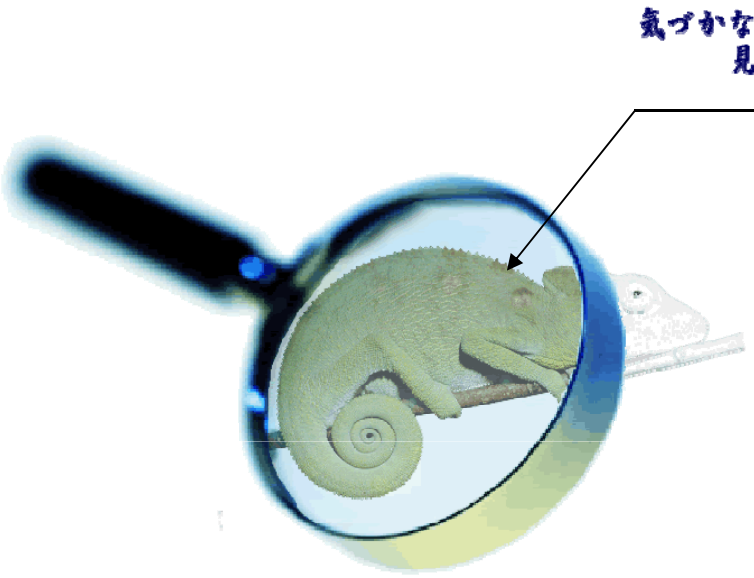
第17回 サイバー犯罪に関する白浜シンポジウム

サイバーセキュリティ関連事象のおさらい

～ 10の代表的トピックスとみえる課題～



2013年5月23日
株式会社ラック
CTO 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

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、情報通信技術のさらなる利活用を支えるため、サイバーセキュリティ分野にて脅威への研究や対策に邁進。

わかりやすさをモットーに、官庁、大学、その他公益法人、企業、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　専務理事 CTO
　　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
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 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。

この度は、
弊社の不手際により、事務局を
はじめとする関係の方々に、
多大なご迷惑をおかけしました。

非礼を、お詫び申し上げます。

1. この一年の事象

→ 私の独断と偏見で。

其の壱　噛みつくアノニマス

「アラブの春」政府側の検閲などを妨害。

麻薬組織への恫喝

違法ダウンロード刑事罰化への対抗

北朝鮮へのちょっかい

次は石油業界？

アノニマスを支援(?)する多くの関連団体

自由、環境、権力への挑戦など

→ 当面、話題は尽きないだろう。

其の弐 定例化する918

少なくとも2010年から2012年まで3年間連続で発生。
→しかも、三連休！

毎年、**9月は演習月間**！
→ **8月は点検月間**！
+2月も。

対策の「副作用」への考慮も必要。
→ 向こうの狙いへの根本対策

其の参 増幅反射するオープンリゾルバ

1. 野良オープンリゾルバへの課題
2. 役割や社会的使命に応じた対抗
3. 限度を超えた攻撃の見方

其の四　ストックされるアカウント

1. ストックされているアカウント情報
2. 攻撃実態はほとんど闇の中
3. 目的も全て明確なわけではない

其の五　踏まれるアプリケーションサーバ

要は「　　」問題。

- 無線**LAN**
- オープンリゾルバ
- 多くの管理されていないパソコン
- 管理されてないアプリケーションサーバ

1. 安価なレンタルサービス
2. 保有・管理から利用の推進
3. 情報システム部門の変化の顕在化

LAC

其の六　復活！銀行強盗

スマート(=　　)

スマートフォン
スマートグリッド
スマートシティ
スマートオフィス
スマートジャパン

これは、まさしく現代の「　　」

其の七　代替え策の企業内システム破壊

1. 一般利用者から企業内へ
2. ねちねち遠隔操作仕込み
3. 利用目的が異なる。自爆的な攻撃。
4. 狙いは？

A. 愉快犯？金銭目的？

B. 主義主張？権益の拡大？

C. 基盤を失う。

今回**ATM**も被害にあったという。
原因は？ マニュアル的な

其の八　素人もすなる遠隔操作

1）仕込みにTOR使用

→ 掲示板へ「殺人予告」などを書き込むことが目的ではない。

→ [redacted]への怨恨・愉快 或いは [redacted]への怨恨・愉快

2）掲示板でソフトをインストール・確保できたウイルス

→ 所謂、にちゃんねらー。

→ 報道されている以外の[redacted]の存在。

→ C#。基本一から作成（コピペあり）。亜種ではない。
　　Web関係プログラミング。日本人。

→ ウイルスの素人。非感染・非難読・非隠蔽。→ 普通のプログラマ

→ 脆弱性の未使用。（使わなくてもクリックする。）→ 対策の常識が、ここでも無効。

其の九　消えたデータと経営

これは、この業者の　　な例なのでは？
大手であれば、　　ではないか？

低価格のサービスに留まらず、第三者に業務を委託をするということは、

1. 契約約款 → 確認してますか？
2. 万一のとき、保証返金はあるのか？
3. 万一のとき、何を保障して、保証してくれるのか？
4. 万一のとき、　　できるのか？
5. 万一のとき、損害賠償要求が出来るのか？

事業インパクトを、よく理解し覚悟しなければならない。
どういう約束でも、　　解決できないことを理解し、
事業の継続を考えておかなければならない。

LAC

其の番外編(1)　低年齢化

子供がネット犯罪！？
ましてや悪質なプログラムを開発？
→ そういう情報から
→ 有害情報！

プログラム開発を有害情報と言われかねない。
→ 勉学、武道、趣味
→ 大人の指導が可能
→ 情報技術になった途端に

知育の観点で、子供への情報技術を指導。

LAC

其の番外編(2)　ネット選挙

選挙関係者の事前対策と、選挙期間という短期間の一発勝負での対応。
現状の環境変化に対して、大きな選挙は大河の流れで、他の選挙で日々の訓練も重要。

一般の有権者が選挙運動を知る。
一般の有権者の選挙運動が増加する。
選挙における不正などはどこの国でも起きているが、一般的にはその国の信頼度を問われるものである。

候補者や政党側よりも、
メディア、保護者、学校の先生への啓発が極めて重要
さらに、当然のことながら、一般有権者の見識に
日本の将来がかかっていることは間違いない。

LAC

2. 明らかになった課題など

→ これまた独断で

1. 金銭目的への課題と対抗

1. 日本語の壁の崩壊
   → 上記の国際連携
2. 国際的に見ての[redacted]凸凹。
3. 国際的に見ての[redacted]凸凹。
4. 取得されているアカウント把握とその取り扱い。
   → [redacted]？
5. 手口の情報連携
   → 誰とどうやって？
   → 侵入手口（脆弱性、なり済まし）
   → 犯人の推測と対抗？

2. 副作用への配慮

1. 政治的な抗議などでの改ざん
   → 対策の浸透がもたらすこと。
2. DDoSへの対抗
   → サイトでの責任
   → データセンターなど
   → 社会基盤
3. [redacted]への対抗
   → ある面、嵌まるのも仕事かも。
   → そのうえで、どう考えるか。

マニュアル対応が被害を拡大？

→ 相手の狙いを意識し、
→ そうならない対策が重要。

LAC

3. いざとなったら見える

「監視社会到来」などと、
→ 暗いイメージで語られることが多い。

逆に監視がない社会って？ → 誰がどうやるのか？

1. ドジを踏まなければほぼ捕まらない。
2. 抑止が効かず、社会コストが増大する。

TORなどを使用した犯罪。
（匿名化、暗号の徹底的な悪用）→ 常態化は必至。
→ 完全犯罪は成立しない。人間系で発覚。
→ いざに備える。
→ 使用する機会を減らす。

4. 情報経営への黎明

1. 利用企業　→ 一般的に利用
2. 活用企業　→ 合理化を推進
3. 基盤企業　→ 事業基盤
4. 社会企業　→ 社会責任
5. 安保企業　→ 安全保障

4. 情報経営への黎明

知識

→ 情報

→ デジタル化

→

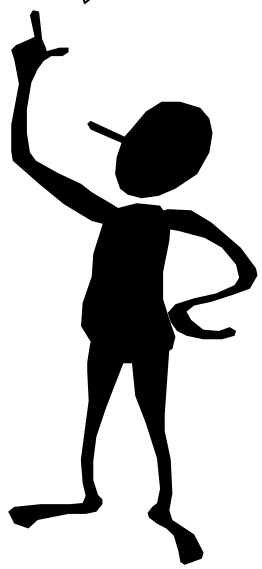
技能

→ ソフトウェア

→

もちろん、これが、
全てではないけど、
起きている変化の
一端がある。

これって、
聞いたことがある



情報通信技術の原則

実は、二つの基本要素がある。

1. 機能

2. データ

4. 情報経営への黎明

制度上の大原則

① [redacted]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、[redacted]

② アクセス制御と[redacted]担保

4. 情報経営への黎明

社員のデータ取り扱い技術の優劣が
成否を握る？
→ これってセキュリティ文化？

一方、経営者に
→ 情報技術感性は必要か？

4. 情報経営への黎明

所謂ビッグデータセキュリティ

→非構造化・非定型的データ中の個人情報。

→ 足りないかな。

　見えてしまうこととひも付け

そんなことやるわけないでしょ！

→ 本当に我慢出来ますか？

ビッグデータポリシー？

5. いつやるか？

今でしょ！

何を？

誰が？

どうやって？

3. 一歩前へ

時代の流れ

1980年頃から始まっているこの変革。

2030年頃に全人類が対象となるらしい。

全ての生命が目を持つ大変革をした、

→ [　　]の五百万年

全ての人類が目を持つに至る、

→ 大変革の[　　]

デジタル文明と
セキュリティ文化

2013年

「まだ」か「もう」かは分からないが、

→この**10**年の[　　]がポイントか。

情報システム部門の今後

直近の課題

CIOで大丈夫でしょうか？

責任分界。利用者

基幹業務の今後。

成長・差別化戦略を支える。

品質・対応

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