中小企業向けの情報セキュリティの勘所

社団法人　情報セキュリティ相談センター　　事務局長
株式会社ピーシーキッド　　情報セキュリティ上席研究員
JSSM（日本セキュリティ・マネジメント学会）　理事
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
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

CFE（公認不正検査士）

萩原　栄幸

Mail: hagiwara@pckids.co.jp
jssm@hoshizora.jp

2010. 7. 10

講師略歴

PC KIDS

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)

2010年年内に待望の
「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！

【2008年からの最近の主な講演】（非公開セミナーや定期講演は割愛しています）

■KDDIユーザー会「情報セキュリティセミナー」2008.1.30
■富士ゼロックス　ビジネスソリューションセミナー2008　2008.2.6/2.8
■海上保安庁「情報セキュリティ講演会」　2008.3.11
■SAAJ（日本システム監査人協会）　月例研究会　2008.05.30
■「情報漏洩事件の本質を探る」秋葉原UDX2008.09.18
■ITproEXPO2008　「可能性を限りなくゼロにさせるために何が必要か」　2008.10.15
■「情報漏洩事件の本質を探る」大阪講演　新大阪MTビル2008.11.7
■@ITソリューションセミナー　誰もが悩む「内部からの情報漏えい対策と運用　2008.12.5
■デジタル・フォレンジックコミュニティ2008　in TOKYO　2008.12.16
■interop Tokyo 2009　「ちょっと早い？・・・名探偵ハギーの情報セキュリティ怪談」　2009年6月12日
■RSA Conference Japan 2009　「企業や組織に潜む情報セキュリティの落とし穴」　2009年6月12日
■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～9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2月民間企業様ハッキング・クラッキングのデモとその対策セミナー
■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

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。（現在月3回平均で全国で講演を行っています）

最近のネット投稿記事

PC KIDS

■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

いずれも極めて高い評価を頂いており昨年（2009年）のITmedia全体の投稿記事のTOP1、2共に私の投稿記事だったそうです。（Itmedia編集担当より）
シーズン4も6月1日、15日、29日・・・と隔週で継続しており、6月30日の午前10時でアクセスランキングで　2位、3位、6位と3本とも同時にトップ10入りを果たすことが出来ました！
感謝！

（1）はじめに・・・

今回は私の経験と実績から学んだいくつかの事象について解説して参ります。項目間の関連は殆どありません。「よもやま話」としてお聞きになり、御社にとって、少しでも情報セキュリティの向上や経営的なヒントになれば幸いです。

情報セキュリティコンサルタントとしての経験や銀行員としての経験が今の実績に繋がっている事実は本当に面白いものだと思います。

（2）パスワード

PC KIDS

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（社則とか〇〇規定とかいう）
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・・・
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。

（2）パスワード

PC KIDS

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5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700万回～1000万回です。
（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」というのは現場の情報セキュリティ管理者や
サーバー運用者なら「お判り」のはず・・・

（2）パスワード

PC KIDS

1：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。
先日も防衛省に7か所の拠点で啓蒙活動を行い、真剣にお聞き
になって頂いた、幹部の方、一般の自衛隊の方々・・・・・・・・・
でも、Winnyなどでの漏洩がその後にまたかと思うほどマスコミ
が騒いでいます・・・啓蒙活動は中小でも大企業でもNASAでも
重要なんです。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・・・ある中堅の東証2部上場
の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・・・

（2）パスワード

PC KIDS

２：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

（3）内部犯罪

PC KIDS

今、内部犯罪向けの対策マニュアルを執筆中で孤軍奮闘しています・・・
ここから中小企業の皆さまへ警告を1つ・・・
CFE（公認不正検査士）の過去20年での結果から抜粋すると
不正を行う人の特徴は20年変化がない
例　・勤続年数が長い
・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、休日出勤も厭わない、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）
・単独で業務をこなしている
・定期的な調査に抵抗感を示す
・自分の仕事場に人を近付けたがらない
・次から次へと仕事を引き受けようとする

などですが「AだからBである」からといって「BだからAである」ではないことに注意してください。

（3）内部犯罪

PC KIDS

今年5月に米国ミネソタ州にて「The Association of Digital Forensics, Security and Law」の内部犯行でのパネルにて公開された情報から抜粋

・21%の人が家族や友人に会社のPCを使わせたことがある
・自分の機器を会社で繋げたことがある・・・51%
・仕事用PCに私物データを入れている・・・約60%
・75%の内部犯罪はばれていない（どっから調べたのかな・・・？）
・毎年内部犯行は15%ずつ増加している
・管理者の40%が内部犯罪に遭遇している

COMPUTERWORLDより

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

（4）STOP The Winny！！！

昨年１１月より毎週もしくは隔週で投稿しており、評価が高かった「会社に潜む情報セキュリティの落とし穴」シリーズ・・・この中でコメント数が５０００を超え、転載していたMSN、Yahoo！、Mixiなどのサイトでもアクセス数がランキング１位になった記事が

Winny利用の果て――家族崩壊した銀行マンの悲劇

http://www.itmedia.co.jp/enterprise/articles/0901/13/news010.html

この内容について再度ご披露して、Winnyの怖さをご理解して頂ければと思います。

更には・・・ある中堅会社でのWinny事件での被疑者自宅に訪問した際での出来事とは！！！

フォレンジック（forensic）というのは、手元の辞書によると「裁判に関する～」や「科学的犯罪捜査の～」という意味を持つ法廷用語の１つ・・・昔の話
でもネット上での国語辞典検索や和英辞典検索でも未だにヒットしない方が多い。（英和のみ）
だが、世界でそして日本で極めて急激な成長をみせているのがいわゆる「コンピュータ・フォレンジック」「デジタル・フォレンジック」の分野である。

「デジタル・フォレンジック」とは？

PC KIDS

インジデント・レスポンス（コンピューターやネットワーク等の資源及び環境の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等、並びにそれらへ至るための行為（事象）等への対応等を言う。）や法的紛争・訴訟に対し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術を言います。

1.ハイテク犯罪や情報漏えい事件などの不正行為発生後にデジタル機器等を調査し、いつどこで誰が何をなぜ行ったか等の情報を適切に取得し、問題を解決するインシデント・レスポンスとして。

2.定期的にフォレンジックを用いた監査を行う事により、不正行為の発生を抑止するとともに発生後の対応を迅速に行えるようにする、広義の意味でのインシデント・レスポンスとして。

3.デジタル・データの保全、解析、保管等の取り扱い手法に関して適切に行われているかを議論する事により、相互の法的権利を正しく守る活動として。

特定非営利活動法人デジタル・フォレンジック研究会（http://www.digitalforensic.jp/）抜粋

簡単に一言でいうと・・・「デジタル鑑識」

では「鑑識」とは・・・

鑑識とは、高度な科学的知識や技術を用いて、犯人が現場に残した物や犯罪に使われた物などを集めたり、犯罪が行われた形跡を調べたり、写真などを撮ったりして、その物がなんであるかを調べ、さらに、それを残した人との結びつきを解明し、犯人の発見や犯罪の証明に役立てようとする仕事を言います。
指紋、足跡、血液は、これらを分析したり、今までに捕まった犯人のものと比べたりして、犯人を見つけだします。また、肉眼で見ることのできないようなごく小さな物でも、電子顕微鏡などを使って分析することで、犯人の手がかりとなることがありますから、例えば、ひき逃げ事件で塗膜片が見つかれば、逃げた車の種類を特定することができます。このため、糸くずのような繊維、ペンキなどの塗膜片、ガラス片、毛髪、金属片などを集める活動を行っています。
（関東管区警察局「警察Q＆A」より）

この作業目的は同じ場合が多いのですが（内部不正や退職者調査）その論理的根拠をパソコンやネットワーク、インターネットなどから求めようとするための専門的な作業が「フォレンジック」という事になります。

皆様が知っておいた方がいい知識

米国などではデジタル情報がそのまま「証拠」になりうるケースが多いのですが、それには「根拠」が必要です。疑わしい人のパソコンを調査するのであれば、必ずその「保全」を行い、調査をする＝環境を変化させ「原本」が変わってしまっては証拠として極めて不完全となります。

・電源を付けただけで数百以上ものファイルが変化してしまいます。
・正義感でパソコンおたくに近い方が、レジストリなどを見る方が一部いらっしゃいますが、その行為は自殺行為に等しいものです。どんどん証拠が希薄になりますので絶対に触らないでください。
・万一犯人の場合には・・・専門家でも矛盾のない証拠隠滅は極めて困難です（多分無理です）。証拠隠滅行為は罪を重くするだけです。早目に上司に相談される事を強くお薦めします。
・フォレンジックは専用機器で訓練を受けた専門の調査員が行います。通常の機材ではどんな専門家でもファイルを変更しないで中を見ることは出来ません。絶対にそのままにしておくことが「鑑識」作業を行う前の鉄則です。ここだけは覚えておいてください。

（補足） SJG事件とは？

SJG（Steve　Jackson　Games,Inc）事件

デジタル・フォレンジックについて話を遡る時に避けては通れない程有名な事件である。既に古典的な事件となったものの考えさせられる事件である。

１９９０年３月１日米国シークレット・サービス（法執行機関）は連邦法上の令状に基づきテキサス州オースチンのSJG社において業務用のコンピュータ３台、外付HDD５台、FD３００枚（そこにあったもの全て）、業務記録全て、出版間近のゲームブック全て・・・を押収した。その結果SJG社は業務の続行が不可能となりもうすぐ完成予定のゲームソフトの出荷が出来なくなった。しかもその後、SJG社の社長がハッカー行為の犯罪者扱いされ信用がガタ落ちとなってしまい、従業員の半数を解雇するに至ってしまった。

（補足） SJG事件とは？

ところが、その後の調査でSJG社も社長もハッカー行為とは全く無関係であると判明したがシークレット・サービスは3ヵ月後の６月になってやっと押収物を返還している。
この事件後、いわゆる「写し（コピー）」の証拠能力が問題となり、原本主義を徹するならあまりにも現代の企業がコンピュータに依存しておりどんな会社でもとたんに業務停止となり倒産する会社も出てしまう・・・押収物を分析して「犯人」かどうかの特定をする法執行機関にとっても極めて重要な問題となっていったのである。よって「完全なる複製」なら押収物としても裁判所への提出物件としても効力があるという理論的な解決方法として開発されたのが「フォレンジックツール」なのである。法執行機関においても一般企業においてもどちらにおいてもこの考え

は重要であり、今日に至っている。
押収物の封印、フォレンジックセンターでの開封とそのすべての完全なデジタルデータの複製・・・・こういう作業が制度化され、企業においてもこのツールを積極的に使用する事で個人情報漏洩防止や漏れた場合の速やかな、かつ論理的な犯人の特定に至るまでの業務フローの確立・・・こういう仕組みが既に出来上がっている。ツールは警察やFBIなどの法執行機関から普及し、フォレンジックセンターの設立に伴い、裁判所、官庁・・・そして金融機関、製造業、サービス業へと広がっていった訳である。
そして大手の会社の殆どで今ではフォレンジックに関する専門の部署が設置されるに至っている。日本は先進国の中では一番遅れていたが近年、総務省、経済産業省、厚生労働省、警察庁、防衛省などが積極的に活動を行っている。

フォレンジックで一番重要なことは
「原本は崩さない」「裁判でもその原本同一性が
担保できる作業で終始していること」・・・・・・・・
このような環境で保全を行いその後、様々なツー
ルを駆使し、分析を行っていきます。
はっきりいって・・・ホリエモンが削除した4万通と
言われたメールなど全て復元され証拠となりまし
た。素人ではとても矛盾のない証跡削除は困難です！

（6）ボットの本当の怖さってご存知ですか？

PC KIDS

Telecom ISAC JapanとJPCERTコーディネーションセンターが行った調査で判明した事

1：国内のPCの2.0～2.5%がボットに感染
（台数ベースでは100万台程度？）

2：ボット端末1台あたりのスパム送信能力は1時間あたり6890通（1秒間に2通程度）。最大では1万通以上になる 。

3：未対策のPCをインターネットに接続すると平均4分間で感染

4：ボットの多くはウイルス対策ソフトウェアの機能停止を試みる

5：企業のイントラネット内に侵入しているケースも散見される

この中で一番怖い情報とは何番でしょうか？

私たちが気をつける事とは？

（7）「掃除」で学ぶ情報漏洩

私が新人の頃・・・毎日、清掃会社の方が夕方に各人の机の横にあるゴミ箱の中をビニール袋の中に入れて回収作業をしていました・・・業務の効率化、経費削減・・・様々な名目のもとでこの類の費用は削られ今では・・・一番多いケースは

・平日は社員が決められた場所に自分でゴミを捨てる
・床やその他の清掃は週１回しかも作業中だと効率悪化するので土曜日に清掃会社で清掃を行う

その結果・・・・・

あなたのビルは如何ですか？

（8）本当に業者を信用してもいいですか？

以前「クローズアップ現代」でNHKと私が共同でランダムに
購入したハードディスクの復元率・・・7割（2002年）
2006年調査では14%（NTTネオメイト調査）
今年2010年の米国からの公開情報からはe-Bayから購入した
中古HDDの34%から情報が漏洩と・・・

業者から聞き出した本音とは？
完全消去って何回上書きすればいいの？
（グートマン論文では35回らしいけど本当ですか？）
注意しなければいけない事とは？

以前、出演した中に「あなたのデータが流出する～パソコンリサイクルの落とし穴～」があります。ここでは秋葉原で購入した30台ものHDDを実際に2日間かけて復元したのです。そこで放映されなかった事とは・・・・
その事実を今ここに！

プライベート（私用）なら・・・1回の上書きでも可
ビジネス（仕事）や公用なら・・・2回の上書きがを推薦します

通常の完全消去ソフトは1回～99回までの指定が可能で
ペンタゴン方式や独陸軍方式など3回以上の上書きを推薦したり
グートマン論文での36回以上を推薦される方がおりますが現実的
ではありません。現在主流の1TBのHDDを36回上書きしたら・・・
多分1週間以上かかります・・・こんな事はもう止めましょう！！！

（9）情報セキュリティ管理者として

PC KIDS

前提：企業に勤めていて情報セキュリティを「業務」の1つ（もしくは全て）として作業される、担当者、管理者、役員（含CIO等）、経営者

①：情報セキュリティとは？

→在り来たりな用語辞典、本の解説はどうでもいい・・・

誤解を恐れずに言うなら・・・

「会社を存続、成長、飛躍させるための大きな「材料」として、もしくは会社を破滅に追いやる「爆弾」として極めて慎重に扱うと同時に他社、他業態の追撃をかわす、もしくはTOPに追いつき、追い越すチャレンジ精神の「道具」として大胆に「王手」をかけるための重要な駒として使い方によって自在に変化する「物」「情報」「精神」である。」

②：極めて珍しい「例外」を作成してはいけない物

→「社長なら・・・」「CIO（情報担当役員）だけは」

という考えは捨てなさい！セキュリティ・ポリシー

は全員（外注の方も、派遣の方も・・・（労基法に抵触しないように））厳守すべきバイブルとなります。

内部統制の原則は「透明性」「統一性」「厳格性」

にあります。

③：アクセス・コントロールは・・・

「業務上、〇と△は駄目！それ以外ならOK！」

この考えは誤りである事に気が付いて下さい！

ネットワークのファイアーウォールと考えは同じ！

つまり・・・デフォルトは全員が更新は無論、アクセスすることも印刷もコピーも全部禁止！・・・・・・・

そこから「真に必要な権限者」に限り、その動向をトレース、監視しつつ許可するのが正しいのです。

④：社長は悪さをしない・・・

そういう考えは捨ててください。

あなたの会社には「社長が悪さをした場合の発見する体制、その場合のプラン」が整っていますか？

なければ・・・不二家、パロマ、船場吉兆の様にあなたの会社の名前が載るかも知れません！

⑤：セキュリティと利便性

相反する・・・確かにそういう面もある・・・しかし

共存共栄することを常に意識することが重要！

大学の先生ではない、企業（如何にして利益を増大させるかが究極の目的）としての創意工夫がここに求められます！

机上の空論より現場百回！

⑥：情報セキュリティ管理者は「経営者」「プロジェクトリーダー」の視点で観察せよ！

ー昔前はセキュリティ関連部署は「ショムニ」的存在であった・・・しかし、今日ではエリートコースの1つになっている企業が少なくない・・・それは、ここの分野では優秀な経営者として、また優れたプロジェクトリーダーとしての視点で判断しなければならない事象が少なくないからである。

内部からの情報漏洩事件・・・私がお伝えしたい事・・・

撲滅するために・・・確信犯での流出を防止すること！

→ここでいう「確信犯」とは故意による金銭搾取目的という事象より「善意」による確信犯という意の方が大きい。

「残業しても終わらない」「性格がルーズ」「昔からの仕事方法を変えられない」「会社の為に頑張っているのだから」「会社の言う事をマトモに聞くと仕事にならない」・・・・・

結果的に99%は大丈夫だろう。でももしもの場合は・・・・

個人も会社もダメージが大きい。

啓蒙活動しても社則で禁止しても、実際に守れない職場、部署、人がいるなら「絵に描いたモチ」に過ぎない。。。

最近、耳に入ってくる内容

→事件、事故を防止するという大義名分のもと、職場が委縮、モラル低下、諦め、という雰囲気が漂い結果として「善意の確信犯」が急増という。これでは、明日にでも御社の情報漏洩事件の謝罪記者会見が行われても不思議ではありません。・・・こういう団体・会社は決して少なくありません。

（NISや自分の公開アドレス「情報セキュリティ相談センター」に寄せられた非公開情報からの傾向です。先月も某地銀の役員から深刻なご相談がございました。）

情報漏洩防止管理者、責任者、担当者はルールの新規策定、強化、検知や防止のためのシステム構築、運用などを通じて監視するだけではありませんか？この考えは過去のものです。会社全体、職場、作業域などの集団の経済活動状況を把握し、ともすれば社員の意向を無視し、モラルの低下、勤労意欲の減退、強いては生産性低下、収益下降という事態を最大限に防止する為に、啓蒙活動、メンタルケア、を積極的に行い、職場の意見に耳を傾け「検証」を行う事がきわめて重要となります。
その為に経営側に懐柔することなく、時には進言する事も必要な場合もあるとお考えください。
時々、仕事をパッチワーク的に考え「私はポリシーを策定すればいい」などと、誤った考えを持つ方がいらっしゃいます。一部のコンサルタントなどから無責任な思考を刷り込まれない様にお願い致します。

現状の人・物・金・システム・業務フローなどのリソースと制約条件に対して、新規のルール、社則の強化、レポートや報告書作成、監査報告の項目増加などを全体として付加加算した場合従業員に過大な負荷を強いる事になっていないか？結果的に破綻する状況になりやしないか？など、必ず検証する様に心がけてください。
壮大なダムも一番脆い箇所からひびが入ります。組織も同じです。新社則や情報漏洩策としての新システム導入など一番影響のある職域、組織、そして人が耐えられるのか？机上での平均値を見ても意味がない。現場で確認し、個人が耐えられるか？を検証すべき時期に来ていませんか？既に決壊している組織かも知れません。（たまたま事件に繋がっていないに過ぎません）善意の確信犯が多数でてはどんな防止策も意味がありま

せん。弱者が守れないルールを押し付けることのないにしてください。大概は情報漏洩防止策がりっぱなものであれば有るほどリスクが大きくなるという事も事実であることをお忘れにならない様にお願い致したい。

ご清聴ありがとうございました！

80分の内容にしては若干詰め込み過ぎたかも知れません。
この場をお借りしてお詫び申し上げます。

萩原栄幸