クラウドセキュリティによる危機管理と企業経営リスク

ISMSセミナー

2020年2月17日

森井昌克

morii@eedept.kobe-u.ac.jp

（**神戸大学大学院　工学研究科**）

中小企業の本当の実態は？

中小企業の４割がサイバー攻撃を受けている（NHKニュース2019年11月27日）！？

ただ、私が解釈するに（決して煽っているわけではなく）

決してセキュリティ業界の「回し者」ではないので！

悲惨な状況、ざっくりいって２割から３割の中小企業は被害を受けている、それに気づかないだけ

他社へ被害拡大も、早急な対策を

標的型攻撃など拡大、支援利用も

警視庁サイバーセキュリティ対策本部

中小企業のサイバー対策

- OSは最新に、Windows 7は早急にアップデート
- ウイルス対策ソフトを導入
- パスワードは複雑に、使い回さない
- 最新のセキュリティ情報を組織で共有
- データのバックアップを

簡単ではない！？

悲惨な状況の原因？

結論になるかもしれないが

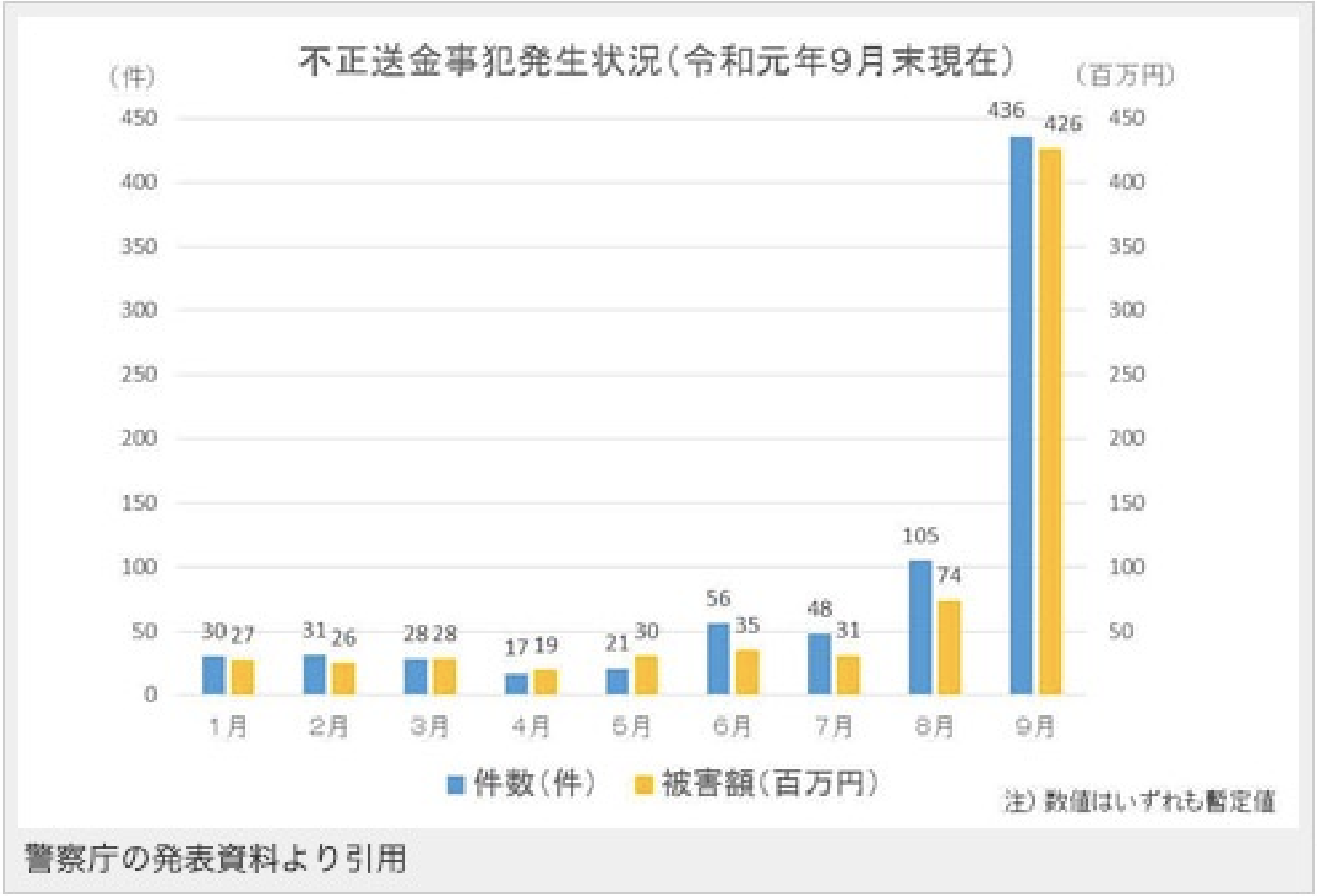
経営層もだが、それ以上に社員のセキュリティ意識が低すぎる！

現実（地縁）社会の意識（モラル、倫理感）は世界的にも極めて高かったのに

中小企業の被害（例）

- 「情報漏えい」だけではない？
  - 「情報漏えい」の深刻さも理解していない？
    - 漏えいして困る情報などない？？？本当か？
- ビジネスメール詐欺（BEC)
  - 実際に数百万円から数千万円の被害が
  - その手口は？
- ネットバンクの不正送金
  - 不正送金被害が急増（2019年11月、金融庁）

ネット銀行で不正送金事案が急増。金融庁が注意喚起



ダークネットで売られるあなたの会社の情報、そして被害も

Dr.森井のサイバーセキュリティ講座

第3回 ダークウェッブで売られる会社の秘密!?

神戸大学大学院 教授
情報セキュリティ大学院大学客員教授
森井 昌克さん

大阪生まれの工学博士。
マルチメディア情報通信工学、ネットワークセキュリティ、情報理論、暗号理論等の研究、教育に従事。インターネットの文化的社会的側面、それを基盤としたネット社会等の研究、啓蒙、社会活動にも従事。

創意とくふう、2018年3月号より引用

◆あなたの会社も被害に!?

サイバーセキュリティ対策を行っているJALですら騙されるのです。あなたの会社の詳細な取引情報がダークウェッブで売られているかもしれません。それを利用してJALのような巧妙な振り込め詐欺に遭うかもしれないのです。

会社の取引情報も含めて、ありとあらゆる情報の管理を厳しくすることはますます重要になってきていますが、それでもダークウェッブに流出し悪用される可能性があります。振り込め詐欺に注意するのは高齢者だけでなく、会社も注意しなければならないのです。

今日の要点

- どの中小企業でも起こり得る身近な犯罪の話
- 今日は、企業がサイバー被害に遭わないための[illegible]の話。
  - [illegible]
    - [illegible]
    - 「お[illegible]の備え」を！
      - [illegible]しかし何が起こるかを十分な覚悟を！
- そして、あなたが受ける被害の話。
  - 想定外の被害をあなたは受ける！？

被害を想定する！
それがリスクマネジメント

いや、遭っても被害ゼロにすれば良い

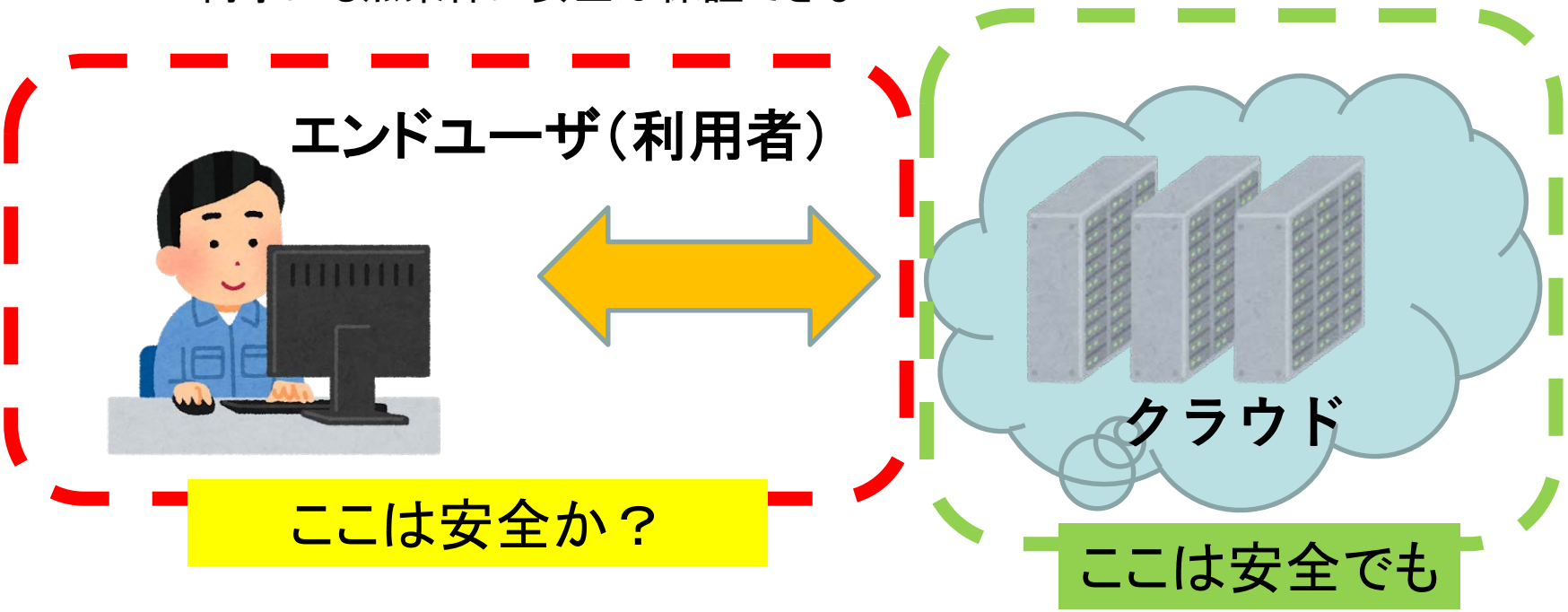
今日の要点(2)

まずサイバー社会のリスク

- 何ができるかを考える
  - 差し迫るリスクを評価する
- 自社の警備体制を考えればよい
  - 現実社会とサイバー社会
    - それぞれを対応させれば理解は容易
      - ドアの鍵はかけているか
      - 社員の入退出管理は？
      - 金庫は？
      - 詐欺に遭わないように？
      - 信用/信頼を得るために

今日の要点(3)

- クラウドセキュリティ
  - クライド自体は安全だが、それを利用することは必ずしも安全ではない！？
    - 何事にも無条件に安全は保証できない！



マルウェアでさえ

- マルウェア
  - 昔はコンピュータウイルスと言われた？
  - 不正なプログラム全般
  - プログラムなので「実行」しなければならない
    - メールを読んだだけでは感染しない？
  - マルウェアは総合不正アクセスツール！
    - 遠隔操作どころか自動で不正をはたらく
      - 悪意のある人工知能みたいなもの
  - マルウェアは小学生でも作れる？

マルウェア

- 昔は、コンピュータウイルスと言われたが…
  - 現在では誤解を防ぐためにマルウェアと呼ぶ。
    - マル-ソフトウェア＝（悪意のある）ソフトウェア
- ちなみに、スマホのマルウェアはマルアプリと呼ぶべき
  - スマホに悪意のあるソフトウェアを仕掛けるためには、悪意のあるアプリを仕掛けるしかない！
    - 不正なアプリを如何に防ぐか？

マルウェアはアンチウイルスソフトで防げるのか？

- 結論から言って、防げない！
  - 流れているウイルスの99%は防げる！
  - 防げないマルウェアも数多く存在
- 対策は？
  - 脆弱性を無くす！
    - システムの脆弱性、ユーザの脆弱性
  - 被害を無くす？！
    - 早期発見、早期対策

マルウェア感染

- マルウェアの初動で感染を検知することは極めて難しい
  - ひそかに活動する能力に富んでいる
    - 通常の業務（動作）と見分けることが難しい
  - 絶対に不可能というわけではないが…
    - 事実上（コストもあって）難しい
- ただし、データを外部に送る、遠隔操作される等の行動は検知できる！(ハズ)

マルウェアはアンチウイルスソフトで防げるのか？

- 結論から言って、防げない！
  - 流れているウイルスの99%は防げる！
  - 防げないマルウェアも数多く存在
- 対策は？
  - 脆弱性を無くす！
    - システムの脆弱性、ユーザの脆弱性
  - 被害を無くす？！
    - 早期発見、早期対策

2020年IPA情報セキュリティ10大脅威

昨年順位	個人	順位	組織	昨年順位
NEW	スマホ決済の不正利用	1位	標的型攻撃による機密情報の窃取	1位
2位	フィッシングによる個人情報の詐取	2位	内部不正による情報漏えい	5位
1位	クレジットカード情報の不正利用	3位	ビジネスメール詐欺による金銭被害	2位
7位	インターネットバンキングの不正利用	4位	サプライチェーンの弱点を悪用した攻撃	4位
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	5位	ランサムウェアによる被害	3位
3位	不正アプリによるスマートフォン利用者への被害	6位	予期せぬIT基盤の障害に伴う業務停止	16位
5位	ネット上の誹謗・中傷・デマ	7位	不注意による情報漏えい（規則は遵守）	10位
8位	インターネット上のサービスへの不正ログイン	8位	インターネット上のサービスからの個人情報の窃取	7位
6位	偽警告によるインターネット詐欺	9位	IoT機器の不正利用	8位
12位	インターネット上のサービスからの個人情報の窃取	10位	サービス妨害攻撃によるサービスの停止	6位

2020年IPA情報セキュリティ10大脅威

内部不正は深刻

ランサムウェアは怖くない！？

標的型攻撃が5年以上も1位

弱点を狙うのがサイバー攻撃の鉄則

順位	組織	昨年順位
1位	標的型攻撃による機密情報の窃取	1位
2位	内部不正による情報漏えい	5位
3位	ビジネスメール詐欺による金銭被害	2位
4位	サプライチェーンの弱点を悪用した攻撃	4位
5位	ランサムウェアによる被害	3位
6位	予期せぬIT基盤の障害に伴う業務停止	16位
7位	不注意による情報漏えい（規則は遵守）	10位
8位	インターネット上のサービスからの個人情報の窃取	7位
9位	IoT機器の不正利用	8位
10位	サービス妨害攻撃によるサービスの停止	6位

標的型メールは標的を選ばない！

- 「標的型メール攻撃」という言葉が悪い？
  - 自分のところは狙われていない！
    - 大いなる錯覚
    - 自分の（情報の）価値を正しく認識していない
    - 踏み台（攻撃の前線基地）になる！
      - 最悪の事態→裁判の矢面に！
- 標的型メール攻撃ではなくAPT
  - 執拗でずる賢い攻撃
    - 年単位の攻撃
      - 2013年3月の韓国全土におけるサイバー攻撃では3年前から準備

標的って云うから？

先日、ある会議で

- ある業界での各社情報システム部局長会議
  - ある会社の部局長が　ちょっと自慢げに
  - 「当社では標的型攻撃の演習を年に数回定期的に行っている！　確実に標的型メールに耐性ができている（引っかかる人は少なくなっている！）」
  - これ、大きな間違い（勘違い）が2つあります。
    - わかりますか？

標的型メール攻撃は防げないのか？

- 標的型メール攻撃は防げない！？
  - 不審なメールなどありえない？
    - 詐欺師（攻撃側）は巧妙な手段を使う
- 標的型メール攻撃の演習は無意味？
  - 「前回１０人が引っ掛かったのが今回2人になった」というのは無意味
  - 一人でも引っ掛かれば感染は広まる！
  - では、それでもなぜ行うのか？
    - セキュリティ意識を高めるため

標的型メール攻撃は防げないのか？

- もはや「おまじないのレベル」
  - 怪しい添付ファイルは開かない！
  - ウイルス対策ソフトを有効に！
  - ファイヤーウォールやUTMを導入！
    - もちろん、UTMは有効であるが…　しかし
      - UTMも「お札」ではない！？

標的型メール攻撃は防げないのか？

- （よく言われるが）標的にならないのでは！？
  - 情報の価値を評価できない
  - その価値が最大の時に漏えいすれば…
  - バックドアを仕掛けられる
  - 他社を攻撃する踏み台に
    - 訴えられる可能性

本当に標的型攻撃を受けているのか？

- 確実に言えるのは攻撃を受け、それが成功しているサイトの70%～80%は気付いていない！
  - しかも楽観的考えても、数%、悲観的に考えれば10%前後のサイトは攻撃受け、事実上の被害を受けている

標的型メール対策の勘違い

- 標的型メール攻撃演習の本来の意味
  - 引っかからないようにすることではなく(それも重要ですが)、その後の処理が大事！
    - どのように連絡し、事後にどのように処理するか。
    - 被害を最小に抑えるための対策

リスクを最小化するハザードトレラントシステム

誰が何のために攻撃(改ざん)するのか？

- 攻撃者は情報を狙うが、その価値を決めるのは、その攻撃者とは限らない？
  - 情報が攻撃者を選ぶ
  - 情報の有為転変性
    - 情報自身が成長し、それ自体が動いていく
    - 価値が増幅する
- 真の攻撃者は情報の価値が最大となるときを待つか、情報の価値を増幅させる

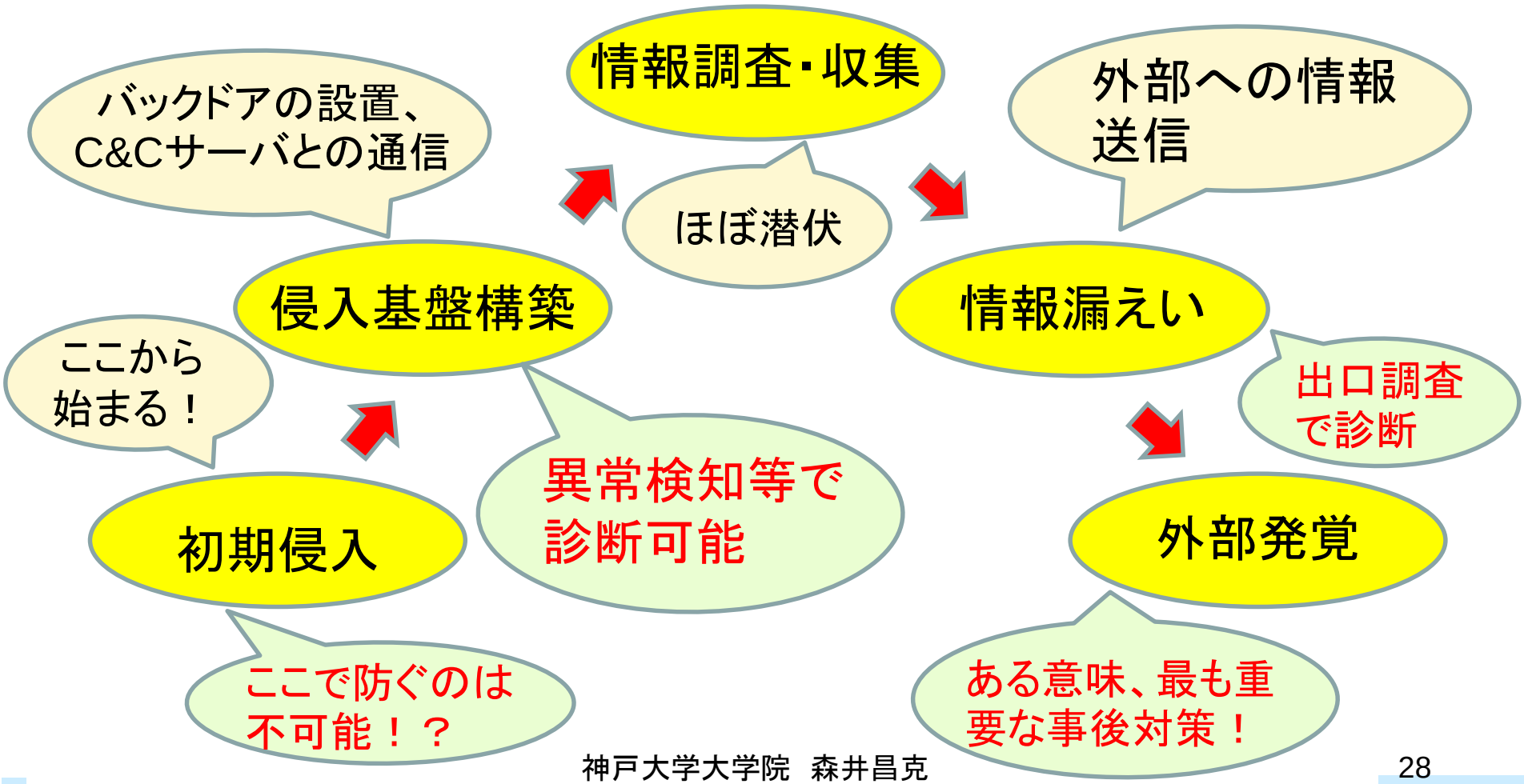
誰が何のために攻撃(改ざん)するのか？

- 攻撃の成功が表面化するのは稀？
  - 攻撃自体の痕跡を消すのは鉄則！
  - 中小企業の90%は攻撃対象であり(攻撃に日々さらされていて)、その中の10%は攻撃が成功していると予想される(楽観的に考えても)
    - 気付いていない！

標的型メール攻撃対策まとめ

- 標的型メール攻撃の実際
  - 初期侵入
  - 侵入基盤構築
  - 内部調査・情報収集
  - 情報発信（漏えい）
  - 犯行目的完遂（外部発覚）
- どこで止めるか！？
  - 最終的には被害がなければ良い？
    - 被害を最小に抑える！

標的型メール攻撃対策まとめ（2）



脆弱性

- 脆弱性とバグは違う
  - なぜ脆弱性は無くならないか？
  - バグは仕様書と異なる動作をすること。
    - これは事前のテストで潰す事ができる
  - 脆弱性は予期しない動作
    - これは予期出来ないのだから潰せない！
  - 脆弱性への対策
    - 迅速な危機管理が基本

なぜ攻撃が容易か？

- 空き巣と同じで「戸締まり」の悪いサイトが存在する
  - 空き巣は一日の行動範囲はわずか数Kmから数十Km
  - ネットでは世界中を簡単に俯瞰できる！
- 空き巣と同じで「様々な道具」を使いこなせる
  - 空き巣が使える道具は高々持ち運べるものぐらいで使いこなすにはかなりの熟練を要する
  - ネットでは最新の機材が、誰でも使いこなせるように準備されている。

最重要なことは！

- 問題は、セキュリティ対策をしないことではない！
  - セキュリティ対策は誰でもできる！
    - 「する、しない」の問題ではなく、程度？の問題。
- 最も大きな問題は、自身（自社）のセキュリティが評価できないこと！
  - 換言すれば、どれだけ危険な状況か理解していないこと
  - （楽観的に考えて）90%の企業・組織が深刻な攻撃を受け、その中で10%は攻撃が成功している
    - 深刻な被害に遭っていることに気づかない！！

セキュリティは総合技術

- セキュリティは簡単ではない！
  - この意味するところは？
    - 素人判断するな！
  - 攻撃するものは誰か？
    - すべてを想定することの困難さ
  - 守るべきものは何か？
    - 意外と出来ていない自己分析

言うは易し、行うは難し

敵を知り、己を知れば
百戦危うからず

まず言っておきたいこと

- ウェブ（ホームページ）が書き換えられても大したことない！　ネットサービスしてないし。
  - マルウェア（コンピュータウイルス）を仕掛けられて、攻撃元になる
    - 警察の捜査を受け、パソコンを押収される上に、被害者に訴えられる。
  - **風評被害**を受ける！
    - ネットでの風評被害は深刻

気付かない！？　気付いた時には被害甚大

最重要なことは！

- 不正確な情報に踊らされるな！
  - 真実から遠い、あるいはデマに近い情報にあふれている、不正アクセス周辺
    - 恐れることはない、必要十分な対策を取ればよい
      - 過剰な反応、対策は愚かである
    - **金がなければ頭を使え、頭がなければ時間を使え！？**
      - セキュリティ対策技術（利用法）はそれほど難しくはない
      - オープンソースも
  - マルウェアの真実？

サイバーテロ対策

- 他人事じゃないサイバーテロ
  - 社会の一員であることを自覚
- サイバー攻撃への対処（一般編）
  - 一人の被害が組織の被害に、そして社会の被害に
  - 一人一人のセキュリティ意識が重要
    - 小さい穴から大きな穴に
    - いきなり「**爆弾**」が落とされる事はまずない！
      - インテリジェンス（コツコツと情報を集めて、**最後に爆発**させる）

早期発見・早期対策

- 予防はもちろんのこと、サイバー攻撃に対する早期発見、そして適切な早期対策が必要！

とはいえ、一番大事なのは、サイバー攻撃を受けたことを前提に、さらに進んでその攻撃が成功したとして、対策を考える。

高度化したサイ

能を有する技術者集団でなければ対応出来ない

被害を最小に抑えるセキュリティ対策を！

特に、一定基準のセキュリティは特化しない。組織に

見合った最適なセキュリティを施す必要がある。

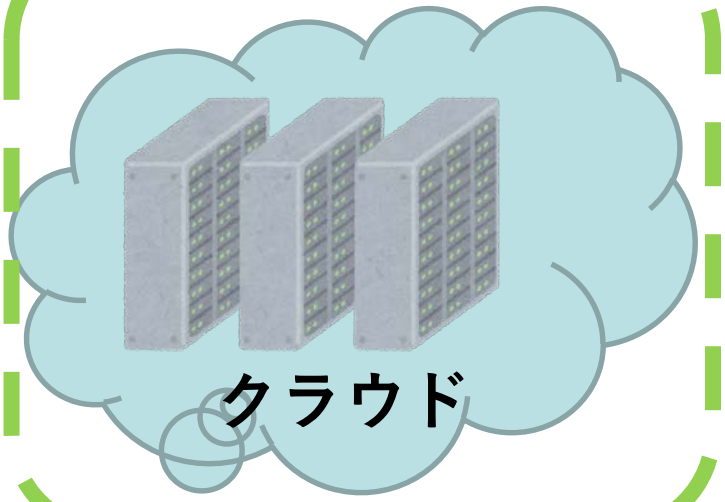
危機管理を！

改めて、セキュリティの本質

- フラットな世界（高い塀で守られた世界ではない）
  - 今までは「守られた」世界
    - いくつもの障壁…　それは財力であったり、技術であったり、はたまた地形であったり、言葉であったり…
  - 攻撃側の障壁はない
    - 普通の小学生が攻撃可能
      - 実際、1歳半の幼児が…
  - 対策の大前提
    - 「知る」こと。
    - そして戦場である事を認識する事！
    - 戦場では武装すること！　あるいは裸（戦う事を止める）であること！？

クラウドセキュリティ

エンドユーザ（利用者）



クラウド

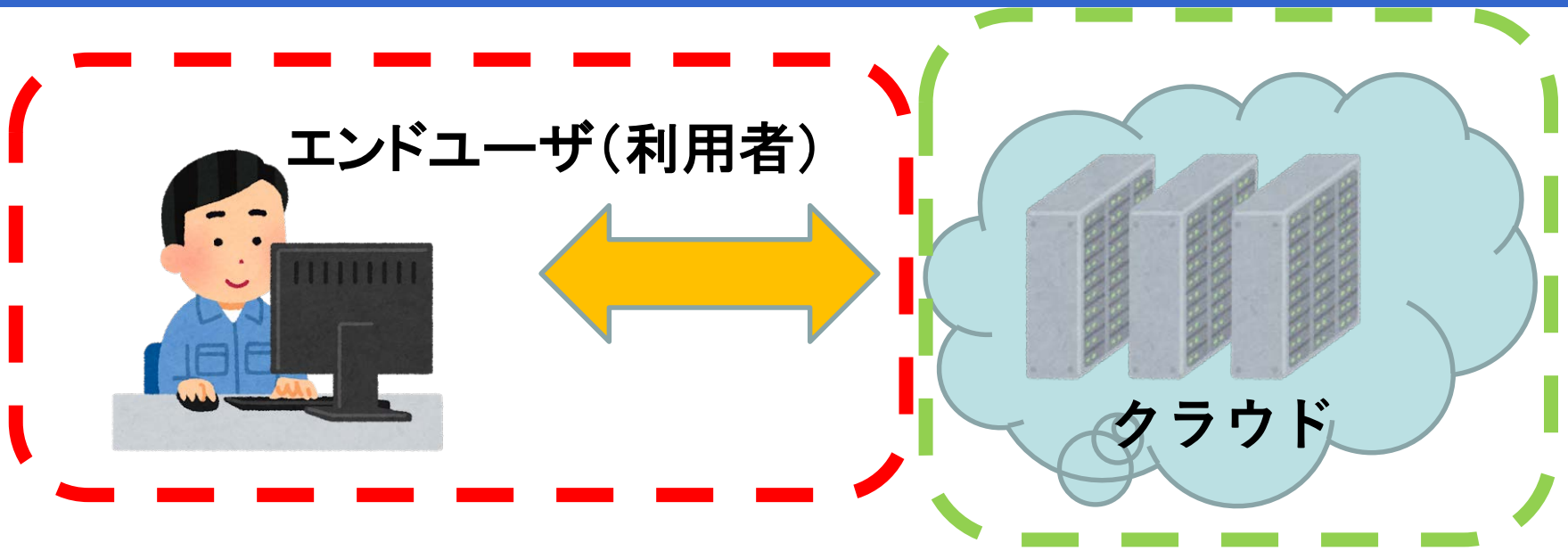
ここは安全か？

- アクセス制御
- T通信路およびデータ暗号化
- セキュアなアプリ/OS
- バックアップ
- クラウド事業者

ここは安全でも

- クラウド自体の信頼性は？

クラウドセキュリティ



- クラウドを利用する上でのリスクと責任
- 新たな情報漏えいリスクとは？
- そもそも、なぜクラウドか？

パラダイムシフト

所有から利用へ

企業トップの責任

- 信用第一の世界に！
  - サイバーフィジカル社会において、信用（情報共有）は何事においても優先される！
    - 社会的信用を失うと、取り返しがつかない。
- 大きな事故を起こさない
  - 大きさの制御はリスクマネジメントの問題

フィジカル社会のセキュリティ

- フィジカル社会（今までの社会）
  - 安心と安全を求めて
    - 誰が誰を、何に何で
  - **企業において安全はすべてにおいて優先する！**
  - **安全とは？**
    - **フィジカル社会では何となくイメージできる？**
      - だからこそ、対策ができる
        - » 防犯設備
        - » コンプライアンス
        - » 警備会社

企業の目的とは？

- **3つの視点（立場）から**
  - **第一層**
    - 会社の利益、利潤
    - 会社の拡大、拡張
    - 経営者自身の生活のため？
    - 株主のため
  - **第二層**
    - 顧客のため
    - 従業員のため
  - **第三層**
    - 人間の幸福のため
    - 地域社会のため
    - 社会の中での役割を担う事業継続のため

企業を継続させるための安全

- 顧客の安全
  - 製品
- 従業員の安全
  - 労働環境
- 企業自体の安全
  - コンプライアンス

3つの安全があってこそ健全に継続できる企業体に

安全なくして生産なし（本田宗一郎）

企業トップの責任

- 信用第一の世界に！
  - サイバーフィジカル社会において、信用（情報共有）は何事においても優先される！
    - 社会的信用を失うと、取り返しがつかない。
- 大きな事故を起こさない
  - 大きさの制御はリスクマネジメントの問題

企業の競争力は安全にあり！

- 「安全」と「安心」を信頼で紡ぐ
  - ヒトや社会は安全ではなく、安心を求めている。
    - 真に安心を与えるためには、「安全」と「信頼」が必要
- リスクマネジメントとは「安全」を直接的に制御するのではなく、「安心」を信頼で紡いで制御する
  - 「安心」と「信頼」が要

リスクマネジメントの実践とは

- リスクはなくならない。
  - そのリスクは押さえることができる、つまり事故を最小にできる
- 安全は価値である！
  - 安全に係る人、組織、機関を評価せよ！
  - 安全は利益を生む
    - 価値は利益を生む
  - 安全は公開しろ！
    - リスクの共有と公開

ポスト・サイバーセキュリティ

- （サイバー社会）∪（物質社会）から（サイバー社会）∩（物質社会）へ

サイバーセキュリティ

Security？　　Safety？

サイバーフィジカルセキュティ

安全安心なSociety5.0へ　→　情報通信（およびAI,IoT, Robot）を軸足にして

第一段階は「機械」対象、SIP2ではサプライチェーン、しかし

最終段階で**「人、社会、組織を意識」**

→Vision Zero
→Safety2.0

ポスト・サイバーセキュリティ

サイバーフィジカルセキュティ

人、そして企業の安全の視点

安全における情報共有の必要性、
そしてその阻害、改ざんに対する
リスクマネジメント

人間と機械とのコミュニケーションの保護←サイバーセキュリティ

サイバーフィジカルセキュリティへ←協調安全の思想を

セキュリティ意識
（サイバー社会）

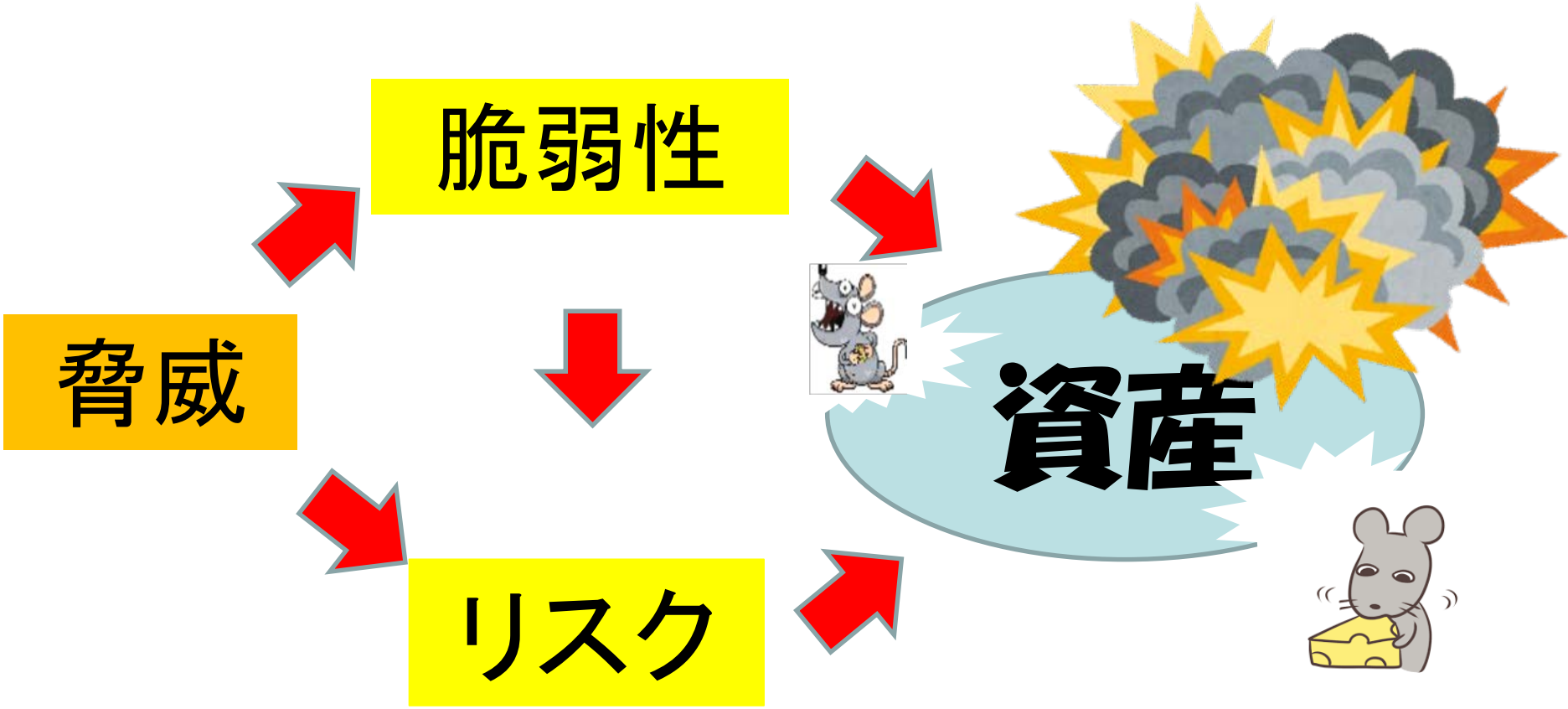
ゼロ災運動

安全意識
（フィジカル社会）

セキュリティは投資である！

- 投資は利益を生み出さなければならない！
  - 利益にとって最大の障害は損失、それも予期せぬ損失である！
    - 損失は予期できなくとも評価できる？
    - 保険会社は「万が一の損失」を評価して、利益を出している！
    - 計算できることが評価である

常にリスクにさらされる資産



サイバーセキュリティ

- サイバーセキュリティはサイバー攻撃ではない！　経営者にとってリスクの話である！
- 経営リスクとは何か？
  - 経営全般での事業体制の不備だけでなく、外的要因による直接、間接的影響からの経営損失の危険性つまり、事業破たんに陥る要因すべて
- リスクマネジメント
  - 未来に確実にあるものは不確実だけだ！

サイバーセキュリティ

- リスクマネジメント
  - 経営において、100万円の利益を出すことと100万円の損失を未然に防ぐことは同じ
  - リスク管理体制
    - リスクの抽出・特定
    - リスクの評価・対策
    - リスク教育
    - リスクの管理・連絡体制

年間予想損失額を査定してみる！

- 製造業を仮定：前提とするセキュリティレベルはウイルス対策ソフト
  業
- （予想損失額）：
  - 直接損失額：製造が止まる損失、パソコン、ネットワーク復旧検査費用
  - 間接損失額：出荷できない違約金、信用度（一部半年間の取引停止）
- 年間発生頻度
  - リスク値から資産

年間予想損失額を査定してみる！（2）

,000万円
基づいて査定
対策対応企業
- 資産5、脅威5、脆弱性5
- 仮定する製造業：

8
こらない≒万が一に

リスク（損害額）を評価する

予想ではなく、年間損害額が想定できる、それがリスクマネージメント

年間予想損失額

- リスク値：万が一にも起こらない≒万が一に起こると仮定
  - 仮定する製造業：資産5、脅威7、脆弱性8
  - （リスク値）＝2^5x2^7x2^8x(1/10,000)x(1/330)
  - ＝1/3

年間予想損失額
＝（年間発生頻度）x（予想損失額）
＝1/3x5,000万円≒1,500万円

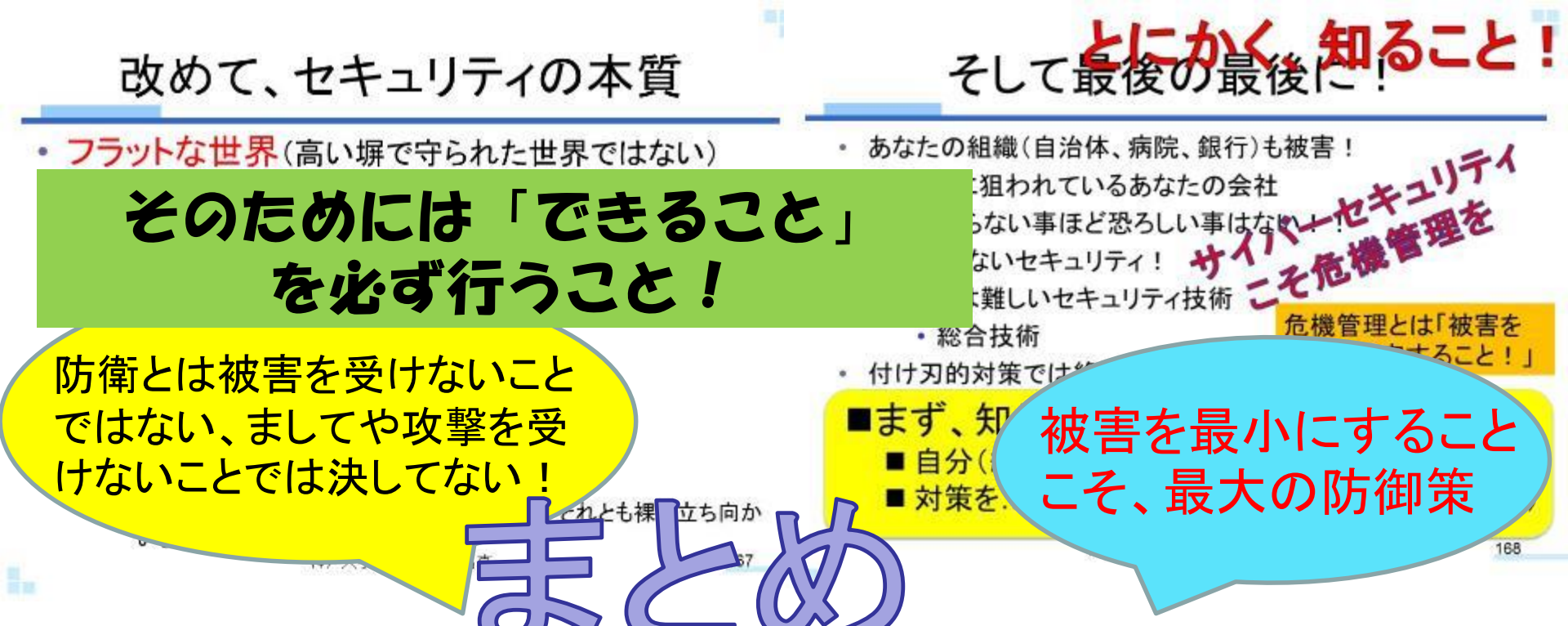
年間予想損失額を査定してみる！（4）

年間予想損失額
＝（年間発生頻度）x（予想損失額）
＝1/3x5,000万円≒1,500万円

【結論】 その1/5（300万円）以下しか年間セキュリティ対策費（あるいは相当の知恵、工夫）を費やさない企業は問題外！

1,000万円前後の年間セキュリティ対策費（あるいは相当の知恵、工夫）が必要！ しないと＊＊する可能性が高い！

あながち無茶な査定、評価ではない！



セキュリティ対策は、利益を生むための、言い換えれば利益を保証し、守るための最善の方策です。まったくセキュリティ対策を考えないことは泥船に乗っているのと同じです。しかもセキュリティ対策は得てして「はだかの王様」になりがちです。第三者の目で、しっかりと査定しましょう、あなたの会社のセキュリティの実態を！