# 脅威の総論

## 脅威のとらえ方


株式会社ラック
サイバーリスク総合研究所
特別研究員　西本 逸郎
itsuro@lac.co.jp
http://www.lac.co.jp/

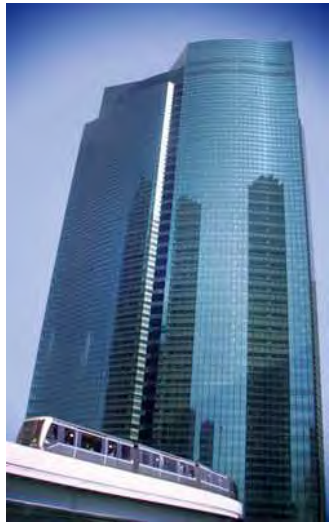
# 株式会社ラック

## 世界トップレベルのセキュリティノウハウを、日本の全てのオフィスへ。

1986年、株式会社ラックは設立されました。”Little eArth Corporation”という社名には、ITの進展で地球が相対的に小さくなっていく中で、ITを基盤に国や企業の発展を支えていこうという理念がこめられています。
独立系セキュリティベンダーとして15年の豊富な実績がお客様の信頼の証です。

**ＪＳＯＣ**（下記参照）、**サイバーリスク総合研究所**、**サイバー救急センター**が特徴です。

| | |
|---|---|
| ● 商　号 | 株式会社ラック<br>LAC：Little eArth Corporation Co., Ltd. |
| ● 設　立 | 1986年(昭和61年)9月 |
| ● 資本金 | 11億5,942万6,500円 |
| ● 株　主 | ラックホールディングス株式会社(100%) |
| ● 代　表 | 代表取締役社長 執行役員社長 齋藤 理 |
| ● 売上高 | 7,480百万円(24期：2008年03月期)<br>※決算期変更による12ケ月換算 |
| | 7,154百万円(22期：2007年12月期) |
| | 6,454百万円(21期：2006年12月期) |
| ● 決算期 | 3月末日 |
| ● 従業員数 | 338名（2009年3月現在） |
| ● 認定資格 | 経済産業省情報セキュリティ監査企業登録<br>情報セキュリティマネジメントシステム<br>(ISO/IEC 27001)認証取得(JSOC)<br>プライバシーマーク認定取得 |



本社　〒105-7111　東京都港区東新橋1-5-2
汐留シティセンター11F
03-5537-2600(大代表)
03-5537-2610(営業)

セキュリティ監視センターJSOC
〒105-0001　東京都港区虎ノ門4-1-17
神谷町プライムプレイス3F

名古屋オフィス
〒 460-0008　名古屋市中区栄3-15-27
名古屋プラザビル 9F


■ JSOC (Japan Security Operation Center)

JSOCは、ラックが運営する情報セキュリティに関するオペレーションセンターです。高度な分析システムや堅牢な設備を誇り、セキュリティ分析官とインシデント対応技術者を配置し24時間365日、運営しています。2000年の九州・沖縄サミットの運用・監視を皮切りに、日本の各分野でのトップ企業などを中心に、高レベルのセキュリティが要求されるお客様に高品質なサービスを提供しています。

# スピーカ

## 西本 逸郎（にしもと いつろう） CISSP

| | |
|---|---|
| 昭和33年 | 福岡県北九州市生まれ |
| 昭和59年3月 | 熊本大学工学部土木工学科中退 |
| 昭和59年4月 | 情報技術開発株式会社入社 |
| 昭和61年10月 | 株式会社ラック入社 |

通信系ソフトウェアやミドルウェアの開発に従事。1993年ドイツのシーメンスニックスドルフ社と提携し、オープンPOS（WindowsPOS）を世界に先駆け開発・実践投入。2000年よりセキュリティ事業に身を転じ、日本最大級のセキュリティセンターJSOCの構築と立ち上げを行う。
さらなるIT利活用を図る上での新たな脅威への研究や対策に邁進中。

情報セキュリティ対策をテーマに官庁、大学、その他公益法人、企業、各種ITイベント、セミナーなどでの講演、新聞・雑誌などへの寄稿等多数

株式会社ラック 取締役 常務執行役員 最高技術責任者
サイバーリスク総合研究所 特別研究員
特定非営利活動法人 日本ネットワークセキュリティ協会 理事、社会活動部会長（現任）、セキュリティ評価WGリーダ/ST作成WGリーダ（歴任）
特定非営利活動法人 日本セキュリティ監査協会 理事
データベースセキュリティコンソーシアム 理事、事務局長

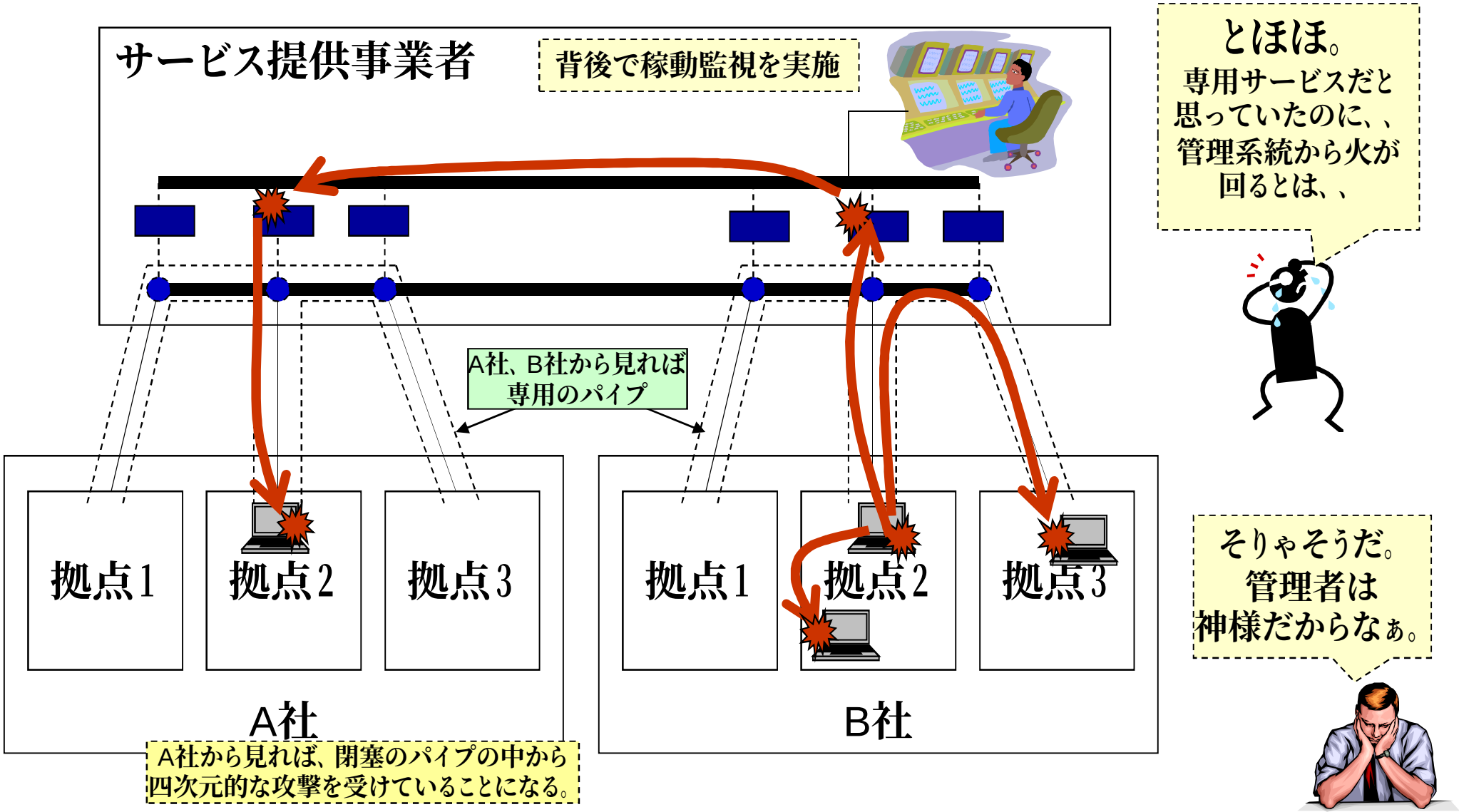
連載・コラム
西本逸郎のセキュリティー表ウラ
セキュリティー表ウラ 検索
http://it.nikkei.co.jp/security/column/nishimoto_security.aspx

ツイッター
http://twitter.com/Dry2

# 0．最近の印象的な事件から

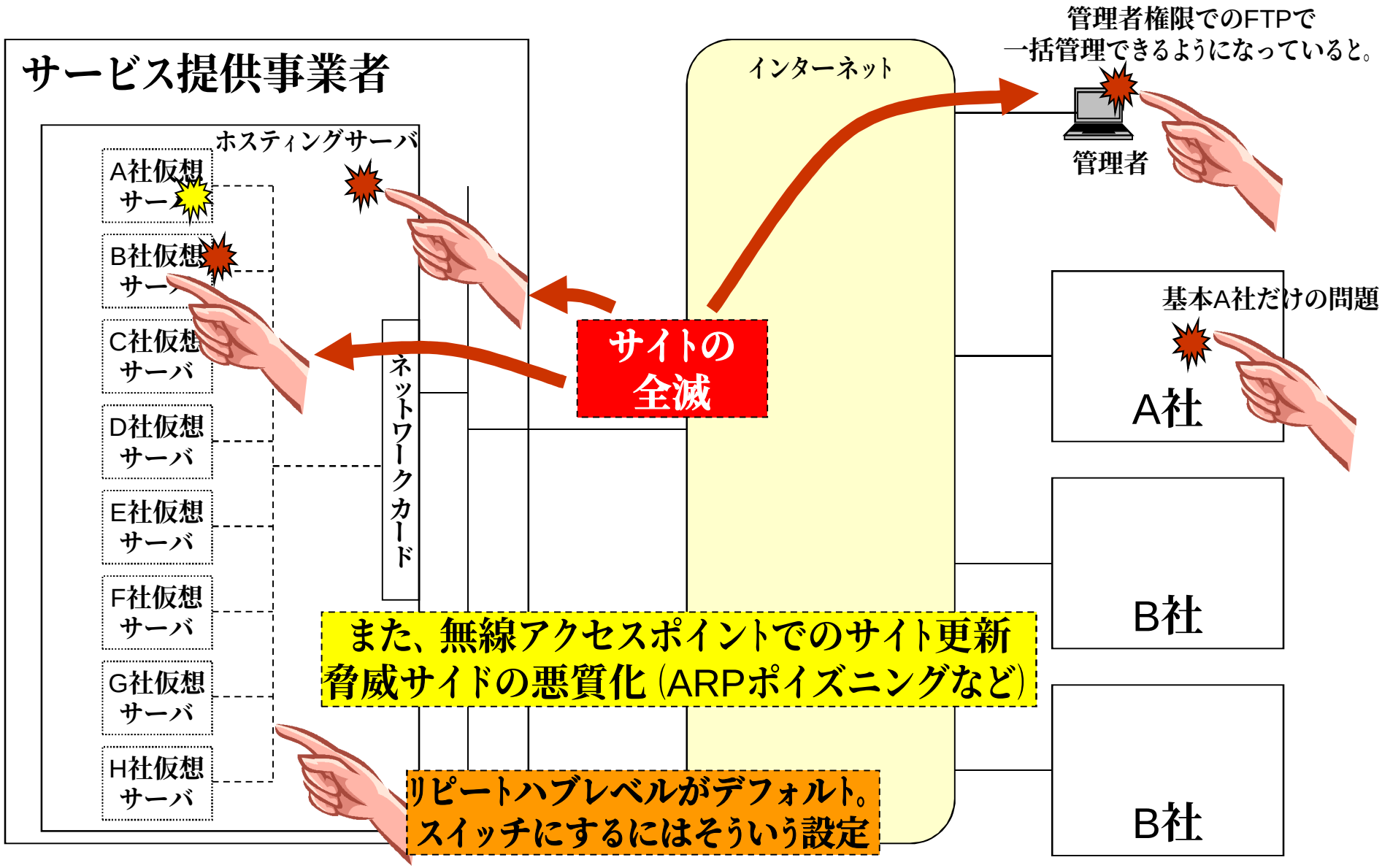
# 印象的な事件

あるサービス会社でのIP-VPNサービスでのウイルス感染事件のイメージ



# 印象的な事件

## あるホスティング会社でのガンブラーウイルス感染事件のイメージ



# 印象的な事件

## サインは V 仮想化 irtualization

## 仮想は、仮想であり、実物ではない。

VPN、広域イーサ（仮想的イーサ）、VLAN、仮想サーバ、仮想デスクトップ、
仮想ドライブ・ストレージ、仮想アプリ、仮想サイト、など

## 「仮想」がついたサービスは、、四次元攻撃が成立する。

管理者は「神様」。サービス事業者（管理者）の信頼度が極めて重要。
そういう認識は一般的には薄くなる。アウトソース ⇒ XaaS ⇒ クラウド

# 1. クラウド インパクト

# クラウド（雲）

# クラウドに走る理由（個人的な意見）

0. 短期的には経費カット

1. 経費の流動化
2. 事業の自由度確保
3. トータルコストの削減

成功へのハードルを低く、
機動力を最大限に。
継続的ダメージを最小限に

<u>生き抜いていくこと。</u>

その為には我々は環境適応し続けなければならない。
将来役に立つかもしれないけど、重たい荷物はいらない。

# 背景

ところで、
　日本人は品質にこだわるっていうのは本当？

海外旅行や出張。航空会社の選択基準は？
SNSやオンラインゲームからのポロロッカ（逆流）

すでに、コンビニや居酒屋
　　多くの物理的サービスの接点

さらに、デフレ・ネイティブの誕生。草食系の台頭。
選択肢の多様化。既存（不採算）サービスの死滅。
参入障壁の破壊。（おまけ的ビジネス）

# 背景

# A.D.201X

クラウドをトリガーとして ビジネス(サービス)の

## 新大航海時代が始まった。

世界的規模のサービスバトル。

**犯罪は既に大航海時代へ。**

しかも、犯罪クラウドサービス利用が当たり前。

BOT、犯罪基盤aaS

# 犯罪者とクラウド

不正クラウドサービス基盤　ボットネット

犯罪用クラウドサービス　　犯罪者向けセンター
RBN など

クラウドサービスの悪用　　アマゾンEC2など

残念なことに、犯罪者側の活用の方が
早いのかもしれない。

# 背景のまとめ

この**３０年の間**でみると、特にここ**数年の変化**があまりにも大きい。

**電算機**と呼ばれ、基幹システムとして君臨
　　情報システム部門が一括管理の時代

ブログ　⇒出版
Twitter ⇒ 取材と公開
　　リアルマーケなど

**汎用パソコン**が導入され、基幹業務以外に、
身の周りのお仕事にも使用。ワープロ、表計算
　　オフィスの生産性、、**EUC**という言葉も。　**EUS**は無いなぁ、、

インターネットを駆使し、ビジネス展開。
　⇒ **知識の平準化**。２４時間の「勤務」

クラウドの時代、仮想化、SaaSなど
　⇒ ガラパゴスの死滅　地域の平準化
　⇒ ビジネスの**新大航海時代**

ビジネスや生活を変えたもの
ウォークマン、ゲーム
ワープロ、**表計算ソフト**
**携帯、メール、検索**
**ブログ、SNS、**amazon、
Twitter　　今後、、？？？

# 時代は繰り返す

『坂の上の雲』とは、封建の世から目覚めたばかりの日本が、そこを登り詰めてさえ行けば、やがては手が届くと思い焦がれた欧米的近代国家というものを「坂の上にたなびく一筋の雲」に例えた切なさと憧憬をこめた題名である。作者が常々問うていた日本特有の精神と文化が、19世紀末の西洋文化に対しどのような反応を示したかを、知るのに最適の作品である。

From Wikipedia

**雲**により再度**大航海時代に突入**した21世紀

出遅れた、我々はどうやって、

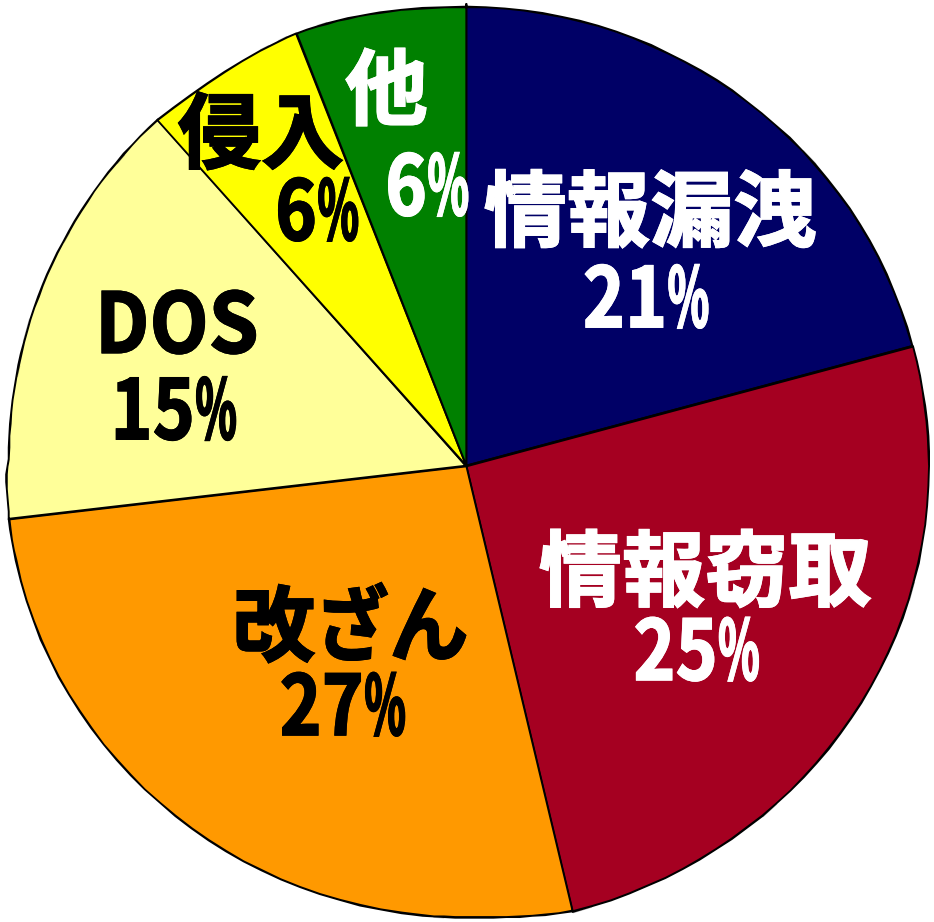
「坂の上の雲」を

つかむことが出来るのか？

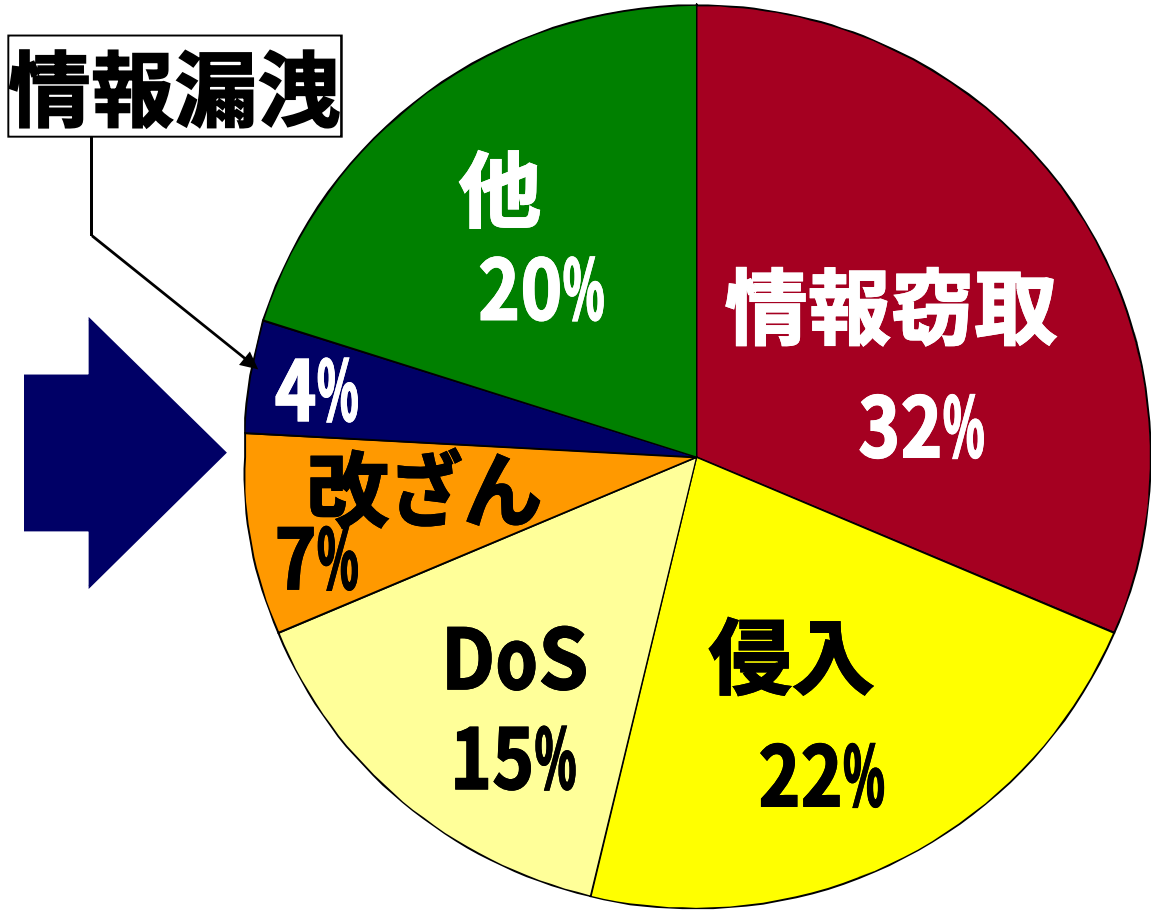
# 2. セキュリティ事件

# サイバー救急センター 出動状況 2009

## 2008年



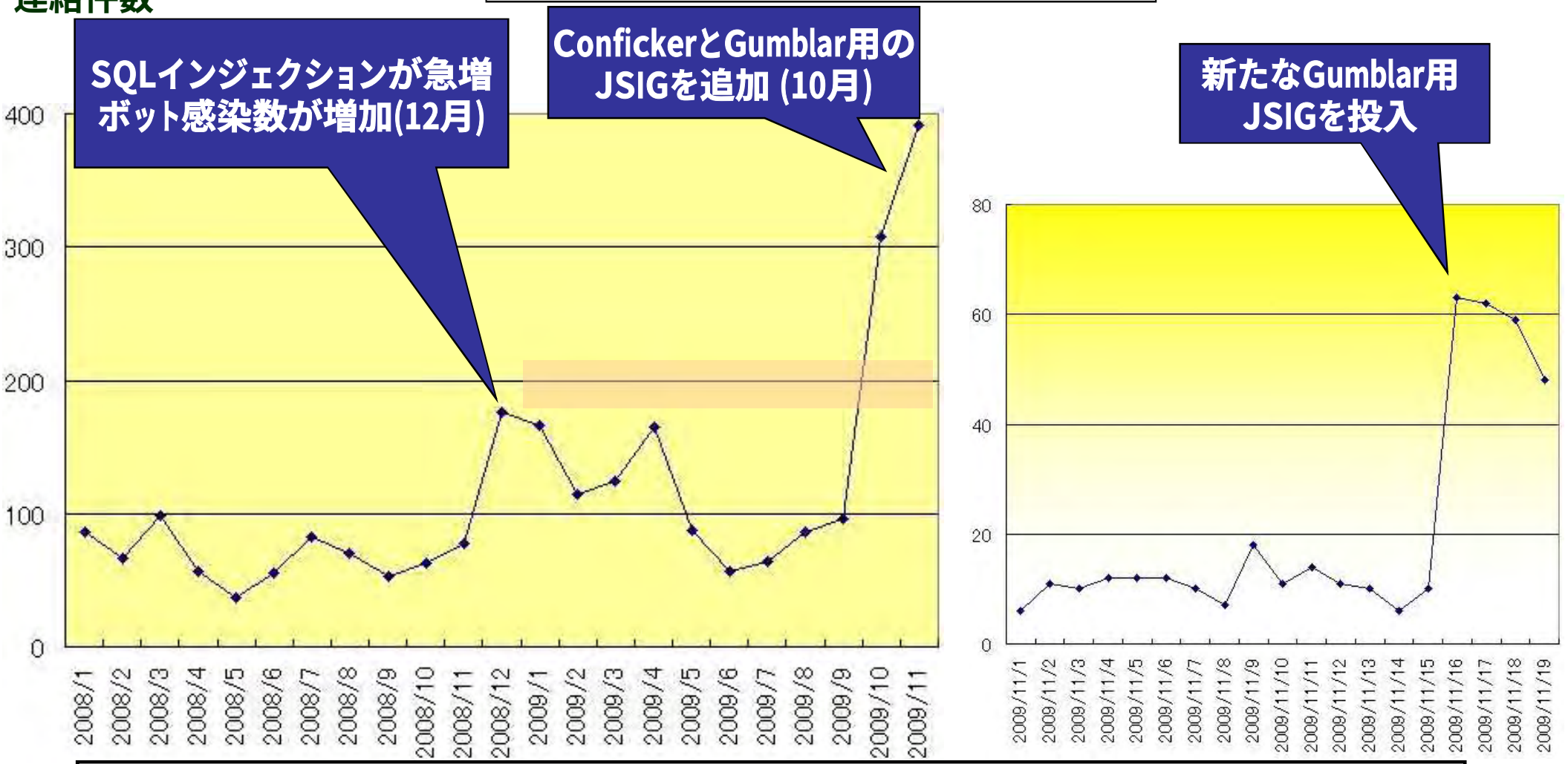

## 2009年10月上旬まで



# 組織内部のウイルス活動

## お客様内部から発生したインシデントの傾向

連絡件数




- 2008年12月にSQLインジェクションでホームページの大量改ざんが発生
- 改ざんされたホームページを参照したユーザはボットを埋め込まれる
- JSOCの１０%のお客様で感染を確認(通常は1%～2%程度)

# ガンブラー　誰にとってどんな脅威が

報道内容「サイト改ざん」

まぁ、わかり易いし、、

本当の狙いは？

しかも、対策や関心は、

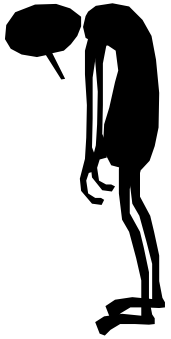
ガンブラーに感染しないように するには？

に、終始している。

脅威と対策が
整合してないのでは？

# サイト改ざん　疑似体験

# まさか、自分が、、、、、



## 何が起きるのか？

利用者からの問い合わせ
Googleで「危害を与える可能性」
比較サイトなどからリンクを切られる
アフィリエイトから外される
メディアから問い合わせ
掲示板で叩かれる、揶揄される
ニュース報道　利用者から苦情
IPA・JPCERTから問い合わせ？
警察から問い合わせ
Pマーク 再審査
株価への影響

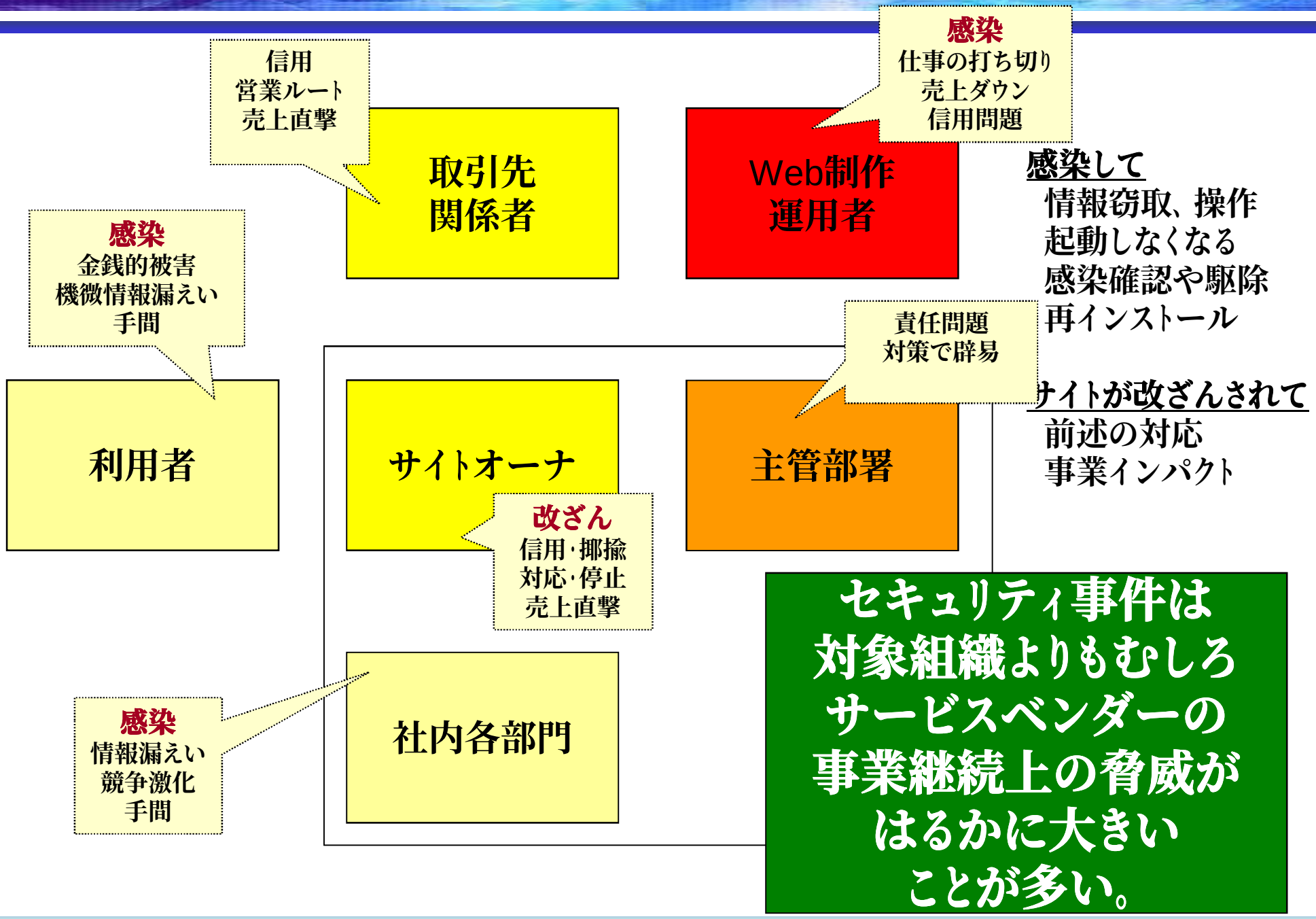
## 何を調べる？

何が起きている？いつから？
被害は出ているのか？情報漏えいは？
被害可能性のボリュームは？
どうすればいいのか？今はどうなんだ？
利用約款、SLA、契約、保険
事業インパクト

## 誰に誰が何をどうやって何時までに？

利用者、従業員、協力会社
取引先、Google、アフィリエイト、比較サイト
証券市場、株主、機関投資家
弁護士、委託先、セキュリティ専門会社
警察、IPA、JPCERT、JIPDEC、監督官庁
保険会社

# ガンブラー　誰にとってどんな脅威が



# そう言えば、ウイルス対策

## ウイルス対策といえば、、、

何故だか、**対策 ＝ 駆除** だと思っている組織があまりにも多い。

いろんな提案を持ってくるが、「うるさい！しっかり駆除できればいいんだ。駆除できるものもってこい！」とおっしゃる方は多い。

組織のスパイ対策は、「スパイを見つけ始末することで終わり」と言っている様なもの。
⇒ もし、スパイを捕まえたらどうしますか？始末して終わりですか？
　スパイの目的を知ることが重要。

逆に言えば、スパイが内部にいるのは前提の組織作りが求められている。

**つまり、ウイルス対策の考え方が、すでに間違っている。**
**ある面、ウイルスはいるのが当たり前。脅威に目をやろう。**

# もうひとつの事件Conficker蔓延

## 2009年3月以降
## Conficker（Downad、Kidoなど）蔓延による、沈静化の緊急出動要請が続出！

出動メンバーが見た光景、、、

疑心暗鬼の目線、、、

誰にも相談できない、苦悩。

# Confickerがゾンビのようによみがえる！

1. オンラインでの管理者ログオン
   ⇒ さっき駆除したマシンには必ず感染活動！
2. 駆除ツールが古い！
   ⇒ 一括管理している駆除ツールを全て最新化出来ない
3. パソコンの電源、出張･外出戻り
   ⇒ 全て完了と思ったのに
4. 知識不足
   ⇒ 駆除ツールにより、動作が異なる
5. USBメモリ、デジカメ
   ⇒ 全て管理できていなかった
6. 新型に変異、他のウイルスの存在
   ⇒ どこまでを前提にするのか。どこから日常なのか。
7. 管理ミス
   ⇒ 台帳管理、駆除手順･確認ミス、勘違い･思い込み

# 参照：「Conficker が駆除できない」

# 世間でのセキュリティ事件

## A証券 元システム部長代理 顧客情報持ちだし売却事件

元システム部長代理Aが、別の従業員のIDとパスワードを使用して顧客情報を管理するサーバーにアクセス(**不正アクセス禁止法違反**:1年以下の懲役または50万円以下の罰金)して顧客情報を抜き出し、

暗号化し作業用のサーバーに保管。(**暗号の目的外使用⇒ポリシー違反？**)

CDを作成する際、オペレータに対して「特殊な作業」と偽って、この暗号化した顧客情報をCDに保存するよう指示。
(**A並びにオペレータのポリシー違反**) ⇒ いや、むしろ **ポリシーや規程の形骸化** ？

システム部で作業すると偽って、約148万人分の情報が入ったCDを自宅に持ち帰り、約5万人分を売却。(約33万円)
さらに、会社で購入した約4439万円相当の企業概要情報を記録したCD2枚を持ち出した。
(**一枚65円相当のCD三枚の窃盗罪**:10年以下の懲役または50万円以下の罰金)

11月12日、東京地裁は **懲役2年(求刑懲役2年6月)の実刑判決** を言い渡した。

日本では、情報窃盗罪が無い。ある面、<u>良く実刑2年まで持って行った</u>。

⇒ 世間感覚では、大罪。しかし、実質には200円足らずの窃盗。
不正アクセスの場合は最大でも1年。法律と現実の大きな乖離。

# 世間でのセキュリティ事件

## A証券 元システム部長代理 顧客情報持ちだし売却事件

金融庁
⇒ 金融商品取引法 に基づく業務改善命令
⇒ 個人情報保護法 に基づく勧告

会社としての損失
⇒ 情報が流出した約5万人に対し「お詫びのしるし」として1万円相当のギフト券で約5億円
⇒ 事件調査、顧客対応、顧客情報の売却先名簿業者との交渉費用、発注減少による逸失利益など

**約70億超** の損失

システム部相応の人間のこの種の犯罪は、**銀行員の横領、証券マンや記者のインサイダー**

くらいに、**恥ずかしく**、しかも、あってはならぬこと。

しかも、お金関係の場合は会社での **穴埋めも可能** だが、**情報漏洩はそうは行かない**。

全く、この種のエンジニアとして **許しがたき大罪。プロ意識の欠如。**

# 閑話休題

## プロ意識といえば、、、

某、大手企業 社長秘書 Aさん のはなし。

社長になり代わり、毎日数多くのメールの送受信を実施。

今まで、誤送信などやったことはありますか？

Aさん「一回もありません。これからもやりません。」

何故そういい切れるのでしょうか？

Aさん「それは、私の仕事だからです。」

メールで間違う **我々はプロ意識が無い** ということで。orz
いずれにせよ、ことのあり様はプロを殺して排除してしまう危険性も。

# 世間でのセキュリティ事件

## A証券 元システム部長代理 顧客情報持ちだし売却事件

考慮ポイント

⇒ 経営者の責任
⇒ プロ意識の欠如とその蔓延
⇒ その上でのポリシーの形骸化

⇒ 形式的なトップダウン、機能しないボトムアップ

ガチガチのセキュリティが必要な会社、或いは要求される会社であっても、

正しい **職業倫理やプロ意識がない組織** は問題。

2010年9月頃より、改正不正競争防止法が施行予定。
ライバル会社に行かなくても、営業秘密の持ち出し売却で適用される。
準備が必要。10年以下の懲役又は1000万円以下の罰金

# 外部からの脅威

1. 侵入事案
   ⇒ 犯人は複数いる。
   以前からひっそりと 侵入している忍者型。
   根こそぎ持っていく海賊型。
2. 大騒ぎウイルスの狙い
   ⇒ やることが大胆 になってきている。
   海賊型、しかも戦利品は売却か？忍者型は駆逐される。
3. 侵入経路
   改ざんホームページ閲覧
   USBメモリ
   標的型メール

# 内部関係者の犯罪

1. 情報システム部門
2. 上司のパソコンの面倒を見ている部下
3. 協力会社（特にオフショア開発・運用）

共通して言えること

# 丸投げ

# 3. 情報セキュリティって？
# 初心に戻って

# セキュリティとは？

情報セキュリティとは、主体が客体にアクセスする上での
**機密性（C）、完全性（I）、可用性（A）**を守ることにある。

**つまんないなぁ**

こういうビジネスマン（会社）はどうですか？

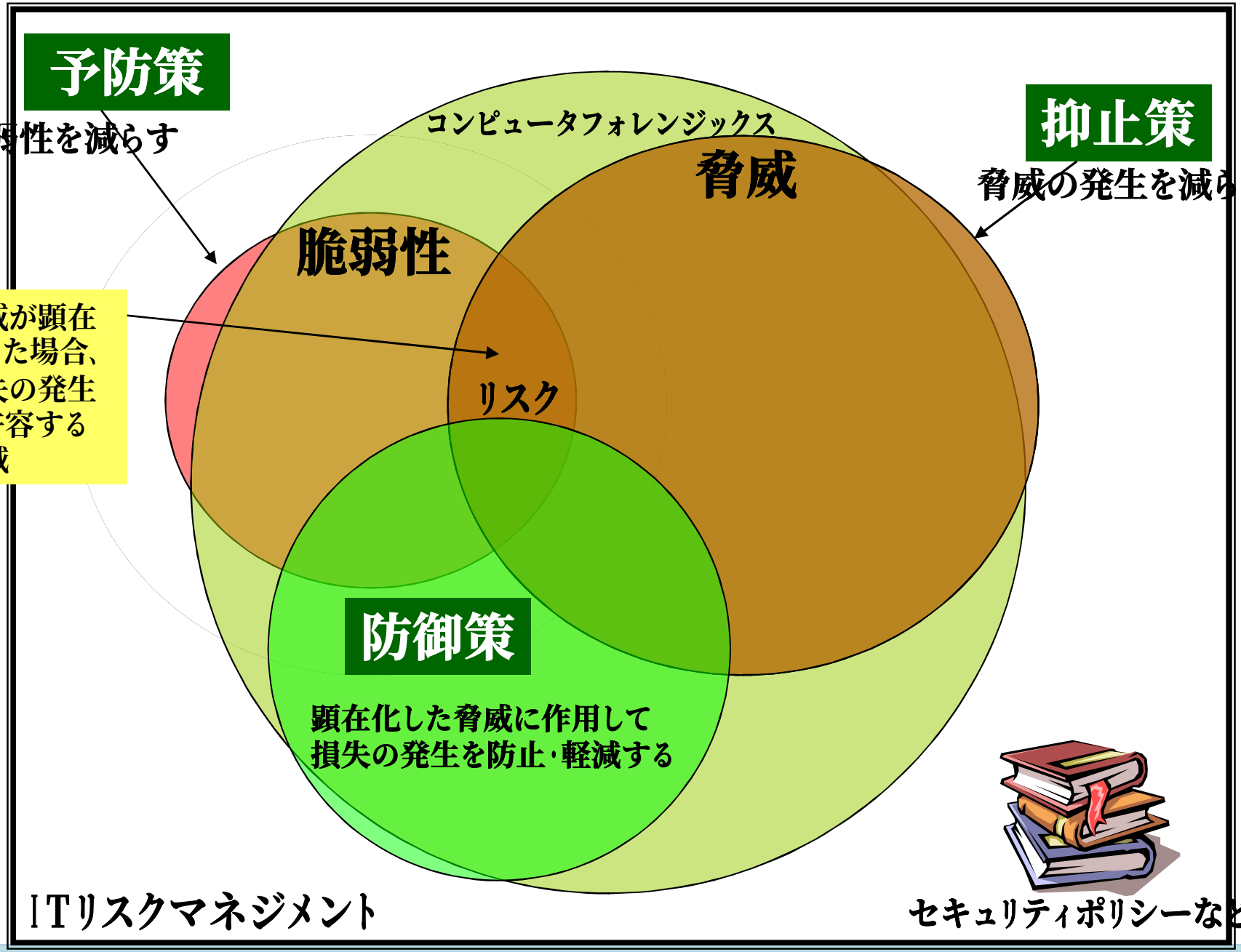
何が秘密か分からない。しかもぺらぺら良くしゃべる。（C）
見積書・請求書は間違いだらけ、納品物も壊れている。（I）
連絡がつかない遅い、肝心なときに遅刻や欠勤する。（A）

実社会においては、
セキュリティの無い
ビジネスは
有り得ないということだ。

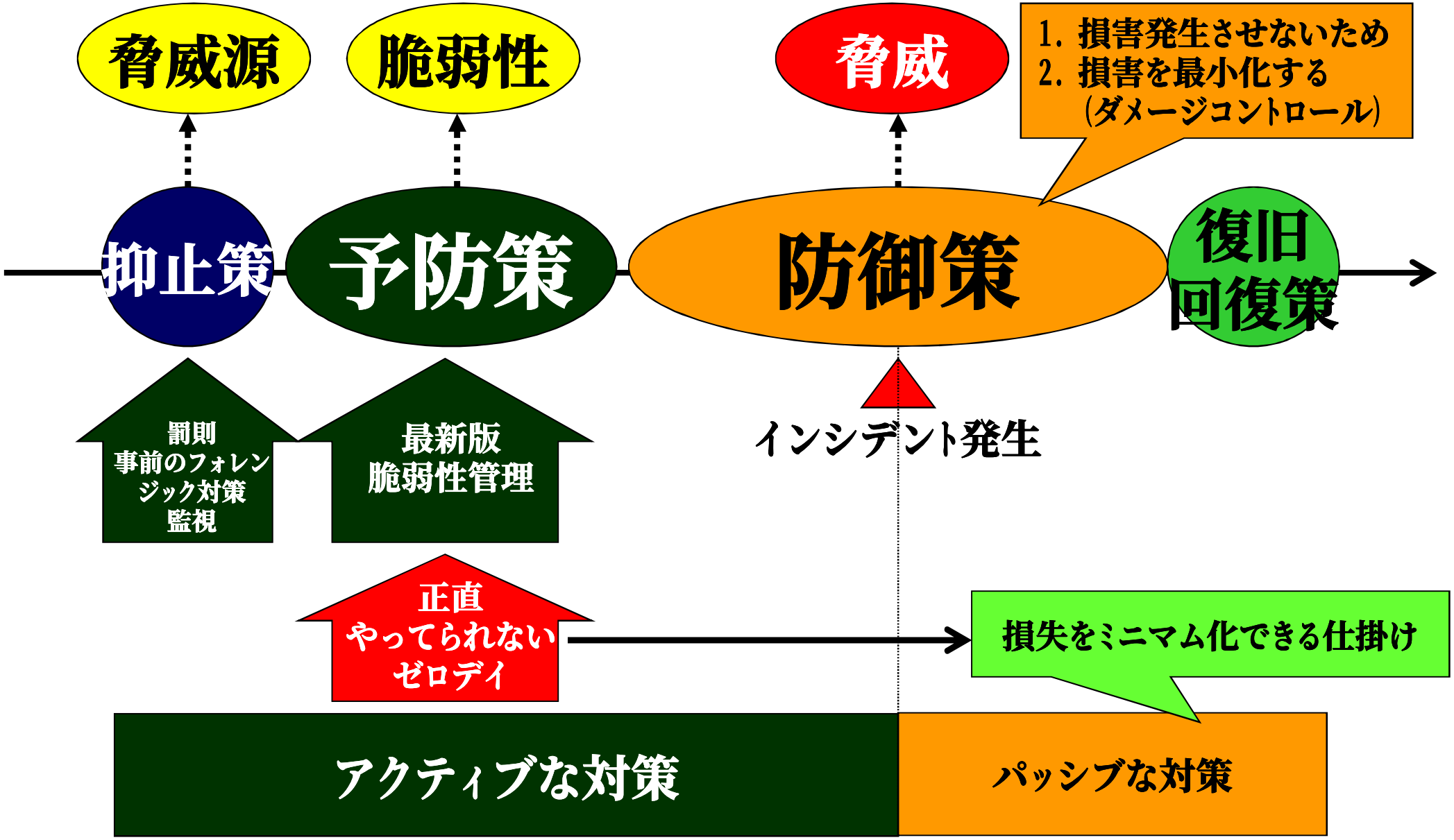
**⇒ こりゃ最悪だ！**

**そりゃそうだ！セキュリティって事業の信頼基盤**

# セキュリティとは？



# セキュリティとは？



# セキュリティとは？

## 1．組織で実施するセキュリティ（トップダウン）

### ① 経営意思やコンプライアンス

宣言する経営意思。
要求されるセキュリティ。例えば、プライバシーマークなど。
種々の基準・規程・ルールなどによる

### ② システム基盤でのセキュリティ

所謂、システム屋の仕事。

システムにより異なるが、より人間をサポートするシステムでは実装は難しくなる。

お金のかかる
セキュリティ

## 2．人で実施するセキュリティ（ボトムアップ）

モラルの高さ。気づき。カイゼン。

**⇒ プロ意識、職場の5S**

お金のかからない
セキュリティ

# 脅威のとらえ方

そろそろ、本音でやりませんか？

セキュリティは何処までやればいいのですか？

脅威のとらえ方

利用者に求めていくこと

# セキュリティ対策はどこまで？

セキュリティは何処までやればいいのですか？

良いリーダーとは？という命題に似ている。

決断力？企画力？統率力？実行力？包容力？・・・・

⇒ このアプローチは限りがない。

素晴らしい人を真似ても所詮、偽物。ものにならない。

⇒ スタイルの欠如！（自分のものになっていない）

そうではなく、最悪を考えてみよう！

最悪のリーダーとは？

優柔不断。手柄の横取り。責任回避。・・・

⇒ この最悪を避けるという具体的アクションから自己スタイルを！

⇒ 最悪の事態 の想定から。

# 脅威のとらえ方

枝葉末節にとらわれてはいけない。

どうなるのか？どうなっているのか？を理解すること。

最終的には経営判断。場合によっては 経営者の決断 が必要

にもかかわらず、

セキュリティ上の課題を、経営上の課題に繋げることの出来る人 が少なすぎる。

我々セキュリティ屋も、セキュリティ家 へ進化しなければならない。

# 脅威のとらえ方

1. 想定すべきとは言っても大変難しい。
   いずれにせよ、抑止、予防、防御のバランス。
   まずやるべきは。発生の**想定**と対応シナリオの**想像**。**決断**者 の確認。

2. 灯台下暗しと想定外
   「改ざんで業務停止」のように、コア事業と無関係と思われるサービスなどでの業務停止。⇒ 知らない間に、温泉旅館の増築

3. 妨害をどの程度許容し、前提とするか
   手を出してはならないこと に対する考慮（法制？）
   資本主義社会での インサイダー、実社会での テロ行為 など


4. リアルとサイバー、ハイテクとローテク
   デマ、風評。知能的手口と力わざ。（全うな事業も似たところもある）
   ブログ、ツイッターのようなソーシャルコミュニケーション社会の特性。
   伝播性、即時性、テキスト、写真、ボイス、動画、ライブ。

# 利用者に求めていくこと

1. セキュリティ対策を過信しない
   プロ意識。職業倫理。
   私たちの仕事の道具は何だ。どういう社会的責任を負っているのか。

2. 不審なメールの見分け方
   簡単なメールの原理、ヘッダの見方。
   クリティカルなお仕事で、オープンなメールを使用するなら 当然 のこと。

3. 信頼をおけないサイトへのアクセス方法とその後
   どんな準備をしてアクセスすべきか。アクセス後にどうすべきか。
   サイトだけではなく、ドキュメントも。（どう開けるか？開けてどうするか？）

4. IT環境は、お仕事の重要な道具で日本を支えるインフラ。
   自分や社会が依存しているものへの理解。
   この志の高さが、我々を救う。

# さいごに

## 日本に効く、一句

坂の上
雲の遥かに
映る峰
大地ささえる
セキュリティかな

21世紀の、坂の上の一筋の雲

つかむには、やはり、「雲」

日本が誇れるのは、アジアに受け入れられる、情報セキュリティを特徴とした、展開ではないだろうか？

セキュリティをコストなんぞと言わず、競争力の源泉であり、推進スタイルとして確立したい。

ありがとうございました。

# *Any question ?*



株式会社ラック
http://www.lac.co.jp/
sales@lac.co.jp