経営視点からの
サイバーセキュリティー対策
～ インターネットが前提の社会 ～

東京大学 大学院 情報理工学系研究科 教授
WIDEプロジェクト 代表
Internet Society 理事
データセンター協会 理事・運営委員長
江崎 浩 (Hiroshi Esaki)

セキュリティー対策。。。。経営側

- **「経営者」に、投資意欲が出てきにくい。**
  1. **必要性は、ある程度認識している ・・・実感はない。**
  2. **常時は邪魔者(効率を下げる) だし、不要。。。。**
  3. **インシデントが上層部にエスカレーションされない！**
     (*) 隠蔽体質 ➔ 企業統治の問題。
     (*) ISAC の仕事
  4. **{短期}利益に貢献しない。 ・・コスト だと考える。**
  5. **インシデントが発生しないと価値が分からない**
  6. **人材がいない。。。 ➔ CIO と CISO が 同じ ！？**

“不具合”で処理

(*) 省エネ・節電、オープン化 も ほぼ 同じ構造

経済産業省「産業サイバーセキュリティー研究会」

1. **サプライチェーン**(=3層構造のValue Creation Network)としてのサイバーセキュリティー

2. **経営・財務**&**企業統治(監査)**への包含

3. **産業分野ごと**に対応策を立案・実施
   a. データセンター業界：**JDCC/GUTPガイドブック**
   b. 全産業：**データセンターの利用**

4. **シルバー人材**の確保と活用

これまでの
インターネット

IP for Everyone

IoT (Internet of Things)
IP for Everything

IP for Everyone

IoT (Internet of Things)
IP for Everything

IP for Everyone

IT業界とは
かけ離れた
過去の世界

ビッグデータ解析・人工知能
実現の ”大” 障壁・障害

アンバンドル化
＝オンライン化

垂直統合型モデル
（閉域システム）

水平統合型モデル
（連携・協調プラットフォーム）

ビッグデータ解析・大[illegible]能
実現の”大”障壁・障害

邪魔をする
これまでの**商慣習**
特に重要インフラ

必須となる
セキュリティー対策

垂直[illegible]
(閉域システム)

[illegible]統合型モデル
(連携・協調プラットフォー[illegible]

頭にくる 常套手段(＝ビジネス慣習)

1. 外部とは接続されませんので、安心してください。
   ✔安全な環境ですので、事故は発生しません。
2. 独自技術ですので、「安全』かつ 『安価』です。
3. お客様がご希望されます機能を提供することは、
   ① 不可能です(実は可能であることは知っている)。
   ② 新たに大きな開発費用と検証費用が発生します。
   ③ 他社との接続をしますと動作保証の対象外になります。
4. 仕様変更・追加は、コスト増加(＝避けるべき)
5. 納期と予算を守るためには、、、、、、、忖度。。。

重要な経験則

- ✓ 「安全」(=100％)は 存在しない。
- ✓ 「インシデントの発生」は、消滅しない。
- ✓ 「安全」だと信じて、「安心する」ことの危険性を認識する。
- ✓ 人に頼り切りになるのは、とても(一番)危険である。
- ✓ 予防接種 と 免疫力の向上は、常時化すべき。
- ✓ 自分で守るが基本原則。 でも、協力し合うと、さぼらず＆経験の共有ができる。

セキュリティに対する考え方

Internet Governance Conference Japan
IGCJ
日本インターネットガバナンス会議

http://igcj.jp/

1. **グローバル**に考え、**ローカル**な施策を行う
2. 「原理主義」ではなく**「実践主義」**で進める
3. 強制する・制限するのではなく、**活動の活力向上**を応援する
4. **「過保護」**は、かえってリスクを増大させる
5. 「やらされる」ではなく、**「やりたくなる」**を目指す
6. セキュリティ対策を、**品質向上のための投資**と捉える
7. 経験と知見の**「共有」**を行う
8. インシデントの経験者は、「被害者」として**「保護・支援」**する
9. **「匿名性」の堅持** と プライバシーの保護
10. **まずは自助、次に共助、最後に公助**

セキュリティに対する考え方

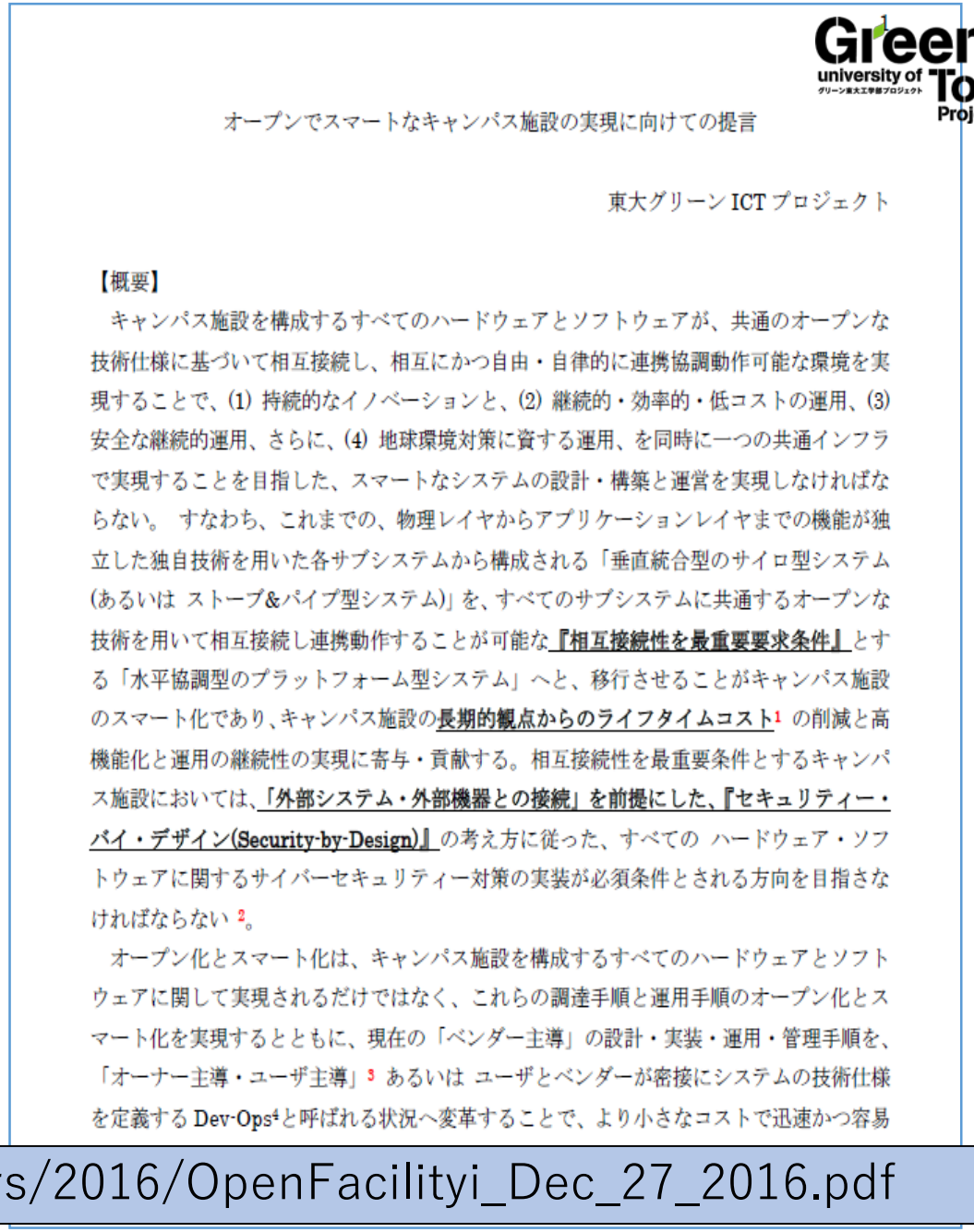
1. グローバルに考え、ローカルな施策を行う
2.
3.
4.
5.
6.
7.
8.
9.
10. ずは自助、次に共助、最後に公助

『まずは自助、
次に共助、
最後に公助 !!! 』

➔ End-to-End の原則 ！

『オープン調達への提言』

1. 相互接続性
2. 外部との接続を前提
   ➔ “Security-by-Design”
3. 調達のオープン化
4. ライフタイムコスト
5. オーナー主導へ



Green university of Tokyo Project

オープンでスマートなキャンパス施設の実現に向けての提言

東大グリーン ICT プロジェクト

【概要】

キャンパス施設を構成するすべてのハードウェアとソフトウェアが、共通のオープンな技術仕様に基づいて相互接続し、相互にかつ自由・自律的に連携協調動作可能な環境を実現することで、(1) 持続的なイノベーションと、(2) 継続的・効率的・低コストの運用、(3) 安全な継続的運用、さらに、(4) 地球環境対策に資する運用、を同時に一つの共通インフラで実現することを目指した、スマートなシステムの設計・構築と運営を実現しなければならない。 すなわち、これまでの、物理レイヤからアプリケーションレイヤまでの機能が独立した独自技術を用いた各サブシステムから構成される「垂直統合型のサイロ型システム(あるいは ストーブ&パイプ型システム)」を、すべてのサブシステムに共通するオープンな技術を用いて相互接続し連携動作することが可能な『相互接続性を最重要要求条件』とする「水平協調型のプラットフォーム型システム」へと、移行させることがキャンパス施設のスマート化であり、キャンパス施設の長期的観点からのライフタイムコスト[1] の削減と高機能化と運用の継続性の実現に寄与・貢献する。相互接続性を最重要条件とするキャンパス施設においては、「外部システム・外部機器との接続」を前提にした、『セキュリティー・バイ・デザイン(Security-by-Design)』の考え方に従った、すべての ハードウェア・ソフトウェアに関するサイバーセキュリティー対策の実装が必須条件とされる方向を目指さなければならない [2]。

オープン化とスマート化は、キャンパス施設を構成するすべてのハードウェアとソフトウェアに関して実現されるだけではなく、これらの調達手順と運用手順のオープン化とスマート化を実現するとともに、現在の「ベンダー主導」の設計・実装・運用・管理手順を、「オーナー主導・ユーザ主導」[3] あるいは ユーザとベンダーが密接にシステムの技術仕様を定義する Dev-Ops[4]と呼ばれる状況へ変革することで、より小さなコストで迅速かつ容易

http://hiroshi1.hongo.wide.ad.jp/hiroshi/papers/2016/OpenFacilityi_Dec_27_2016.pdf

最近、お金が余っています？

お金が余ると、**税金を払うより “先行投資“ ➔ SDG**

◆戦略長期投資 ➔ IR への反映

リスク回避・減少、**ブランド向上**(品質の向上・持続➔**会社の価値**)

潜在的な含み損(BS と PL の両方) を 減少させる。

➔ インシデントの発生確率を下げられれば、 BS /PL/CFに貢献

ノウハウの蓄積(＝**長期的競争力**向上)

企業統治
鍵は”調達”

◆ これは、、、CISO・**監査役**・社外取

1. CIO と CISO が同じ人だったりしません？
2. 米国政府の構造： 財務省, GAO, GSA, NIST

ＩｏＴ投資の抜本強化（コネクテッド・インダストリーズ税制の創設）

新設

（所得税・法人税・法人住民税・事業税）

（平成30年6月6日）
経済産業省

- **一定のサイバーセキュリティ対策**が講じられた**データ連携・利活用**により、**生産性を向上させる取組**について、それに必要となる**システムや、センサー・ロボット等の導入**に対して、**特別償却30%又は税額控除3%（賃上げを伴う場合は5%）**を措置。
- 事業者は当該取組内容に関する**事業計画を作成**し、**主務大臣が認定**。**認定計画に含まれる設備投資**に対して、**税制措置を適用（適用期限は平成32年度末まで）**。

【計画認定の要件】

①データ連携・利活用の内容

・社外データやこれまで取得したことのないデータを社内データと連携

・企業の競争力における重要データをグループ企業間や事業所間で連携

②セキュリティ面

必要なセキュリティ対策が講じられていることをセキュリティの専門家(登録セキスペ等)が担保

③生産性向上目標

投資年度から一定期間において、以下のいずれも達成見込みがあること

・労働生産性：年平均伸率２%以上

・投資利益率：年平均15%以上

認定された事業計画に基づいて行う設備投資について、以下の措置を講じる。

対象設備	特別償却	税額控除
ソフトウェア		3%
器具備品	30%	（法人税額の15%を限度）
機械装置		5%
		（法人税額の20%を限度）

【対象設備の例】

データ収集機器（センサー等）、データ分析に自動で連動するロボット・工作機械、データ連携・分析に必要なシステム（サーバ、ネットワーク等）、セキュリティ対策製品　等

最低投資額：300万円

※計画の認定に加え、継続雇用者給与等支給額の対前年度増加率＋2%を満たした場合。

コネクテッド・インダストリーズ税制

【計画認定の要件】

② セキュリティー面

必要なセキュリティー対策が講じられていることをセキュリティーの専門家(登録セキスペ等)が担保

http://www.meti.go.jp/policy/it_policy/data-katsuyo/iot-zeisei/iot-zeisei.html

【命題】　社長に、セキュリティー対策に『投資』してもらう

1. 戦略　：　利益と売上に貢献
2. 戦術　：　エコ システム(➔Multiple-Pay-off)
   “One Asset for Multiple Use“
3. 武器　：　調達(オープン・プラットフォーム化)

潜在的損失項目

投資効率

組織統治（監査機能）
e.g., 米国連邦政府
(GAO, GSA, NIST,DHS)

Society5.0 で重きを置くべき課題

「また、製品やサービスを提供する際には、任務保証の考え方に基づき取り組むことが重要であり、また、**セキュリティ品質の実現が欠かせない。**セキュリティ品質を確保するための費用はコストでなく価値を生み出すための投資である。

その実現には、企画・設計段階からセキュリティ確保を盛り込む**セキュリティ・バイ・デザインの考え方**を持ち、開発時や運用時においては個々のＩｏＴシステムの階層構造を踏まえたデータとＩｏＴシステム全体のセキュリティ確保を図ること、異なる分野を連携協調させる際にはＩｏＴシステム間の相互連携を図り、ＩｏＴシステム全体としてのセキュリティを確保すること、の２点が重要である。さらに、日々進化し高度化するサイバー攻撃に対応するためには、セキュリティ確保のための人材育成も必要な取組である。セキュリティ技術の高度化及び社会実装の推進については、**重要インフラ等から優先的に対応する**。具体的には、サイバーセキュリティ技術の研究開発を推進するとともに、**業界内・業界間でのサイバー攻撃等の情報共有を共通化・自動化を実現する仕組みを構築**し、さらに業種間を跨ぐ情報共有の環境整備に取り組む。これにより、イベント単位で短期間の設置も想定される**セキュリティオペレーションセンター（Security Operation Center、以下「SOC」という。）**の整備促進や業界間のＳＯＣ整備の促進にもつながる。」

WG1の検討体制

- サイバー・フィジカル・セキュリティ対策フレームワークの標準モデルを検討し、**業界毎に順次展開**して、具体的適用のためのセキュリティポリシーを検討。

ＷＧ１　制度･技術･標準化

標準モデル

Industry by Industryで検討
(分野ごとに検討するSWGを設置※)

- ビル（エレベーター、エネルギー管理等）
- 電力
- 防衛産業
- 自動運転
- その他コネイン関係分野（スマートホーム等）

標準化･技術開発等の連携

標準化･規格･認証関連機関

IPA	セキュリティ対策を牽引する独立行政法人
ECSEC	ICチップ等のセキュリティ技術研究組合
JIPDEC	セキュリティマネジメントの認証組織
CSSC	制御系セキュリティ技術組合
CRYPTREC	暗号化標準団体

セキュリティ技術開発に関する産学官の各種プロジェクト

企業　大学　国研

国際標準提案 / 相互承認提案

Report by GAO

(United States Government Accountability Office)

財務省
- GAO：監査機能
- GSA： 調達管理
- NIST ：調達仕様(推奨)

設備セキュリティは『**国家安全保障**』としての サイバーセキュリティ対策 という認識と施策の実施

http://www.gao.gov/assets/670/667512.pdf

DHS: Department of Homeland Security (国土安全保障省)

GSA: General Service Administration (連邦政府調達局)

- P.9-11: Facilities in Buildings
  - closed circuit camera systems
  - access control systems
  - fire annunciation and suppression systems
  - heating, ventilation, and air conditioning systems
  - power and lighting control systems
  - elevator control systems

- P.9-11: Facilities in Buildings
  - c[illegible] circuit camera systems
  - acce[illegible]rol systems
  - fire an[illegible]
  - heati[illegible]
  - pow[illegible]

要は、たくさんの
非 IT業界の 電子機器
が設備を管理・制御し
ているのです。。。

- **P.18 : Cyber Security Risk**
  - allowing people to gain unauthorized **access to facilities**;
  - damaging temperature-sensitive equipment, **such as in data centers**
  - causing life-safety systems such as fire alarms or sprinklers to give false alarms or fail to alarm **in the event of an emergency**, **malfunctions** that could result in injury or a loss of life;
  - **disabling facilities** due to lack of power or other environmental needs;
  - providing access to information systems;
  - having to temporarily evacuate facilities; -
  - damaging the government's credibility if it was unable to protect its employees.

- **P.18 : Cyber Security Risk**
  - al[illegible]ng people to gain unauthorized **access to facilities**;
  - damag[illegible]emperature [illegible]e **data c[illegible]**
  - causi[illegible] to gi[illegible] **e[illegible]**
  - [illegible]
  - [illegible]
  - h[illegible]
  - damagin[illegible] to protect its e[illegible]

要は、たくさんの 危険要素が
放置されているし、、、、
これがHackingされると、、、
致命的に危険なことが
起こってしまいます。

Report by GAO

(United States Government Accountability Office)

財務省

- **GAO：監査機能**
- **GSA： 調達管理**
- **NIST ：調達仕様(推奨)**

設備セキュリティは『**国家安全保障**』としての サイバーセキュリティ対策 という認識と施策の実施

http://www.gao.gov/assets/670/667512.pdf

DHS: Department of Homeland Security (国土安全保障省)

GSA: General Service Administration (連邦政府調達局)

FedRAMP from FISMA

- **Fed**eral **R**isk and **A**uthorization **M**anagement **P**rogram
  - **連邦政府共通のクラウドサービス調達のためのセキュリティ基準**。クラウドサービスプロバイダーが、このプログラムの認証を受けて登録されると、省庁ごとに新たな調達評価の手続きを経ることなく、提供／調達することが可能な仕組。
  - 「連邦情報セキュリティマネジメント

    FISMA＝Federal Information Security Modernization Act.(2002年12月)

    ✓ **NISTに連邦政府がFISMAに準拠するた**
    支援をすることを義務付けている。国土安全
    保障省（DHS）配下の情報セキュリティ対
    組織である「US-CERT」設置の根拠法令。

事例： ある都内の有名なビル での 経験と対処

- CSSC(制御システムセキュリティーセンタ) の専門家が、ビルを訪問、幹部の眼の前で Hacking !!!!
- 運用管理センターの前の床に、{ウィルスはない健全で安全な}USBメモリを 残した。
  ➔ 拾って、運用管理センターのパソコンに接続。。。

抜本的＆根本的な
管理マニュアル と 調達要件の見直し

JDCC 日本データセンター協会 Japan Data Center Council

Green university of Tokyo Project グリーン東大工学部プロジェクト

SAKURA internet

https://www.sakura.ad.jp/

Data Center by **IEEE1888 for DCEM(Data Center Energy Management)**

1. **Cyber Security for Facility and IoT devices**
2. **Big-Data analysis with own technologies**

というわけで、

【命題】
社長(経営者)に
セキュリティー対策に対して
投資をしてもらうには？

ということで、重要な 考え方と 施策

1. 個別システムごとのサイバーセキュリティー対策
   ➔ サプライチェーン(=value creation network)としての対策
2. 既存システム と 新規システム
   a. 既存システムへの 緊急対策
   b. 新規システムへの 戦略的対策 (“調達条件“)
3. 利益にならなかったコスト部門に 利益を出させる！！
   a. 財務管理・財務表への包含
   b. 潜在的損失項目(BS&PL) vs 損失削減投資(PL)
4. 『実装機能』の確認・認証
   ➔ 『統治耐性 と プロセス(手順)』の確認・認証

1. 監査機能
2. IR 評価

経済産業省 「産業サイバーセキュリティー研究会」

1. サプライチェーン (=3層構造のValue Creation Network)としてのサイバーセキュリティー

2. 経営・財務&企業統治(監査)への包含

悪行の手口を熟知 !!
やり過ぎも熟知！

プロセス監査は、
労働集約型職種。。。

b. 全産業・データセンターの利用

4. シルバー人材の確保と活用

経済産業省「産業サイバーセキュリティー研究会」

1. **サプライチェーン**(=3層構造のValue Creation Network)としてのサイバーセキュリティー

2. **経営・財務**&**企業統治(監査)**への包含

3. **産業分野ごと**に対応策を立案・実施
   a. データセンター業界：**JDCC/GUTPガイドブック**
   b. 全産業：**データセンターの利用**

4. **シルバー人材**の確保と活用