最新のサイバー攻撃状況と今後の対応

～破壊的環境変化を楽しむ人材育成でリードしよう～

気づかなかったわけではなく

見えなかったのです。

LAC

ともに、イキル

2018年7月25日 株式会社ラック

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　西本 逸郎
売上高	連結 384億円 （2018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）

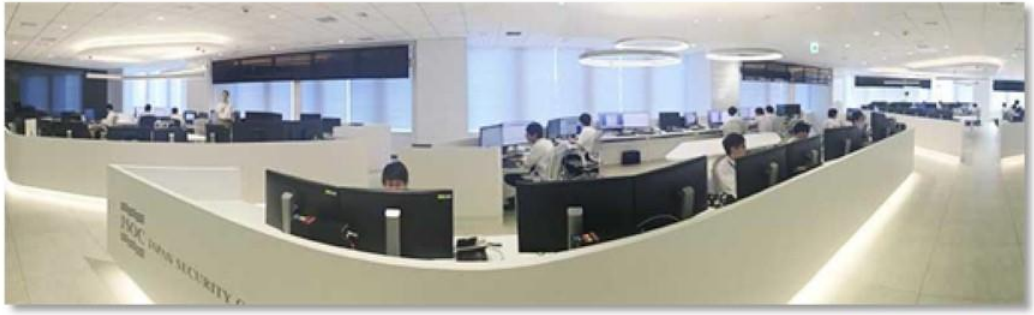
福岡事業所
〒812-0011　福岡市博多区博多駅前3-9-1
大賀博多駅前ビル5F

アクシス事業所
〒966-0902　喜多方市松山町村松字馬道上
3313-4

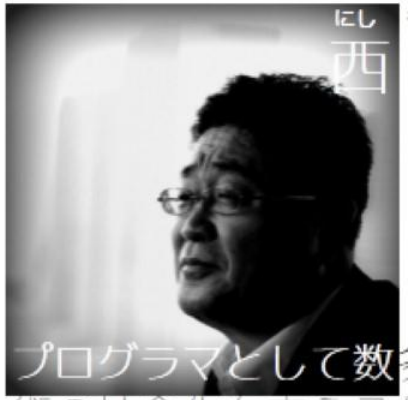
中部事業部
〒460-0002 愛知県名古屋市中区丸の内3-20-17 KDX桜通ビル16F

■ 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・沖縄ユニットの運用・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

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　三好崇司　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、サイバー戦略は「陸・海・空・宇宙」に続く第５の戦場として位置づけました。本書は、現在のサイバースペースを取り巻く現状を紹介し、世界各国や大企業の取り組みや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諜報術なのです。不正アクセス・どう防ぐ？」（日経新聞）

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　代表取締役社長

株式会社ブロードバンドタワー 社外取締役
一般社団法人 セキュリティキャンプ協議会 代表理事 会長
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
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

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 歴任

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

現状のおさらい

情報セキュリティやサイバーセキュリティ

（プライバシーマーク取得）

セキュリティ対策＝個人情報漏洩対策

と、思っていませんか？

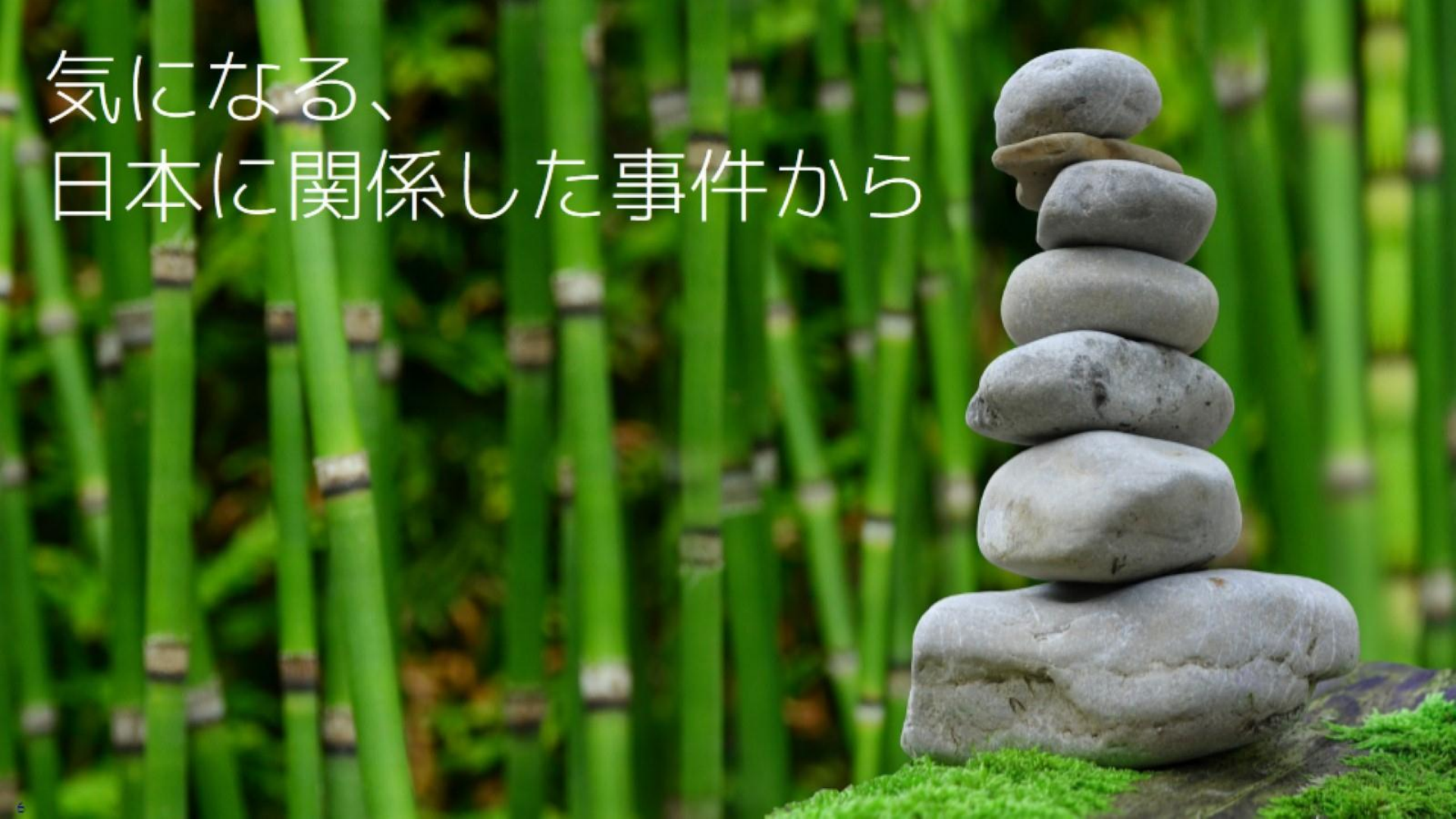
情報セキュリティやサイバーセキュリティ

また, 個人情報漏洩対策は
何故やるのでしょうか？

これが, これまでの常識かと思います。

ところが状況が一変しつつあります。

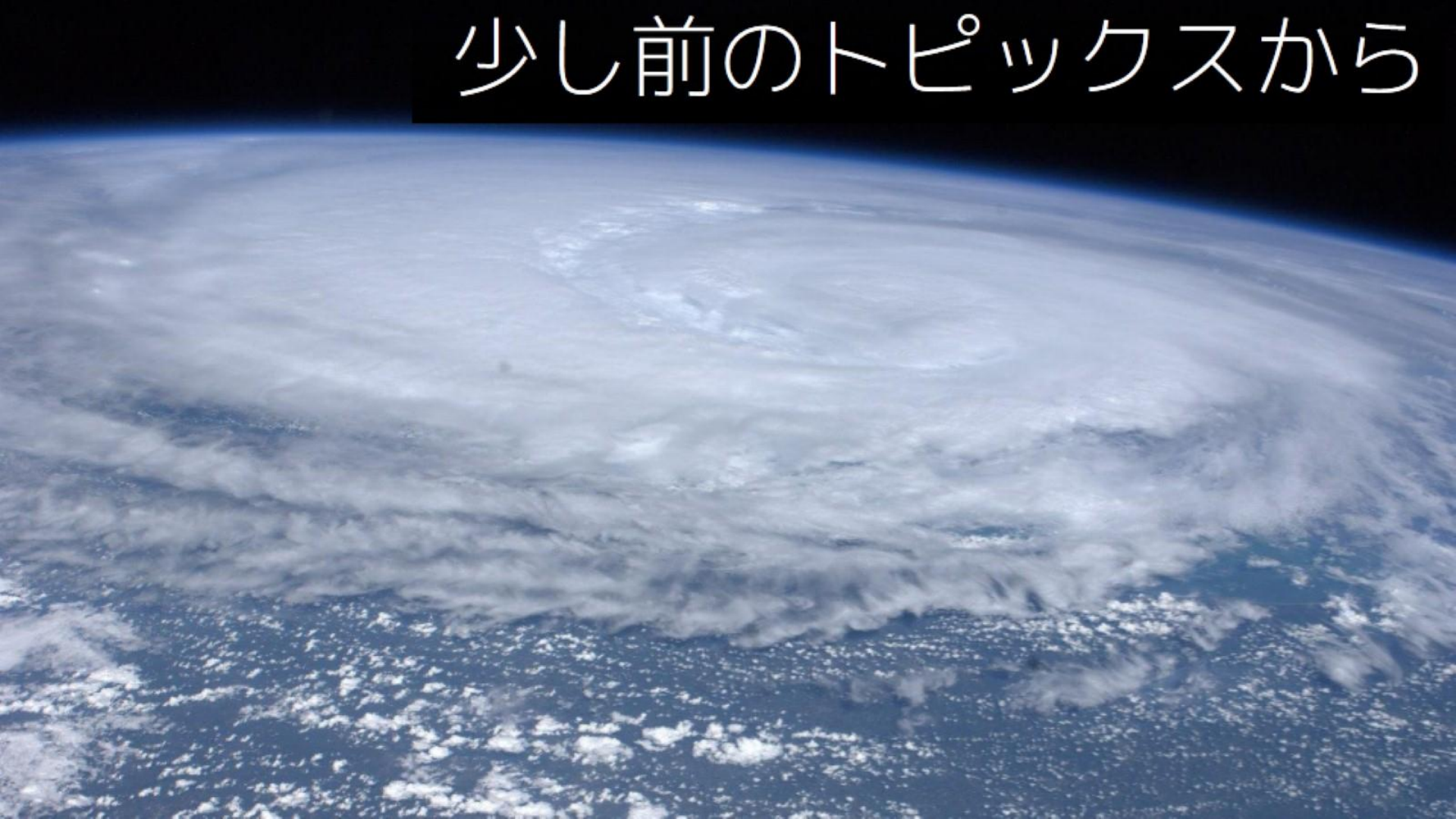
気になる、
日本に関係した事件から



日本での教訓

ロシアでの教訓

少し前のトピックスから



古い話で恐縮ですが、

Not WannaCry!

本日は，昨年有名となった
ワナクライではなく

Not Petya

本日は, ノットペトヤ（ペトヤ, ゴールデンアイなど）のお話から。

2017年6月27日 欧州を中心に大規模なサイバー攻撃発生。多数の組織で業務に支障が出るなどの深刻な被害が。

→ Petya or NotPetyaなどと呼ばれるマルウェアの仕業。身代金要求を行う。

侵入手口：会計ソフトのアップデータにより侵入

→ 管理者権限の乗っ取りと機器の脆弱性を通じて組織内へ浸透拡散

行動：機器の論理的破壊

→ 社内のITが全滅、若しくは大打撃。← 従来は潜んで盗聴など

北欧の海運大手マースク社では4千台のサーバと4万5千台のPCが全滅。

当初復旧には半年はかかると言われたが、恐らくは奮闘によりシステム復旧まで10日程度で完了し，停止に伴う事業縮小は20%で済ませ、残りの80%は手作業でこなしたらしい。

← それでも、システム全停止は10日間。システムの80%を手作業でこなせるって？

⇒侵入手口と内部機器破壊はデジャブ。

→ 過去には韓国の放送局や銀行で。

ランサムウェア（身代金要求）を装っているが，偽装であり，破壊目的とみられている。⇒ 米国などはロシアの仕業と見立て。

ランサムウェアの類型は？

① 純然たるビジネス(笑)
② スパイの隠れ蓑(証拠隠滅)
③ 破壊目的の隠れ蓑(所謂テロ)
④ その他

これにより，対応や騒ぎ方も異なる。

どんなものが破壊(人質に)？

① データや機能

1) かけがえのないデータ(個人)
2) 事業場のバイタルデータ(経理財務など)
3) 知的財産などの重要資産
4) 信用や個人の機微に係るプライバシー情報
5) プログラムやシステムなどの機能
6) 仮想通貨などの金融資産
7) 医療情報などの人命関わる情報

② プロセスやオペレーション

1) 操作IDや端末などの業務プロセスを構成する要素
2) 特権管理や運用管理を行うIDや端末などの要素

③ 装置や工場、オフィスなどの設備

④ 社会インフラサービス など

電力、情報通信、金融とクレジット等決済、航空・鉄道・物流 、行政、医療、水道、石油・化学・ガス

つながる時代
今後、びっくりするものが人質になる可能性がある。

IT基盤上に構築された世界

IT基盤の崩壊が即事業崩壊、社会サービスの停止などにつながりかねない。

ある面、機密情報漏洩よりIT基盤喪失ほうがより喫緊の課題で待ったなしであるという現実も見えてきてしまったのかも。

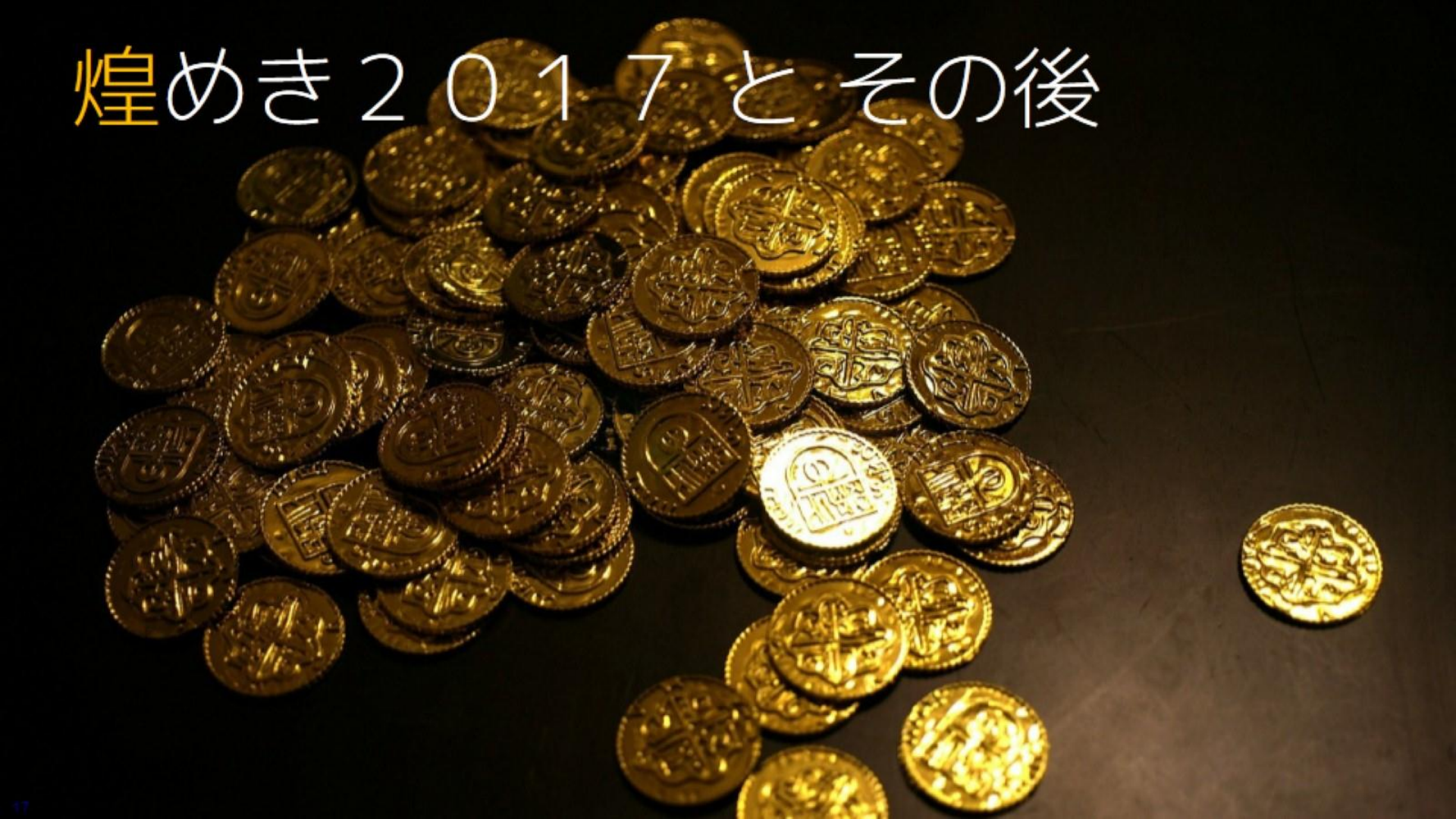
今後のIT依存前提社会においての喫緊の課題かと。

① 喪失しない対策
② 喪失しても大丈夫な対策
③ 完全喪失はしにくい対策

どれも外せない

社会的責任や影響などを分析し，決断。

煌めき２０１７とその後



少々，古い話で恐縮です

この「煌めき」のような一連の騒動 → déjà-vu

法の未整備や隙間をついて一世風靡
→ 法規制

「金融庁」が報告命令、改善命令、立入調査

業者側の意識
→ あくまでもIT(FinTech)のスタートアップ

取り扱い資産価値の激変から

これは特殊なケースかもしれないが, 様々なサービスなども同様に考える必要がある。

① システムが支えなければならない資産価値
② システムが及ぼすサプライチェイン上の責任
③ システムが及ぼす社会的責任
　上記は刻々と変化する。

アジャイルや永遠のベータ時代で押さえるべき策
SoE(システム連携・つながる社会)による影響

さて，世界ではこの分野
中国をはじめ禁止している国も多い。

その中、我が国では、

①ビットコインの法的な扱いについて閣議決定

→ 2014年3月7日，ビットコインの法的な扱いについての質問への回答書というかたち

② 法改正の実施

→ 仮想通貨は貨幣の機能をもつと金融庁が認め国会で法改正、よって、民間銀行によるビットコインの扱り扱いなどが可能になった。(改正資金決済法や改正銀行法)

日本は珍しく世界でも先行していると言って良い
グレーな存在ではない。正規に取り扱える。

これは
チャンスじゃない！？

ふと，周りを見渡してみると

昨今の話題

IoT, AI, Connected Industry, 働き方改革等

⇒ Society 5.0

要は, 何でもつながる世界・社会

消費者, 店舗, 卸, 工場, 建設, 農業,漁業, 行政などがつながる社会

らしい。

一部は, 既に始まっている。

要は、
デジタル・トランスフォーメーション

Digital Transformation → デジタルへ変換？

⇒ う〜ん。ピンとこないです。(笑)

デジタルへの変身！

⇒ こちらのほうがベタでイメージしやすいかも。

（Dive to Digital でも良いかも？）

そういえば、

最近の, 某国のDigital Transformation
すごいと思いませんか？

→ デジタル機器などの製造技術に留まらず決済システムや
様々なシェアサービスなどの黎明

また世界の時価総額ランキングをみると

→ トップテンでは米国７社に中国３社

これは逆に考えれば、サイバー攻撃を受けやすい国
トップ２ということかもしれない。

某国のデジタル・トランスフォーメーションの狙い？

経済力強化（ITを基軸にした経済による圧倒）ができるのも，
ITを活用した国の統治システムが完成したと考えるべきでは？
→ 足元を固めたからこそ，大胆なDigital Transformationをかけてきたのではないか？

つまり，(攻撃力を含んだ)サイバー防衛力が，経済や成長力を支える源泉になっていることだと考えられる。

今後、IT活用と統治（防衛力）システムのセットで，世界での影響範囲の拡大を図っていくのかもしれない。

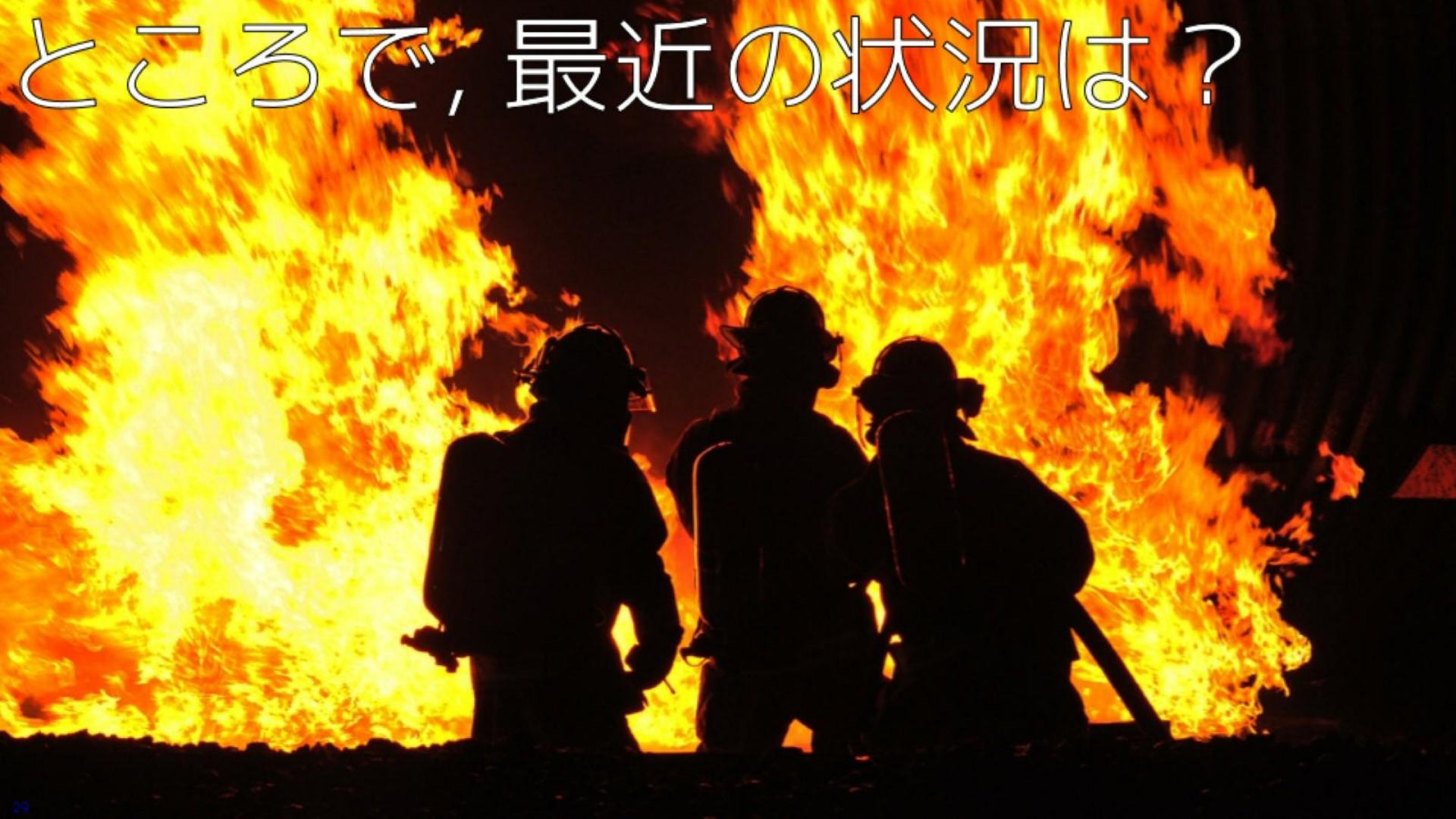
という中で，先日，
某国はICO，仮想通貨の
採掘や取引などを禁止へ。

ということは,

この分野に関して, 未だ統治できてない
ということの証左？

今後、統治可能にして
戻ってくるのだろう。

ところで，最近の状況は？



金銭目的系は？

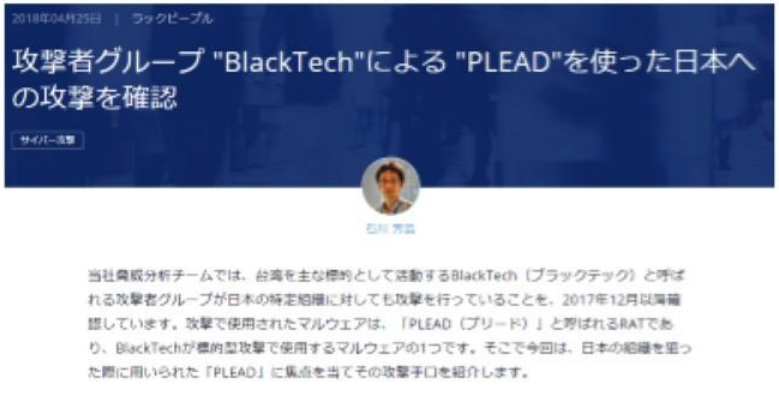
犯罪者側の生き残り(？)のためには,
費用対効果とリスク軽減策を念頭に収益モデルを発掘し, 手口開発し続ける必要がある。

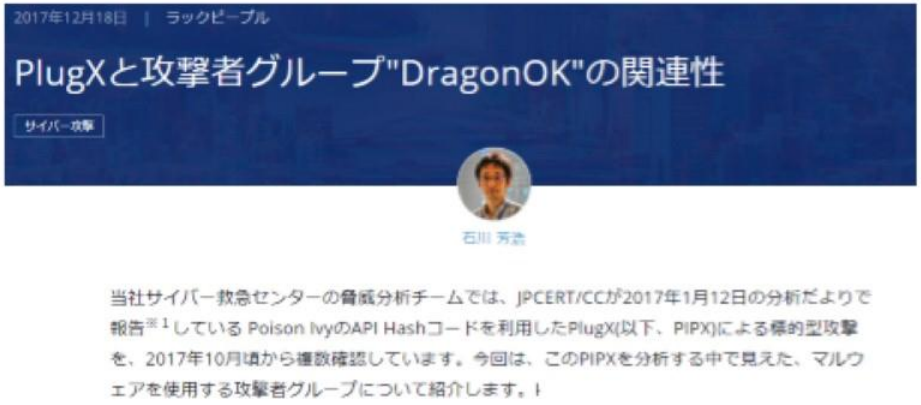
その為,

身代金要求や銀行などの不正送金などの手口より,

仮想通貨周りがブーム。

一方，スパイ系は？





某国 や 某国 或いは 某国辺りと推測される攻撃は，世界情勢などとは関係なく，日常的なルーティンとして継続している。

→ 警戒してないのは.

もう一点重要なこと

スパイは、

→ 指先ひとつで破壊者に変貌可能！

破壊者となったスパイは，「クリフエッジ※」を超えているという認識が必須。

→ 現状では「侵入が前提」である。

→ 多くの多重防御は意味がない？

※ 想定外の事案などで、多重の安全装置が機能停止し代替え機能も働かないなど致命的な状態に陥る事象
→ 例：内部犯行は想定していない

基本的な考え

① 日本の格言「つなみてんでんこ」

→ 自律 分散 協調
　いざの見極め、継続させる範囲とその手段
→ クリフエッジを知る (こう来たらヤバい)

② 過冷却状態※の見極め

→ 責任者(CISO?)の重要ミッション

※ 様々な環境変化により、当初想定の対策が効かなくなっている状態
　攻撃内容の変化、守るべき資産価値の変化、社会的な影響度の変化など

まとめ

① 一般的に, これまでは「情報漏えい」のみを意識。(Cia)

直接消費者と接するBtoCビジネスでもなければ,
→ セキュリティ対策≒個人情報漏洩対策≒Pマークで完了。

② 昨今は情報漏えい以上に, 「IT基盤喪失」の想定が必須。(AIc)

事業継続に直結する経営課題として,
→ サイバーセキュリティへの取り組みを。
※ 個人情報漏えいを重要視していた理由は事業継続に直結するからに他ならない。

IT基盤が合理化/生産性向上の道具から,
知らない間に実は「事業基盤に進化」していることもある。

人材育成に関して

厳しい指導や地獄のプロジェクト経験が当たり前の世代

現代社会でどうすれば良いのか？

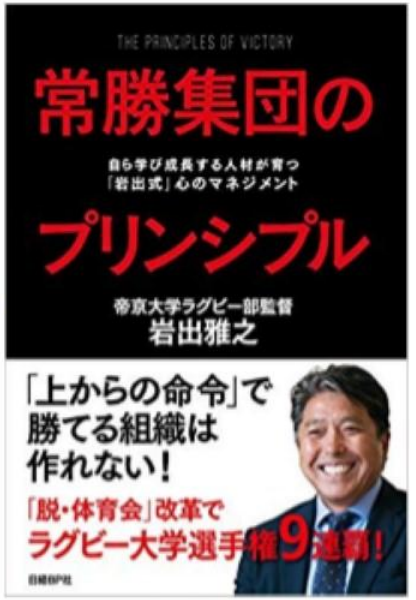
勉強せえ！限界まで働いてみろ！
などとは口が裂けても言えない時代
→ ブラック、関係法規、働き方改革

人材育成に関して

私自身の経験則では難しい。

私で言えているのは, 火事場が好き。

さて, 帝京大学ラグビー部
岩出監督が面白い →→→→



人材育成に関して（私流の解釈）

好きなことに没頭できる環境づくり

→ 好きになる仕組みづくり

→ 組織や先輩社員の好感度

→ 共感と誠実さ ⇒ 人柄

→ 考え方 × 笑顔 × 聞く力

→ 信頼度 ＝ 能力 × 人柄

※岩出監督の講演メモ
（本人未承諾）
（私の勝手な理解）

会社の業績やプロジェクトの完遂は手段

→目的は？

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
https://www.lac.co.jp/
sales@lac.co.jp