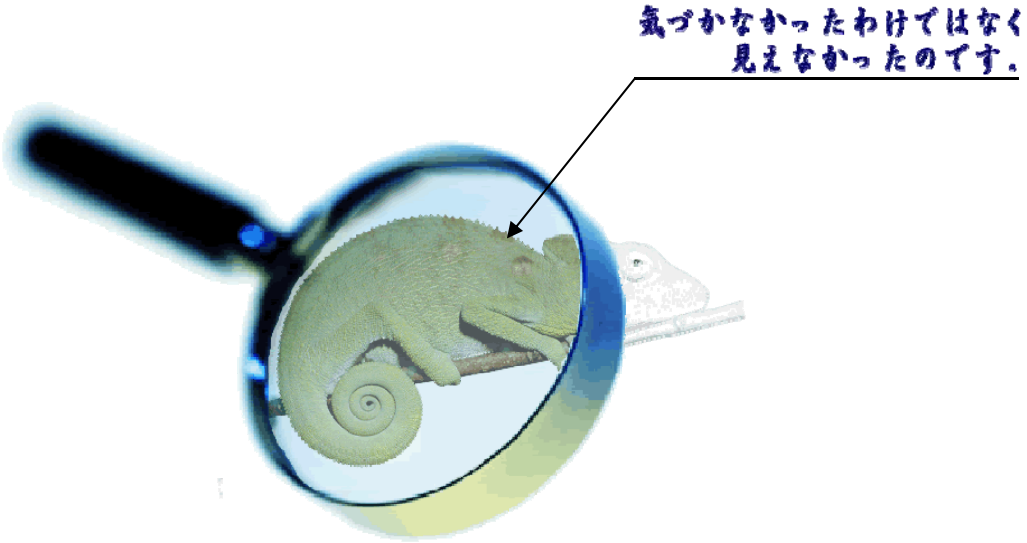
特定非営利活動法人
日本ネットワークセキュリティ協会
Japan Network Security Association

組織で働く人間による不正・事故は止められるのか？ ～「内部不正対策14の論点」発売記念セミナー～

内部不正に向き合うために

～組織のありようと対策の要諦～



CYBER GRID JAPAN

2015年9月9日 株式会社ラック
CTO 西本 逸郎

株式会社ラック

セキュリティで、お客様の成長に貢献し、
安心・安全な情報社会を実現します。

お客様とともに。 社会とともに。 安心とともに。

※ JSOC(下記参照)、サイバー救急センター、サイバー・グリッド・ジャパン、が特徴です。

商　号	株式会社ラック LAC：LAC Co., Ltd.
設　立	2007年10月1日　(旧ラック1986年9月)
資本金	10億円
代　表	代表取締役社長　髙梨　輝彦
売上高	連結 328億円 (2015年3月期)
決算期	3月末日
認定資格	経済産業省情報セキュリティ監査企業登録 情報セキュリティマネジメントシステム (ISO/IEC 27001)認証取得(JSOC) プライバシーマーク認定取得

- ✓ http://www.lac.co.jp/
- ✓ sales@lac.co.jp
- ✓ Twitter　@lac_security
- ✓ YouTube　laccotv
- ✓ Facebook　Little.eArth.Corp or 株式会社ラック

・本社
〒102-0093　東京都千代田区平河町 2-16-1
平河町森タワー
03-6757-0111(代表)
03-6757-0113 (営業窓口)

・韓国ソウル 子会社 CSLAC
Cyber Security LAC Co.,Ltd.

・名古屋オフィス
〒460-0002 愛知県名古屋市中区丸の内3-20-17 KDX桜通ビル16F

・福岡オフィス
〒812-0011　福岡市博多区博多駅前3-9-1
大賀博多駅前ビル5F

■ 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。24時間365日運営。高度な分析官とインシデント対応技術者を配置しています。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に、高品質なサービスを提供しています。

わたし

もと　いつ　ろう
本　逸　郎　CISSP

ブログ どらいつ 検索
@dry2

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

プログラマとして数多くの情報通信技術システムの開発や企画を担当。2000年より、情報通信技術の社会化を支えるため、サイバーセキュリティ分野にて新たな脅威への研究や対策に邁進。

わかりやすさをモットーに、サイバーセキュリティ対策の観点で、官庁や公益法人、企業、大学、各種イベントやセミナーなどでの講演や新聞・雑誌などへの寄稿、テレビやラジオなどでコメントなど多数実施。

株式会社ラック　取締役 CTO スマート・ビジネス・ファクトリ GM
　標的型攻撃対策本部長、サイバー救急センター 調査員
ネットエージェント株式会社 取締役 CTO
株式会社ブロードバンドタワー 社外取締役
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
一般社団法人 日本スマートフォンセキュリティ協会 理事、事務局長
一般財団法人 日本サイバー犯罪対策センター 理事
一般財団法人 草の根サイバーセキュリティ対策全国連絡会 顧問
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
セキュリティキャンプ実施協議会 事務局長
セキュアドローン協議会 理事

2009年度情報化月間 総務省　情報通信国際戦略局長表彰
2013年情報セキュリティ文化賞

内閣官房 情報セキュリティ政策会議 普及啓発・人材育成専門委員会 歴任
総務省 スマートフォン・クラウドセキュリティ研究会 歴任
経済産業省　サイバーセキュリティと経済 研究会 歴任
警察庁 総合セキュリティ対策会議 委員

産業技術大学院大学 運営諮問委員

国・企業・メディアが決して語らない
サイバー戦争の真実

著者 ： 西本逸郎・三好尊信
定価： 1,050 円(税込)
ページ数： 208
初版発行： 2012-02
ISBN： 978-4-8061-4293-5

2011年7月に、米国防省が「サイバー攻撃は戦争行為だ」との見解を表明し、サイバー空間は陸・海・空・宇宙に続く第5の戦場として規定されました。本書は、現在のサイバースペースを取り巻く環境を紹介し、世界各国や大企業の攻防から私達個人のセキュリティーまでをわかりやすく解説します。

日本経済新聞社「いますぐはじめる　サイバー護身術　なりすまし、不正アクセス…どう防ぐ？」(日経e新書)

【前提】

1. 西本個人の意見であり、私の所属するラック社や各種団体の意見などを代表したものではありません。
2. 個別事案の「機密に触れる」ことと「当事者が特定されること」がないよう趣旨を変えずに表現を変えている部分があります。
3. 特定の企業や組織の批判もしくは擁護する意図はありません。

サイバーセキュリティ専門家として、みなさまのセキュリティ対策の一助になることを目的としています。

1. 背景から

① 社会のIT化

② 取り残される一般の企業

個人はIT活用で、
生活スタイルを
変革！

仕掛ける
プラット
フォーマー

一般の企業は、活用
できてない。むしろ
邪魔な存在。セキュ
リティリスク。

社会が
IT化！

使えないの
は何故？

課題：合理化(機能)⇒社会のIT化(連携とデータ)
1)社会ITの従業員や取引先などとの関係
2)社会ITの活用
3)社会ITでビジネス、サービス提供

IT化
合理化目的

③ 日本でもようやく

デジタル社会に痕跡を残して活動していることを理解しなければならない。それがどう影響するのか？

特に海外では、
　犯罪組織が悪用しないか？
そもそも、
　その国の捜査機関は信用できるか？

2. 事件トピックス

① 発覚する内部不正 周辺機器の制御

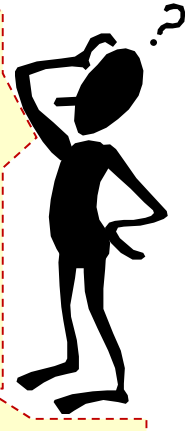
以前の周辺機器
→ 接続設定が大変！

USBの登場
→ プラグアンドプレイ！
→ パソコン側も便利に

プラグアンドプレイ
→ USBだけじゃない！
→ Bluetooth、Wifi、赤外線
→ ネットに繋がったあらゆる機器

現実的には、対応しているということと、実際に機能するというのも異なる。

新しいバージョンを入れておけば対応していたのか？利用企業側の何らかの設定が必要なのか？



全てのプラグアンドプレイデバイス(要はコンピュータ)を制御できるのか？大元から絶つ必要もあるが、そもそも可能なのか？

② 発覚する内部不正 大規模流出事件

1)不備があったので事故が発生
 (1)対策を行っているが故の事件発覚
  → 対策してない会社は暴くことすらできない。(事件化しない)
  → 対策実施の反面リスクとして覚悟。(全うな会社)
 (2)個人情報保護法から10年。
  → 運用の形骸化、対策へのフィードバック
 (3)対策への過信
  → セキュリティ対策を行ったが故の安心が裏目に出る。
   防御策の過信は組織を弱体化する。
2)システム運用とデータ運用への理解
 (1)システム運用の実態が変化している。
  → 多くがデータ検索や分析が運用の実態に。リスク増大。
3)発覚のきっかけとなった名簿流通と利用企業
 (1)情報取得と利用手順の形骸化 → 名簿市場の隆盛
  → 名簿屋と利用企業の再発防止推進。(巧妙に)

③ 発覚する内部不正　多くの内部不正

1）不正者の現状

大体末端の技術者が多い。再委託先や派遣など、
勿論、社内の技術者の例も、
いずれにせよ、リスペクトが無い。

→社会を支えている末端の技術者と抱える会社の生存方法！
　便利に、頼りになる存在。あらゆる権限が集中！

→リスペクトがないままに、時代が変わった。
　システムが合理化目的の単なる機能の提供から、
　データが売れる時代！規制により価値上昇のジレンマ。

→システム運用とデータ運用の混在。（データ運用への考慮が無い）

2）個人情報価値の変化

正規市場の存在。クレカなどとは異なる。
事件や法制度の充実が、価値を高騰させる。

④ 敵も味方もすなる(スパイ)

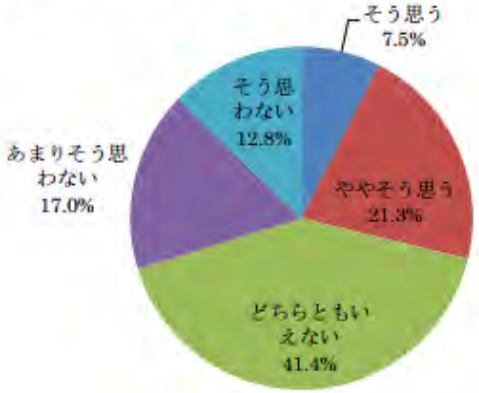
諜報活動は、どこでもやっていること。

特にデジタル社会においては、益々データが集中し、従来手法に加え圧倒的に仕掛ける側に有利な状況である。

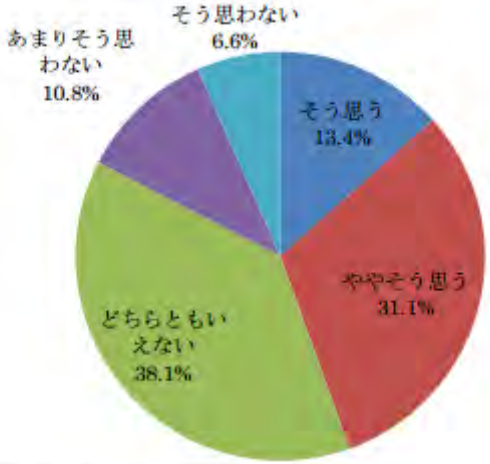
守りきることは困難と心得、ある面、諜報を受けていることを前提とした運用が重要。⇒ 諜報前提社会！

⑤ DBSCの調査結果

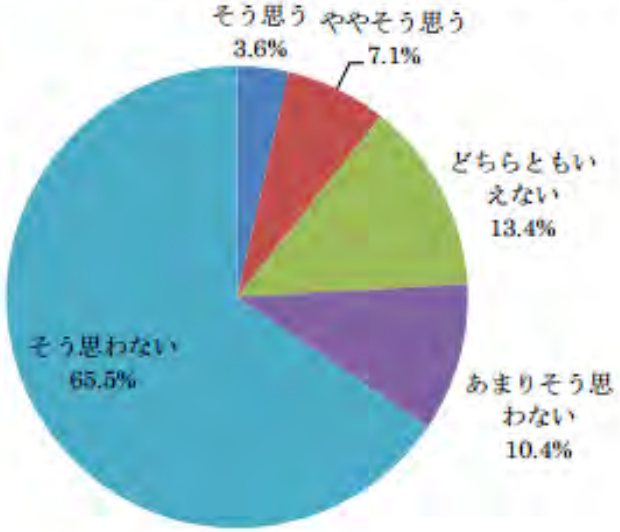
Q: あなたの給与は適切にあなた自身の業績評価を反映している。(図 1-6)



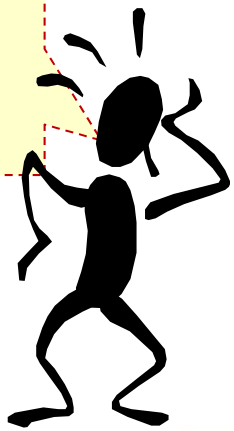
Q: この会社が気に入っている。(図 1-7)



Q: 将来、データベースに格納されている情報をこっそり売却するかも知れない。(図 1-9)



10%程度は潜在的な動機はありそうである。



⑥ 隠ぺいできない社会

デジタル社会！よく言われること

→ 簡単に改ざんでき、コピーも消去も簡単！信頼できない。

ところが、

→ ログイン、システム、メール、閲覧、ソーシャルメディア、アプリ、接続、入退室など、あらゆる局面であらゆる活動が記録される。

詳しく調べると不正は必ず暴かれる。

→ フロッピーディスク改ざん事件、不正会計など

デジタル化がもたらす

⇒ 透明な社会！？


3. 我々が陥る罠
H&M
この先150m
Essential
もんじゃ
Debut!!
薬

① 陥る「単一障害点」の罠

複雑化する「繋がり」と「相互依存」。「機能」連携と「データ」連携。

「思わぬこと」が起きるだけではなく、「思わぬこと」で事業が止まる。

1）利便性の追求

個人や中小企業で多い。スマホ、クラウド、丸投げ。

2）合理化の追求

いつでも昔に戻れるわけではない。

3）差異化の追求

依存性が高まり、選択肢がなくなる。

4）種々の管理施策

セキュリティ管理、資産管理、一括管理など。

しかも、
職責不分離
権限集中
監督・監視がない

単一障害点を無くす行為が、複雑化を呼び、さらに単一障害点を作り出すことも

② 陥る「正論」の罠

1）前述の、利便性・合理化・差異化などの「徹底」追及が、単一障害点を生み出していく。

2）わかっていることは「必要な無駄」をマネジメントすることであるが、

→ これが、なかなか出来ない。

→ 正論に打ち勝てない。

しかも、これはセキュリティに限った話ではない。

③ 陥る「日本式」の罠

1）丸投げ

部下、情報システム部門、協力会社 → 三兄弟

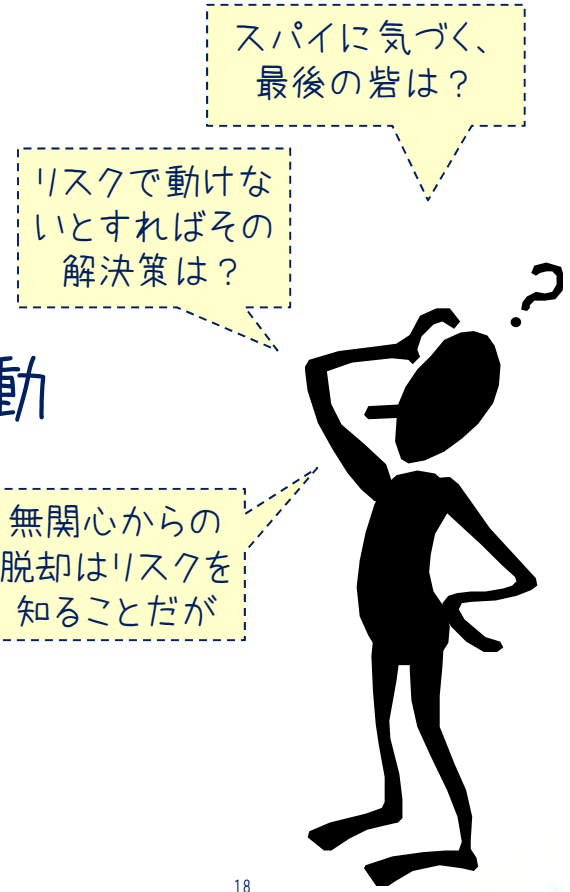
2）先送り

(1)リスクだけで動けない
→ しかも、許容もできない。

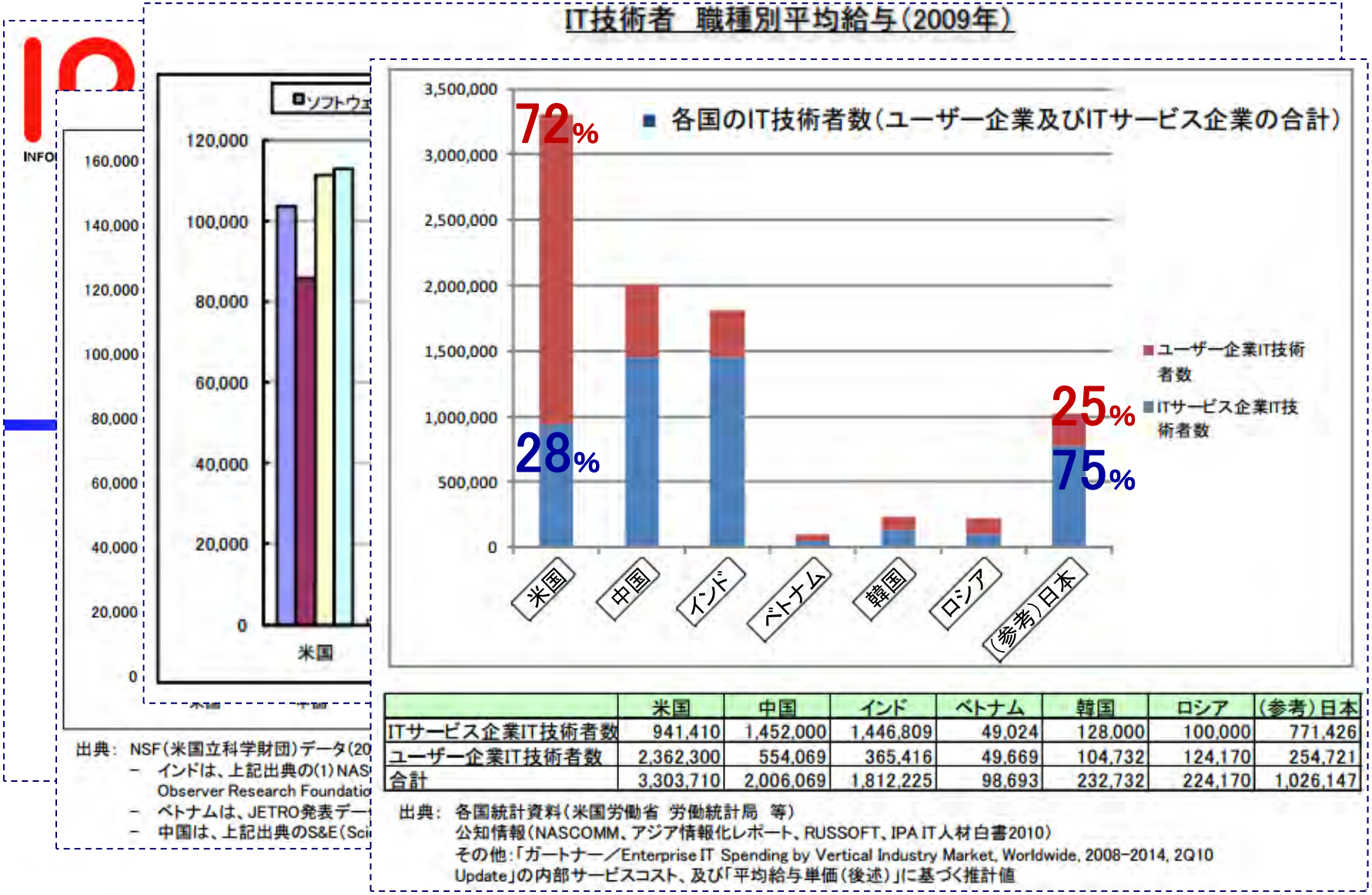
(2)組織的記憶喪失
→（良くも悪くも）定期人事異動
→ 施策は基本4年持たない

3）無関心

→ 誰かに守られている
→ なんとかなるという　勘違い



③ 陥る「特殊性」の罠



	米国	中国	インド	ベトナム	韓国	ロシア	（参考）日本
ITサービス企業IT技術者数	941,410	1,452,000	1,446,809	49,024	128,000	100,000	771,426
ユーザー企業IT技術者数	2,362,300	554,069	365,416	49,669	104,732	124,170	254,721
合計	3,303,710	2,006,069	1,812,225	98,693	232,732	224,170	1,026,147

出典：　各国統計資料（米国労働省 労働統計局 等）
公知情報（NASCOMM、アジア情報化レポート、RUSSOFT、IPA IT人材白書2010）
その他：「ガートナー／Enterprise IT Spending by Vertical Industry Market, Worldwide, 2008-2014, 2Q10 Update」の内部サービスコスト、及び「平均給与単価（後述）」に基づく推計値

出典：　NSF（米国立科学財団）データ（20
- インドは、上記出典の(1) NAS
Observer Research Foundatio
- ベトナムは、JETRO発表デー
- 中国は、上記出典のS&E（Sci

http://www.ipa.go.jp/jinzai/jigyou/global-report.html

「グローバル化を支えるIT人材確保・育成施策に関する調査」調査結果（2011/3/31掲載）

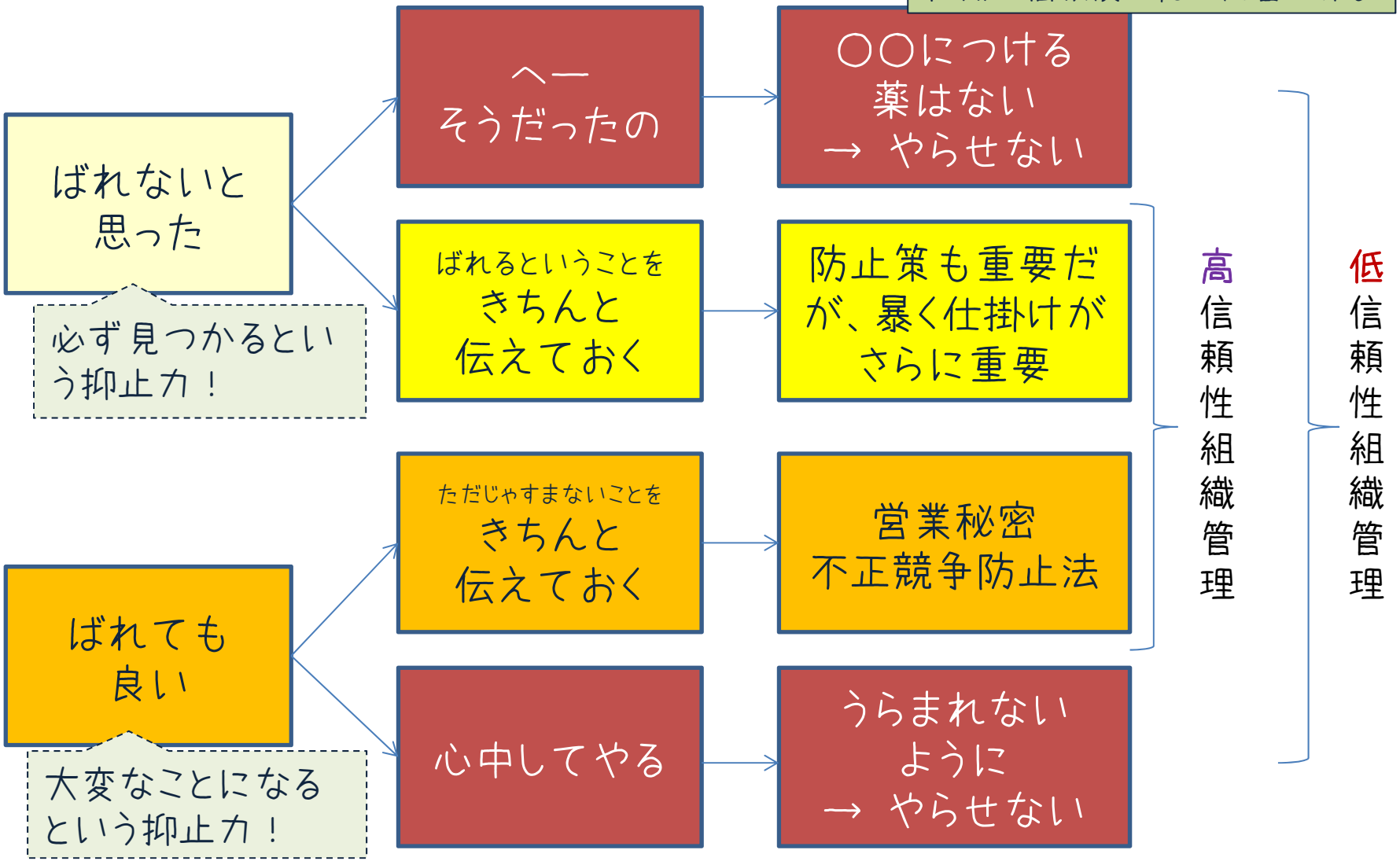
4. 対策のヒント

「しなやかでしたたか」な対応

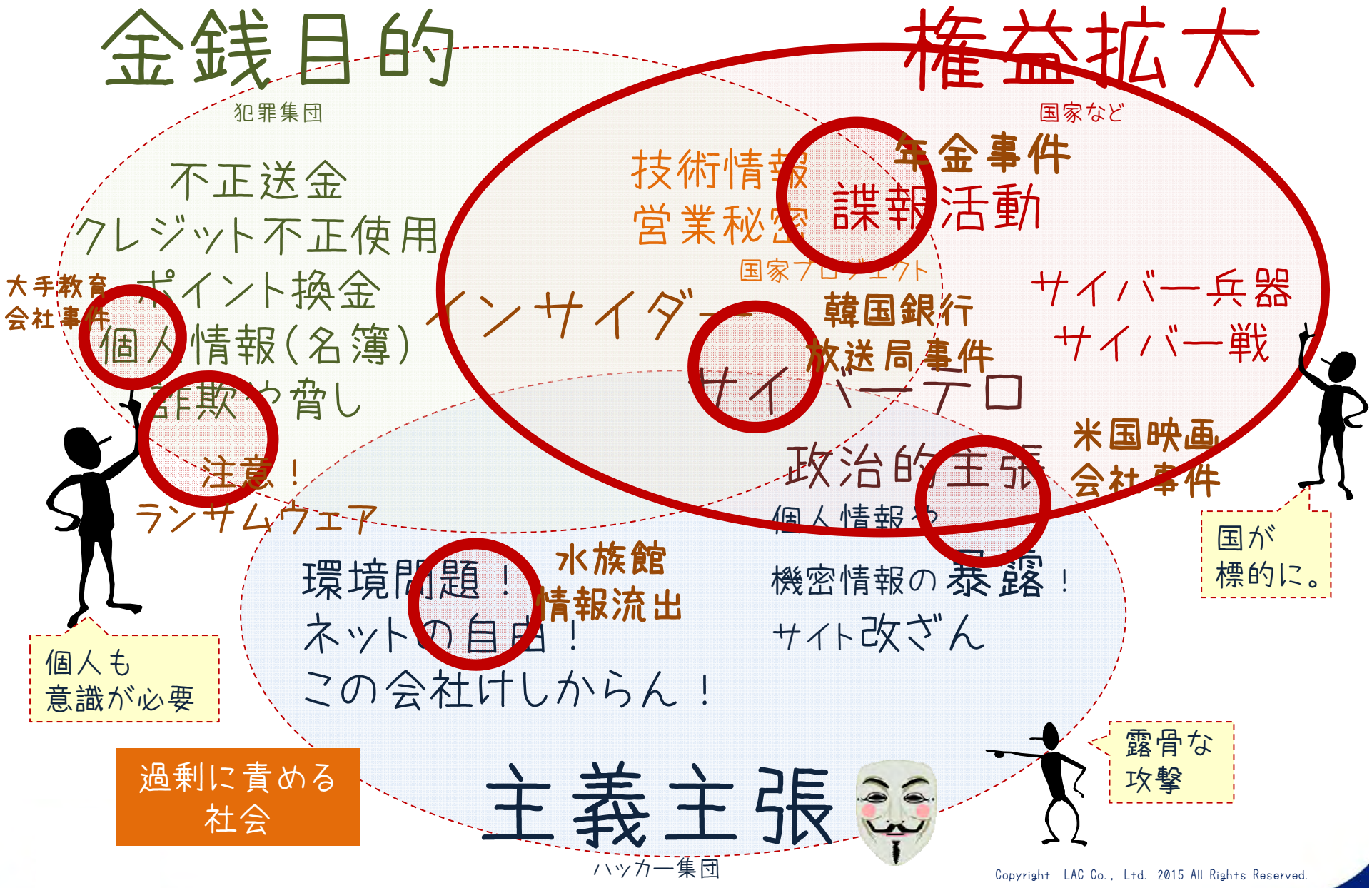
→「事故前提」の対応力、「やらかし」への対抗。

① 内部不正事件の理解

教訓
個人情報保護法と営業秘密指定の抱き合わせが必須。
組織の信頼度に応じた管理策。



② 戦う相手の理解(内部不正も同様)



③ IT活用の原理原則

「機能」と「データ」の理解。

「機能」と「データ」
サービス提供者が全部やってくれるように勘違いしていませんか？ 職責分離！

1）アプリ(=機能)

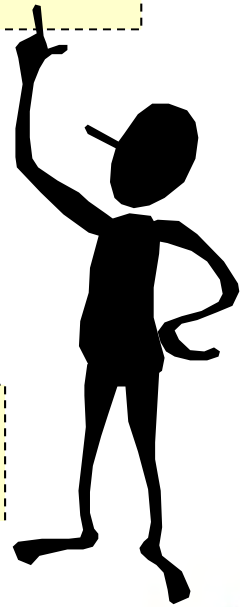
(1) 基本的に専門家から提供される。
(2) 基本的に代替え策がある。
(3) 基本的にどんどん進化する。

代替策のない、「機能」は分かっていますか？

2）データ

(1) 基本的に利用者が責任者。
(2) 基本的に代替え策がない。
(3) 基本的に変化しない。

個人も意識が重要！



④ セキュリティの原理原則

制度上の大原則

① 職責の分離

② 最小権限(特権)

→ その上での各種施策

情報システムには、
機能とデータがある。
それぞれの
オーナは誰？

施策上の大原則

① 識別、認証、認可

② アクセス制御と追跡性担保

⑤「解決」への糸口　組織の性格を理解(分ける)

1)低信頼性組織
- (1)マニュアルと再発防止策
- (2)防止・全容不可視の仕掛け
- (3)性悪説が前提

2)高信頼性組織
- (1)ルールと(裏切りへの)重い処罰
- (2)暴く仕掛けとうっかり対策
- (3)性弱説を想定

⑥ やるべきこと

1）割れ窓をなくしておく

→ 事件で発覚するルール違反は致命的

例えば、個人情報流出事件でその原因となったルール違反が発覚！？そこで処罰を検討！？

私たちの特性 ⇒ ルールを作って安心。
→ 事件が起きると、ルールはあったのですが、、
一時しのぎは定着出来ず、放置すると割れ窓に。

管理者は割れ窓を管理し、経営者は管理できているかを監督する。

割れ窓は経営責任！

⑦ やるべきこと

2)対策の限界と骨子を理解する

(1)内部不正犯を暴くことができますか？
　→ まずはこれをやる。記録はありますか？　ないと、、

(2)内部不正に気付くことができますか？
　→ 監視、点検が重要だけど、絵に描いた餅だと、、

(3)内部不正を防止できますか？
　→ アクセス制御、暗号化、、、

(4)内部不正を抑止できますか？
　→ 高信頼組織、透明性の理解

さて、どれからやりますか？

⑧ 参考 DB内部不正対策ガイドライン

DB 内部不正対策ガイドライン

第 0.9 版

2015 年 7 月 28 日

データベース・セキュリティ・コンソーシ

DB 内部不正対策 WG

1

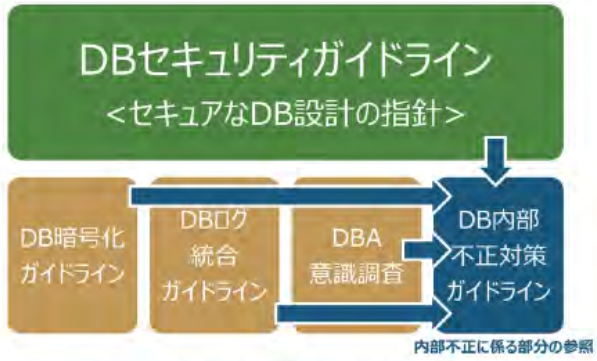
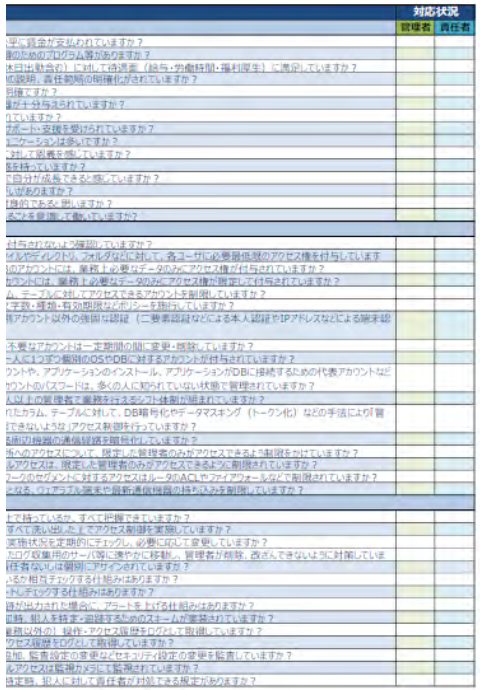


図 1.2.2 DB 内部不正対策ガイドラインとその他 DBSCWG との関係

- 本ガイドラインにおける「責任者」「管理者」「分析者」の相関関係については、以下のとおりである。
  → 責任者は管理者に対して内部不正につながらないための管理を各項目（管理者の誘因に対する項目参照）について実施する必要があり、また管理者はその作業内容について報告を徹底しなければならない。一方で分析者は管理者が規定通り DB の管理を行っているか、運用の実施状況を監視する必要があり、管理者の逸脱について責任者へ報告する必要がある。別途分析者を設けられない組織においては、責任者が兼務する形で補うことを想定する。

図 1.2.3 責任者・管理者・分析者の相関関係



⑨ まとめ

いずれにせよ、

1）CSIRT的な組織は必須
2）ルールと割れ窓排除
3）最低限のIT知識

異変を見つける能力を専門部署だけではなく、一人ひとりが持つ時代。
また、一人ひとりがデータの取扱いを意識しなければならない。

ご清聴、

ありがとうございました。

CYBER GRID JAPAN

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