資料3

社会問題から見たサイバーセキュリティに関する技術課題

サイバーセキュリティ戦略本部研究開発戦略専門調査会　講演資料（抜粋）

株式会社三菱総合研究所
社会ICTイノベーション本部
サイバーセキュリティ戦略グループ
石黒　正揮, Ph.D.

目次

１．社会問題から見たサイバーセキュリティの技術課題 2

２．サプライチェーンセキュリティの動向と課題 8

３．IoT進展におけるセーフティとセキュリティの統合リスク分析手法 17

４．サイバーセキュリティ経済学 27

５．技術課題の整理 36

１．社会問題から見たサイバーセキュリティの技術課題

社会課題から見たサイバーセキュリティの取組み俯瞰

● 注目テーマとして、サイバーとフィジカルの融合、サプライチェーンの複雑化に対応して、認証制度、セキュリティ診断・監査サービス、セキュリティ・アシュアランスなど、政策的解決策、ビジネス解決策、要素技術を組合わせた取組みの検討が期待される。

政策×ビジネス×技術の組合せで解決

解決が期待される課題（チャレンジ）	社会問題
サイバーとフィジカルの融合	産業制御システムへのサイバー攻撃 IoTエコシステムへのサイバー攻撃
サイバー犯罪・サイバー攻撃対策	組織・サプライチェーンに対するサイバー攻撃 セキュリティリテラシーの低さ 国境をまたいだ犯罪の増大
情報の自由な流通／サイバー空間における国家主権	デジタル経済の不安定化・脆弱性 データローカライゼーションの進展
国際競争力の向上	IT産業の競争力低下 セキュリティ投資のインセンティブの低迷
重要インフラ・イベントのテロ対策	重要インフラへのテロ攻撃 イベント施設へのテロ攻撃

制度的解決策

- 安全基準等の策定
- 国際標準化
- 政府調達基準
- 機器認証制度
- 国等によるガイドライン等の策定
- 普及啓発
- ISMS等の評価認証制度
- サイバー犯罪条約の批准国の拡大
- 犯罪捜査能力の向上
- サイバー空間に関する国際的ルール作り
- 徴税能力の強化
- 規制や税制の国際的ハーモナイゼーション
- サイバーセキュリティ投資に対する優遇策
- サイバーセキュリティ研究開発の支援
- 省庁横断・包括的な体制強化

ビジネスによる解決策

- セキュリティ評価・診断・監査サービス
- 産業システム・IoT向けセキュリティ対策アプライアンス
- ネットワークセキュリティ製品
- エンドポイントセキュリティ製品
- セキュリティ運用監視サービス
- システムの評価・診断・監査
- ISMSコンサルティング
- セキュリティ教育・研修
- サイバー演習・訓練
- 業界検証テストベッド
- 先進技術の導入コンサルティング

要素技術

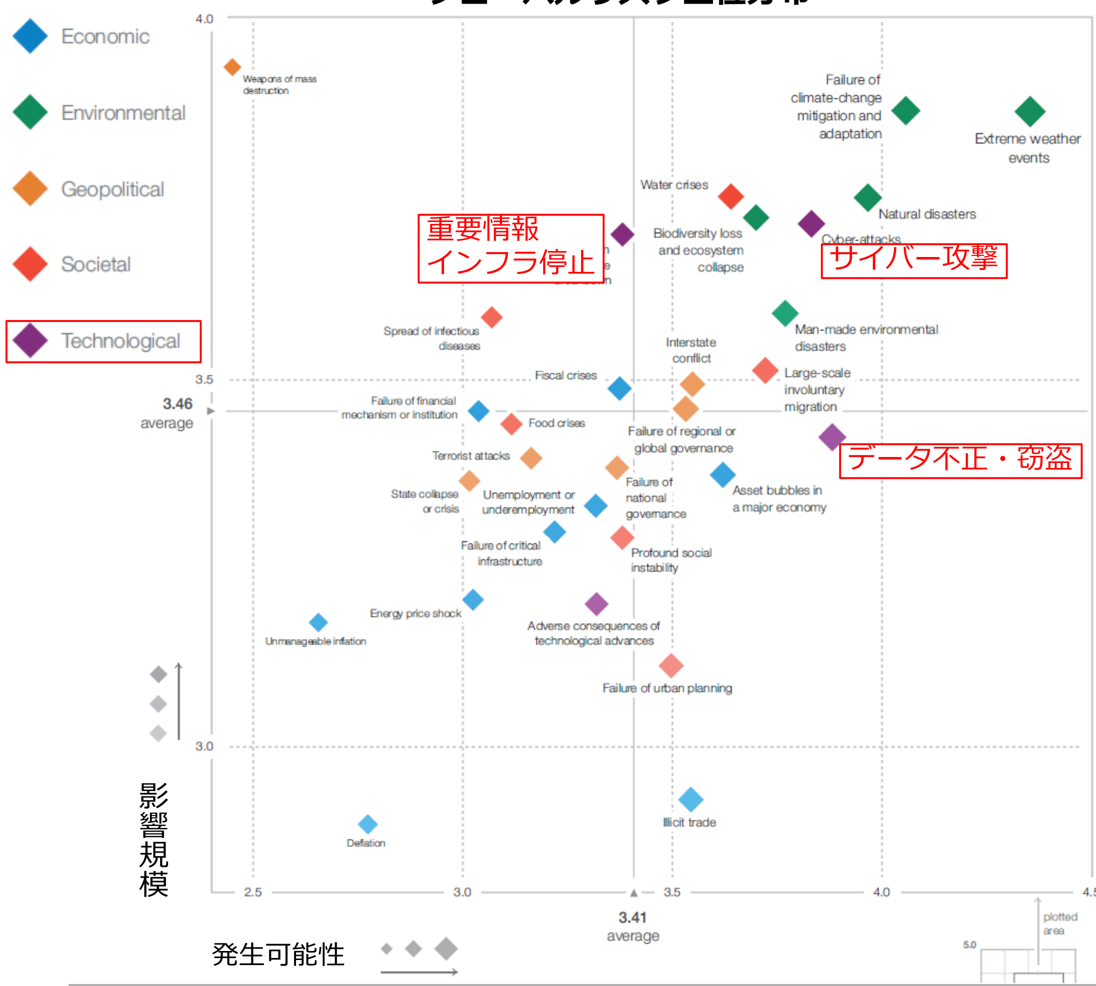
- サイバー攻撃検知・防御技術（AI・ホワイトリスト）
- セキュリティ・アシュアランス技術
- トラスト基盤とインテグリティ技術
- フォーマルメソッド
- サイバー攻撃観測・可視化技術
- DDoS対策技術
- 認証技術
- エンドポイントセキュリティ技術
- 攻撃実験検証技術
- バイオメトリクス技術
- トラステッド・コンピューティング技術
- セキュアプログラミング
- セキュアOS
- サンドボックス・仮想化
- 静的解析・動的解析
- システムアシュアランス
- 量子暗号・軽量暗号
- ブロックチェーン
- サイバーセキュリティ経済学
- 画像解析(顔認証、不審行動)、音声解析、群集行動解析

（出所）三菱総合研究所

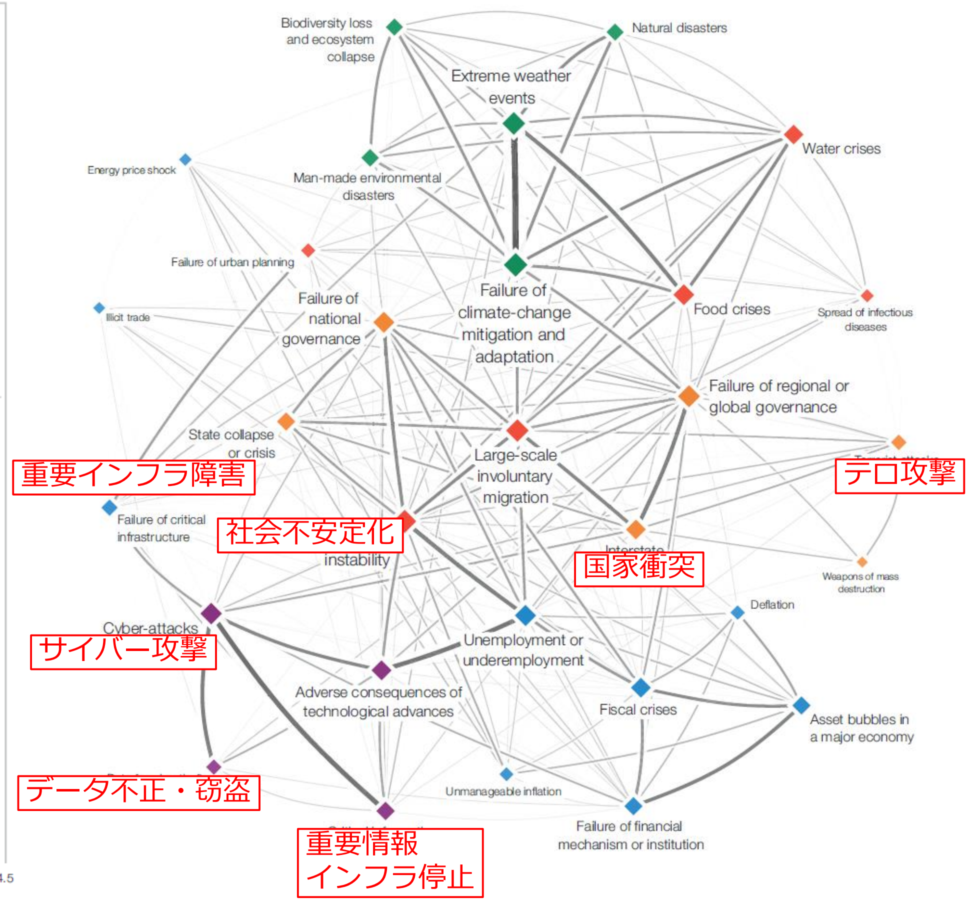
サイバーセキュリティリスクは広範な領域の中でも上位に位置付けられる

- 経済、社会、環境、技術等に渡る広範な領域におけるリスクのうち、サイバー攻撃、重要インフラの停止、データ不正・窃盗等のセキュリティ脅威は、近年、上位に位置する。
- サイバー攻撃は、社会不安定化、国家衝突、テロ攻撃に影響を与える。

グローバルリスク上位分布



グローバルリスク相互関連マップ



Global Risk＝今後10年間で大規模な損害をもたらす不確実な事象

(出所) Global Risk Report 2019, World Economic Forum

主なインシデントの俯瞰（2017年2月～8月）

- ランサムウェアWannaCry, NotPetya, BadRabbitなどによる大規模被害、重要インフラ組織への影響
- 自動車、医療機器など安全性に係わるIoT機器の脆弱性が継続的に発見される

凡例　重要インフラ　その他制御系　情報系

2月　3月　4月　5月　6月　7月　8月

DDoS
- 全米1億7千万台超のIoT機器がDDoS攻撃に利用可能
- CAN BUSプロトコルにDoS攻撃される脆弱性

マルウェア感染
- PLCルートキットHARVEYで監視情報の改ざん可能
- ランサムウェアWannaCryの世界規模の感染
- Petyaランサムウェアの亜種が世界に感染拡大
- マルウェアDreamBotが仮想通貨取引所等に攻撃

不正アクセス
- ハニーポットHoneyTrainで鉄道への攻撃を確認
- 米国防系ネットワークに侵入可能
- Bosch製機器の脆弱性によりエンジン停止等攻撃される可能性
- Cisco Linksysルータ等リモートログインできるコード
- Tesla社の自動車にリモートで操作できる脆弱性
- ネット銀行の2要素認証コードを窃取するスミッシング攻撃
- SAP社のPOSシステムに商品価格を変更できる脆弱性

インジェクション
- ブラジル大手銀行がDNSリダイレクトにより情報搾取
- gSOAPライブラリに任意のコードが実行される脆弱性
- Siemens社のCTスキャナー等の医療機器に脆弱性
- Eaton社のPLC用ソフトウェアに脆弱性が発見

標的型攻撃等
- サムスン等8社のスマートフォンにマルウェア混入
- Ireland国営送電事業者EirGridがサイバー攻撃被害
- 日本の防衛産業を標的とした攻撃キャンペーンを確認

その他脆弱性攻撃等
- Apache Struts 2にリモートコード実行可能な脆弱性
- シマンテック社のSSL証明書の脆弱性を悪用可能
- BIND9でサービスが停止する脆弱性
- 4社のペースメーカ等に8,000以上の脆弱性が発見
- MSマルウェア対策エンジンの脆弱性による大規模影響
- SMA社の太陽光発電設備に大規模停電に導く脆弱性
- Universal Robots社等の協働ロボットに安全設定を変更される脆弱性

※ 事例は、主な攻撃分類、報告日等で配置
（出所）NEDO委託調査（三菱総合研究所作成）

主なインシデントの俯瞰（2017年9月～2018年2月）

- **広範囲に影響するIT基盤部の脆弱性発見が相次ぐ：WPA2、Bluetooth等の無線プロトコル、RSAライブラリ、CPU投機機構**
- TRITON, DragonFly2.0など重要インフラへの脅威に対して米国政府(DHS/US-CERT)が公式に関係業界に注意喚起

凡例　重要インフラ　その他制御系　情報系

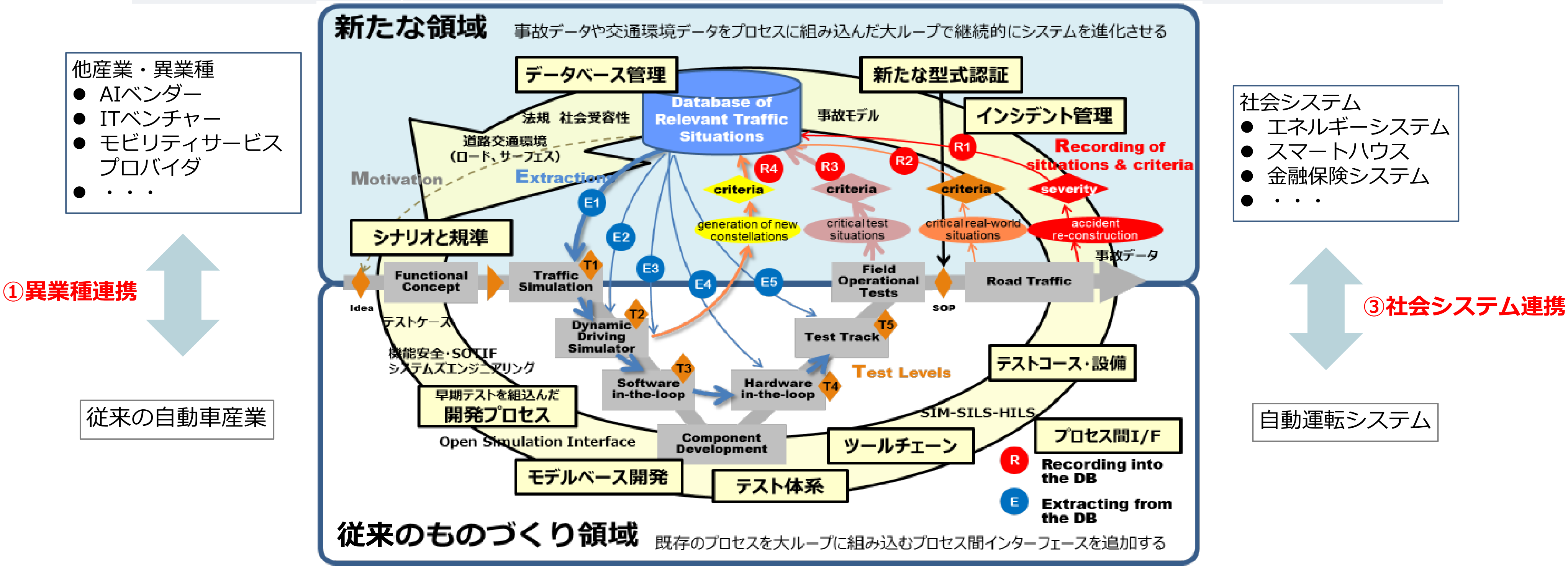
	9月	10月	11月	12月	1月	2月
DDoS		スウェーデン運輸当局のITシステムにDDoS攻撃				**キャッシュサーバmemcachedを踏み台にするDDoS攻撃**
マルウェア感染		**ランサムウェアBad Rabbitにより地下鉄機関等の影響**	google検索のSEOポイズニングによるマルウェアの拡散 MS Officeの脆弱性を悪用するマルウェアCobalt	**産業制御系フレームワークへ攻撃するTRITON**	ARCプロセッサをターゲットするマルウェアSatoriの亜種 医療機関を標的にするランサムウェアSamSamの亜種	マルウェア検出を回避できる新型ランサムウェアShurl0ckr
不正アクセス	ドイツの電子投票システムPC-Wahlに脆弱性 スマートホームInsteon HubとWink Hub 2に脆弱性 米国21州の選挙システムに不正侵入	RDPの認証情報がダークウェブで大量売買された	米Uberから個人情報5,700万件の流出を公表 **MacOS High Sierraに容易にroot権限取得できる問題** ボーイング757型機のシステムに無線通信を介して侵入	攻撃グループMoneyTakerが米露銀行から数百万ドル Intel MEの隠し機能God Modeを利用できる脆弱性 **53億台のデバイスに影響を与えるBluetoothの脆弱性** 医療情報管理システムOpenEMRに脆弱性	Oracle社WebLogicの脆弱性を利用する仮想通貨のマイニング 仮想通貨取引所Coincheckから約580億円分の仮想通貨が流出	
インジェクション	Bluetooth機器を乗っ取る脆弱性BlueBorn **Equifax社がStruts2脆弱性により大規模の情報漏洩**			データベースをターゲットするHex-Men攻撃 PLCのWAGO PFC200に脆弱性		
標的型攻撃等	**米欧重要インフラ事業者に攻撃するDragonFly2.0**		カリフォルニア州サクラメント運輸当局へのサイバー攻撃	攻撃ツールCopperfieldは中東の重要インフラを標的に		平昌オリンピック開会式のドローンがサイバー攻撃
その他脆弱性攻撃等		**Infineon社組込み用RSAライブラリの脆弱性** **無線LANのWPA2におけるプロトコル脆弱性**	**北朝鮮攻撃グループHIDDEN COBRAの活動**	Bank of America等のアプリに中間者攻撃にされうる	**Intel, AMD,ARM等のCPUの脆弱性により大規模の影響**	

※ 事例は、主な攻撃分類、報告日等で配置
（出所）NEDO委託調査（三菱総合研究所作成）

サプライチェーンの進化：パイプライン型からプラットフォーム型のエコシステムへと進化

例：製造業（自動車業界）（米国では、Critical Manufacturingは重要インフラ16分野の一つに位置付けられる）
100年に一度と言われる自動車CASE革命による変革 ①異業種連携、②スパイラル開発、③システム連携、④新しい安全性評価、に伴い運用サービス領域を含むセキュリティ脅威への対策の要求が高まっている。

観点	今後求められる新しい開発モデル
①異業種連携	自動車業界を超えた異業種のプレイヤが連携するエコシステムを前提とした開発
②スパイラル開発	開発と利用データのフィードバックによるスパイラル型開発プロセスへの対応
③社会システム連携	社会システムと自動運転システムが連携する進化型のモビリティサービスの開発
④新しい安全性評価	自動運転に対応した安全性評価、アシュアランスと社会的受容性を確保する開発手法



図：「自動走行の実現に向けた取組方針」Version2.0を元に加筆

（出所）METI委託調査（三菱総合研究所作成）をもとに作成

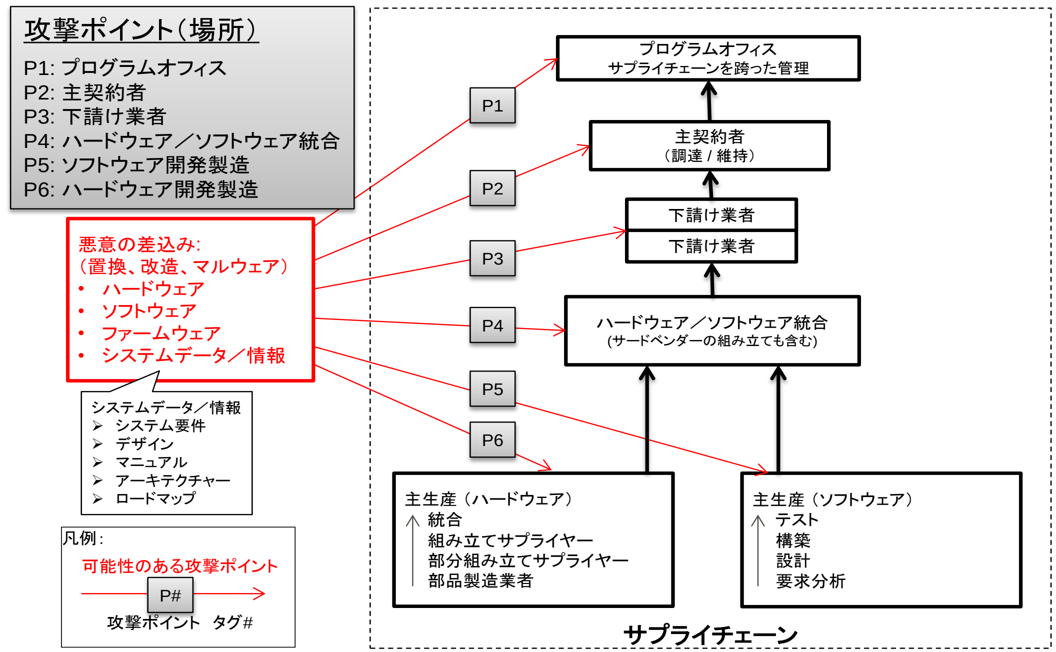
2．サプライチェーンセキュリティの動向と課題

サプライチェーンに係わるセキュリティ脅威のトレンド

- サプライチェーン、エコシステムの多様化が進み、不正コード、脆弱性混入の脅威が拡大
- IoT機器のライフサイクルプロセス全体を通じた企業間の取引関係におけるセキュリティ確保が必要

サプライチェーン脅威の典型例

- 連邦政府システムの調達における脅威
  - エネルギー省、国土安全保障省、法務省、防衛省は、調達システムに係わるサプライチェーン脅威が高い。このうち、エネルギー省、国土安全保障省は、サプライチェーンセキュリティ対策が不十分との指摘（GAO, IT SUPPLY CHAIN National Security-Related Agencies Need to Better Address Risks)
- ハードウェア・トロイの脅威
  - 集積回路に不正コードを仕込むことで、ある条件で動作し、無線発信による機密情報の漏洩などを引き起こす。組込みデバイスのハードウェアは、アウトソースされることが増え、設計仕様に準拠したハードウェアの完全性の確保が難しい。
- 供給者によるマルウェア、バックドアの仕込み
  - 開発、流通、運用時の意図的な改ざん、マルウェアの挿入
  - 納品前、納品時に偽造部品に置き換え（ENISA Supply Chain Integrity)
- サプライチェーンの弱点となる中小企業がターゲット
  - 情報漏洩全体のうち92%は中小企業による。（CERT-UK, Cyber-security risks in the supply chain）
- サードパーティ・インシデント
  - 情報漏洩全体のうち76%は、サードパーティベンダーが原因となっている(Trustwave 2012 Global Security Report)



米連邦政府システム調達におけるサプライチェーンリスクの俯瞰図
（出所:）MITRE, Supply Chain Attack Framework and Attack Patterns

政府システム調達においては、サプライチェーンにおける様々な業者間の取引において攻撃を受ける可能性のあるポイントが存在する。

（出所）NEDO委託調査（三菱総合研究所作成）

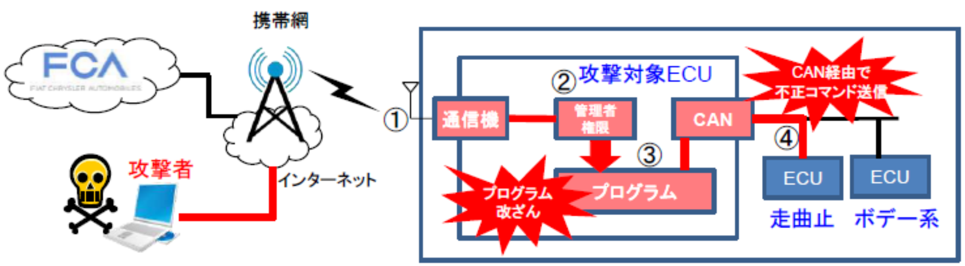
問題認識：セキュリティ・アシュアランスの必要性

- 複雑化、常に進化するマルチステークホルダー・エコシステムにおいてセキュリティの確保について説明責任が求められる。
- エコシステムにおいて、取引相手などのステークホルダーについて組織、システム、製品、サービス、データ等に関するセキュリティを客観的、合理的に確保するための仕組み（セキュリティ・アシュアランス）が必要。

コネクテッドカーへの攻撃による自動車制御の奪取

- Uconnectの脆弱性を悪用してブレーキ、ステアリング制御を奪取可能な脅威
- ソフトウェアアップデートがスムーズに進まず、140万台のリコールにまで発展。

Uconnectに対する攻撃の流れ

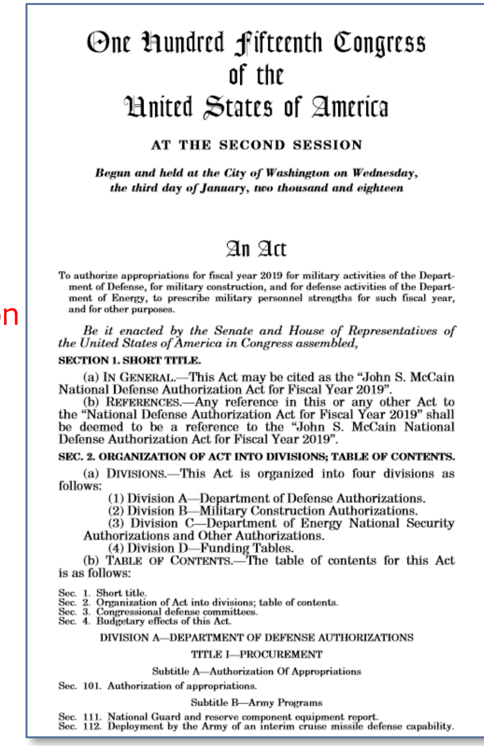


図：デンソー

① 遠隔から携帯通信網経由で攻撃対象に接続
② ECUの管理者権限を取得
③ ECUのプログラムを改ざん
④ 不正なCANコマンドを対象ECUに送信

サプライチェーンセキュリティとテクノロジー冷戦

- 米政府、Huawei等の機器排除を盛込んだ法案を可決
  H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019
  - SEC. 889. Prohibition on certain telecommunications and video surveillance services or equipment.
    (A) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation
- 日本政府「IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」
- セキュリティ・アシュアランスケース、コンフォーマンスによる説明責任が求められている。


One Hundred Fifteenth Congress
of the
United States of America

AT THE SECOND SESSION

Begun and held at the City of Washington on Wednesday, the third day of January, two thousand and eighteen

An Act

To authorize appropriations for fiscal year 2019 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

(a) IN GENERAL.—This Act may be cited as the "John S. McCain National Defense Authorization Act for Fiscal Year 2019".
(b) REFERENCES.—Any reference in this or any other Act to the "National Defense Authorization Act for Fiscal Year 2019" shall be deemed to be a reference to the "John S. McCain National Defense Authorization Act for Fiscal Year 2019".

SEC. 2. ORGANIZATION OF ACT INTO DIVISIONS; TABLE OF CONTENTS.

(a) DIVISIONS.—This Act is organized into four divisions as follows:
(1) Division A—Department of Defense Authorizations.
(2) Division B—Military Construction Authorizations.
(3) Division C—Department of Energy National Security Authorizations and Other Authorizations.
(4) Division D—Funding Tables.
(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title.
Sec. 2. Organization of Act into divisions; table of contents.
Sec. 3. Congressional defense committees.
Sec. 4. Budgetary effects of this Act.

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

TITLE I—PROCUREMENT

Subtitle A—Authorization Of Appropriations

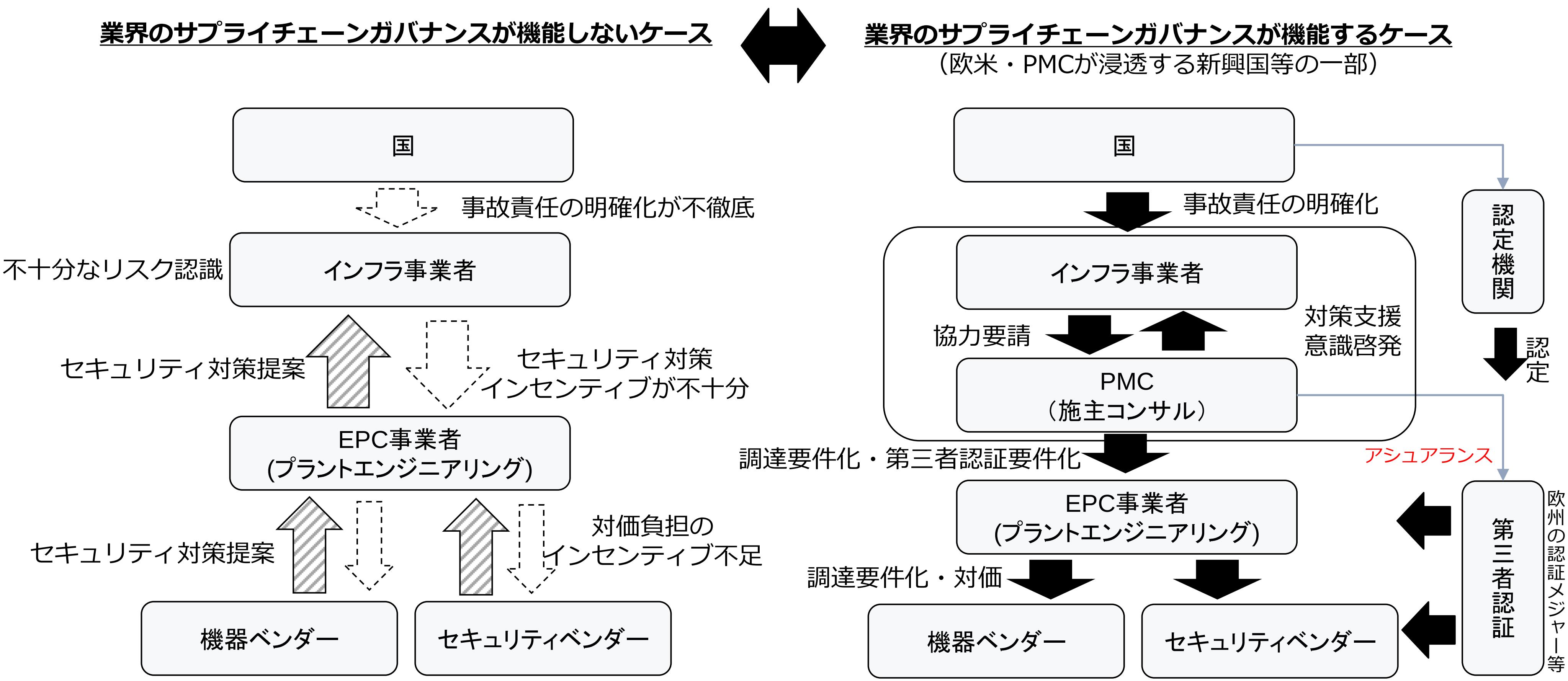
Sec. 101. Authorization of appropriations.

Subtitle B—Army Programs

Sec. 111. National Guard and reserve component equipment report.
Sec. 112. Deployment by the Army of an interim cruise missile defense capability.

問題認識：サイバーセキュリティに係わるステークホルダーのガバナンス確保が必要

- (1)インフラ事業者に対する事故責任の明確化、(2)PMCの支援によるリスク影響分析・調達要件化、(3)第三者認証によるアシュアランスの確保（適合性評価）等のサプライチェーンガバナンスの仕組み作りが不可欠



（出所）三菱総合研究所

サプライチェーン・セキュリティの取組み動向（全体像）

- サプライチェーンセキュリティは、プロダクトに対するインテグリティ確保とプロセス等に関するマネジメントに分かれる
- CNCIイニシアチブから始まりソフトウェアアシュアランス、サプライチェーンリスク管理など強化の取組みが推進されてきた

プロセス/マネジメント（プロセス/組織）　←→　プロダクト/テクノロジー（プロダクト/ツール等）

2000年

インフォメーション・アシュアランス

National Information Assurance (IA) Acquisition Policy No.11(2000)

DoD, Information Assurance Certification and Accreditation Process (2006)

2008年

NSPD54/HSPD23 Comprehensive National Cybersecurity Initiatives (CNCI) #11(2008)

NIST ICT SCRMプログラム開始(2008)

ソフトウェア・アシュアランス

IATAC/DoD, Software Security Assurance State-of-the-Art Report (2008)

DHS, Build Security In (Software and Supply Chain Assurance) (2008)

SAFECode, Software Assurance Fundamental Practices for Secure Software Development (2008,2011)

サプライチェーン・リスクマネジメント

2009年

DHS, Cyber Security Procurement Language for Control Systems (2009)

SAIC/UMD, Building A Cyber Supply Chain Assurance Reference Model (2009)

NIST, IR 7622: National Supply Chain Risk Management Practices (2011)

2012年

DHS, National Strategy for Global Supply Chain Security (2012/1)

GAO, IT Supply Chain National Security-Related Agencies Need to Better Address Risks (2012/3)

米国議会Huawei, ZTE製品排除勧告(2012/10)
米国議会レポートにより,Huawei,ZTE製通信機器のセキュリティリスク論の高まり

サプライチェーン・リスクマネジメントの補強・整備

BAH, Managing Risk in Global ICT Supply Chains (2012)

ENISA, Supply Chain Integrity (2012/11)

2013年

MITRE/DoD, Supply Chain Attack Framework and Attack Patterns (2013)

UMD, Proof of Concept for an Enterprise ICT SCRM Assessment Package (2013)

2014年

ISO/IEC 27036:2014 Information security for supplier relationships (2014)

2015年

NIST SP800-161: Supply Chain Risk Management Practices (2015)

SANS, Combatting Cyber Risks in the Supply Chain (2015)

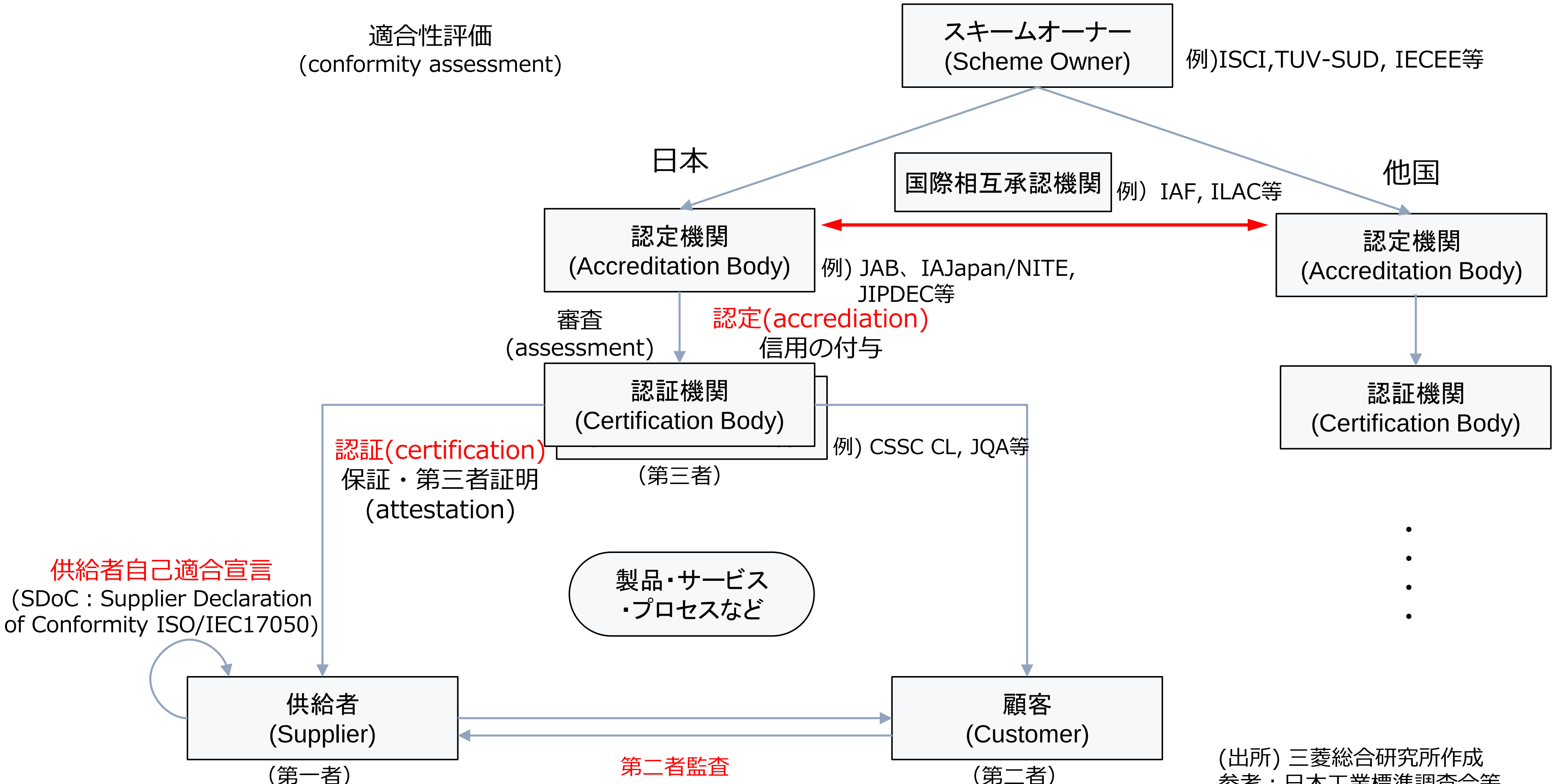
NIST SP800-171: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations (2015)

凡例　政府　民間等　注目事例（後述）

（出所）NEDO委託調査（三菱総合研究所作成）

適合性評価のフレームワークと認証スキームの国際標準（ISO/IEC17000)

- 認証は、 (1)認定機関による認証機関の認定（信用の付与）と(2)認証機関による認証対象（製品、プロセス、システム、要員等）に対する適合性の評価と第三者証明の発行、という２段階で行われる。
- 国際相互承認協定により、各国の認証制度による認証結果を認めあうことでワンストップ認証を可能にする



(出所) 三菱総合研究所作成
参考：日本工業標準調査会等

セキュリティ関連の主な認証制度の比較分析と活用アプローチ

- 米国では、インフラ相互依存の基盤となる電力分野において、NERC-CIPは、国(FERC)による強制基準(規制)となっている。
- CC, CMVPを、政府調達基準とする国は多く、国際相互承認も進んでいる。認証取得件数は増加傾向にある（付録参照）。
- EDSAなど国際的な調達要件やISMSなどサイバー保険の割引適用に認証取得が条件とされるケースもある。

区分		認証制度		スキームオーナ	基準/標準	認定機関	認証機関	国際相互承認MRA	概要
政府	任意	CSMS		(METI/JIPDEC)	CSMS認証基準 (IEC 62443-2-1相当)	JIPDEC	JQA, BSI Japan	無し	制御システムを対象としたセキュリティマネジメントシステム
		ISMS		(METI/JIPDEC)	ISO 27000シリーズ	JIPDEC	JQA, TUV Rheinland, DNV	IAFで検討中	組織の情報セキュリティに関するマネジメントシステム。セキュリティ向上と国際的な信頼向上が目的
	政府調達基準※	Common Criteria	CCEVS	NIAP (NIST,NSA)	ISO/IEC15408	NIAP	NIAP (CC testing Lab’s)	CCRA 17ヶ国	IT 関連製品(複合機、情報システム、ICカード、ソフトウェア等)の情報セキュリティ（JISEC制度 2001年創設,2003年CCRAに加盟）
			JISEC	（経産省/IPA）	ISO/IEC15408	IPA/NITE	IPA(ECSEC等)		
		CMVP	CMVP	米NIST/ 加CSEC	FIPS 140-3	NIST (NVLAP)	CygnaCom, InfoGuard等	NIST-IPA 共同認証 (2012年)	暗号モジュールの暗号アルゴリズムの実装と鍵、ID、パスワード等の重要情報のセキュリティ確保 (CMVP1995開始、JCMVP2007年正式運用開始）
			JCMVP	(経産省/IPA)	JIS X 19790 (FIPS 140-3)	IPA/NITE	IPA (ITSC, ECSEC等）		
	強制	NERC-CIP		FERC	CIP V5	FERC	NERC	無し	電力事業者等に対するサイバーセキュリティ対策
		中国CCC		国家認証認可監督管理委員会 (CNCA)	中国国家標準（GB）	CNCA	指定認証期間 (CQC等）	無し	輸入されるITセキュリティ製品、自動車関係、電気製品等の指定製品の安全確保、環境保全（中国政府調達品の自国品優遇制度の懸念あり）
民間	任意	EDSA/ISASecure		ISCI	EDSA標準 (IEC 62443-4-2 等に相当)	ANSI/ACLASS(米国)	Exida	IAF	制御システム･コンポーネントのセキュリティ確保。Wurldtech, Achiless等のツールを用いる
						JAB(日本)	CSSC CL		
		CAP		UL	UL 2900 (IEC 62443参照)	(ANSI規格になった場合、OSHA)	ULのみ	無し	ネットワーク接続型製品ならびにシステムのサイバーセキュリティ確保。Synopsisのツールなどを用いる
		TUV SUD IEC 62443 certification		TUV SUD	IEC 62443-4-1, 3-3, 2-4	—	TUV-SUD	無し	制御システムの管理、システム、コンポーネントに関するセキュリティ確保
		情報セキュリティ格付		(株)ISレーティング	マネジメント成熟度等	—	(株)ISレーティング	無し	企業や組織が取り扱う技術情報、営業機密、個人情報についてセキュリティのレベルを格付

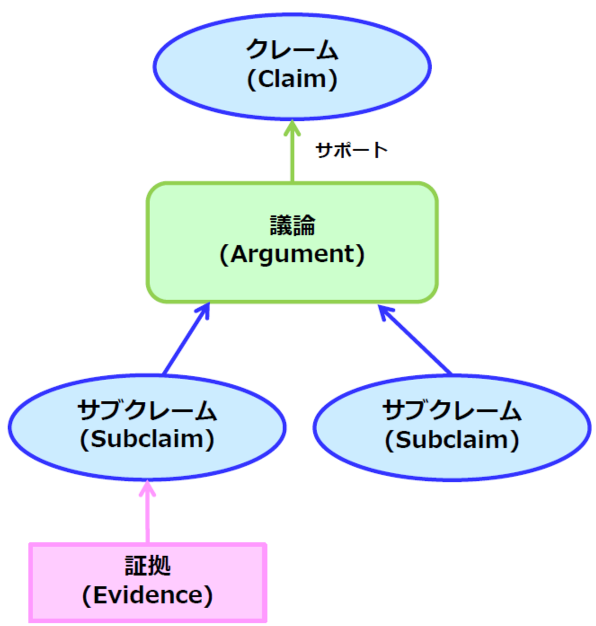
三菱総合研究所作成

※ CCは、20 か国以上で政府調達基準。日本では、NISC政府機関の情報セキュリティ対策のための統一管理基準。CMVPは、米国政府調達基準、日本ではNISC府省庁対策基準策定のためのガイドライン

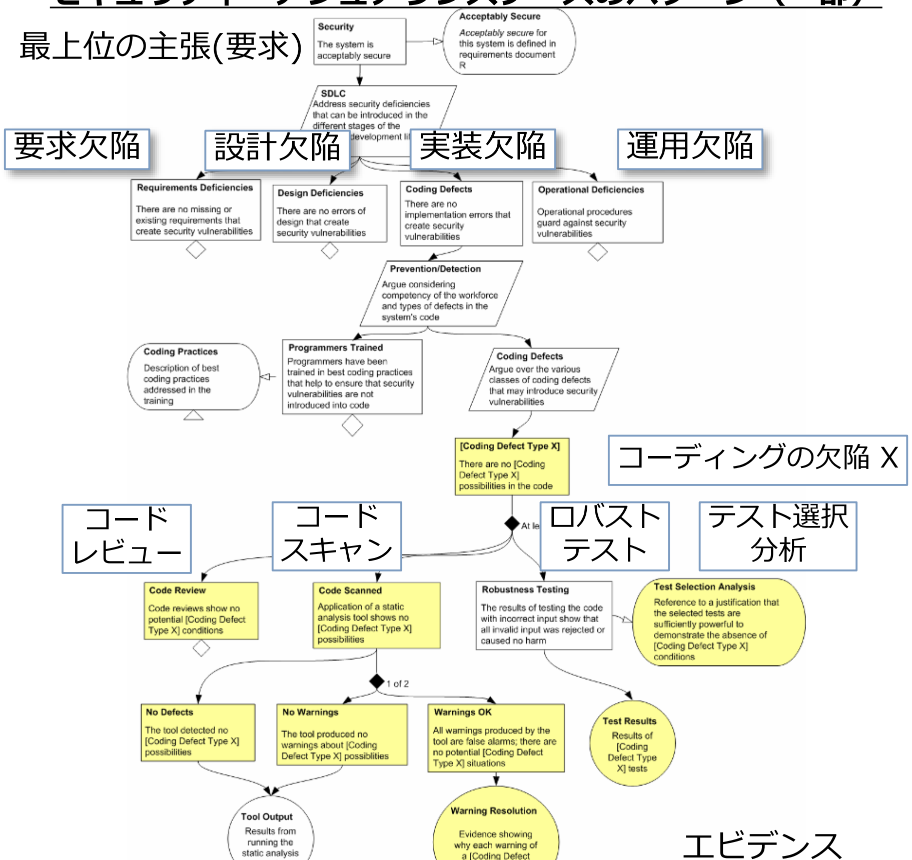
技術課題：セキュリティ・アシュアランスケースの標準パターンの必要性

- Security Assurance Casesとは、製品やサービスの提供者が、利用者や調達者など他のステークホルダーに対して、セキュリティに関する要求が満たされていることを客観的なエビデンスに基づき論理的に示すための体系（文書）である。
- 鉄道や自動車などセーフティの分野では、Assurance Case は業界標準や基準などにより要件化されているが、セキュリティ分野ではまだあまり知られていない。
- 基本構造は、主張(Claim)→論証(Argument)→証拠(Evidence)からなる。リスクと防御の構造を論理的に体系整理し、リスクコミュニケーションのツールとしても利用できる。

CAE (Claim Argument Evidence)論理の基本構造
（イギリスAdelard社、City University London）



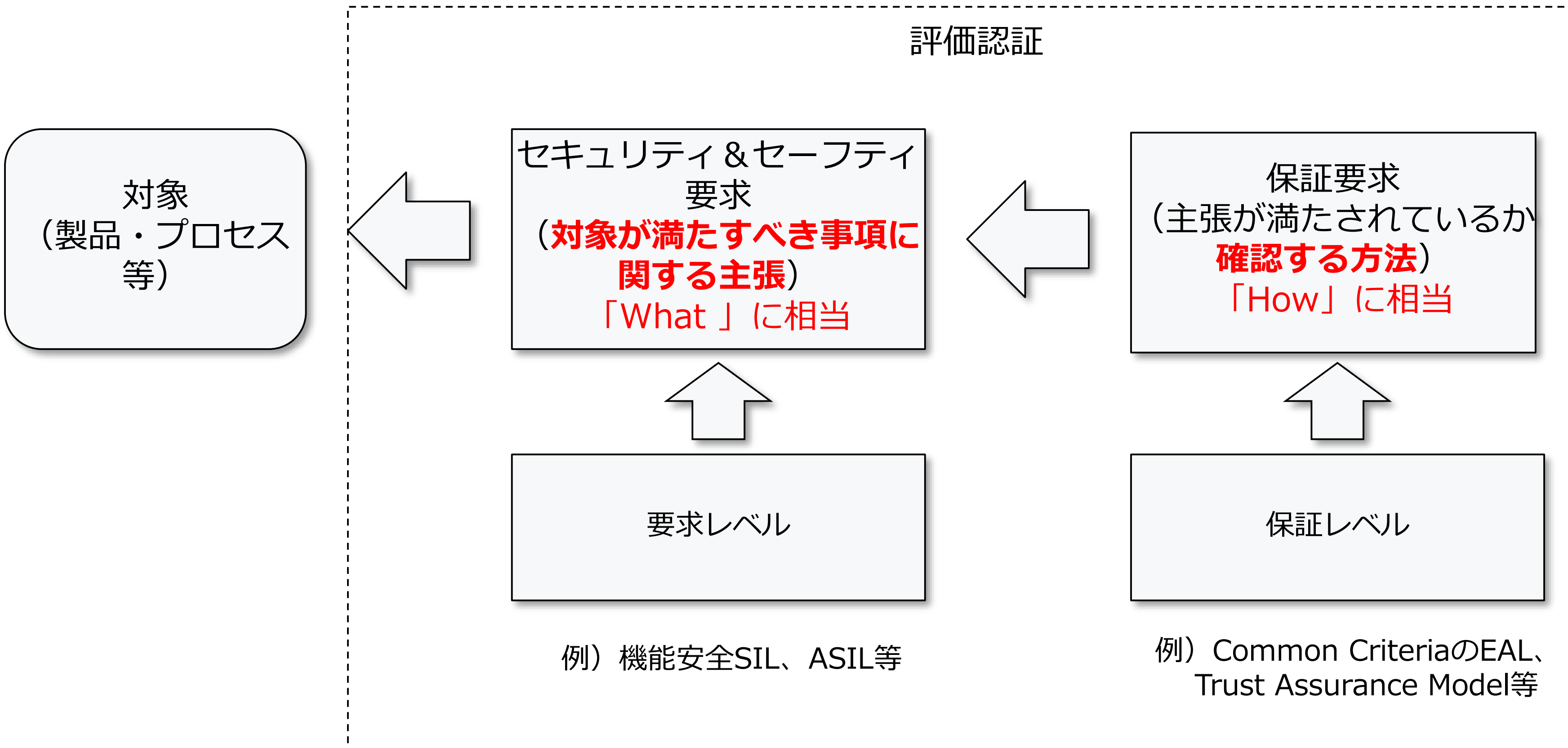
セキュリティ・アシュアランスケースのパターン（一部）



（出所）DHS Security Assurance Case

認証基準における**セキュリティ要求**vs **保証要求(アシュアランス)** の概念の違い

- セキュリティ、セーフティ等における評価認証基準においては、達成することを明確にするため要求レベルと保証レベルの概念が用いられる。
- 要求レベルは、対象が満たすセキュリティやセーフティに関する主張のレベル（Whatに相当）
- 保証レベルは、対象に関する主張が確かに満たされていることを確認するレベル(Howに相当)



出所：三菱総合研究所作成
参考： SESAMO, ISO 26262, IEC 61508, ISO 15408等

３．IoT進展におけるセーフティとセキュリティの統合リスク分析手法

IoTシステムの技術課題の全体像

※色は、目的区分（次頁参照）

● ディペンダビリティ確保、エッジとクラウドに跨る統合技術、モデリング技術の活用などが注目される。

システム上の実現レイヤー

システム区分				課題（目的ベース）			
開発運用ツール	開発環境			8. モデルベース開発による上流工程重点化による効率化	2. システムの複雑化に対応した段階的設計検証によるディペンダビリティ確保	10. 設計・実装モジュールの再利用技術	29. 実行可能モデル等による全体システムのシミュレーション
開発運用ツール	開発環境			30. 重複開発を避ける開発ツールチェーン	28. 連携システム共通のセーフティ、セキュリティ要件によるシステムの開発方法論		
開発運用ツール	運用・保守ツール			16. モデルベースの運用保守、開発へのフィードバック技術			
構成技術	要素技術	アプリケーション		1. センサーデータを複合的に活用したリアルタイム制御の高度化	26. 画像認識系技術の高度化	18. 大規模データから本質的なデータを抽出する技術	22. 生活空間で利用するIoT機器のプラットフォーム
構成技術	要素技術	アプリケーション		27.「学習済みモデル」の組込み向け活用技術	19. 機械学習による適応性・自律性の実現	24. ユーザの状況に応じた適応的なリアルタイム処理	34. 拡張現実(AR)、仮想現実(VR)を活用したUX（ユーザエクスペリエンス）の基盤
構成技術	要素技術	基盤	ミドルウェア	12. 相互接続プラットフォームによる開発の効率化	23. センサーネットワーク向けプラットフォーム	33. 人間協調型ロボットにおけるユーザインタフェース基盤	
構成技術	要素技術	基盤	OS	5. リソース制約に対応したソフトウェア技術	6. 新しいハードウェアを活用するソフトウェア技術	21. リアルタイム処理向け組込みクラウド・プラットフォーム	
構成技術	統合技術	アーキテクチャ・統合化		9. CPS/統合システムのアーキテクチャモデルの確立	11. IoT/統合システムにおけるデータと機能配置の最適化	17. IoTネットワークアーキテクチャの確立	
構成技術	統合技術	アーキテクチャ・統合化		14. IoTネットワークの問題検出・自動修復技術	25. ラピッド開発用の設計インタフェース	32. 参照アーキテクチャ上のプラットフォームと国際標準対応	
構成技術	統合技術	ディペンダビリティ セキュリティ、セーフティ、プライバシー等		3. 人が介在するシステムのディペンダビリティ確保	4. 運用データを活用した障害の検知・診断・復旧	7. 自動車通信等における信用フレームワークの構築	13. IoTネットワークの管理とセキュリティ確保の仕組み
構成技術	統合技術	ディペンダビリティ セキュリティ、セーフティ、プライバシー等		15. セーフティとセキュリティの統合手法の確立	20.ソフトウェア脆弱性の自動管理 と自己治癒	31. 制御のロバストネスの確保	

（出所）三菱総合研究所作成（NEDO委託調査）

IoTシステムに係る技術開発の方向性

環境変化と課題・ニーズ

安全安心に係る脅威の拡大

- セキュリティ脅威により安全性に影響を与えるインシデント
  コネクテッドカーの脆弱性により走行制御を遠隔操作可能に
- セーフティとセキュリティの重複対応の無駄
  共通する概念や取組みが重複し、コスト増大
- 機器の多様化、セキュリティ・リテラシーの違い
  コンシューマ、事業者などリテラシーが大きく異なる。

開発から運用へのフォーカス

- 有益な運用データの未活用
  運用データは開発・運用の最適化のための宝の山
- フォーマルメソッド導入の敷居とコスト
  スキル、工数などが高く、先端技術の導入が困難
- 下流工程まで不具合が残留することによる手戻りコスト
  上流で検証できず、不具合が下流まで残留する。

機械学習等の技術的ブレイク・スルー

- ディープラーニングによるブレークスルー
  画像認識処理で飛躍的な向上が繰り返し達成
- ルールベースのリアルタイム・アルゴリズムの発見
  連想記憶に基づく高速なルール処理アルゴリズムが実現
- スパースコーディング等の技術進歩
  膨大なデータから本質的な少数のデータを抽出可能に

新しいハードウェアの登場

- マルチコア/メニーコア、GPGPU、FPGA等の進歩
  最新のハードウェア活用による機器のイノベーション
- 電力、計算能力、コストなどリソースの制約と多様性
  限られたリソース制約のもとで無駄な処理の回避が必要

今後の研究開発の方向性

新たなディペンダビリティの仕組み（技術課題3,16,20等）

- セーフティとセキュリティの統合化手法の確立
  共通する対策、手法の統合化により、対策と認証を効率化
- ソフトウェア脆弱性の自動検出と自己治癒技術
  自己治癒型セキュリティにより多様なIoT機器ユーザのセキュリティを確保
- 人が介在するシステム(HITL)のディペンダビリティ確保
  人のミスを防止、リカバリーにより安全・安心の確保

モデルに基づく開発と運用のイノベーション （技術課題2,8,16等）

- モデルを活用した上流工程重点化技術（フロントローディング）
  燃焼系など物理モデルの精度向上により効果が飛躍的に高まる
- モデルベース運用保守(MBO&M)※4と開発へのフィードバック技術
  運用フェーズや開発フェーズへのフィードバックにモデルを活用
- フォーマルメソッドのスケーラビリティ向上技術
  段階的設計・検証やライトウェイト化により、手法の適用分野を拡大

エッジ・インテリジェンスの実現 （技術課題1,19,26等）

- センサーデータを複合的に活用したリアルタイム制御
  複合イベント処理をリアルタイムで実現するための基盤開発
- 機械学習によるエッジ搭載型の自律・適応処理基盤
  エッジ搭載型のディープラーニングによる自律的な機能の実現
- 機械学習による画像認識系の高度化による付加価値創出
  自動車衝突防止など画像認識系を活用した制御の高度化

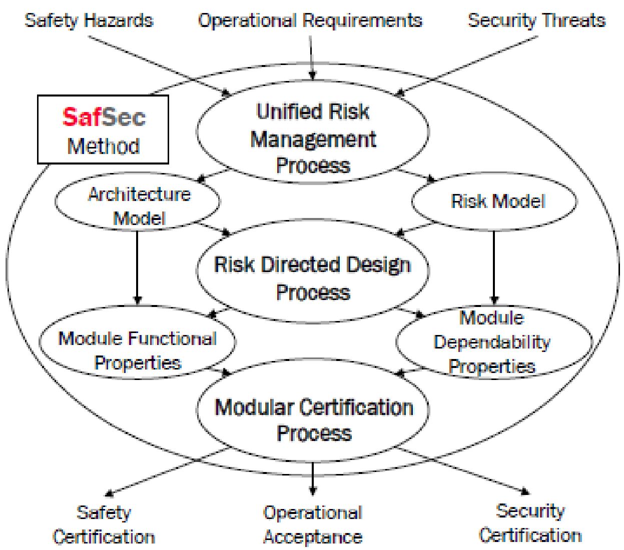
ソフトウェア・デファインド・デバイスによる柔軟性確保（技術課題5,6,31等）

- 新しいデバイスを活用するソフトウェア技術
  マルチコア/メニーコア、GPGPU、FPGA等に対応した柔軟なソフトウェア
  ソフトウェアによるデバイスの抽象化と柔軟性の確保
- リソース制約に対応したソフトウェア技術
  電力等のリソース制限に応じて、動的にソフトウェアを選択し実行する。

（出所）三菱総合研究所作成（NEDO委託調査）

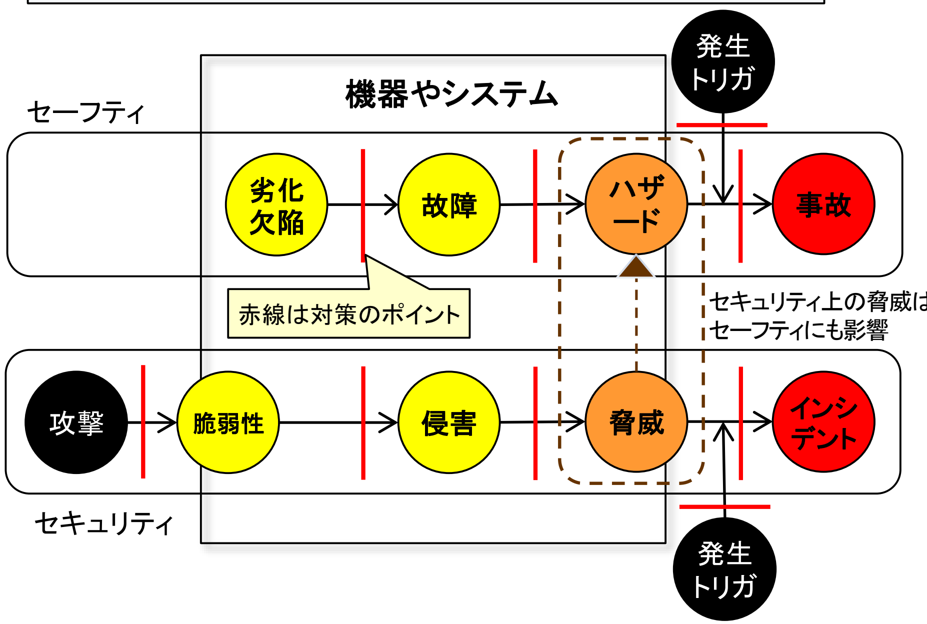
セーフティとセキュリティの統合化アプローチ

- SafSec（英国）：既存の安全規格(Def Stan 00-56)とセキュリティ規格(コモンクライテリアISO/IEC 15408)の共通部分を統合化し、効率的にセーフティとセキュリティの対策と認証取得を実現する。
- SESAMO（EU）：セーフティとセキュリティ・エンジニアリングのベストプラクティスを統合したプロセスを目指した設計評価手法。アーキテクチャレベルのセーフティとセキュリティの統合により生じる根本原因に対処する。



出所：SafSec: Commonalities Between Safety and Security Assurance

SESAMOアプローチの特徴：
- セーフティとセキュリティの統合的な分析手法
- セーフティとセキュリティを実現する構成的な手法
- セーフティとセキュリティ・メカニズムの相互依存性を低減し、統合的にそれらの性質を保証する
- セーフティ＆セキュリティ・クリティカル・システムにおいて、包括的な設計手法と統合的な分析手法を活用したツールチェーン



出所：英国RSSB「The Yellow Book」及びSESAMOプロジェクト「SECURITY AND SAFETY MODELLING FOR EMBEDDED SYSTEMS」を基に作成

セーフティとセキュリティの概念対応表

セーフティ	セキュリティ	SafSec（統合手法）
SIL(要求レベル)	EAL（保証レベル）	アシュアランス要求
FTA, FMEA	脅威/脆弱性分析	原因分析
セーフティ・ケース	ST（セキュリティ・ターゲット）	ディペンダビリティ・ケース
安全要求	セキュリティ・オブジェクト	ディペンダビリティ要求
ハザード	脆弱性	ロス
頻度×深刻度	頻度×深刻度	リスク

【参考】情報処理学会誌　特集「IoT時代のセーフティとセキュリティ」

編集にあたって

石黒正揮（(株) 三菱総合研究所　社会 ICT イノベーション本部）
細野　繁（日本電気 (株)）
後藤厚宏（情報セキュリティ大学院大学）

自動車，産業機器，社会インフラなどさまざまな分野において IoT (Internet of Things) を活用して生み出される価値に注目が集まっている．**IoT を活用した新しいビジネスモデルにより，既存のモノ（製品）やサービスが新たに「再発明」され，産業にイノベーションをもたらしている．**たとえば，自動車とスマートフォンの位置情報（GPS 等）を活用し，配車（タクシー等）の利用者と提供者をリアルタイムにマッチングするライドシェアサービスなど，海外を中心に既存の産業を変革するビジネスが多数登場している．

IoT が急速に進展する中で，「モノ」の制御にともない生じる人身の安全性（セーフティ）への影響や，異なる分野の機器のネットワーク接続により生じるセキュリティの脅威などのリスクの拡大が問題となっている．従来から**セーフティとセキュリティの技術は，それぞれ独立に発展してきたため，セーフティとセキュリティの分野間で技術，人材，文化のギャップは大きい．セーフティとセキュリティの両面に渡る専門家は国際的にまだ少なく，**双方の統合的なテクノロジーの開発は黎明期にある．**これからの IoT の発展に向けて，セーフティとセキュリティの統合的なアプローチの確立は不可欠となっている．**

本特集では，IoT の進展に伴い生じるセーフティとセキュリティの新たなリスクや問題点とその対策にかかわる方法論や取組みに焦点をあて，最新動向や今後の展望についてまとめる．

そのために，**セーフティとセキュリティの両面に渡り①研究（アカデミア），②産業界（インダストリ），③政府（ガバメント）の分野を網羅するように特集を組んでいる．**

「**1. IoT の進展に伴うセーフティとセキュリティのリスクと課題**」では，先端研究にかかわる田口氏に，セーフティとセキュリティの両立に関する課題と解決アプローチという視点で，解説いただいた．セーフティとセキュリティは，ときには互いに相反する状況が生じる場合もあり，双方を満足するシステムを開発するためのアプローチと今後の展望を示している．

「**2. 機能安全と制御セキュリティの標準化動向**」では，プラントなどの産業制御システムに関するセーフティ（機能安全）とセキュリティの国際標準化活動にかかわる神余氏に，同分野における問題認識や標準化の経緯・動向および今後の取組みの方向性について考え方をまとめていただいた．安全制御システムの開発および運用にあたっては，セーフティとセキュリティの要求を同時に達成しなくてはならないが，セーフティとセキュリティのリスク分析を同時に実施することは難しく，その実現（対策）が競合する場合もある．このような点を示しつつ，日本が提案国となり検討を進めている IEC TR 63069 などをもとに，セーフティとセキュリティに跨る用語，コンセプト，ライフサイクルなどに関する内容をまとめていただいた．

「**3. 自動車分野のセーフティとセキュリティの動向と展望―自律走行の実現に向けて―**」では，自動車制御システムの研究開発に取り組む松原氏，倉地氏，高田氏に，情報処理の観点から，同分野におけるセーフティとセキュリティに関する現状と今後取り組むべき課題やその方向性について概説いただいた．自動車を取り巻く環境は，特定のシステムのみとつながる閉じた利用環境（クローズドシステム）だけでなく，さまざまなシステムに繋がる開かれた利用環境（オープンシステム）を前提とするパラダイムシフトが起きつつある．このような環境における課題や対策について今後の展望を示している．

「**4. 社会インフラストラクチャを支える制御システムにおけるセーフティとセキュリティ**」では，社会インフラシステムにおける制御システムのディペンダビリティやセーフティとセキュリティの国際標準化活動に取り組む金川氏，山田氏に，セーフティとセキュリティの重要概念や双方を満たす有望なアプローチについてまとめていただいた．制御システムの特徴であるリアルタイム性，信頼性，拡張性の要求を示し，「フェールセーフ性」などのセーフティの重要概念や制御システムセキュリティの特徴と対策の動向についてまとめ，セーフティとセキュリティの両立のために有望なアプローチとして，デザインダイバーシティ（多様性）とフォルトトレランスをサイバーセキュリティに広げたアプローチを示している．

「**5. 政府におけるセーフティとセキュリティの取組み**」では，政府におけるセーフティとセキュリティにかかわる取組みについて結城氏にまとめていただいた．ここでは，IoT システム導入において，利便性，セキュリティ，安全性をバランスよく達成することが重要であるとの認識のもとに，政府による取組みとして「安全な IoT システムに関する一般的枠組み」について取り上げ，(1) 新しい課題への挑戦であることを踏まえた考え方の体系化の必要性，(2) 安全や品質といった我が国の強みを持って世界に貢献，(3) IoT システムにおいて「当初からつながる前提で進める」ことの必要性などの考え方や基本原則を示し，IoT システムの発展に向けた方向性を示している．

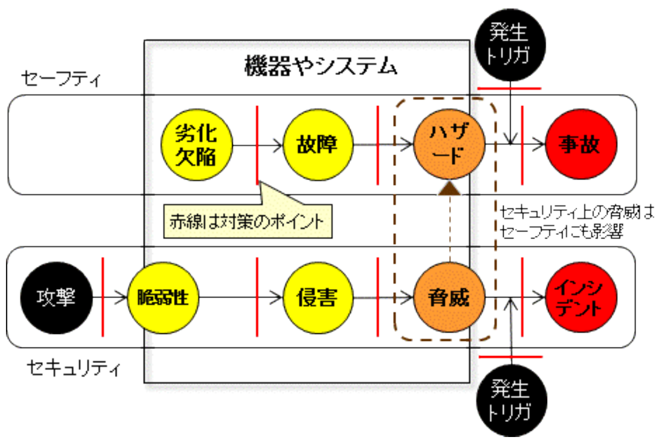
「**6. 重要インフラにおける取組みと展望**」では，重要インフラにおけるセーフティとセキュリティの研究開発にかかわる後藤氏が同分野の問題認識と今後の方向性についてまとめた．重要インフラのセーフティとセキュリティに関する問題認識や概念について整理し，それらに対して現在進められている国家的な取組みの考え方と展望についてまとめている．重要インフラにおいては，従来から安全性，安定性，一貫性の要求は高く，それらにセキュリティ脅威への対応を加えた総合的な対策アプローチに関する考え方と今後の展望についてまとめている．

IoT の進展に伴いセーフティとセキュリティが影響しあうことで生じる問題は，近年顕在化してきたものである．それらに対して求められる新たな解決アプローチの確立は，これからの IoT の普及発展に向けた必要条件となる．本特集により，IoT にかかわるさまざまな分野において，セーフティとセキュリティの確保にかかわる技術開発や取組みが進展し，IoT の普及拡大に寄与することを期待したい．

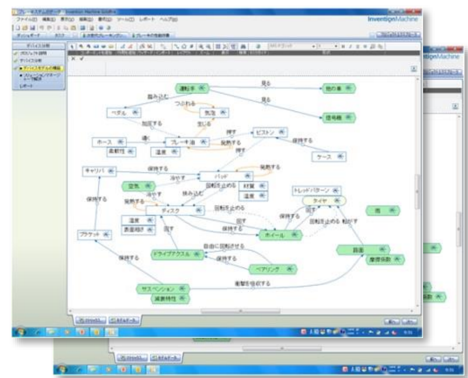
(2017 年 8 月 21 日)

技術課題：セーフティとセキュリティの統合リスク分析手法の開発

問題・ニーズ	● 自動車等のセーフティに係る機器がネットワークにつながることで、人命に係る脅威が拡大 ● セーフティとセキュリティのリスク分析の統合手法の確立していないため、 →　セキュリティ脅威に起因するセーフティの確保ができない
技術課題	● セーフティ・ハザード分析とセキュリティ脅威分析の共通概念の対応関係から、統合的に分析するフレームワークを開発する。また、リスク分析、脅威検知、自動回復の統合プラットフォームを開発する ● セーフティとセキュリティの同時認証可能な国際標準化活動を推進
有効性	● 自動車分野では、ネットワーク化、自動運転により産業構造変化が進む中で、セーフティとセキュリティは競争力の中核 ● 日本の強みである組込システムの品質・信頼性を生かし、日本の弱みであるセキュリティを補強し、組合せることで、市場競争力の向上に大きく貢献できる
取組み主体	● 国が音頭をとり、ベンダーが協調して、手法とツールプラットフォームを開発する

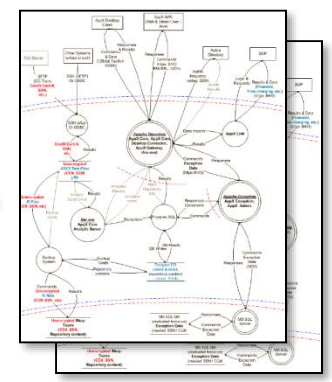


セーフティとセキュリティの概念の共通化



セーフティ分析手法・ツール
（FTA, FMEA, HAZOP等）

未統合



セキュリティ分析手法・ツール
（AttackTree, STRIDE等）

統合化

出所：英国RSSB「The Yellow Book」及びSESAMOプロジェクト「SECURITY AND SAFETY MODELLING FOR EMBEDDED SYSTEMS」を基に作成

セーフティ・セキュリティ統合化手法＆
ツールプラットフォーム

（出所）三菱総合研究所作成

セキュリティ対策区分と国内外の機関の取組み事例（概観）

凡例：導入済み　開発中　課題

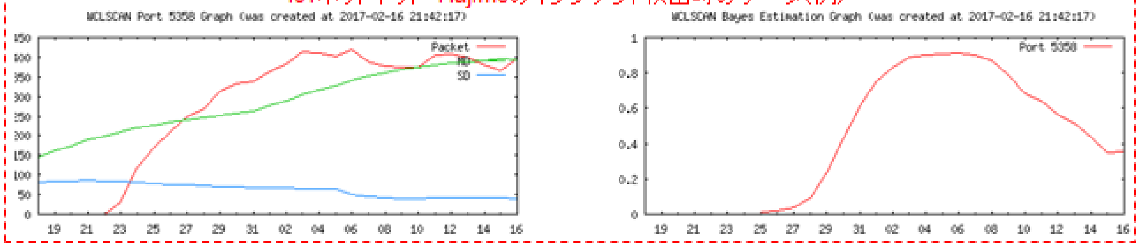
	セキュリティ対策区分（ISMSベース）	具体策の例	主な取り組み		
			SIP第1期(2016～2019)	国内	海外（電力、自動車、鉄道等）
	情報セキュリティのための方針群	セキュリティポリシー策定、情報資産管理、文書管理等	(b4-2) 事前対策立案等	JNSA情報セキュリティポリシーサンプル	
	情報セキュリティのための組織	組織体制、セキュリティ委員会の設置、契約の管理等	(b4-1) 事業継続等	METI/IPAサイバーセキュリティ経営ガイドライン	
	人的資源のセキュリティ	教育、研修、サイバー演習等	(b4-1) 情報共有プロセス等の人材育成、知識スキル (b4-2) インシデント対応人材	NISC, METI, CSSCサイバー演習 総務省CYDER、IISEC/JPCERT/MRIセキュリティ教育カリキュラム	
	資産の管理	情報資産の分類、媒体の取り扱い、資産の管理等		JIPDEC ISMS適合性評価 MRI/東大/METI インシデント損失額評価	WESI Cybersecurity Economics
技術的対策	アクセス制御	ID管理・認証、VPN,リモートアクセス環境、特権管理、PKI基盤等		NTT IDベース認証鍵交換	TCG TPM 2.0 Automotive-Thin、C2C-CC認証、Cisco ASA Firewall VPN
技術的対策	暗号	文書暗号化、署名、鍵管理策、乱数生成等	(a4-1) 楕円曲線暗号によるリソース制限への対応 (a4-2) 乱数アルゴリズムの実装検証	NTT 秘密計算アルゴリズムの高速化	ENCS CPS低リソース暗号、AUTOSAR CSM
技術的対策	物理的および環境的セキュリティ	入退室管理、バイオメトリクス、監視カメラ、記憶媒体の管理等		東北大　ディープラーニング顔認証	
技術的対策	運用のセキュリティ	マルウェア対策、フィルタリング、改ざん検知、検疫、DLP	(a1)真正性・完全性検証、(a3)ホワイトリスト (b4-1)評価検証人材	ACTIVEマルウェア対策、 NII マルウェア分類	
技術的対策		ログ監視、SIEM、運用ソフトウェア管理、バックアップ、運用の手順及び責任	(a2)動作監視による異常検知・バックドア検知	MRI/CSSC ICSイベント相関分析、 横国大 IoTマルウェアDDoS攻撃分析	INLハイブリッド侵入検知、Cyber Kill Chainリアルタイム管理・脅威検知、Thales 脆弱性分析可視化ツール
技術的対策	通信のセキュリティ	FW、IDS/IPS、WAF、UTM、インターネット観測、ポリシーアクティビティ管理	(a2)IoT機器監視ゲートウェイ	WCLSCAN(MRI)ベイズ脅威分析、JPCERT TUBAME, NICT NIRVANA改	DOE広域管理レジリエント・ネットワーク、NERC CIP データダイオード、UMTRI Safety Pilot
技術的対策	システムの取得、開発および保守	ソースコード解析、ファジング、セキュアプログラミング、ペネトレーションテスト		MRIバッファーオーバーフロー解析ツール IPA セキュア・プログラミング講座	Wurldtech Achilles Test Platform, ADSC FMVEA分析手法, SAE J.3061
技術的対策		脆弱性管理、脆弱性対策、アップデート	(b2)情報共有プラットフォーム(b3)評価検証環境	JPCERT/IPA早期警戒パートナーシップ	
技術的対策	サプライヤーセキュリティ	供給者の管理、供給者との合意、ICTサプライチェーンセキュリティ	(b1)認証制度に要件検討(a1)完全性・真正性検査	CSSC認証ラボラトリーEDSA認証、JIPDEC CSMS認証	MITRE/DoDサプライチェーン攻撃パターン, Reliability Standard CIP-013-1, DARPA TRUST program, TCG TPM 2.0 Automotive-Thin, NIST SP800-161
技術的対策	情報セキュリティインシデント管理	インシデント情報の共有と管理、評価、インシデント対応	(b2)情報共有プラットフォーム(b4-2)インシデント対応人材育成	JPCERTインシデント対応・国際連携	DOE CEDS Realtime Forensics, WESI Cybersecurity Economics, Auto-ISAC, ENISA相互依存性解析
技術的対策	事業継続マネジメント	事業継続管理、冗長性確保		METI事業継続計画策定ガイドライン	
	遵守	法的及び契約上の要求事項の遵守、情報セキュリティのレビュー	(b1)認証制度の要件検討		EU General Data Protection Regulation

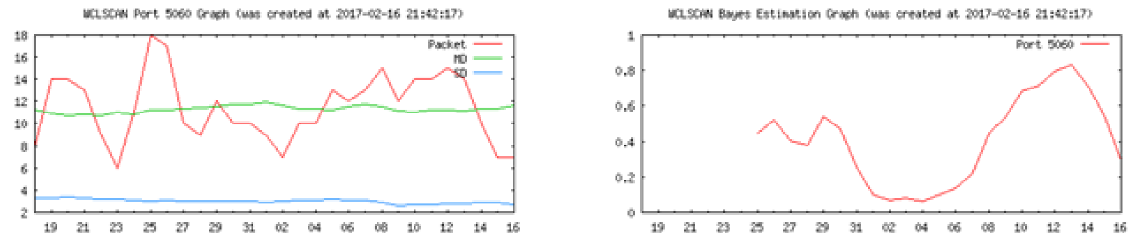
三菱総合研究所作成

インターネット脅威検知システム　(WCLSAN/三菱総合研究所/早稲田大学)

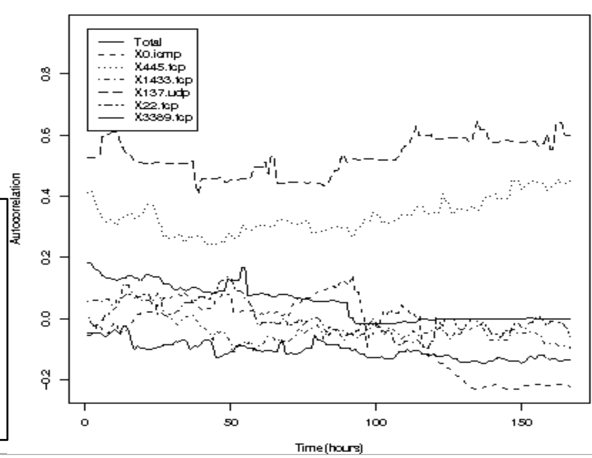
- 攻撃観測データ分析により新型IoTボット Hajime, Mirai等の脅威検知を実現する基盤を構築・運用中
- インターネット上の国内外に通信観測センサーを設置し、不正パケットのパターンや変化から攻撃検知、脅威検知を行う。

IoTボットネット　Hajimeのインシデント検出時のデータ(例)

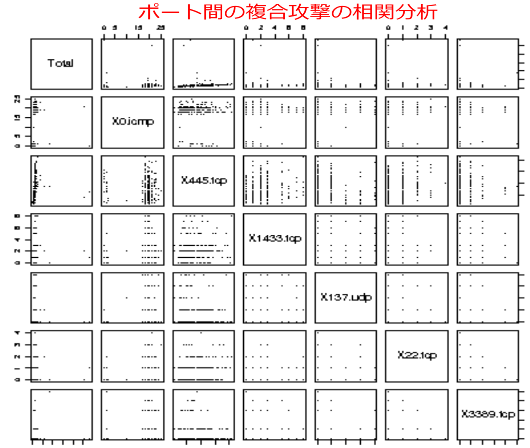




ポートの攻撃履歴の相関分析



ポート間の複合攻撃の相関分析



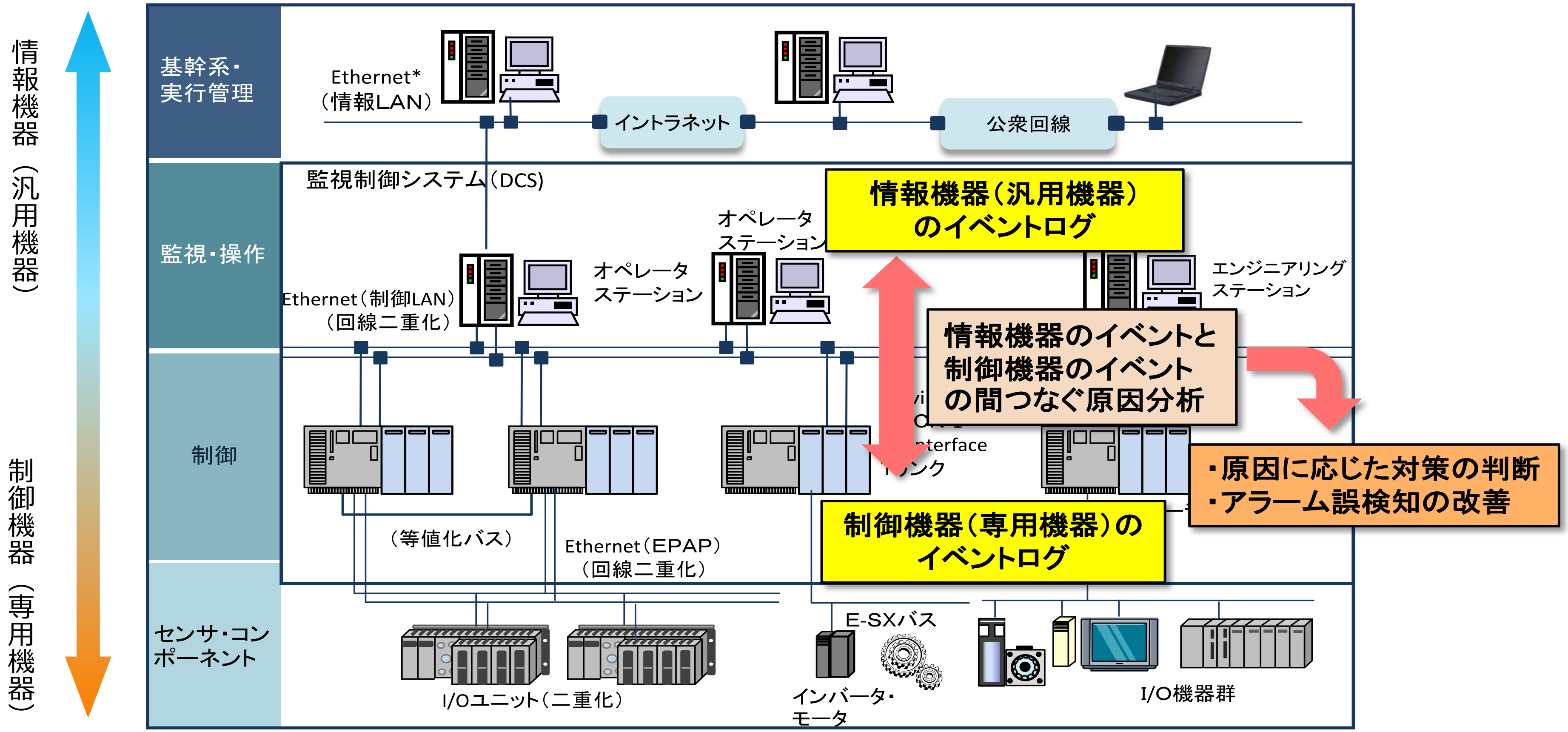
【参考】世界のインターネット脅威分析システム

1999年～　MRI ／WCLSCAN※
2001年～　SANS Internet Storm Center
2002年～　CAIDA Network Telescopes
2003年～　Symantec DeepSight
2003年～　JPCERT/CC
2004年～　警察庁@police

※Masaki Ishiguro, Hironobu Suzuki, Yoichi Shinoda, Ichiro Murase, Shigeki Goto, An Internet Threat Evaluation Method based on Access Graph of Malicious Packets, 19th Annual FIRST Security Conference, June 2007.

制御システムネットワークにおけるセキュリティ・イベント相関分析(MRI/CSSC)

- ●従来、制御システムにおけるログ分析は、制御機器のログを対象としたアラーム分析が中心で、IDSやWindowsなど情報機器におけるセキュリティイベントとの関係を把握できなかった。
- ●制御機器のログだけでなく、セキュリティイベントを含む情報機器のログを対象にイベント関係を追跡しインシデントの原因分析を行うことにより、原因に応じた対策の判断や誤検知の解消に役立てることができる。
- ●制御システムを対象としたIDSの攻撃検知ルールはあるが、それらはネットワークの深層に侵入する一連の攻撃イベントを広域的に追跡することが困難である。

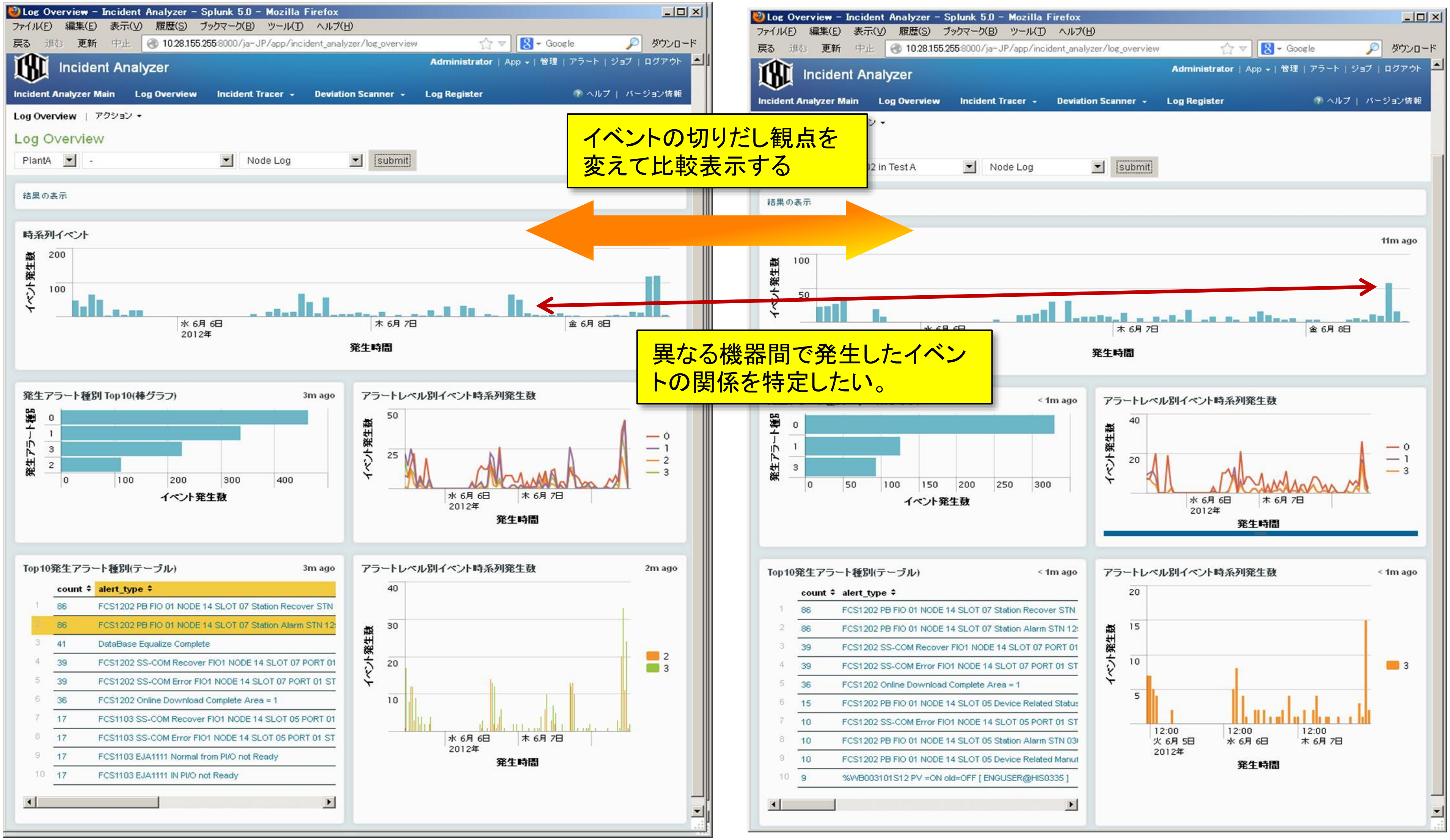


図：制御システムの構成とイベント分析の課題　　富士時報 Vol84.No4.2011を元に三菱総合研究所作成

(出所)インシデント分析機能を備えた仮想化されたサイバーセキュリティテストベッドの研究開発、制御システムセキュリティセンター（三菱総合研究所作成）

制御システムネットワークにおけるセキュリティ・イベント相関分析(MRI/CSSC)

- 分析対象機器（ホスト）、イベントタイプなどを選択し、イベントの発生状況を可視化



(出所)インシデント分析機能を備えた仮想化されたサイバーセキュリティテストベッドの研究開発、制御システムセキュリティセンター（三菱総合研究所作成）

４．サイバーセキュリティ経済学

サイバーセキュリティの本質的な問題とサイバーセキュリティ経済学を通じた解決の必要性

対策投資のインセンティブを低下させる要因

セキュリティ分野の市場の失敗
（＝セキュリティ対策投資に関して適正な市場メカニズムが働かない状況。）

■ **外部不経済**
マルウェア感染等で踏み台としてDDoS攻撃に悪用される場合など、セキュリティ投資を行うものと、被害を受けるものがずれている（取引者以外に悪影響を与える）ため、対策投資のインセンティブが働かない。

■ **情報の非対称性**
ウィルス対策ソフトのように提供者と購入者の技術知識に差がある場合、ソフトの価値が適切に評価されず、適正な対価を払うインセンティブが働かない。

■ **無形資産に対するリスクが過小評価**
セキュリティ事故における復旧対策、システム停止により逸失利益など直接被害以外に、信用失墜、顧客離れによる将来に渡る収益減少に伴う企業価値（無形資産）の毀損が評価されないため、対策投資額も過小となる。

■ **リスク認知のバイアス（Cognitive Bias）**
行動心理学によれば、人間は「不確実な損失」を過小評価する傾向があるため、対策投資額が過小となる。

サイバーセキュリティ経済学を通じた対策

市場の失敗においては政府の取組みが不可欠

政府関与	正のインセンティブ	負のインセンティブ
低	政府調達基準、ベンチマーク、表彰制度、推進団体設立	法的責任制度、脆弱性報奨金制度
中	標準化、政府R&D、免責特権、認証、格付け、実証事業、補助金	事故報告開示義務化、強制保険、総括原価方式の賦課金
高	税額控除	規制、罰則金

■ **リスク定量化**
無形資産を含む企業価値毀損額の定量評価

■ **インシデントデータベース**
リスク定量化、製品性能の評価のためにインシデントデータを蓄積しリスク定量化の研究に役立てる。

■ **アシュアランスケース（利用者、第三者に対する可視化）**
セキュリティ対策を利用者、第三者に客観的・合理的に可視化する。

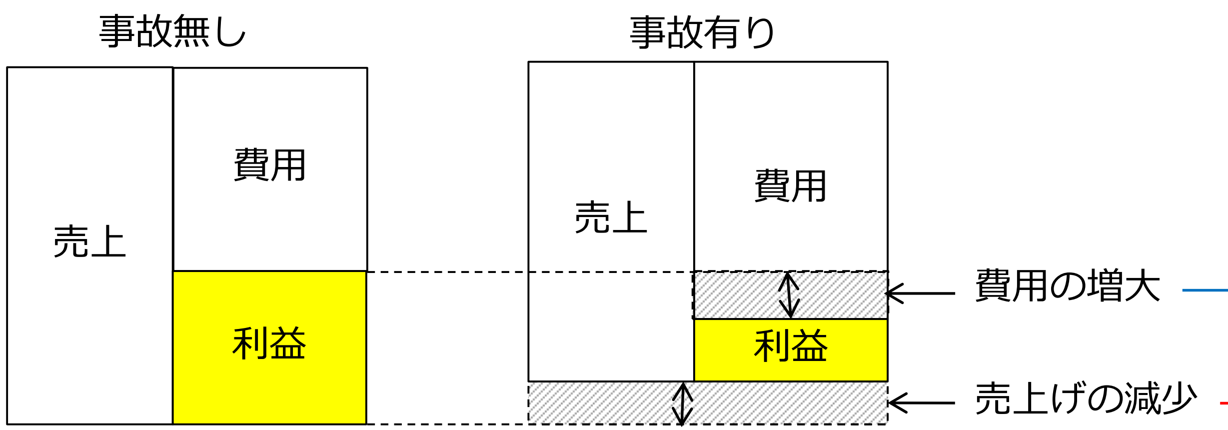
■ **セキュリティ保険**
事故発生可能性が非常に低く、発生時の損害影響が極めて大きい場合、セキュリティ保険によるリスク移転も検討

（出所）三菱総合研究所　石黒正揮

セキュリティ・インシデントに関わる損失額評価の対象範囲

- 損失額は、インシデントに関する直接的影響と波及的影響からなる。
- 直接的影響、波及的影響は、それぞれ費用の増大と売上の減少の要因に分けることができる。
- 波及的影響のうち売上の減少は、長年に渡り影響が続き、評価が難しい。

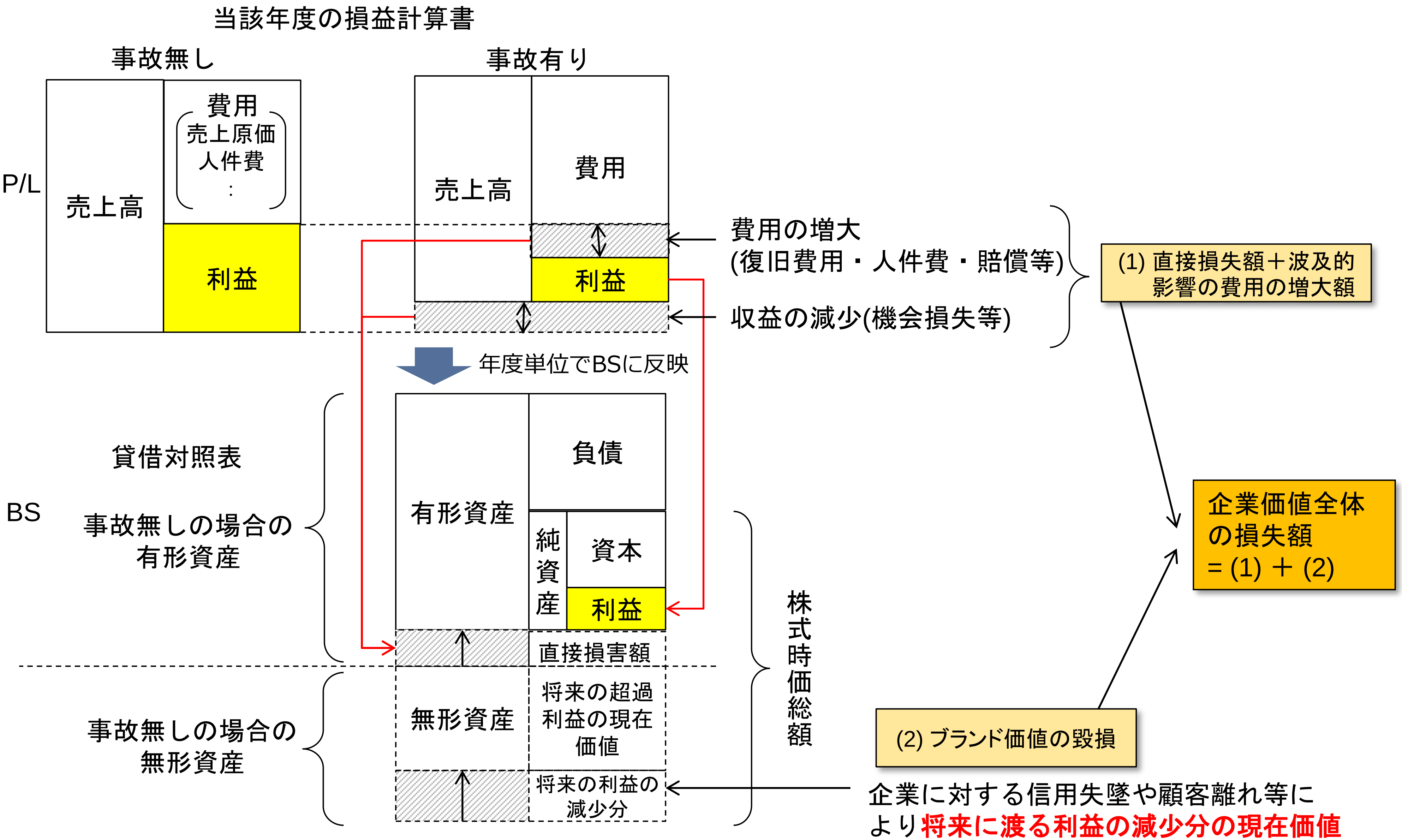
損益計算書



損害タイプ	影響タイプ	
	直接的影響	波及的影響(間接的影響)
費用の増大	● 原因究明・システム復旧 ● データ破壊・流出 ● 顧客対応 ● 補償、損害賠償、お見舞金 JNSA	● 信頼回復のための広報 ● 訴訟費用 ● 体制強化
売上の減少	● システム停止、業務中断 ● 機会損失 Ponemon (cyber Impact)	● ブランド価値毀損(顧客離れ、信用失墜) ● 風評被害 三菱総合研究所/東大/経産省、 CSIS

（出所）三菱総合研究所作成

サイバーセキュリティ事故の損失額の評価対象範囲の関係（会計学的な整理）



（出所）三菱総合研究所、IPA被害額調査委員会　講演

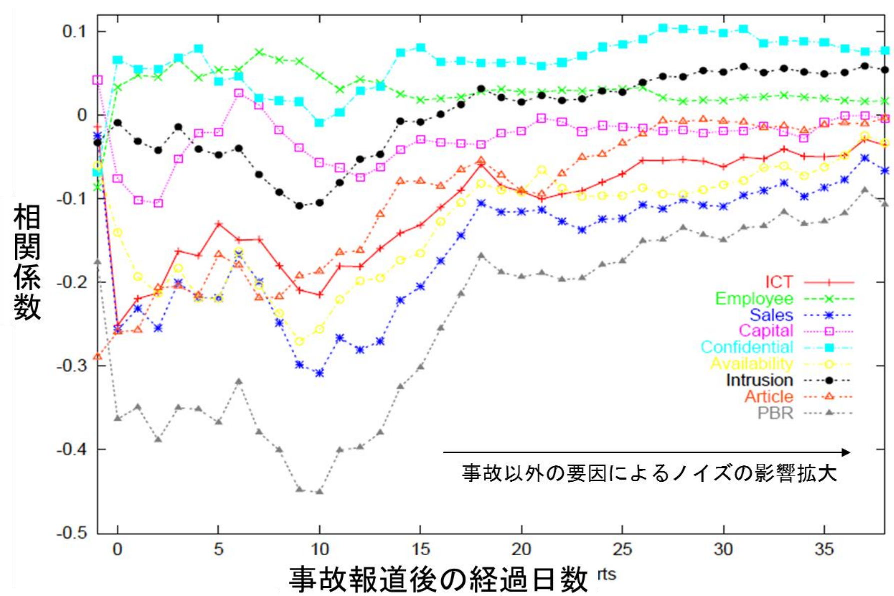
サイバーセキュリティ事故による企業価値の毀損額に関する評価(MRI/東京大学)

- 株式市場における企業価値の分析手法（CAR）をベースとした事故による企業価値毀損額の評価
- 復旧コスト等の直接損失だけでなく、将来に渡る顧客離れ・収益減少等のブランド価値を含む企業価値全体の影響評価
- 事故70件を対象に分析したところ、特定の事故種別や業種で、統計的に有意な評価が可能（有意水準5%(信頼度95%)
- PBR(株価資産倍率), 業種(小売、ICT企業等)、事故種別(機密情報漏洩、不正アクセス）の影響が大きいことを定量的実証
- 三菱総合研究所が機密情報漏洩事故を起した場合の企業価値毀損額は、11 億円（期待値）、2.5 億円（95%信頼上限）（2006年時点、上場前）と試算

説明変数と目的変数の関係の有意性検定

	属性	標本数	有意確率	t 統計量	検定力	標本平均	標本標準偏差	上側信頼限界
	事故属性区分							
事故種別	機密漏洩	28	0.0175	-2.2194	0.0001	-0.0225	0.0536	-0.0052
事故種別	業務障害	6	0.0939	-1.5248	0.0014	-0.1092	0.1754	0.0351
事故種別	不正アクセス	27	0.0486	-1.7202	0.0004	-0.0318	0.0961	-0.0003
	企業属性区分							
	資本占有率	49	0.1634	-0.9906	0.0044	-0.0176	0.1245	0.0122
	社員数	28	0.0618	-1.5897	0.0007	-0.0176	0.0585	0.0013
業種	全業種	70	0.0801	-1.4195	0.0011	-0.0189	0.1116	0.0033
業種	銀行	30	0.2854	-0.5733	0.0137	-0.0137	0.1314	0.0270
業種	サービス	4	0.0385	-2.6500	0.0001	-0.0489	0.0369	-0.0055
業種	電気機器	3	0.0254	-4.2685	0.0000	-0.0231	0.0094	-0.0073
業種	情報・通信	5	0.2161	-0.8726	0.0084	-0.0846	0.2167	0.1220
業種	その他金融	11	0.0960	-1.3990	0.0016	-0.0307	0.0727	0.0091
業種	小売	4	0.8616	1.3262	0.2726	0.0261	0.0394	0.0725
	報道属性区分							
	報道影響力	50	0.0628	-1.5586	0.0007	-0.0194	0.0879	0.0015
	株価推定属性区分							
	決定係数	27	0.1950	-0.8743	0.0063	-0.0078	0.0462	0.0074
	DW 系列相関	48	0.2817	-0.5820	0.0133	-0.0098	0.1167	0.0185

事故発生後の要因変数の相関変化



(出典)

[1]石黒正揮（三菱総合研究所）、情報セキュリティ事故等による企業価値に与える影響　2012年11月12日 （独立行政法人情報処理推進機構 被害額調査委員会 講演資料）
[2] Masaki Ishiguro, Hideyuki Tanaka, Kanta Matsuura, Ichiro Murase, The Effect of Information Security Incidents on Corporate Values in the Japanese Stock Market, Workshop on the Economics of Securing the Information Infrastructure（WESII 2006)
[3] 石黒正揮（三菱総合研究所），松浦幹太（東京大学），田中秀幸（東京大学）、村瀬一郎（三菱総合研究所），情報セキュリティ対策による企業価値向上に関する影響分析、暗号と情報セキュリティシンポジウム2009（2009年1月21日）

Gordon-Loebサイバーセキュリティ投資評価モデル

- セキュリティ投資により低減できる損失額と投資額の関係についてモデル化
- セキュリティ投資により低減できる損失額から投資額を引いたものを最大化する額が最適投資額と定義
- 典型的なケースについて潜在的な最大損失額の36%以上のセキュリティ投資は過剰であると主張(投資効果が頭打ちとなり、投資に見合った効果が期待できなくなる)

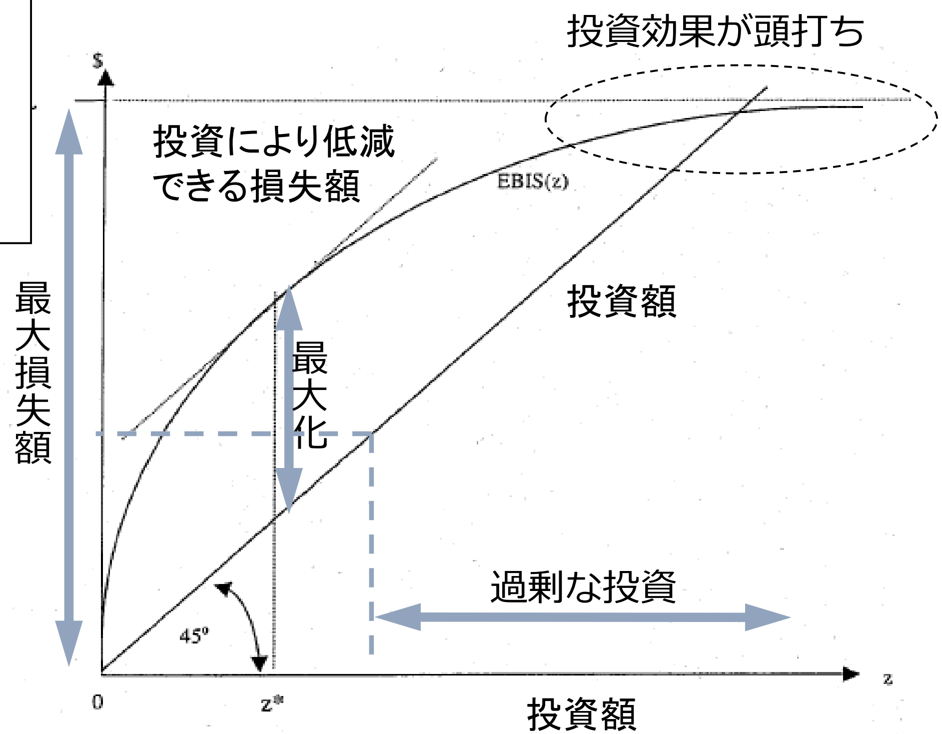
（投資による正味利益の期待値）

＝（投資により低減できる損失額）－（セキュリティ投資額）

＝{（投資前の事故確率）－（投資後の事故確率）} ×
（攻撃の発生確率）×（事故時の最大損失額）－（セキュリティ投資額）

＝ {v – S(z, v)} t λ – z

ただし、
v ：投資前に攻撃を受けた場合に事故につながる確率（脆弱性）
t ：攻撃が発生する確率
λ ：事故が発生した場合の最大損失額
z ：セキュリティ投資額
S(z, v) ：投資額z、脆弱性vにおいて攻撃を受けた場合に事故につながる条件付確率



(出典) The Economics of Information Security Investment by L. A. Gordon et al.

サイバーセキュリティのグローバルリスクの規模評価

- サイバーセキュリティインシデントによる潜在的損害リスクは、国や世界の経済全体では無形資産を含め数十兆円を超える規模に達する
- ブランド価値等を含む波及的影響は損失全体のうち大きなウェートを占める

評価主体	対象分野	一企業あたり		経済全体	
		直接的影響	全体（波及的影響を含む）	直接的影響	全体（波及的影響を含む）
RISI Database	世界・産業制御システム分野	損失額が11億円を上回る事例は6%(28年間)			
Ponemon (Cyber Crime)	世界7ヶ国・全産業	平均年間コストは、公共・エネルギーが14億円(2015年)			
JNSA	国内・全産業	一件当りの個人情報漏えい平均想定損害賠償額3.4億円(2015年)		想定損害賠償総額2541億円(799件、496万人)(2015年)	
Ponemon (Cyber Impact)	世界37ヶ国・全産業		SCADA等のサイバーリスクの予想最大損失額の平均は約712億円(2015年)		
CSIS	世界・全産業				個人情報窃盗による世界経済の損失は年間53兆円(2013年)
AFCEA	米国・全産業				経済的影響110兆円(2008年)
三菱総合研究所/経済産業省	国内・全産業				国内上場企業の不正アクセス、機密情報漏えいの損失リスク29兆円(2007年)

2017, 三菱総合研究所作成

技術課題：リスク評価のためのインシデントデータベース

- リスク評価に基づき適切にセキュリティ対策を実施するためにインシデントデータの蓄積が必要
- 匿名化されたインシデントデータを業界で共有し、企業のリスク管理者及び保険会社がサイバー脅威のトレンドの特定やサイバーリスクの評価が進めば、適正なセキュリティ投資が促進される。

米国DHS/CISAのインシデントデータベースCIDARの要点

（Cyber Incident Data and Analysis Database）

- サイバーインシデントのリスクを評価するためはインシデントデータの蓄積が必要。
- サイバーセキュリティ保険市場の活性化は、セキュリティ対策の度合いに応じた保険料設定により、様々な予防措置やセキュリティ対策が促進される。
- CIDARには、攻撃の種類、重大性、インシデントの時系列、攻撃者の目的、要因、特定の制御障害、危殆化された資産、検知・緩和手法、攻撃による被害額を含まれる。
- 企業のサイバーリスクを算定するために十分なデータを収集するには、10～15年の期間を要する見込み
- サイバーインシデントデータリポジトリCIDARの構築は、セキュリティインシデントや犯罪戦術のパターン研究にも資する

米国DHS/CISAのインシデントデータベースのPJサイト

【参考】情報処理学会誌　特集「デジタルエコノミー時代のサイバーセキュリティ」

特集
Special Feature

ディジタルエコノミー時代のサイバーセキュリティ
―ディジタルトランスフォーメーション促進の基盤確立に向けて―

編集にあたって

石黒正揮 (株) 三菱総合研究所　細野　繁 日本電気（株）　手塚　悟 慶應義塾大学

産業, 経済, 社会のさまざまな領域で進展するディジタル化によるビジネスモデルの変革（ディジタルトランスフォーメーション）は新たな価値を生み出す一方で, 新たなセキュリティの脅威や問題をもたらしている.

今日のディジタル化の潮流は, ビジネス構造の変革を伴うもので, 数十年前から始まった従来のIT化の流れとは一線を画している. 実世界の機器などからなるフィジカル空間と情報システムやインターネットなどからなるサイバー空間がデータ連携により融合し, 異なる分野の組合せによるイノベーションを誘発している. また, 業界の枠内でのディジタル化にとどまらず, ベンチャーや他業界など従来の業界の枠を越えた連携・協業によるサプライチェーン・エコシステムの拡大が進んでいる.

さまざまな機器がネットワークに繋がることでシステム的な攻撃ポイントが増えるとともに, サプライチェーン・エコシステムの拡大に伴い組織的に脆弱なポイントが増え, システムと組織の両面でセキュリティのリスクが高まっている.

このようなことから, 本特集では, サイバーとフィジカルが融合する新しいディジタルエコノミーの進展に伴い, 従来のサイバーセキュリティでは対応できない脅威や課題について取り上げ, それらに対する取り組みや今後の方向性について展望する.

本特集内の「サイバーセキュリティ経済学―インセンティブの適正化を通じたサイバーセキュリティの確保―」でも示す通り, サイバーセキュリティは産官学の連携による包括的な取り組みが不可欠であることから, 本特集では, インダストリ（産）, ガバメント（官）, アカデミア（学）のステークホルダの協力を得てとりまとめることとした.

本特集の構成は以下のようになっている.

(1) ディジタル化とデータ活用により進化する社会インフラセキュリティ

宮尾健氏, 谷本順一氏により, データ活用にかかわる社会インフラ（インフラストラクチャ）の脅威とセキュリティ対策の方向性を取り上げていただいた. 製造機器や情報システムが繋がることで進化するサイバーフィジカルシステムにおける脅威に対して, サイバーBCP（事業継続性計画）のうち技術面に焦点を当て, アセット管理とディジタルエビデンスと呼ばれる対策を挙げ, サプライチェーンを構成する組織群や社会全体のニーズと課題を整理している.

(2) 国際連携を踏まえたトラストサービスとトラスト基盤

手塚悟により, 超スマート社会（Society 5.0）における信頼の連鎖の確保について取り上げた. サプライチェーンにおいて生まれるさまざまなサービスの安全性を保証するための技術として,「トラストサービス」と「トラスト基盤」の重要性を挙げている. また, 米国, EUにおける関連する取り組みを概観し, 国際連携の重要性を示している.

(3) サプライチェーンサイバーセキュリティの強化に向けて―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策定―

奥家敏和氏にサイバーフィジカルセキュリティ対策フレームワークについて解説いただいた. 異分野間のシステム連携・協調が進む中で, 製品・サービスを生み出す工程（サプライチェーン）の変化と脅威について取り上げ,「企業間のつながり」を捉える第1層,「フィジカル空間とサイバー空間のつながり」を捉える第2層, そして「サイバー空間におけるつながり」を捉える第3層という3つの層に分けたフレームワークとしてセキュリティ対策の指針を示している.

(4) IoT機器の普及とサイバーセキュリティ政策

谷脇康彦氏にIoT機器にかかわるサイバーセキュリティ政策について執筆いただいた. データがリアル空間とサイバー空間を循環しながら社会課題の解決につなげていくデータ主導社会において, リアル空間において急激に増加する多様なIoT機器のセキュリティ水準を引き上げるボトムアップアプローチや機器間でリスクが波及するリスクの連鎖を回避する仕組みについての政策を解説いただいた.

(5) フィンテックのセキュリティ

岩下直行氏にフィンテックにかかわるセキュリティの問題認識についてまとめていただいた. 従来の伝統的金融の枠組みを越えて進展するフィンテックのうち, 仮想通貨のセキュリティ事故を経て, 金融機関のシステムとセキュリティに対するスタンスと管理体制について問題を提起している.

(6) AIをセキュリティリスクから守るために―AIへのサイバー攻撃とその対策―

古澤一憲氏にAIにかかわるセキュリティの新たな課題と対策の方向性についてまとめていただいた. AIの有用性が示される一方で, 悪意を持った攻撃を受けた場合には一転して大きな危険にさらされる可能性がある. AIのリスクに関する内外の議論を紹介するとともに, AI特有のサイバー攻撃手法を分類し, それらに対する対策の考え方やアプローチについてまとめている.

(7) サイバーセキュリティ経済学―インセンティブの適正化を通じたサイバーセキュリティの確保―

石黒正揮が, サイバーセキュリティ対策投資にかかわる問題と取り組みアプローチについて解説した. サイバーセキュリティ分野においては, 技術だけでは解決できない, インセンティブにかかわる本質的な問題がある. その問題に対するアプローチとして, 経済メカニズム, 人の行動モデルなどの観点から問題の解決を目指すサイバーセキュリティ経済学について解説し, 今後の展望を示す.

本特集で紹介したサイバーセキュリティに関する包括的な取り組みが, サイバー空間とリアル空間が融合する異業種連携におけるセキュリティと安全性を確保し, ディジタルトランスフォーメーションを促進することを期待したい.

(2018年9月24日)

5．技術課題の整理

- **セキュリティ・アシュアランスケース**
運用フェーズを含むエコシステムの複雑化、進化に対応したサプライチェーンセキュリティとして、エビデンスに基づく客観的、論理的な説明体系であるセキュリティ・アシュアランスケースの標準パターン開発、事例開発が重要

- **セーフティとセキュリティの統合リスク分析手法**
セーフティのハザードリスク分析とセキュリティ分野の脅威リスク分析を統合的に行い、セキュリティ脅威に起因するセーフティの毀損を含む統合リスク分析手法の開発が必要

- **産業分野ごとのシステムに最適化した脅威検知手法**
産業分野ごとのシステムリソース、環境などに応じて動作し、本番系のシステムに影響を与えない分野に最適化された脅威検知手法が必要

- **サイバーセキュリティ経済学**
企業価値に基づく損害額を適切に評価できるリスク評価モデルの開発、インシデントデータに基づくリスク評価の適正化をおこなうために、インシデントデータベースを構築し、匿名化により広くセキュリティ対策に活用する。

株式会社三菱総合研究所

住所　〒100-8141　東京都千代田区永田町2-10-3

組織　株式会社三菱総合研究所
社会ＩＣＴイノベーション本部
サイバーセキュリティ戦略グループ

石黒　正揮，Ph.D.　masa@mri.co.jp

TEL：03-6858-3578