経済産業省

資料６

電力分野のサイバーセキュリティ対策について

平成２８年２月９日

資源エネルギー庁

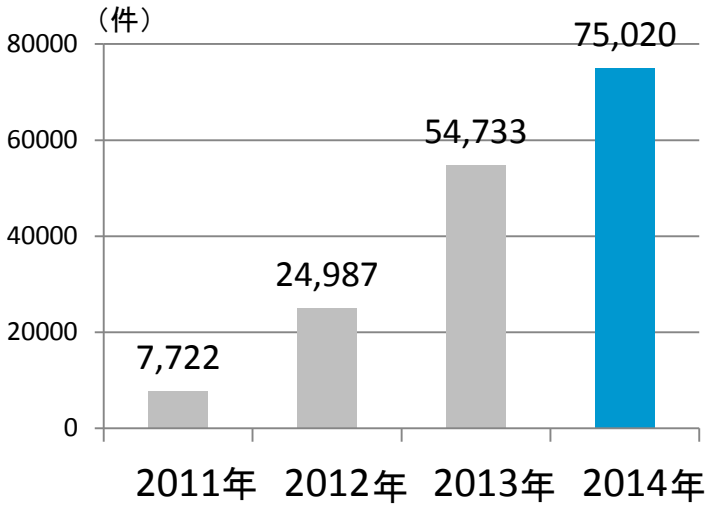
背景・問題状況

- 日本の電力制御系システムのサイバーセキュリティ対策は、従来、政府全体の重要インフラのセキュリティ枠組みをベースとした対策がなされてきた。しかし、サイバー攻撃の脅威が高まる中、各インフラ分野においては、それぞれの実情に即した、より具体的かつ実効的な対策が求められている。
- 電力分野においてはこれまで、発電・送配電・小売を一体的に担う電力会社によって一定のセキュリティ水準が保たれてきたが、自由化の進展により、コスト低減のための汎用技術の採用やシステムに接続する事業者の増加・多様化が見込まれ、サイバー攻撃のリスクが増大する可能性が高い。
- こうした新たな環境変化に対応し、２０２０年の東京オリンピック・パラリンピック大会も見据え、電力自由化を進めてきた諸外国の取組も参考にしつつ、自由化時代の電力分野におけるサイバーセキュリティ対策を検討する必要がある。

サイバーセキュリティに関する環境の変化

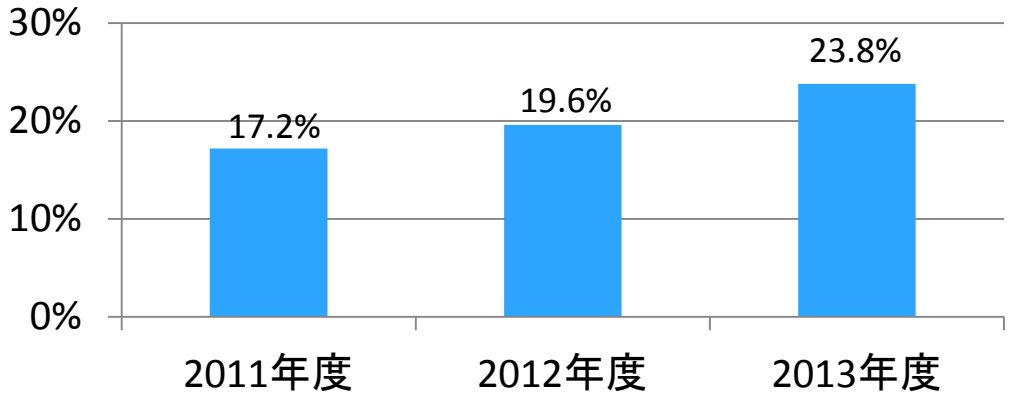
- IT利活用拡大とともに、サイバー攻撃の脅威も増大。
  - ーサイバー攻撃の事案は増加傾向
  - ー従来のばらまき型の攻撃ではなく、特定の政府関係機関や企業を狙った標的型サイバー攻撃により、個人情報等の情報が漏洩
  - ー組織的あるいは国家的な攻撃が疑われる事例も存在
  - ー近年は、制御系システムへのサイバー攻撃により、物理的な被害に及ぶ事案も発生

＜インシデント報告件数（2011年～の累計）＞



（出典）JPCERT/CCｲﾝｼﾃﾞﾝﾄ報告対応ﾚﾎﾟｰﾄにおけるｻｲﾊﾞｰ攻撃の報告受付数より経済産業省作成

＜標的型攻撃による情報漏洩等が確認された割合＞



※　母集団：従業員300人以上の企業（出典）ＩＰＡ「情報セキュリティ事象被害状況調査」2013年度、2012年度、2011年度より経済産業省作成

＜サイバー攻撃による製鉄所の操業停止（2014年）＞

・標的型メール攻撃によりドイツの製鉄所のオフィスネットワークが感染。生産設備の制御システムに侵入が拡大し、不正操作によって溶鉱炉が正常停止できず設備が破損する被害が発生。

（参考）制御系システムへのサイバー攻撃事例

＜クライスラー社・ジープチェロキーへのサイバー攻撃＞

- 昨年7月、セキュリティの研究者がクライスラー社の「コネクテッドカー」システム（スマホを使ってエンジン起動やGPSで車の現在位置を把握することができるシステム）の脆弱性を突いてハッキングできることを証明。
- 具体的には、第三者がスマホを使って遠隔操作でエンジンを切ったり、ブレーキ操作が可能。
- 同社は、約140万台をリコール。

（出典：Wired Magazine）

＜重要インフラに対する攻撃の事例＞

発電所の制御システム停止（米国、2003年）

発電所の制御システムがワームに感染。制御システムが約5時間にわたって停止。

（出典：各種報道）

ロンドン五輪への攻撃（イギリス、2012年）

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。（実際に攻撃があったかは不明）

（出典：IPA資料）

製鉄所の溶鉱炉損傷（ドイツ、2014年）

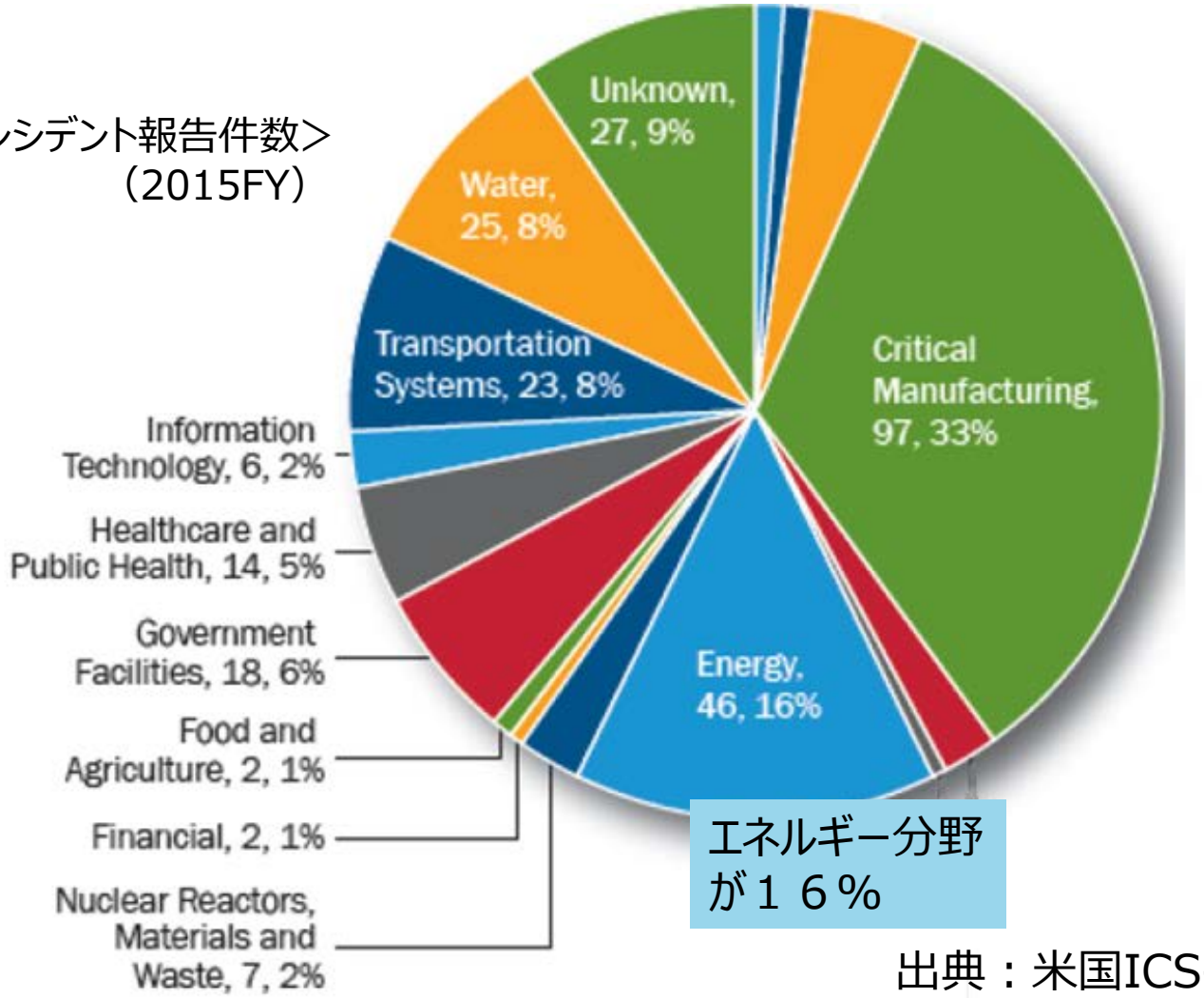
標的型攻撃により、何者かが製鉄所の制御システムに侵入し、不正操作をしたため、生産設備が損傷。

（出典：独BSI資料）

エネルギー分野の攻撃増加（海外）

- 海外の例では、重要インフラの中でも、エネルギー分野（電力・ガス・石油等）への攻撃は多い。

＜米国ICS-CERTへのインシデント報告件数＞
（2015FY）



エネルギー分野が１６％

※ICS-CERT：Industrial Control Systems Cyber Emergency Response Team
米国の国土安全保障省傘下の機関。制御系システムのサイバーインシデントについての対応・分析等を行っている。

出典：米国ICS-CERT資料

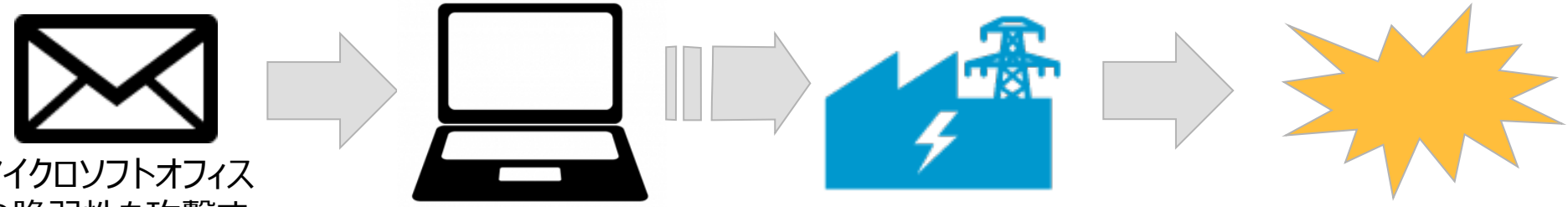
（参考）ウクライナ西部で発生した大規模停電について

- 昨年１２月、ウクライナ西部数万世帯で、数時間に渡る大規模停電が発生
- 同停電の原因はサイバー攻撃（マルウェア付きメールによる標的型攻撃が発端）と見られる
- 同停電はサイバー攻撃によって実際に大規模な停電に至った初めての事例と見られる

＜概要＞

発生日時：２０１５年１２月２３日
場所：イヴァーノ＝フランキーウシク州（ウクライナ西部）
関連するウィルス：Black Energy3（ロシアのハッカー集団sandwormが開発したとされるマルウェア）等
侵入先：州内電力会社（最大3社）関連設備
被害：リモートからのシステム制御を通じ、変電所（３０カ所）のブレーカー遮断とカスタマーサービスセンターへの問い合わせ遮断
備考：手動で復旧したため、早期（３－６時間）に停電は解消された。

＜停電までの経緯＞



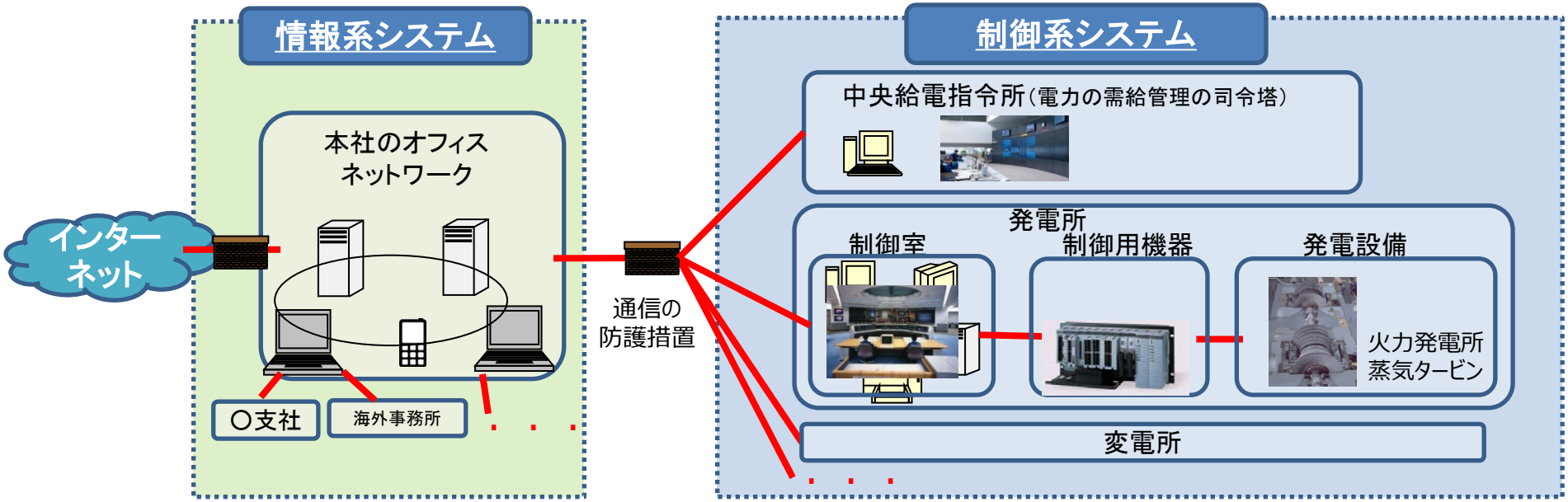
（出典：SANS, 各種報道等）

※現段階で発表・報道されている情報を集約したもの。詳細は現在国際的に調査中。

課題の整理（制御系システムと情報系システム）

- 一般的に産業用のシステムは、オフィスネットワーク等の情報系システムと、機器制御等を行う制御系システムに大別される。重要インフラサービス（電力分野では電力の安定供給）は、基本的に制御系システムによってコントロールされる。※制御系システムを有さない重要インフラ業種も存在
- 情報系システムへの攻撃に比べ、①外部との直接の接続が少なく、②事業者毎に固有の仕様部分が多い制御系システムは、詳細な内部仕様等を把握できない限り、外部からの攻撃が困難だった。
- しかし、標準技術・汎用製品利用の増加、外部ネットワークへの接続などにより、制御系システムでも、外部からのサイバー攻撃の可能性は増してきている。攻撃の脅威が存在することを前提とした対策が必要とされている。

＜情報系・制御系システムの模式図（電力分野の例）＞



（参考）課題の整理（電力システムについて一般に指摘されている脅威）

- 一般的に指摘されているサイバー攻撃の脅威には、日本の現在の電力システムに当てはまるものと、そうでないものが混在。現状を整理した上で、必要な対策を検討する必要。

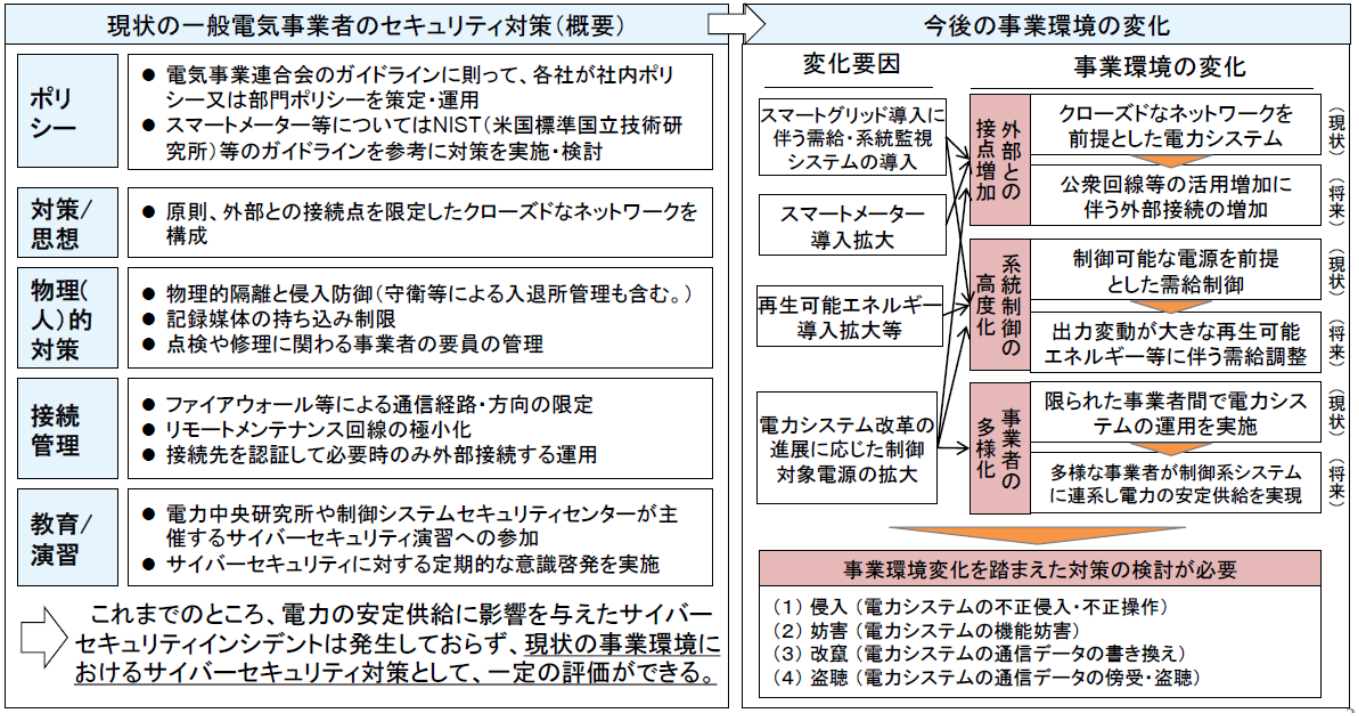
＜想定される脅威＞	＜日本の電力システムの現状＞
スマートメーターを乗っ取り、実使用量より多い使用量であるように送信すると、それを元に中央給電指令所が発電量を増やす指令を出し続ける結果、需給バランスが崩れ大停電が起こるのではないか。	スマートメーターシステムは、直接需要家付近まで機器が展開している等の特徴から、攻撃を受けやすいと想定される。ただし、日本の中央給電指令所では、スマートメーターからの使用量情報をリアルタイムの需給バランス調整に使用していないため、誤情報により大停電に至る可能性はない。
インターネットから中央給電指令所のシステムに侵入し、誤った指令を発電所等に出すことで、大規模な停電等を起こすことが可能なのではないか。	中央給電指令所システムを含む制御系システムとインターネットとの間には、多重の防壁が設置されている。また、日本では、制御系ネットワークを公衆回線を用いずに構築している。制御系ネットワークにインターネット等の公衆回線を使用している国・事業者と比較すると、直接インターネットからの侵入は相当に困難。
USB等の外部記憶媒体を用いることで、変電所等の制御系システムの端末にマルウェアを感染させ、そこから中央給電指令所にマルウェアを送り込むことができるのではないか。	USB等の外部記憶媒体のウィルスチェック等の措置は行われているが、必ずしも万全ではない。他方、中央給電指令所システムでは、通信手順に則った特定の情報しか変電所から受け付けない設計となっており、仮に変電所端末にマルウェアを感染させることができたとしても、中央給電指令所にマルウェアを送り込むことは困難。

※ここでは、「スマートメーターシステム」と「制御系システム」を区別して記載している（システム上も独立）

課題の整理（電力分野の制御系システムを取り巻く状況の変化）

- 日本の電力制御系システムでも、コスト低減の取組等により、これまでのシステム毎の固有仕様ではなく、標準技術・汎用製品の採用が進みつつある。また、IT化の進展等により、高度なIT機能が組み込まれる一方、外部との接続が増加することも想定される。
- また、システム改革によるプレーヤーの増加により、日本の電力制御系システムに関わる主体にも変化が生じていくことが見込まれる。

○現状の事業環境におけるサイバーセキュリティ対策について、一般電気事業者各社へのヒアリング及びアンケートによる詳細調査を実施。調査結果の分析によると、現状の対策は一定の評価ができる。
○ただし、今後の事業環境変化を踏まえた対策の検討が必要。



日本の電力制御系システムの現状のセキュリティ対策は一定の評価がされている。
今後の環境変化を見据えた対策が必要。

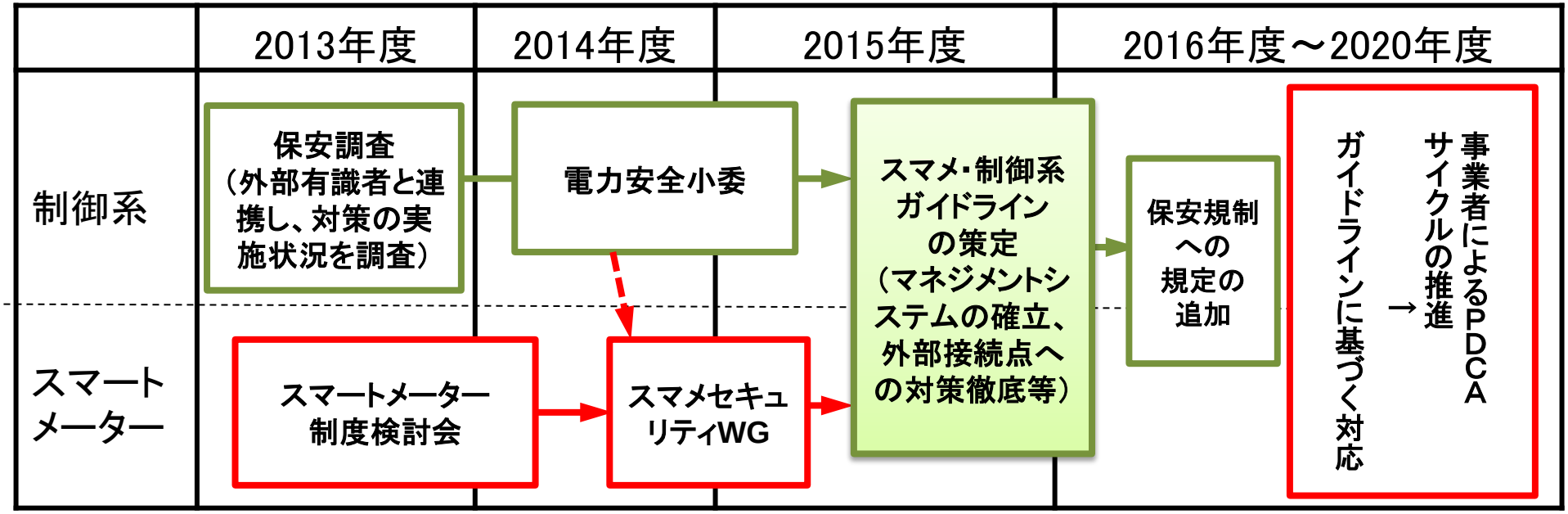
出典：産業構造審議会 保安分科会 電力安全小委員会（第5回）資料

（参考）米国の電力分野のサイバーセキュリティ対策

項目	米国の対策
①基準	NERC CIP （電力分野の義務基準） 等 ※北米電力信頼度協議会（NERC）策定の案をエネルギー規制委員会（FERC）が承認 （義務的な基準） ・NERC-CIP Standard version 3 ※今年4月からversion5が発効予定 （任意のガイドライン） ・NIST IR 7628（スマートグリッド向けガイドライン） ・ES-C2M2（マネジメント成熟度モデル） ・NIST Framework（重要インフラ全般向けガイドライン） ・NIST SP 800-82（制御系システム全般向けガイドライン） 等
②監査	北米電力信頼度協議会（NERC） ※州による規制がある場合は州政府も実施
③侵入検査（ペネトレーションテスト）	各事業者判断で実施 ※脆弱性アセスメント（机上あるいは動的なもの）についてはNERC CIPで実施を義務づけ
④情報共有	セキュリティ情報共有組織（E-ISAC）
⑤演習等	Grid Ex（系統事業者のセキュリティ演習）、Cyber Storm（米国大のサイバーセキュリティ演習）等 制御系システムセキュリティについての技術開発等も実施

電力分野のセキュリティの取組（政府及び電力業界の取組予定）

- 制御系システムについては、産業構造審議会 保安分科会 電力安全小委員会で対策を検討、取りまとめ。スマートメーターシステムについては、スマートメーター制度検討会セキュリティＷＧで対策を検討、取りまとめ。組織的・技術的な対策要件も提示。
- スマートメーターシステム、制御系システムとも、JESC（日本電気技術規格委員会）の下の専門家会議でガイドラインを策定中。策定されたガイドラインを、電気事業法の保安規制に組み込み、実効性を担保する予定。
- スマートメーターシステムについては、情報共有体制の構築・外部監査を行うことを整理。制御系システムについても、PDCAサイクルを回し続けるための仕組みの整理が必要。



（参考）重要インフラ全般のセキュリティ枠組み
（重要インフラの情報セキュリティに係る第3次行動計画）

官民連携による重要インフラ防護の推進

重要インフラにおけるサービスの持続的な提供を行い、
自然災害やサイバー攻撃等に起因するＩＴ障害が国民生活や社会経済活動に重大な影響を及ぼさないよう、
ＩＴ障害の発生を可能な限り減らすとともにＩＴ障害発生時の迅速な復旧を図ることで重要インフラを防護する

重要インフラ（１３分野）

- 情報通信
- 金融
- 航空
- 鉄道
- 電力
- ガス
- 政府・行政サービス（含・地方公共団体）
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油

ＮＩＳＣによる調整・連携

重要インフラ所管省庁（５省庁）

- 金融庁　［金融］
- 総務省　［情報通信、行政］
- 厚生労働省　［医療、水道］
- 経済産業省　［電力、ガス、化学、クレジット、石油］
- 国土交通省　［航空、鉄道、物流］

関係機関等

- 情報セキュリティ関係省庁［総務省、経済産業省等］
- 事案対処省庁［警察庁、防衛省等］
- 防災関係府省庁［内閣府、各省庁等］
- 情報セキュリティ関係機関［NICT、IPA、JPCERT等］
- サイバー空間関連事業者［各種ベンダー等］

重要インフラの情報セキュリティに係る第３次行動計画

H26.5.19 情報セキュリティ政策会議 策定
H27.5.25 サイバーセキュリティ戦略本部改訂

安全基準等の整備・浸透

重要インフラ各分野に横断的な対策の策定とそれに基づく、各分野の「安全基準」等の整備・浸透の促進

情報共有体制の強化

ＩＴ障害関係情報の共有による、官民の関係者全体での平時・大規模IT障害発生時における連携・対応体制の強化

障害対応体制の強化

官民が連携して行う演習等の実施・演習・訓練間の連携によるＩＴ障害対応体制の総合的な強化

リスクマネジメント

重要インフラ事業者等における リスク評価を含む包括的なマネジメントの支援

防護基盤の強化

広報公聴活動、国際連携の強化、規格・標準及び参照すべき規程類の整理・活用・国際展開

（参考）重要インフラ全般のセキュリティ枠組み（電力事業者の対応）

- 政府の「重要インフラの情報セキュリティ対策に係る行動計画」に基づき、電事連で自主ガイドラインを作成、電力各社が、外部接続の限定等、自主的に取組を行ってきた。
- 上記「行動計画」に基づいた情報共有に加えて、IPAの標的型攻撃に関する情報共有の枠組み（J-CSIP）などに参加。電事連内の情報共有体制も存在。
- また、ＮＩＳＣ、ＣＳＳＣ等のセキュリティ機関が主催するサイバー演習に参加。電力中央研究所を中心に、電力業界独自のサイバー演習も実施。

＜用語の概説＞

・NISC：
内閣サイバーセキュリティセンター。
「重要インフラの情報セキュリティ対策に係る行動計画（第１次～第３次）」の策定主体であり、重要インフラ全体でのセキュリティ対策の中心。

・CSSC：
制御システムセキュリティセンター。
国内のベンダーを中心とする技術研究組合。
制御機器の模擬機を有し、制御システムセキュリティの技術的な研究や演習等を行っている。

・IPA：
独立行政法人　情報処理推進機構。
情報セキュリティ、情報処理システムの信頼性向上、IT人材育成をミッションとする機関。

・J-CSIP：
IPAが主導する主に情報系システムへの標的型攻撃に関する情報共有枠組み。重工・重電等の機器メーカー及び電力・ガス・化学・石油等の重要インフラ分野の事業者による情報共有を行っている。

（参考）日本の政府全体でのサイバーセキュリティの取組

- 年金流出事案等を踏まえ、対策の強化を図るため、昨年９月にサイバーセキュリティ戦略を策定。

新たなサイバーセキュリティ戦略に基づく最初の年次計画として、2015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に係る大規模な事業に対し、セキュリティ・バイ・デザインに必要な働きかけを実施【内閣官房】
- M2M機器・IoTのセキュリティに係る横断的なガイドラインの策定【総務省及び経済産業省】
- エネルギー分野のガイドラインとして、スマートメーターのセキュリティ評価技術・手順を実証【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

- サイバー攻撃によるリスクを投資家に開示することの可能性を検討【内閣官房及び金融庁】
- 経営ガイドラインの策定【経済産業省】
- 「橋渡し人材層」としての能力向上を図るセミナー等を実施【内閣官房及び経済産業省】
- ISACを活用した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

- 政府系ファンド等の活用検討【経済産業省】
- 著作権法における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】
- 制御システムセキュリティ認証の拡大【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

- マルウェアに感染したユーザーを検知し、マルウェアの除去等を促す取組を実施【総務省】
- 安全な無線LAN環境の整備に向けて、必要となる対策の検討、周知啓発を実施【総務省】
- 通信履歴等の保存の在り方について、ガイドラインの解説の改正を踏まえ対応【警察庁及び総務省】

■重要インフラを守るための取組

- 東京オリンピック・パラリンピック競技大会に重大な影響を与えるサービス・事業者・分野の候補を選定【内閣官房】
- マイナンバーの監視・監督体制や、LGWANにおける集中的なセキュリティ監視機能の整備【特定個人情報保護委員会、内閣官房及び総務省 他】

■政府機関を守るための取組

- 各府省庁の情報システムに対してペネトレーションテストを実施【内閣官房】
- 国の行政機関における統一基準群等に基づく施策の取組状況に関する監査制度を設計するとともに、試行的な監査を実施【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

- 情報収集・分析機能の強化に加え、サイバー攻撃対策に係る訓練を実施【警察庁】
- カウンターインテリジェンスに係る取組の推進【内閣官房】
- サイバー攻撃時においても持続的な部隊運用を確保するための取組を継続【防衛省】
- 部外インフラ等、関係主体との連携深化【防衛省】

■国際社会の平和・安定

- 二国間協議や多国間協議に参画し、国際法の適用や国際的なルール・規範作り等に積極的に関与し、我が国の意向を反映【内閣官房及び外務省】
- 国際テロ組織の活動等に関する情報の収集・分析の強化【内閣官房、警察庁及び法務省】
- 各国における能力構築を支援【内閣官房 他】

■世界各国との協力連携

- ASEAN諸国との連携を強化【内閣官房 他】
- インターネットエコノミーに関する日米政策協力対話にて一致した、米国との情報共有を強化【総務省】
- 包括的な日米サイバー防衛の連携【防衛省】

横断的施策

■研究開発の推進

- 世界最先端のサイバー攻撃観測・分析技術、暗号基盤技術等に関する研究開発を実施【総務省】
- 法律や国際関係、安全保障、経営学等の社会科学的視点も含め様々な領域の研究との連携、融合領域の研究を促進【内閣官房】
- 戦略的イノベーション創造プログラム（SIP）の枠組み等により研究開発を推進【内閣府】

■人材の育成・確保

- 高度なITの知識と経営などその他の領域における専門知識を併せもつ人材の育成【文部科学省及び経済産業省】
- 初等中等教育に携わる教員等を対象とした研修、情報交換【文部科学省】
- 情報処理技術者試験において実践的な能力を適時適切に評価するための更新制度の導入の検討【経済産業省】
- サイバー防御演習を通じた実践的セキュリティ人材の育成【総務省】

推進体制

- 伊勢志摩サミットにおけるサイバーセキュリティの確保や東京オリンピック・パラリンピック競技大会に向けた対策の検討【内閣官房】