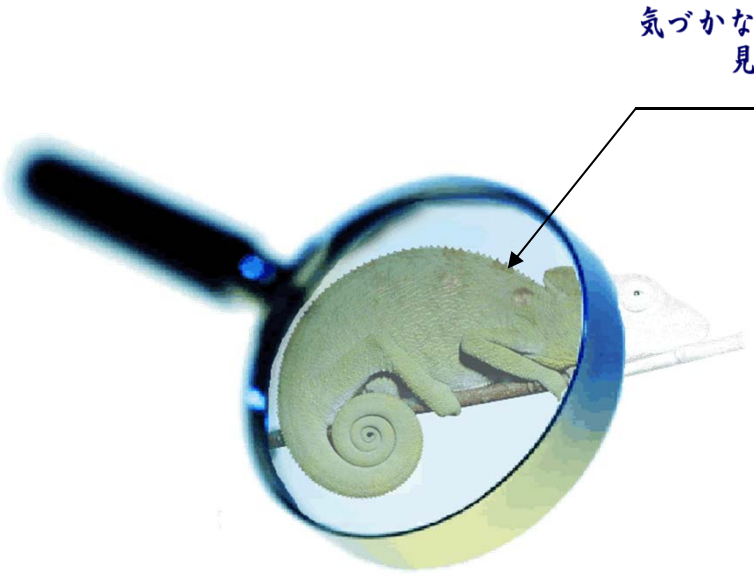
サイバーセキュリティ、現状と対策

安心とともに

～企業等におけるサイバー攻撃対策と
スマートフォンの利活用とセキュリティ対策～



2013年2月1日

株式会社ラック
セキュリティ事業統括 専務理事 西本 逸郎
http://www.lac.co.jp/

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）、サイバーセキュリティ研究所、サイバー救急センターが特徴です。

商　号	株式会社ラック LAC：LAC Co., Ltd.
設　立	2007年10月1日
資本金	10億円
代　表	代表取締役社長　髙梨　輝彦
売上高	連結 315億円（2012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）

・名古屋オフィス
〒460-0002　名古屋市中区丸の内2-18-11
46KTビル4F

・米国ニューヨークオフィス USLAC

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

・中国上海 子会社 LAC CHINA
上海楽客網絡技術有限公司

■ 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

にし　もと　　いつ　ろう
西 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

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　専務理事 セキュリティ事業統括
　　サイバー救急センター 調査員
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
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
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

2009年度情報化月間 総務省　国際戦略局長表彰

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 委員
総務省 スマートフォン・クラウドセキュリティ研究会 委員
経済産業省　サイバーセキュリティと経済 研究会　委員
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。

LAC

1. 昨今の諸事情

→ 昨今の情報セキュリティ問題の背景、原因の解説

其の壱 スパイたち！

25 → 2008年～2011年までの対応数

27 → 2012年での対応数

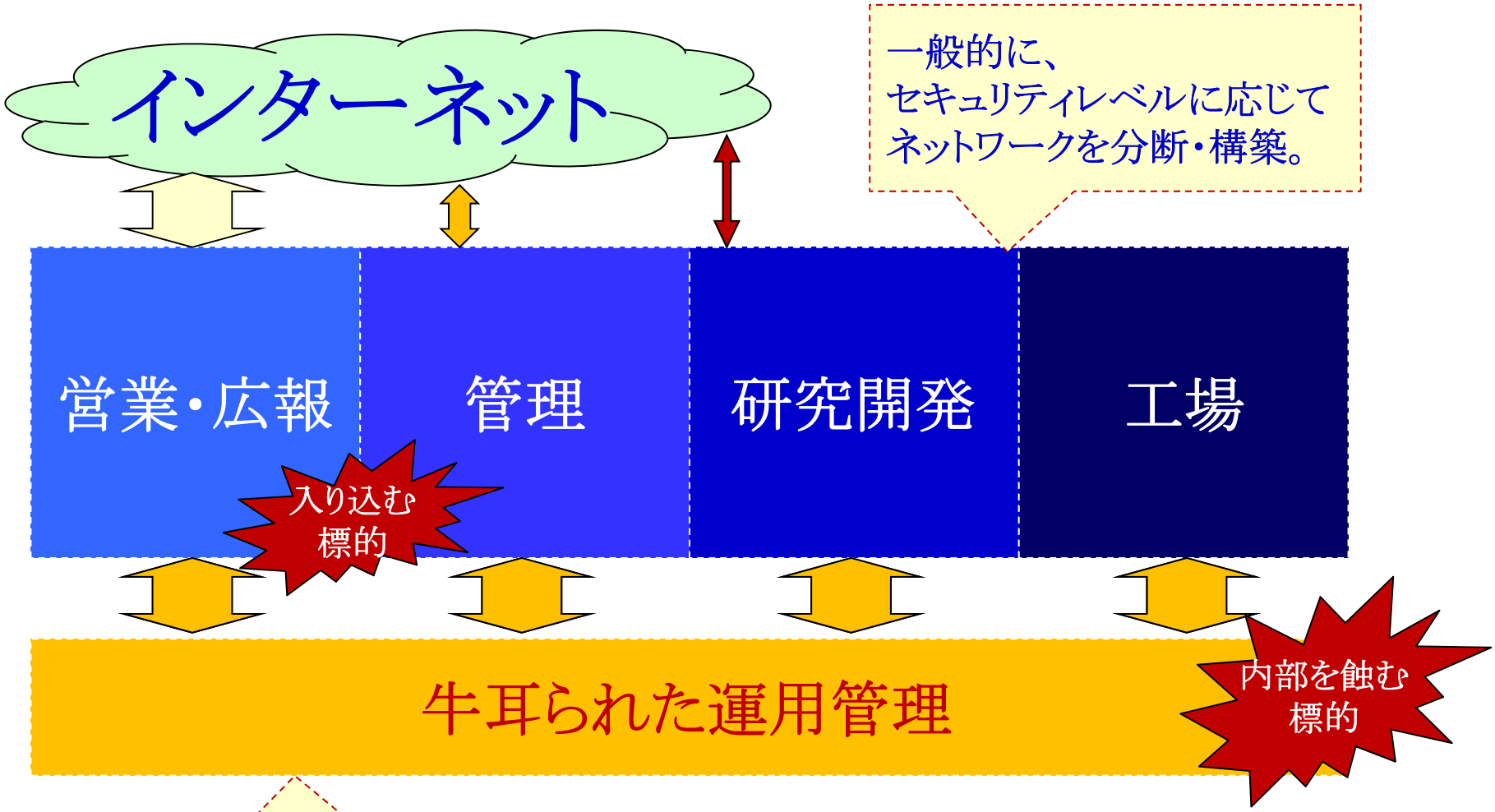
18 → 侵入時期が2011年3月～5月頃だった事件
(67%)

3 → 侵入時期が2009年12月～2010年1月だった事件
(11%)

5 → 52事件中、管理者権限を取られてなかった件数
(10%)

LAC

其の壱 スパイたち！



LAC

其の弐 主張する人たち！ 霞が関？霞ヶ浦？

1. 今回の表向きの攻撃
   1）アプリケーションサーバの脆弱性で改ざん
   → アプリケーションサーバ問題は根が深い。使用理由。運用管理をやりたくない！
   2）**DDoS**（ツール・やり方の提示）

2. 多くの攻撃は検索エンジンから
   → 金銭目的では以前からの常套手段
3. 機密を盗み暴露したいはず。
   → 大手電機の米子会社でやったような個人情報
   → メールなどの公にできない秘密
   → 関係者のプライバシーの暴露など
4. 日本への飛び火や連携。

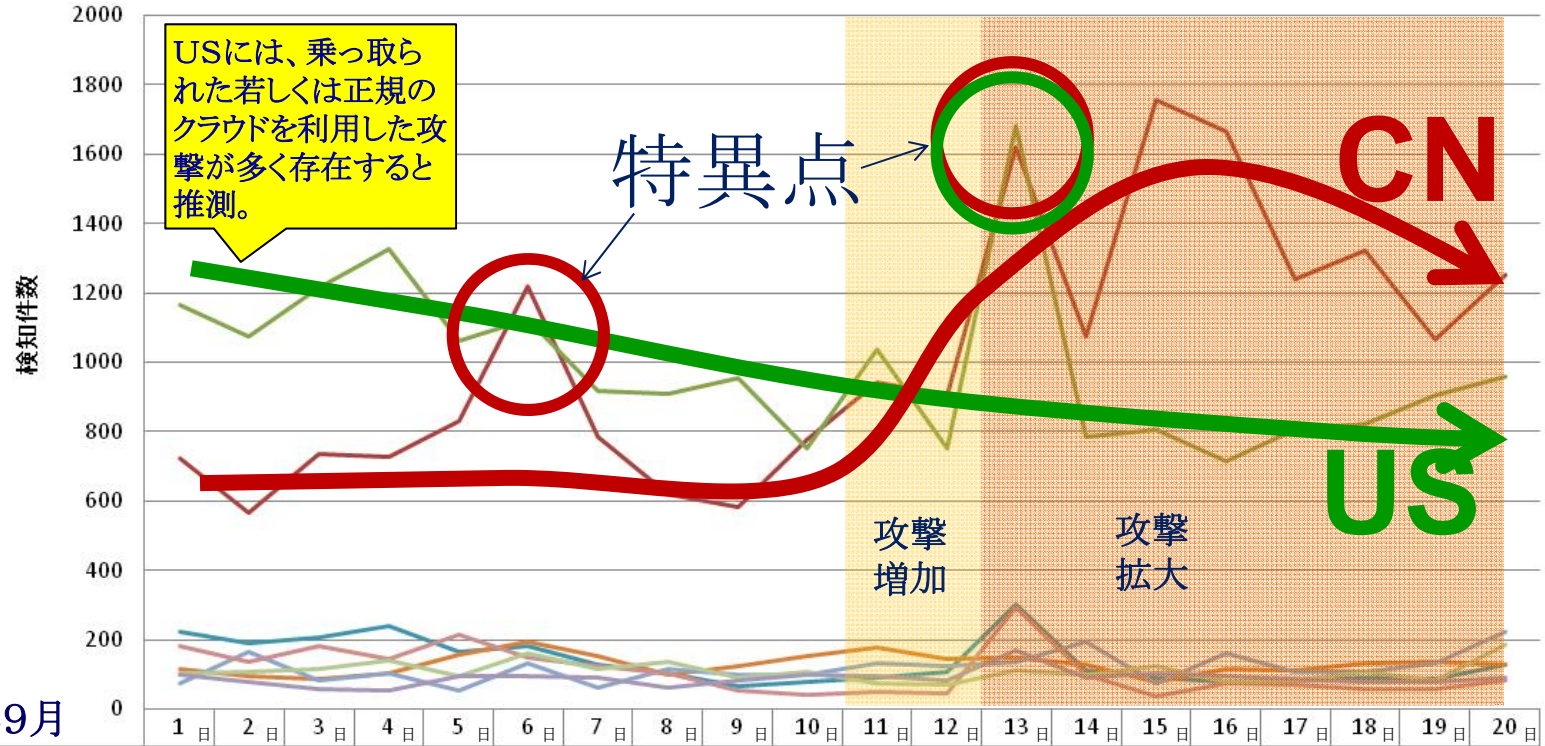
抗議行動だとすれば、誰が困っているか？狙い通りになっていないことをキャンペーンするのも、手。

LAC

其の弐 主張する人たち！ 昨今の政治的サイバーデモ

当社JSOCでの観測状況

攻撃イベント件数（国別）



2012年9月

	1日	2日	3日	4日	5日	6日	7日	8日	9日	10日	11日	12日	13日	14日	15日	16日	17日	18日	19日	20日
CN (China)	722	566	737	727	829	1221	785	621	583	775	944	905	1619	1074	1755	1664	1241	1324	1065	1252
US (United States)	1166	1075	1216	1328	1061	1125	918	909	955	753	1038	752	1681	785	805	714	805	821	905	957
FR (France)	223	188	206	239	164	182	126	104	64	80	89	106	301	111	90	77	81	90	87	127
BR (Brazil)	114	94	87	102	157	196	153	100	123	153	178	146	147	126	78	117	110	133	138	128
TW (Taiwan)	74	164	84	103	55	133	62	116	99	98	130	125	137	192	75	160	106	109	131	222
DE (Germany)	182	136	180	145	214	148	123	104	52	41	50	47	295	98	37	73	72	58	58	82
KR (Korea, Republic of)	105	109	116	140	94	161	116	137	92	108	74	68	112	99	124	79	84	109	82	185
CA (Canada)	100	78	59	53	96	95	91	61	82	99	95	82	169	90	103	95	88	80	77	89

其の弐 主張する人たち！ 昨今の政治的サイバーデモ

サイト妨害（**DDoS**）は別として、改ざんは、

まずは政府関係機関（**go.jp**）や名指しされた組織
次に関係機関（**or.jp**、**ac.jp**など）、日本ならどこでも（**jp**）
さらに、日本語を使用しているページを対象。

そして、自分たちの道具が有効なところ。無差別に改ざん！

基本は、
アプリケーションサーバや
CMSなどのフレームワークの
既知の脆弱性を突き侵入できる道具。

LAC

其の参　愉快犯！ 遠隔操作

少々考察

1）新しい事件なのか？
→ 遠隔操作ウイルスって。以前から存在している。
→ **D-Type**：金銭目的、**E-Type:**権限拡大目的では、主流の手口。
→ **C-Type**：主義主張者、或いは**A-Type**：愉快犯が、この手を使った。

2）踏み台にされた被害者は？
→ 全く責任はないのか？　→ 盗まれた車で犯罪を犯されたら？
CSRFのリンクを踏んだこと。　→ 掲示板運営側の責任は？
ウイルスをインストールしたこと。　→ 迂闊な行為？
→ 企業のリスク管理の観点では関係ないのか？
→ 社内感染での情報漏えいは？　→ 要は暴露される標的。
→ 社会的地位のある方が被害者だったら？

3）今後のホラーストーリは？
単純な模倣犯や、否認の多発は、さておき。
→ 企業インパクトは計り知れないことが判明。
→ 単なるアプリなので、スマホに行く。
→ **IT**技術者の社会的信頼損失が加速。

重要な情報資産を守れば良いというわけではないのか。

（単なる、つぶやき）デジタル指名手配やプロファイリングを考えたらどうだろうか。

LAC

其の四 金銭目的 本格化する国際化

欧米ではずいぶん前から
→ 日本の銀行や利用者が対象となってきた。
日本の標的化と日本人の国際化が融合。
→ 丸損か？
→ 犯罪の温床？

はなから損失を要求する人たちの存在？

特に企業での銀行とのやり取りをする端末
→ まさか、ネットサーフィンやメールの閲覧を
やってないですよね？

LAC

其の五 サイバー兵器？

高度な不正プログラム（ウイルス）

サイバー兵器と言って良いかもしれない。

21世紀、
こういう不正プログラム同士の戦い？

→「切り離しているから大丈夫」の崩壊。

其の六 社会インフラへの打撃？

1. 安全保障は必須
   →悪用されない考慮も重要。

2. 犯人や原因の特定も重要
   →被害の拡大防止
   →事業やサービスの継続・再開
   が、さらに重要である。

LAC

2. スマートフォン とタブレット

→ 今どきのスマートフォン

さて、スマート　　が、旬らしい

スマート=賢い？？
イメージできないぁ

スマートって何？

キーワードはスマート

スマート=「インターネットとの融合」

例えば、

インターネットと融合した 都市、インターネットと融合した 電力供給

インターネットと融合した PC

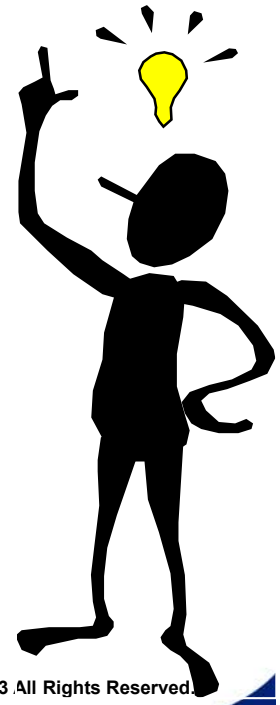
インターネットと融合した オフィス

インターネットと融合した 市役所

インターネットと融合した 大学、学校

インターネットと融合した 国家

置換してみましょう！
sed -e 's/スマート/インターネットと融合した/'



LAC

スマートフォンの位置づけ

企業利用を考えると

1. 現段階で、スマートフォンのスマートな活用。
   → 正直、無理がある。
2. コストダウンと安全性を考慮した活用が無難。
   → 業務専用タブレット（簡易PCの位置づけ）
3. その中でスマートな活用に慣れていく。
   → 2年間程度
   スマートフォンとクラウドの進化
   社会的合意の形成
4. 1年後を目途に次の展開を計画する。
   → 今後のワークスタイル・ライフスタイル
   コストの変動費化と削減の推進。

LAC

一方、BYODといっても

単にBYODと言っても使い方がいろいろあるぞ。
人によって定義が違うのでは？

1. FATスマホ
   パソコンのようにデータを保持して利用
2. メールやセキュアなブラウジング
   メールやドキュメントの閲覧、決裁など。
3. シンクライアント
   社内のデスクトップの呼び出し
4. カプセル化したセキュアなアプリやコンテナ

一方、BYODといっても

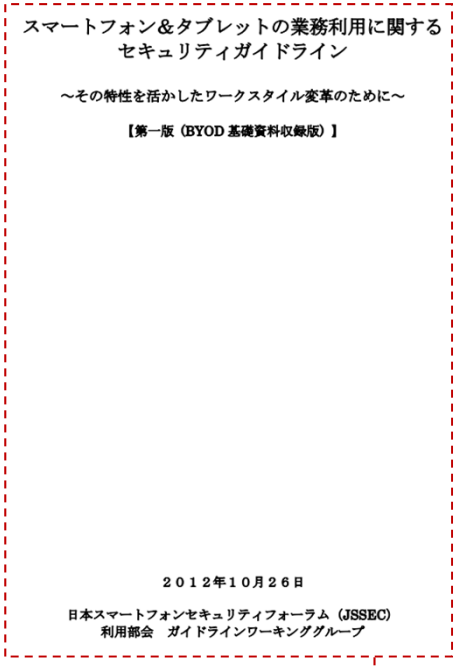
BYODの意識すべきポイント。

1. 管理境界
   端末まで？ ← BYODではあり得ないのでは。
   端末上のある領域まで？ ← 恐らく機器に依存する。
   アプリまで？ ← 合理的。配布方法。

2. 繋ぎ方
   端末は内部の機器。 ← 企業内ネットワークに直接接続
   外部の機器。 ← ホットスポット、4G・4Gなど外部から接続

3. 同意や注意事項
   労務関係 ← 拘束時間、時間外労働など
   利用者情報 ← 位置情報などのプライバシーに関わる情報の取り扱い

4. 当然のことながら、利用目的、対象者、マイルストーン
   今後のスマホの発展、経営者・従業員などのリテラシー度合い



スマートフォン&タブレットの業務利用に関する
セキュリティガイドライン

～その特性を活かしたワークスタイル変革のために～

【第一版（BYOD 基礎資料収録版）】

２０１２年１０月２６日

日本スマートフォンセキュリティフォーラム（JSSEC）
利用部会　ガイドラインワーキンググループ

付録 B-表１　個人所有スマートフォンの業務利用におけるパターン

分類項目(※1) ＼ パターン(※2)	舵取り型	踏み出し型	なし崩し型	知らん振り型	忍び型
所有形態	個人所有				
利用目的	業務利用と個人利用の併用				
利用場所	問わない				
管理者のリスク認識	あり	あり	あり	なし	「舵取り型」と「BYOD 禁止」の場合に存在
導入の意向	あり	あり	決めていない	考えていない	
導入の意思決定	あり	あり	なし	なし	
規定	あり	なし	なし	なし	
規定に基づく許可	あり	なし	なし	なし	

※「BYOD 禁止」とは、BYOD の導入を組織として禁止している状態です。

などを意識してご活用ください。

→ JSSECでBYODでの考慮事項の整理を公開。

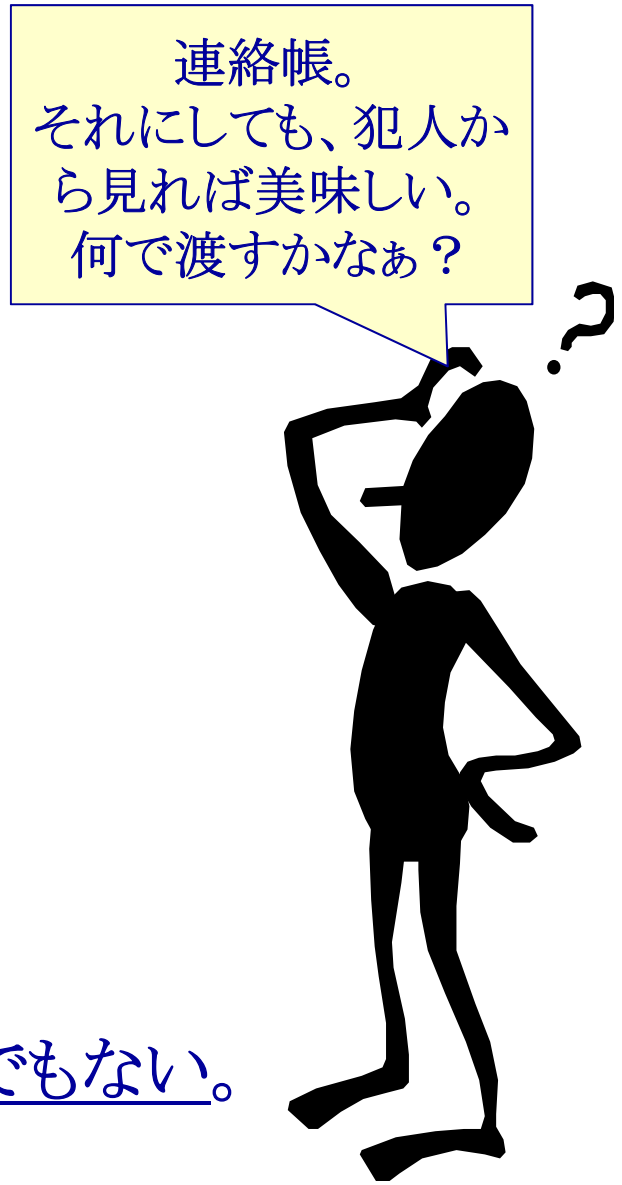
こういう事件は？

やった人間がとんでもないのは
当たり前の話

① マーケット管理
　→ 危険なアプリ
　→ 攻撃性を持ったアプリ
② 開発者の見極め
　→ 悪意のある開発者
　→ しょぼい開発者

が、しかし。

連絡帳に知り合いを登録している
という意識は重要。
単に、自分の身を守れば良いというものでもない。



LAC

ところで、情報保護

1. 個人情報保護法

→ 全うな会社への管理要求
→ 流出した情報の保護は？

2. 不正競争防止法

→ 営業秘密の保護。
　　場合によっては差し押さえも。

3. 所謂ウイルス作成・供用罪

→ やった行為には言及なし。

4. 不正アクセス禁止法

→ 所謂、アクセス制御の回避。IDとパスワード

悪意を持って、
盗られた、取られた、
流通した個人情報は
取り返せない。

持ち主が個人情報取り扱い事業者の場合は、管理責任が生じる。

ところが、1000万人は、自分が登録されていることすら知らない可能性が高い。

LAC

スマホでの注意事項

1. お天道様に恥ずかしくないように

①アプリ作成者やサービス提供者
②利用者 → アプリの目的外使用（自分で or 他人へ）

2. 人に迷惑をかけるな

①保護責任 → 例えば連絡帳
②踏み台・ボット

3. 賢い利用者に

①自爆 → SNSなどでの発言、暴露、無知、飲酒
② 詐欺・脅し・泥棒・ストーカなど ← みんなここに注目するけど、一番最後でい良いのでは？

LAC

3. 対策のヒント

→ 事故を前提とした対応力、心構え　等

事故は、
前提になっていますか？

事故が前提とは。例えば、

1. 「もう、既に」の危機意識
2. 万一の決断と予算想定
3. 万一のプロセス想定
4. 必要な技術と勘所の理解
5. 演習と専門家連携

敵と同時に己も知る必要がある？

敵は何を狙いたいのか？

愉快犯　：基本的にはセキュリティレベルの高い有名組織

主義主張：政治的、アノニマス的、内部告発的、総会屋的

金銭目的：クレジットカード、アカウント、インサイダー、知的財産

権限拡大：防衛機密、国家機密、知的財産
日々の活動、人脈関係、不祥事

知的財産って、どこにありますか？
→ファイル、データベース、システム

それぞれの最悪を意識すると優先度が見える。

LAC

手口から考えられること？

アノニマス？政治的主張？金銭目的？破壊的愉快犯？

新しい手口が次々と？

侵入手口と目的を分離して考えるのがポイント。

侵入手口：← 大きな変化はない。

1）脆弱性や設定の不備などを突き、能動的に侵入する。

2）リンクのクリック、添付の開封、アプリのインストールなど、受動的に侵入する。

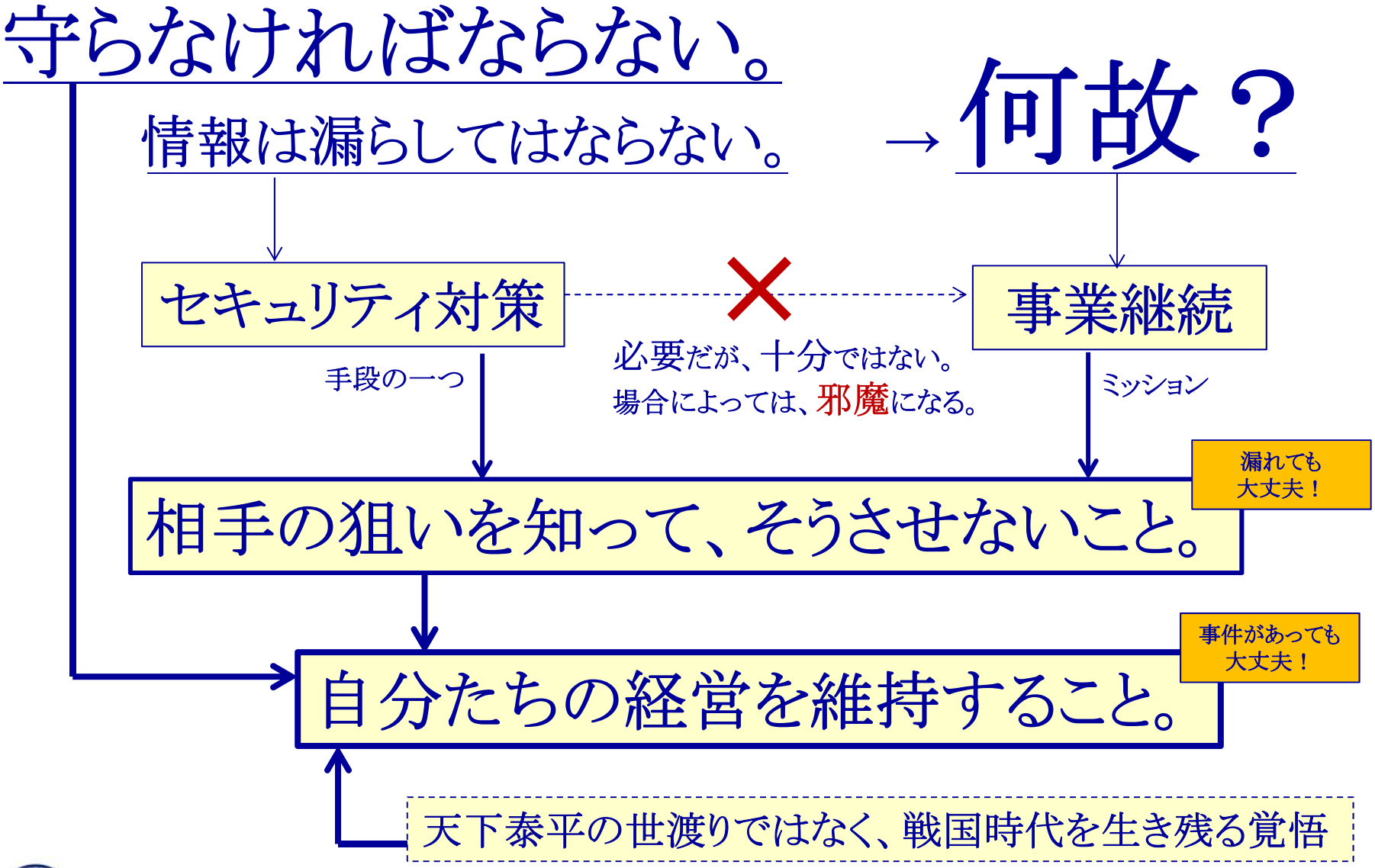
目的：← ここが変化している。

前述の、**A,C,D,E,F**の各**Type**毎に異なる。

例えば、情報窃取を考慮しても、金銭目的、主義主張、権益拡大、ストーカでは使い道が異なり、脅威も異なる。

LAC

何が必要か？



アリバイ対策ではない原点

曖昧にやってる。
やるなら意識的に。

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

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

LAC

例えば、データの管理は誰がやる？

情報は守るものではない。

→ 共有するものである。

これまでのアプローチ

→ しっかり管理してね！

→ とはいっても前述の状況。

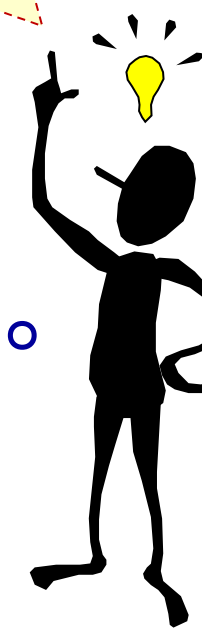
→ 本丸からではなく弱いところから。

→ しかも、内部犯も。

自ら情報管理を。 → サービス継続も同様

→ 他人任せには出来ない人から。

明快！
システム管理者と
データオーナの
責任範囲は異なる！



LAC

セキュリティをやる意味

何事も、価値観が重要。
セキュリティ価値観を考えてみましょう。

日本にお勧めの価値観

お天道様に恥ずかしくない。
人に迷惑をかけるな。
賢くあれ。

自分たちの経営が出来なくなることが最大の脅威である。顧客（市場）を守り、組織の生き残りを図っていく。

情報セキュリティは、情報システム部門で！
などの悠長な時代は終焉。
経営者の決断が、まず第一歩となる。

LAC

4. 基礎知識

→ 情報セキュリティに関する基本的知識と新常識

情報セキュリティとは？

学問的には、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。

C　覗かれるな！　覗くな！

セキュリティはこれ！と、
思っている人が、大半。

I　騙されるな！悪用されるな！　騙すな！悪用するな！

間違ったら結局だめ。
被害者ではなく加害者に。

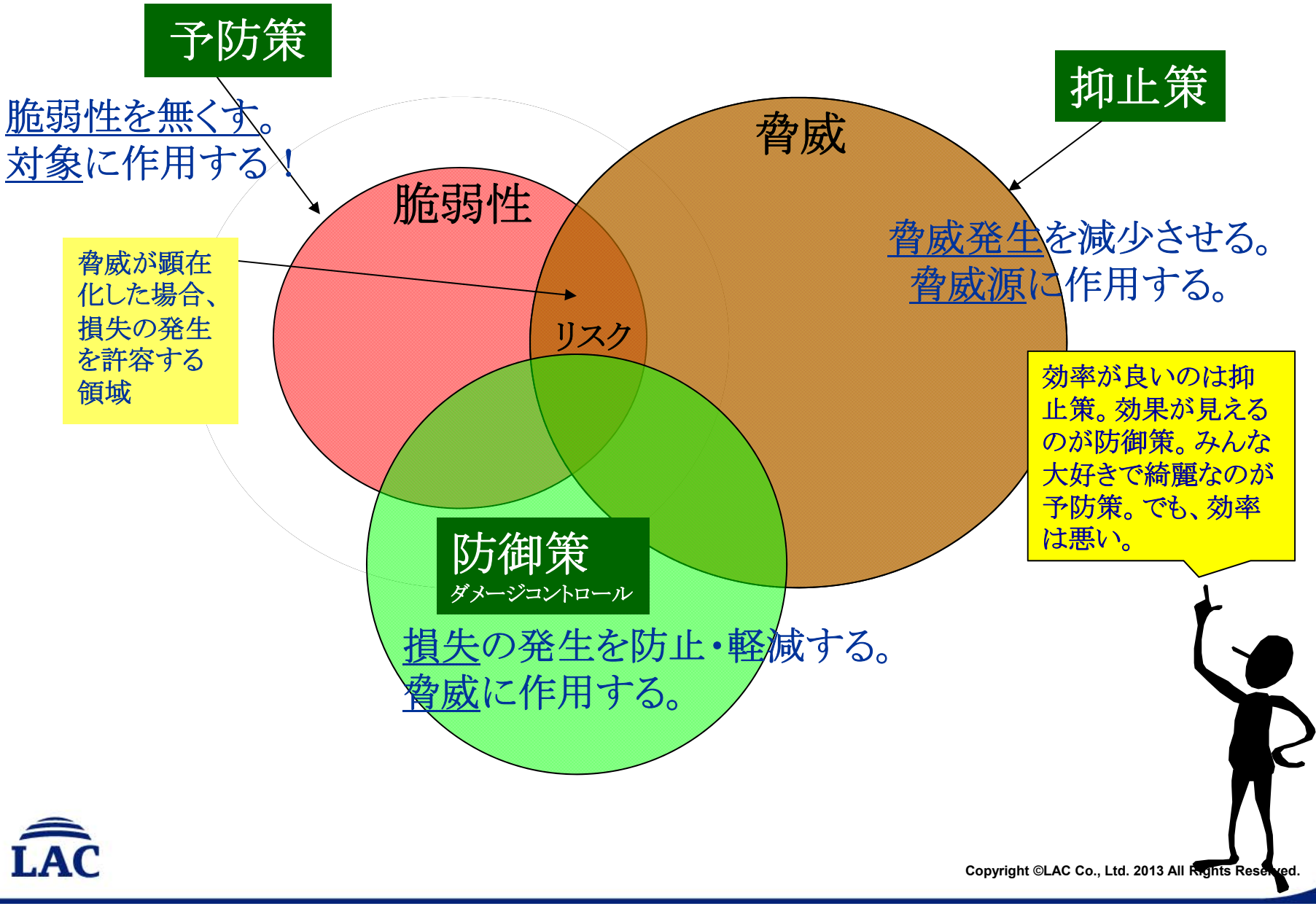
A　邪魔されるな！　邪魔するな！

サービス・事業の継続！

結局、CもIもA のため。

LAC

情報セキュリティとは？



LAC

セキュリティが必要な理由

セキュリティは
何故必要なのか？

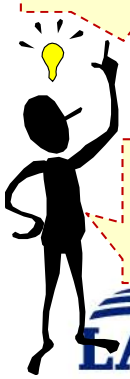
セキュリティが
ブレーキだとしたら。

ブレーキは
何故必要なのか？

1. 捕まる・叱られる！ → 性能ではない。付いていればよい。
2. 万一のため！
   → 永遠の課題？
   → どこまでやれば良いのでしょうか。

我々が遅れているのはセキュリティではない！

---- これより上の議論が大半。それほどの成長は必要ない？ ----



車（IT）を未だに、高々下駄だと思っている！

3. 速く走るため！
   → ブレーキなしでは無理。

速く走らなくても！
良いんじゃない？

大原則:敵を知る　知彼知己、百戦不殆

A-type：愉快犯
愉快犯・自己顕示欲などは以前から存在し、恐らく今後も存在。

B-type：市場支配(プラットフォーマ)
市場支配者或いは支配を狙っている人。選択肢のない強制。

C-type：主義主張
国家や企業の犯罪告発。国家などの「制限や統制」に対する攻撃。政治的嫌がらせ。

D-type：金銭
金銭を得る目的での、情報窃取や業務妨害と恐喝まがいの商売など。

E-type：権益拡大
平和維持、権益拡大のための諜報活動。他国の権益拡大行為や軍事活動の妨害。

F-type：ストーカ
個人相手だけではなく、企業も対象となる可能性。

LAC

ありがとうございました。

Any question ?

LAC

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