第20回サイバー犯罪に関する白浜シンポジウム『サイバー犯罪 温故知新』南紀白浜 2016年

サイバーセキュリティ対策推進の肝を紐解いてみる

～それは、火中のクリか黄金か？～

LAC
ともに、イキル

2016年5月21日 株式会社ラック
CTO/CISO 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。　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

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 369億円 （2016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

※ 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。

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)

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

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

■ 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

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

ブログ どらいつ 検索
@dry2

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）

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 / CISO 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

一般社団法人 東京福岡県人会 理事

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

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

前提

1. 個人の意見などであり、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. 個別事案では「機密に触れる」「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. 特定組織や政策など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、

みなさまの対策の一助になることを目的としています。

時代の流れと環境変化

第20回
白浜シンポジウム

20年目の2016年
サイバーセキュリティ

3 + 1

サイバー犯罪
金銭目的犯罪は多様化か？

金鉱脈発見の感
直接的と間接的
火事場泥棒

ランサムウェアなどへの対抗

1. 上場企業、行政機関など
   反社会的勢力へは利益供与しない。屈しない。決意しておく。
   株価操作に悪用されない。

2. 非上場企業
   こっそりと処置可能。
   病院/教育機関/公益団体など。
   仲介業者が活躍できるかも。

3. 個人
   流れ弾に当たらないように。
   クラウドの活用。

組織を守る観点ではクマ理論！

クマに狙われた場合、

クマを倒すことも、クマより早く走る必要もない。

標的型攻撃対策

流れ弾対策

でもクマのこと，もっと知りたくない？

クマは何処で出没してるの？
どんな被害にあったの？
どうやって助かったの？

さらに，別の目線も大切！

クマの被害を全体的に抑えたい。
クマとイノシシの関係は？
誰がクマを操り，どう組織化しているのか？

単に，組織を守る策は
見えて来てるが，その
高度化，捜査や抑制に
関し問題は山積み！

やることは沢山あるぞ！

さらに，サイバーテロ
多目的化も油断ならぬ

不正書き込み
火付盗賊
株価操作

時代の流れとしては

例えば, Bitcoin。

難しいことは置いておいて、

犯罪者にも、システムを支える機会を。

（そう狙ったかはわからないけど）

発想として、

「　　」は悪くない。

→ 21世紀型ビジネスモデルなのかもしれない。

Anyway

高度情報化社会は
高度な社会であり

であることは間違いなさそうである。

サイバーセキュリティの位置づけ

もうひとつ重要なこと

情報技術(IT)後進国ニッポン

正面突破は重要だけど、
考えなければならないことも
アルよ。

サイバーセキュリティ人材

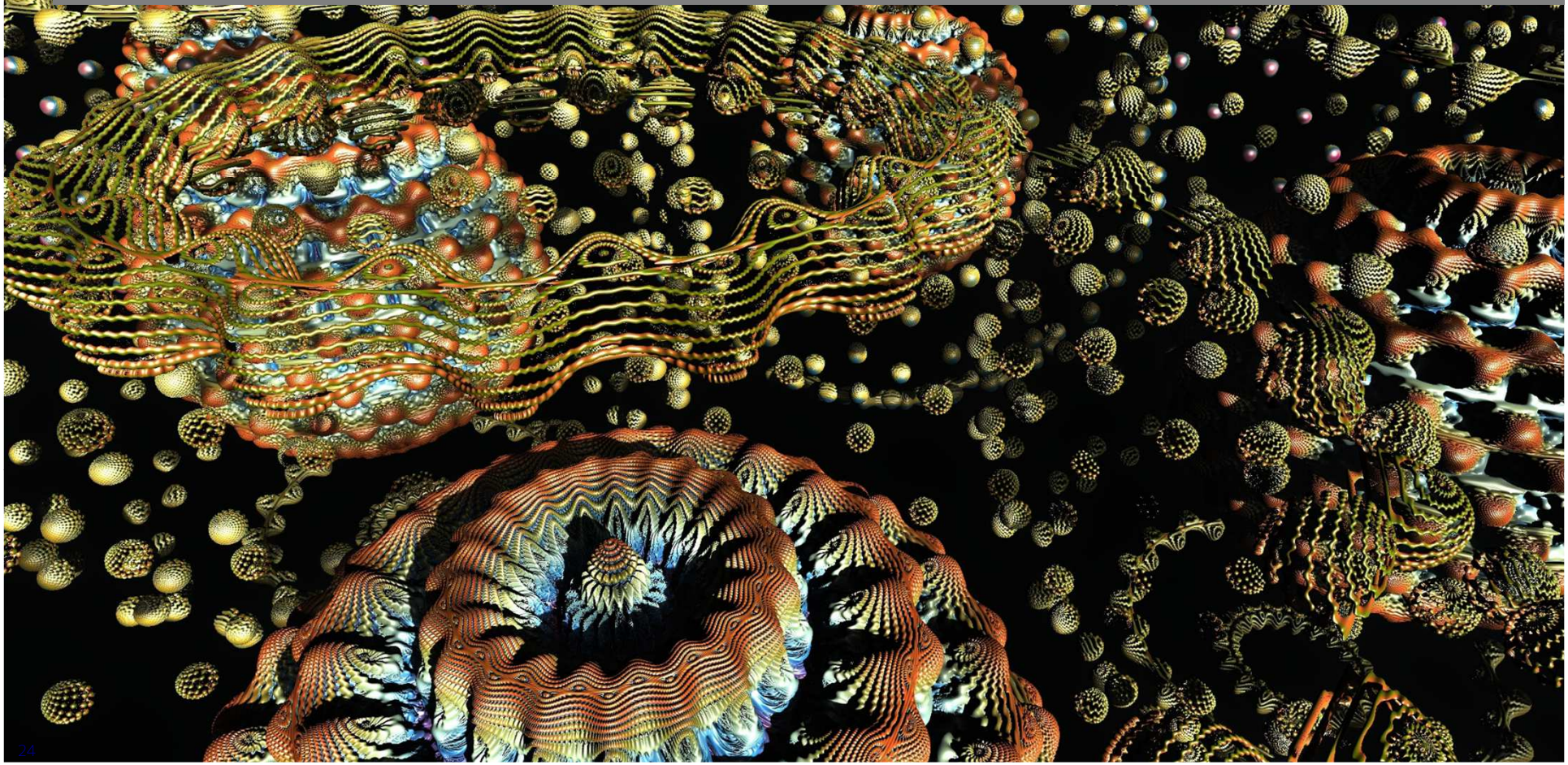
セキュリティ人材が足りないらしい。

セキュリティ人材のキャリアはどう考える？

政府の政策推進に関与
有名大手や行政機関などでのCISO, CSIRT経験
学術機関での教鞭や研究
捜査機関や国防機関での活躍

どうも,
暴く力を身に着けることが,
重要そうだぞ。

使われているコードを暴く



高度コード社会

そのコード,

基本はオープンソースらしい。

また,人が作っているらしい!

mjsk!?

著作権や脆弱性管理の観点
oss管理は非常に，
重要な位置を占める。
時代はIoT，チップにもossか？

また、あらゆるシステムや
「もの」に潜んでいるかもしれない,
仕込み, トラップ,
からくり, 時限爆弾, 仕込みなど

誰がやっているのか？

所謂、おれおれ詐欺での役割例

電話で騙す「①掛け子」に、管理する「②番頭」
現金を手にする「③出し子」や「④受け子」に「⑤見張り役」
「出し子」や「受け子」などの「⑥リクルーター」
携帯や口座などは「⑦道具屋」、犯行拠点は「⑧代行屋」
「⑨名簿屋」が有力対象者情報を提供する
さらに、
シナリオを準備する「⑩脚本家」や全体を仕切る「⑪監督」
主犯格として、
事業を仕切る「⑫胴元」と資金を提供し収益を得る「⑬投資家」
などがシステムとして機能していると言われている。

対抗側もシステムとして闘わないとダメなのは自明の理

さらに、見えづらいサイバー犯罪

さて、サイバー犯罪の相手

JC3での分析でも，
組織的に動いている
ことは見てとれる。

システムには，
システムで！
AIには，AIで！

相手を追い込むために

【ハンター・鑑識】
① 出し子ハンター
② ウイルスハンター（鑑識）
③ C2・Botnetハンター
④ プロファイル
アトリビューション など

【コーチ】
① ハンターコーチ
② 技術

※ CEC

【エンジニアリング】
① 分析・解析技術
② 分析・解析システム など

【編集・広報】
① POC
② 編集
③ PR・SR など

【マネジメント・スタッフ】
① チームリーダー・マネージャ
② 脅威分析
③ コーチングディレクター
④ 営業・スポンサー

相手を追い込むために

我々の得意分野をよく考慮して推進する必要がある。相手組織のプロファイルやアトリビューションには，協力国関係機関との密な協調が必須。

前向きな協力を引き出すためには，こちらから情報を出せないと話にならない。Give Give and Take!

日本独自で推進できる，コード解析(鑑識)は，中立性や品質面での立ち位置含め，
日本には合っているのではないか？


私たちが勝負できること

ところで, 次の20年を
考えてみたい。

中立かつ技術的に
淡々と全て暴く国

そのためには，産官学，
関係機関の連携が鍵を握る。

サイバーセキュリティの将来における産官学の使命を考えてみる。

【産業界】
① 事業継続に雇用と研究開発の継続
② 行動原則の相互理解と共有並びに意思決定 など

【政府や公的機関】
① 至る社会に向け, 我が国生き残りのための選択と集中投資(少々乱暴に!)
特に捜査や監査機関等の調査/解析能力の飛躍的向上とリーダーシップ
② サイバーセキュリティ人材流動化推進, 人材の継続雇用
③ 被害共有, 踏み台(犯罪基盤)の調査義務 など

【学校や研究機関】
① AI技術などのフォレンジック/コード解析への応用研究
② 囮踏み台など共同研究や踏み台(犯罪基盤)の調査義務 など

ラグビーでは，一発のタックルが
試合を変える。

日本は攻撃的防御が可能となる，
「暴く力」を徹底し，
世界に貢献する道はある。

要は火中のクリを
拾わないことには
黄金の国の復権はない。

May Shirahama be with you.

白浜と共にあらんことを

わたし

にし　もと　いつ　ろう
西本 逸郎　CISSP

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

ブログ どらいつ 検索
@dry2

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）

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 / CISO 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

一般社団法人 東京福岡県人会 理事

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

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

ご清聴、

ありがとうございました。

LAC ともに、イキル

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