2016年の振り返り

～ブラックセキュリティの認知から～

LAC
ともに、イキル

2016年12月2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

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
一般社団法人 セキュアドローン協議会 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

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


昨今の取り巻く環境のおさらいから

① 富山大学（水素同位体科学研究センター）標的型サイバー攻撃

1. 現場の少数
   → 現場対応
2. 事故対応
   → 被害拡大
   ウイル
3. 何が問題な
   → 一番足り
4. 経営層の関
   → 公開さ
5. 様々な事件
   → 常態化している予算削減要求や競争激化に辟易している？
   → 取扱い情報や関係者を軽く見ている(そうせざるを得ない)？

前提
1) 明らかにこの種の研究者、人脈、体制などが標的
2) 相手は国がバック或いは相当な組織

報告書からわかる事実
1) 通信ログの解析に２週間（調査対象期間は不明）
2) パソコン内の情報確認に1か月半（流出可能性把握？）
3) パソコンの詳細調査に2か月（恐らくはフォレンジック）

素朴な疑問
1) 一台の調査で済んだのは何故か？（普通は内部に拡散）
2) 関係機関への連絡が4か月後なのは何故か？
3) 被害でメールに言及してないのは何故か？

富山大学ホームページより

② 考察（推測）

【1台の調査で済んだのは何故か？】

→極めて重要なこと。通常は管理者権限が取られ, 内部に展開される。
つまり, 当該パソコンを操り, 他のパソコンを踏み台にして作業を行う。

1) 当該パソコンの管理方法

(1) Active Directory での → 一括管理 or not
(2) ローカルアドミン → 全部同じ or not

2) ネットワーク構成

ひょっとして多層ネットワークを構成(封じ込め)か？

3) 本当は気づいていない？

ゼロではないと思うが, ログ解析も実施, 見逃しの可能性は低い。
→ ネットワークフォレンジックは掛けたか？ ログ解析だけではあぶり出しは難しい。

③ 考察（推測）

【関係機関への連絡が4か月後なのは何故か？】

→ 本来被害拡大防止の観点から可能性の段階で共有すべき。

1) 本当は知らせていたが公式にはこういう表現になった
2) 関係機関がどこかわからなかった
3) 誤報となる可能性を排除するまで待った
4) 連絡の意識がなかった ← 誰が？どのレベルが？

【被害でメールに言及してないのは何故か？】

→ 基本, メールは全て持っていく。

1) 調べたがとても公開できるような内容ではなかった？
2) プライバシーに触れるので調査することができない？

④ 考察（推測）

【後、老婆心 気になること】

再発防止策 → セキュリティ強化の前にやるべきことがある。

(1) 自組織で全てのインシデント対応
根本的にインシデント対応を一組織だけでやり切るのは無理。
とはいえ, 個別に予算を計上するのも無駄。
みんなで利用できる環境整備が急務。誰がやるべきか？

(2) 予算に見合った事業展開
環境に合わせた運用コストや資源の配分ができないなら
利用をやめる, 事業を継続すべきかから考慮する必要がある。

要は, 多くの組織のセキュリティ対策は

我々は各個に磨いた竹やりで,
各個で国家レベルにに対抗！

何とか頑張れというのは, 要は
企業の論理。一時的にはあっても常態
化は無理。この意識を特にトップから
持つ必要あり。→「トップ」とはその手が打てる人。

何を事前準備しておくべきか？


その対策、
現場で拾っ
て良いの？

ところで,セキュリティ対策は

コスト？

それとも

投資？

ビジネス＋IT
http://www.sbbit.jp/article/cont1/32614

インターポール中谷氏
「セキュリティへ投資しないことがコストであり、リスクである」

サイバー犯罪はビジネスにとってだけでなく、国家や政府にとっても非常に大きな脅威となっている。IoT時代はサイバーセキュリティへ投資しないことこそがコストであり、リスクであるという認識が必要だ――そう指摘するのは、インターポール グローバルコンプレックス・フォー・イノベーション 総局長の中谷昇氏だ。サイバー犯罪に対処する国際機関の視点から、中谷氏が現在の国際的なサイバー犯罪の傾向と対策方法を解説する。

読売新聞 2016年9月30日

会計検査院指摘　政府の情報システム　通信履歴７割解析せず

それって投資？ いくら儲かるの？

コスト＝ 黙っていても発生

→ どれだけ削減できるか？ 現場責任

投資＝ やらなくても済む

→ やるかやらないか？ 経営責任

現場での継続が困難な課題には,
経営者のリーダシップが問われる。

逆に言えば, それが経営の優劣を
決めるのかもしれない。

ひょっとして,
IT運用は,うまくいってて当たり前

これを経営と言わなくて何という？
何も起きないなら社長は不要！
同じように,IT運用もリスクを
予見し手を打つことが必須。

だとすると,

ITを使用しなければよい！

組織は使わないようにしても
個人は違う。(現在の変革の本質)
個人環境でお仕事をするだけ。

そもそも,

お仕事をするにはその役割と責任に
あったスキルが必要。
読み書きそろばん, 電車に乗る
旅費の精算ができる,計画を立てる
自動車を運転する,電話を使う,

ちなみに,

セクハラ, パワハラ, サービス残業など
皆さんの会社では如何でしょうか？

現場で解決すべき課題ですか？
経営者が率先して取り組むべき？

経済産業省からの経営ガイドライン

2015年12月28日経済産業省より、経営ガイドラインが。

一丁目一番地で、経営上の問題だと定義された。

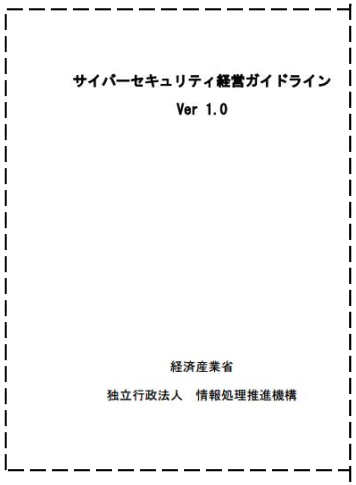
この問題を解決すべき課題かどうか決めるのは, 経営者。

ただ, 監督官庁からのガイドライン提示は

伝家の宝刀！

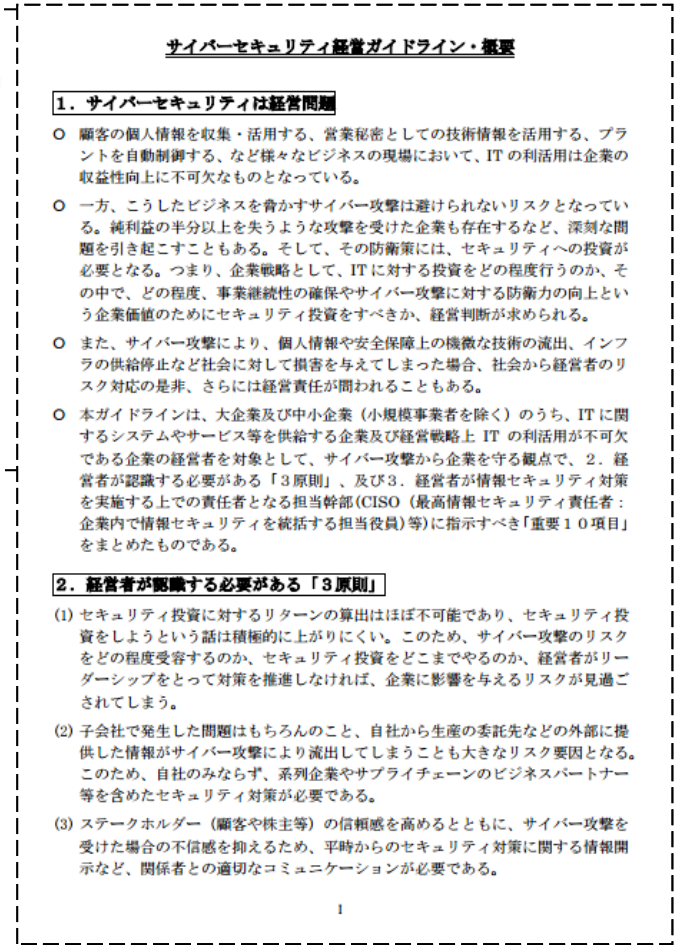
少なくとも全ての企業はよく読み, 趣旨を理解し, 基本姿勢を決める必要がある。

端的に言って やるかやらないか！の二択。



サイバーセキュリティ経営ガイドライン
Ver 1.0

経済産業省
独立行政法人　情報処理推進機構



サイバーセキュリティ経営ガイドライン・概要

1．サイバーセキュリティは経営問題

- 顧客の個人情報を収集・活用する、営業秘密としての技術情報を活用する、プラントを自動制御する、など様々なビジネスの現場において、IT の利活用は企業の収益性向上に不可欠なものとなっている。
- 一方、こうしたビジネスを脅かすサイバー攻撃は避けられないリスクとなっている。純利益の半分以上を失うような攻撃を受けた企業も存在するなど、深刻な問題を引き起こすこともある。そして、その防衛策には、セキュリティへの投資が必要となる。つまり、企業戦略として、IT に対する投資をどの程度行うのか、その中で、どの程度、事業継続性の確保やサイバー攻撃に対する防衛力の向上という企業価値のためにセキュリティ投資をすべきか、経営判断が求められる。
- また、サイバー攻撃により、個人情報や安全保障上の機微な技術の流出、インフラの供給停止など社会に対して損害を与えてしまった場合、社会から経営者のリスク対応の是非、さらには経営責任が問われることもある。
- 本ガイドラインは、大企業及び中小企業（小規模事業者を除く）のうち、IT に関するシステムやサービス等を供給する企業及び経営戦略上 IT の利活用が不可欠である企業の経営者を対象として、サイバー攻撃から企業を守る観点で、2．経営者が認識する必要がある「3 原則」、及び3．経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO（最高情報セキュリティ責任者：企業内で情報セキュリティを統括する担当役員）等）に指示すべき「重要１０項目」をまとめたものである。

2．経営者が認識する必要がある「3 原則」

(1) セキュリティ投資に対するリターンの算出はほぼ不可能であり、セキュリティ投資をしようという話は積極的に上がりにくい。このため、サイバー攻撃のリスクをどの程度受容するのか、セキュリティ投資をどこまでやるのか、経営者がリーダーシップをとって対策を推進しなければ、企業に影響を与えるリスクが見過ごされてしまう。

(2) 子会社で発生した問題はもちろんのこと、自社から生産の委託先などの外部に提供した情報がサイバー攻撃により流出してしまうことも大きなリスク要因となる。このため、自社のみならず、系列企業やサプライチェーンのビジネスパートナー等を含めたセキュリティ対策が必要である。

(3) ステークホルダー（顧客や株主等）の信頼感を高めるとともに、サイバー攻撃を受けた場合の不信感を抑えるため、平時からのセキュリティ対策に関する情報開示など、関係者との適切なコミュニケーションが必要である。

1

経済産業省からの経営ガイドライン

ざっくり言うと，CISOを配置し，
そして，CSIRTを構築せよ！
と，いうことかと

対策は，いつも通り！
取り敢えず任命し，
取り敢えず構築し、完了！

※ＣＩＳＯ（Chief Information Security Officerの略。「情報セキュリティ統括役員」）
※ＣＳＩＲＴ（Computer Security Incident Response Teamの略。「シーサート」）

経済産業省からの経営ガイドライン

さてさて，任命されたCISO，

ガイドラインを見て愕然！？

名ばかりで良かったのでは？

実施は，様々な内部/外部のキーマンや
組織との協力，連携などが欠かせない。

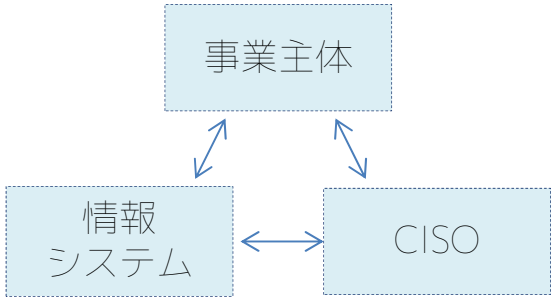
責任大きいし，やること沢山！

経済産業省からの経営ガイドライン

経営者が意識すべき三原則

1. リーダーシップを発揮せよ

→ 放っておくと誰もやらない。やる仕掛けが必要。
例えば、三権分立など。
事業主体 → 情報システム → CISO



2. 委託先など含め管理/制御せよ

→ 丸投げはだめよ！

3. いざに備えよ

→ 関係者との対話の道を開発しておくこと。
（安心はするな）

経営者が指示すべき重要10項目（CISOの仕事）

①セキュリティポリシーの策定
②CISOの任命と責任の明確化
③経営資産へのリスク把握と対応計画の策定
④PDCA実装とその実施報告並びに情報開示
⑤これを委託先など含め実施
⑥これらに対する予算と人的資源の確保
⑦ITシステム運用の自社と委託運用を分離。
　また、委託先も同様の対応をさせよ。
⑧社会的耐性強化に協力せよ
（情報を収集し、他へ共有せよ。CSIRT協議会）
⑨インシデント対応に備えよ
（CSIRTの整備と演習）
⑩被害発生に備えよ

CISOはどのレベルで動かなければならないかを爆速で判断し，関係キーマンや組織と連携し任務を遂行する。

その為，攻撃者と戦い忍者を探査するだけではなく，個人情報を扱うなどの危険な業務の中止や分離，関係者への注意喚起，お上への相談などの算段を行い駿足で手足を動かし問題解決を図るのがCSIRTである。

CISOとCSIRTのお仕事

CISOの責任の考え方

1) 適切な事故対応
   被害拡大防止と封じ込め
   → 全うして,初めて被害者になれる可能性が。
2) ルール違反のあるなし
   → 所謂,「割れ窓放置」は問答無用。
3) ルールは適正だったか
   要求されていることを知る
   → そんなこともやってなかったの？

事故そのものはCISOの責任ではない


茹で蛙現象
環境変化に気づかず,茹で上がってしまう
これはある面これで良いのかもしれない。

過冷却現象

順調に見えるが,
何かのきっかけで
全てが凍り付く

もう一点，学べることが！

早期に 渋滞を解消 するには？

基本的には前の車が動くのを確認して走り出す。

＝流体力学(情報の伝わり)

つまりは，反応が速い ほど渋滞は早く解消する。

ということは，様々なことを分解して
個々の基本動作速度を上げることは，
極めて重要なこと。→ 消防団の訓練

インテリジェントは鍵

茹でガエルに陥っていないか？ 過冷却現象が発生していないか？

常に目を光らせておく

CISOとCSIRTの重要任務。

次に、頑張りすぎないこと

目的は何かを考えて行動する。

頑張りすぎ自体が過冷却現象！

ところで, やっぱり罰則の強化！

信賞必罰のとらえ方。重過失は別として,

罰則でのセキュリティ維持は困難！

例えば, 標的型メール開封やウイルス感染など

基本的な考え方として, 例えば,

→ 個々の従業員 →

→ 管理職 →

もちろん, 部門によっては罰則でのマネジメントも必要だが、
一般的には, このあたりを起点として捉えないと極めて難しい。

最後に，社会的責任も考慮

自分さえよければ。→ [redacted] セキュリティ

対策には「情報」が重要なのは常識　みんな欲しい！

→ 接続先，痕跡の残り方，検体(ハッシュ，ブツ)，侵入手口(原因)など

あぶり出しや防御策へ展開

捜査機関やJPCERT/CCなどへの相談や連携

業界での連携 → 犯人は個別組織より案外業界を？

自助／共助／公助で [redacted] を

みんなで考えることは，
であることに気づき

この**共助**が機能する
仕掛けづくり！

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