経済産業省
Ministry of Economy, Trade and Industry

制御システムのサイバーセキュリティに関する我が国の取組み

平成２６年１月１５日
商務情報政策局
情報セキュリティ政策室
上村昌博

サイバーセキュリティ対策を支える体制　政府内の役割分担

経済産業省
Ministry of Economy, Trade and Industry

IT戦略本部（本部長：内閣総理大臣）

情報セキュリティ政策会議（議長：内閣官房長官）　2005年 設置

・基本戦略
・国際戦略
・政府総合対策
・重要インフラ対策
・事案対処支援

NISC National Information Security Center　内閣官房情報セキュリティセンター

協力

重要インフラ（１０分野）
所管省庁
（金融、国交、厚生）

警察庁　総務省　外務省　経済産業省　防衛省　庶務５省庁

●政府対策基準の策定
●政府機関へのサイバー攻撃防御

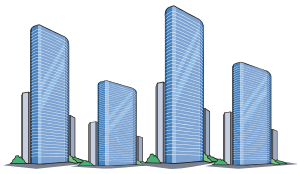
●情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流

●サイバー犯罪対策

●国家防衛

●通信ネットワーク対策
●自治体の対策

●すべての基礎を支える情報システムの対策
●重要インフラ（電力、ガス）
●企業・個人の対策



政府機関

重要インフラ

企業

個人

サイバーセキュリティ戦略概要

経済産業省 Ministry of Economy, Trade and Industry

1. 環境の変化

サイバー空間と実空間の「融合・一体化」
► 情報通信技術の普及・高度化・利活用の進展

サイバー空間を取り巻く「リスクの深刻化」
► リスクの甚大化・拡散・グローバル化

2. 基本的な方針

(1) 目指すべき社会像:「サイバーセキュリティ立国」の実現

国家の安全保障・危機管理、社会経済の発展、国民の安全・安心確保のため、
「世界を率先する」「強靭で」「活力ある」サイバー空間を構築し、
サイバー攻撃等に強く、イノベーションに満ちた、世界に誇れる社会を実現

(2) 基本的な考え方

① 情報の自由な流通の確保
► 表現の自由やプライバシーの保護等が確保され、経済成長等を享受

② 深刻化するリスクへの新たな対応
► リスクの変化に迅速・的確に対応できる多層的な取組が必要

③ リスクベースによる対応の強化
► 動的対応力を通じ、リスクの性質を踏まえた対応の強化が必要

④ 社会的責務を踏まえた行動と共助
► 多種多様な主体が各々の役割を発揮し、相互連携・共助が必要

(3) 各主体の役割

① 国
► サイバー空間の外交・防衛・犯罪対策、政府機関等における対策強化・対処態勢整備 等

② 重要インフラ事業者等
► 現行10分野の取組強化、新たな分野における必要な対策の実施 等
(10分野:情報通信、金融、航空、鉄道、電力、ｶﾞｽ、政府・行政ｻｰﾋﾞｽ(地方公共団体を含む)、医療、水道、物流)

③ **企業や教育・研究機関**
► **情報共有等の集団的対策、産学連携による高度技術・人材の供給 等**

④ 一般利用者や中小企業
►「他者に迷惑かけない」認識醸成やリテラシー向上など自律的取組、情報共有 等

⑤ サイバー空間関連事業者
► 製品等の脆弱性への対応、インシデント認知・解析、国際競争力の強化 等

3. 取組分野

経済産業省 Ministry of Economy, Trade and Industry

(1)「強靭な」サイバー空間の構築

※GSOC: Government Security Operation Coordination team
CSIRT: Computer Security Incident Response Team
CYMAT: Cyber Incident Mobile Assistant Team

① 政府機関等における対策：情報システム等に関する対策及びサイバー攻撃への対処態勢を一層強化

例
- 政府共通プラットフォームによる情報システムのクラウド化、技術標準化等を通じ、攻撃等に強いシステム基盤構築。
- 国家機密等に関する情報及び情報システムの重要度等に応じてセキュリティ対策を重点化。
- 国の安全に関する重要な情報の国以外の事業者による取扱い、独立行政法人等におけるセキュリティ強化。
- GSOCを抜本的に強化し、監視対象を拡大するとともに、インシデント情報を効果的に収集・活用。
- CYMAT、CSIRT等の間の連携強化により、政府内におけるインシデント情報共有・即応体制を一層強化。
- 大規模サイバー攻撃事態等を想定した対処訓練を毎年度実施するなど対処態勢を強化。

② 重要インフラ事業者等における対策：政府機関等における対策に準じた取組

例
- 重要インフラ事業者等とサイバー空間関連事業者との間の、攻撃情報等の情報共有を促進。
- GSOCが保有するインシデント情報等を重要インフラ事業者等と共有するための仕組みを整備。
- 重要インフラの範囲及び対応の在り方等を検討し、対策をとりまとめた新たな「行動計画」を策定。

③ 企業・研究機関等における対策：インシデントの認知・情報共有の強化、CSIRT構築促進や演習等

例
- セキュリティ投資促進のためのインセンティブ検討等により、中小企業等におけるサイバー攻撃認知機能等を強化。
- **演習用テストベッドを利用した実践的な防御演習等により、企業等におけるサイバー攻撃への対応能力を向上。**
- 企業・研究機関等のCSIRT構築促進・連携強化を図り、インシデント発生時の対応能力を向上。

④ サイバー空間の衛生：個々の主体による対策に加え、社会全体が参加した予防的対策実施

例
- 「サイバー・クリーン・デー」（仮称）の新設などサイバー空間の衛生確保を国民運動化。
- 悪性サイトにアクセスしようとする一般利用者に対するISP等による注意喚起等を行うための仕組みを構築。
- セキュリティ目的の通信解析の可能性等、通信の秘密等に配慮した、関連制度の柔軟な運用の在り方を検討。

⑤ サイバー空間の犯罪対策： 対処能力強化や民間事業者等の知見の活用等による対処態勢強化

例
- 日本版NCFTAの創設、アンチウイルスベンダーとの情報共有枠組みの構築等の取組を強化。
- サイバー犯罪に対する事後追跡可能性を確保するため、関係事業者における通信履歴等に関するログの保存の在り方やデジタルフォレンジックに関する取組を促進するための方策について検討。

※NCFTA: National Cyber-Forensics and Training Alliance

(1)「強靱な」サイバー空間の構築 ［続き］

⑥ サイバー空間の防衛：国家レベルのサイバー攻撃から我が国に係るサイバー空間を守るための対応強化

例
- 重要インフラ等の情報システムに対する攻撃における自衛隊など非常時における関係機関の役割を整理し、必要な体制・機密情報等の共有システムや制度の整備等を行うとともに、個別具体的な国際法の適用も併せて整理。
- 武力攻撃の一環としてサイバー攻撃が行われた場合に対処する任務を負う自衛隊等の能力・態勢等を強化。

(2)「活力ある」サイバー空間の構築

① 産業活性化：海外製品等への依存度が高い我が国のサイバーセキュリティ産業の国際競争力強化

例
- **国際標準化や評価・認証の国際的な相互承認枠組み作りに積極的に関与するとともに、産業制御システムの評価・認証機関を設立。**
- 新たな技術が採用された製品等の政府による積極的な調達。

② 研究開発：リスクの変化に適切に対応できる、創意と工夫に満ちたセキュリティ技術の創出

例
- サイバー攻撃の検知や高度解析等の向上に向けた技術の研究開発等を加速させ、最先端の研究開発を保持・向上。
- 潜在型マルウェア等多様・高度化するサイバー攻撃に対し、有効な革新的技術を確立するため、先端技術を開発。

③ 人材育成：高度かつ国際的なセキュリティ人材の育成

例
- ソフトウェア関連分野における優れた個人を発掘等するための合宿研修や実践的技能を競うコンテスト等を官民で連携実施。
- グローバルに活躍できる人材の育成等のため、国際会議への参加や海外の専門大学院等への留学を支援。

④ リテラシー向上：一般国民のリテラシーの向上

例
- 初等中等教育において、情報セキュリティを含む情報モラルやソフトウェアのプログラミングに関する教育、デジタル教科書の活用など実践的な取組を推進。高齢者に対するセキュリティ啓発のためのサポーター等を育成・活用。
- スマートフォンのアプリについて、一般利用者がリスクを認知し、利用等の判断を行う自ら行える仕組みを構築。

(3)「世界を率先する」サイバー空間の構築

① 外交：基本的な価値観を共有する国等とのパートナーシップ関係の多角的構築・強化

例
- サイバー空間を利用した行為に対する国連憲章や国際人道法等の個別具体的な国際法の適用について引き続き検討。
- **米国等との間で、サイバー領域での具体的対処の在り方、国際的なルール作りといった分野における議論を深化。**

② 国際展開：ASEAN等とともに成長できる関係を構築し、サイバー攻撃への対応能力構築の支援

例
- 諸外国と連携してサイバー攻撃に関する情報収集ネットワークを構築し、攻撃の発生予知、即応等に関する研究開発を実施。
- 官民連携によるボットウイルス対策など国内における成功事例の紹介や共同プロジェクト、机上演習等を実施。

③ 国際連携：国境を越えるサイバー攻撃に関するインシデントへの対応・連携の強化

例
- 外国捜査機関等とのサイバー犯罪に係る情報交換を継続的に行うとともに、連携強化等のため、職員を派遣。
- 相互不信による不測事態回避のため、我が国の基本的な立場等を共有するとともに、インシデント発生した場合の相互の連絡体制等を平時から構築し、国際共同研究や複数国間におけるサイバー攻撃対応演習等を実施。

4. 推進体制等

- NISCについて権限等の必要な組織体制を整備し、**2015年度を目途として「サイバーセキュリティセンター」（仮称）に改組・機能強化**
- 政府機関や重要インフラ事業者等におけるサイバー攻撃関連情報の共有促進のための枠組み整備
- 取組を進めるにあたっての具体的な中長期（2015年度・2020年）の目標の管理

例
- 2015年度までに、政府機関等におけるサイバー攻撃関連情報の共有体制のカバー率向上、マルウェア感染率や国民の不安感の改善、国際インシデント調整の対応連携が可能な国等の３割増
- **2020年までに、国内の情報セキュリティ市場規模の倍増、セキュリティ人材の不足割合の半減**

- 2015年度までの3年間を戦略の対象とし、年次計画の策定・評価等を実施
- 国際分野における総合的な対応を推進するための方針を策定

「サイバーセキュリティ戦略」（平成25年6月　情報セキュリティ政策会議決定）

経済産業省 Ministry of Economy, Trade and Industry

1. 環境の変化

(1)サイバー空間の拡大・浸透

①サイバー空間と実空間の「融合・一体化」の進展

・・・サイバー空間の拡大・浸透は、情報通信技術の普及・高度化と、当該技術に係る利活用の進展の結果生じている。・・・**電子商取引、医療、教育、交通、社会インフラ管理、行政等の多様な分野**において利活用されている。

サイバー空間は、我が国の成長力強化にとって不可欠であり、今後も一層拡大・浸透していくと考えられる。例えば、**成長力強化にとって重要な安全・便利で経済的な次世代インフラや、クリーンかつ経済的なエネルギー需給を実現するためには、オープンデータやビッグデータを利活用したITS やスマートグリッドが必要**である。これらを構成する情報システムや情報通信ネットワーク等は、**サイバー空間の更なる拡大・浸透をもたらす**ことになる。・・・

②サイバー空間を取り巻く「リスクの深刻化」

・・・サイバー攻撃の手法についても、複雑・巧妙化してきている。例えば、・・・**インターネット等外部との接続を持たないクローズドな制御系ネットワークに対するUSBメモリ等経由による攻撃**・・・などが出現してきている。これらの中には、国家レベルの関与が必要と思われる高度の技術と計画性が指摘されているものもある。また、サイバー攻撃の対象となり得る範囲も・・・**社会インフラ等の公的な空間まで広がってきている**。・・・**店舗におけるPOS端末や防犯カメラ等の設置、社会インフラ等の施設におけるセンサー等の活用など**、情報通信機器が様々な人やモノ、場所へ分散してきている。・・・サイバー攻撃に係るリスクは、その目的や手法等の変化により、従来の想定をはるかに超えた水準まで高まってきている。とりわけ**「甚大化するリスク」、「拡散するリスク」、「グローバルリスク」として顕著に進行**し、「リスクの深刻化」という新たな局面を迎えており、我が国の安全保障・危機管理に影響を及ぼすとともに、国際的な競争力を揺るがし、国民に多大な不安をもたらす恐れが生じている。

「サイバーセキュリティ戦略」（平成25年6月　情報セキュリティ政策会議決定）

経済産業省
Ministry of Economy, Trade and Industry

【甚大化するリスク】

・・・重要インフラ事業などから機密や技術情報等を窃取することが目的とみられる標的型攻撃の脅威の顕在化も指摘されている 。・・・

海外においては、交通メッセージを表示する信号機システムに対するサイバー攻撃 や、複雑・巧妙さから国家レベルの組織の関与も疑われている基幹インフラの制御系システム等に対する高度なサイバー攻撃も発生しており、大規模な社会的混乱等を引き起こされるリスクが現実の問題となっている。

今後は、通信インフラにおけるSDN 、交通インフラにおけるITSや電力インフラにおけるスマートグリッドの普及等により様々な社会インフラがネットワークに常時接続され、ソフトウェアにより管理・制御される状態へ進展していくと考えられる。これらにおけるソフトウェアの脆弱性等を狙うサイバー攻撃により、通信障害、交通混乱やブラックアウトといった事態が発生し大規模な社会的混乱や人の生死に直接的な影響をもたらすことも可能性として想定される 。

【拡散するリスク】

・・・リスクが甚大化すると同時に、リスクが急速に拡散している。・・・M2M・センサーネットワークの拡大、あらゆるモノがインターネットに接続され得る状態（Internet of Things）の出現等により、サイバー攻撃の対象となり得る機器が我々の身の周りの隅々まで行き渡ることによるリスクの拡散が進行・・・。

・・・また、M2M・センサーネットワークの普及により、家電、自動車、コピー機等の複合機、防犯カメラ等のモノにもリスクが拡散している。これまでネットワークに接続されてこなかった機器がインターネットに接続され、人を介在しない情報交換により制御等される結果、これらに対するサイバー攻撃により予期せぬ動作が起きる恐れがある。・・・インターネットに接続された家電や自動車から家庭内の生活関連情報や走行場所等の位置情報などがサイバー攻撃により流出する恐れや、・・・

さらに、・・・情報系ネットワーク等の外部ネットワークと切り離されたクローズドな独立系システムもサイバー攻撃の対象となっている。例えば、基幹的なインフラの制御系システムに対して、USBメモリを媒介してマルウェアに感染し、インフラにおける機器を稼働不能とすることも現実の問題となっている 。

「サイバーセキュリティ戦略」（平成25年6月　情報セキュリティ政策会議決定）

経済産業省 Ministry of Economy, Trade and Industry

3. 取組分野

(1)「強靭な」サイバー空間の構築

②重要インフラ事業者等における対策

・・・障害情報及び攻撃・脅威・脆弱性等に関する情報については、引き続き重要インフラ事業者等及びCEPTOAR との間における情報共有を推進するとともに、業種間での情報共有が難しい**標的型攻撃に関する情報については、秘密保持契約に基づく情報共有体制を深化・拡充**する。・・・重要インフラ事業者等、サイバー空間関連事業者及び関係CSIRTの間で、民間組織間の信頼関係を前提に、サイバー演習等の実施を促進しサイバー攻撃に対する連携対応能力の強化を図る。

重要インフラ分野におけるサプライチェーン・リスクへの対応強化を図るとともに、情報セキュリティの評価・認証の導入を進めていくことが重要である。具体的には、重要インフラ事業者等とサイバー空間関連事業者との脆弱性情報や攻撃情報等の情報共有等による連携の促進、**SCADA等の制御系機器・システム等の調達・運用における国際標準に則った評価・認証導入の在り方の検討や、制御系機器・システムの評価・認証機関の設立に向けた取組を進めていく**。

(2)「活力ある」サイバー空間の構築

①　産業活性化

・・・　情報セキュリティ対策に関する高度な技術の研究開発、**国際標準化や評価・認証を含んだ制度整備等が必要**である。・・・具体的には、**M2M等を基盤としたスマートコミュニティ・スマートグリッド、スマートシティやスマートタウンにおける情報セキュリティ関連技術、**・・・今後、情報通信技術を利活用した製品やサービスが、**国際的な取引において、サイバーセキュリティ上の信頼性を求められるようになる中、**それを証明するものとして、**国際標準化や評価・認証、情報セキュリティ監査の重要性が**増してくると考えられる。このため、国際貿易において我が国が有利になるよう、**国際標準化や評価・認証の国際的な相互承認枠組み作りに関して、積極的に参画・働きかけを進める**とともに、**関係する民間部門への支援や国内の評価・認証機能の整備も進めていく**ことが必要である。具体的には、・・・**セキュリティ検証施設を中核とした産業制御システムの評価・認証機関の整備を進めていく。**

「サイバーセキュリティ戦略」（平成25年6月　情報セキュリティ政策会議決定）

経済産業省 Ministry of Economy, Trade and Industry

(3)「世界を率先する」サイバー空間の構築

②国際展開

・・・加えて、国際貿易において、あらゆる情報通信技術を利活用した製品・サービスが、サイバーセキュリティ上の安全性を求められるようになる中、**産業活性化の観点からは、**我が国が強みを持つ複合機や**制御システム等の日本製品が不利な扱いを受けることのないよう、セキュリティの国際標準化や評価・認証の国際的な相互承認枠組み作りに関して、我が国として積極的に参画、働きかけを進めていく**。・・・

サイバーセキュリティ国際連携取組方針～j-initiative for Cyber Security～（平成25年10月 情報セキュリティ政策会議決定）

4. 重点取組分野

(3)　サイバーセキュリティに関する国際的なルール作り

①　国際的な技術基準策定

サイバー空間のセキュリティを確保するためのシステムなどは広く国際的に取引されるようになってきているが、その相互運用性や求められるセキュリティ水準を確保するための技術的な標準の重要性が増している。このため、様々な国際標準化の取組が行われている中で、サイバーセキュリティ技術に関する国際標準の策定・普及や相互承認枠組作りを進めていくことが重要である。その際、実際に基準を用いて取引を行うのは企業などの主体であり、官民の連携による対応が不可欠となる。

我が国では、2013年に制御システムセキュリティセンター（CSSC: Control System Security Center）を設立したところであり、CSSCを拠点として制御システムセキュリティの評価・認証技術を確立するとともに、その技術の利用促進のための評価・認証機関を設置し、CSSCに参加する企業や団体を中心としてCSSCの活用による新たな国際標準の提案活動にも寄与する。・・・

日本再興戦略における制御システムセキュリティ

経済産業省
Ministry of Economy, Trade and Industry

○ 本年6月に閣議決定された「日本再興戦略」において、世界最高水準のIT 社会にふさわしい、強靭で活力あるサイバー空間を構築するため、「サイバーセキュリティ戦略」を踏まえ、サイバーセキュリティ対策を強力に展開する旨が記載。

日本再興戦略（平成25年6月14日閣議決定）

第Ⅱ． 3つのアクションプラン

一．日本産業再興プラン

4．世界最高水準のIT社会の実現

⑤サイバーセキュリティ対策の推進

世界最高水準のIT 社会にふさわしい、強靭で活力あるサイバー空間を構築するため、「サイバーセキュリティ戦略」を踏まえ、政府機関や重要インフラにおけるセキュリティ水準及び対処態勢の充実強化や国際戦略の推進等、サイバーセキュリティ対策を強力に展開する。

○重要インフラ分野におけるインシデント対策の強化

- サイバー攻撃に対する重要インフラの防護を強化するため、重要インフラ事業者等及び政府機関との間における情報共有の仕組みや重要インフラの範囲等について検討を進め、今年度中に、「情報セキュリティ政策会議」において、新たな行動計画を策定する。

○サイバーセキュリティに関する国際戦略の策定

- 我が国と戦略的に強い結び付きのある国・地域との多角的パートナーシップの強化、我が国が強みを持つセキュリ ティ技術の国際展開等を政府一体となって加速させるため、今年度中に、「情報セキュリティ政策会議」において新 たにサイバーセキュリティ国際戦略を策定するとともに、来年度中に制御システム等のセキュリティの国内での評価・認証を開始し、インフラの整備・輸出等を促進する。

日米サイバー対話における制御システムセキュリティ

経済産業省
Ministry of Economy, Trade and Industry

○ 首脳間合意に基づく日米サイバー対話は、重要な二国間及び国際的な問題に関する両国の広範な関与と長期間に及ぶ協力関係を反映するもの。重要インフラに対する共通の脅威に対抗するための取組や計画における協力について、共同声明を発表。

第1回日米サイバー対話　共同声明（平成25年5月9日～10日）

日米サイバー対話は、以下の取組により、サイバーに関する幅広い協力を深化させ、日米同盟を強化した。

- サイバーに関する共通の課題についての情報交換及びあり得べき協力の手段についての議論。
- サイバーに関する国際的な協議の場における共通目的の確認。特に、サイバー空間における責任ある国家としての行動規範。
- サイバー空間におけるリスク軽減のための実効的な信頼醸成措置の構築及び政府横断的サイバー戦略の実施の支援。
- 複数のステークホルダーによるインターネットガバナンスによる開放性や相互運用性強化のための支援の確認。
- 第三国のサイバー能力構築支援に係る協力の調整。
- **政府や民間部門が重要インフラ保護のためにとることのできる行動・措置の特定。**
- 防衛・安全保障戦略において重要性を増しているサイバー防衛の役割に関する取組及び二国間のサイバー防衛協力上の新たな分野に関する議論。

日・EUインターネット・セキュリティフォーラム（平成24年11月）

経済産業省
Ministry of Economy, Trade and Industry

○「日・EUインターネット・セキュリティフォーラム」は、インターネットにおけるセキュリティ確保に関する政策や技術の動向等について日・EU間で情報交換を行う場として開催。

日・EUインターネット・セキュリティフォーラム では、

(1) インターネットにおけるセキュリティに関する政策動向についての意見交換、

(2) インターネットにおけるセキュリティに関する日EU双方のグッド・プラクティスの共有、

(3) 重要インフラ防護、官民の情報共有の在り方等についての日EU双方の取組の共有、

(4) インターネットにおけるセキュリティに関する日EU双方における意識啓発活動についての意見交換、

(5) EUにおけるオンライン上のプライバシー等に関する意見交換、

を実施。

日・EUインターネット・セキュリティフォーラムでの議論を通じて、日・EU双方において、インターネットにおけるセキュリティの確保に向けて取り組むに当たっては国際的な連携を推進することが重要であることを再確認。

「サイバーセキュリティと経済研究会」中間報告書

（平成23年8月　経産省商務情報政策局長の検討会）

経済産業省 Ministry of Economy, Trade and Industry

2010.1 Google等に対する標的型サイバー攻撃

2010.9 我が国政府機関に対するサイバー攻撃

2010.9 スタックスネットによるイランの核施設へのサイバー攻撃

2010.10 警視庁国際テロ情報流出

2010.11 尖閣諸島沖中国漁船衝突映像流出

2010.11 ウィキリークスによる米国外交公電等の暴露

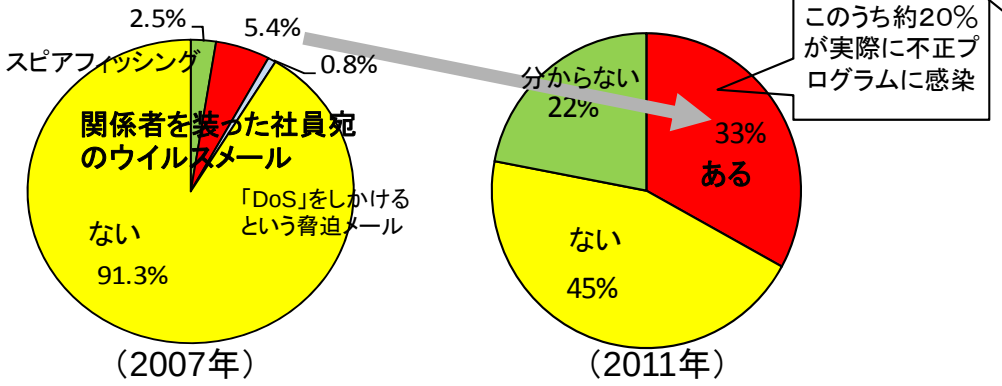
2011.3 東日本大震災によるサプライチェーン・ライフラインへの損壊

2011.4 ソニーに対するサイバー攻撃により大規模な個人情報漏えい

標的型サイバー攻撃の増加

特定の組織を標的とし、主として知的財産の詐取を目的とした**標的型サイバー攻撃が、我が国において4年間で6倍に増加**。

【我が国における標的型サイバー攻撃の有無】

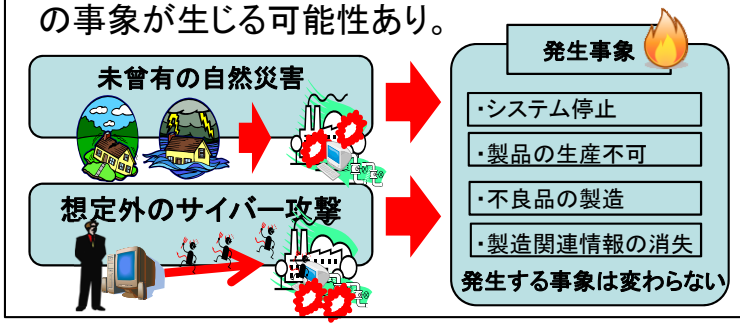


制御システムへの脅威も出現

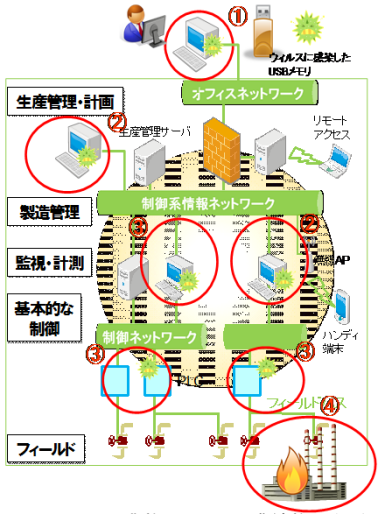
■ 発電所や工場等のプラント動作を監視・制御する**制御システムに対するサイバー攻撃が出現**。

- 海外では、プラントが1週間完全停止した事例あり。
- 日本では、設備系PC100台がウイルス感染し、工場のシステムが停止した事例などが数例あり。

■ 想定外のサイバー攻撃で東日本大震災と同様の事象が生じる可能性あり。



【スタックスネットの攻撃事例】

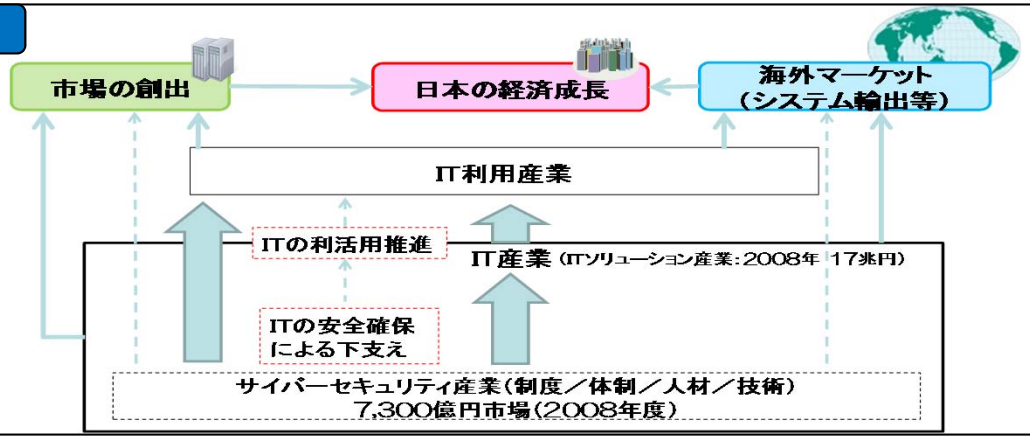


価値の源泉となる知的財産流出

企業の競争条件を悪化

情報セキュリティと経済成長

ITの安全確保は、産業の発展に必要となるITの利活用を下支えしており、我が国の経済成長に不可欠。



制御システム停止等

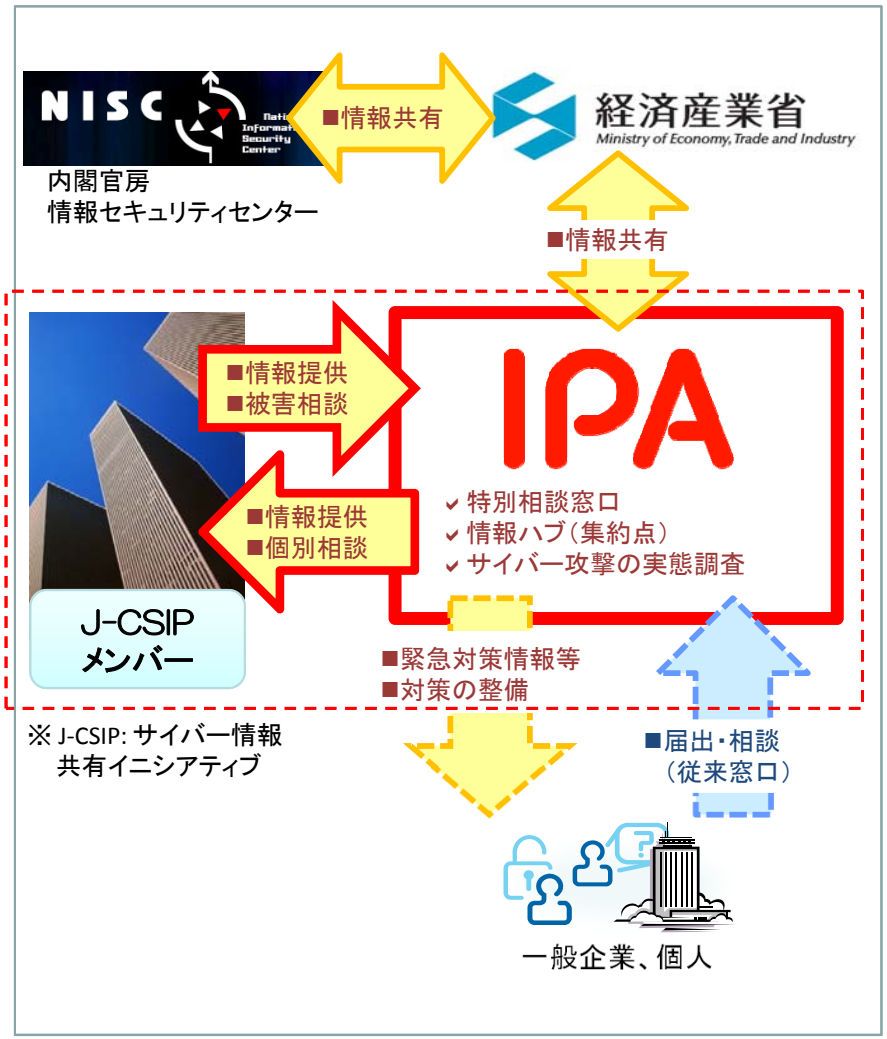
サプライチェーン ライフラインへの影響

重要インフラ等に係るサイバー情報共有イニシアティブ（J-CSIP）

経済産業省 Ministry of Economy, Trade and Industry

J-CSIP: initiative for Cyber Security Information sharing Partnership of Japan

標的型サイバー攻撃に対しては、個別企業の利害関係を越えた情報共有が社会全体の観点での最大のメリット。IPAは公的機関として、NDA（秘密保持契約）の締結を前提に、メンバー企業間の信頼できる情報ハブ（集約点）の役割を担う。



※ J-CSIP: サイバー情報共有イニシアティブ

1 「標的型サイバー攻撃特別相談窓口」の設置

ITユーザーが標的型攻撃を受けた際、駆け込み寺として、専門的知見を有する相談員による窓口を設置。

2 情報の匿名化 ＋ メンバー間での情報共有

標的型攻撃メールの内容や攻撃に使用されたウイルス等の分析結果を、信頼できる情報ハブを介して情報共有することにより、同様の標的型サイバー攻撃を未然に防止する。

3 標的型サイバー攻撃の実態調査

メンバー企業より提供された標的型攻撃メールを分析するとともに、IPAが特に「重大な攻撃が発生している」と判断する場合、対象メンバー企業の協力のもと、攻撃の実態調査を行う。

（例）・検出された不審なファイルの分析
・現地での一次調査

サイバー情報共有イニシアティブ（J-CSIP）の現状

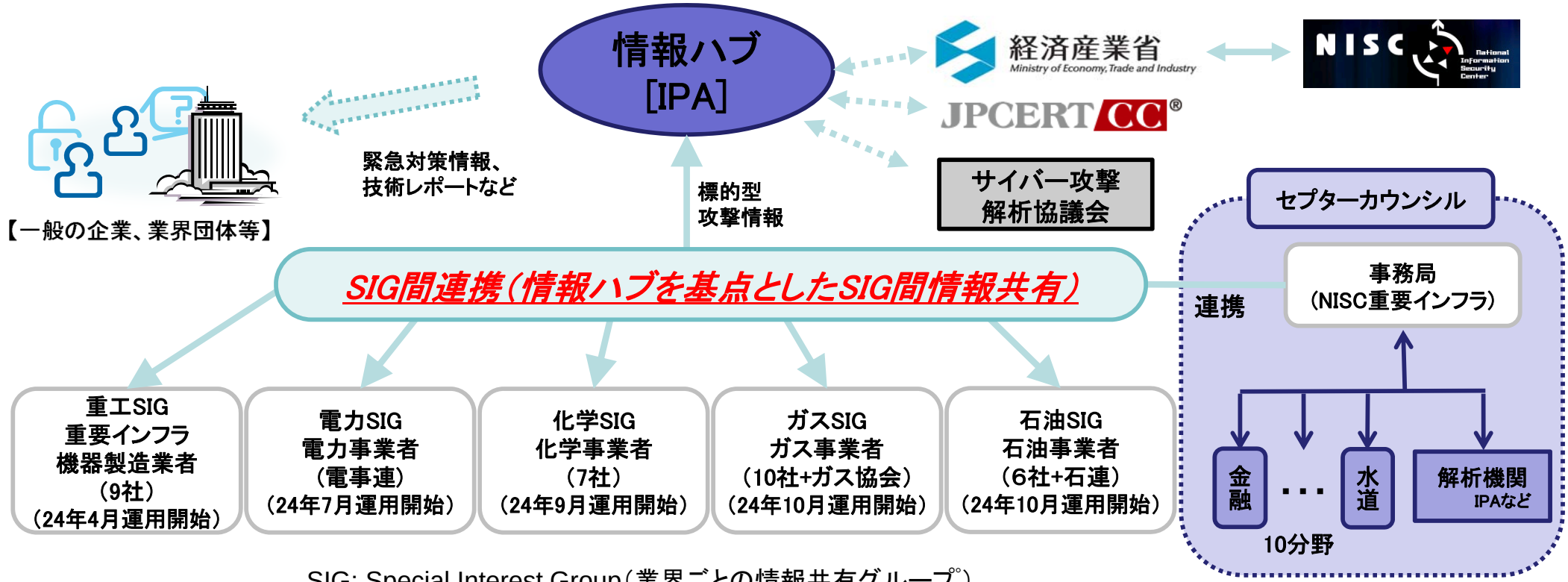
経済産業省 Ministry of Economy, Trade and Industry

＜活動の目的と背景＞

一昨年の経済産業省「サイバーセキュリティと経済研究会」の提言及び大手企業及び政府機関への標的型攻撃事案を受け早急に標的型サイバー攻撃を含む情報セキュリティ政策としての情報共有の枠組みを構築する必要から、経済産業省主管の下、重工、重電等、重要インフラで利用される機器の製造業者（9社）を中心とした**情報共有、早期対応の場としてJ-CSIPを発足（平成23年10月25日）**。

＜現状：SIG拡大とSIG間共有を実施＞

- 重工各社との間で**秘密保持契約（NDA）及び運用ルールを策定、攻撃情報の共有を開始（平成24年4月）**。
- 重工以外の重要業界毎においても情報共有体制の確立を推進することとして、電力、化学、ガス、石油業界等の代表企業と秘密保持契約を締結（～平成24年10月）。**5つの業界SIG、45組織での情報共有を実現**。
- 単一の業界内に留まらず、**業界間が連携した情報共有・連携を開始（平成24年10月～）**。



SIG: Special Interest Group（業界ごとの情報共有グループ）

J-CSIP情報共有活動の効果

経済産業省
Ministry of Economy, Trade and Industry

共有情報の活用	① 類似攻撃の早期検知（メール着弾検索） ② 攻撃侵攻の早期発見（外部アクセスログ・中間生成ファイル検索） ③ 将来攻撃のブロック（攻撃利用IPアドレスのブラックリスト設定）

活動の効果

・従来、他事業者への攻撃は全く把握できていなかったが、業界を狙った同一もしくは類似の攻撃が実際に行われていることが把握でき、共同で検知・防御できるようになった。
・NDA下で、近い業種 ／迅速な解析により密度の濃い有効な情報の共有となっており、検知と防御に有効である。
・IPAが情報共有の中継点（ハブ）となることにより、多数行われている攻撃間の相関が、ある程度、把握できるようになってきた。

2012年度の情報共有の実績

項番	項目	件数（5つのSIG、39組織での合算）
1	IPAへの情報提供件数	246件
2	参加組織への情報共有実施件数	160件　※1

※1 同等の攻撃メールが複数情報提供された際に情報共有を1件に集約して配付したり、広く無差別にばら撒かれたウイルスメールと判断して情報共有対象としない場合等があるため、情報提供件数と情報共有実施件数には差が生じる。

【参考】 ・標的型攻撃の防御に向けた産業界との情報共有の枠組み、J-CSIP（ジェイシップ）の活動レポートを公開 ＜2013/4/17＞
http://www.ipa.go.jp/about/press/20130417.html

我が国の制御システムでの脅威

経済産業省
Ministry of Economy, Trade and Industry

USBメモリ

- USBメモリからのウィルス感染事例は頻繁に発生している
- 制御システムではUSBメモリデバイス装着数が膨大であり、なくすことは不可能

リモートメンテナンス回線

- 某社は米国の中央監視室からリモートメンテナンス回線により施設をリアルタイム監視
- リモートメンテナンス回線の先の端末からの不正アクセス・マルウェア混入

操作端末の入れ替え

- 製造工場において、ベンダが入れ替えた端末にウィルスが混入していた事例あり
- 操作端末は、Windows等汎用パソコンであることが一般的

その他

- 内部犯行者は物理セキュリティをすり抜ける
- スイッチに直接PCを接続すると、不正パケット送信や盗聴可能
- 工業用無線LANからの侵入
- PCのIDやパスワードは共通化、壁に張出し

その他過去の事例：

- 端末をインターネットに接続してゲームを行っていたところウィルスに感染
- ICS-CERTで国産企業のPLCの脆弱性が公開された

日本の取組み状況

経済産業省
Ministry of Economy, Trade and Industry

2010 | 2011 | 2012 | 2013 | 2014 | 2015-

海外でのセキュリティ関連規格認証制度の普及・拡大

サイバーセキュリティと経済研究会
2010.12-2011.8

制御システムセキュリティ検討タスクフォース
2011.10-2012.4

3分野(電力・ガス・ビル)のサイバー演習

4分野(電力・ガス・ビル・化学)のサイバー演習

東北多賀城本部
セキュリティテストベッド(CSS-Base6)

東京研究センター

CSSC

技術研究組合制御システムセキュリティセンター(CSSC)
2012.3.6発足

EDSAパイロット認証プロジェクト@CSSC

CSMSパイロット認証プロジェクト@JIPDEC

技術研究組合制御システムセキュリティセンター（CSSC）

経済産業省
Ministry of Economy, Trade and Industry

http://www.css-center.or.jp/

宮城県多賀城市桜木3-4-1

みやぎ復興パーク　F21棟6階

東北多賀城本部

東京研究センター

東京都江東区青海2-4-7

独立行政法人産業技術総合研究所

臨海副都心センター別館8F

7種類の模擬システム

経済産業省
Ministry of Economy, Trade and Industry

ガスプラント

排水・下水プラント

組立プラント

化学プラント

7種類の模擬システムを構築。
サイバー攻撃によって発生した
インシデントの再現や普及啓発に活用。

ビル制御
システム

広域制御
（スマートシティ）

火力発電所訓練シミュレータ

EDSA適合性評価制度の 認証機関設置を目指して

経済産業省
Ministry of Economy, Trade and Industry

新興国を中心とした世界のインフラ需要は膨大であり、急速な都市化と経済成長により、今後の更なる市場の拡大が見込まれる。我が国は 10兆円（2010年）→ 30兆円（2020年）のインフラ製品の輸出拡大を目指す。
(**インフラシステム輸出戦略**)

分野共通的な国産の評価・認証ツールを開発し、我が国初となる制御システムの評価・認証機関を確立。民間事業者による当技術を活用した評価・認証機関の自立運営を目指す。

2012.4 — **国際標準化活動**

2013.4 — **EDSA認定審査**

2014.4 — **事業化準備（評価・認証技術開発等）**

事業化

CSSC 設立

- 評価・認証で利用できる国産ツールの開発
- 制御システム機器のパイロット認証の実施
- 評価・認証基準の策定
- 評価・認証要員の育成

国産ツールを活用し、
評価・認証を事業化

まとめ

- NISC（内閣官房情報セキュリティセンター）が取りまとめた、最新のサイバーセキュリティ戦略でも、経済とセキュリティの重要性に言及。
- 経産省では、こうした枠組の中、情報共有、重要インフラ防護のための制御システムセキュリティに取り組むとともに、産業振興にも視座を据える。
- 貿易とセキュリティ、ハードウェアとソフトウェアのセキュリティのためにも、国際標準、認証制度の活用の推進。
- 国際的な関係では、米国、EU、ASEAN等との連携。