米国における電力インフラと IT をめぐる動向

八山　幸司
JETRO/IPA New York

1　はじめに

電力インフラは、安定した電力供給のために様々な取り組みが進められてきたが、効率的な電力の使用や多様化する電源の統合を目指して IT の導入が加速している。これまで、消費者の需要に応じて電力を送る形であった電力インフラだが、インターネットやスマート機器の普及によって電力需要の細かい制御が可能となり、電力網の信頼性向上のためにビッグデータや人工知能が使われ始めている。一方で、重要インフラに対するサイバーセキュリティへの懸念も拡大しており、米国ではサイバーセキュリティの情報共有や産学官の連携が強化されている。今号では、米国における電力インフラと IT の取り組みについて紹介する。

最初に、電力インフラの変化と市場の動向について紹介する。再生可能エネルギーなど電源の多様化により、大型発電所を中心とした従来の電力インフラは、IT や分散型電源を活用したスマートグリッドへと変化しつつある。また、需給バランスの細かい調整を行うためにスマート機器を用いたデマンドレスポンスや、電気の効率的な使用を可能にする電力管理システムが注目を集めており、特に、電力管理システムの市場は世界全体で大きく拡大すると見られている。

次に、電力インフラにおける IT の活用について紹介する。ニューヨーク州では、多様化する電源の統合と安定した電力供給を目指してスマートグリッドの導入を進めており、電力系統においてリアルタイムで異常を検知できる監視システムを構築している。デマンドレスポンスを活用した新しいサービスではネガワット取引と呼ばれるビジネスモデルが注目を集め、ベンチャー企業やスマート機器を提供する企業が電力会社と提携してネガワット取引を使った電力の需要調整に取り組んでいる。人工知能も様々なサービスで取り入れられ始めており、IBM 社は人工知能 Watson を様々なサービスに導入し、Verdigris 社は小型センサーと人工知能のみでオフィス内で使用されている各機器の電力使用を追跡できるサービスを提供している。

電力インフラにおけるサイバーセキュリティの動向では、サイバー攻撃の事例や取り組みについて紹介する。2015 年 12 月にウクライナで発生した電力会社を狙ったサイバー攻撃では大規模な停電が発生しており、標的型攻撃により通常のコンピューターから電力の制御システムへのアクセスが行われた。米国ではサイバーセキュリティの情報共有が積極的に進められており、情報共有の自動化に使われるプロトコールである STIX と TAXII は DHS が導入を検討するなど注目を集めている。この他、政府機関や大学機関が提供するサイバーセキュリティの標準、ガイドライン、診断ツール、診断ソフトウェアについて紹介する。

最後に、産学官における取り組みを紹介する。オバマ政権では、様々な形で重要インフラ保護の取り組みを進め、サイバーセキュリティの情報共有の強化につながった。州政府も独自の専門チームや官民連携の取り組みを進め、即応体制や情報共有を強化している。業界団体の取り組みでは、電力分野のサイバーセキュリティの情報共有を担当している E-ISAC が、政府機関を含めた大規模な模擬訓練を実施している。

電力インフラはインターネットとの統合により大きく変わろうとしているが、インターネットと電力インフラの境界が薄れてきたことでサイバー攻撃の脅威が大きくなり、サイバーセキュリティはますます重要となってきている。ウクライナの事例のようにサイバー攻撃による被害は現実のものとなってきており、米国でも国家安

全保障の優先課題として取り組まれている。次世代の電力インフラの開発とサイバーセキュリティを求められる、米国の電力インフラと IT の取り組みについて紹介する。

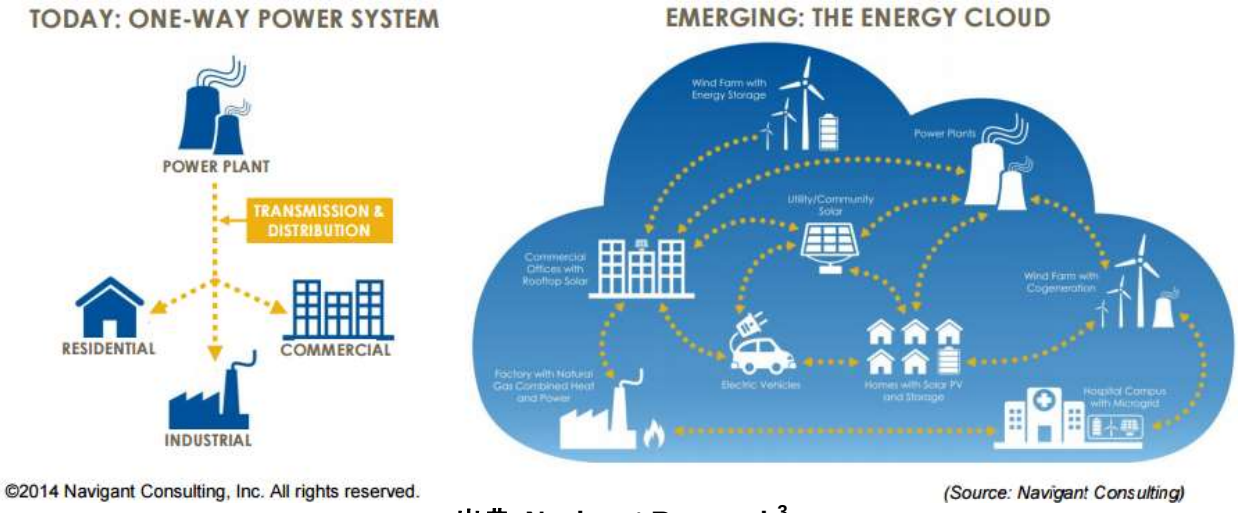
2　電力インフラと IT の市場

（1）　電力インフラの変化

発電所を中心とした電力インフラは、分散型電源や IT を活用したスマートグリッドへと移行している。従来の電力インフラは、大型発電所を中心としたものであったが、温暖化ガス削減を目的とした再生可能エネルギーの導入などにより、太陽光発電や風力発電などの分散型電源が電力インフラに統合され始めている。消費者に対しては、インターネットを使った細かい電力使用のアドバイスやスマート家電などを用いたデマンドレスポンスによる使用電力の調整など、電力ピーク時の需要を抑えるための取り組みが進められている。さらに近年では、個人での発電、エネルギー貯蔵を目的とした蓄電システム、電気自動車向けの充電ステーションなど、電力インフラは大きく変化しており、これらの変化によってこれまで大型発電所を中心としていた電力インフラは、分散型電源を活用したスマートグリッドへと変化している[1]。米調査会社 Navigant Research 社によると、分散型電源の導入は世界全体で増加傾向にあり、新しく設置される分散型電源は 2014 年の年間 87.3GW から 2023 年には年間 165.5GW に達し、2018 年には大型発電所などの集中型電源を追い抜くと見られている[2]。

図表 1 は、電力インフラの変化を示したイメージ図であり、左が従来の大型発電所を中心とした電力インフラで、右が分散型電源を活用したスマートグリッドとなっている

図表 1：電力インフラの変化



出典：Navigant Research[3]

[1] https://www.navigantresearch.com/wp-assets/brochures/WP-ECLOUD-15-Navigant-Research.pdf p.3～9

[2] https://www.navigantresearch.com/wp-assets/brochures/WP-ECLOUD-15-Navigant-Research.pdf p.4
https://www.navigantresearch.com/research/global-distributed-generation-deployment-forecast

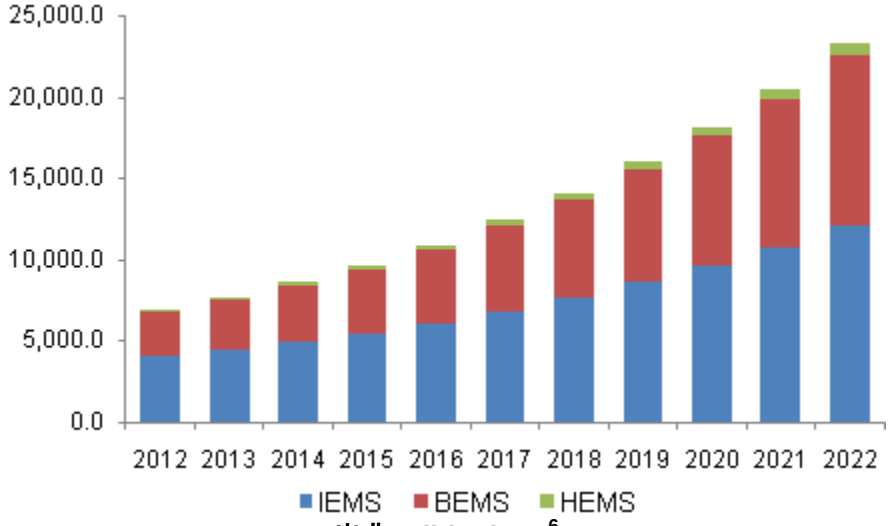
[3] https://www.navigantresearch.com/wp-assets/brochures/WP-ECLOUD-15-Navigant-Research.pdf p.9

（2） 電力管理システムの市場

スマートグリッドを活用した IT サービスの中で、顧客に様々な電力使用のアドバイスを提供する電力管理システムが注目を集めている。イギリスの調査会社 Kable Global ICT Intelligence 社によると、電力関連企業による新規システム構築への投資が増えつつあり、特に、データセンター、通信ネットワーク、アプリケーションへの投資が大きく伸びると見られている[4]。また、これらの IT 設備を使ってデータ分析を行い、効率的なエネルギー管理を行うエネルギーマネジメントシステム（Energy Management System：EMS）への投資拡大が見込まれている。米調査会社 Grand View Research 社によると、EMS の世界市場は 2014 年の 204.9 億ドルから 2022 年には 585.9 億ドルにまで拡大すると見られ、特に産業向け EMS（Industrial Energy Management System：IEMS）とビル管理向け EMS（Building Energy Management System：BEMS）の需要が高く、市場の大部分を占めると予測している[5]。

図表 2 は、エネルギーマネジメントシステム（EMS）の世界市場となっている。

図表 2：EMS の世界市場



出典：SlideShare[6]

3 電力インフラにおける IT の活用

（1） ニューヨーク州のスマートグリッドへの取り組み

電力の自由化を積極的に支援するニューヨーク州では、安価な電力と信頼性を確保するために新しい電力制御システムを導入している。米国では、1996 年に電力の小売自由化が認められたものの自由化の判断は州政府に委ねられており、2000 年に発生したカリフォルニア州の電力危機などの影響もあって、現在、電力の自由化を導入しているのは 16 州とワシントン D.C.にとどまっている[7]。その 1 つであるニューヨーク

[4] http://www.cbronline.com/news/verticals/finance/how-billion-energy-companies-invest-in-it-4684402
[5] http://www.slideshare.net/DhanashreePawar2/energy-management-systems-market-trends-company-share-to-2022-grand-view-research-inc
http://www.grandviewresearch.com/industry-analysis/energy-management-systems-market
[6] http://www.slideshare.net/DhanashreePawar2/energy-management-systems-market-trends-company-share-to-2022-grand-view-research-inc
[7] http://www.pbs.org/wgbh/pages/frontline/shows/blackout/california/timeline.html
http://www.energyserviceforless.com/deregulation-of-energy.html

州は、安定した電力供給のためにスマートグリッドの導入を支援しており、独立系統運用者[8]New York Independent System Operator（NYISO）と消費者へ電力を供給する電力会社[9]8 社がスマートグリッドを構築している。NYISO では、電力系統の位相、電圧、電流などの電力潮流関連データを収集する Phasor Measurement Unit（PMU）と呼ばれる装置を州内 50 箇所に設置し、電力系統の状態の可視化とリアルタイム監視が可能な広域監視制御システム（Wide Area Monitoring System：WAMS）を構築している。WAMS では、1 秒間に 30 回という頻度で PMU から送電施設のデータを収集し、専用回線を通して、各拠点の PMU のデータを NYISO と 8 つの電力会社へ送る仕組みとなっている。送信されるデータは GPS を使った正確な時刻のタイムスタンプが付されており、受信したデータをビッグデータとして分析することで送電網のどこで異常が発生したかリアルタイムで把握できるようになっている。これまで送電網の異常を把握するには NYISO が電力会社にデータを要請して分析する必要があったが、WAMS により直接データを受信しリアルタイムでの分析が可能になる[10]。

NYISO は、2014 年 5 月にスマートグリッドに対応した系統制御所を開設した。新しい系統制御所には、北米最大規模の管理スクリーンが設置され、電力系統の状態、電力の需供状況、PMU のデータを基にした異常検知の情報、ニューヨーク州周辺の電力市場価格などが表示される。また、天候などのデータから風力発電や太陽光発電の発電量を予測するなど、多様化する電源の統合にも対応している[11]。この他、ニューヨーク州では分散電源や再生可能エネルギーなどを促進するイニシアチブ Reforming Energy Vision（REV）を進めており、州政府からの支援を受けて電力会社の 1 つである Con Edison 社が 470 万個のスマートメーターの設置を進めるなど、様々なスマートグリッドの取り組みが進められている[12]。

図表 3 は、NYISO の系統制御所となっている。

図表 3：NYISO の系統制御所

出典：Transmission & Distribution World[13]

http://www.quantumgas.com/list_of_energy_deregulated_states_in_united_states.html

[8] 電力系統を安定して運用することを目的とした中立的な機関。電力系統の所有権は電力会社が持ち、独立系統運用者が運用を行う。

[9] 実際には電力系統を所有する送電設備所有者（Transmission Owner）と呼ばれるが、これらの企業は発電や小売も行っているため、ここでは電力会社と呼ぶ。

[10] http://www.energy.gov/sites/prod/files/2016/03/f30/Advancement%20of%20Sychrophasor%20Technology%20Report%20March%202016.pdf p.5, 75～78

[11] http://tdworld.com/asset-management-service/nyiso-opens-new-power-control-center
http://nyssmartgrid.com/nyiso-control-center/

[12] https://www.governor.ny.gov/news/governor-cuomo-announces-fundamental-shift-utility-regulation
http://www.greentechmedia.com/articles/read/new-york-prepares-for-millions-of-smart-meters-under-rev

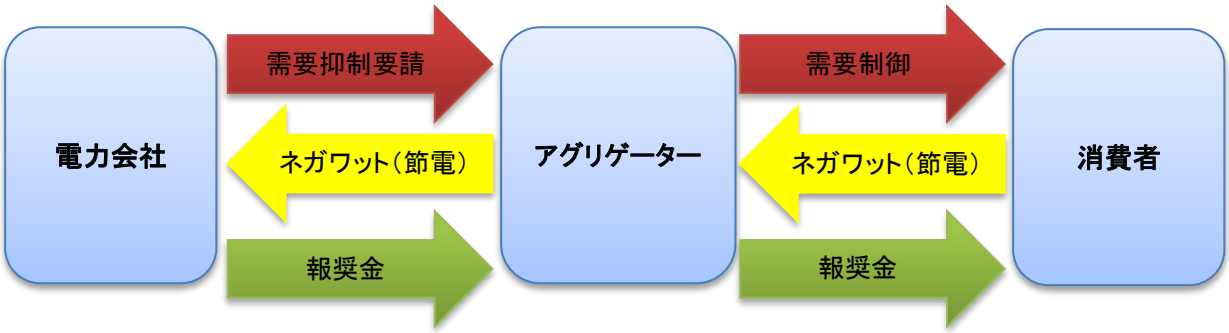
[13] http://tdworld.com/asset-management-service/nyiso-opens-new-power-control-center

（2） デマンドレスポンスを活用した新しいサービス

電力使用のピーク時に需要を抑える新しい方法として、デマンドレスポンスを活用したネガワット取引が注目を集めている。ネガワット取引とは、電力使用のピーク時に家庭や企業に節電を要請して電力需要を抑え、節電に協力した家庭や企業は節電した電力量によって払戻金やインセンティブを受けることができるビジネスモデルである。節電による電力使用の削減分はネガワット（Negawatt）と呼ばれ、ネガワットを発電と同等とみなして節電量（ネガワット量）の取引を行う。電力会社は、アグリゲーター（Aggregator）と呼ばれる企業と契約を結んであらかじめ節電する電力量を設定し、アグリゲーターは電力会社からの依頼に応じて家庭や企業の電力消費を抑制して電力需要を抑える。アグリゲーターは、節電により発生したネガワットの対価を電力会社から受け取り、その一部を消費者へと還元する仕組みとなっている。電力使用のピーク時に電気料金を引き上げることで電力需要を抑える方法に比べ、契約に応じて節電が行われるため、電力会社には確実な需要抑制ができるというメリットがある[14]。

図表 4 は、ネガワット取引の概要となっている。

図表 4：ネガワット取引の概要



出典：各種資料を基に作成[15]

すでに様々な企業がネガワット取引のサービスを提供している。EnerNOC 社は、商業ビルや企業を中心にネガワット取引のサービスを提供しており、契約した企業の消費電力を分析し、ユーザーに節電方法の指示やスマート機器を通して直接ビルの設備を操作することも可能である。同社では、企業が電力を使用する時間帯、電力量、使用用途を分析し、リアルタイムで電力料金や天候と比較して、空調の温度調節や照明の使用を控えるなどの指示を出している[16]。同社はすでに多くの電力会社と契約しており、米東部の電力会社 PJM 社、カリフォルニア州の Southern California Edison 社、テネシー州の Tennessee Valley Authority 社などのサービス地域でネガワット取引を提供し[17]、ペンシルバニア州の一部学区やビルを管理する不動産会社とも電力管理で契約している[18]。近年では、より柔軟な電力の需要調整を目指して米自動車メーカーTesla 社と蓄電システム構築での提携や、商業施設への太陽光発電を促進するために米太陽電池パネルメーカーSunPower 社と提携している[19]。

[14] http://www.meti.go.jp/committee/sougouenergy/shoene_shinene/sho_ene/pdf/011_04_00.pdf
[15] http://www.negawattmarketproject.org/what.html
[16] http://www.forbes.com/sites/jamesconca/2015/10/13/epas-clean-power-plan-needs-a-demand-response/#6ed3b1575c94
http://www.csmonitor.com/Environment/2013/1006/Energy-efficiency-How-the-Internet-can-lower-your-electric-bill
http://www.cnet.com/news/warming-up-to-climate-control-tech/
[17] https://www.enernoc.com/resources/product/demand-response/type/datasheets-brochures?search_api_views_fulltext=&page=1
[18] http://www.forbes.com/sites/jamesconca/2015/10/13/epas-clean-power-plan-needs-a-demand-response/#6ed3b1575c94
[19] http://investor.enernoc.com/releasedetail.cfm?releaseid=910188

図表 5 は、EnerNOC 社のユーザー側のデマンドレスポンスの管理画面となっている。

図表 5：EnerNOC 社のデマンドレスポンス

出典：Forbes[20]

Comverge 社は、一般家庭を対象としたネガワット取引を提供している。同社では、専用のサーモスタット（空調用リモコン）や電気温水器の制御装置を提供しており、それらの機器を調節してデマンドレスポンスを実現している。また、同社が電力管理ソフトウェア IntelliSOURCE の API[21]を使うことで他の機器でもデマンドレスポンスに利用できる[22]。様々な電力会社と提携しており、ワシントン D.C.周辺の電力会社 Pepco 社のサービス地域では、39 万個の同社のサーモスタットが設置されている[23]。

この他、スマート家電を提供する企業が電力会社と提携してネガワット取引と同様の取り組みを進めている。Google 社傘下の Nest Labs 社では、同社のサーモスタットを使った Rush Hour Rewards プログラムを提供している。同プログラムに参加している電力会社のサービス地域であれば、サーモスタットを使って節電に協力すると電力料金の払い戻しなどの特典を受けることができる[24]。ニューヨーク州の電力会社 Con Edison 社では、デマンドレスポンスに対応していない設備でもネガワット取引が可能な Smart AC プログラムを実施している。これは、Wi-fi 機能のついたスマート電源タップを使い、窓に取りつけるタイプの旧式のエアコンやスマート機能のついていない照明でも、遠隔からの操作や設定温度に応じた自動オフ機能により電気機器の使用を抑えてデマンドレスポンスを可能にするというもの。旧式のエアコンではリモコンがついていないものも多いため、サーモスタットを使ったデマンドレスポンスに参加できないという問題があり、スマート電源タップを使うことで新しいエアコンを購入することなくデマンドレスポンスに参加できるというメリットがある。特に、ニューヨーク市では窓に取り付けるタイプの旧式のエアコンが 600 万台稼動していると見られ

http://www.greentechmedia.com/articles/read/enernoc-and-sunpower-sign-exclusive-agreement
[20] http://www.forbes.com/sites/jamesconca/2015/10/13/epas-clean-power-plan-needs-a-demand-response/#1c09516a5c94
[21] Application Program Interface の略。外部のプログラムを利用するために必要な命令や規約をまとめたもので、API を使うことで容易に外部プログラムを利用できる。
[22] http://www.comverge.com/home/demand-response/load-control/#flexible
[23] http://www.comverge.com/comverge/media/pdf/Case%20Studies/Pepco-Holdings,-Inc-Case-Study.pdf
[24] https://nest.com/legal/customer-agreements-for-rush-hour-rewards/

ており、エアコンによる消費電力の大きさが問題となっている。このため Smart AC プログラムでは、低コストでデマンドレスポンスに参加し、節電によるインセンティブを受けることができるようになっている[25]。

図表 6 は、左が Nest 社の Thermostat で、右が Think Eco 社のスマート電源タップとなっている。

図表 6：Nest 社の Thermostat（左）と、Think Eco 社のスマート電源タップ（右）

出典：Hot Hardware Popular Mechanics[26]

（3） 人工知能を使ったテクノロジー

人工知能を活用した電力インフラの監視やエネルギー管理のサービスが登場している。IBM 社では、同社の人工知能 Watson を使い、スマートグリッドの監視からビルのエネルギー管理まで様々なソリューションを提供している。2016 年 1 月、米家電メーカーWhirlpool 社は IBM 社と提携しスマート家電のデータ分析に Watson を導入することを発表した。Whirlpool 社はスマート家電から送られる膨大なデータの解析に Watson を使うことで個人ごとにカスタマイズしたサービスの提供が可能となり、より効果的な節電や節水ができると見ている[27]。2016 年 2 月には、フィンランドの電力会社 Fingrid 社が電力系統の監視システムに Watson の IoT プラットフォーム「Watson IoT」を導入することを発表した。同社は、電力系統の監視システムに Watson IoT を導入することで、これまで数日かかっていたデータの解析時間の大幅な短縮が可能となり、メンテナンスの頻度の最適化や電力系統の信頼性向上につながると見ている[28]。また同月には、IBM 社とドイツの Siemens 社が提携し、Siemens 社のビル管理プラットフォームに Watson IoT を導入することが発表された。Siemens 社は、同社のビル管理プラットフォーム Navigator に Watson IoT を導入することで、ビルのエネルギー管理、ビル設備の故障予測、細かいコスト管理が可能になると見ている[29]。

Verdigris 社では、人工知能を使った電力消費の分析を行っている。同社では、企業を中心に電力消費の分析を行うサービスを提供しており、人工知能を使ったデータ分析により電力を使用している機器を識別し、リアルタイムで分析結果を企業へ提供している。データの収集には同社が提供する小型センサーをビル内

[25] http://www.prnewswire.com/news-releases/no-sweat-coolnyc-keeps-window-acs-from-hogging-all-the-electricity-300101118.html
https://conedsmartac.com/
[26] http://hothardware.com/news/google-updates-nest-thermostat-with-larger-display-slimmer-body-and-bluetooth-le
http://www.popularmechanics.com/technology/gadgets/how-to/a9174/you-can-control-your-window-ac-from-your-phone-15655768/
[27] http://www-03.ibm.com/press/us/en/pressrelease/48762.wss
[28] http://www.smartgridtoday.com/public/Fingrid-transmission-picks-IBM-Watson-for-IOT-analytics.cfm
[29] http://www-03.ibm.com/press/us/en/pressrelease/49159.wss

のブレーカーに取り付けるだけとなっている。同社は、宿泊施設、医療機関、工場などでの利用を想定しており、すでに海外の企業で導入されているという[30]。
図表 7 は、左の画像が Verdigris 社の電力管理画面で、右の画像が小型センサーとなっている。

図表 7：Verdigris 社の電力管理画面（左）と小型センサー（右）

出典：TechCrunch[31]

米 IT 企業 SmartCloud 社では、人工知能を使った産業システムの監視プラットフォーム CRex を提供している。Crex は、人工知能を使って産業システムから送られる膨大なデータの分析を行い、産業システムに異常が発生した場合のリアルタイムでの異常検知や、欠落しているデータの自動補正も可能であるという。CRex は、電力インフラ、水道インフラ、製造システムなど様々な産業システムへ利用することができるため、デマンドレスポンスや産業機器の管理など幅広く利用できる。同社は、北アメリカの電力系統の信頼性向上を目的とした機関 North American Electric Reliability Corporation（NERC）にリアルタイム監視システム SAFNR を納入しており、2015 年 8 月には同システムを人工知能の使ったシステムへとアップグレードした。人工知能を活用することで、データの遅延や重複した場合には人工知能を使ったデータ修正が可能となり、電力系統の監視データの精度向上が期待されている[32]。

4　重要インフラにおけるサイバーセキュリティ

（1）　重要インフラとサイバーセキュリティの現状

a.　重要インフラへのサイバー攻撃

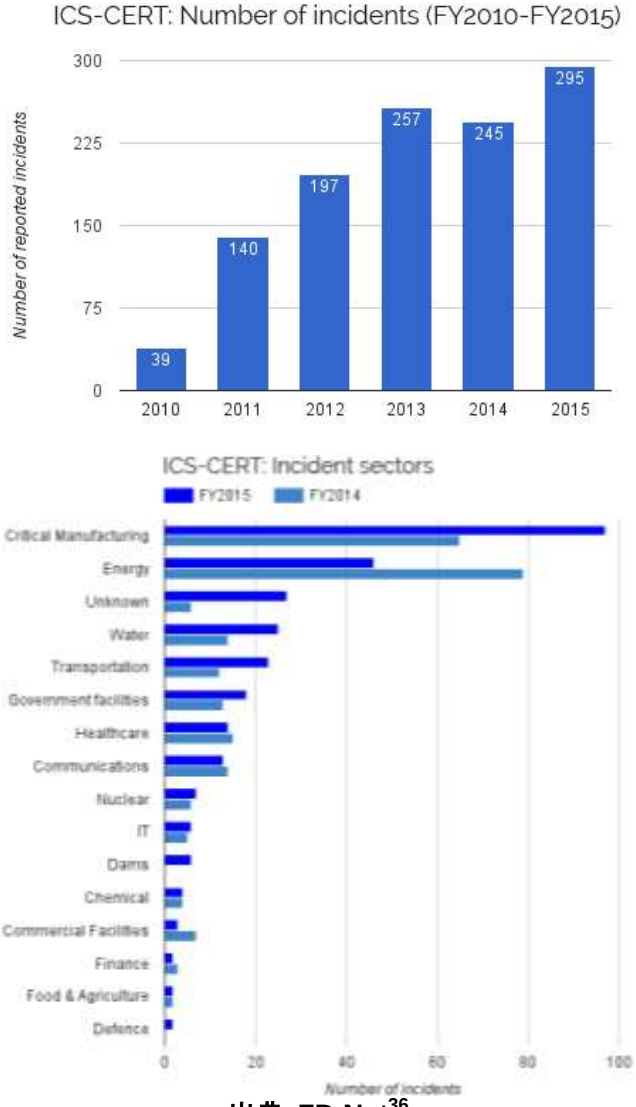
重要インフラへのサイバー攻撃は増加傾向にあり、電力インフラだけでなく様々な分野が標的となっている。米国土安全保障省（Department of Homeland Security：DHS）の傘下に置かれる、産業システムのサイバー即応チーム Industrial Control Systems Cyber Emergency Response Team（ICS-CERT）によると、2015 年度に報告された重要インフラへのサイバー攻撃による被害は 295 件にのぼり、前年の 245 件から約 20%の増加となった。分野別[33]に見た場合、重要製造業（自動車産業や航空産業など）が 97 件と最も多

[30] http://techcrunch.com/2016/03/24/verdigris-takes-9m-to-power-its-ai-energy-consumption-analytics-b2b-startup/
[31] http://techcrunch.com/2016/03/24/verdigris-takes-9m-to-power-its-ai-energy-consumption-analytics-b2b-startup/
[32] http://www.smartcloudinc.com/#!smart-grid/galleryPage
http://energy.gov/sites/prod/files/2015/04/f22/SmartCloud%20-%20Hunt.pdf p.3
http://www.businesswire.com/news/home/20150813005045/en/SmartCloud-Upgrades-AI-Driven-Situational-Awareness-NERC
[33] DHS が重要インフラと定める 16 分野。化学、商業施設、通信、重要製造業、ダム、救急サービス、情報技術、原子力、農業・食料、防衛基盤産業、エネルギー、健康＆公衆衛生、金融サービス、水、政府施設、交通システムが該当する。

く、エネルギー（46 件）、水道（25 件）、交通機関（23 件）などが続いており、様々な分野が標的となってきている。サイバー攻撃の手法別で見た場合、スピアフィッシング（Spear-phishing）[34]が 109 件と全体の 3 分の 1 以上を占めており、スピアフィッシングを用いた攻撃が重要製造業を標的として大規模に行われたため、重要製造業の被害件数が増加したと見られている。その他、ネットワークへの侵入がサイバー攻撃の手法として多く見られ、ICS-CERT は、電気、水道、ガス、石油といったネットワークを活用する重要インフラに対してサイバー攻撃への警戒を呼びかけている[35]。

図表 8 は、重要インフラへのサイバー攻撃の件数を示したグラフとなっており、上のグラフが 2010 年から 2015 年までのサイバー攻撃の件数、下のグラフが分野別のサイバー攻撃の件数となっている。

図表 8：重要インフラへのサイバー攻撃の件数



出典：ZD Net[36]

[34] 標的型攻撃とも呼ばれ、特定の個人を狙ったサイバー攻撃の一種。SNS などから個人情報を集めて知り合いを装ったメールを送り、マルウェアが感染した添付ファイルを実行させるなどの手法が使われる。
[35] https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf p.17
https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2014_Final.pdf p.6
http://thehill.com/policy/cybersecurity/266081-dhs-critical-manufacturing-cyberattacks-have-nearly-doubled
[36] http://www.zdnet.com/article/how-hackers-attacked-ukraines-power-grid-implications-for-industrial-iot-security/

b. 重要インフラを狙ったサイバー攻撃の事例

重要インフラを狙ったサイバー攻撃により、大規模な被害も現実のものとなっている。2015 年 12 月にウクライナで発生した電力会社へのサイバー攻撃では、140 万人が住む地域の約半分が 3 時間にわたって停電となり、近年発生したサイバー攻撃で大きな被害が発生した事例の 1 つとなった[37]。このサイバー攻撃では、BlackEnergy と呼ばれる強力なマルウェアとスピアフィッシングが使われており、最初の侵入経路の確保ではウクライナ議会の議員を装ったメールが電力会社の職員へ送られ、職員が重要なメールと思って添付ファイルを開いた結果、添付ファイルに感染していた BlackEnergy が活動を開始し企業内のコンピューターへ感染した。攻撃者は、感染したコンピューターを使って企業のネットワーク内を探索して、電力会社のネットワークの一部が電力系統の制御システムにつながっていることを突き止め、制御システムにアクセスして妨害工作を実行した。さらに、このサイバー攻撃と同時に電力会社のコールセンターに対して DoS 攻撃が行われており、停電の被害を拡大するために市民からの停電に関する連絡を妨害することが目的であったと見られている[38]。

スピアフィッシングを使い、「人間」という脆弱性を突いてネットワークへの入り口を確保する手法はサイバー攻撃ではよく使われる手法だが、ウクライナの事例ではこれに加え、社内ネットワークに電力系統の制御システムが接続されたネットワーク構成も悪用された。米セキュリティ企業 SentinelOne 社の CISO（最高情報セキュリティ責任者）Ehud Shamir 氏は、「IoT、SCADA、産業用制御システムは、通常の Windows が搭載されたコンピューターによって制御されていることを理解しなければならない」と述べ、通常のコンピューターが産業用制御システムの脆弱性になっていることを示した。また、ICS-CERT の調査では、2015 年に報告があったサイバー攻撃のうち約 12%が産業用制御システムのつながれている業務ネットワークにまで到達しており、通常の IT システムと産業用制御システムが密接につながれていることもサイバー攻撃に対する脆弱性として浮き彫りとなっている[39]。

重要インフラを狙ったサイバー攻撃は、情報偵察という形で表面化してきている。2013 年に米国ニューヨーク近郊のボウマン・アベニュー・ダムという洪水対策用の小型ダムの管理システムがサイバー攻撃を受け、ダムへの被害は出ていないものの情報収集が行われており、2016 年 3 月に米国政府はこのサイバー攻撃をイランによる攻撃と断定しイランのハッカー7 人を起訴した[40]。ハッカーはこの小さなダムでハッキングの練習をしていたのではないかと見られている。**図表 9** は、ボウマン･アベニュー・ダムの様子であり、非常に小さなダムであることがわかる。

[37] https://www.washingtonpost.com/opinions/a-cautionary-blackout-in-ukraine/2016/02/17/da2d58ac-b4c5-11e5-9388-466021d971de_story.html
[38] http://www.zdnet.com/article/how-hackers-attacked-ukraines-power-grid-implications-for-industrial-iot-security/
[39] http://www.zdnet.com/article/how-hackers-attacked-ukraines-power-grid-implications-for-industrial-iot-security/
[40] http://www.nytimes.com/2016/03/25/world/middleeast/us-indicts-iranians-in-cyberattacks-on-banks-and-a-dam.html

図表 9:イランのハッカーからサイバー攻撃を受けたニューヨークのボウマン･アベニュー･ダム

出典:筆者撮影

2015 年 12 月には米エネルギー大手 Calpine 社が不正アクセスを受け、ネットワークへ接続するための認証情報や米国内の 71 の発電所の設計図の情報が盗まれた[41]。この他、インターネット上のアンダーグラウンド掲示板では、侵入済みの SCADA へのアクセスを販売する書き込みが発見されており、フランスの水力発電所の管理システムと思われる画面のスクリーンショットや、テスト用アクセスのパスワードなどが書き込まれていた(実際の管理システムかどうかは確認されていない)[42]。

図表 10 は、近年発生した重要インフラへのサイバー攻撃の一覧となっている。

図表 10:近年発生した重要インフラへのサイバー攻撃

年	地域	分野	概要
2006 年	米国	水道	ペンシルバニア州の浄水施設において、SCADA にマルウェアが感染した。実害は無かったものの、水質を操作できる状態であった[43]。
2007 年	米国など	電力	Night Dragon と呼ばれるマルウェアが電力会社などのエネルギー関連企業に攻撃し、多数の機密情報が盗まれる[44]。
2010 年	イラン	電力	Siemens 社の産業用制御装置を標的としたマルウェア Stuxnet が、イランのウラン濃縮施設で遠心分離機を破壊[45]。
2013 年	米国	治水	ニューヨーク州のダム管理システムがサイバー攻撃を受け、水門を制御される事態になっていたことが 2015 年 12 月に判明した。
2014 年	米国、欧州	電力	発電所、電力系統、石油パイプラインなどのインフラを標的したマル

[41] https://blog.fortinet.com/2016/04/05/scada-security-report-2016
[42] https://blog.fortinet.com/2016/04/05/scada-security-report-2016
[43] https://ciip.wordpress.com/2009/06/21/a-list-of-reported-scada-incidents/
[44] http://www.mcafee.com/jp/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf
[45] http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

	など	石油	ウェア Dragon Fly が、米国や欧州の数百社の企業のシステムに感染し、多数の情報が盗まれた[46]。
2014 年	ウクライナ	電力	ウクライナの発電所にマルウェア BlackEnergy が感染し、大規模な停電を発生させた[47]。
2014 年	米国	電力 石油 水道	2011 年から米国内の電力、石油パイプライン、水道など様々な重要インフラのシステムに、強力なマルウェアが感染していたことを DHS が発表した。マルウェアが活動しなかったため被害はなかったと見られる[48]。
2015 年	米国	電力	米エネルギーFirstEnergy 社に大規模な DoS 攻撃が行われたが、侵入を防ぐことに成功した[49]。
2016 年	ドイツ	電力	ドイツの原子力発電所で、燃料棒の監視を行うシステムが複数のマルウェアに感染した。システムがインターネットに接続されていなかったためマルウェアは活動しなかったが USB メモリからも発見された[50]。
2016 年	イスラエル	電力	イスラエル電力公社が深刻なハッキング攻撃の被害を受けて 2 日間にわたって業務に影響が出た[51]。ハッキング攻撃ではなく、ランサムウェア[52]による被害ではないかとも見られている[53]。
2016 年	米国	医療	ロサンゼルスの病院がランサムウェアによってシステムが使用不能となった。手作業で業務は行われたが、最終的にはハッカーへ 1 万 7,000 ドルを支払った[54]。

（2） サイバーセキュリティへの対応

a. サイバーセキュリティの情報共有の自動化に向けた取り組み

サイバーセキュリティの情報共有を促進するために、情報共有の自動化が可能なプラットフォームの開発が進められている。2016 年 4 月、DHS は、重要インフラに関するサイバーセキュリティの情報共有を迅速化するために新しいシステムの導入を検討することを発表した。DHS は重要インフラにおけるサイバー脅威に関する情報の共有を担当しているが、現在使用しているシステムはペーパーワークなどの作業が発生し情報共有に時間がかかるという問題があった。2015 年 12 月に成立したサイバーセキュリティ法 Cybersecurity Information Sharing Act（CISA）において DHS がサイバーセキュリティ情報を自動的に取得することが認められ、新しい情報共有システムではサイバーセキュリティに関する情報を完全に電子化して企業や政府機関との情報共有の自動化を目指している。DHS は新しいシステムの検討に際して様々な意見を求めており、その中で、情報共有に使用するプロトコール（共有する情報や通信の技術仕様）に、政

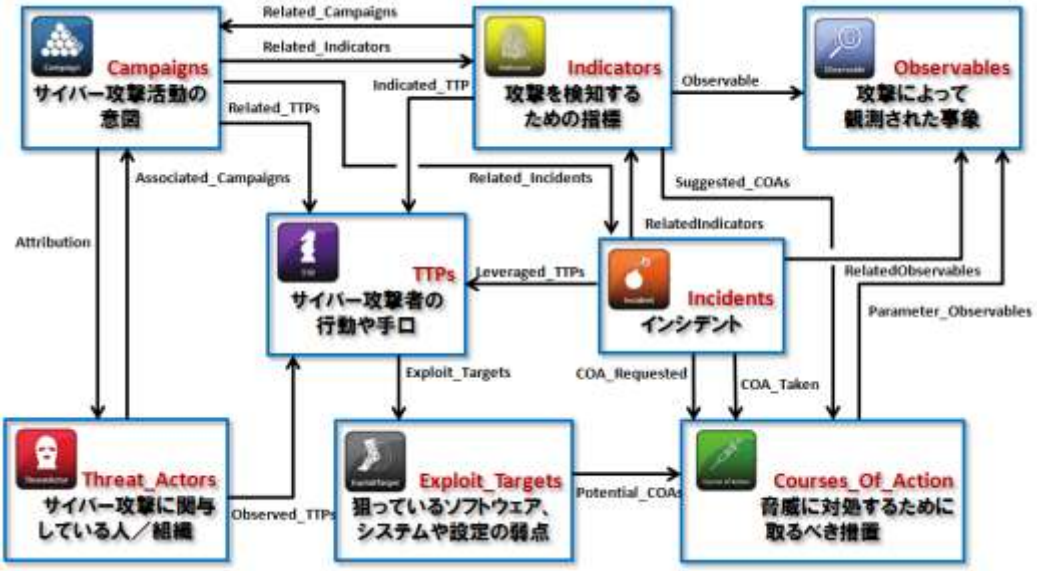
46 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf
47 http://www.zdnet.com/article/how-hackers-attacked-ukraines-power-grid-implications-for-industrial-iot-security/
48 http://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers-2011/story?id=26737476
49 http://www.utilitydive.com/news/after-fending-off-cyber-attack-firstenergy-says-government-coordination-la/407878/
50 http://arstechnica.com/security/2016/04/german-nuclear-plants-fuel-rod-system-swarming-with-old-malware/
51 http://arstechnica.com/security/2016/01/israels-electric-grid-hit-by-severe-hack-attack/
52 コンピューターを乗っ取り、ユーザーに金銭を要求するために使われるマルウェア。コンピューターを使用不能にした上で、コンピューターを復旧させるために金銭を要求するメッセージを表示することから、Ransom（身代金）とマルウェアをかけてランサムウェアと呼ばれる。
53 http://www.computerworld.com/article/3026609/security/no-israels-power-grid-wasnt-hacked-but-ransomware-hit-israels-electric-authority.html
54 http://bigstory.ap.org/article/d89e63ffea8b46d98583bfe06cf2c5af/hospital-paid-17k-ransom-hackers-its-computer-network

府向けの技術支援や研究開発を行う非営利組織 MITRE 社が策定する STIX と TAXII を候補として挙げた[55]。

STIX（Structured Threat Information eXpression）は、サイバー攻撃活動に関する様々な情報や名称を定義し標準化したもので、一定のフォーマットを用いた情報共有の自動化や、共有された情報を誤認する可能性を下げることを目的としている。STIX で標準化される脅威情報は 8 つの情報群に分けられ、サイバー攻撃活動（Campaigns）、攻撃者（Threat_Actors）、攻撃の手口（TTPs）、検知指標（Indicators）、観測事象（Observables）、インシデント（Incidents）、対処措置（Courses_Of_Action）、攻撃対象（Exploit_Targets）に分類される。例えば、「サイバー攻撃活動」の中にある「攻撃者のタイプ」の項目では、サイバー諜報活動、ブラックハッカー、ホワイトハッカー、ハクティビスト、内部脅威など、攻撃者の種類を 17 に分類している。STIX の現在のバージョンは 1.2 となっている[56]。

図表 11 は、STIX の 8 つの情報群を示した図となっている。

図表 11：STIX の 8 つの情報群



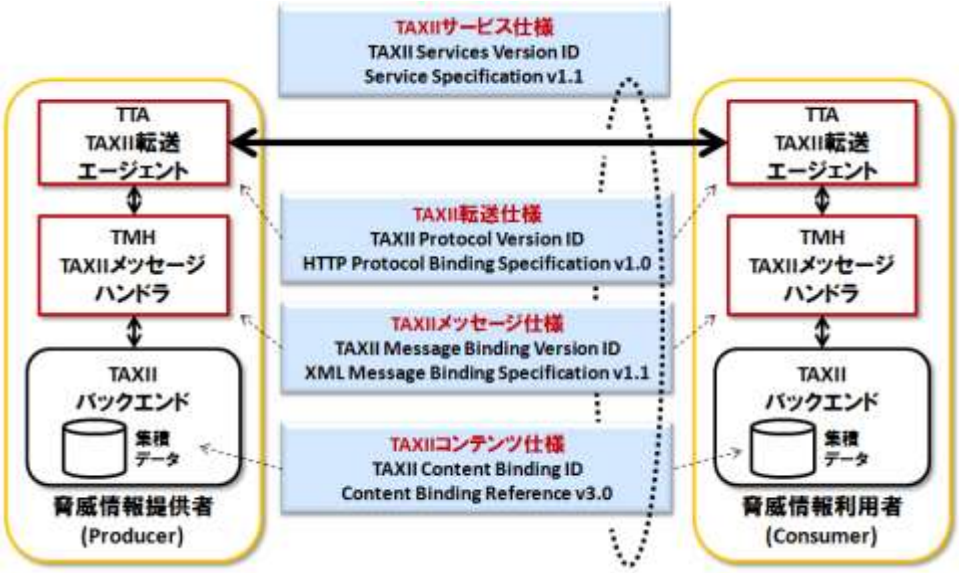
出典：IPA[57]

TAXII（Trusted Automated eXchange of Indicator Information）は、情報共有を行う際に必要なデータ通信の転送仕様やメッセージの仕様をまとめたものとなっている。TAXII で規定されている仕様は、サービス仕様、転送仕様、メッセージ仕様、コンテンツ仕様の 4 つとなっており、例えばサービス仕様では、情報の提供、情報の参照、情報の取得、情報の投稿を選び、脅威情報を提供するか受信するか選択する。通信は HTTP か HTTPS が用いられ、1 対 1 の通信だけでなく、複数への情報配信やピアツーピア（P2P）など様々な形式の通信に対応している。TAXII の現在のバージョンは 1.1 となっている[58]。

[55] http://www.nextgov.com/cybersecurity/2016/04/dhs-wants-overhaul-system-storing-sensitive-critical-infrastructure-data/127653/
[56] https://securityintelligence.com/navigating-a-sea-of-threat-intelligence-specifications/
http://www.ipa.go.jp/security/vuln/STIX.html
http://stixproject.github.io/releases/1.2/
[57] http://www.ipa.go.jp/security/vuln/STIX.html
[58] http://taxiiproject.github.io/releases/
https://securityintelligence.com/navigating-a-sea-of-threat-intelligence-specifications/
https://www.ipa.go.jp/security/vuln/TAXII.html

図表 12 は、TAXII の概要を示した図となっている。

図表 12：TAXII の概要



出典：IPA[59]

b. 様々なセキュリティガイドラインと診断ツール

電力インフラに対するサイバーセキュリティを強化するために、様々なサイバーセキュリティの標準や診断ツールが開発されている。ここでは、政府機関や大学機関が提供するサイバーセキュリティの標準、ガイドライン、診断ツール、診断ソフトウェアについて紹介する。

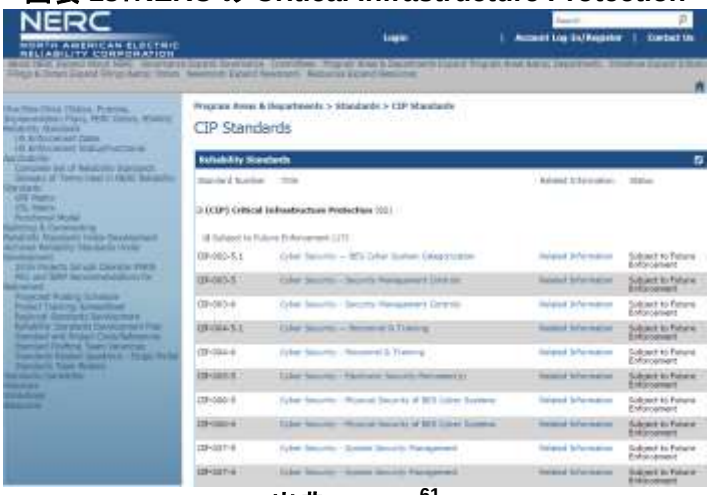
＜NERC Critical Infrastructure Protection：標準＞

北アメリカの電力系統の信頼性向上を目的とした機関である NERC（North American Electric Reliability Corporation）は、電力インフラにおけるサイバーセキュリティ対策の標準 Critical Infrastructure Protection（CIP）を提供しており、各事業者には順守が義務付けられ、違反した場合には罰則もある電力分野では重要な標準となっている。CIP では、重要施設の分類、人的資源の配置やトレーニング、インシデント発生時の対応、攻撃を受けた場合の復旧計画の策定、情報保護など、電力インフラにおける包括的なサイバーセキュリティ対策の基準が定められている。CIP はチェックリスト方式となっており、チェックリストに従って進めることでセキュリティが必要なネットワークの範囲を識別し、設備ごとに必要な対策や確認方法が定められている。2016 年 1 月には最新となるバージョン 6 が連邦エネルギー規制委員会（Federal Energy Regulatory Commission：FERC）によって承認され、これまで大規模な発電所や送電施設を対象としていたが小規模の施設まで含まれることとなった[60]。

図表 13 は、NERC の Critical Infrastructure Protection を紹介するウェブサイトとなっている。

[59] https://www.ipa.go.jp/security/vuln/TAXII.html
[60] http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
http://searchcompliance.techtarget.com/definition/NERC-CIP-critical-infrastructure-protection
http://www.subnet.com/libraries/nerc_cip_documents/guidance_for_enforcement_of_cip_standards.sflb.ashx
http://www.tripwire.com/state-of-security/regulatory-compliance/nerc-cip/hello-there-nerc-cipv6/

図表 13：NERC の Critical Infrastructure Protection



出典：NERC[61]

＜NISTIR 7628：ガイドライン＞

米国立標準技術研究所（National Institute of Standards and Technology：NIST）は、スマートグリッドのサイバーセキュリティに関するガイドラインとして NIST IR 7628 を提供している。NIST IR 7628 では、セキュリティ要件、リスク評価、スマートグリッドの設計に必要なツール、個人データを扱う際のプライバシーへの取り組みに必要なガイドなど幅広くカバーしており、電力分野の様々な事業者が利用できる内容となっている。実際の使用では、以下の 5 つのステップを踏むことでセキュリティ対策を行うことができる[62]。

1. ユースケース（使用事例）の選択
2. リスク評価
3. スマートグリッドを構成する機器の分類
4. セキュリティ要件の作成
5. スマートグリッドへの適合テスト

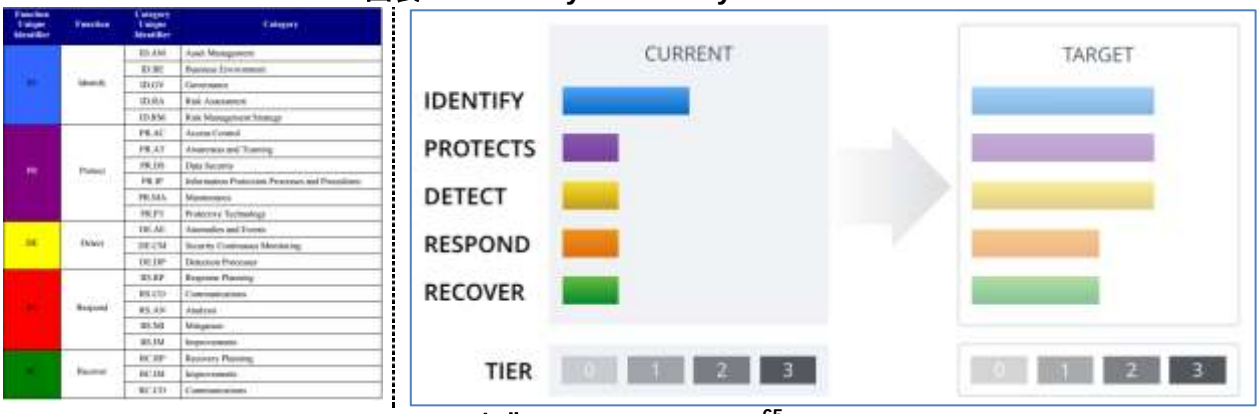
＜NIST Cybersecurity Framework：自己診断ツール＞

NIST が提供する NIST Cybersecurity Framework（NIST CSF）は、電力分野を含む重要インフラ全体を対象としたサイバーセキュリティのガイドラインとなっている。NIST CSF は、コアと呼ばれる 5 つのセキュリティ機能[63]と、ティアと呼ばれるリスクマネジメントの成熟度の 2 つで定義されている。コアの中では様々なセキュリティの要件と参照情報として様々な標準が記されており、これらを基にセキュリティ評価を行うことで現在のサイバーセキュリティへの取り組みの状況と今後の対策を把握することができる[64]。

図表 14 の左は NIST CSF のコアとなっており、右が NIST CSF を使用した場合に得られる分析結果のイメージとなっている。

[61] http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
[62] https://www.smartgrid.gov/files/nistir_7628_.pdf
http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf
[63] Identify（特定）、Protect（保護）、Detect（検知）、Respond（対応）、Recover（復旧）の 5 つのセキュリティ機能。
[64] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

図表 14：NIST Cybersecurity Framework



出典：NIST、Praetorian[65]

NIST CSF は、様々な企業で導入が進んでおり、米セキュリティ企業 Tenable Network Security 社と米調査会社 Dimensional Research 社が米国内の IT 技術者 300 人に対して行った調査によると、84%の企業が NIST CSF をサイバーセキュリティ・フレームワークの 1 つとして採用しており、約 70%が最も良いフレームワークと捉えている。また、NIST CSF を採用している企業のうち 29%が他社からビジネス要件として求められ、28%が政府との調達契約の要件として求められたため導入したという[66]。NIST CSF をサイバー保険に活用する動きも出ており、2016 年 4 月に開催された Cybersecurity Framework Workshop 2016 では、Zurich Insurance 社など複数の保険会社が NIST CSF のサイバー保険のリスク査定への活用について議論した。その内容によると、NIST CSF を活用することでサイバーセキュリティのリスクについて業界の共通基準が生まれ、保険会社、ブローカー、保険の引き受け企業などの間で議論をしやすくなり、より良い保険商品を低価格で出すことにつながるのではないかと見ている[67]。

＜Cybersecurity Capability Maturity Model：自己診断ツール＞

DOE は、電力分野の企業向けにサイバーセキュリティの取り組みを自己診断できる Electricity Subsector Cybersecurity Capability Maturity Model（ES-C2M2）を提供している。ES-C2M2 は、サイバーセキュリティへの対応強化、評価とベンチマークの実施、知識やベストプラクティスの情報共有、必要な対応の優先順位の把握など、主に企業のマネジメントの面からセキュリティ評価をする自己診断ツールとなっている。企業のサイバーセキュリティへの対応状況を、リスク、資産、即応体制、情報共有、人員といった 10 分野に分け、対応状況を 4 段階に分けて評価する。ES-C2M2 では、サイバーセキュリティへの対応状況の評価が行われるのみであり、改善策は企業が検討する必要があるため、繰り返し ES-C2M2 を使った評価を行って、進行状況を確認する必要がある[68]。

＜Smart Grid Maturity Model：自己診断ツール＞

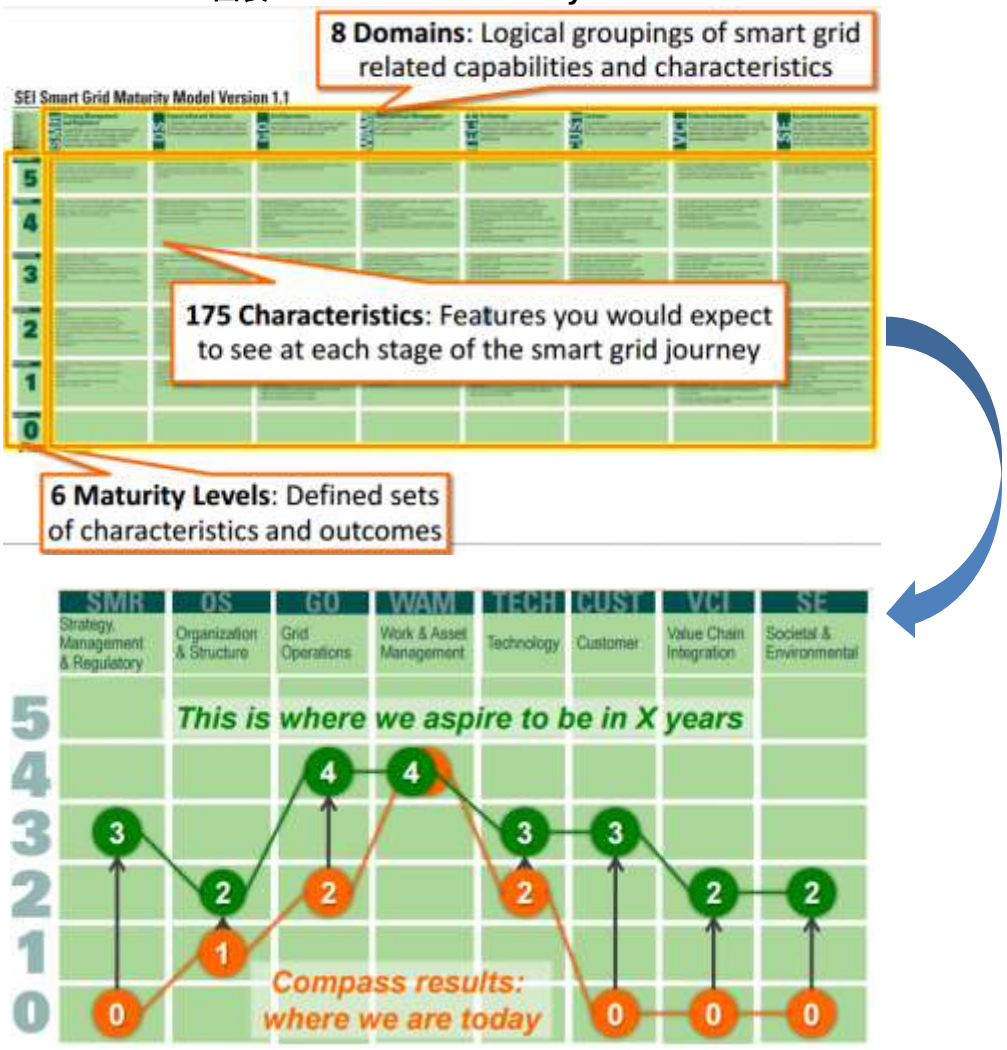
Carnegie Mellon University のソフトウェア研究所 Software Engineering Institute（SEI）は、スマートグリッドの取り組み状況を確認できる自己診断ツール Smart Grid Maturity Model（SGMM）を提供している。SGMM は、スマートグリッドの成熟度を段階的に示し、現在のスマートグリッドの導入状況や割り当てられるリソースを把握し、将来的な導入に向けた戦略を立てることができる自己診断ツールとなっている。SGMM は質問形式となっており、スマートグリッドへの取り組みについて戦略、組織、技術、運用など 8 つの分野について様々な質問への回答を行い、それぞれの成熟度を 6 段階に分けて評価を行う。今後の戦

[65] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
https://www.praetorian.com/blog/nist-cybersecurity-framework-vs-nist-special-publication-800-53
[66] http://static.tenable.com/marketing/tenable-csf-report.pdf p.2
[67] https://multimedia.telos.com/blog/empowering-nist-cybersecurity-framework-cyber-insurance/
[68] http://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf

略について策定する場合には、SEI から認定を受けた SGMM Navigator からのサポートが必要となる。SGMM を導入している企業は 2011 年の時点で 120 社にのぼり、米国以外にもアジアなどで導入されている[69]。

図表 15 は、Smart Grid Maturity Model の概要となっている。上の図は、8 つの分野と 6 段階の成熟度を表にまとめたもので、その中にはそれぞれの成熟度の段階で達成すべき基準が書かれている。下の図は、評価を行った場合のイメージとなっており、現在の成熟度の段階から目標とする段階までに取り組むべき内容を確認できるようになっている。

図表 15：Smart Grid Maturity Model



出典：Department of Energy[70]

＜Cyber Security Evaluation Tool：自己診断ソフトウェア＞

ICS-CERT は、産業システムのセキュリティ評価が可能なソフトウェア Cyber Security Evaluation Tool（CSET）を提供している。CSET は、NERC CIP や NIST CSF など複数のセキュリティ基準をベースに、情

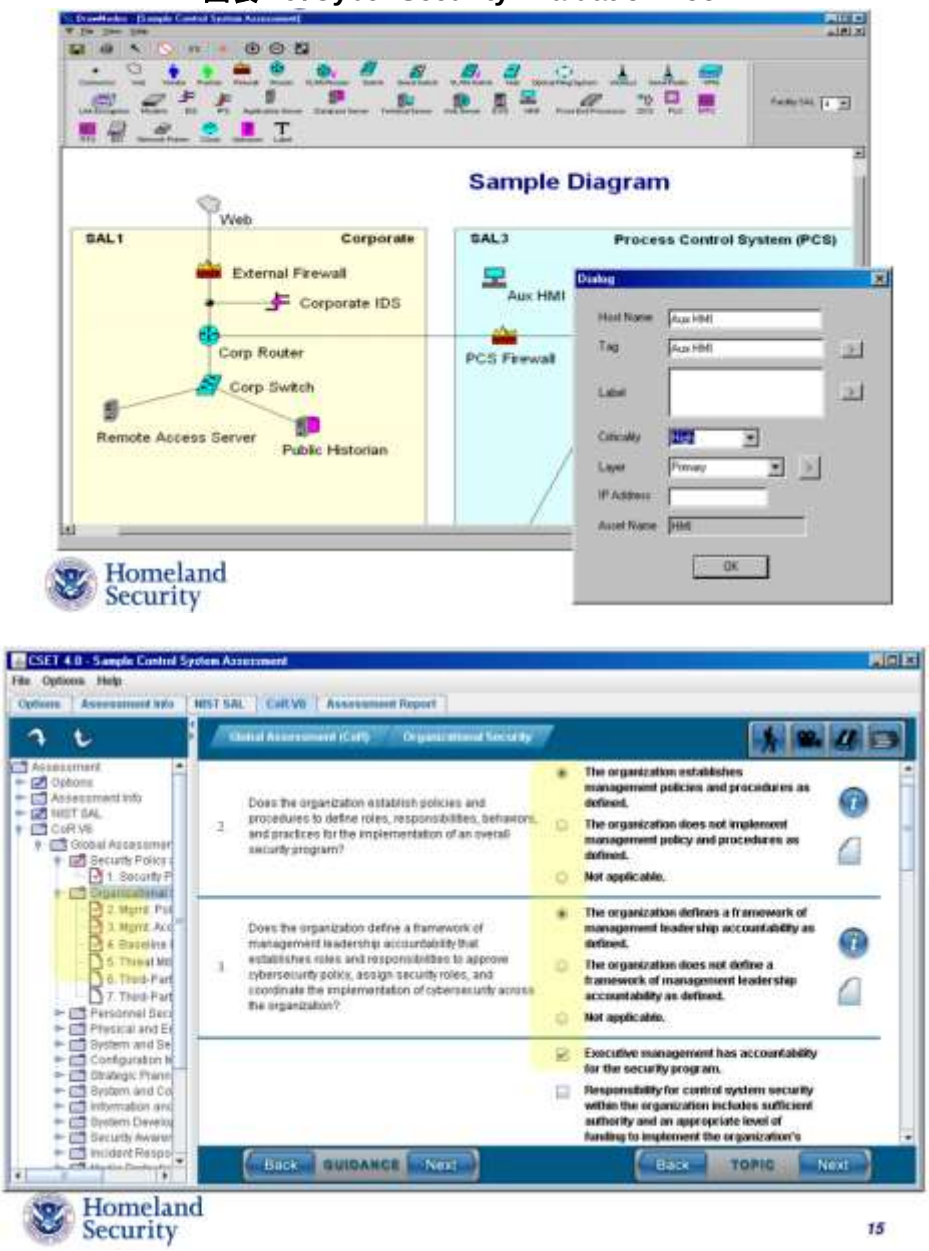
[69] https://resources.sei.cmu.edu/asset_files/Brochure/2011_015_001_28227.pdf
http://www.sei.cmu.edu/certification/opportunities/sgmm/

[70] http://energy.gov/sites/prod/files/SG%202010%20Peer%20Review%20-%20Smart%20Grid%20Maturity%20Model%20-%20Austin%20Montgomery,%20CMU.pdf

報システムや産業用制御システムのサイバーセキュリティの対策状況を評価できるソフトウェアとなっている。CSET は質問形式だが、セキュリティ基準や目標とするセキュリティレベルを選択し、ネットワークやシステム構成を画面上で作成すると、セキュリティ評価に必要な質問が自動生成される。評価結果は、対応すべきセキュリティの優先順位や改善案とともにレポートとして出力される[71]。

図表 16 は、Cyber Security Evaluation Tool の画面となっている。

図表 16：Cyber Security Evaluation Tool



出典：Department of Homeland Security[72]

[71] https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_CSET_S508C.pdf
https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_CRR_CSET_S508C.pdf
http://www.novasame.org/presentations/ephs-2012-dhs.pdf
[72] http://www.novasame.org/presentations/ephs-2012-dhs.pdf

5　産学官における取り組み

（1）　連邦・地方政府によるサイバーセキュリティへの取り組み

a.　連邦政府の取り組み

オバマ政権では、重要インフラのサイバーセキュリティを国家戦略と位置づけ、様々な取り組みにより情報共有の強化につながった。オバマ政権で重要インフラに関連した最初の具体的な取り組みは、2013 年 2 月に出された大統領令 13636 号（EO 13636）と大統領政策指令 21 号（PPD-21）であり、この 2 つでは NIST へのサイバーセキュリティ・フレームワークの作成や、DHS に重要インフラのセキュリティ確保に向けた取り組みが盛り込まれた[73]。2014 年 12 月に成立した National Cybersecurity Protection Act では、DHS 内に設置されている National Cybersecurity and Communications Integration Center（NCCIC）の法的権限を明確化した[74]。

2015 年 2 月には、官民間のサイバーセキュリティの情報共有の促進を目的とした大統領令 13691 号（EO 13691）と[75]、サイバー攻撃の情報を分析する Cyber Threat Intelligence Integration Center（CTIIC）がホワイトハウス主導により設立された[76]。大統領令 13691 号では、サイバーセキュリティに関する情報共有を重要インフラの各分野や地域ごとに行う団体 ISAO（Information Sharing and Analysis Organization）の立ち上げが提言されているが、重要インフラの分野ごとに情報共有を行う団体 ISAC（Information Sharing and Analysis Center）とは異なり、ISAO では会計や法律といった分野横断的な取り組みや地域ごとの情報共有など、より柔軟なサイバーセキュリティの情報共有を目的としたものとなっている[77]。

2015 年 12 月にはサイバーセキュリティの情報共有に関する法律 Cybersecurity Information Sharing Act（CISA）が成立し、企業は、サイバーセキュリティの脅威に関する情報を政府や他の企業と共有しても罪に問われないことが定められた[78]。2016 年 2 月には、ホワイトハウスからサイバーセキュリティの長期的な戦略計画として Cybersecurity National Action Plan（CNAP）が発表され、サイバーセキュリティ強化委員会の設置や、2017 年度予算におけるサイバーセキュリティ関連予算の 190 億ドルの増額が盛り込まれた[79]。

b.　州政府の取り組み

州政府による重要インフラのサイバーセキュリティへの取り組みは、専門チームや官民連携によって進められている。カリフォルニア州はサイバーセキュリティに対応した様々なチームを立ち上げており、州の危機管理局（California Office of Emergency Services：Cal OES）に重要インフラ保護の実行部隊として Critical Infrastructure Protection（CIP）部門が設置されている。2013 年には自治体や企業と連携して州全体のサイバーセキュリティの向上に取り組む Cybersecurity Task Force（CTC）が設立されており、CTC によって

[73] https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
[74] https://www.insideprivacy.com/united-states/congress-passes-four-cybersecurity-bills/
[75] https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari
[76] https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center
[77] http://www.boozallen.com/content/dam/boozallen/documents/building-the-next-generation-isac_fs.pdf
https://www.dhs.gov/isao-faq
https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari
[78] https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/
[79] https://www.insideprivacy.com/data-security/cybersecurity/white-houses-cybersecurity-national-action-plan-cnap-includes-cybersecurity-awareness-campaign-creation-of-federal-privacy-council/

サイバーセキュリティ人材を民間から育成する CyberCalifornia イニシアチブが立ち上げられた[80]。2015 年 8 月には Jerry Brown 州知事により、サイバー攻撃の即応チームとして California Cybersecurity Integration Center（Cal-CSIC）が設立されるなど、様々なサイバーセキュリティの専門チームが立ち上げられている[81]。この他、カリフォルニア州の公共事業委員会 California Public Utilities Commission（CPUC）が州独自のサイバーセキュリティ情報共有プログラム CES-21 を立ち上げており、各事業者と研究機関で情報共有を行うなど、独自のサイバーセキュリティへの取り組みを進めている[82]。

ニューヨーク州におけるサイバーセキュリティ対策では、官民連携による取り組みが進められている。ニューヨーク州政府のサイバーセキュリティは、Enterprise Information Security Office（EISO）が一手に担っており、傘下には、緊急即応チーム Cyber Incident Response Team（CIRT）やセキュリティ司令室 Cyber Security Operations Center（CSOC）などが配置されている[83]。2016 年 5 月には、ニューヨーク州の上院議会がサイバーセキュリティへの取り組みを強化する法案を通過させており、同法案では、重要インフラのセキュリティ強化を目的に大きく分けて、①サイバーセキュリティに関する情報共有の強化、②市民や企業との連携の強化、③サイバーセキュリティの助言を出す諮問機関の設置が定められている[84]。この他、スマートグリッドの関係企業で構成されるコンソーシアム New York State Smart Grid Consortium では、官民連携によるサイバーセキュリティを含めたスマートグリッドの取り組みを進めている[85]。

（2） 業界団体や産学官の取り組み

a. 業界団体の取り組み

電力分野の業界団体では、NERC が中心となって、サイバーセキュリティのガイドライン策定や情報共有などに取り組んでいる。同機関は、電力分野におけるサイバーセキュリティの情報共有を担当する Electricity ISAC（E-ISAC）を管理しており、E-ISAC には 800 以上の企業と 3,400 人以上の専門家が参加している。E-ISAC では、参加企業や他分野の ISAC から寄せられたセキュリティに関する情報を対策センターである Security Operations Center へと集めて専門チームによる分析を行っており、サイバーセキュリティに関する情報以外にもテロリズムや自然災害など幅広い情報を取り扱っている[86]。

E-ISAC は、電力系統への攻撃を想定した模擬訓練を 2 年ごとに開催しており、2015 年 11 月には第 3 回目となる「GridEx III」が開催され、364 の企業や政府機関から 4,400 名以上が参加した。GridEx III は、電力系統への様々な攻撃を想定したシナリオへ対応するというもので、電力系統を管理する企業は攻撃を受けた場合のシナリオを電子メールで受け取ってそれぞれが対応を進め、ホワイトハウス、DOE、DHS、米軍の担当組織なども政府側からシナリオに対応する訓練内容となっている[87]。電力系統への攻撃を想定したシナリオはサイバー攻撃だけでなく、発電所へのドローンの飛来、変電所での火事、銃火器を用いた直接的な攻撃、通信機能の喪失、地震などの災害といった様々な内容が想定されている[88]。

[80] http://pellcenter.org/wp-content/uploads/2015/11/Pell-Center-State-of-the-States-Report.pdf p.9～13
[81] http://pellcenter.org/wp-content/uploads/2015/11/Pell-Center-State-of-the-States-Report.pdf p.9～13
[82] http://www.sgip.org/wp-content/uploads/SGIP-White-Paper-Cybersecurity-Information-Sharing-in-Electric-Utilities.pdf p.5
[83] http://pellcenter.org/wp-content/uploads/2015/11/Pell-Center-State-of-the-States-Report.pdf p.26～27
[84] https://www.nysenate.gov/newsroom/press-releases/senate-passes-legislation-strengthen-cyber-security-defense-new-york
[85] http://nyssmartgrid.com/
[86] http://www.texasre.org/CPDL/Spring%202016%20Standards%20and%20Compliance%20-%205%20-%20E-ISAC%20-%20Dave%20Halla%20and%20Darrell%20Moore%20-%20for%20posting.pdf p.4～6
[87] http://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf p.1～3
[88] http://www.iso-ne.com/static-assets/documents/2016/04/a7_gridex_3_results.pdf p.11～12
http://www.eenews.net/stories/1060029575

b. 産学連携の取り組み

電力分野における産学官連携の取り組みは、サイバーセキュリティやオープンソースのソフトウェア開発など様々な取り組みが進められている。米下院の国土安全委員会（Homeland Security Committee）は、2016 年 4 月、産学官連携による地方レベルでのサイバーセキュリティを支援する法案を承認した。この法案は、国家戦略的なサイバーセキュリティに取り組む複数の大学機関で構成される National Cybersecurity Preparedness Consortium と DHS が連携し、重要インフラ企業、自治体、州政府機関にサイバーセキュリティトレーニングや技術支援を提供するというもので、2021 年までに 300 万ドルの投資を行う。具体的には、サイバー攻撃の即応機関への技術支援、官民の協力体制を強化するための分野横断的なトレーニング、地域間での情報共有の支援となっている。法案を提出した Joaquin Castro 下院議員（民主党、テキサス州選出）は、サイバーセキュリティは中央省庁や大企業だけでなく、地方レベルでも影響があると述べている[89]。

6 終わりに

電力インフラは、我々の生活になくてはならない重要インフラであり、近年急速に IT 化が進むことで、新しい機能も生み出してきている。今回紹介したような、IoT や人工知能の活用により、利便性は益々高まると共に、エネルギーの効率化や省エネへの対応も向上している。電力インフラの重要性は今後も変わらないであろうが、IT 化が進展することによってサイバー攻撃の脅威も高まっている。電力の異常は、生活やビジネスへの影響も多大なものになるだけに、より一層のサイバーセキュリティ対策が求められている。米国では、電力分野におけるサイバーセキュリティ対策は国家的な課題と位置づけられ、連邦政府をはじめ産学官それぞれが連携をとりながら様々な対策を進めている。電力の重要性は我が国でも同じであり、米国の取り組は参考になると共に、米国との連携は非常に意義があるのではないだろうか。

[89] http://www.executivegov.com/2016/05/cbo-natl-cybersecurity-preparedness-consortium-bill-would-not-affect-revenue-direct-spending/
https://castro.house.gov/media-center/press-releases/homeland-security-committee-passes-castro-cybersecurity-legislation