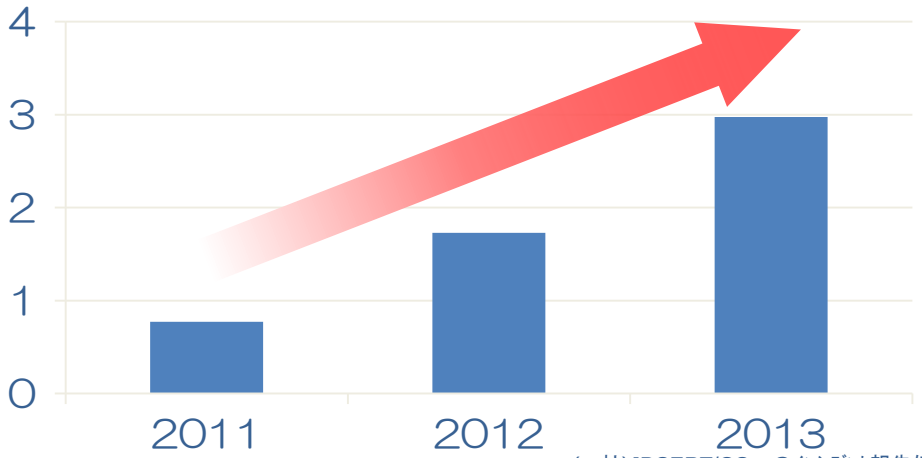
政府の情報セキュリティ政策と経済産業省における取組み

平成27年5月
商務情報政策局
情報セキュリティ政策室
室長　上村昌博

近年のサイバー攻撃の傾向

件数の増加



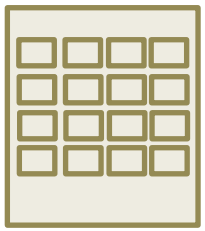
(一社)JPCERT/CCへのｲﾝｼﾃﾞﾝﾄ報告件数

※ ﾌｨｯｼﾝｸﾞ件数は100倍（2012→2013）ﾌｨｯｼﾝｸﾞ対策協議会
※ 制御ｼｽﾃﾑｲﾝｼﾃﾞﾝﾄは70%増（2012→2013） US-CERT
※ 不正送金 200倍（2012→2013） 警察庁 Webサイト改ざん2．7倍

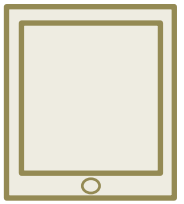
対象の拡大

（被害例）・Stuxnet イラン核施設
・DOWNAD ブラジル製鉄所
・米ﾀｰｹﾞｯﾄ社POSｼｽﾃﾑ

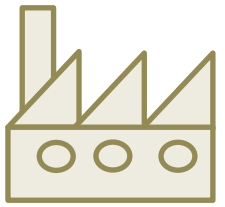
企業のネットワーク、個人PC



タブレット・スマホ



電力・ガス等のプラント



手口の進化

従来	現在
・ﾌｨｯｼﾝｸﾞｻｲﾄによるID・パスの取得	より見つかりにくく ・端末内で監視し、ﾜﾝﾀｲﾑﾊﾟｽﾜｰﾄﾞを奪取
・総当たり、辞書攻撃等による不正ログイン	より大規模に ・奪取済みのID・パスリストの当てはめによる大量不正ログイン
・メールにマルウェアを添付	より効率的に ・“水飲み場攻撃” ニュースサイト等を改ざんし、特定者からのアクセスの場合に、マルウェアを自動配信

新種マルウェアの急増

出典: McAfee Labs, 2014.

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）

	政府機関・独立行政法人等	重要インフラ事業者	企業・一般個人
「強靭な」サイバー空間（守り強化）	●機微情報を守るためのリスク評価手法の確立【2014年6月】・統一基準の見直し【同年5月】 ●GSOCの強化、CYMAT・CSIRTとの連携による 的確・迅速な対応 ●対処訓練の実施（3・18（サイバー）の日）、警察・自衛隊等の関係機関の役割整理 ●SNS・グループメールを含む新サービスに伴う新たな脅威への対応【2014年5月】	●重要インフラの範囲拡大や安全基準見直し等行動計画の見直し【2014年5月】 ●政府機関やシステムベンダー等との情報共有の強化 ●事業継続確保のための分野横断的な演習 ●重要インフラで利用される制御機器等を国際標準に則って評価・認証するための基盤構築	●スマートフォン不正アプリへの対応 ●情報セキュリティ月間・「サイバーセキュリティの日」創設【毎年2月】 ●普及啓発プログラム（2011年情報セキュリティ政策会議）の改訂【2014年7月】 ●税制など中小企業のセキュリティ投資の促進 ●ISP等による個人への感染に関する注意喚起などIT 関係事業者の取組 ●ログ保存の在り方検討などサイバー犯罪の事後追跡可能性の確保
「活力ある」サイバー空間（基礎体力）	●人材育成プログラム（2011年情報セキュリティ政策会議）の改訂【2014年5月】 ●研究開発戦略（2011年情報セキュリティ政策会議）の見直し【2014年7月】		
「世界を率先する」サイバー空間（国際戦略）	●サイバーセキュリティ国際連携取組方針の策定【2013年10月】 ●地域会合・二国間対話等によるサイバー分野の国際連携の推進・信頼醸成 ➢ 日ASEAN情報セキュリティ政策会議 ➢ 日英サイバー協議 ➢ 日印サイバー協議 ➢ 日米サイバー対話 ➢ 日EUサイバー対話 ➢ 日中韓サイバー協議 ➢ 日イスラエルサイバー協議 ➢ 日仏サイバー協議 ➢ 日エストニアサイバー協議 ●サイバー空間の国際規範づくり等に関する会議（国連政府専門家会合、サイバー空間に関するロンドン会議プロセス）等 ●IWWN注1（2014年5月・東京） ●MERIDIAN注2（2014年11月・東京）		〈注1〉サイバー空間の脆弱性、脅威、攻撃に関する国際的取組の促進。米・独・英・日等の政府機関、CERTが参加。 〈注2〉重要インフラ防護等のベストプラクティス共有や国際連携等に関する意見交換。米・英・独・日等の政府機関が参加。 ●共同意識啓発活動【毎年10月】
組織体制	●NISCの機能強化（サイバーセキュリティセンター（仮称）への改組）【2015年1月】		・GSOCの強化 ・GSOC保有情報の重要インフラ事業者との共有の仕組み ・必要な人材等の在り方　等

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国際連携取組方針／情報セキュリティ研究開発戦略（改訂版）

サイバーセキュリティ国際連携取組方針（平成 25年10月2日）

●基本原則
① 情報の自由な流通の確保
② 深刻化するリスクへの新たな対応
③ リスクベースによる対応の強化
④ 社会的責務を踏まえた行動と共助

●基本方針
① グローバルな共通認識の漸進的な醸成
② グローバルコミュニティへのわが国の貢献
③ 技術フロンティアのグローバルな拡大

●重点取組分野
(1) サイバー事案への動的対応の実践
① 多層的な情報共有体制の強化
② サイバー犯罪への適切な対応
③ サイバー安全保障における協力体制の確立
(2) 動的対応に備えた「基礎体力」の向上
① グローバルな浄化活動体制の構築支援
② 啓発活動の推進
③ 国際連携による研究開発の強化
(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
CSSC を拠点とした制御システムセキュリティの評価・認証技術を確立、CSSC の活用による新たな国際標準の提案活動への寄与
② 国際的な規範作り

情報セキュリティ研究開発戦略（改定版）（平成24年7月10日）

●今後の情報セキュリティ研究開発取組方針
(1) サイバー攻撃の検知・防御能力の向上
(2) 社会システム等を防護するためのセキュリティ技術の強化
［推進すべき施策例］
CSSCにおける制御システムセキュリティに係る国際標準化の推進とそれをベースとした国際的な相互認証制度の確立
(3) 産業活性化につながる新サービス等におけるセキュリティ研究開発
(4) 情報セキュリティのコア技術の保持
(5) 国際連携による研究開発の強化等
［推進すべき施策例］
CSSCの活用による新たな国際標準の提案活動の推進

●研究開発の効果・成果を高めるための方策等
(1) 研究成果の社会還元の推進
(2) 必要な研究開発リソースの確保と柔軟性確保
(3) 情報セキュリティ技術と他分野の融合

●情報セキュリティの研究開発における重要分野
(1) 情報通信システム全体のセキュリティ向上
(2) ハードウェア・ソフトウェアのセキュリティ向上
(3) 個人情報等の安全性の高い管理の実現
(4) 研究開発の促進基盤の確立と情報セキュリティ理論の体系化
(5) 発展が期待される応用分野でのセキュリティ確保

日本再興戦略　-JAPAN is BACK-（平成 25 年6月 14 日）

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。

〇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。

〇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。

CPS社会に求められるサイバーセキュリティ

1. ネットワークでつながる主体・端末数が増加

例）ヘルスケアデータの
予防医療等への活用

例）電力消費情報の流通
による小売市場活性化

求められるセキュリティ経営のポイント

- ビジネスパートナーへの一定基準のセキュリティ対策の要求
- 第三者認証等を活用した自組織のセキュリティ対策の情報開示

2. 所有・分析するデータの増加

例）業務委託・クラウドの活用によるビッグデータの蓄積・解析

求められるセキュリティ経営のポイント

- 委託先管理の徹底
- クラウド活用におけるセキュリティチェック

3. 影響の大きい重要システムへのつながり

例）センサーによる
インフラ管理

例）自動走行等による
交通インフラの管理

求められるセキュリティ経営のポイント

- サイバー攻撃情報の業種横断的共有による対策のアップデート
- 攻撃を受ける前提での緊急体制の整備・リスクファイナンス等の活用

予想されるリスク

○ サイバー攻撃により窃取できる企業情報の付加価値が上がり、不正な取引の対象となるおそれ

○ サプライチェーンおいて、取引先企業のセキュリティホールが原因で情報が漏洩するおそれ

○ 重要インフラにおいて、予期せぬ機器・ネットワークの入口から致命的な攻撃を受ける懸念

CPSによるデータ駆動型社会の到来を見据えた変革

CPSによるデータ駆動型社会の実現のための横断的取組

日本を、活発な企業連携等を通じて、スピード感を持って企業が試行錯誤できる「テストベッド」に

方向性Ⅰ：制度を変える

【課題】

▶ITの技術進歩を前提としていない現行制度が新たなビジネスモデルの創出を躊躇させ、企業間のデータ流通を萎縮させている。

例えば、

・ドローンと航空法との関係、シェアリングビジネスと既存業法との関係など既存規制に抵触する可能性

・セキュリティーやプライバシーへの懸念

新ビジネス創出のための制度を整備

－データを活用した新ビジネス創出のための枠組

－セキュリティリスクへの対応力向上のための枠組

－上記を含めた情報処理促進法の見直しや執行体制の整備を検討

方向性Ⅱ：チャレンジを促す

【課題】

▶自前主義に固執し、自社の強みを活かした他社との連携によるエコシステムの構築・参画ができていない。

▶ベンチャーを含め、ゲームチェンジを起こすチャレンジが限定的。

企業間連携により、新たな産業モデルを生み出す

－CPSをビジネス化する具体事例を各分野で展開
・特区活用も含め、規制改革と一体的に推進
・プライバシー、標準、セキュリティ等のルール策定

－企業間連携の中核拠点として「CPS推進協議会(仮称)」を年内に創設

－「データ流通市場」を創出するための契約ひな形等を整備

企業がCPSにチャレンジする環境を抜本的に強化

－攻めのデータ経営への転換を市場が評価する仕組みの構築(情報開示の推進等)

－ゲームチェンジを起こすITスタートアップ企業創出に向け、起業成功者が起業家を育てるスタートアップアクセラレータ組織を組成

方向性Ⅲ：基盤を整備する

【課題1：セキュリティ】

▶サイバー攻撃の高度化により、サイバーセキュリティリスクが深刻化。

国がイニシアティブを取った企業等のサイバーセキュリティ対策強化

－CPSの到来を見据えた「セキュリティ経営ガイドライン」策定

－第三者認証の強化による企業等の取組を「見える化」、同認証の国際標準化

－サイバー攻撃情報や対応策に関する、官民及び業種の垣根を越えた情報共有の仕組みづくり

【課題2：技術】

▶CPSの実現を支えるコアテクノロジーの蓄積が不十分。

CPSのコアテクノロジーを世界最先端に

－人工知能（AI）の実用化と基礎研究の進展の好循環を生むプラットフォーム機能を果たす人工知能の研究センターを産総研に整備

－外部電源が不要な自立センサシステムや大容量データの処理技術等の研究開発を強化

【課題3：人材】

▶IT人材が質・量ともにCPSに対応できていない。下請構造による低い生産性。

CPS関連のIT人材確保強化

－インド、ベトナム等の優れたIT人材活用に向け、日本への留学、就職等を支援するための官民の枠組を構築

－非効率でセキュリティリスクも高い「丸投げ下請」を防止するための「下請ガイドライン」の強化

資料：産業構造審議会 商務流通情報分科会 情報経済小委員会　中間取りまとめ（案）

サイバーセキュリティリスクと企業経営に関する研究会

研究会の目的

○　経済産業省及び（独）情報処理推進機構（IPA）は、昨年成立した**サイバーセキュリティ基本法の下**、**重要インフラ等民間事業者におけるセキュリティ対策促進**の観点から、国内外の状況整理、政策のあり方の検討を行うため、**「サイバーセキュリティリスクと企業経営に関する研究会」**を開催。

○　本研究会では、**企業の経営者の意識向上**や**官民の情報共有の促進**等を通じて、**重要インフラ企業におけるセキュリティ経営**を推進し、**安全なオリンピック**の開催、**企業価値の向上**、**リスクファイナンス市場の形成**等の**成長の好循環を作り出す**ことを念頭に、以下の論点について検討を行う予定。

【　検討事項　】

- セキュリティ経営の方法論
- セキュリティ経営を評価する仕組み
- 情報共有のあり方
- セキュリティリスクの市場化
- 2020年東京オリンピックパラリンピックに向けた対応

スケジュール

2015年1月より月１回程度開催し、6月を目途にとりまとめ。

今後の取組みの方向性（案）

1. CPS社会に求められるサイバーセキュリティ経営ガイドラインの策定

以下を主な内容とするガイドラインを、平成27年度に有識者委員会を設置して策定してはどうか。

- ○ CPS社会に求められるサイバーセキュリティ経営のポイント
- ○ CPS社会における経営層のリーダーシップと社内専門組織の設置・運用
- ○ サイバーセキュリティ人材の確保・育成
- ○ つながるビジネスパートナーと連携したセキュリティ対策の実施
- ○ 高度なサイバー攻撃に対応するための技術的対策
- ○ ステークホルダーへの情報開示のあり方

2. 同ガイドラインに基づいた第三者認証制度の確立

- ○ 1. のガイドラインも踏まえ、約4,600社が取得するISMS認証に上乗せとなる認証制度を確立。
  （注） 制御システム機器に関するIEC62443やクラウドに関する国際基準等も踏まえる予定
- ○ 第三者認証取得企業のリスクを算出し、保険会社と共有。サイバー保険を促進する仕組みの構築。
- ○ 中小事業者向けの“軽量版”認証基準についても併せて検討。

3. 官民・業種を越えた情報共有の促進

- ○ IPA（（独）情報処理推進機構）が分析ハブとなった情報共有活動（J-CSIP）の参加業種・参加企業等の拡大。
- ○ 対策向上のために共有する情報の種類等の充実も検討。

制御システムにおけるサイバーセキュリティ演習

演習の目的と概要

●目的

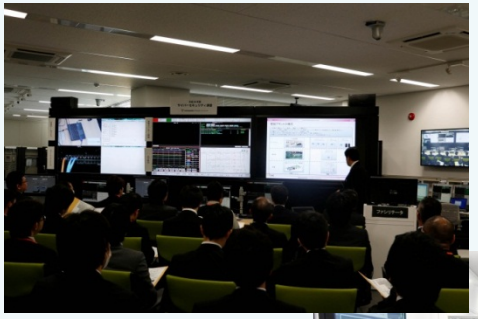
電力分野、ガス分野、ビル分野、化学分野において、現場の担当者、技術者、関係するベンダ等が、制御システムにおけるセキュリティ上の脅威を認識し、セキュリティインシデント発生の検知手順や障害対応手順の妥当性の検証を目的とするサイバーセキュリティ演習を実施し、各分野の参加者における制御システムセキュリティにおける対策を中心とした知見の獲得を促す。

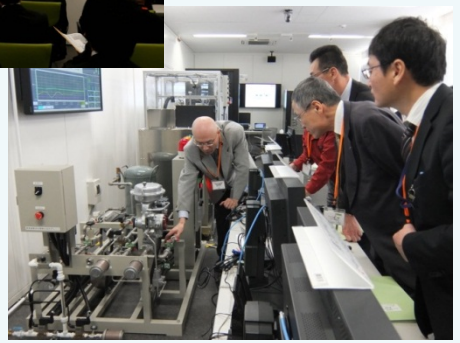
●概要

各分野において、机上演習及びCSSCの模擬プラントを用いた機能演習、意見交換会を実施。

制御システムの脅威、インシデント事例、効果的な対策、制御システム関連規格（IEC62443）等に関して習得。

日時・場所	2014年12月～2015年2月にかけて4分野、4回に分けてCSSC東北多賀城本部にて実施 ※平成26年度は3回目の実施	
参加者	4分野、109名（見学者含む）	
	電力(2/12-13)	1日目50名(うち見学17名)、 2日目52名(うち見学19名)
	ガス(12/16-17)	1日目29名、2日目29名
	ビル(1/23-24)	1日目15名(うち見学7名)、 2日目15名(うち見学7名)
	化学(1/19-20)	1日目13名、2日目13名





ASEAN地域の重要インフラ関係者等に対する情報セキュリティ強化支援

研修の目的と概要

●経緯と目的

ASEAN地域における情報セキュリティ向上のため、ASEAN関係者に対しISMSやCSMS、情報セキュリティ全般の重要性について理解を深めてもらい、参加者が自国にてそれらの取組の普及を図ることを期待。

●概要

名称：「ASEAN地域の重要インフラ関係者等に対する情報セキュリティ強化支援」研修コース
日時：平成27年2月16日(月)～2月25日(水)　※平成27年は3回目の実施
場所：一般財団法人海外産業人材育成協会(HIDA)・東京研修センター
　　技術研究組合制御システムセキュリティセンター東北多賀城本部(TTHQ)
参加者：ASEAN加盟8か国(カンボジア、フィリピン、インドネシア、ラオス、マレーシア、ミャンマー、タイ、ベトナム)の官民関係者計30名(IT関係者、エネルギー関連事業者)が参加。
研修内容：

(1) 最新の情報セキュリティトレンド、情報セキュリティの重要性、ISO/IEC27000シリーズに関する説明、制御システムの現状と将来性
(2) ISMS概論(ISO/IEC27001)
(3) CSMS概論(IEC62443-2-1)
(4) ワークショップ
(5) 企業視察