特集
Special Feature

［社会インフラシステムにおけるサイバーセキュリティ―レジリエントで持続可能なデジタル経済社会に向けて―］

1 電力分野におけるサイバーセキュリティの現状と今後の展望

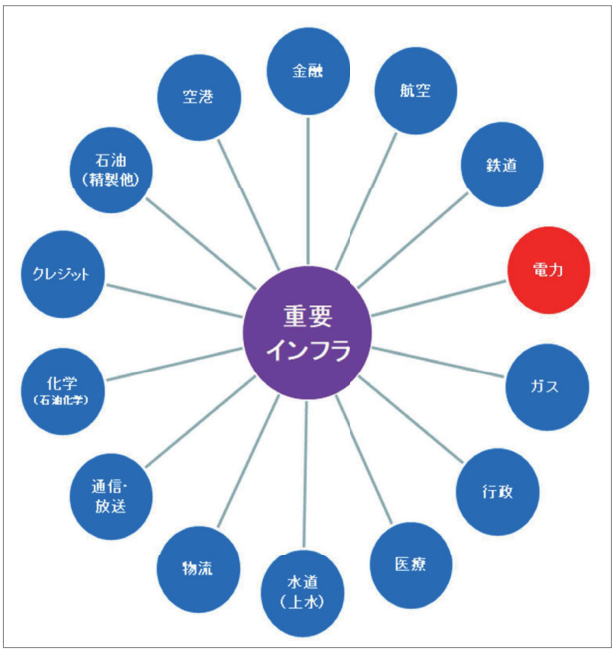
―社会インフラシステムの要（かなめ）としての役割―

応用

渡辺研司　名古屋工業大学大学院社会工学専攻

社会インフラシステムの要（かなめ）としての電力分野

社会インフラシステムを構成する分野のうち特に重要と考えられる重要インフラ分野は，サイバーセキュリティ基本法に規定する重要社会基盤事業者等として定義されており，本稿執筆時点では，情報通信，金融，航空，空港，鉄道，電力，ガス，政府・行政サービス，医療，水道（上水），物流，化学，クレジット，石油の 14 分野が具体的に指定されている（図 -1）．



■図 -1　重要インフラ 14 分野

これらは，国民生活や経済活動の基盤となる社会インフラのうち，機能が停止したり，低下したりすれば特に大きな混乱を招くと見込まれるものであり，各分野でサービスを供給する事業者や組織は，分野を所管する省庁と連携しながらサイバーセキュリティのレベル向上に取り組んでいる．

そして，それぞれの重要インフラ分野は独立して存在しているのではなく，相互に依存し合いながらサービスを提供しており，その重要インフラ間の相互依存関係の要（かなめ）となっているのが電力分野である．その観点を踏まえると，攻撃者の立場からしても，電力分野はサービス停止や機能低下の社会的影響が大きいため，社会混乱を引き起こしたり，身代金を要求するような攻撃の恰好のターゲットになり得ることから，より確実かつ強固なサイバーセキュリティ体制が求められる立場にある．

その電力分野では，電力自由化に伴う産業構造の変化や発電・送配電・制御などにかかわる新たな技術やプラットフォームの導入などに伴い，人材面も含めて，もはや既存の情報セキュリティにかかわる枠組みだけではマネジメントしきれない局面を迎えている．

官民にまたがる電力分野の取り組み

このように，電力分野の経営環境やサイバーセキュリティを取り巻く状況変化を受け，電力分野のサイバーセキュリティにかかわる主な利害関係者となる電気事業者（既存・新規参入），所管省庁（経済産業省・資源エネルギー庁），業界団体（電気事業連合会等），電力 ISAC（Information Sharing and Analysis Center）などではそれぞれの課題認識に基づき，専門家・有識者委員会などからの助言を得ながら，官民連携の構図を基盤としたサイバーセキュリティ体制の強化に取り組んでいる．

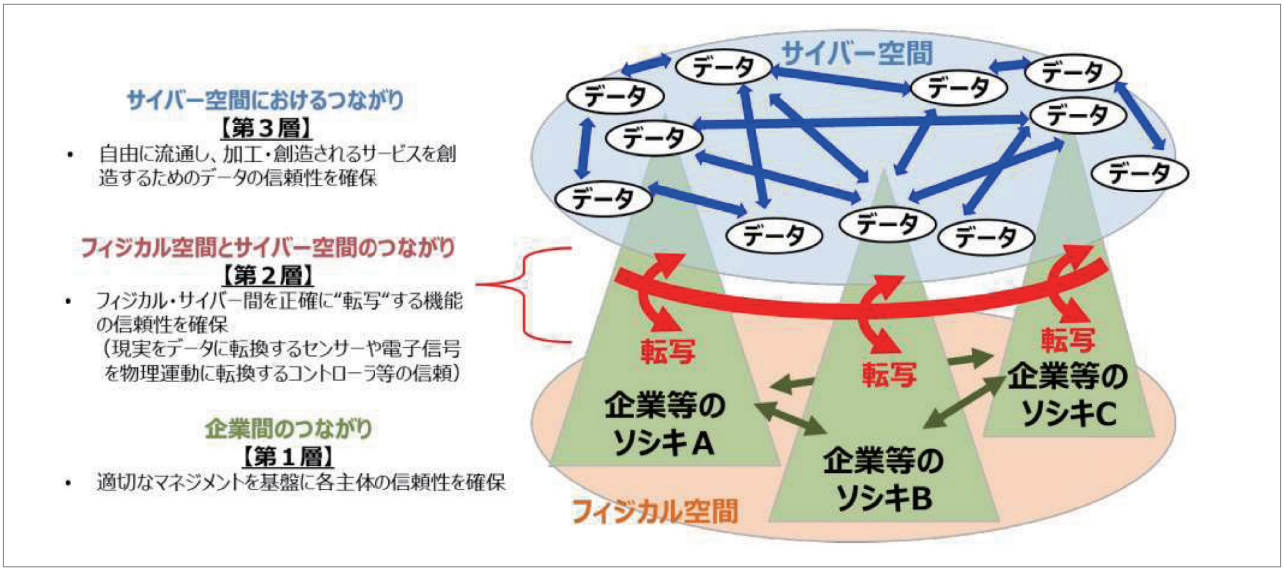
電力事業者自体の取り組みは各社各様であるが，共通して関係する主な利害関係者の取り組み状況の概要は以下の通りである．

経済産業省（産業保安グループ電力安全課・商務情報局サイバーセキュリティ課他）・資源エネルギー庁（電力産業・市場室）：

産業構造審議会に設置された保安・消費生活製品安全分科会の電力安全小委員会にて，電気事業を取り巻く環境変化に対応した今後の電気保安規制，保安人材の育成，監視制御の遠隔化等にかかわる課題認識に基づいた議論が展開されており，現在，電気保安規制の見直しの方向性や電力レジリエンスの議論にサイバーセキュリティの観点を加える形で展開されている[1]．

また，産業サイバーセキュリティ研究会ではサイバーセキュリティ政策の方向性を議論するためのワーキンググループ（WG）群を立ち上げており，そのうちの WG 1（制度・技術・標準化）の下に電力サブワーキンググループ（SWG）が設置され，電力分野のサイバーセキュリティを取り巻く現状，諸外国の状況を分析し，官民が取り組むべき課題と方向性についての議論を重ねている．その過程においては，現在，日本提案で国際規格化が進められているサイバーフィジカルセキュリティフレームワーク（CPSF）の枠組み（図 -2）を意識しながら，大手電気事業者のサイバーセキュリティ対策，新規プレーヤのサイバーセキュリティ対策，そしてサプライチェーンリスクへの対応等に焦点を当てた議論が展開されている[2]．

また，次世代のスマートメーターのセキュリティ対策については，仕様の変更や業界を超えたビジネ



■図 -2　国際標準化を進める CPSF[3]
「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の概要」P.8 より引用
https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

スの将来像を踏まえながら，次世代スマートメーター制度検討会に設置された次世代スマートメーターセキュリティ検討ワーキンググループにて検討が進められている．

電気事業連合会（電事連）：

電気事業者の業界団体である電事連の従来からの中核メンバであった大手電力会社は，電力自由化に伴い新規に参入してきた事業者が，電力ネットワークで相互に接続されるにもかかわらず，必ずしも大手電力会社と同等レベルのサイバーセキュリティ対応の体制が組めるわけではないとの認識から，大手電気事業者としての体制を強化する取り組みと並行して，小規模電気事業者も含めた電力業界全体の対策強化を推進しつつある．

また，関連して日本電気技術規格委員会が電力制御システムセキュリティガイドライン（2019）とスマートメーターシステムセキュリティガイドライン（2019）を日本電気技術規格委員会規格（JESC）として発行しており，主な電気事業者はその適合を目指しながら電力制御システムおよびスマートメーターシステムのセキュリティ強化にかかわる取り組みの効率化を図っている．

電力 ISAC（Information Sharing and Analysis Center）：

2017 年に，電力系統の運用を担う一般送配電事業者と，発電事業等の電力系統に連係する事業者等が連携してサイバーセキュリティへの取り組みを推進するために設立され，会員企業間のサイバーセキュリティに関する情報収集・分析・共有を行うと同時に，内閣サイバーセキュリティセンター（NISC）関連組織として官民で情報共有を行う電力 CEPTOR（Capacity for Engineering of Protection, Technical Operation, Analysis and Response）の事務局も担っている．また，業界内で連携したサイバーセキュリティ事案対応能力の向上を目指し，大手電力 10 社やＪパワー（電源開発），JERA，新電力事業者などが参加するサイバー演習も行っている．直近の演習では，新型コロナウイルス感染が拡大する状況下でも，自然災害とマルウェア感染の２要因で停電が発生するといった複合型の演習シナリオを用いて事案対応能力の確認を行う等の取り組みを実施している．

電力分野における課題と求められる取り組み

ここまでで述べてきたように，電力分野におけるサイバーセキュリティ関連の諸々のリスクが高まっている傾向は，今後さらに加速されると同時に，産業構造の変化や自動化や遠隔制御等に関する多用な新技術の導入が伴うことで，電力分野のサイバーセキュリティの実効性を確保するためには，電力供給サイドの組織単体や業界団体や所管省庁との連携だけでは太刀打ちできない局面が多発すると考えられる．

そのため，官民の組織形態を越えた下記のような事項を実現する必要があると考える．

（1）電力供給サプライチェーン横断的な取り組み：

サイバーセキュリティの最終的な目的は，電力供給サイドの安定供給力を完璧に確保することが不可能であることを考えれば，最終需要者・消費者サイドが必要な電力を必要なときに確保できる状態にすることと考えられる．このような観点からすると，従来の電力分野だけではなく，燃料調達，発電，送配電，卸売・小売り，蓄電・消費といった電力供給のサプライチェーンを構成する各組織やプロセス個々のレジリエンス（しなやかな回復力）をサイバーとフィジカルの両面で強化する必要がある．

（2）需要・消費サイドの自助体制の強化：

上記に関連して電力需要と供給の２つの側面に着目すれば，電力の供給サイドの努力だけではなく，効率的・効果的なリスクコミュニケーションを介し

て，需要・消費サイドにも働きかけることが肝要である．具体的には，供給サイドに何らかの不具合が発生した場合でも，需要・消費サイドの組織が自らの社会的使命として，継続もしくは早期復旧しなければならない業務やサービスを，代替手段の適用や復旧優先業務に絞ったオペレーションへのシフトといった，事業継続計画（BCP: Business Continuity Plan）に基づいた自主的な行動により維持する体制がとれるようにすることが必要である．

（3）サイバーセキュリティ事案対応能力の強化：

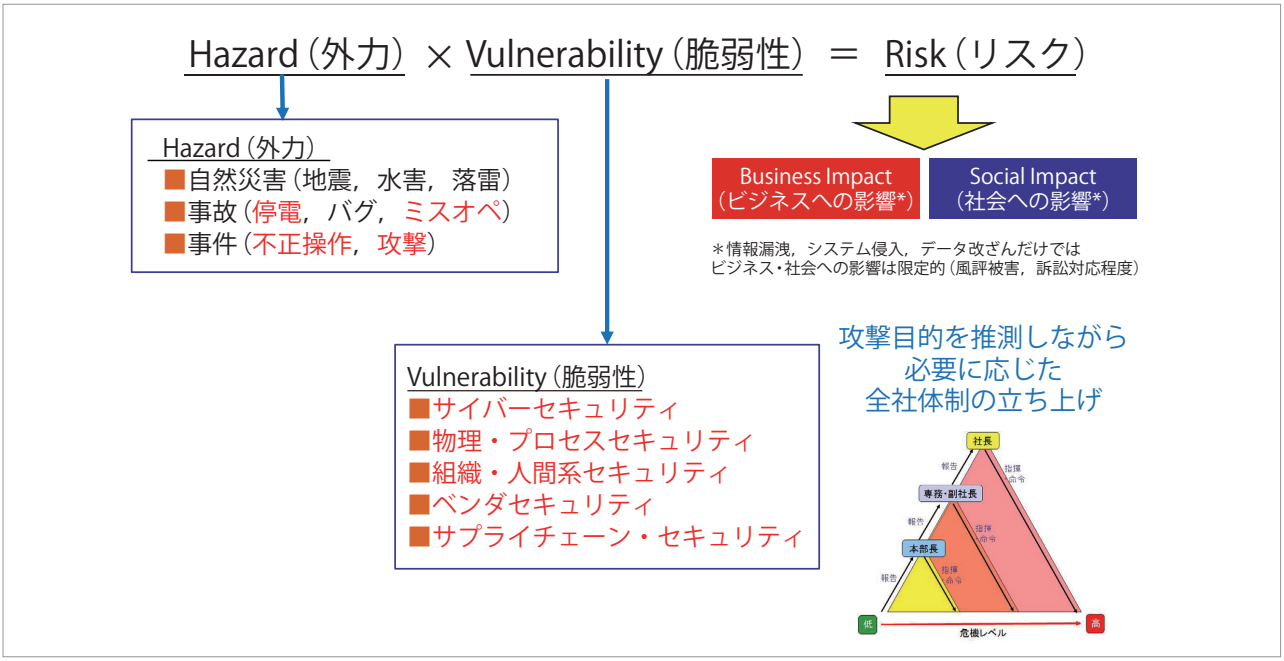
電力事業者は重要インフラ事業者とはいえ民間企業のため株主や金融機関といった利害関係者から常に経済的な合理性を経営上求められていることから，サイバーセキュリティに多大な経営資源を投下し続けることはできない．このような民業の限界については，業界内の共助と官民共助（公助ではなく）などでカバーしながら電力分野全体のサイバーセキュリティ事案対応能力の強化を目指すべきである．

また，電力事業者組織内の体制としても，情報システム関連部門やサイバーセキュリティ部門に任せきりにするのではなく，きっかけはサイバー事案であったとしても，結果として電力供給の停止や低下につながる可能性のあるような事案については，早期にトップマネジメントを巻き込んで，経営判断を加えながら，外部の利害関係者とも適時にコミュニケーションを取るような体制を構築し，その実効性を常日頃からの訓練や演習で担保し続けることが電力事業者には求められる（図 -3）．

状況によっては電力事業者自らが能動的に電力供給を停止するという経営判断も求められるのである．

（4）動的システムセキュリティマネジメント体制の確立：

サイバーセキュリティの対象となる「システム」は，ICT や情報システムだけでは機能しない仕組みであり，人間やプロセスの関与がなくしては最終的なサービスの提供や各種業務の遂行ができない．この「三位一体」のような構造（図 -4）を考えれば，サイバーセキュリティだからといって ICT や情報システムの部分だけの対策や対応をとるだけでは最終的に「システム」を防護することはできない．

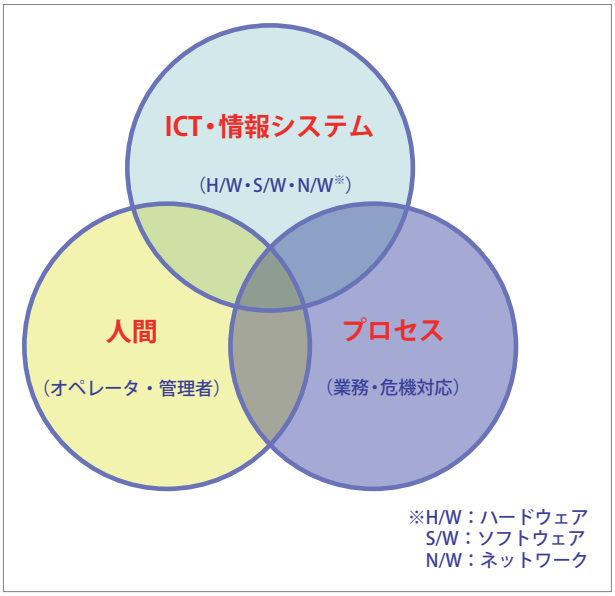


■図 -3　事案のインパクト評価に基づく事案対応体制

また，重要インフラを狙う攻撃者にとってもサイバー攻撃はあくまで攻撃手段の 1 つであり，人間系やプロセス系の脆弱性をつくような攻撃と併せた複合型の攻撃でその目的を効率的に達成しようとするはずである．したがって，防護側もサイバー，フィジカル問わず，三位一体の枠組みでセキュリティ体制の現状を見直すことで，組織の業務や資産を守り，社員・職員も守りながら，電力分野のサイバー・フィジカルレジリエンスを確保することが可能になる．

今後の展望：大都市圏における電力分野を中心とした分野横断的事案対応体制構築の重要性

電力の停止や機能低下の結果は社会経済活動の停止・停滞や社会混乱に直結しやすく，結果事象としての実例はサイバーセキュリティを起因とした事案よりも地震や風水雪害といった自然災害ですでに顕現化している．このことは，サイバーセキュリティ事案も電力分野においては，自然災害同様のフィジカルな被害をもたらすことを示しており，先述の CPSF の概念にもあるように，サイバーとフィジカルな両面を見据えたセキュリティマネジメントの運用が不可欠となる．



■図 -4　動的システム・セキュリティ・マネジメント

特に東京・大阪・名古屋を中心とした大都市圏では，人流・物流・金流・情報流の継続的な集中と流入・流出の動的変化が激しくなっており，新型コロナ禍でも人流が抑制された一方で，物流・情報流が急増した．このような状況の背景には社会経済活動の効率性や合理性を求めて，サプライチェーンやネットワークを介した水平分業と商品・サービスの提供先の地理的な集中が推進されてきたことがある．これは社会経済活動間の人・物・金・情報を介した相互依存性の急増にもつながっており，このような平時の効率性や合理性を確保するための仕組みが，電力分野も含めた重要インフラ分野のサービス障害発生時には皮肉にも多様な連鎖被害を引き起こす脆弱性となっている．

社会経済活動の集中に伴う電力障害感応度の急増

このような大都市圏における社会経済活動間の相互依存性と脆弱性の急増が，停電や低下等の電力関連障害発生の時間帯・曜日・季節・天候・大規模イベント開催の有無などのコンテクスト（context）によっては，事前に想定し得なかったような被害の動的な拡大に繋がるような事例が散見されることが多くなってきた．

特に大都市圏への通勤・通学による日中の人の流入・流出の激しさは，たとえば，東京都心部の昼夜間人口の差がきわめて高いことにも見てとれ，電力障害に起因して重要インフラ間の依存性を介した都市機能の同時多発的機能不全は，社会混乱や n 次災害（2 次災害以降の連鎖）を伴う危険な状況に陥る可能性が高くなっていることを示している．

このような状況を踏まえると，大都市圏の電力障害に対する感応度は急増しており，その結果として大都市圏におけるサイバーリスクとその社会経済活

動への影響の増加も加速していると言える．

また，電気・ガス・水道・通信といったライフライン系の重要インフラ分野の機能障害に連鎖して発生する運輸・金融・物流・行政・医療・放送等の重要インフラで発生した障害は，都市機能の途絶やサービス・レベルの低下に直結し，大都市圏のすべての社会経済活動に多大な影響を及ぼす．

そして，重要インフラへの被害の同時多発的な発生と，重要インフラ間の相互依存性を介した複合的な連鎖は都市機能を麻痺させ，その時点に大都市圏内に滞留する人々を危険にさらし，地域全体を混乱に陥れる結果にもなり得る．これも先述の通り，攻撃者にとって重要インフラを狙うインセンティブにもなっている．

急がれる大都市圏ごとの地域内重要インフラ事業者連携と相互運用性の確立

重要インフラにかかわる国全体としてのサイバーセキュリティについては重要インフラ専門調査会で議論され，また，毎年，数千人規模の参加者が行う官民連携による重要インフラ分野横断的演習でその実効性の検証が継続されている．しかしながら，重要インフラで発生するサイバー事案はフィジカルな結果として発生する可能性が高いため，特定地域内，特に大都市圏においては，その地で実際に事業を展開する重要インフラ事業者間の連携と相互運用性を確保する必要がある．

このような取り組みを実際に行っている中部地域の CCSC（中部サイバーセキュリティコミュニティ）が地元電力会社を事務局として，ガス・通信・鉄道・空港・金融・高速道路といった重要インフラ事業者に県警察と有識者・専門家が加わり，地域に特化した体制での情報共有や演習の実施を推進している．

今後は重要インフラの 1 つの分野としての電力分野単位でのサイバーセキュリティの取り組みにとどまらず，電力サプライチェーンや地域内分野横断的な枠組み等も加えることで，より実効性の高い運用体制の構築を推し進める必要がある．その際重要なのは，電力分野関係者が社会全体のサイバーセキュリティを取り巻く状況を俯瞰しながら，電力分野としての取り組みが「木を見て森を見ず」といったような断片的な個別最適にとどまらないよう絶えず意識しながら進めることである．

参考文献

1）産業構造審議会　保安・消費生活用製品安全分科会　電力安全小委員会，https://www.meti.go.jp/shingikai/sankoshin/hoan_shohi/denryoku_anzen/index.html（2022.2.7 現在）
2）産業サイバーセキュリティ研究会　ワーキンググループ 1（制度・技術・標準化）電力サブワーキンググループ，https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/index.html（2022.2.7 現在）
3）経済産業省商務情報政策局サイバーセキュリティ課，「産業分野におけるサイバーセキュリティ政策」，JIPDEC　ISMS セミナー資料（2020 年 2 月）．

（2022 年 1 月 14 日受付）

■渡辺研司　watanabe.kenji@nitech.ac.jp

名古屋工業大学大学院社会工学専攻・教授．内閣サイバーセキュリティ戦略本部・重要インフラ専門調査会会長他，電力分野のサイバーセキュリティ関連委員会等の座長・委員などを務める．工学博士，MBA（経営学修士）．