHUBなどに変更する事も有効で本件ではこれも採用した。（後者では相手が誰かを認識できるので無条件にメールを飛ばさずに該当者のクライアントのところだけメールを飛ばす機能がある）
今ではこれらのソフト類の大部分はスパイ専用ソフトで捕捉可能となっている。


29

# 例2：部長成りすまし事件

・自動車販売会社　本社営業第二部
・20代の入社5年目の男性（役職なし）
・ショルダーハッキングの応用でID、パスワードを入手

経営サイドしか知らない社内情報や同僚の人事考課の内容の覗き見及び自分の人事考課の改ざん

原因：出世コースに乗り遅れまいという切迫感。部長の無理解
防止策：ID、パスワードの変更管理、ログ情報のチェック、
深夜での実行禁止、評価の透明性確保、面談の強化
メンタル面での会社としてのサポート、ソフトでの対応も


30

# 例3：パスワード・クラック・ツールを駆使していた人

・製薬会社　仙台工場　第四基礎研究部

・30代男性（主任：係長級）

・有名なJohnでのパスワード解析して同僚の研究を覗き見

原因：斬新なアイデアが出なくなったあせり。妬み。趣味と実益が一致。
　　社外ではその道のマニアの間では有名人。

防止策　Johnを自宅で行うには絶対にパスワードファイルが必須。
　　DUMP処理を実行させないためには該当パソコンやLAN上で
　　Adminの権限で実行させない仕組みが必須。
　　ネット監視、エージェントの監視、不要なJob実行の禁止、強制終了
　　パスワード変更のタイミングを短期にする。時間帯でのAdmin実行
　　の制限もしくはシステム管理者の許可制導入検討


31

# 例4：仕事熱心？・・・いや、病気だったある若者

・総合商社　　大阪事業部繊維第一部
・20代　入社2年目の新人男性
・フロア全員のパソコンにキーロガーを仕込む
　週1回くらいのペースで採取（その為には最低週1回は最後まで居残り
　をする必要があった）一見、仕事熱心で残業大好き人間だった。
原因：彼の場合は極度のストレスによる精神病の疑いが後日判明。
防止策：前に述べた内容の応用。ここでのユニークな内容というなら、
キーロガーは年々進化している。画面キャプチャーできるもの、ステルスで
動くもの、メールに自動返信するものなど・・・毎年見直しが必要かも知れな
い。


32

# 例５：利息の端数を集めたら・・・・

（有名な事件なので追加）
・米国のある金融機関
・預金の利息計算プログラム担当のプログラマーが１セント以下の端数を特定口座に加算していた。全体の金額は当然ながら一致するので気がつかなかった。決算時に毎回数万ドルにもなったらしい。（未確認）
（計算）１人の平均余り額は統計学的に0.5セント。もしこの金融機関の決算対象口座が１０００万人（都銀はもっと多い）とするなら、決算の度に5万ドルが入る計算となる。
（防止策）プログラミングの検証内容に「不正ロジックの検知」追加、また検証は必ず第三者が複数で行うなどのチェック体制強化。従業員教育啓蒙活動の実施、プログラム内の不正ロジック検知プログラムの実行。システム監査強化、検査部検査強化、不審な行動をチェックする体制。


33

# 例6：社内留学制度でつまずいた研究者

・総合電機メーカー　　中央研究所勤務
・30代　主任研究員
・社内留学が決定。彼はデジカメを持っていたがメモリが小さく他人から
　借りる事に・・・・・それが理由でクビになった！なぜ？


34

# 例7：社内インターネットカフェ幽霊事件

（これも実際に遭遇したケースだが）

・ある物流会社　本社内

・50代　取締役

・社内でインターネットカフェを従業員組合が音頭をとって開業・・・

なにか、おかしい？？？

その事実と予防策をお伝えします。



35

# 番外：クラウド絡み事件

米国でも造幣局がクラウド化を推進していたが、いつのまにかサイトが
不正アクセスされていた・・・
サービスを提供していた管理者端末が汚染されていたことに気がつかず
ホスティングサーバーから仮想の造幣局サーバーやらX社の仮想サーバー
Y社の仮想サーバー・・・と全滅さrていた・・・

外からじゃ判らない！
しょせん仮想！
同居しているテナントが脆弱なら？
管理者端末が汚染されていたら？

ヤフーメールも以前1300人分のメールが消失！

# 番外：クラウド絡み事件

今まで報告されているクラウドの「お客様」からの内部犯罪は
通常はクラウド化されていないシステムなどからの切り崩しが多い。

例
１：協力会社の社員
２：管理者権限を持つ情報システム部門
３：役員が「便利屋」として重宝している社員

だが、業者からの内部犯罪は少なくともそれを兆候として捉える事は「お客様」側からは無理！！！

ここがある意味一番の問題となるので
逆に業者にとってはここを担保出来るサービスが提供できるなら
差別化が期待できる

## その他の犯罪アラカルト

LAC情報だけでも・・・
・AmazonEC2を悪用したパスワード解析、LAC調査でアルファベットと数字だけなら8ケタで45ドルでクラック出来る
・AWSのIPアドレス経由の攻撃は2009年11月で昨年の5倍！
・「闇のクラウド」を提供する小規模ISP（MoColoなど）を確認！

でもこういうところにビジネスチャンスあり！
「うちのクラウドはここまでセキュリティを強化しています！だからちょっとはお高いけど実は極めて安心・安全にお使い頂けます！」
もしくは、
「通常のセキュリティレベルは当然対応しています。でもバンキングの様なセキュリティは求めません。だから簡単容易に導入出来、しかも安価なのです！」・・・というところがあってもいいのでは！

LACの新井悠研究センター長投稿記事からの抜粋

クラウドを悪用した攻撃の実態

１：大量処理能力を悪用

２：非偏在性を悪用

３：ボットネットの代替としての悪用

４：その他、個別具体的な脆弱性の攻撃

技術的解説が多いので詳細解説は省きますがきちんと検討されて
「うちはどうする？」という問題意識は持って頂きたいと思います。

# 【補足】内部統制上の内部通報制度について

- （監査人、調査担当者、不正検査士以外に）不正の兆候を最も察知しやすい立場にあるのはそれらの兆候が示されている部署の近くで働いている従業員である。…しかし、現場の従業員は不正の兆候やそれを察知したときの対応についてほとんど訓練を受けていない（出典：Thomas　Caulfield, CFE, CIG, CIGI“The Anatomy&Illusiveness of Procurement Fraud”）
- 　上述の引用を見るまでもなく、私たちの周りを見てみると意外なほど、従業員の「不正」に対する明確な方針が定まっていない。それは「あたり前だから、いちいち記入するものでもない」という常識にとらわれていないだろうか？　だが、その「あたり前」のことを「あたり前」に行うことこそが難しくなっているという現実から目をそむけているような気がしてならない・・・

- 「内部通報制度」とは、企業において、法令違反や不正行為などのコンプライアンス違反の発生またはその恐れのある状況を知った者が、そのような状況に適切に対応できる窓口に直接通報することができる仕組みのことです。名称は、「ヘルプライン」「ホットライン」「コンプライアンス相談窓口」などさまざまです。
- コンプライアンス経営において重要な役割を果たす「情報伝達」には、上司やコンプライアンス担当者などを経由する通常ルートと、通常ルートが何らかの理由で機能しない場合の非常時のルートが必要であり、内部通報制度は後者の伝達ルートとして位置づけられます。内部通報制度は、企業のコンプライアンス経営を有効に機能させるうえで重要な役割を担っている制度なのです。」（出典：KPMGビジネスアシュアランス（株）編、『早わかり リスクマネジメント＆内部統制』、日科技連出版社、2006年9月15日第1刷発行、ホームページ
http://www.kpmg.or.jp/resources/keywords/hotline.html）

内部通達制度を整備している、もしくは整備しつつある会社は多い。（内閣府調査では予定を含め、上場企業の91%になる）ただ、一部の管理者の方は、これらの制度が有効に活用されているのか良くわからないという声をよくきく。不正をいち早く認識し、その情報をすばやくすくい、対応するという点で内部通達制度はマッチしたシステムではある。そこで、統計的に調査した数字から御社の状況（特に「通達件数」）を判断して頂きたい。

通報件数177000件（2003～2006年）の傾向を分析した結果は、

（1）全体平均で従業員1000人あたり年間8.3件の通報がされている。

（2）65%は調査を要する重大な内容であり、全体の45%は調査の結果、何らかの是正処置がとられた。

（3）通報者の71%は管理者に事前に通報せず、直接通報制度を利用した。

（4）通報内容は、人事管理関連が一番多く、次いで社内／職業規範違反、雇用法違反、汚職・不正という順になっている。

（5）匿名は53%

（6）業種でみる1000人あたりの年間通報件数

トップ3

①小売業　18.39件

②運輸・通信・公共事業　9.42件

③卸売業　7.26件

逆にもっとも低いのは建設業で1.63件となっている。米国の事例なのでそのままうのみにするのは不適切ではあるが参考にはなると思われる。

出典:“2007 Corporate Governance and Compliance Hotline Benchmarking Report”

＊最新版は2009が既に公開しているが上記の切り口での情報はあまりなかったので2007版を採用しました。

## 内部通報制度の考え方

ここで一番重要な事例
「あなたの声をちゃんと聞きますよ」と思わせること。（当然ながら思わせているだけではいけない。PRが重要という意）従業員の方々がそう考えてくれないと絶対に成功しない。従業員が経営者に対して不信感をもっているなら、その時点でこの制度は失敗であると断言できる。

# 内部統制から見た「罰則は抑止力足るか？」

罰則は内部不正の抑止力として効果があるか？

罰則は不正行為が組織上の正当な部署に報告されて、はじめて効力を発揮する。いいかえれば、そもそも
①監視／観察が甘い
②報告する組織がない
③会社全体として（通報する）雰囲気がない
④報告した内容が握りつぶされている
こういう不安のある組織では、その罰則は有効に機能しない。
「不正行為は必ずわかってしまう」と従業員全員が納得のいく組織体制、システムを構築することで、初めて罰則の効果が最大限に活かされるのである。コンプライアンスの強化で一番しなければいけないものとは？

→社会、組織のTOPがその意識を尊重し、「うそ」は表向きも裏向きも、絶対にしてはいけないというメッセージを常々発信し続けることにある。
人間は弱い。ゆえに「正直が得」「うそをつくのは大損。目の前のわずかな利のために、比較にならない程大きな損となって返ってくる」と思わせる教育…それは倫理面もそうだが実際の状況においても、そういう体制、組織にしておくことが重要ではないだろうか？

ただし、組織上、すでにこのスパイラルにおちいっている所もある。そういう場合でも、とりつくろうことなく、きちんとした対応をすることで、その組織の努力しだいでまた復活もできるということを「伝える」ことである。

では「必ず発見される」という意識はどうやって従業員のほとんどすべての人に根付かせればよいのだろうか…　基本は啓蒙活動、セミナー、講習会、朝礼、社内掲示板（社内SNS等ネット上も含む）通知／通達／メールなどを通じて、検査という相互牽制、システムでの自動的なログ採取、メールのキーワードチェック、システム上のセキュリティ強化等を通じて「やってもムダ」的考えの浸透、こういう中での目安箱としての「内部通報制度」も相互牽制機能にあたると思われる。自分が降格処分になる、ボーナスや給与が大幅に減る。プライドが傷つく…などの状況と「逮捕！」「刑務所」というデメリットを天秤にかけた場合、どちらが重要かは明らかなはずである。社内が健全でも中間層が「ダメ」なら正当な会社運営は望むべくもない。（＝内部通報制度も機能しなくなる）

特に内部不正を勇気をふりしぼって通報するという流れをスムーズにするために中間管理職が毅然とした態度でのぞまなければ、一般従業員は通報しようという気がなくなってしまう。
ルールや体制だけ整備しても、そこに「心」が入らなければ、そのルールは死んでいるに等しい。よって経営側は前述した通報件数や社員の活力を見極め「通報が0」＝「うちは通報するような事態に陥っていない」とするのが適切なのか。「通報すらできない風通しの悪い状況」なのかを判断しなければならない。

# 【PR】社団法人情報セキュリティ相談センター

情報セキュリティにおける金融機関の対応は殆ど整備されていない・・・なんとか出来ないものか？

そう考え、社団法人「情報セキュリティ相談センター」を設立致しました！

何か情報セキュリティで問題が発生したら、取り敢えず「情報セキュリティ相談センター」に連絡すればいい・・・

そういう組織です。加入は無料でノーリスク・ハイリターンです

http://www.cis.or.jp/

# 吸収できるニーズのパターンイメージ

・会計不正の調査をしたい！（パソコンというより帳簿の不正探索）
・パケットの監視をしたい！
・フォレンジック調査を希望！
・内部通報者制度の適応を検討！
・USBの管理ができないか！
・この会議室は盗聴・盗撮の危険はないのか！
・DISKが壊れた（クラッシュ！水没！RAIDコントローラー不整、火災に真っ黒に・・・etc）
・セキュリティ・コンサルを希望！
・うちの事業所でセキュリティセミナーを開催して欲しい！（＋J－SOX＋内部統制・・・）
・ISMSの取得サポートを是非！（BS7799などの亜流も含める）
・Winnyで情報漏洩を起こした社員がでた！至急コンサルタントを依頼したい！
・従業員の自宅パソコンの監視までしたい！
・退職者パソコンの定期的調査を行いたい！
・Webの脆弱性検査を実施したい！（XSS、SQLインジェクション、OSコマンドインジェクション、CSRF・・・）
・2チャンネルで騒がれているみたい・・・どうすればいい！
・定期的に自社の情報が漏洩されているかチェックできないか！
・犯人はほぼ特定しているが証拠が欲しい！
・パソコンでの不正検査を被疑者の人の自宅パソコンで実施したい！
・クライアント様から情報漏洩の相談が来ている早く対応したい！
・社内に情報漏洩対策チームを組成した。助言を期待したいのだが・・・
・社長の行動があやしい。創設者だが挙動が不審なので不正調査士と相談したい！
・マスコミの会見をどう乗り越えれば一番ダメージが少なくなるか知りたい！

などなど・・・

# 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、ネット情報セキュリティ研究会でも各種技術指導を行う。
2008年6月まで三菱東京UFJ銀行に勤務。今年1月よりピーシーキッド株式会社上席研究員。

【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)

**2011年春に待望の**
**「情報漏洩/内部不正防止対策マニュアル」(仮称)が日科技連出版より刊行予定！**

# 【2009年後半からの最近の主な講演】（非公開セミナーや内部講演は割愛しています）

■福島県警招聘情報セキュリティセミナー（2009年7月15日）
■防衛省　情報セキュリティ教育（2009年8月～10月計6回実施）
■任天堂 「管理者・経営者向け情報セキュリティ啓蒙教育」　2009年10月14～15日
■FITフォーラム基調講演（福岡銀行協会、大阪銀行協会、名古屋銀行協会） 2010年1月～2月
■新潟県情報セキュリティの日制定記念セミナー 2010.2.19
■2010年2月日本セキュリティマネジメント学会「先端技術・情報犯罪研究部会」にて講演
■2010年3月10日情報セキュリティってこんなに面白い！感動の3時間をあなたに！セミナー
■2010年3月23日～26日　海外講演
■日本システム監査人協会CSAフォーラム 2010.4.26
■情報セキュリティEXPO「謎探偵ハギーセミナー」 2010.5.12～14
■2010年5月26日情報セキュリティってこんなに面白い！Vol.2セミナー
■2010年6月8日～9日　金融機関向け情報セキュリティ管理者養成コース
■ 2010年6月23日　実演でみる情報セキュリティの本当の恐ろしさVol.1
■ 2010年6月30日　第二回プライベート・セミナー
■ 2010年7月10日　ITC実務研究会セミナー（経済産業省、LAC、萩原で共同セミナー）
■ 2010年7月15日「クラウド・コンピューティングも危ない、なるほど、内部犯罪事例とその対策」セミナー
■ 2010年7月21日「金融機関内情報管理における情報漏洩防止策」ACCSとの共同セミナー
■ 2010年9月17日　ジャパン・クラウド・フォーラム2010　～The Dark Side of Cloud: クラウドの暗黒面～
■ 2010年9月22日　金融機関における内部犯罪/内部不正の事例と対策　～クラウド・コンピューティングも聖域ではない！～
■ 2010年10月21日～22日　金融機関向け「情報セキュリティ管理者養成コース」
■ 2010年11月29日中小企業同友会「情報セキュリティ」セミナー
■ 2010年12月1日ITmedia エンタープライズソリューションセミナー『あなたの会社は大丈夫？　組織内部に潜む犯罪の現実』

他多数

過去では海上保安庁や和歌山県警など数百以上ものセミナーや講演の経験を持ちます。

一般企業様の内部セミナーは原則非公開となっております。ご了承ください。

# 最近のネット投稿記事

■Itmedia 投稿記事

今までの記事　http://www.itmedia.co.jp/keywords/haggy2.html

シーズン1　ハギーが解説 目からウロコの情報セキュリティ事情　シリーズ

シーズン2　会社に潜む情報セキュリティの落とし穴　シリーズ

シーズン3　2009年12月21日より不正事件に学ぶ社内セキュリティの強化策シリーズ

シーズン4　2010年6月1日より「IT悪用の不正を防ぐ対策マニュアル」シリーズ

シーズン5　2010年9月26日より「会社を強くする経営者のためのセキュリティ講座」シリーズ

直近　2010年11月24日の投稿記事

第5回　社内のセキュリティ状況を把握する（環境チェック編）

http://www.itmedia.co.jp/enterprise/articles/1011/24/news012.html

# ご清聴ありがとうございました！

メール　jssm@hoshizora.jp

萩原栄幸

不定期にセミナーのご案内や有料セミナーの無料優待や割引の実施、最近の動向（経営者向け、技術者向けの2種あり）などについて平易に解説したメールをお届けしております。ご希望の方は上記のアドレスに「無料メール会員の登録希望」と件名に明記の上、氏名、会社名、会社（もしくはご自宅）の住所、お電話番号、所属、肩書きなどを記載してお申込みください。