経済産業省

日本を取り巻くサイバー攻撃に対する経済産業省の取組

経済産業省
サイバーセキュリティ・情報化審議官
伊東　寛

自己紹介

【主な履歴／経歴】

1978年3月 慶応義塾大学工学部電気工学科卒
1980年3月 慶応義塾大学大学院修士課程修了
1980年4月 陸上自衛隊　入隊
2007年3月 退職（1等陸佐）
2007年4月 （株）シマンテック総合研究所　入社
2010年6月 株式会社ラック　入社
　　特別研究員
2011年4月 執行役員　サイバーセキュリティ研究所長
2013年4月 常務理事　ナショナルセキュリティ研究所長
2016年5月 経済産業省　サイバーセキュリティ審議官

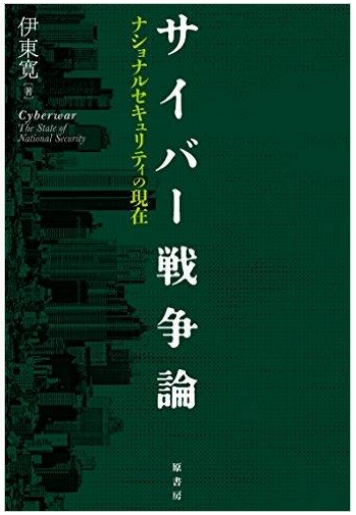
＜趣味＞
戦術、歴史、SF

＜特技・資格＞
工学博士、陸上自衛隊特級射手

＜論文等＞
サイバー攻撃及び安全保障に関する論文多数

＜著書等＞
- 「第5の戦場　サイバー戦の脅威」 祥伝社
- 「究極の危機管理」 安全保障危機管理学会
  （共著）
- 「サイバー・インテリジェンス」 祥伝社
- 「サイバー犯罪から身を守る30の知恵」 並木書房
  （共著）
- 「サイバー戦争論」 原書房

等



最近の日本に対するサイバー攻撃の趨勢

2015.6

	年金機構事件の前	年金機構事件の後	2015年末以来
被害者	民間企業	公的機関	中央省庁
攻撃の内容	技術資料等の窃盗	個人情報等の窃盗	業務妨害？
手段	標的型攻撃	標的型攻撃	DoS攻撃
公表	ほとんどされない	されることが多い	されることが多い

2015.11 厚生労働省
2016.02 金融庁、国税庁

最近は、被害者民間企業、対象個人情報になったようにも見える

サイバー攻撃の脅威

- IT利活用拡大とともに、サイバー攻撃の脅威も増大。
  －サイバー攻撃の事案は増加傾向
  －攻撃の手口が巧妙化
  －政府関係機関や企業への標的型サイバー攻撃（※）により、個人情報や重要技術等の情報が漏洩

（※）ターゲットに対し、マルウェアに感染させるためのファイルを添付したメールを送り、開封させることにより、コンピューター上に保存されているファイルを窃取する攻撃

【攻撃の手口の巧妙化】

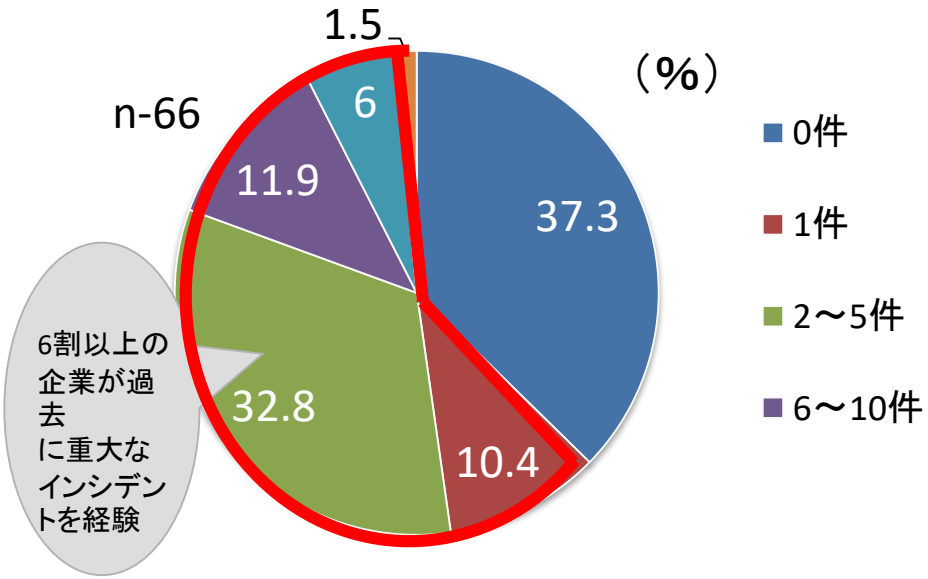
➢**不正なプログラムによる感染**
（従来）メールに不正なプログラムを添付

（最近）ウェブサイトを改ざんし、閲覧するだけで、不正なプログラムが自動的にダウンロード

➢**ＩＤ・パスワードの不正利用**
（従来）ＩＤ・パス入力を総当たり

（最近）取得済みのＩＤ・パスワードのリストを当てはめ、様々なサイトで成功率高く不正ログイン

【過去５年間に経験した重大なインシデント件数】



（出典）ＩＰＡ「企業CISOやCSIRTに関する実態調査2016」より経済産業省作成

社会インフラを狙った攻撃の増加

- 近年は社会インフラを標的として物理的なダメージを与えるサイバー攻撃のリスクが増大。
- テロリストや他国家からなされるサイバー攻撃には、産業界に直接攻撃がなされ、大規模停電のような国民の生命や財産を脅かす明確な意図を持って行われるものがある。
- このため、国民の安全の確保に責任を持つ政府と、インフラの安定的な運用に責任を持つ事業者が連携し、対策に取り組む必要がある。

原発の制御システム停止（米国、2003年）

発電所の制御システムがウィルスに感染。制御システムが約５時間にわたって停止。

石油パイプラインの爆発（トルコ、2008年）

何者かが石油事業者のネットワークに侵入。パイプラインの圧力を高めて爆発。

ロンドン五輪への攻撃（イギリス、2012年）

毎秒約１万件の不正通信。開会式会場の電力システムへの攻撃情報。手動に切り替え。

製鉄所の溶鉱炉損傷（ドイツ、2014年）

何者かが製鉄所の制御システムに侵入し、不正操作をしたため、生産設備が損傷。

発電所へのサイバー攻撃（ウクライナ、2015年）

マルウェアの感染により、変電所が遠隔制御された結果、数万世帯で3～6時間にわたる大停電が発生。

経済産業省における
サイバーセキュリティ対策の取組

サイバーセキュリティ基本法
（平成26年11月12日公布）

サイバーセキュリティ基本法（平成26年11月12日公布）

各主体の責務

国（第4条）：サイバーセキュリティ戦略の策定・実施

地方公共団体（第5条）：
サイバーセキュリティの自主的施策の策定・実施

重要社会基盤事業者その他企業（第6条）：
自主的・積極的にセキュリティ確保、国・地公体の施策への協力

教育研究機関（第8条）：
自主的・積極的にセキュリティ確保、人材育成、研究及び成果の普及、国・地公体の施策への協力

国民（第9条）：サイバーセキュリティへの注意

サイバーセキュリティ戦略本部の創設

- **サイバーセキュリティ戦略**案の作成（第25条第1項）
- 行政機関の**セキュリティ基準策定・監査実施**（第25条第2項）
- 行政機関における**インシデント事後調査**（第25条第3項）
- 国家安全保障会議（NSC）・IT総合戦略本部との連携（第25条第3項、第4項）

国の基本的施策

＜各主体への取組み＞

- **国の行政機関への対策**（第13条）
  セキュリティ統一基準の策定、不正通信等の監視・分析、演習・訓練、関係機関との連携、脅威情報の共有等
- **重要社会基盤事業者等への対策**（第14条）
  セキュリティ基準策定、演習・訓練、脅威情報の共有等
- **一般企業・教育研究機関への対策**（第15条第1項）
  中小企業等企業・研究機関等における知的財産が国の国際競争力の強化にとって重要との位置づけ。
  セキュリティ対策の促進、普及啓発、相談対応、情報提供・助言
- **国民への対策**（第15条第2項）
  相談対応、情報提供・助言

＜横断的課題への取組み＞

- **関係機関との連携**（第16条）
- **犯罪の取り締まり・被害拡大防止**（第17条）
- **安全保障に関わる事案への対処**（第18条）
- **セキュリティ産業の振興・国際競争力の強化**（第19条）
  サイバーセキュリティ能力を国が有することが重要であることから、サイバーセキュリティ産業が成長産業とすべきとの位置づけ。
  研究開発の推進、人材育成・確保、経営基盤強化・新事業開拓、国際標準化・相互認証の枠組みへの参画等
- **研究開発の促進**（第20条）：
- **人材の確保等**（第21条）：資格制度の活用、若年技術者育成等
- **教育・学習の振興、普及啓発等**（第22条）
- **国際協力の推進**（第23条）：国際間の信頼性構築・情報共有等

サイバーセキュリティ戦略本部の概要

設置根拠

○ 設置根拠：**サイバーセキュリティ基本法**（平成26年11月成立、平成28年4月改正法案成立）
※ＩＴ戦略本部長決定（平成17年5月）による「情報セキュリティ政策会議」が、同法に基づきサイバーセキュリティ戦略本部へ格上げ。

○ 本部の所掌事務：

① 政府全体のサイバーセキュリティ戦略の案の策定、同戦略の実施推進
② 各省及び独法が守るべきセキュリティ基準の策定、それに基づく各省等の施策評価
③ 各省に対する重大なサイバー攻撃事案に関し原因究明のための調査等の実施
④ 重要な施策の調査審議、関係行政機関の経費の見積もり方針の作成、その他総合調整

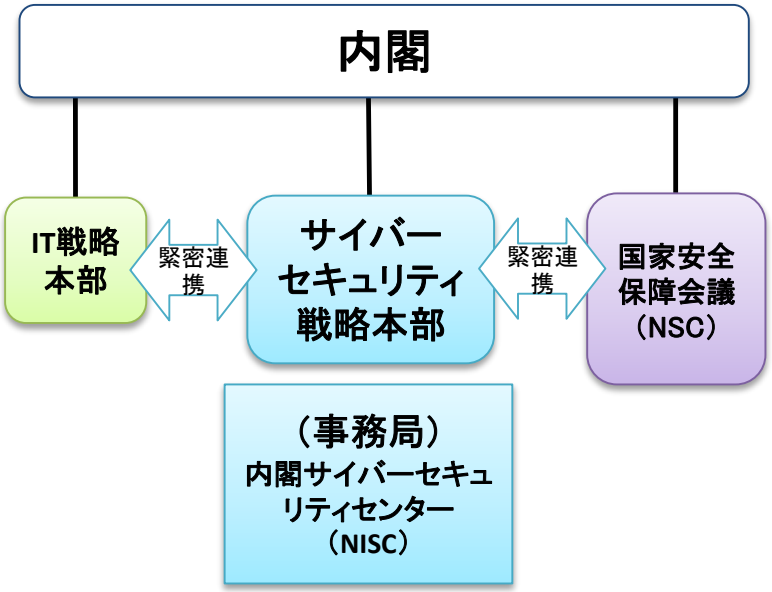
構成（※従来の「情報セキュリティ政策会議」の構成員を引継）

本部長　：内閣官房長官
副本部長：事務担当大臣（オリパラ担当大臣）
本部員　：国家公安委員会委員長、総務大臣、外務大臣、
経済産業大臣、防衛大臣、IT担当大臣、オリパラ担当大臣、有識者

＜有識者本部員＞

遠藤　信博　日本電気株式会社（ＮＥＣ）代表取締役会長
小野寺　正　ＫＤＤＩ株式会社 代表取締役会長
中谷　和弘　東京大学大学院法学政治学研究科 教授
野原佐和子　株式会社イプシ・マーケティング研究所 代表取締役社長
林　紘一郎　情報セキュリティ大学院大学 教授
前田　雅英　日本大学大学院法務研究科 教授
村井　　純　慶応義塾大学 教授

本部等の法制化により、事務・権限を強化



サイバーセキュリティ戦略

サイバーセキュリティ戦略の全体像

● 平成２７年９月、サイバーセキュリティ戦略を閣議決定。

１．基本的考え方

○ あらゆるモノがインターネットに連接される社会となるに伴い、サイバー攻撃による国民生活の影響も深刻化。

○ このため、「自由、公正かつ安全なサイバー空間」を創出・発展させるため、サイバーセキュリティ対策を強化

２．目的達成のための施策

経済社会の活力の向上及び持続的発展

○安全なＩｏＴシステムの創出

○セキュリティマインドを持った企業経営の推進

○セキュリティに係るビジネス環境の整備

国民が安全で安心して暮らせる社会の実現

○国民・社会を守るための取組

○政府機関を守るための取組

○重要インフラを守るための取組

国際社会の平和・安定及び我が国の安全保障

○我が国の安全の確保

○国際社会の平和・安定

○世界各国との協力・連携

横断的施策

○研究開発の推進

○人材の育成・確保

３．推進体制

NISCと政府機関の連携、IPA((独）情報処理推進機構）等の知見の活用等

サイバーセキュリティ2016の概要について

サイバーセキュリティ戦略に基づく２期目の年次計画として、2016年度に実施する具体的な取組を戦略の体系に沿って示したもの（以下は主な施策例）。

経済社会の活力の向上及び持続的発展

～ 費用から投資へ ～

■安全なIoTシステムの創出

- IoT（Internet of Things）に係る大規模な事業に対し、企画・設計段階からセキュリティを確保するために必要な働きかけを引き続き実施【内閣官房】
- IoT推進コンソーシアムを通じてIoTセキュリティガイドラインを策定し、対策を推進【総務省及び経済産業省】

■セキュリティマインドを持った企業経営の推進

- サイバーセキュリティ経営ガイドラインの普及【経済産業省】
- 情報開示の推進とインセンティブの検討【内閣官房】
- 金融業界横断的な演習を実施【金融庁】
- ICT分野の情報共有体制の拡充【総務省】

■セキュリティに係るビジネス環境の整備

- 企業育成等、セキュリティの成長産業化【経済産業省】
- 著作権法におけるソフトウェア製品等の解析（リバースエンジニアリング）に関する適法性を明確化【文部科学省】
- IoTシステムのセキュリティ認証制度にかかる評価・検討【経済産業省】

国民が安全で安心して暮らせる社会の実現

～ 2020年・その後に向けた基盤形成 ～

■国民・社会を守るための取組

- IoTに関する攻撃を含む攻撃観測網の強化【総務省】
- 民間の取組主体と協力し、サイバーセキュリティに関する普及啓発を実施【内閣官房】
- 地方公共団体における緊急時対応の支援【総務省】
- 一般財団法人日本サイバー犯罪対策センターとの連携【警察庁】

■重要インフラを守るための取組

- 「重要インフラの情報セキュリティ対策に係る第３次行動計画の見直しに向けたロードマップ」に従った検討【内閣官房及び重要インフラ所管省庁等】
- 重要インフラ対策の中核を担う人材育成や技術開発を行う体制を強化【経済産業省】

■政府機関を守るための取組

- 統一基準群の改定及び各府省庁の情報セキュリティポリシーの整備促進【内閣官房】
- 試行的な監査の結果を踏まえた各府省庁に対する監査及び厚生労働省（日本年金機構を含む）に対する施策の評価の実施【内閣官房】

国際社会の平和・安定及び我が国の安全保障

～ サイバー空間における積極的平和主義 ～

■我が国の安全の確保

- 対処機関における情報収集・分析機能及び対処能力向上【警察庁、法務省、防衛省、関係各省】
- 社会インフラへのサイバー攻撃に関する任務保証の観点からの知見向上・関係主体との連携深化【防衛省】

■国際社会の平和・安定

- 国際的な情報発信の強化【内閣官房、外務省、関係各省】
- 国際法・規範の議論と法執行の国際連携の両面から、サイバー空間への法の支配の確立に積極的に関与【内閣官房、外務省、関係各省】
- ASEAN等における能力構築を政府一体的に支援【内閣官房、外務省、関係各省】

■世界各国との協力連携

- G7伊勢志摩サミットにおいて立ち上げが決定された「サイバーに関するG7作業部会」を通じ、G7各国との政策協調及び実務的な協力を強化【内閣官房、外務省】
- 二国間協議や多国間協議を通じたASEANや米国等、世界各地域のパートナーとの連携の更なる強化【内閣官房、外務省、関係各省】

横断的施策

■研究開発の推進

- 政府、重要インフラ、企業・団体、個人等に対するサイバー攻撃の対策技術やサイバーセキュリティ関連情報の大規模集約技術の研究開発を行う【総務省】
- IoT・ビッグデータ・AI（人工知能）等の進化により実世界とサイバー空間が相互連関する社会を支える研究開発等の実施【経済産業省】
- 戦略的イノベーション創造プログラム（SIP）の枠組みにより、制御・通信機器の真正性／完全性確認技術を含む研究開発を行う【内閣府】

■人材の育成・確保

- 「新・情報セキュリティ人材育成プログラム」及び「サイバーセキュリティ人材育成総合強化方針」に基づく施策を促進【内閣官房】
- 「情報処理安全確保支援士」の創設に係る必要な制度整備を行うとともに、制度の普及を図る【経済産業省】
- サイバー攻撃への対処能力の向上に向けた実践的サイバー防御演習（CYDER）等を通じサイバーセキュリティ人材育成を行う【総務省】

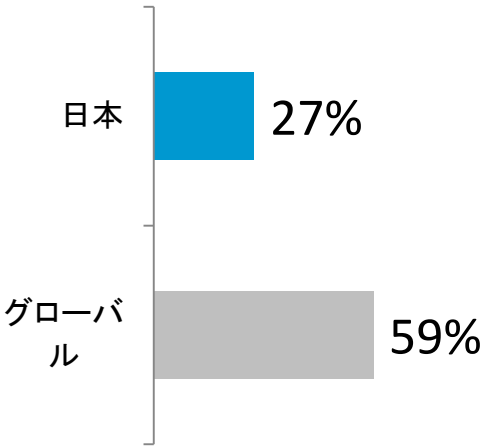
推進体制 ➢ 東京オリンピック・パラリンピック競技大会を見据えたリスク評価、対処体制の構築、総合的分析機能の強化、関係機関との協力体制の整備等【内閣官房】

サイバーセキュリティ経営ガイドライン

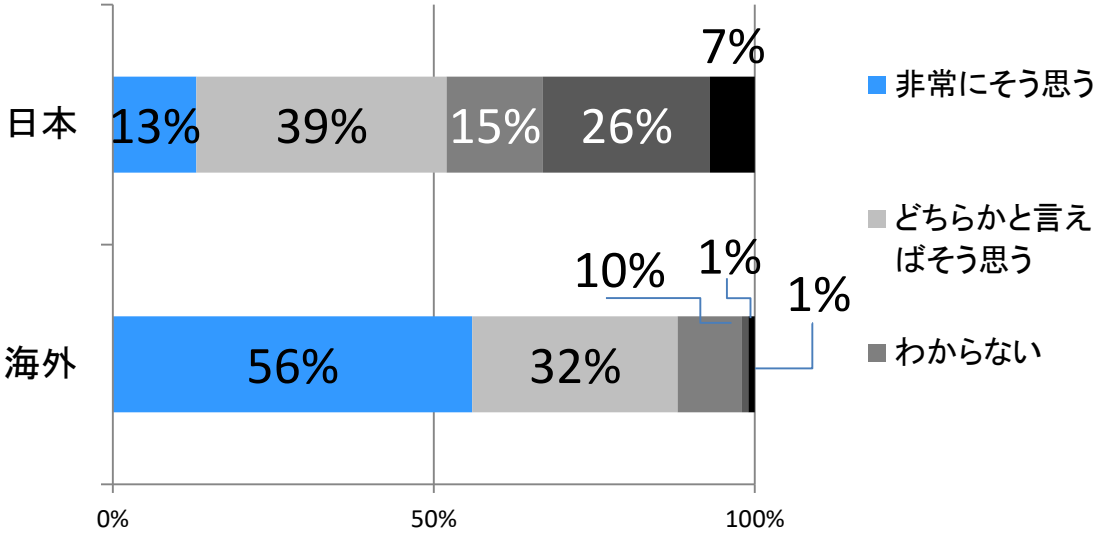
サイバーセキュリティ対策の現状（経営者の意識）

- しかしながら、日本では、サイバーセキュリティ対策において、経営者が十分なリーダーシップを発揮していない可能性がある。

【積極的にセキュリティ対策を推進する経営幹部がいる企業】



【サイバー攻撃の予防は取締役レベルで議論すべきか】



（出典） プライスウォーターハウスクーパース（株）「グローバル情報セキュリティ調査2014」より経済産業省作成

（出典）KPMGジャパン「KPMG Insight 日本におけるサイバー攻撃の状況と課題
ーセキュリティサーベイ2013からー」より経済産業省作成

サイバーセキュリティ経営ガイドラインの構成

１．経営者が認識すべき３原則

（１）経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要
（２）自社のみならず、ビジネスパートナーを含めた対策が必要
（３）平時及び緊急時のいずれにおいても、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要

２．経営者がＣＩＳＯ等に指示をすべき１０の重要事項

リーダーシップの表明と体制の構築
（１）サイバーセキュリティリスクの認識、組織全体での対応の策定
（２）サイバーセキュリティリスク管理体制の構築

サイバーセキュリティリスク管理の枠組み決定
（３）サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定
（４）サイバーセキュリティ対策フレームワーク構築（PDCA）と対策の開示
（５）系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施及び状況把握

リスクを踏まえた攻撃を防ぐための事前対策
（６）サイバーセキュリティ対策のための資源（予算、人材等）確保
（７）ITシステム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保
（８）情報共有活動への参加を通じた攻撃情報の入手とその有効活用のための環境整備

サイバー攻撃を受けた場合に備えた準備
（９）緊急時の対応体制（緊急連絡先や初動対応マニュアル、CSIRT）の整備、定期的かつ実践的な演習の実施
（10）被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備

情報共有体制（J-CSIP）

対応支援

重要インフラ事業者に対するサイバー攻撃情報共有体制（J-CSIP）の構築

- 電力・ガス等の重要インフラ企業に対するサイバー攻撃の情報共有が、組織的な防御力向上に不可欠。
- IPAは、重要インフラ事業者に対するサイバー攻撃情報共有体制を構築。
（J-CSIP（ジェイシップ）：Initiative for **C**yber **S**ecurity **I**nformation sharing **P**artnership of **J**apan、7業種、87組織が参加）
- 公的機関としての信頼性を基に、秘密保持等契約を結び、企業から情報を収集、解析、秘匿化し、迅速に共有することにより被害拡大を防止。

【J-CSIPの仕組み】

重要インフラ等企業（重工、電気、ガス、化学、石油、資源開発、自動車：7業種87組織）

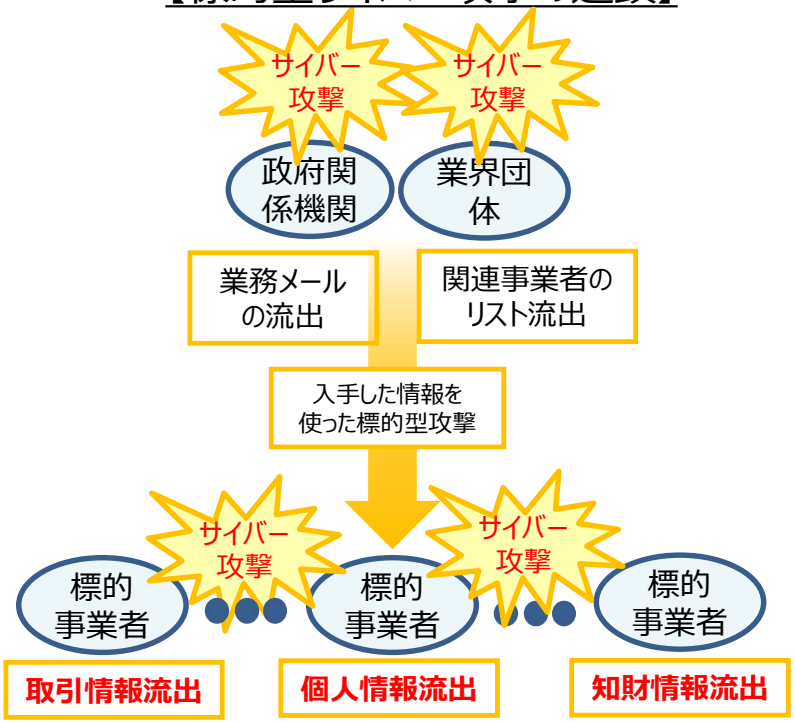
攻撃手口を解析し、提供者の営業秘密等保護のための匿名化を行った上で共有。

共有件数
（700件以上）
（2012年5月からの累計）

高度標的型サイバー攻撃を受けた組織への初動対応支援

- 平成26年7月、IPAに、個々の組織の能力では対処困難な、高度標的型サイバー攻撃を受けた組織に対する初動対応を行う「サイバーレスキュー隊」を立ち上げ。
- 最初の標的となり、対応遅延が社会や産業に重大な影響を及ぼすと判断される組織（主として、重要インフラ事業者、業界団体・独法等）に対して支援を実施。

【標的型サイバー攻撃の連鎖】



【サイバーレスキュー隊の活動】

政府関係機関、業界団体等

経済社会に被害が拡大するおそれが強く、一組織で対処が困難な深刻なサイバー攻撃の発生

初動時の緊急処置の助言、被害状況の理解促進、対応体制の早急な立ち上げの支援

支援数
１４２件（累計）
※2015年度９月末時点

IPA 独立行政法人情報処理推進機構 Information-technology Promotion Agency, Japan

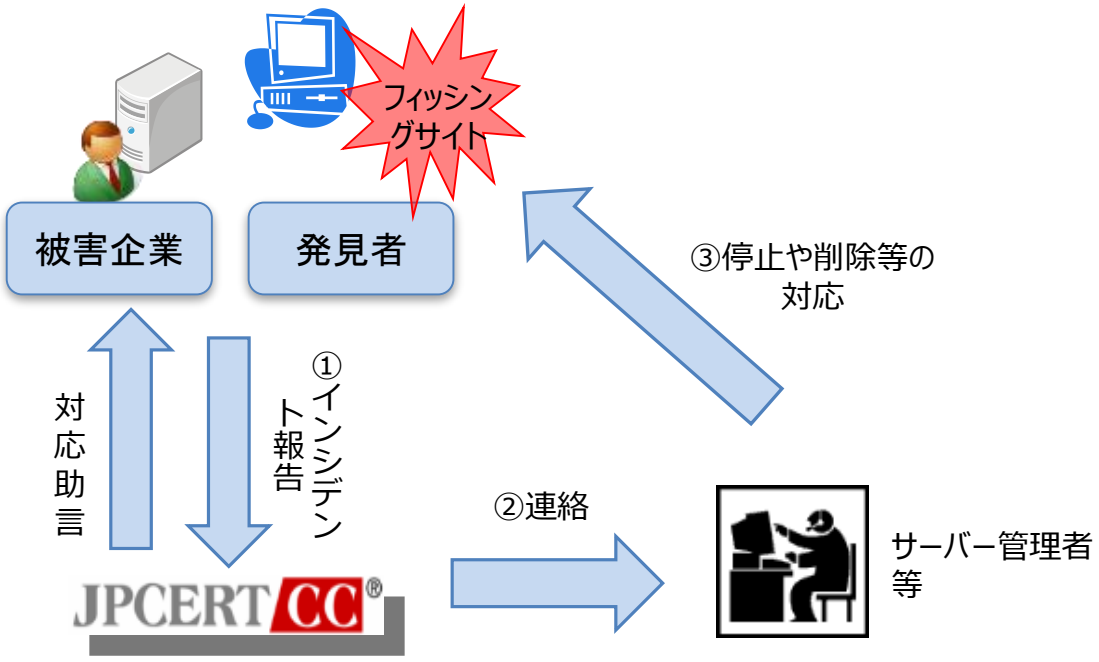
サイバーレスキュー隊

インシデントへの対応支援

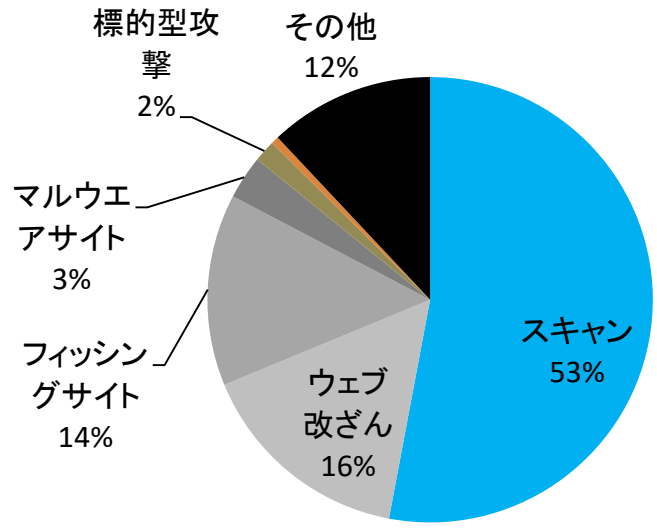
- 一般社団法人JPCERT/CCは、国内におけるインシデントへの対応支援も実施。
- 例えば、被害者や発見者から、ウェブサイト改ざん、DoS・DDoS等のサービス妨害攻撃、マルウエア配付サイトや、マルウエア添付メール等によるシステムへの不正侵入などのインシデント報告を受けて、ISP・ASP事業者やシステム管理者等に連絡し、インシデント発生元への対応依頼など、被害拡大の抑止を実施。

※ISP:インターネットサービスプロバイダ。ASP：アプリケーションサービスプロバイダ

【インシデント対応のイメージ】



【JPCERTが報告を受けたインシデント件数の割合】

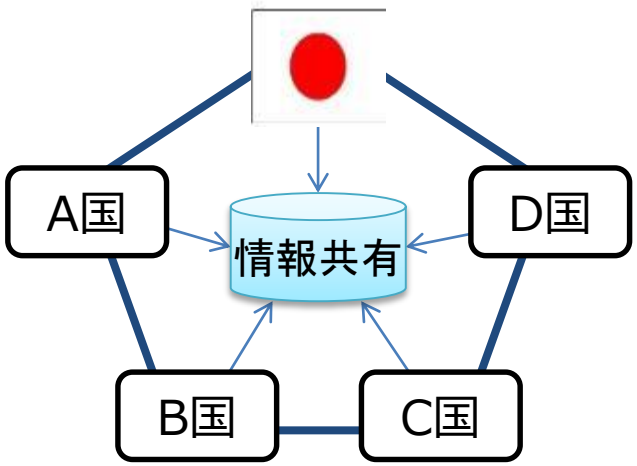


（出典）JPCERT/CCインシデント報告対応レポート(2015年7月1日～9月30日)より作成

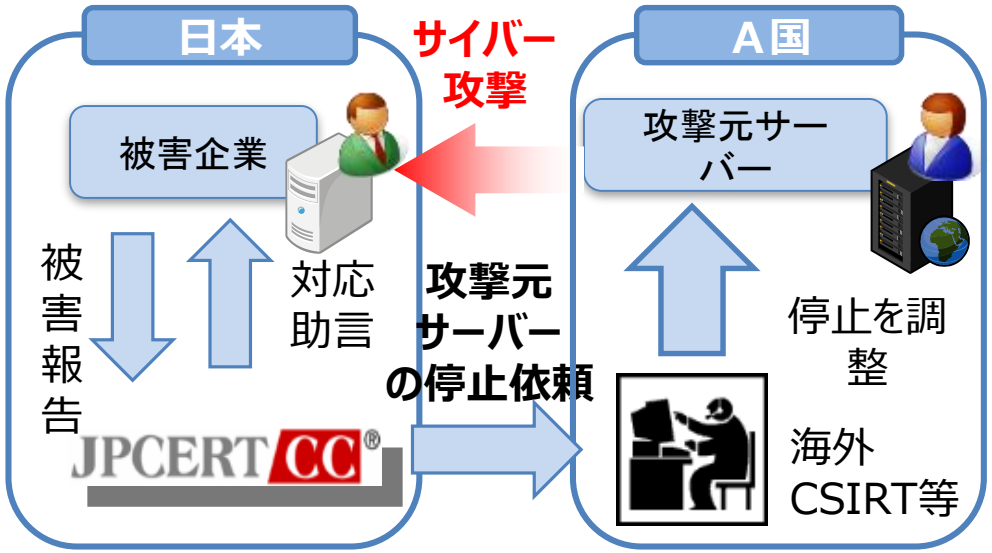
国際連携によるサイバー攻撃対処

- 一般社団法人JPCERT/CCは、サイバー攻撃対処のための日本で唯一の国際連携窓口業務を実施。
- 世界100カ国以上のCSIRT（シーサート: Computer Security Incident Response Team）と連携し、民間企業がサイバー攻撃にあった際に、各国との情報共有や、海外の攻撃元サーバの停止等を海外の窓口と調整。
- 途上国からの攻撃に対応するため、アジア・アフリカ諸国のCSIRT構築や運用も支援。
- サイバー攻撃の分析結果や脆弱性情報を共有し、グローバルなサイバー空間のセキュリティ向上に貢献。

各国の窓口CSIRTが、攻撃基盤に係る情報を共有し、共同対処。



【国際連携によるサーバの停止等の対応】



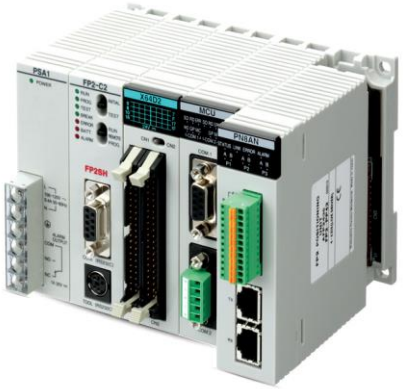
制御システムの
セキュリティ対策推進

制御システムのセキュリティ対策の推進

- 重要インフラでは、制御機器・システムの信頼性とセキュリティの品質確保が重要。CSSC（技術研究組合制御システムセキュリティセンター）では、制御機器のセキュリティ認証（平成28年3月現在、３社の製品を認証）を実施。
- 制御システムへのサイバー攻撃を模擬したサイバーセキュリティ演習では、2015年度、電力・ガス・ビル・化学の４分野の制御システム担当者・技術者等合計８９名が参加。今年度も同４分野で実施予定。

＜認証対象製品例　：　制御機器＞

○インフラ施設のセンサーからの情報を基にプログラムに従ってガス流量等を自動制御する機器



＜サイバー演習の様子＞

火力発電所模擬プラント

ガス模擬プラント

机上演習（例題システムにおける脅威と対策の検討）

IoT

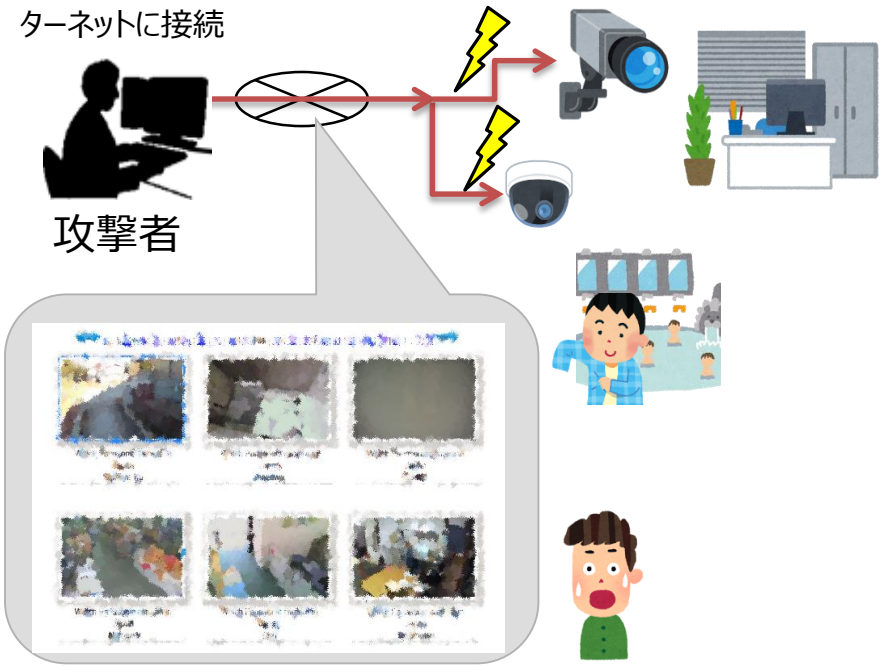
IoTの新たなセキュリティ上の脅威

IoTでは、これまで接続されていなかった自動車やカメラなどの機器が、WiFiや携帯電話網などを介してインターネットに接続されることにより、新たな脅威が発生し、それに対するセキュリティ対策が必要となった。

自動車へのハッキングよる遠隔操作

人命にも関わる事故が起こせることが証明され、
自動車会社は**140万台にも及ぶリコール**を実施。

監視カメラの映像がインターネット上に公開



セキュリティ対策が不十分な**日本国内の多数の監視カメラの映像が海外のインターネット上に公開**。
（ID，パスワードなどの初期設定が必要）

IoTセキュリティガイドラインについて①

Ｉｏ Ｔ特有の性質に着目したセキュリティガイドラインを策定すべく、経済産業省と総務省が連携し、昨年１月より「Ｉｏ Ｔ推進コンソーシアム・Ｉｏ Ｔセキュリティワーキンググループ」を開催し、検討を進めてきた。昨年７月５日（火）に公表。

■　本ガイドラインの目的は、IoT特有の性質とセキュリティ対策の必要性を踏まえて、 IoT機器やシステム、サービスについて、その関係者が**セキュリティ確保の観点から求められる基本的な取組を、セキュリティ・バイ・デザインを基本原則としつつ、明確化することによって、産業界による積極的な開発等の取組を促す**とともに、**利用者が安心してIoT機器やシステム、サービスを利用できる環境を生み出す**ことにつなげるもの。

■　なお、本ガイドラインの目的は、サイバー攻撃などによる被害発生時における関係者間の法的責任の所在を一律に明らかにすることではなく、むしろ**関係者が取り組むべきIoTのセキュリティ対策の認識を促すとともに、その認識のもと、関係者間の相互の情報共有を促すための材料を提供すること**である。

■　本ガイドラインは、その対象者に対し、一律に具体的なセキュリティ対策の実施を求めるものではなく、**守るべきものやリスクの大きさ等を踏まえ、役割・立場に応じて適切なセキュリティ対策の検討が行われることを期待**する。

IoTセキュリティガイドラインについて②

■　本ガイドラインは、IoT機器やシステム、サービスの提供にあたってのライフサイクル（方針、分析、設計、構築・接続、運用・保守）における指針を定めるとともに、一般利用者のためのルールを定めたもの。
■　各指針等においては、具体的な対策を要点としてまとめている。

	指針	主な要点
方針	IoTの性質を考慮した基本方針を定める	• 経営者がIoTセキュリティにコミットする • 内部不正やミスに備える
分析	IoTのリスクを認識する	• 守るべきものを特定する • つながることによるリスクを想定する
設計	守るべきものを守る設計を考える	• つながる相手に迷惑をかけない設計をする • 不特定の相手とつなげられても安全安心を確保できる設計をする • 安全安心を実現する設計の評価・検証を行う
構築・接続	ネットワーク上での対策を考える	• 機能及び用途に応じて適切にネットワーク接続する • 初期設定に留意する • 認証機能を導入する
運用・保守	安全安心な状態を維持し、情報発信・共有を行う	• 出荷・リリース後も安全安心な状態を維持する • 出荷・リリース後もIoTリスクを把握し、関係者に守ってもらいたいことを伝える • IoTシステム・サービスにおける関係者の役割を認識する • 脆弱な機器を把握し、適切に注意喚起を行う
一般利用者のためのルール		• 問合せ窓口やサポートがない機器やサービスの購入・利用を控える • 初期設定に気をつける • 使用しなくなった機器については電源を切る • 機器を手放す時はデータを消す

企業活動におけるサイバーセキュリティ対策

- 企業にとって、自然災害等の脅威に比べ、サイバー攻撃の脅威は肌感覚では認識しがたいもの。また、サイバー攻撃の脅威は、日々、高度化を続けている。
- このため、経営者において、①模擬攻撃等を通じたリスク分析によりサイバー攻撃の脅威を正しく認識し、②システム更新・人材育成等のセキュリティを高めるための投資を行い、さらに、③これらを企業活動における継続的サイクルとして根付かせていく、というアプローチが有効。
- 我が国において、こうした企業活動を定着させ、経済活動として循環させていくことにより、セキュリティ産業を振興・強化していく。

【サイバーセキュリティ対策を実装するためのプロセス】

①サイバー攻撃の脅威の認識

- 情報共有
- リスク分析・評価

②セキュリティ投資の実施

- ◆ 社内システム等へのセキュリティ投資
  - 社内システムの改善
- ◆ 対策の中核を担う人材の育成・配置
  - 産業サイバーセキュリティセンターの活用
  - セキュリティ人材のキャリアパス構築

③ 継続的サイクルとして定着

産業の振興・強化

「産業サイバーセキュリティセンター」の設立

重要インフラのサイバーセキュリティ対策を担う人材の育成

- 本年４月に、（独）情報処理推進機構（IPA）に産業サイバーセキュリティセンターを設置し、官民の共同によりサイバーセキュリティ対策の中核となる人材を育成。
- 模擬プラントを用いた演習や実システムの安全性検証等の実践経験を通じて、重要インフラ・産業基盤のサイバーセキュリティ対策の根幹を担う人材・技術・ノウハウを生み出す。
- 他業界や同業他社のセキュリティ責任者やホワイトハッカー等の専門家、海外有識者等との人脈を形成した人材が、各社において総合的なセキュリティ戦略立案を担う。

模擬プラントを用いた対策立案

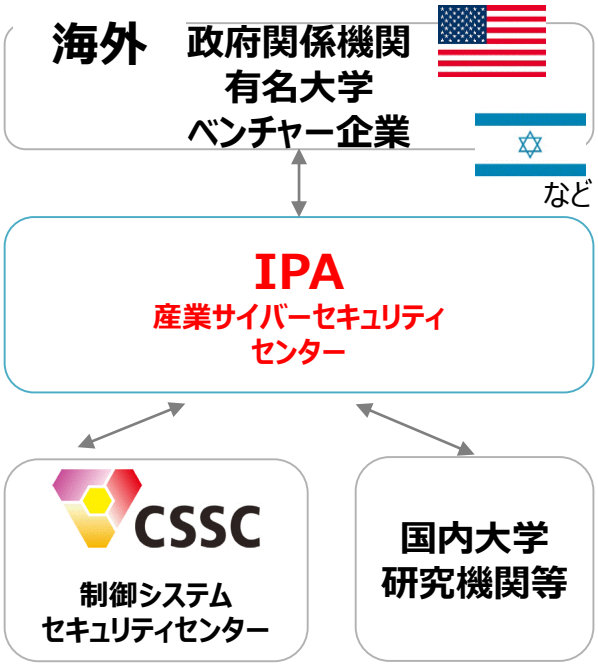
- 情報系システムから制御系システムまでを想定した模擬プラントを設置。専門家と共に安全性・信頼性の検証や早期復旧の演習を行う。
- 海外との連携も積極的に実施。

実際の制御システムの安全性・信頼性検証等

- ユーザーからの依頼に基づき、企業が今後導入する制御システムやIoT機器の安全性・信頼性を検証。
- あらゆる攻撃可能性を検証し、必要な対策立案を行う。

攻撃情報の調査・分析

- おとりシステムの観察や民間専門機関が持つ攻撃情報を収集。新たな攻撃手法等を調査・分析。



セキュリティ対策の目的はシステムを守ること。

そのために敵のコストをあげ、我のリスクを下げるための方策を検討し実施する。

企業に於けるセキュリティのヒント（1）

- かけたコストに対して得られる安心の度合いを計る指標は無く、いくらお金をかけても絶対の安心は無い。

○少なくとも同業他社よりは、セキュリティ対策をしっかりしておくことが重要。（お金儲けが目的の攻撃者対策）

犯罪者にもコスト管理があり、同じお金を稼げるならば、より楽な目標を狙う。
同業他社よりセキュリティのレベルをあげておく事で、攻撃の対象になることを
ある程度予防する事ができる。

○突破されることを前提とし、被害の極限を図る対策を行う。（情報目的の攻撃者対策）

攻撃者が政府機関等である場合は、コスト的に、かなう相手ではない。
ダメージコントロールの概念を持つことが重要。

企業に於けるセキュリティのヒント(2)

- ✓ 敵は　誰で何を欲しているのか？
  では、何を守ればよいか。

- ✓ 敵は　どこから侵入してくるだろうか？
  では、どこを守ればよいか。

- ✓ 敵は　どうやって侵入してくるだろうか？
  では、どうやって守ればよいか。

企業に於けるセキュリティのヒント(3)

家の塀と同じで、高い塀を巡らせても一番低い所や弱い所から泥棒に入られる。
つまり一番弱い部分が全体の強さを決める。
　→技術と運用を統括した一元的なセキュリティ対策が必要。

また、いくらセキュリティに投資しても、正面玄関から入られたら何にもならない。
この危険は、ID とパスワードの管理。標的型攻撃そして内部犯行である。
　→人間対策

官民が力を合わせて、
安全／安心な社会を
作りましょう

ご静聴ありがとうございました