2015/12 ITソリューション塾

Security and Governance

株式会社アスタリスク・リサーチ
Executive Researcher 岡田良太郎
質問・感想・相談は： riotaro@rsrch.jp

岡田良太郎 / Riotaro OKADA

risk researcher

https://jp.linkedin.com/in/riotaro
https://www.facebook.com/riotaro.okada
Twitter: @okdt

The Local Leader of Global Security Community

The Organizer of Expert Competition Hardening Business Security

One of Facilitator of Disaster recovery Community

Entrepreneur focusing on the Software Risk Control

OWASP JAPAN

Hardening Project

情報支援レスキュー隊 DART Disaster Assistance Response Team

Asterisk Research, Inc.

Our Core Service

https://www.asteriskresearch.com

Riotaro OKADA
Executive Researcher
CISA, MBA

riotaro@rsrch.jp
ご相談ください

1. セキュリティ・トレーニング、アドバイザサービス
   （一般社員、エキスパート、経営・管理職対応）

2. ビルトイン・セキュリティ・ソリューション提供
   （セキュア開発ツール、セキュリティ・テストを提供）

3. セキュリティ・マネジメントサービス
   （アウトソーシング）

公共・実績

- 「教養としてのサイバーセキュリティ」担当（BBT大学）
- セキュリティキャンプ インストラクタ (経済産業省)
- 政府IT担当者向けサイバー演習 CYDER 委員（総務省）
- マレーシア政府セキュリティイニシアチブ教育インストラクタ（外務省, 2015）
- 自治体IT調達調査、災害支援サイト調査 (IPA, 2006-2013)

Agenda? 今日、何を知りたいですか？
塾長からのメールより

1. 「セキュリティ対策」という言葉があるが、そもそも何をすることなのでしょうか。
   その目的と具体的な対策について説明して下さい。

2. セキュリティとガバナンスは、どんな関係にあるのでしょうか。

3. IoTやスマートフォン、ウエアラブルなど、私たちの生活やビジネスの身近にITデバイスが存在する時代となりました。

   このような時代のセキュリティ対策は、これまでのITセキュリティのあり方をどのように変えて行く必要があるのでしょうか。

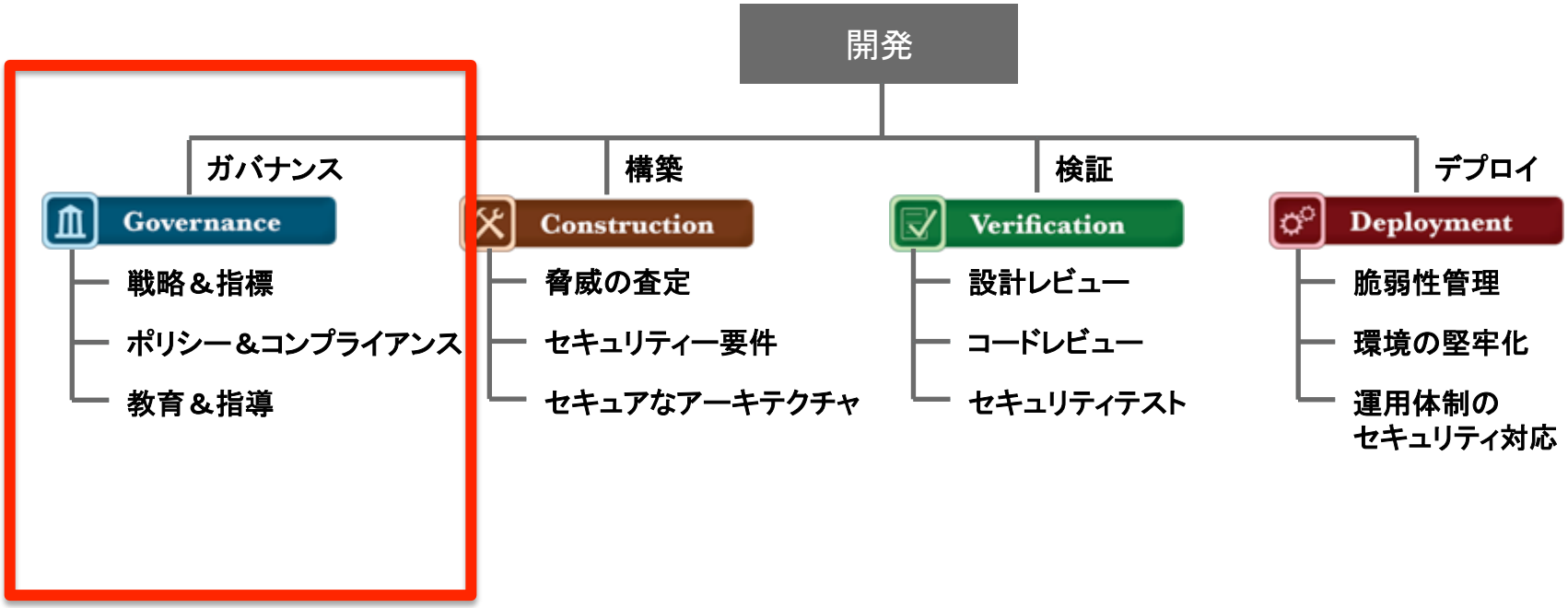
   何が変わらないかも合わせて、説明して下さい。

ガバナンス

情報セキュリティが保たれている状態を維持する仕組みをつくること。

OpenSAMMの全体像

ビジネス機能と各フェーズでのセキュリティ対策：

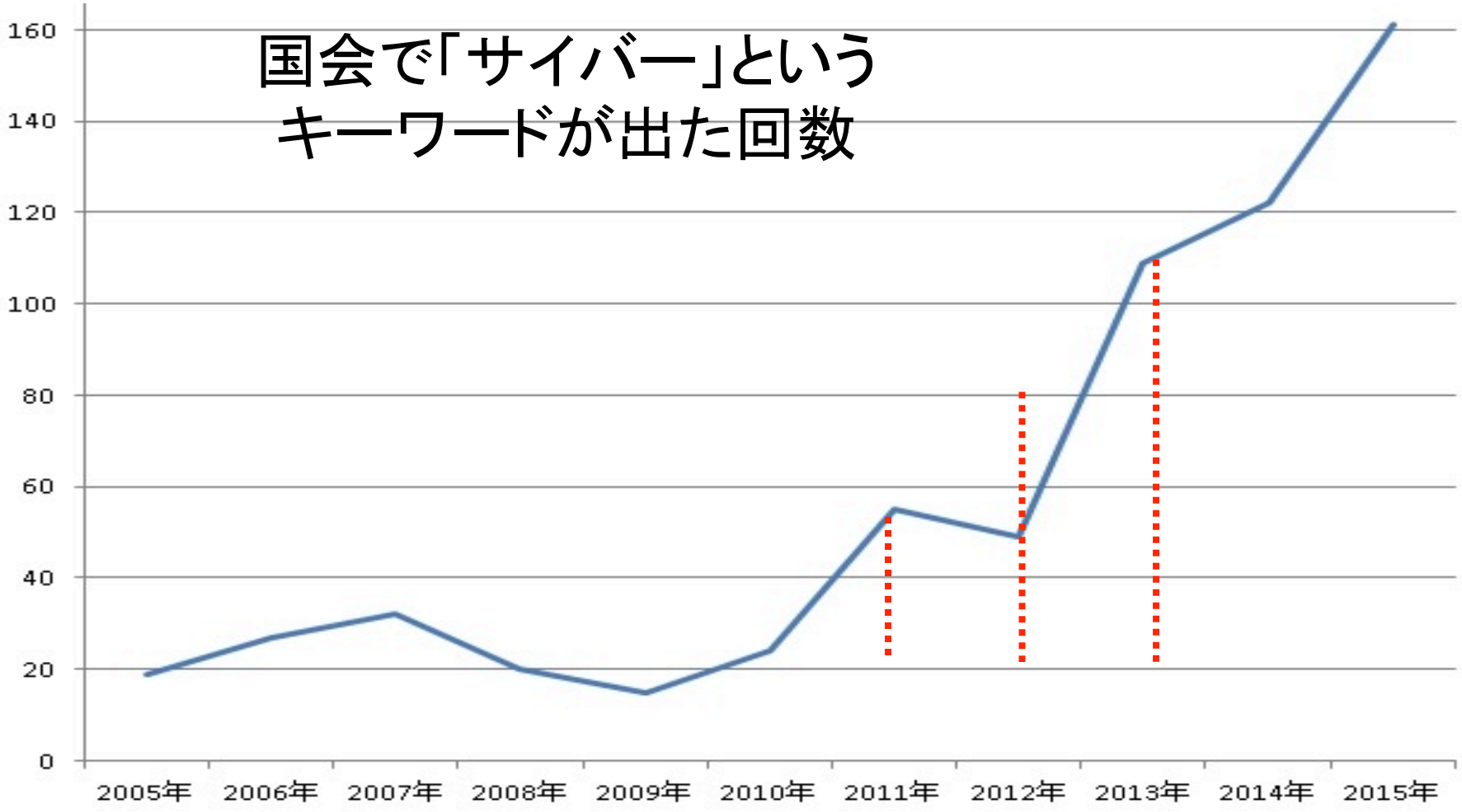


agenda

- サイバーセキュリテイの挑戦
- サイバーリスク
- セキュリティの基本のき
- リスク･コントロールの実際
- おまけ

サイバーセキュリティの挑戦

これは何でしょう？



Cyberspace

- Cybernetics (サイバネティクス)
  - 数学者Norbert Wienerが提唱:
    - 通信・制御・生物学などを統合した学問の名前。フィードバックに着目した。

サイバースペースでの出来事を考える時、
The Netに特化するものとしてではなく、
そのフィードバックとして起きるリアルの事象や
連動する仕組みをとらえる。

サイバー空間への「入口」

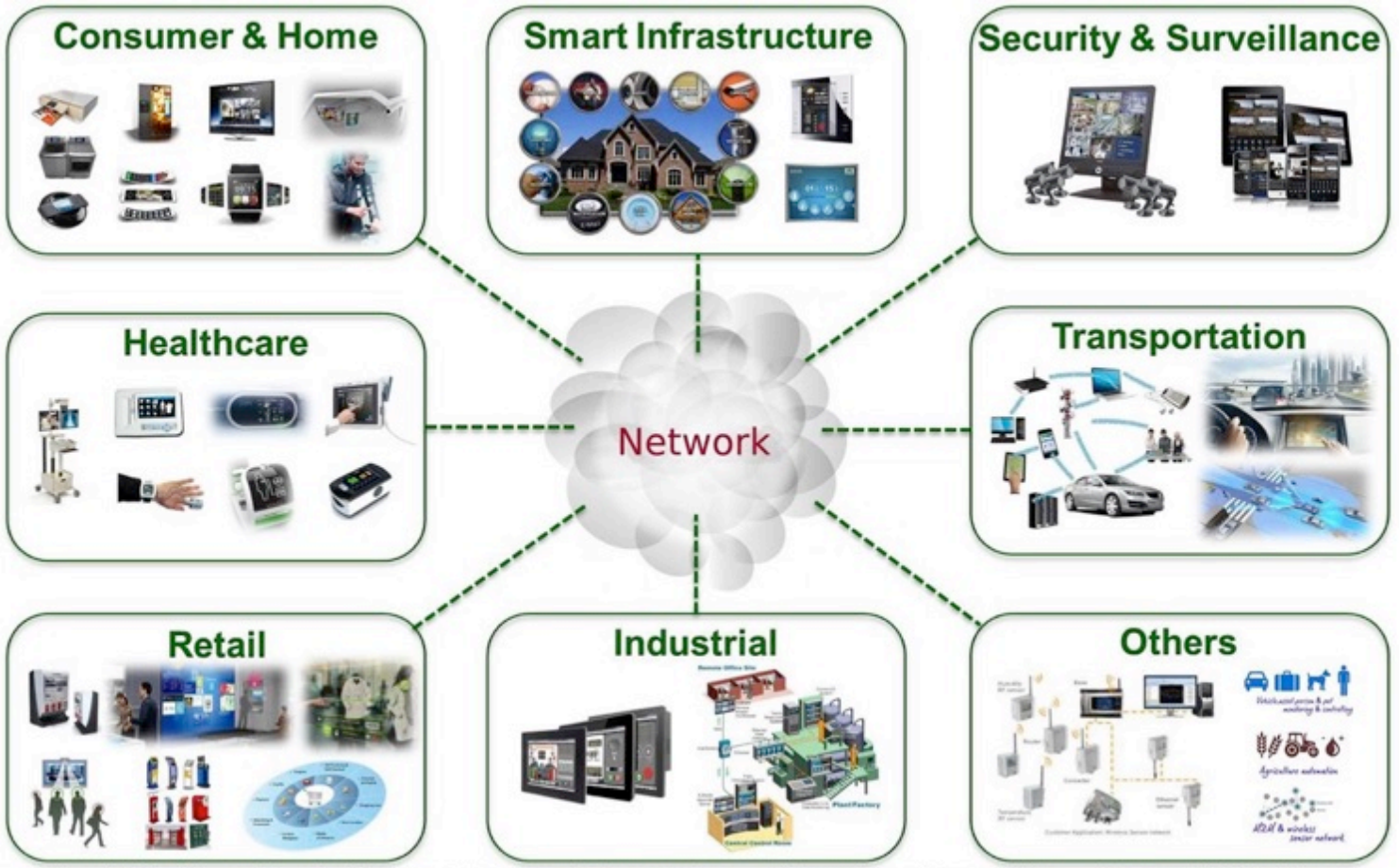
- パソコン・ノートパソコン
- タブレット
- スマートフォン
- スマートウォッチ

ハブとしてのスマートフォン

- カメラ･マイク
- GPSセンサー
- ジャイロセンサー
- 加速度センサー
- 照度センサー
- 近傍センサー
- 圧力センサー
- 温度センサー
- …

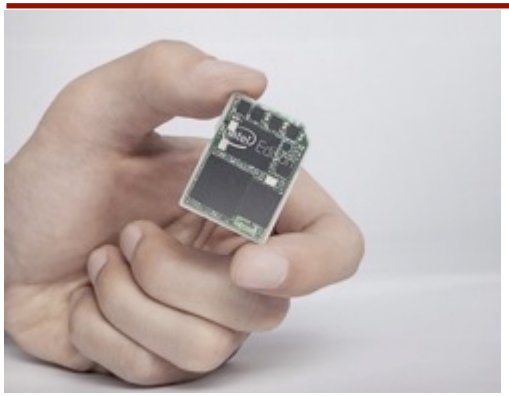
“IoT” = Internet Of Things

モノが直接インターネットにつながる



Intel Edison SD Card size PC

数百円で実現できる時代が目前。コスト破壊がイネーブラに

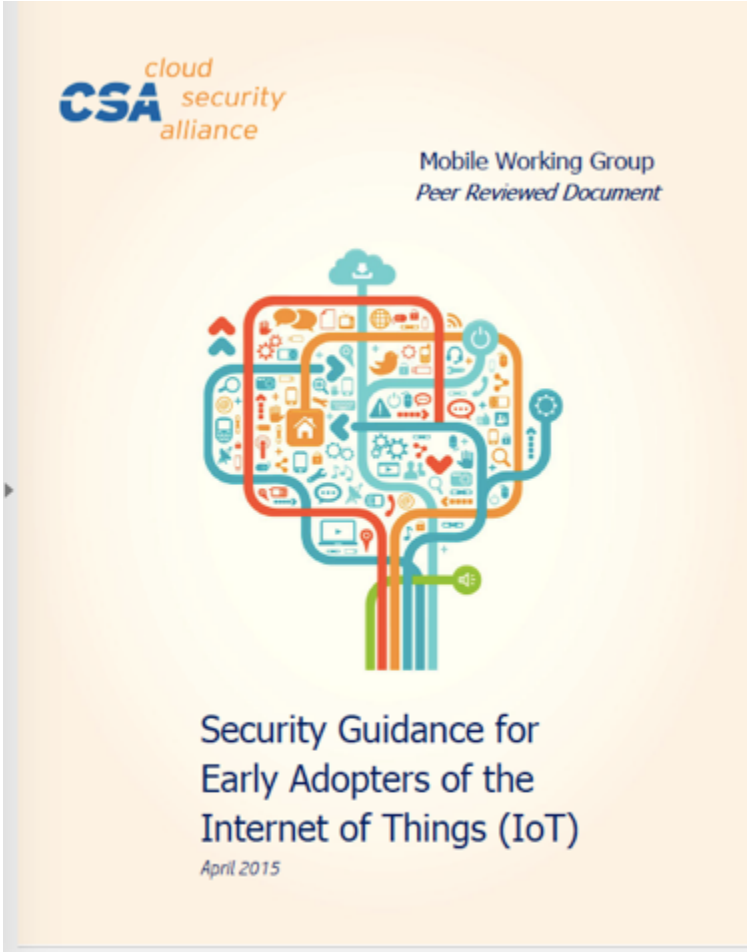


- Bluetooth/LE
- Wi-Fi
- Dual Core IA
- 24x32x2.1mm
- 22nm 500MHz
- Linux
- 1GB RAM
- 4GB storage

“パソコンやスマートデバイスだけではなく、コーヒーメーカーや椅子もネットに接続できるマシンになります。.”

http://www.intel.com/content/www/us/en/do-it-yourself/edison.html

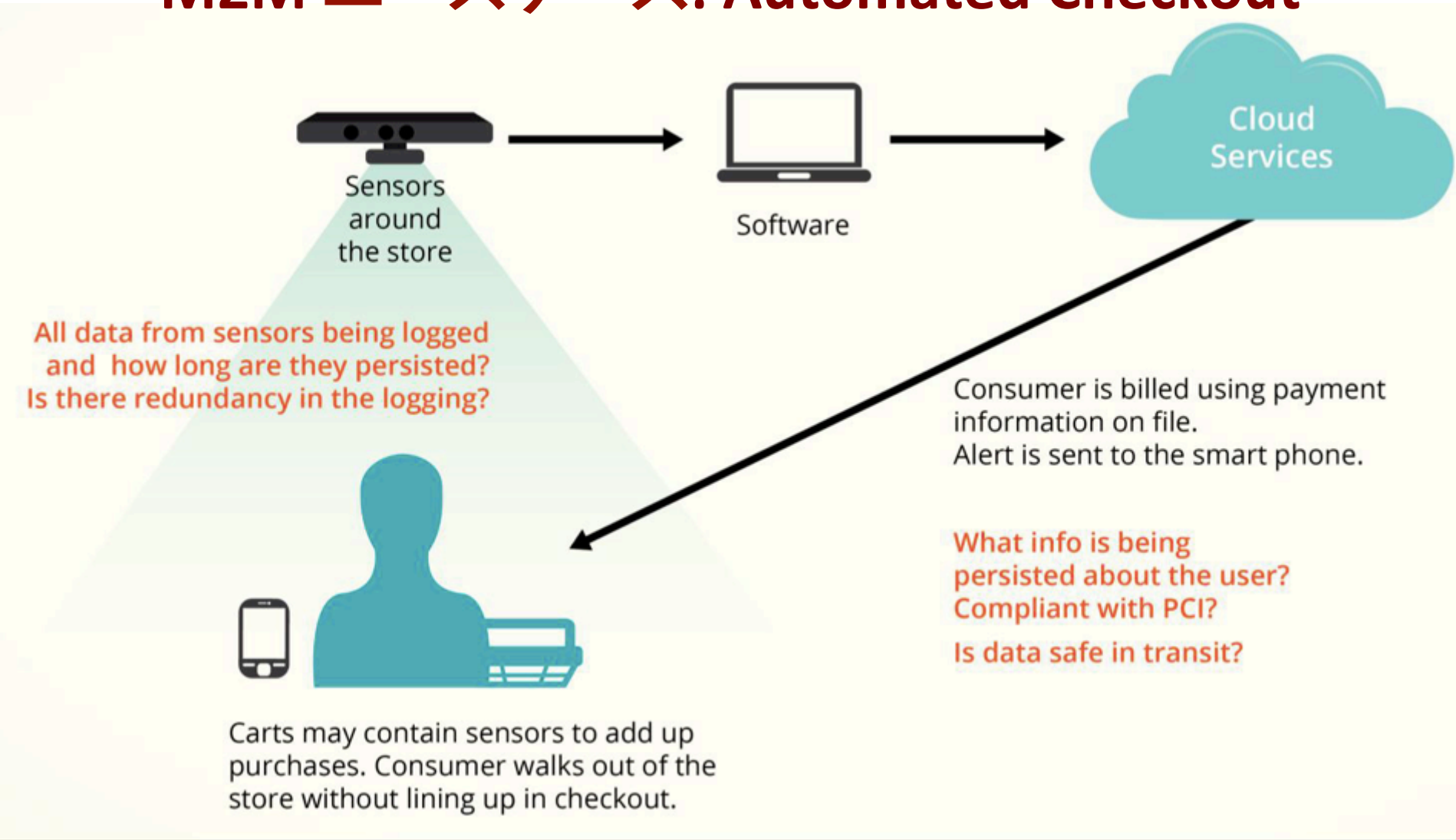
Security Guidance for Early Adopters of the IoT



- Secure by default
- Privacy by default

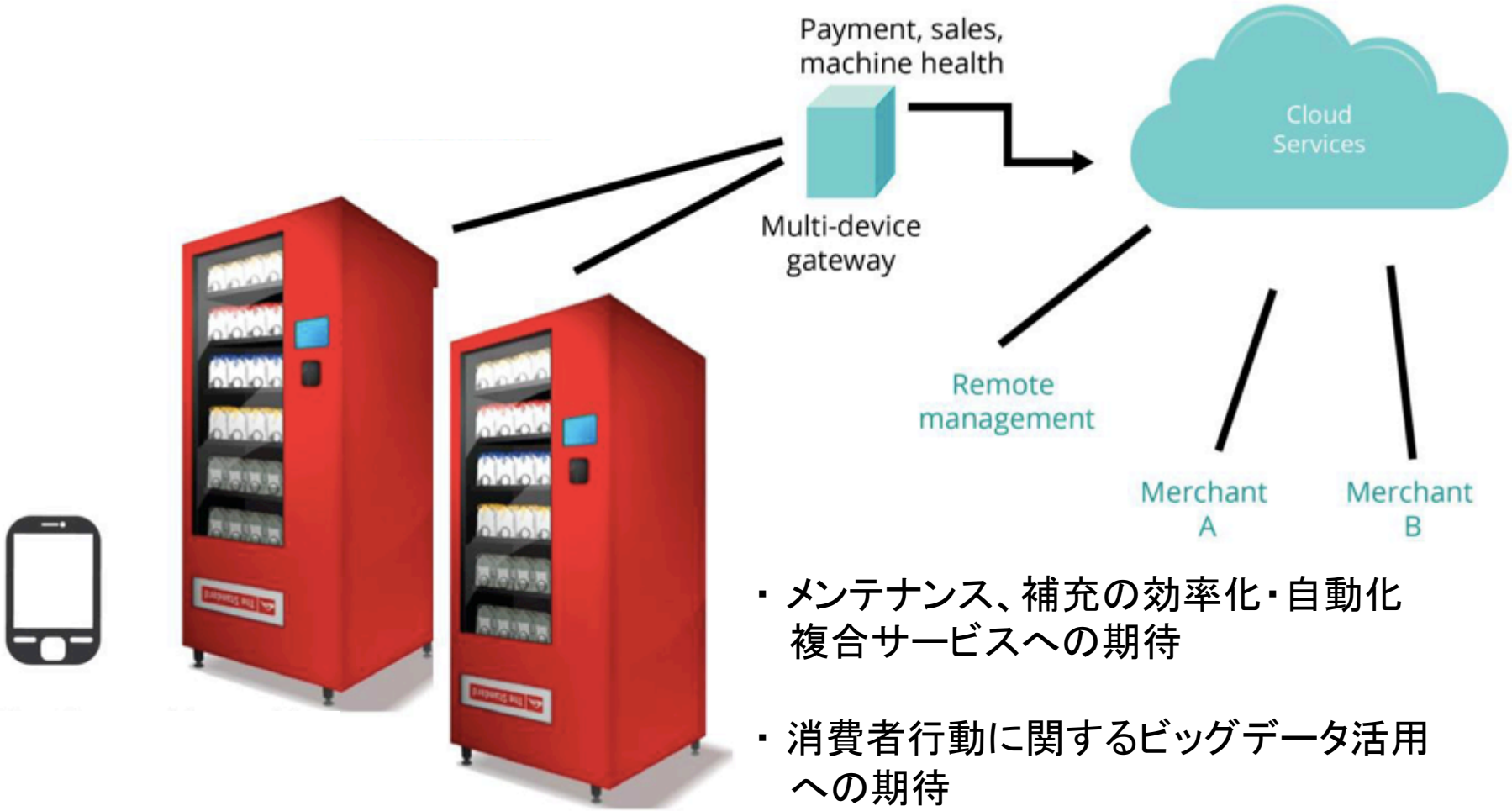
CSA Alliance Security Guide for Early Adopters of IoT
https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

M2M ユースケース: Automated Checkout



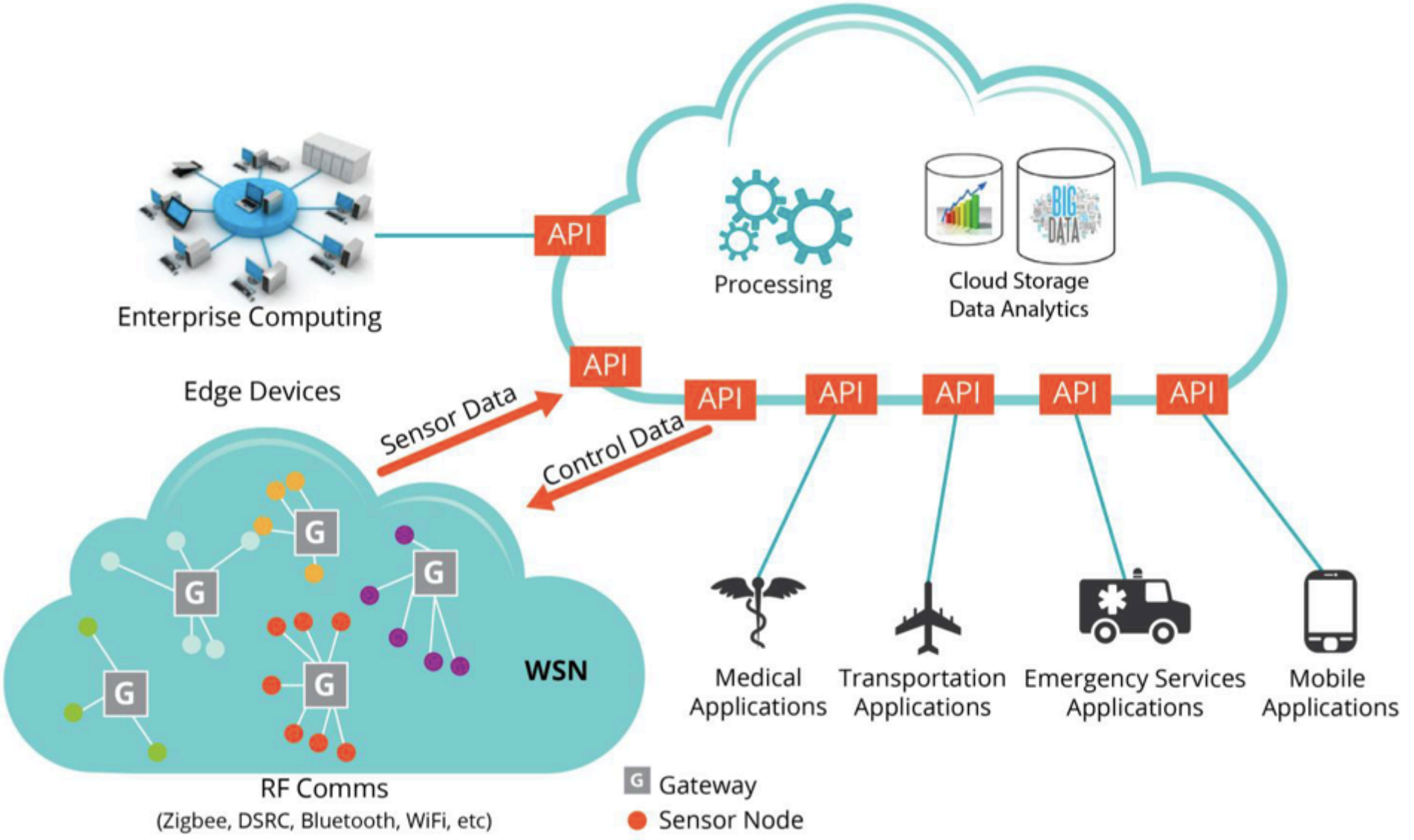
CSA Alliance Security Guide for Early Adopters of IoT
https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

M2M ユースケース: スマート自動販売機



- メンテナンス、補充の効率化・自動化 複合サービスへの期待
- 消費者行動に関するビッグデータ活用への期待

CSA Alliance Security Guide for Early Adopters of IoT
https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf



CSA Alliance Security Guide for Early Adopters of IoT
https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

Privacy-by-Design Principals

- Proactive not Reactive:
  Preventive not Remedial
- Privacy as the default
  - and
    - Privacy Embedded
    - Full Functionality
    - End-to-end Security
    - Visibility and Transparency
    - Respect for User Privacy
    - Privacy Impact Assessment

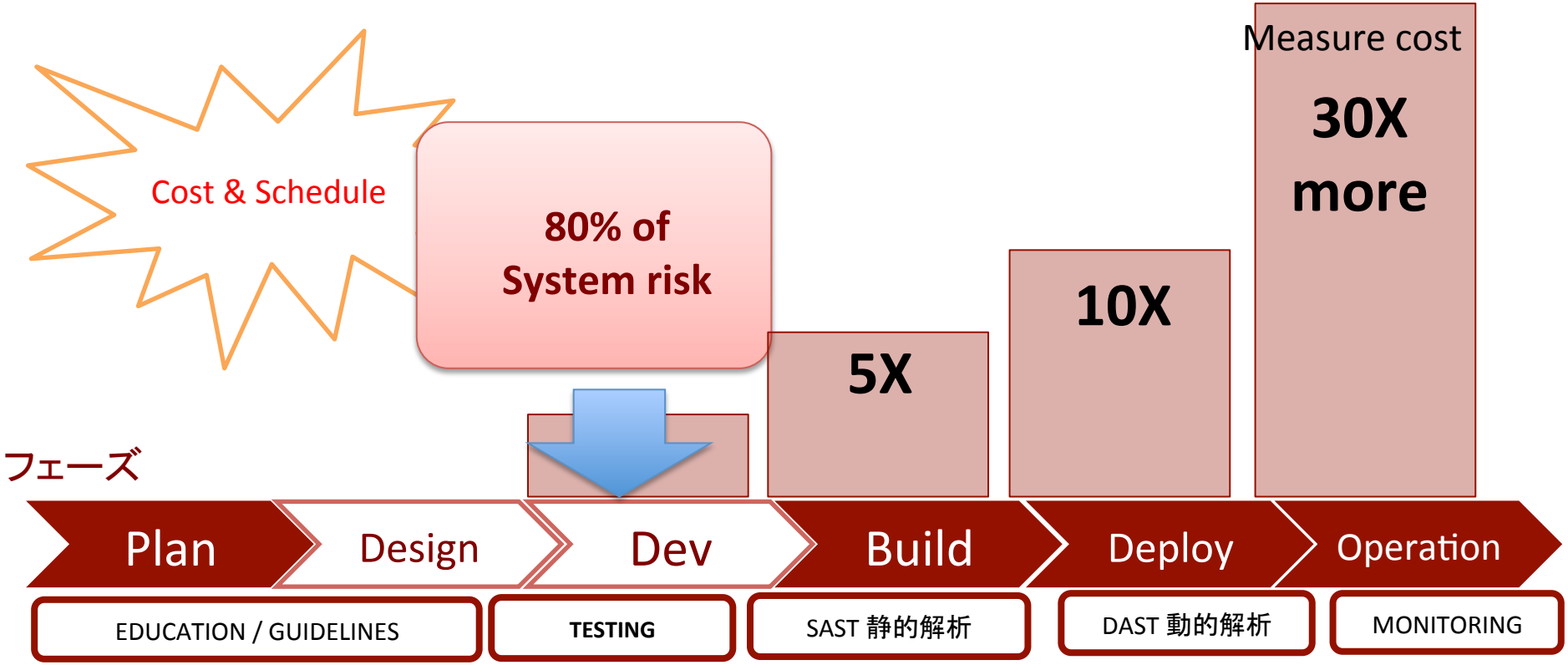
CSA Alliance Security Guide for Early Adopters of IoT
https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

OWASP Internet of Things Top 10

I1 安全でないウェブインターフェース
I2 欠陥のある認証・認可機構
I3 安全でないネットワークサービス
I4 通信路の暗号化の欠如
I5 プライバシー
I6 安全でないクラウドインターフェース
I7 弱いモバイルインターフェース
I8 設定の不備
I9 ソフトウェア・ファームウェアの問題
I10 物理的な問題

https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

開発時における対策の必要は大きい。
プロアクティブなアプローチは、事後対応より
はるかにコストとスケジュールにやさしい。



ご相談ください support@rsrch.jp

実装のディテールが重要でなはいクルマ？

開発時のコストカットがリリース後の大出費を招く例

政府も強調「セキュリティ・バイ・デザイン」

2015/9/4 サイバーセキュリティ戦略 閣議決定

このため、2020 年までに、市場ニーズに応える安全な IoT システムを実現し、我が国の IoT システムの国際的評価を高めることを目指し、以下の取組を実施する。

(1) 安全な IoT システムを活用した新規事業の振興

IoT システムに係る新たな事業を成功させるためには、競争力の源泉となる高いレベルでのセキュリティ品質の実現が不可欠である。しかし、セキュリティを後付けで導入しても、IoT システムが本質的に安全になるものではない。むしろ単にコストの大幅な増加の要因となる。このため、連携される既存システムを含めて、IoT システム全体の企画・設計段階からセキュリティの確保を盛り込むセキュリティ・バイ・デザイン（Security By Design）の考え方を推進する。具体的には、IoT システムに係る事業について、セキュリティ・バイ・デザインの考え方に基づき所要のセキュリティ対策を業態横断的に推進し、メリハリをもって、積極的に新規事業の振興を図る

サイバーセキュリティ戦略
http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-kakugikettei.pdf

サイバーセキュリティの常識を知る人が必要

- 人口1億2千万人中 86%がインターネット接続者なのに
  現状：急激な進歩に常識がついてこれていない。
  - リスクの伝播性
    - 問題の発生により、自社だけでなく関連企業、ひいては市場全体に急激に被害が拡大する傾向がある。
  - 技術革新
    - メリット・コスト・リスクのバランスが激動している。
  - 人材不足？
    - サイバーセキュリティの専門家だけではない。
    - 買う側のリテラシーも必要。

サイバーセキュリティについてのリテラシーを
身につけることは、ビジネス・パーソンの基礎教養。

さらに「動体視力」を身につけることを目指す。

日本人のプライバシー意識は低い？

- 「プライバシー保護に対する日本人の行動意識は15カ国/地域中最も低い結果に」
  （EMCジャパン社発表(2014年7月)）
  - 世界平均、33%がソーシャルネットワークのプライバシー設定をカスタマイズしていないところ、日本は50% で最下位。
  - 世界平均 39%がモバイル デバイスをパスワードで保護していないが、日本は64%で最下位。

EMC ：http://japan.emc.com/about/news/press/japan/2014/20140702-1.htm

受け入れられるリスク・受け入れられないリスク

例：食堂やカフェのテーブルに、ノートパソコンを置いたままでトイレに行く人

・スクリーンロックをしていない場合、どんなリスクがありますか？そうしても構わないケースがありますか？

・スマートフォンなら、どうでしょうか。

自分のやりたいことについてのリスクについて、
メリットは大きめ、デメリットは小さめに考える傾向がある。

最悪の扱いを受けているパスワード

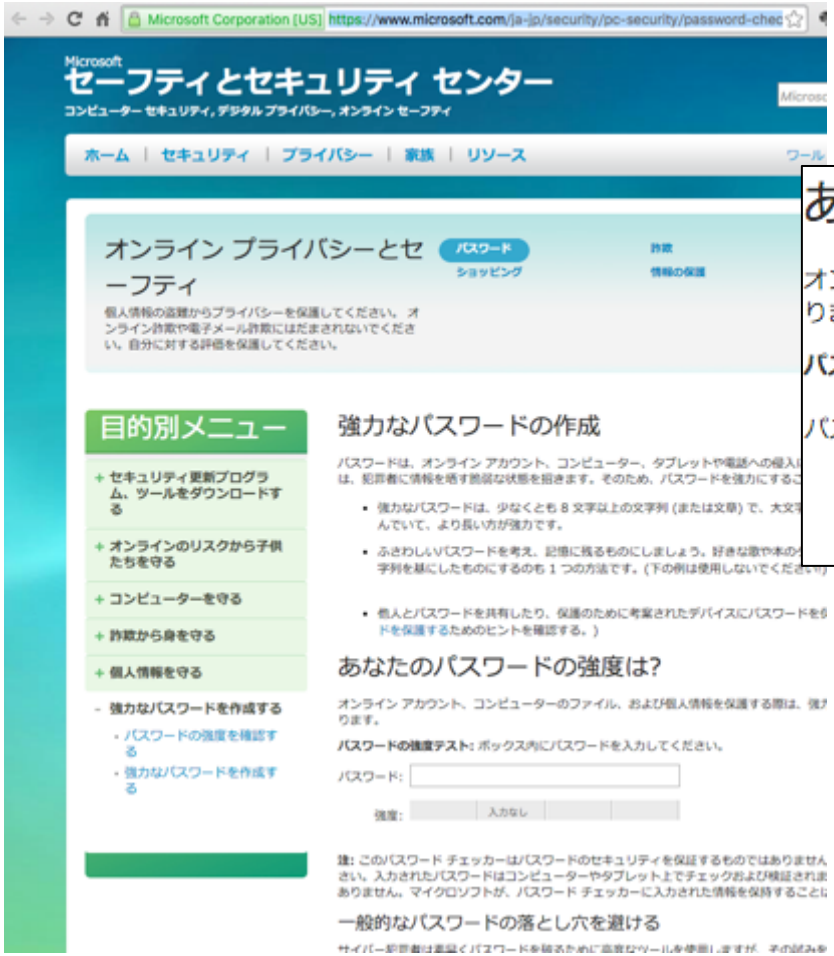
- “2014年の最悪パスワードランキング”
  (SlpashData社発表)
  - 1位は「123456」(2013年から)、2位は「password」

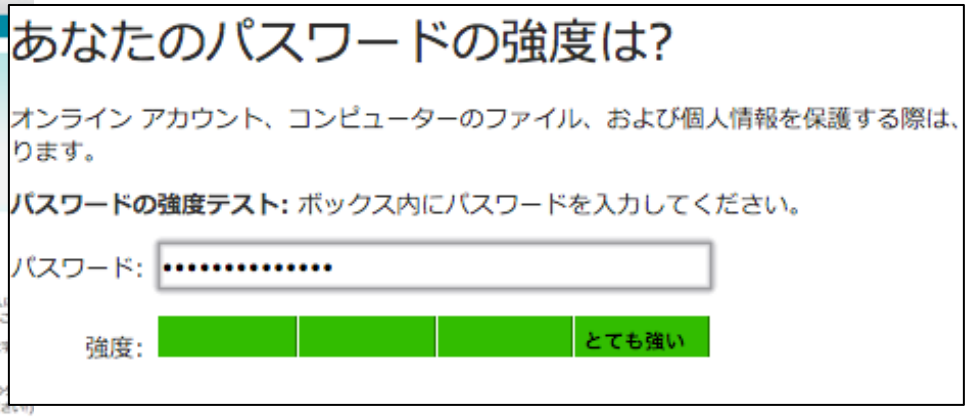
- “Password1” was still the most common password
  (TrustWave社発表(2012年、2015年))

SplashData http://www.prweb.com/releases/2015/01/prweb12456779.htm#.VL5dc1s-yoE.mailto

Microsoft パスワード強度チェッカ

https://www.microsoft.com/ja-jp/security/pc-security/password-checker.aspx

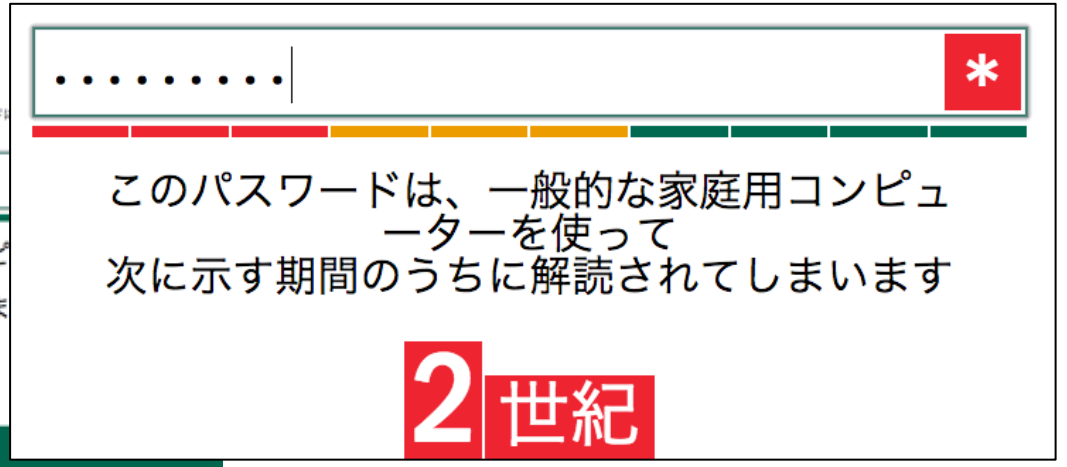




「とても強い」 レベルに何文字で到達できますか？

Kaspersky セキュアパスワードチェック

https://blog.kaspersky.co.jp/password-check/



これくらいかかれば、
しばらくは安心でしょうか・・・ね？

難しいパスワードのコツ

手法		
シード+α α+シード α+シード+β	難読化したシードに単語あるいはフレーズを決め、それに2,3桁の数字・英文字・記号を足すパターン。	@1rCAm6us15!
文章置き換え法	文章の頭文字をパスワードの文字にしていくパターン。	Cs8Tn4Na!Or#
ジェネレータを使う	http://www.graviness.com/temp/pw_creator/ ブラウザにもパスワード生成・記憶機能がついているものもある。	

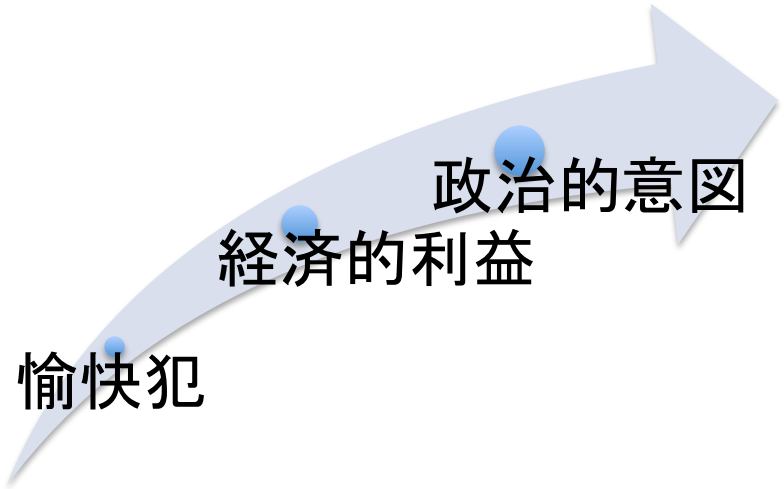
リスク・脅威・脆弱性

サイバーリスク

サイバー攻撃時代

- 攻撃者の明確な意志と目的
  - 無差別攻撃
  - 長期的で執拗なことも
- 攻撃対象
  - 不特定多数
  - 特定の組織や企業を狙ったもの（標的型）

- 攻撃シナリオ
  - 普及しているソフトウェアの脆弱性
  - ウェブ・アプリケーションの脆弱性
  - ソーシャルエンジニアリング
  - ゼロデイアタック
  - マルウェア入りのメール
  - 組織内アクセス制御不備への攻撃
  - 管理アカウント、管理用の機構



キーワード「脆弱性」

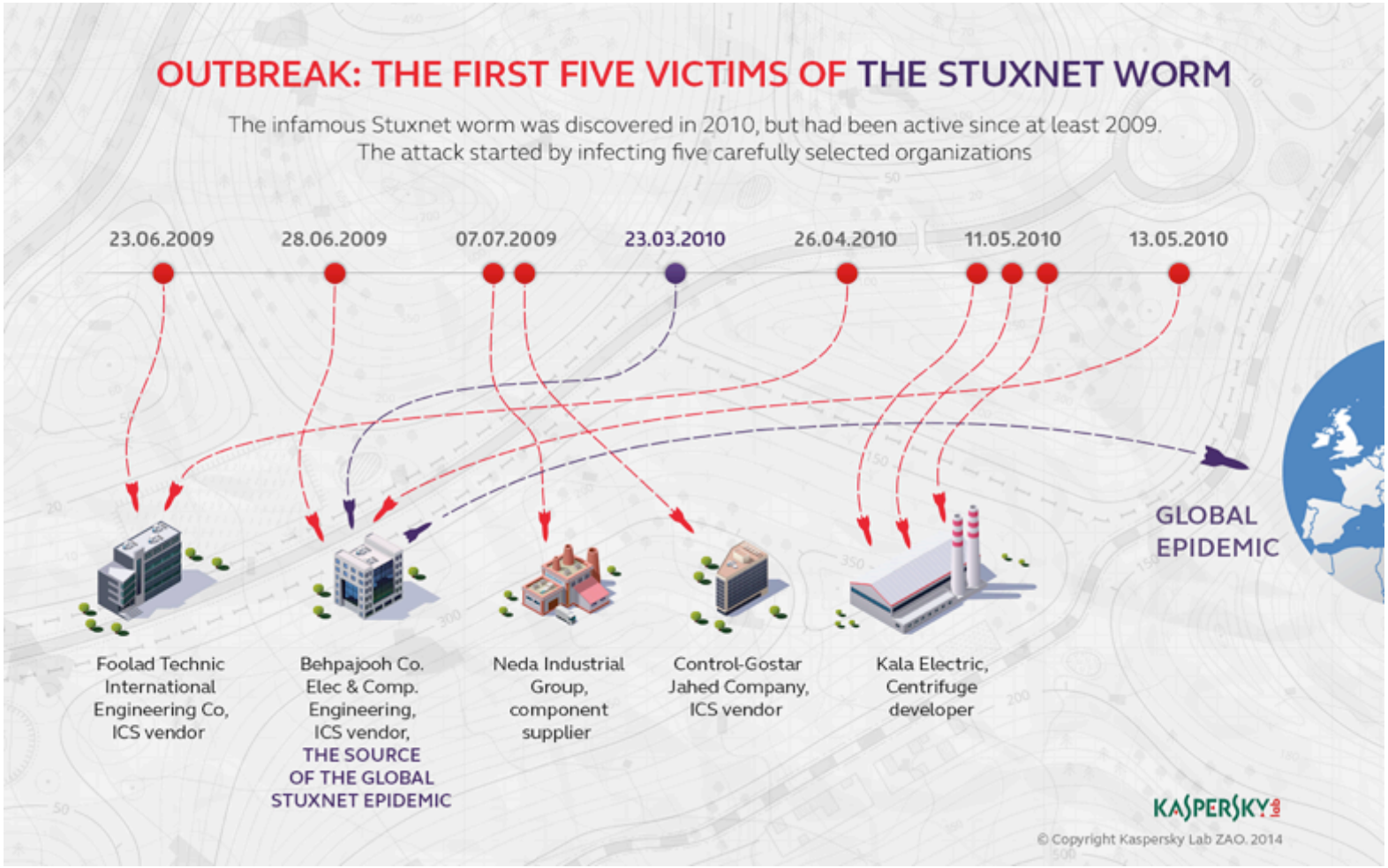
「脆弱性（ぜいじゃくせい）」Vulnerability

- 悪用されるおそれのある、
  ソフトウェアの弱点のこと。
  - 例：「その機関の用いていたソフトウェアは古く、脆弱だった」
  - 例：「アプリの脆弱性を悪用されて記録データを改ざんされた」
  - 例：「xx社の脆弱性テストは高額で報告の意味がわからない」

新しいソフトウェアでは、統計上、新しい脆弱性は存在することが考えられる。
利用者はアップデートすることで、リスク低減。
開発者は、脆弱性を作りこまない事前の対応が重要。

Stuxnet

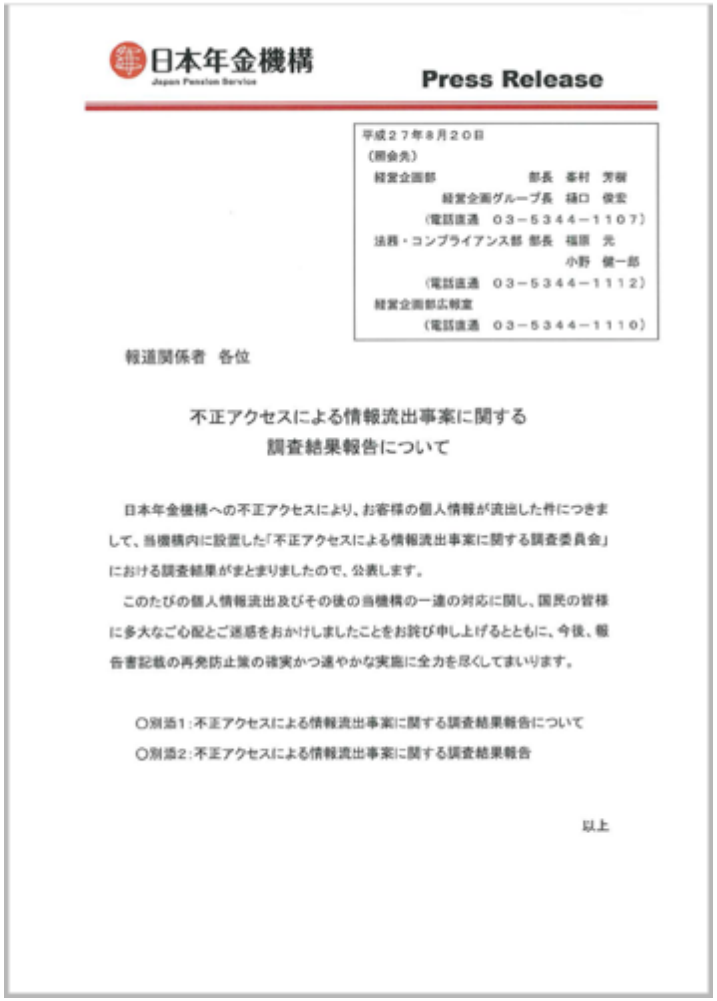
2010年6月: 制御系PLCに感染する“ワーム”。オフラインのUSBメモリなどでも感染する衝撃。



https://securelist.com/analysis/publications/67483/stuxnet-zero-victims/

日本年金機構

2015年5月発覚。
標的型攻撃メールと職員の不備により、100万件以上の情報流出



日本年金機構 Japan Pension Service

Press Release

平成２７年８月２０日
（照会先）
経営企画部　部長　峯村　芳樹
経営企画グループ長　福口　俊宏
（電話直通　０３－５３４４－１１０７）
法務・コンプライアンス部　部長　福原　元
小野　健一郎
（電話直通　０３－５３４４－１１１２）
経営企画部広報室
（電話直通　０３－５３４４－１１１０）

報道関係者　各位

不正アクセスによる情報流出事案に関する
調査結果報告について

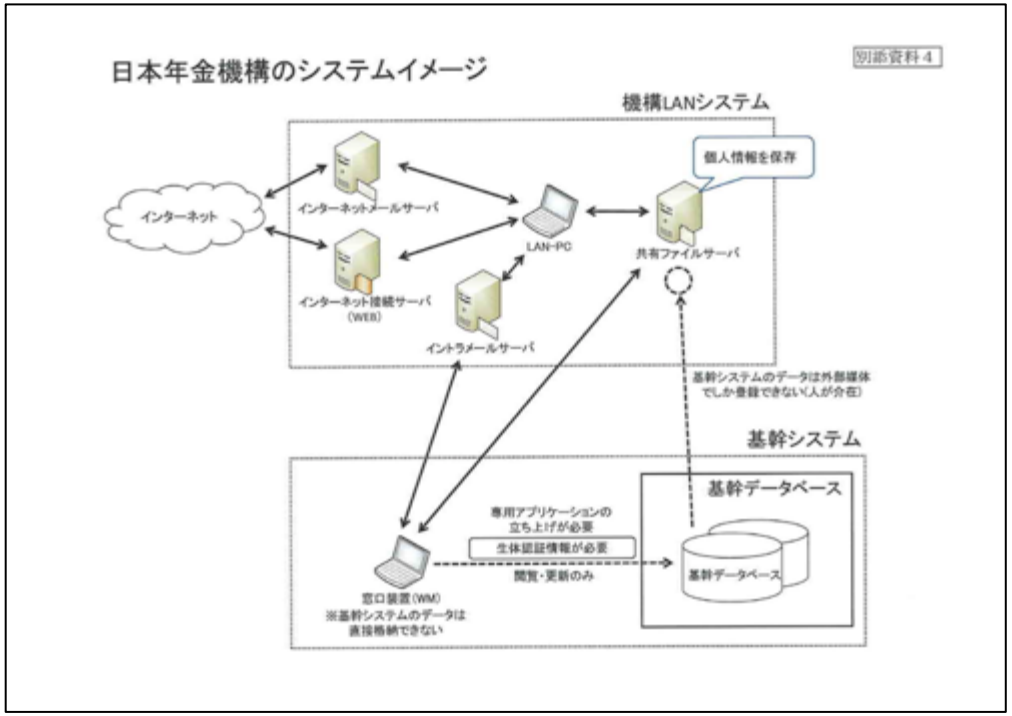
日本年金機構への不正アクセスにより、お客様の個人情報が流出した件につきまして、当機構内に設置した「不正アクセスによる情報流出事案に関する調査委員会」における調査結果がまとまりましたので、公表します。

このたびの個人情報流出及びその後の当機構の一連の対応に関し、国民の皆様に多大なご心配とご迷惑をおかけしましたことをお詫び申し上げるとともに、今後、報告書記載の再発防止策の確実かつ速やかな実施に全力を尽くしてまいります。

○別添1：不正アクセスによる情報流出事案に関する調査結果報告について
○別添2：不正アクセスによる情報流出事案に関する調査結果報告

以上

流出したとみられる個人情報：約125万件
・3情報（氏名・年金番号・生年月日）116万件
・4情報（上記に加え、住所）　5.2万件



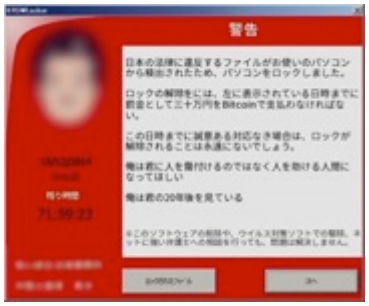
https://www.nenkin.go.jp/oshirase/press/2015/201508/20150820-02.html

サイバー攻撃として個人を狙う組織的犯罪により、経済的な被害が多発

LINEアカウント乗っ取り詐欺)

個人情報流出を騙る詐欺

ランサムウェア (*2)

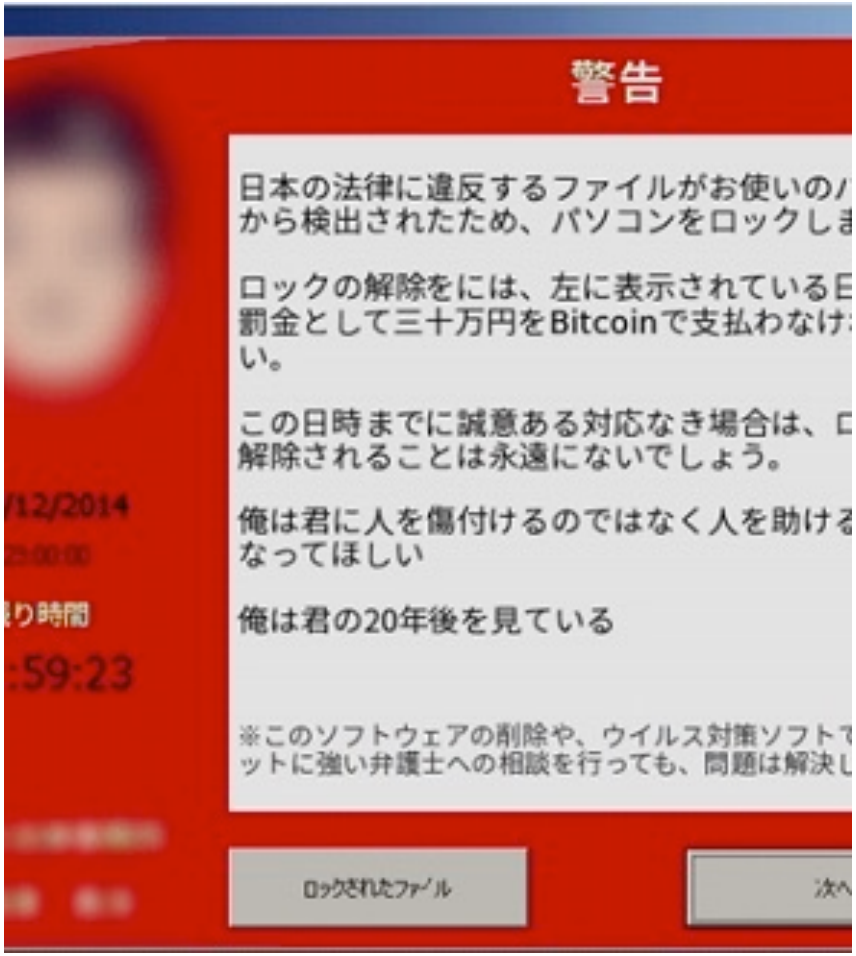


ワンクリック広告詐欺(*1)

アカウント乗っ取り、個人情報流出詐欺、ランサムウェア、
ワンクリック広告、オークション詐欺、スパム、ゲームの乗っ取り、
盗聴、盗撮、不正送金、銀行の偽画面

*1 ITMedia http://www.itmedia.co.jp/news/articles/1506/09/news108.html
*2 Symantec Blogより http://www.symantec.com/connect/blogs/torlocker

ランサムウェア



- メール、ウェブから感染
- データを「人質」にとる
  - ハードディスクを暗号化し、身代金を要求する。
  - 平均3万円程度
  - 支払っても元に戻らない
- 対策
  - バックアップ
- 対応
  - 再感染を防ぐこと

Edward Joseph Snowden

中央情報局(CIA)、国家安全保障局(NSA)の元局員。

2013年、NSAによる以下の活動を暴露

- インターネットの傍受
- 電話回線の傍受
- “PRISM”という検閲システム
  - 各種有名企業、サイトが協力させられていたことも明らかにした。

写真のライセンス：CC 表示 3.0

日本におけるサイバー犯罪の状況例

匿名ネットワークのアンダーグラウンド犯罪グループの存在*

- BBSは2000以上存在とも言われる
- サイトのアカウントとクレジットカードデータ、PayPalアカウントを有効性チェックして売買している。
  - クレジットカードデータ：平均60ドル、PayPalのアカウント 2ドル など
  - 偽造パスポート、武器、ハッキング手法などの情報交換・販売も

* From :The Japanese Underground: Japan's Unique Cybercriminal Economy, Trend Micro 2015

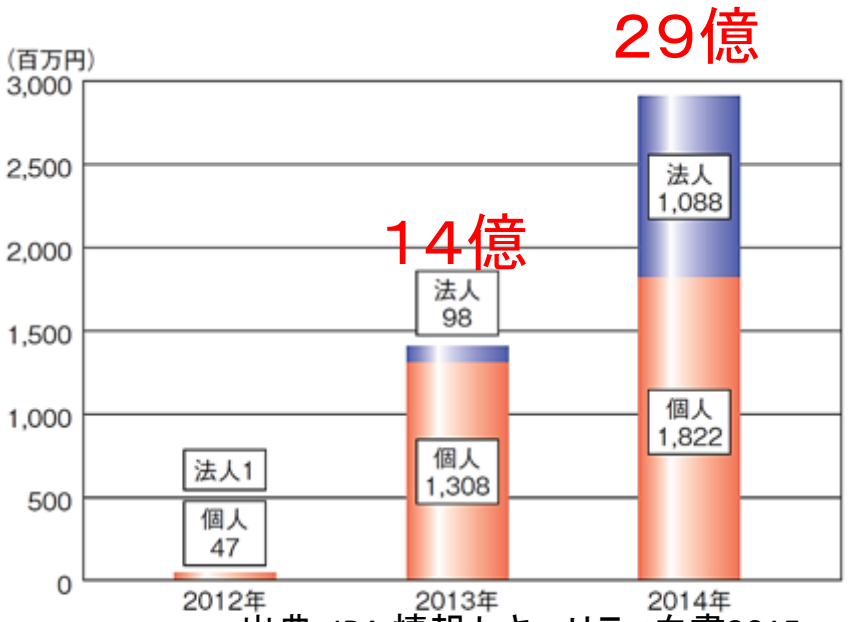
情報セキュリティ白書 10大脅威

表 2.1:情報セキュリティ 10 大脅威 2015

順位	タイトル
1	**インターネットバンキングやクレジットカード情報の不正利用** ～個人口座だけではなく法人口座もターゲットに～
2	**内部不正による情報漏えい** ～内部不正が事業に多大な悪影響を及ぼす～
3	**標的型攻撃による諜報活動** ～標的組織への侵入手口が巧妙化～
4	**ウェブサービスへの不正ログイン** ～利用者は適切なパスワード管理を～
5	**ウェブサービスからの顧客情報の窃取** ～脆弱性や設定の不備を突かれ顧客情報が盗まれる～
6	**ハッカー集団によるサイバーテロ** ～破壊活動や内部情報の暴露を目的としたサイバー攻撃～
7	**ウェブサイトの改ざん** ～知らぬ間に、ウイルス感染サイトに仕立てられる～
8	**インターネット基盤技術を悪用した攻撃** ～インターネット事業者は厳重な警戒を～
9	**脆弱性公表に伴う攻撃** ～求められる迅速な脆弱性対策～
10	**悪意のあるスマートフォンアプリ** ～アプリのインストールで友人に被害が及ぶことも～

1位 インターネットバンキングや クレジットカード情報の不正利用

- 法人の被害が大きい
  - 甚大な被害
- 手口
  - フィッシング
  - ログイン情報盗難



出典:IPA 情報セキュリティ白書2015

不正送金は中小・零細企業でも起きうる問題。
ビジネスへのダメージが大きい。

キーワード: ログイン情報強化、権限管理。

2位 内部不正による情報漏えい

- 2014年7月
  - 株式会社ベネッセコーポレーションの顧客DBを保守管理するグループ会社の業務委託先元職員が金銭取得目的で個人情報を流出

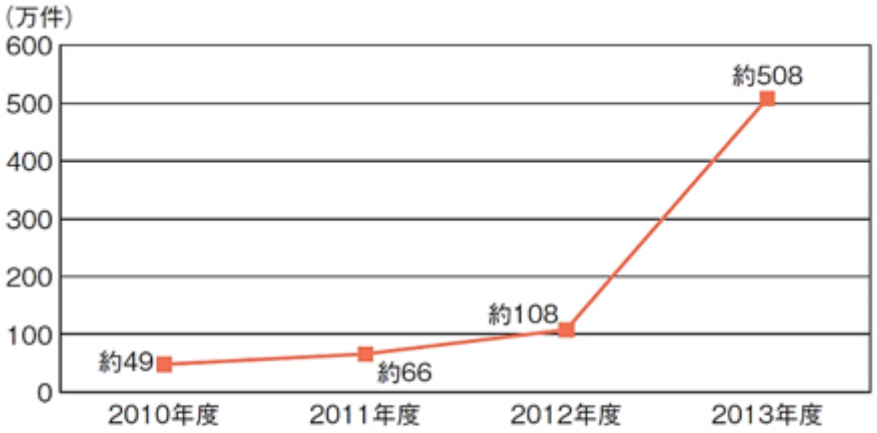
- 2015年1月
  - 家電量販店大手エディオンの子会社の元役員が遠隔操作ソフトを用いて営業秘密を不正に入手

内部不正はシステムの問題よりも動機が根深く、
保障を含めると解決までに多くの時間が必要とされる。

キーワード：アクセス権限、機密情報の保護、監視体制。

3位 標的型攻撃による諜報活動

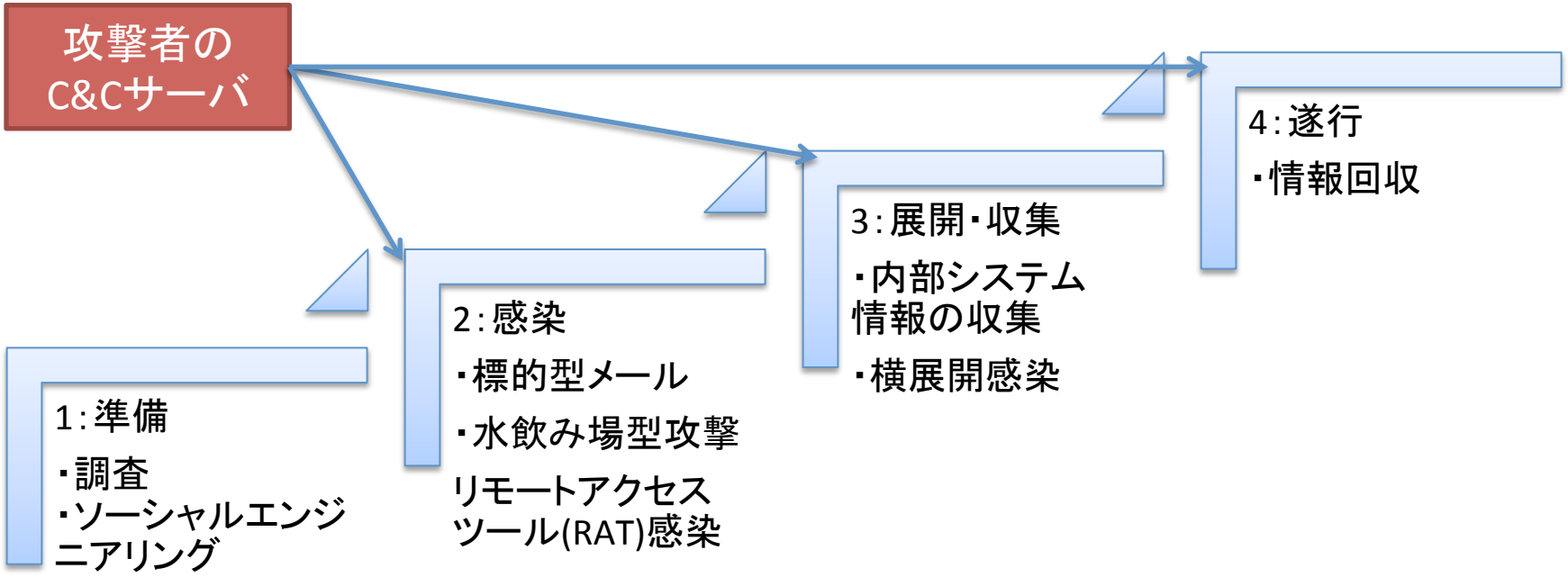
- 世界各地で、政府機関や重要インフラ企業の機密を狙った標的型攻撃が多発。
  - 「一太郎」、Microsoft Word文書に偽装したウィルスの添付メール。
  - 悪意のあるウェブサイトに待ち受けるAdobe Flashを使った「水飲み場」型攻撃もある。
- 人の情報、計画、企業秘密、研究開発情報などの窃取を目的とする。



■図 1-2-5 GSOC センサーで認知された政府機関への脅威の件数の推移
(出典)NISC※71「サイバーセキュリティ政策に係る年次報告(2013 年度)※72「政府機関における情報セキュリティに係る年次報告(平成 24 年度)※73」を基に IPA が作成

出典:IPA 情報セキュリティ白書2015

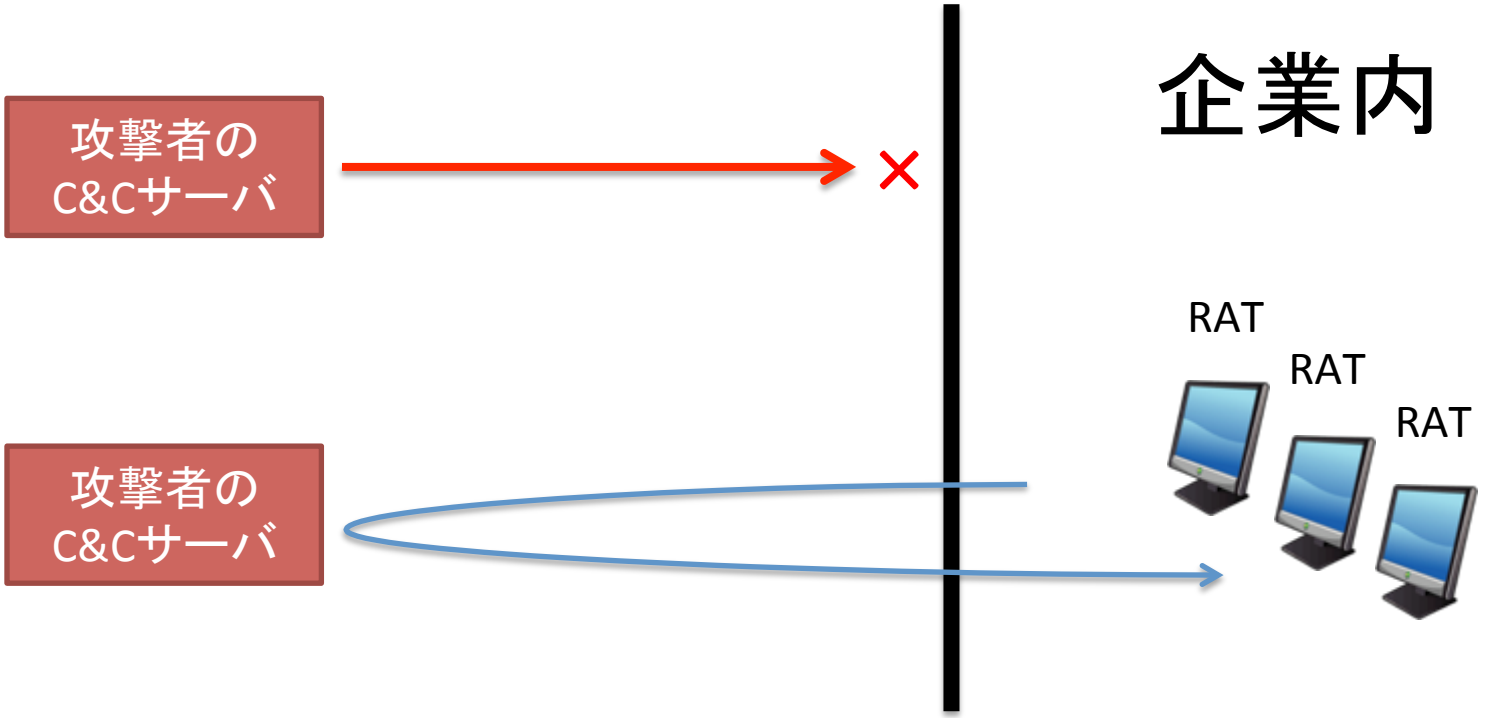
標的型攻撃 APT



HTTPSなど正当なアクセスを使うため、検知しにくい。
標的型攻撃は、実際にリモートアクセスツール（RAT）に
感染してから、情報の吸い上げまで数ヶ月かけることがある。

キーワード：C&Cサーバ、RAT、不審な通信、機密情報の保護、監視体制。

APT 3.遂行



リスク・脅威・脆弱性

セキュリティの基本のキ

国際標準ISO

ISO 27001定義

- “The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.”
  - ISO/IEC 27001:2013, 0.1 General

- “情報セキュリティマネジメント・システム(ISMS)は、リスクマネジメントプロセスを適用することによって情報の機密性、完全性及び可用性をバランス良く維持・改善し、リスクを適切に管理しているという信頼を利害関係者に与えることにある。”

セキュリティの目的
CIA Triad

- Confidentiality 機密性
- Integrity 完全性
- Availability 可用性

Confidentiality 機密性

- 機密性 ≒ プライバシー
  機微情報が不用意に見られるべきでない範囲に開示されてしまうことを防ぐ。
  - 個人情報
  - 口座情報、決済情報、クレジットカード情報
  - 健康関連情報
  - 位置情報(GPS)
  - 取引先情報

機密性への脅威は多い

- 機密情報を脅かすメカニズム
  - ネットワーク
  - ショルダーハック
  - ID/パスワード窃取
  - 暗号を見破る
  - ソーシャル・エンジニアリング
  - 脆弱性を攻撃

- リスク・コントロール
  - データを守る (refer: PCI DSS)
    - データ暗号化
    - 暗号化通信
  - アクセス制御
    - ユーザIDとパスワード
    - 二要素認証
    - 生体認証

Integrity 完全性

- 正確さ・完全さ。データが転送中であっても変更されず、権限のない人にすり替えられたりしないこと。

Q. 権限のないひとに、データがすり替えられるどんなシナリオがありますか。考えてください。

Integrity 完全性のリスクが生じるとき

- システムリスク
  - ウィルス・マルウェア・APT(標的型攻撃)
  - システムのバックドア
- 結果として
  - 改ざん、すり替え、不整合データへの変更

- リスク・コントロール:
  - 厳密なアクセスコントロール
  - 侵入検知
  - 暗号化・ハッシュ化

Integrity 完全性のリスクが生じるとき

- ユーザのミス
  - マルウェアインストール
  - システムファイルを誤って変更・誤って削除してしまう
  - 誤入力（1個300円と書くところを300個1円）

- リスク・コントロール:
  - システムの重要ファイルへのアクセスを制限
  - 入力値検証（Validation）
  - 間違えにくい機能デザイン

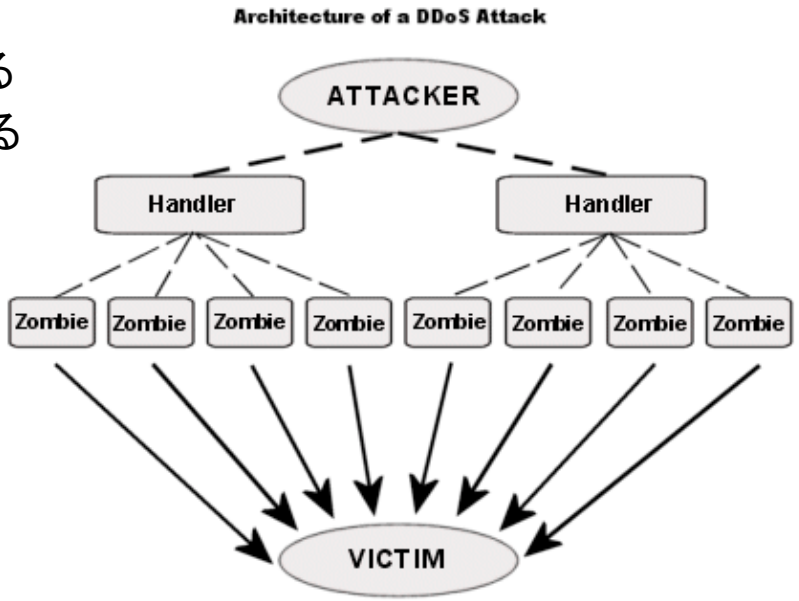
Availability 可用性

- アクセスしてよいユーザが、そうする必要があるときには、使用可能であること
  - システムの維持と、ユーザを保護する仕組み。

Q. 可用性が重要な
どんなシステムが
ありますか？

Availability のリスク
DoS(Denial of service) アタック

- “denial-of-service” アタック
  - サービスをユーザが使えない状態にする攻撃
    - ネットワークの洪水
    - 特定の個人に対してアクセスを妨害する
    - 特定のサービスあるいは人を混乱させる
    - システムダウンによる妨害
    - を、予告する脅迫



対策：アクセス環境の確保・保護・多重化
リソースの確保

http://www.cert.org/information-for/denial_of_service.cfm?

DD4BC (DDoS for Bitcoin)

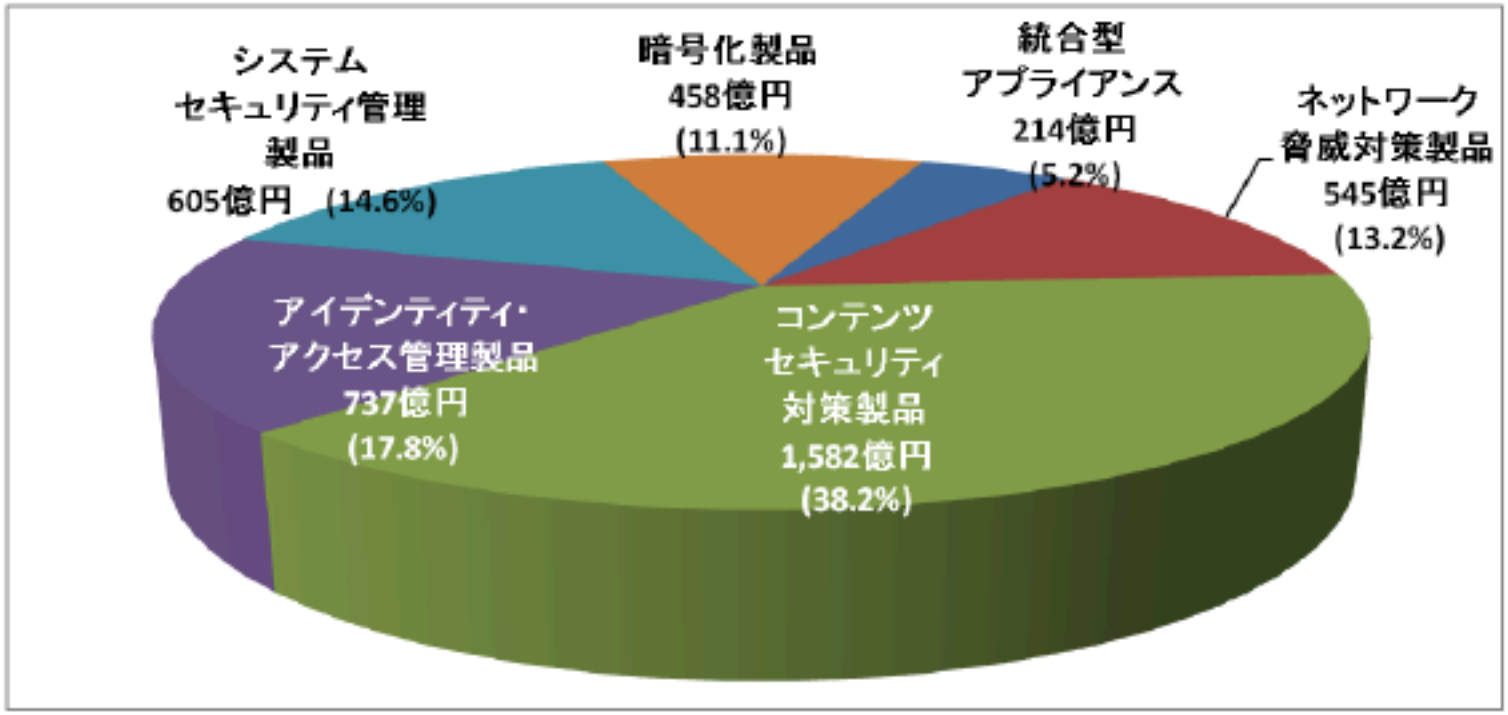
- セブン銀行
  - 残高照会、振り込みサービス
  - DDoS攻撃に伴う脅迫メールを送られた。
  - Akamai社が公表

Availability のリスク
環境面

- ソフトウェアコンポーネント
  - OSやソフトウェアが動かなくなる
- オフィス
  - 火事、電気系統の故障
- 自然災害
  - 洪水・水漏れ
  - 火山
  - 地震
  - 津波
- 実際の盗難

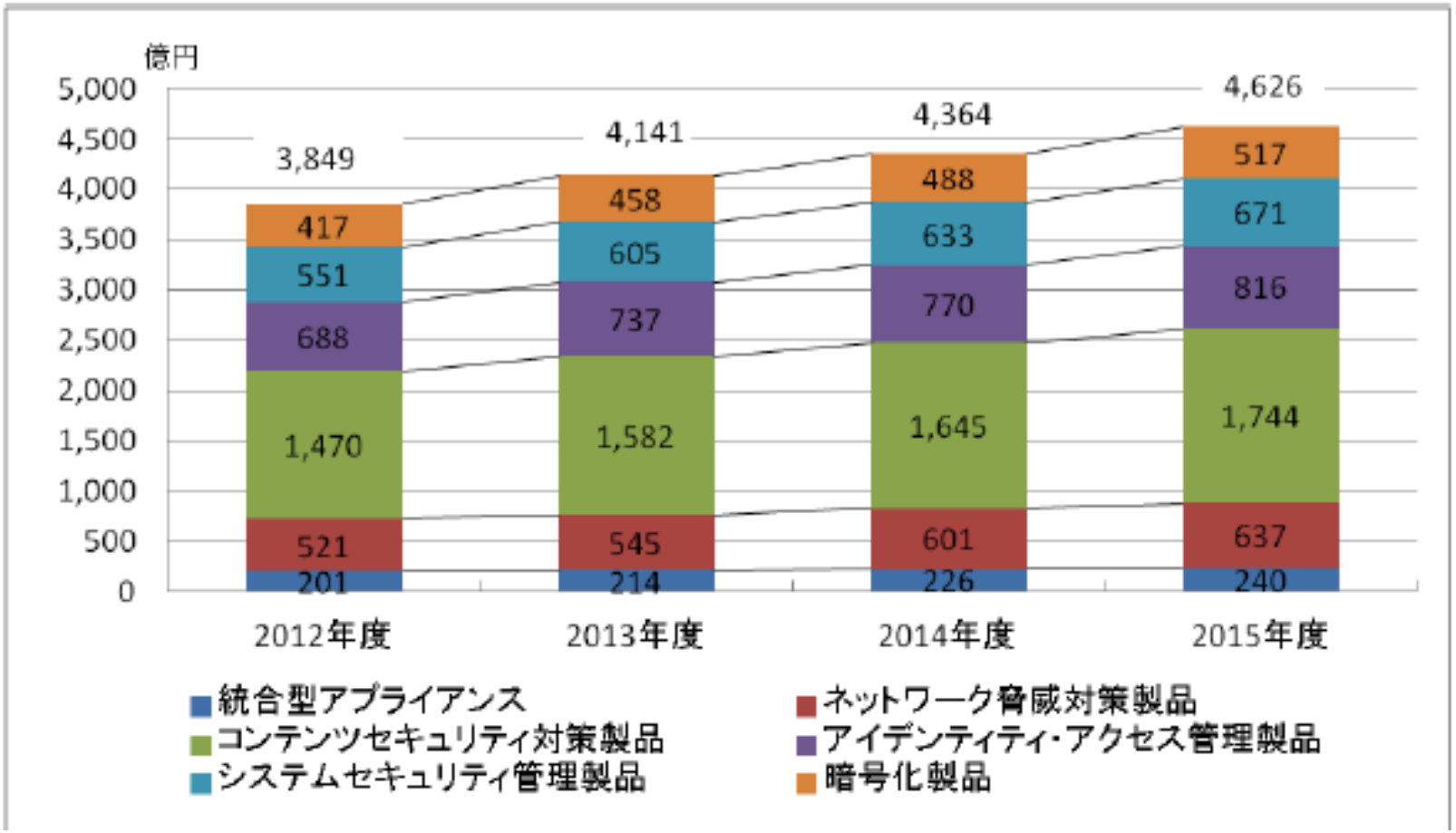
セキュリティ・ツール市場
CIA視点で見てみよう。

図 2　2013 年度の国内情報セキュリティツール市場



出典：　JNSA 2014年度情報セキュリティ市場調査報告書

セキュリティ・ツール市場
CIA視点で見てみよう。



出典： JNSA 2014年度情報セキュリティ市場調査報告書

リスク・脅威・脆弱性

リスク・コントロールの実際

リスクコントロール
事業への打撃を受けるリスクをどうするか

技術的アプローチを中心に	**リスク回避** • 原因となる活動をしない	**リスク低減** • 発生可能性を低減
財務的アプローチ	**リスク受容・保有** • 受け入れる	**リスク移転** • 全部あるいは一部を転嫁

効果的なサイバーディフェンスのための CIS Control v6.0

http://www.cisecurity.org/critical-controls/

CIS Control “クリティカルコントロール” v6.0
企業が実務上取り組むべき主要20項目

1. 認可された/されていない機器の棚卸し
2. 認可された/されていないソフトウェアの棚卸し
3. IT機器（モバイルデバイスのハードとソフト、ラップトップ、ワークステーション、サーバ)のハードウェア、ソフトウェアのセキュリティ堅牢化設定
4. 継続的な脆弱性の検査と改善
5. 管理者権限の制約的使用
6. 監査ログの維持・監視・分析
7. E-mailとウェブブラウザの保護
8. マルウェア（ウィルス）対策
9. ネットワークのポート、プロトコル、サービスなどの制限と管理
10. データ復旧能力
11. ネットワーク機器(ファイアウォール、ルーター、スイッチ)の堅牢化設定
12. 境界防御
13. データ保護
14. 知る必要性に基づいたアクセス管理
15. 無線機器の管理
16. アカウントの監視と制御
17. ギャップを埋めるためのセキュリティスキルの調査と適切なトレーニング
18. アプリケーション・ソフトウェアのセキュリティ
19. インシデント対応と管理
20. ペネトレーションテストと演習

http://www.cisecurity.org/critical-controls/
※ 日本語訳はAsterisk Research, Incによる。

CIS Control “クリティカルコントロール” v6.0
例1. 認可された/されていない機器の棚卸し

攻撃者の視点

- メンテナンスされていない機器は侵入経路、攻撃の踏み台、情報窃取の手段になる。

チェック

- 自宅のホームルーター
  - ルーターの情報「DHCPv4サーバ払い出し状況」をチェック
  - 知らない機器はつながっていないか？
- 対策
  - ネットワークに何がつながっているかチェック
  - DHCPをリリース(解放)する
  - 無線LANのパスワードを変えてみる(後述)

CIS Control “クリティカルコントロール” v6.0
例2. 認可された/されていないソフトウェアの棚卸し

攻撃者の視点

- 木は森に隠しやすい。
- 古いソフトウェアは、脆弱性も多く、悪用しやすい。
- アプリの中にも、不正な方法でビルドしたものがある

チェック

- Mac「アプリケーション」フォルダ
- Win「プログラムと機能」フォルダ
- iPhone, Androidアプリ
  - 随分以前にインストールしたままになっているもの
  - もう使っていないもの
  - なんだか覚えていないもの

CIS Control “クリティカルコントロール” v6.0
以下の項目は経営センスをもって
組織的なアプローチが必要

17.ギャップを埋めるためのセキュリティスキルの調査と適切なトレーニング

18.アプリケーション・ソフトウェアのセキュリティ

19.インシデント対応と管理

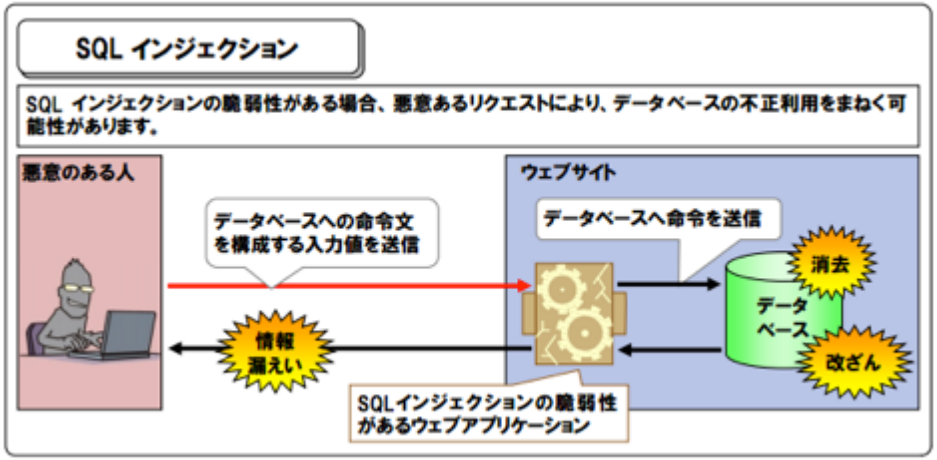
20.ペネトレーションテストと演習

ご相談ください support@rsrch.jp

CIS Control “クリティカルコントロール” v6.0
例18.アプリケーション・ソフトウェアのセキュリティ

攻撃者の視点

- アプリケーションの脆弱性は、データやインターフェースに直接アクセスできるので効率が良い
- 広く普及しているウェブ・アプリケーションなどは、攻撃を統一できるので便利。



チェック

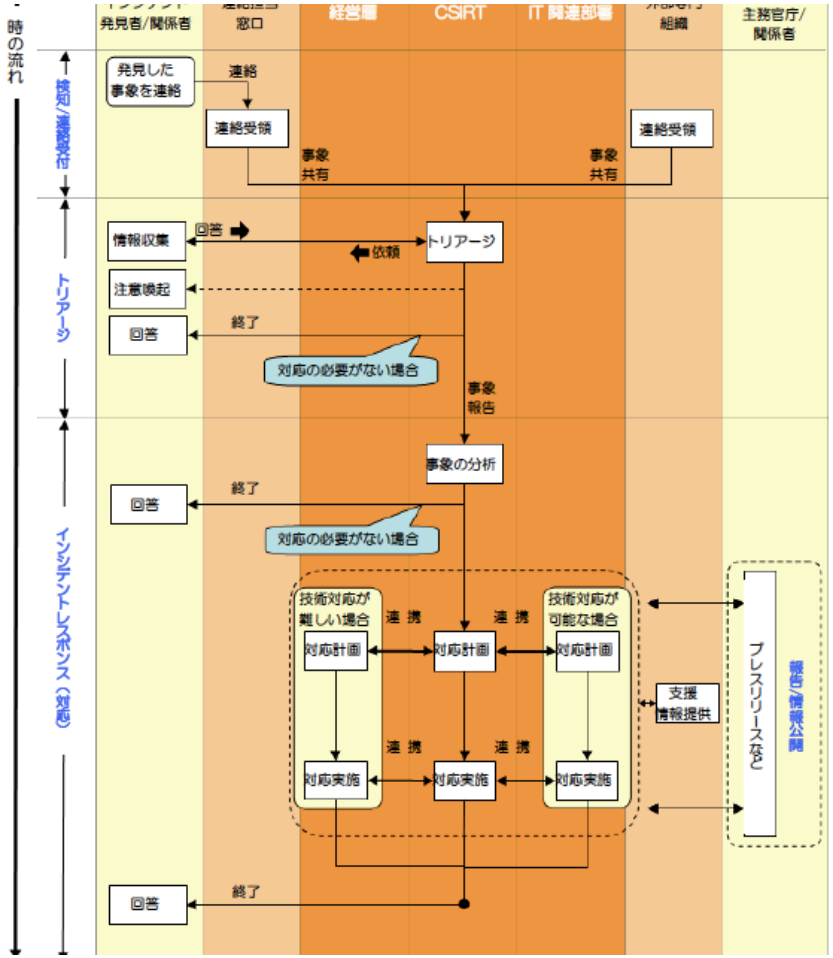
- 業者に発注したシステム
  ex. 構築したWordPress
  - 最新への更新の頻度は？

アプリ・ウェブサイト開発

- 重大な脆弱性を作りこまないようにする。
- 開発ツール、トレーニング
- ソースコード検査
- 脆弱性テストを実施する

参考：安全なウェブサイトの作り方https://www.ipa.go.jp/security/vuln/websecurity.html

CIS Control “クリティカルコントロール” v6.0
例19. インシデント対応と管理

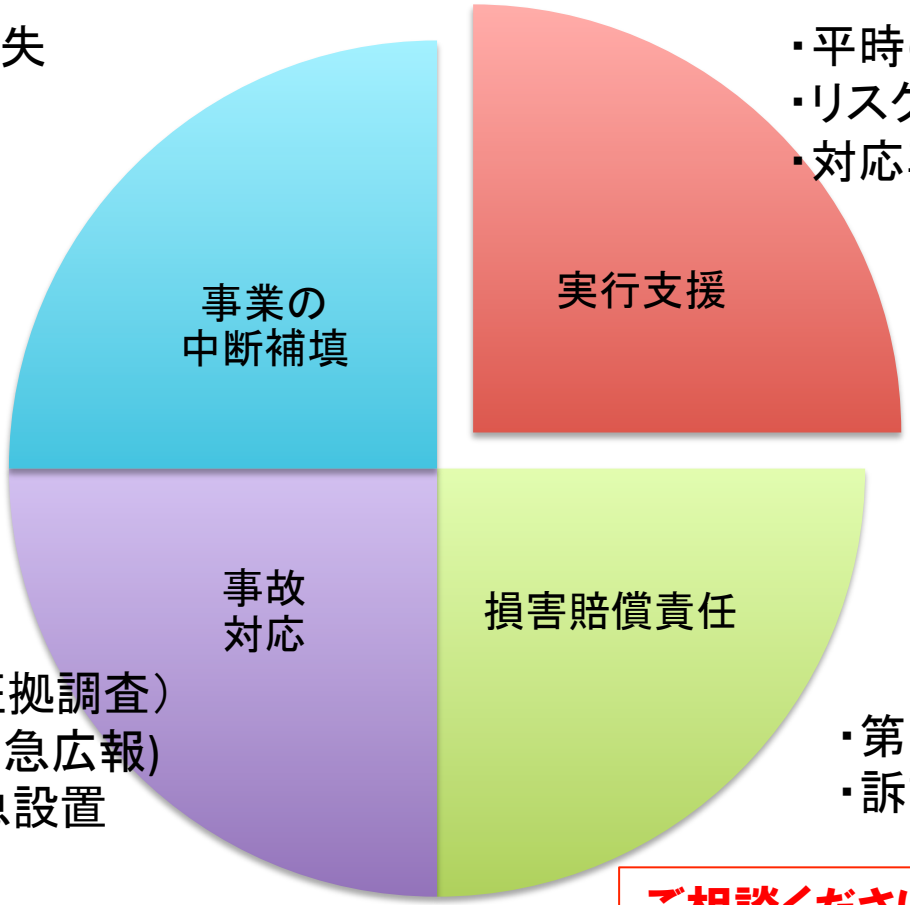


1. 検知/連絡受付
2. トリアージ
3. インシデント・レスポンス
4. 報告/情報公開

JPCERT インシデントハンドリングマニュアル

サイバーリスクが実際に起こったら

・事業停止期間の損失
・復旧費用
・代替装置費用



・平時の情報提供
・リスク診断
・対応専門事業者への相談

・危機管理対応
・フォレンジックス（証拠調査）
・レピュテーション(緊急広報)
・コールセンター緊急設置
・法的対応費用

・第三者への損害賠償
・訴訟対応費用

ご相談ください support@rsrch.jp

フィナンシャルリスク対策：サイバーリスク保険

- 米国では加入者が急成長
- IT企業はリスクが高い業種
- 個人情報、機微情報を取り扱う企業が続々加入
  - ヘルスケア、小売、技術、情報通信分野の75～80%が加入
  - 小売業界：クレジットカード情報
  - 製造業：取引先企業情報、特許情報

企業規模(売上規模USD)	主な掛け金レベル(USD)	保険上限(USD)
小企業(3000万)	3000	10万-50万
中企業(2億以下)	11万-15万	1000万（複数保険）
大企業(10億)	250万	1億（複数保険）

2015年3月 IPA/JETROニューヨーク「米国等のサイバーセキュリティに関する動向」参照

日本でもサイバーセキュリティ対策保険が続々と発売開始

- 2013/1 米国AIGグループ AIU保険がサイバーリスク保険「CyberEdge」発売
- 2015/2 東京海上日動「サイバーリスク保険」
- 2015/9 三井住友海上火災保険、あいおいニッセイ同和損害保険の共同開発保険
- 2015/9 損保ジャパン日本興亜「サイバー保険」を10/1から発売

日本では、掛け金と支払い額は、基本的に業種と売上規模で決まる。

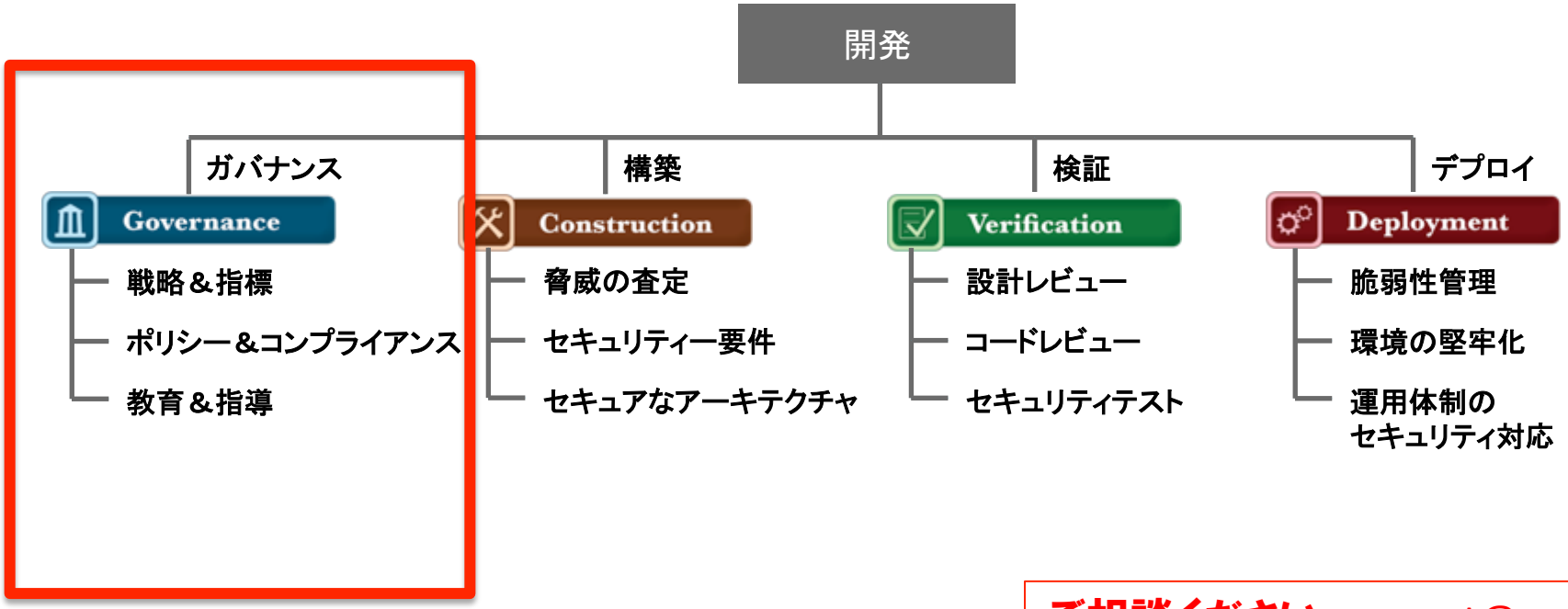
売上高10億円の企業が、賠償責任10億円、事故対応などの各種費用1億円の保険に入る場合、年間保険料は50万円～100万円程度（東京海上日動）

ご相談ください support@rsrch.jp

ガバナンス(統制)＝
情報セキュリティを経営視点で統合すること

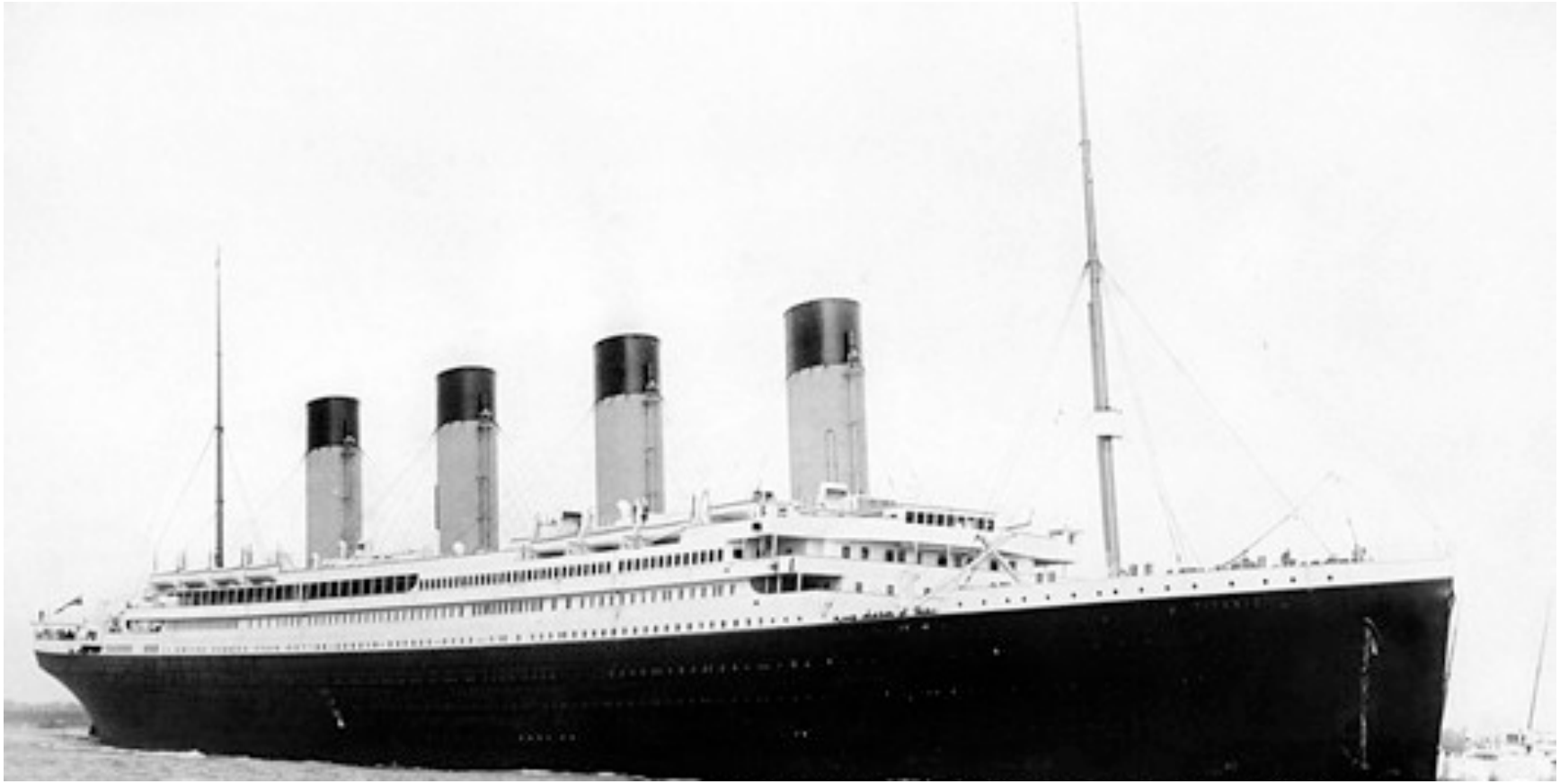
OpenSAMMの全体像

ビジネス機能と各フェーズでのセキュリティ対策:



ご相談ください support@rsrch.jp

The biggest risk is “思い込み”



RMS Titanic departing Southampton on April 10, 1912. (Photo: Creative Commons)

Asterisk
Research,Inc.