日本2015年のセキュリティまとめ！

～重い腰を上げたJAPAN！～

CYBER GRID JAPAN

2015年11月20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
「手を取り合って、垣根を超えて」
⇒ 色々つながろう！
と言う意味かな？

① つながることで発展！

産業革命 ドラッカーさんの2000年の頃の考察

蒸気機関の発明 → 大量生産 生産性・合理化

本質 → 人を運ぶ鉄道の発明 スタイルを変革した

→ 都市と都市をつなげた。⇒ 自動車でさらに細かく

→ その前に、帆船により大陸と大陸。 ⇒ 航空機

2000年の頃のITは変革の序章に過ぎない。⇒ 生産性・合理化

分岐点は2005年 ⇒ ドラッカーさんの亡くなった年

スマホ→人と社会 、SNS→人と人、IoT→ものとものさて2015年、分岐点から10年！

つなげて何を？ ⇒ 対話・情報・体験

さらに、エネルギー、物流・自動制御

今後何と何が

② そのIoTで最低限考慮すべきこと

脅威としてとらえておきたいこと(例)

1)人間の意志ではない脅威への対抗
　故障、災害や事故などに起因すること

2)故意の脅威への対抗
　(1) 外部の攻撃者によるもの(直接、成り済まし、間接)
　(2) IoT提供者の意図した攻撃
　(3) IoT利用者からの意図した攻撃
　(4) 利用部品の脅威
　→ 設計・テスト・維持・廃棄

3)ビジネス上の脅威(い・き・の・こ・り)への対抗
　収益構造、社会問題、風評被害


2. 2015年インシデント
いろいろ

① 今年のトピックス

西本が選んでみた2015年10大ニュース

1）日本年金機構事件と標的型攻撃活動
2）サイバーセキュリティ基本法施行とサイバーセキュリティ戦略2015の再仕切り
3）セキュリティ人材枯渇が喫緊の課題へ
4）継続するインタネットバンキング不正送金
5）本格化したランサムウェアによる恐喝
6）ついに日本でもDDoS勃発 ちょっと意味不明なところも
7）アノニマス 業務妨害や窃取情報の暴露
8）マイナンバー導入によるセキュリティ騒ぎ
9）未成年もすなるサイバー犯罪
10）サイバー抗争激化

② その日本年金機構事件を振り返る

1）油断と遮断の決断

入るまであの手この手、油断を誘発し執拗に
実際の対応はシステムでというより、人力が重要 ‥ 課題

2）割れ窓放置の発覚

本音と建前の崩壊 経営責任は問われるのか？
システムにおける5S 少なくとも整理整頓は？

3）無謬性・正論の跋扈

事故はあってはならぬもの 風邪をひいてはならない
結局事故ると責められる → セキュリティはやらない

歴史的勝利！覚えてますか？
日本代表の波状攻撃！

BREAK THROUGH
壁を打ち破れ

闇雲に突入してる？
一つ一つが計算されている。
縦に横に誰を標的に！

最終的に左に一気に振って歴史的トライ！

それと同様！

標的型攻撃メール！稚拙なメールも？
油断、慣れ、辟易、消耗などを狙う
　違うのは、
標的型攻撃にはペナルティは存在しない
　また、
標的型攻撃にはノーサイドはない！
　さらに、
攻撃自体が見えないことが普通。

③ その三つの報告書から学べること

1）経営の無監督 がばれた

組織の横割れが発生、名ばかりCIO、CISO
善管注意義務、管理責任、親会社の無統制

2）やっている ことにはなっている

CSIRT体制表はある。CIO，CISOも存在はしている。担当も居る。
社内にキャリアパスが存在しない。貧乏くじはいやだ！

3）建前の監査 がばれた

情報セキュリティ監査が重要だと言われるがその次元ではない
やると言ったことをやっているか？のレベル。有効性などは先の先。

④ 体制に関するヒント

年金機構事件を受けて厚労省が取った策

（9月18日発表）

第2　今回の事案を踏まえた再発防止策

1．厚生労働省における情報セキュリティ対策の強化

組織的対策

○来年度に向け、省内の情報システム、情報セキュリティに関する機能を再編し、情報セキュリティ対策の司令塔機能を強化。それまでの間は、以下の措置を速やかに講じる。

①情報セキュリティ対策の実務部門の強化として、情報セキュリティ対策室（仮称）を設置。

②即応性の向上、権限の強化（予算、人事、業務面）の観点から、CISO（最高情報セキュリティ責任者）及びCSIRT体制（インシデント対応チーム）の見直し。

- CISOを官房長から厚生労働審議官に、CSIRT責任者を官房長から情報政策・政策評価審議官に見直し。
- CSIRT要員として、補佐、係長クラスの職員（事案の対処支援や関係者との連絡調整に従事）を充てる。

人的対策

○毎年、全職員の意識向上を図るための情報セキュリティに対する独自の集中的な取組期間を設定。幹部職員においては、情報

職責分離を図っていると考えられる。
一般的には、CSIRTは危機管理系経営直下に配置。
さらに、実オペレーションを担うSOCは、このCSIRT配下に置くのが基本。

この体制をとっている組織は少数。
日本国は？

⑤ 総務省の中間報告から

http://www.soumu.go.jp/main_sosiki/kenkyu/jichitaijyouhou_security/02gyosei07_03000086.html

自治体情報セキュリティ対策検討チーム　8月12日付報告書

主な論点

1．組織体制の再検討、職員の訓練等の徹底
- （1）CISO・CSIRTの設置等
- （2）インシデント連絡ルートの再構築（多重化）
- （3）緊急時対応計画の見直しと緊急時対応訓練の逐次実施
- （4）特に標的型攻撃に対する対策の徹底

名ばかりではなく
役割と責任の
取り決めが重要！ ①

②
事故があっても
致命傷を負わない
ための喫緊での要求

③
防御策は最低限
既に実施項目の
確認と今後実施し
て欲しいこと。

2．インシデント即応体制の整備
- （1）インシデント連絡ルートに沿って、都道府県による支援体制を再確認
- （2）不正通信の監視機能の強化
- （3）自治体情報セキュリティ支援プラットフォーム（仮称）の創設

3．インターネットのリスクへの対応
- （1）安全性の確認
- （2）システム全体の強靱性の向上
- （3）自治体情報セキュリティクラウドの検討

マイナンバーの切り離し
割れ窓確認と維持

インシデント
レスポンス
強化 ④

4．総務省の役割

重要だとわかっているが
今は手が出ない。
自治体クラウドに期待し、
来期以降順次整備かと。

要求を理解し、
体力を鑑みて、
合理的に推進！

1

⑥ 落ちてきた必須事項

遠隔操作や情報窃取をやられる疑いがあると連絡を受けたり気づいたら

① 外部(ブラックリスト)への通信を遮断！(必須)
事前に出口は一本化されているかを確認。(内⇒外)
⇒ 一般的にはファイアウォールかプロクシサーバで制御。

② 速やかに感染端末を特定し、ネットワークから切り離し！(必須)
さらに、他の感染端末(予備機含め)あぶり出しと切り離し(必須)
⇒ 一般的にはプロクシサーバで調査と制御。

③ 外部とのやり取り状況や感染規模を把握（事件の震度）(必須)
疑わしい通信先や内容を把握するために、外部への通信内容を調査。
⇒ 一般的にはプロクシサーバのログを調査(記録期間は原則1年)

④ 内部で被害が生じている可能性ある場合
感染端末が存在したネットワークと基幹システムが接続している場合、直ちに基幹システムから遮断。

⑤ 感染端末が存在したネットワークに個人情報など機微情報が存在している場合
インターネット遮断を実施。
⇒ インターネット遮断方法の事前検討。公開サーバ、メールサーバ。 Web閲覧、メール受信、情報発信。
⇒ 一般的には緊急用端末の準備

⑥ 個人情報流出の懸念を払しょくできない場合、関係機関などへ報告(必須)
⇒ 連携するセキュリティ専門機関との事前調整。報告相手と報告基準の考慮
ウイルス解析、端末やサーバのフォレンジックなどの依頼。

必須が準備できてない場合はインターネットと基幹システム遮断が前提。

となると、プロクシの導入と適切な記録保持、遮断の確認、それらの事前訓練が必須。

⑦ 落ちてくる必須事項

最低限必要な事前準備

1)CISOの役割確認（厚労省新体制）
リスクをとらえ適切なセキュリティ計画を立案し推進する責任者。「割れ窓」責任。
⇒ 一般的には、やるべきことをやる責任。
事件を起こさない責任とは異なる。

2)緊急時はCSIRTが経営直下（危機管理）で動く。
CISOが兼務する場合、その弊害を事前に考慮し、緊急時の取り決めを行っておく

⑧ 一般企業としての基本的なシナリオ

1）27年度
緊急時に備える
⇒ インシデントレスポンス体制整備
一般社員への基礎教育

2）28年度
自己検知能力の向上
⇒ インシデントレスポンス体制強化
一般社員のIT力

3）29年度
防御能力向上 一通りの運用

⑨ 重要インフラ企業としての考慮事項

一般的に、何かあると 止める　or　通す
　　某航空会社事例 or 某鉄道会社事例

1）事故だけではなく、故意の意識
　・利用者、内部関係者、取引先など
2）相手の目的の封じ込めと人命保護
　・脊髄反射が標的に
　・人質に取るようなものだけど、、
3）過剰な規制や要求
　・監督官庁や捜査機関など

3. 避けられない課題

① 枯渇人材に関して

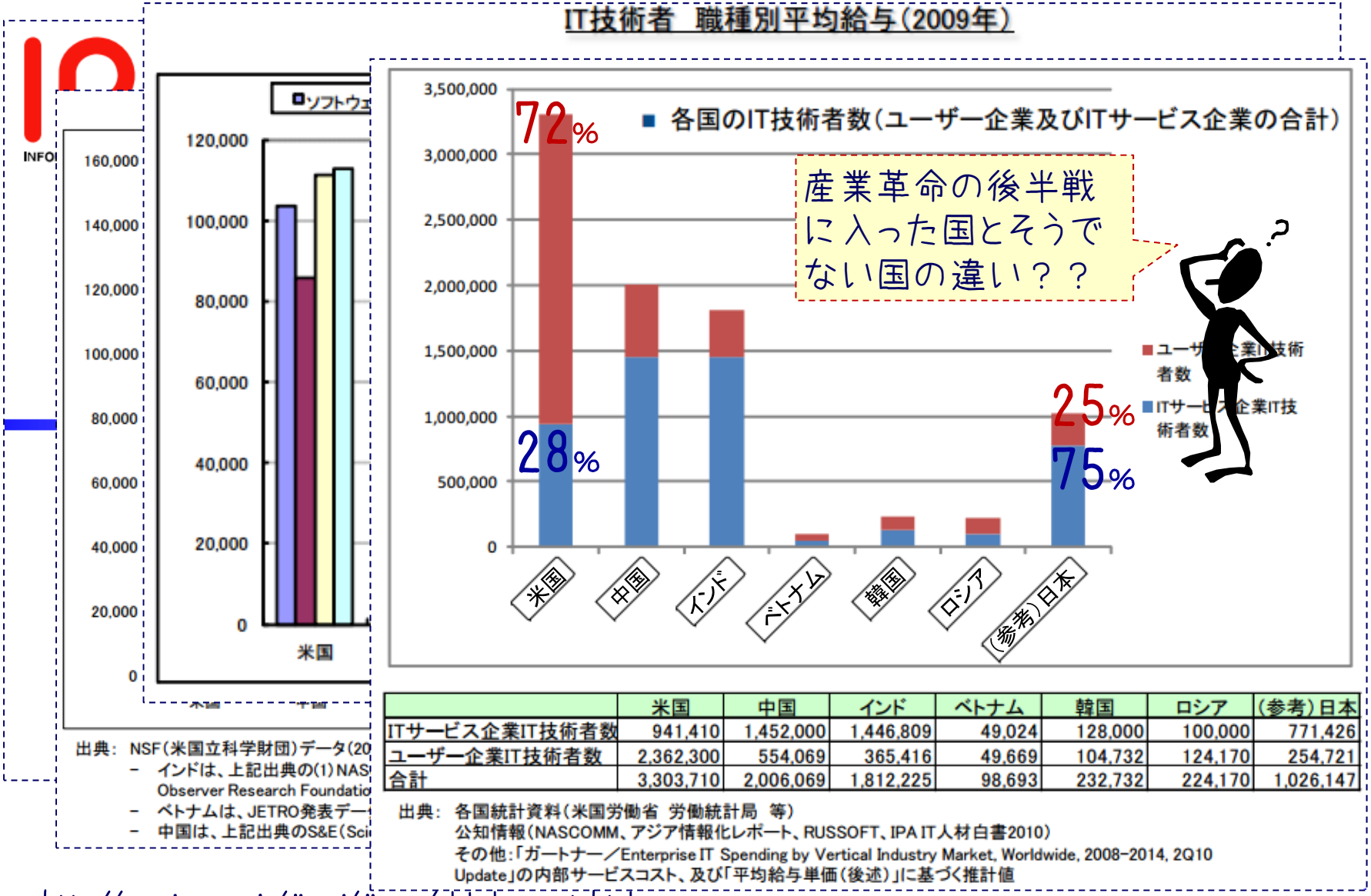
キャリアパス

1）一企業で同じ人材を確保？
2）一企業でキャリアパスを準備？

とはいえ、霞が関をはじめ人材が枯渇していることは事実。

でも、その前にIT人材は？

② IT技術者の活躍場所



	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：　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

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

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)

③ 枯渇から瑞々しさへ

セキュリティとIT人材の地産地消は必須に。

企業サイド→ 無いものねだりは無理。
人材サイド→ キャリアプラン。

新しい剣と盾を身につけ転職しよう！

人材の流動化が鍵を握る！

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