平成 25 年度次世代電力システムに関する電力保安調査

報告書

2014 年 2 月

株式会社日本総合研究所

1. 調査の背景と目的

我が国では、送配変電設備を中心に一般電気事業者の役割は大きくかつ重要である。このため、一般電気事業者はサイバーセキュリティを含む電力の保安に十分に配慮し、安定供給を図ってきた。一方、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・制御等されることに伴いこれらの脆弱性等を狙うサイバー攻撃やインターネットに接続されない制御システムへのサイバー攻撃が現実のものになりつつある。サイバー攻撃の手法についても、複雑・巧妙化してきており、セキュリティリスクが上昇している。これらのリスクの重要性にかんがみ、政府として「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会議）がとりまとめられたところ。

また、新たな電力システムの在り方として「電力システム改革専門委員会報告書（平成２５年２月）を踏まえ、政府として「電力システムに関する改革方針」（平成２５年４月）が閣議決定されたところ。

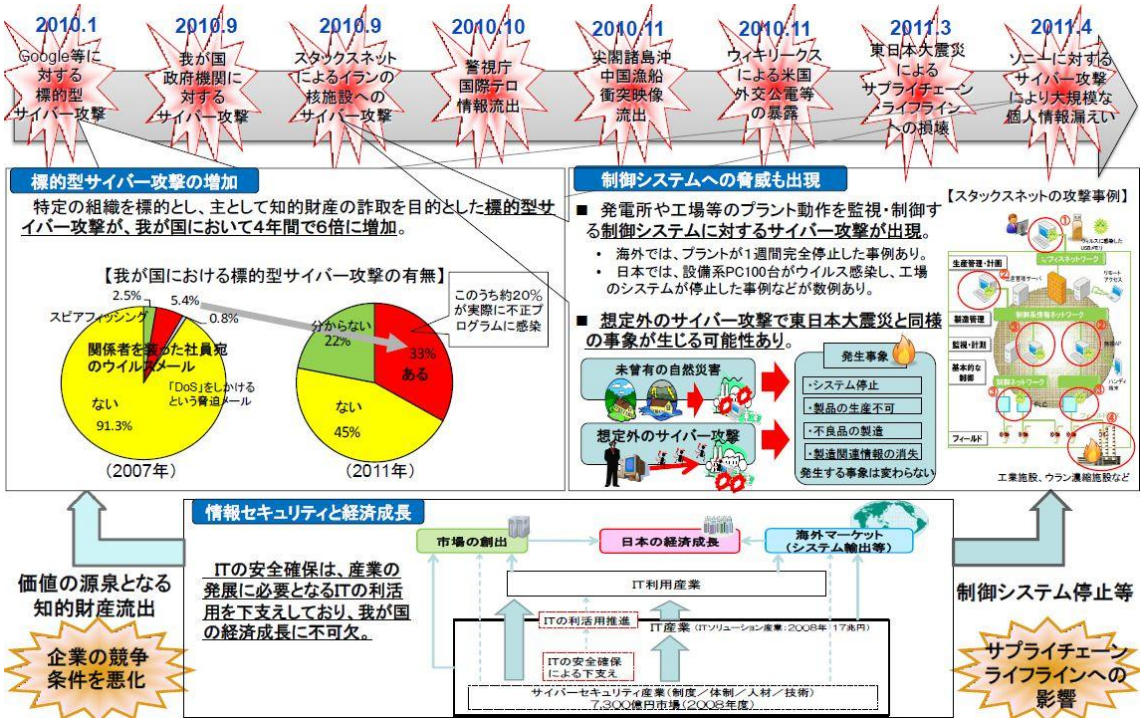
このような事業環境の変化は、これまで一般電気事業者を中心に実施されてきた電力保安対策のあり方にも大きな変革を迫る可能性がある。具体的な事業環境変化要因は次のとおり。

①社会インフラ関連施設に対するサイバー攻撃の増加
②汎用 OS の普及・外部との接続点の増加
③再生可能エネルギー導入拡大
④電力システム改革の進展

①社会インフラ関連施設に対するサイバー攻撃の増加

海外においてはサイバー攻撃の対象として社会インフラ施設が狙われる頻度が上昇しており、米国等においても電力システムや水道システムに対するサイバー攻撃事例が多数、報告されている。我が国の電力システムにおいても、今後このようなサイバー攻撃の対象となる可能性も考えられ、複雑化・巧妙化するサイバー攻撃を想定してセキュリティ水準を高める取り組みが必要となる。

図表 1.1-1　複雑化・巧妙化するサイバー攻撃



（出所）経済産業省「サイバーセキュリティと経済研究会 中間とりまとめ」（2011 年 8 月）

②汎用 OS の普及・外部との接続点の増加

従来ではインターネットに接続されない制御システムは外部ネットワークからのサイバー攻撃に対して安全であると考えられてきたが、制御システム内で汎用ＯＳの活用が図られてきた結果、可搬記録媒体等を通じて制御システム内に侵入し内部からサイバー攻撃を行う事例も生じ始めており、既に海外においてはウラン濃縮施設でのサイバーインシデント（平成２２年１１月）が報告されている。

また、制御システム以外のシステムにおいても、インターネットや汎用ＯＳの活用が進んできた。今後は、スマートメーター・スマートグリッドの導入等により、これらと外部との接点が増加すると考えられる。

③再生可能エネルギー導入拡大

我が国では、再生可能エネルギーの導入拡大として平成２４年９月１４日のエネルギー・環境会議において「革新的エネルギー・環境会議」を決定。再生可能エネルギー導入目標は、2030 年までに 3,000 億 kWh とされた。平成２４年７月からは導入をより拡大するべく、再生可能エネルギーの固定買取制度も開始され、今後ますます再生可能エネルギーの導入量は拡大する見通しである。太陽光発電や風力発電などの再生可能エネルギーは、日照や風況により時々

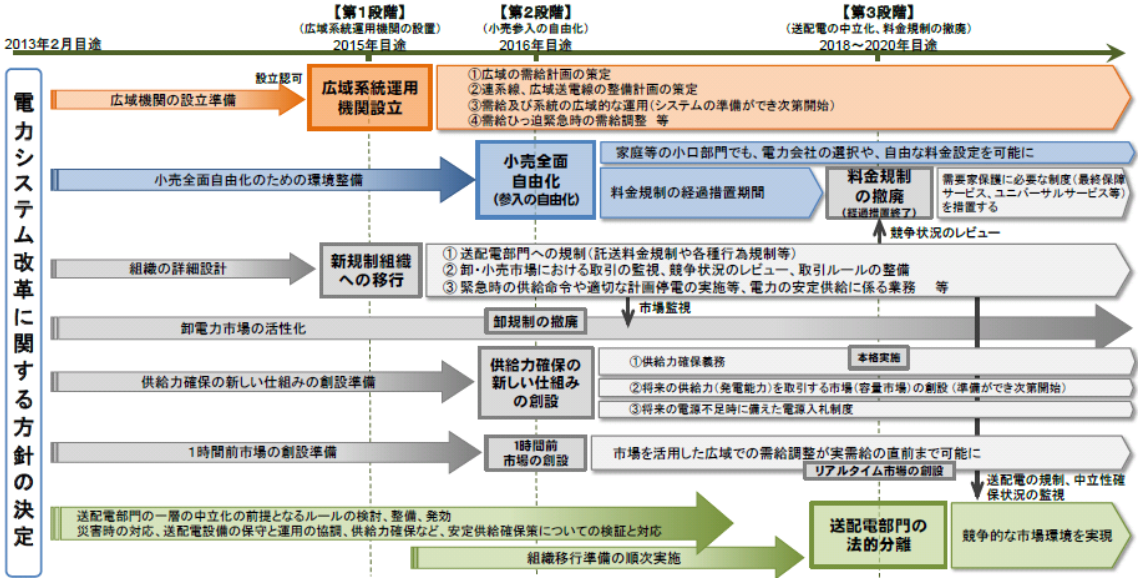
刻々と変化する電源であるため、これらの系統への連系が進むと、需給調整が困難になり、安定的な電力供給に影響を及ぼす可能性もあるため、再生可能エネルギー等の出力等の情報が、発電事業者・送配電事業者等の異なる事業者間で適切に共有されることが重要になる。

④電力システム改革の進展

現在議論されている将来の電力システムにおいては、小売参入の全面自由化、法的分離による送配電部門の一層の中立化、取引所の利用拡大などが予定されており、発電や小売の分野における競争の促進や新たな事業者の参入等により、安定な電力供給を実現しつつ、電気料金の最大限の抑制を実現することが期待されている。

これまでの電力システムにおいては、電力の融通や発電所の運転制御、系統保護等の運用は同一の電気事業者内、あるいは少数の電気事業者間に閉じて行われてきたが、今後は様々な新規参入を含む多様な事業者間が円滑に協働して、これを実現することも考えられる。

図表 1.1-2　電力システム改革の工程表



（出所）経済産業省「電力システム改革専門委員会報告書」（2013 年 2 月）

実効性のあるサイバーセキュリティ対策を検討するためには、これら事業環境の変化を踏まえつつ、電力分野としての特殊性・個別性を考慮した詳細な検討が必要である。

かかる認識の下、本調査は、現在及び今後の情報セキュリティ対策や電力システムへのサイバー攻撃のリスクに対する対応策等の調査を行うことで、電気設備の事故等の未然防止等に資するとともに、必要な保安水準の確保策を検討することとした。

2. 諸外国におけるサイバーセキュリティ対策からの示唆

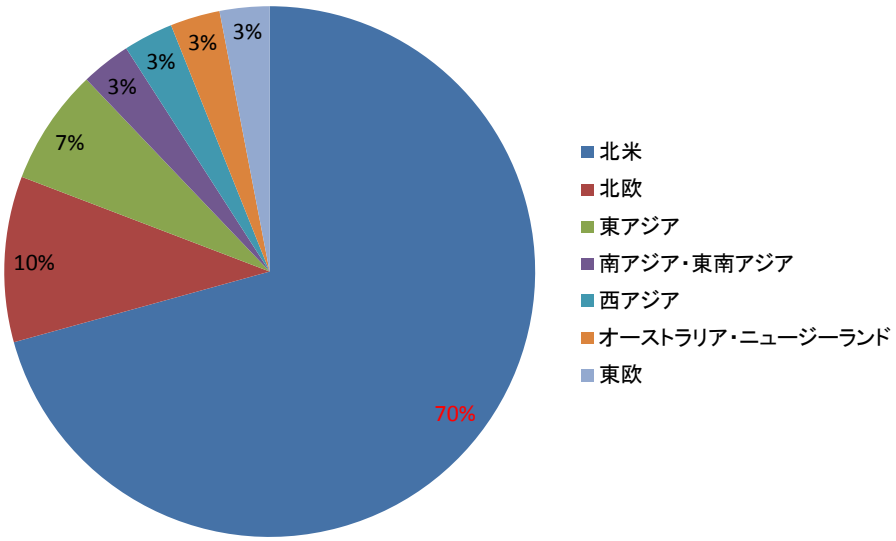
2.1. 海外の電力システムにおけるサイバーインシデント発生状況

電力システムにおけるインシデント事例はその性格上、公表されにくい側面があるが、現実には少なからず発生している。非営利法人の Security Incidents Organization に運営される RISI（The Repository of Industrial Security Incidents）は、電力システムをはじめとする各産業分野別に、オペレーションシステムに影響を及ぼしたサイバーセキュリティインシデントのデータベースを構築している。

データベースの項目として、感染した装置、侵入口、インシデント種別、インパクトなどインシデントにつながる要因を特定し、将来のインシデント発生を防ぐなど、過去のデータから得られる教訓を共有することが可能。また、セキュリティの継続的な改善に向け業界へベンチマークとなるデータ、セキュリティ管理者がセキュリティ対策費用を確保する際に参考となる事業分野ごとの統計を提供することにも重点を置いている。

本データベースでは、偶発的なサイバー関連事故や外部からの侵入、DoS（Denial of Service）攻撃、ウイルスやワームの感染などが具体的なインシデントとして報告されており、RISI の集計によると、電力インフラに対するサイバー攻撃被害事例は、米国の施設で起きたものが最も多く、全世界の 70%を占める。次いで欧州、アジアでサイバーインシデントが報告されている。

図表 2.1-1　地域別電力システムサイバーセキュリティインシデント割合

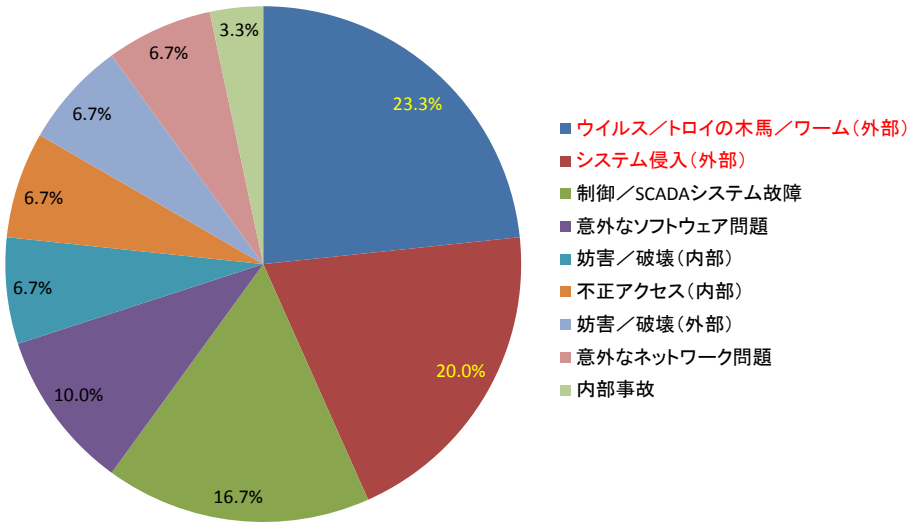


（出所）：RISI（Repository for Industrial Security Incident）の資料（2010 年 9 月）を基に日本総研作成

これまでに被害の詳細が報告されている 30 例を分析すると、外部からのウイルス／トロイの木馬／ワーム、システム侵入及び妨害／破壊によって引き起こされた例が全体の半分以上を占めている。その被害範囲は、操業／生産停止、労働時間の損失、設備の制御喪失など、電力の安定供給を脅かしかねない被害につながった事例が多い。また、被害から 1 時間以内に復旧できた割合は 46%程度に留まり、報告された半数以上の事例では被害からの復旧に 1 時間以上の時間を要した。

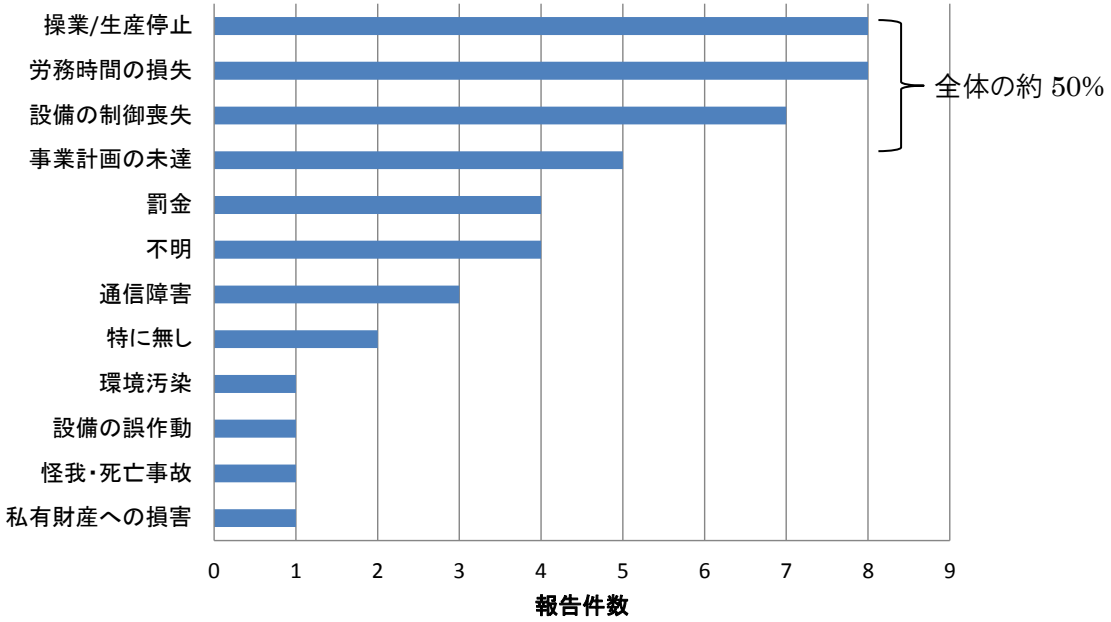
このように、電力システムに対するサイバー攻撃によって被害が生じた場合、電力の安定供給に大きな影響を及ぼす可能性があり、諸外国ではその被害が現実のものとなりつつある。

図表 2.1-2　電力インフラにおけるサイバーインシデントの発生要因（N=30）



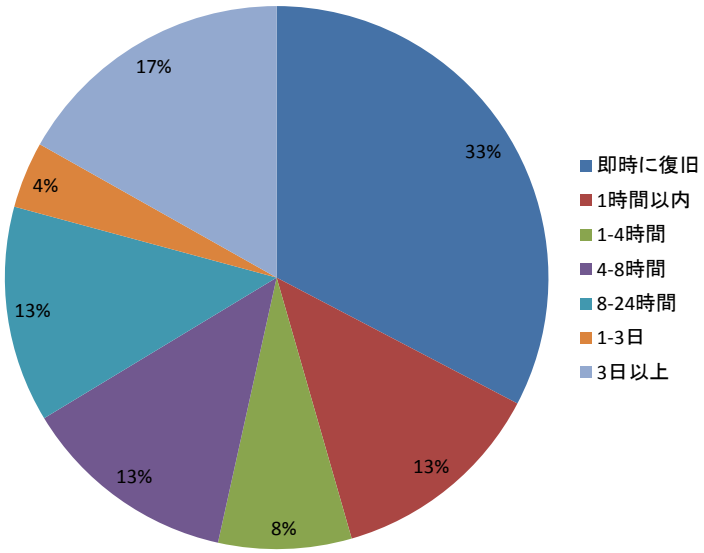
（出所）：RISI（Repository for Industrial Security Incident）の資料（2010 年 9 月）を基に日本総研作成

図表 2.1-3　電力インフラにおけるサイバーインシデントの被害範囲（N=30）



（出所）：RISI（Repository for Industrial Security Incident）の資料
（2010 年 9 月）を基に日本総研作成

図表 2.1-4　サイバーインシデントからの復旧に要した期間（N=30）



（出所）：RISI（Repository for Industrial Security Incident）の資料
（2010 年 9 月）を基に日本総研作成

2.2. 海外の電力システムにおけるサイバーインシデント事例

海外において報告されている具体的なサイバーインシデントの事例は以下のとおり。

図表 2.2-1　諸外国での電力システムに関するインシデント事例

対象	発生国	発生時期	被害内容	原因
ウラン濃縮施設	イラン	2010年	ウラン濃縮施設における約8,400台の遠心分離機がすべて停止	マルウェア（Stuxnet）のコンピューター感染
スマートメーター	米国	2009年	電力消費量記録の改竄	インターネット上で調達可能なソフトウェアによるハッキング
業務システム	米国	2009年	重要データの社外漏洩 / 需給予測システムへの攻撃（未遂）	アクセス権限抹消に要するタイムラグを不正に利用された
SCADAシステム	米国	2007年	SCADAシステムにアクセス可能なPCのアクセス権限が不正に取得された。	フィッシングメール+Windows DNSの脆弱性
系統監視制御システム（アリゾナ州）	米国	2007年	141の分配回路ブレーカーが開き、98,700人の顧客を巻き込む停電が発生	SCADAシステムのベンダがアプリケーションを自動更新し、それを電力施設に伝えなかった。
原子力発電所（ブラウンズ・フェリー）	米国	2006年	発電所の再循環水ポンプが制御不能	発電所統合ネットワーク上の過度の情報量による制御装置の不調
送電システム	米国・カナダ	2003年	米国北東部とカナダでの電源障害	ハッカーがグリッドのセキュリティを侵害するために一日で約100回攻撃
発電所監視システム	米国	2003年	265の発電所で、508ユニット分の発電機が停止（61,800MW相当）	SCADAシステムのアラームプロセッサー障害により、オペレーターが適切に運用できず
原子力発電所（Davis Besse）	米国	2003年	SCADAシステムが5時間、プロセスコンピュータを6時間停止	Slammerとして知られているワームがVPN接続を介して侵入・感染
変電所	米国	不明	変電所の通信障害	Slammerのトラフィックによる通信障害
配電所	欧州	不明	3日間、変電所の半分と通信障害	パッチ不適用のルータにワームが感染

（出所）各種公開資料を基に日本総研作成

2009 年に発生した米 Energy Future Holdings 社のデータ漏洩事例では、解雇した人間のアクセス権限を抹消するまでのタイムラグを利用され、重要データの漏洩に至った。攻撃者は、発電所監視制御システムへ侵入を試みた痕跡が発見されており、重大事故につながる危険もあったが、早期の発見により未然に防止されている。

また 2007 年に報告されているアクセス権限の不正取得事例では、SCADA システムを有する施設に設置された PC に対してフィッシングメールを大量に送信し、Windows DNS の脆弱性を利用してエネルギー会社の社員のアクセス権限を不正に取得した。結果的に被害は生じていないが、SCADA システムにアクセス可能な PC もウイルスに感染しており、SCADA システムに対する不正アクセスに至る可能性もあったとされる。

さらに 2003 年に報告された米 Davis-Besse 原子力発電所の SCADA システム停止事例では、サーバーアプリケーションを開発する外部委託先のシステムエンジニアが、リモートメンテナンス回線で社外のサーバーと通信し、Windows SQL アプリケーションを起動したところ Slammer に感染し、発電所内部まで感染が広がった。

このように被害事例を見ると、クローズドなネットワークという前提が覆され、被害に至った例が多いことが分かる。外部接続ポートや F/W の管理、またアクセス権限を有する要員の管理などには特に注意を払うことが必要である。

さらに近年では、制御システムを狙った Stuxnet の感染が拡大しているとされ、完全にクローズドなネットワーク下にあるシステムでも、可搬記憶媒体等を通じて感染する事例が多く報告されている。このような複雑かつ巧妙化するウイルス・マルウェアの存在を前提としたセキュリティ対策も必要となりつつある。

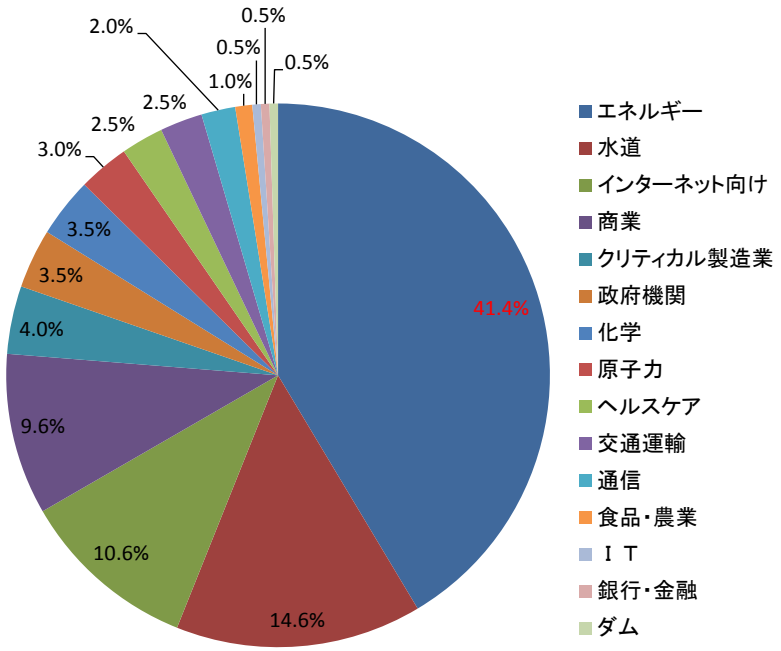
最後に、海外では日本に先行してスマートメーターが普及しているが、例えば米国ではインターネット上で特定メーカーのスマートメーターのソフトウェアを改竄するツールが公開されており、スマートメーター内部に記録される電力消費記録を改竄する事例が報告されている。スマートメーターは電力会社所有の資産であるが、他の電力関連設備と異なり、個人の物理的アクセスが極めて容易であり、悪意のある個人が解析等を行うことで、脆弱性を悪用する事態も生じつつある。

2.3. 米国の重要インフラにおけるサイバー攻撃発生状況

米国では従来よりサイバー攻撃の発生状況が多い地域であったが、近年は重要インフラに対するサイバーセキュリティの比重が高まっている。この原因として、ひとたび安定稼働が脅かされるとその影響が広範囲に及び甚大な被害を引き起こすため、悪意ある攻撃者の格好の攻撃対象となっていること、これまでは独自 OS やクローズドなネットワーク構成で運用されてきた各種のインフラ関連システムにおいて、汎用 OS の普及や外部接続点の増加によってサイバーセキュリティリスクが高まっていること、被害事例が明らかになるにつれこれまで秘匿されてきたシステムの構造が徐々に明らかになりつつあり攻撃が成功する確率が増加していることなどが挙げられる。

特に近年では、重要インフラの中でも電力を含むエネルギーインフラが狙われる事例が多い。米国土安全保障省（DHS）の運営する ICS-CERT（Industrial Control Systems Cyber Emergency Response Team）のデータによると、米国では、2012 年度に重要インフラにおけるサイバーインシデント事例として 198 例が報告されたが、そのうち電力インフラを対象に発生した事例が最も多く、82 件（41.4%）を占める。

図表 2.3-1　セグメント別米国における重要インフラサイバーインシデント
（2012 年度、2011.10.1～2012.9.30、N=198）



（出所）米国 DHS's ICS-CERT の資料を基に日本総研作成

2.4. 米国の電力インフラにおけるサイバーセキュリティ対策

米国ではこのような状況を踏まえ、特に 9.11 の同時多発テロ事件以降、重要インフラにおけるサイバーセキュリティ対策を段階的に強化してきた。

図表 2.4-1　米国の重要インフラに対するサイバーセキュリティ対策の経緯

年月	イベント	概要
1998 年 5 月	大統領令第 63 号：PDD-63	重要インフラ保護とサイバーセキュリティに関する連邦政府のアプローチを規定。エネルギーセクターの主導機関を DOE に指定し、重要インフラをサイバー攻撃に関する情報共有・分析を目的とした情報共有分析センターを設立。
2002 年 11 月	国土安全保障法	9.11 同時多発テロ事件を機に、重要インフラ保護に関する責務全般を国土安全保障省に課す。
2003 年 2 月	サイバーセキュリティ国家戦略（ホワイトハウス）	①重要インフラ及び主要リソースの保護を目的とした全国計画の開発、②情報システムが攻撃を受けた際の危機管理の実施、③情報システム障害時の公共・民間セクターへの技術サポート提供、④州・地方政府及び民間セクターへの警告情報の提供、⑤国土安全確保の技術研究への資金提供を行う機能をホワイトハウス内に設置。
2003 年 12 月	国土安全保障に関する大統領令第 7 号：HSPD-7	DHS（国土安全保障省）に重要インフラ及び主要リソースの特定・優先順位づけ・保護を目的とした活動を統合（PDD-63 は HSPE-7 により廃止）。
2006 年	国家インフラ保護計画：NIPP（DHS）	農業・食料、軍事産業基盤、エネルギー、医療・公衆衛生、国家的記念建造物・象徴物、銀行・金融、水道、化学薬品、商業施設、重要製造業、ダム、救急サービス、原子炉・核物質・核廃棄物、情報技術、コミュニケーション、郵便・運送、交通システム、政府施設を重要インフラに指定。
2006 年	ロードマップ発表（DOE）	「エネルギーセクターにおける制御システムのセキュリティ確保のための 2006 年ロードマップ」を発表。
2007 年 5 月	エネルギーセクター計画：SSP	エネルギー政府調整協議会（DOE・DHS 主導）が電力・石油・天然ガスセクターの調整機関（電力は NERC）と連携し、国家インフラ保護計画への提言として策定。
2009 年 6 月	サイバースペース政策見直し	連邦政府全体のサイバーセキュリティ政策及び企画を担当するサイバーセキュリティ調整官を設置することを決定。

2010 年 9 月	NISTIR 7628 を発表	「スマートグリッド・サイバーセキュリティに関するガイドライン（NISTIR 7628）」を発表。①Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements 、② Privacy and the Smart Grid、③Supportive Analyses and References の三部構成。
2011 年 9 月	ロードマップ改定（DOE）	「エネルギー供給システムにおけるサイバーセキュリティ確保のための 2011 年ロードマップ」を発表。今後 10 年間の戦略的枠組みの概要を示す。
2011 年	ガイドラインの発表（DOE）	DOE は NIST・NERC と連携し、「電力業界におけるサイバーセキュリティリスクの管理ガイドライン」を発表。
2011 年	重要インフラ保護の信頼性基準	NERC が開発し、FERC が発表する形で、「重要インフラ保護の信頼性基準」を策定

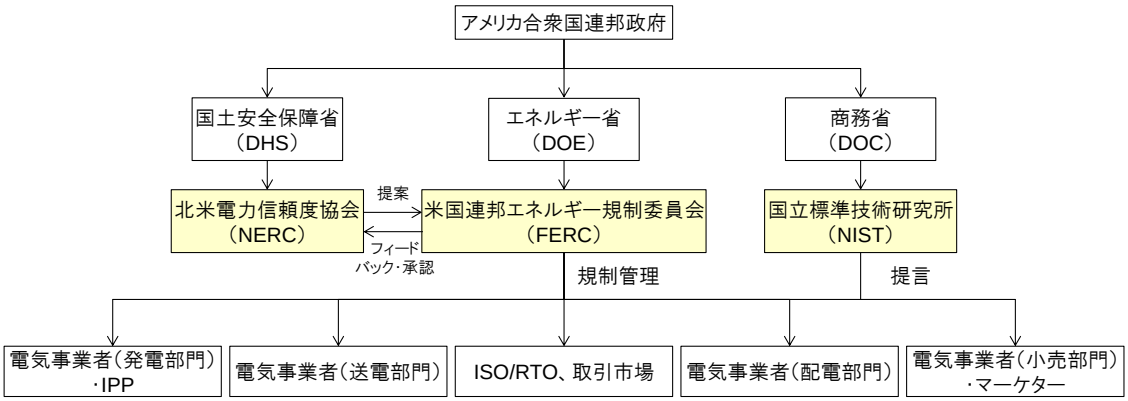
（出所）各種公開資料を基に日本総研作成

このような経緯の中、米国では電力システム（およびエネルギーセクター全般）におけるサイバーセキュリティに対する政府の取り組みは進展し続けており、連邦および州レベルで様々な機関やプログラムへと発展している。

2.4.1.電力セクターのサイバーセキュリティに関する連邦政府機関

米国の電力セクターのサイバーセキュリティへの取り組みに関する主要政府機関には、DHS 傘下の北米電力信頼度協議会（NERC: North American Electric Reliability Council）、エネルギー省傘下の米国連邦エネルギー規制委員会（FERC：Federal Energy Regulatory Commission）、商務省傘下の国立標準技術研究所（NIST: National Institute of Standards and Technology）が主体となり、電力インフラに対するサイバーセキュリティ基準（規格・ガイドライン）策定を推進している。

図表 2.4-2　米国電力サイバーセキュリティ関連組織構造図



（出所）各種公開資料を基に日本総研作成

1）北米電力信頼度協議会
（NERC：North American Electric Reliability Council）

北米全域に影響を及ぼした大規模停電被害を踏まえ、「2005 年エネルギー政策法（EPAct 2005）」により、米国初の電力信頼性機関（ERO：Electric Reliability Organization）の設立が認可された。ERO とは、米国電力システムのユーザー、所有者、プロバイダーすべてに対し、電力の信頼性に関する義務的な規制を課す独立した自主規制機関である（但し規格の発効には FERC の承認が必要となる）。

NERC は 1960 年代より電力業界の任意団体として長く活動を続けてきたが、2007 年 1 月からは FERC に定められていた米国唯一の ERO としても活動している。電力システムに対するサイバーセキュリティ基準を定めた NERC CIP（Critical Infrastructure Protection） サイバーセキュリティ標準は、NERC が ERO として FERC に承認される以前には、NERC 会員のために設けた NERC による自主規制であったが、FERC に ERO として定められた以降は、サイバーセキュリティ対策を含む電力システム全体の信頼性確保に対する公的な基準として機能している。

NERC は重要インフラ保護（CIP）政策を実現する基幹の一つとして、基幹電力系統の物理的およびサイバー上のセキュリティ向上に向けての取り組みを

定める。これらの取り組みには、規格開発、コンプライアンスの啓発、リスクアセスメントおよびリスクに対する準備、警告の発信による業界への重要情報の普及、主要課題に対する認識の向上などが含まれる。

また、NERC は米国政府の重要インフラ保護計画において、電力セクターを代表する機関でもある。NERC の重要インフラ保護委員会（CIPC）の執行委員会は、大統領および NERC の CEO と共に電力セクター調整協議会として機能し、電力セクターの重要インフラとセキュリティに関する問題について、DHS 及び DOE と連携する。

NERC は様々な業界向けのセキュリティガイドラインを開発し、制御システムのセキュリティ、ファイアーウォール、侵入検知、アクセス制御などの問題に対処している。2008 年、NERC の開発した重要インフラ規格（NERC 1300：CIP-002-3～CIP-009-3 のプロトタイプ）が FERC により承認された。これらの規格により、基幹電力系統の運用およびサポートに必要な電子情報を交換する際の安全性を確保し、重要サイバー資産への物理的および電子的な不正アクセスを阻止するための要件が確立された。

これらの規格は、基幹電力系統の特定のユーザー、所有者、プロバイダーに対し、制御システムへの物理的・電子的アクセスの保護、重要サイバー資産の保護、セキュリティ関連業務に従事する人員の訓練、セキュリティ事故の報告、サイバー事故発生時の復旧対策を実施するためのセキュリティ方針、計画、運用手順を確立するよう義務付けている。

2）米国連邦エネルギー規制委員会
（FERC：Federal Energy Regulatory Commission）

電力システムの主要規制機関である米国連邦エネルギー規制委員会（FERC）は、サイバーセキュリティに関する規格開発等を担う ERO を選択・承認する役割を担う。現在、電力システムにおけるサイバーセキュリティ規格としては、2009 年に FERC が採択・承認した NERC CIP サイバーセキュリティ標準が発効されている。

電力システムに対するサイバーセキュリティ規格としては、他にも後述する NIST が定めるガイドラインも存在するが、全米公益事業規制委員協会（NARUC：National Association of Regulatory Utility Commissioners）などの利害関係者間でのコンセンサスが不十分であるとの理由から、FERC の承認は得られていない。ただし現在でも FERC は NIST の継続的なスマートグリッドへの取り組み、特にスマートグリッド相互運用性パネル（SGIP: Smart Grid lnteroperability Panel）の強化について高く評価しており、NIST が策定を進めるスマートグリッドに関するサイバーセキュリティガイドラインは（FERC の承認は得られていないものの）実効性のあるガイドラインとして認知されている。

3）国立標準技術研究所
（NIST：National Institute of Standards and Technology）

「2007 年エネルギー自給・安全保障法（EISA)」によって、国立標準技術研究所（NIST）の主な役割は、スマートグリッドシステムおよびネットワークの相互運用性などの確保を目的とした枠組み・規格開発と定められている。

その活動の一環として NIST は、これらのシステムやネットワークの安全性を確保するためのサイバーセキュリティ規格の策定を行っている。2009 年 3 月、NIST は、各団体（公共事業、機器製造業者、規制機関など）向け開発ガイドラインの作成などを目的とした、スマートグリッドのサイバーセキュリティに関する作業部会 CSCTG (Cyber Security Coordination Task Group）を設立した。2009 年秋からは第 2 フェーズとして、関連業界の代表で構成される NIST SGIP が設置され、CSCTG は 2010 年 1 月に SGIP（675 の公共・民間団体と、1,800 名近くの個人メンバーを有する）傘下の CSWG(Cyber Security Working Group)として活動を継続している。

CSWG の主要な目的の 1 つは、スマートグリッドに必要な情報セキュリティ要件を明らかにし、既存の規格や技術とのギャンプを抽出することにある。CSWG は現在、関連分野の専門家が 400 名以上参画し、オープンな議論とその結果をガイドラインとして文書化する活動を進めている。

そして、2010 年 1 月 19 日、NIST は「フレームワークおよびロードマップ」を発行し、重要な規格のリスト、サイバーセキュリティの一次戦略、および米国スマートグリッドの開発をサポートするその他の枠組みに関する情報を公表した。また、業種を問わず適用出来る IT システム及び制御システムのセキュリティ対策をそれぞれ NIST SP-800-53 Recommended Security Controls for Federal Information Systems（連邦政府情報システムにおける推奨セキュリティ管理策)、NIST SP 800-82 Guide to Industrial Control System Security（産業用制御システムセキュリティのためのガイド）という形式で策定した。さらに将来的にスマートグリッドが確立された際には、エネルギーサービスプロバイダーなど既存電力事業者以外のプレイヤーが電力システムに参加することになるとの見通しから、2010 年 9 月 2 日、NIST がスマートグリッド向けのサイバーセキュリティ対策として「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（NISTIR 7628)」の第 1 版を発行した。

NIST の活動は現在も進行中であり、電力研究所、グリッドワイズ・アーキテクチャ協議会、全米電気機器製造業者協会、米国電気電子学会（IEEE)、NERC などを含む様々な利害関係者と連携して行われている。

また、NIST は 2011 年 9 月 13 日、欧州連合（EU）のスマートグリッド調整グループ（SG-CG、欧州標準化機構（CEN)、欧州電気標準化機構（CENELEC)、欧州電気通信標準化機構（ETSI）の 3 つの民間セクターの標準化機構を代表し

ている）と共同でスマートグリッド標準規格の開発を開始したと発表した。サイバーセキュリティ要件や技術情報を含む、定期的な情報交換の推進を目的としている。

4）エネルギー省（DOE）配電・電力信頼性局（OE）

DOE の配電・電力信頼性局（OE）は、電力網の近代化およびインフラの安全性と信頼性の向上を目指す連邦政府の取り組みで DOE を主導する部門である。NIST、NERC、FERC は主に規格・規制の開発に重点を置いているが、DOE の OE は、サイバーセキュリティに関する各種技術の研究開発とテストに重点を置いている。例えば、OE はサイバーセキュリティを支援する次の活動を行っている：

- 安全で復元力のある電力インフラを構築するための先進技術の研究開発への資金提供
- サイバーセキュリティの向上を目指したリスク管理のベストプラクティスおよび戦略の促進
- DOE のテストプログラムへの支援（DOE のナショナル SCADA テストベッド「NSTB」計画など）
- 電力セクターにおけるサイバーセキュリティ要員の強化・増員

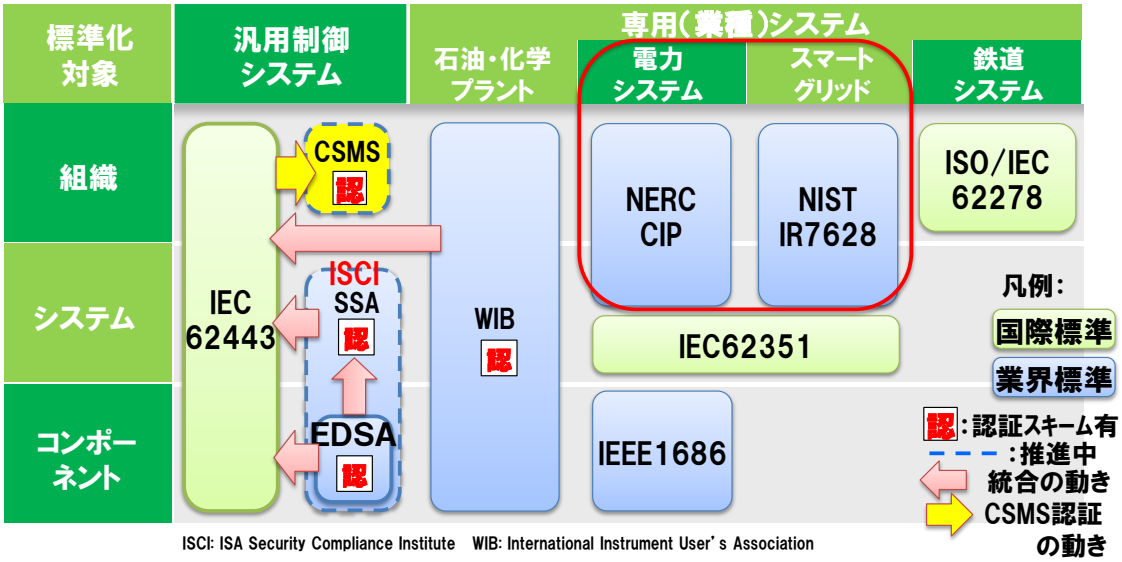
主要な取り組みとしては、大学と共同研究プログラムを立ち上げたり、DOE の OE は米国再生・再投資法（ARRA）に準じ、何十億ドルで米国全土にわたって 100 以上のスマートグリッドへの投資および実証プロジェクト（サイバーリスク評価、軽減策、デバイスやベンダー選定時のサイバーセキュリティ基準などを含む）を支援したり、UCA 国際ユーザーグループ（UCAIug）配下のオープンスマートグリッド（OpenSG）セキュリティ作業部会タスクフォースの基盤づくりに協力したり、INL を通じて NERC 認定の 2 コースを含む、オペレーターおよびその他の利害関係者のセキュリティ関連トレーニングを実施したりしており、サイバーセキュリティ計画の開発と実施の促進に尽力している。また、2010 年、DOE は、EnergySec、電力研究所（EPRI）と共に 1,650 万ドルを投資し、電力セクターのサイバーセキュリティに関する 2 つの機構、NESCO（米国電力セクター・サイバーセキュリティー機構）と NESCOR（米国電力セクター・サイバーセキュリティー機構リソース）を設立した。

2011 年 9 月、DOE は、「エネルギー供給システムにおけるサイバーセキュリティ確保のための 2011 年ロードマップ」を発表した。その中に業界、ベンダー、学界、政府関係者が安全なエネルギー供給システムを開発していくための、今後 10 年間にわたる戦略的枠組みの概要が示されている。同時に、NIST、NERC と連携し、「電力業界におけるサイバーセキュリティリスク管理ガイドライン」の草稿を発表する。同ガイドラインは、米国の電気事業者が全組織レベルでサイバーセキュリティリスクを管理するための方法を提供する。DOE の OE もまた、多数のサイバーセキュリティ関連技術プログラムを実施中である。

2.4.2. 電力セクターのサイバーセキュリティに関する規格・ガイドライン

米国の電力セクターに対するサイバーセキュリティ規格・ガイドラインのうち影響力の高いものは、電力システムを対象として NERC が策定・発行している NERC CIP サイバーセキュリティ標準と、スマートグリッドを対象として NIST が策定している NIST IR7628 が挙げられる。

図表 2.4-3 主要なサイバーセキュリティ規格・ガイドラインの全体像



(出所) CSSC「制御システムセキュリティ認証への取り組み～ISA/IEC62443 の概要と認証について～」(2014 年 1 月) を基に日本総研作成

1) NERC CIP

NERC Cyber-security Critical Infrastructure Protection (CIP) (北米電力信頼性協会：重要インフラ保護基準) は、ERO として NERC が策定し、FERC が承認しているものである。現在は version3 が発効しており、現在 version 5 のドラフトが策定・公開されている。NERC CIP 標準は、北米全域に影響を及ぼした大規模停電被害を踏まえて策定されており、北米の大規模電力システム (主として送電と大規模発電設備) を念頭に検討されたものである。

NERC CIP では、サイバーセキュリティ対策の対象となる重要資産 (及びそれらに関連する重要 IT 資産) の特定について CIP-002 で定義しており、資産所有者が自らの資産を評価し、Critical Assets (重要資産) 及びそれらに関連する重要 IT 資産を特定するよう要求している。資産所有者はこの特定のための方法論及び決定に関する裁量権を持つ。CIP が要求する各種の セキュリティ要件は、全て資産所有者が指定した重要資産を対象として適用されるため、規制対象となる電力会社はセキュリティ管理策が必要な少数の重要資産を特定するようなアプローチを採用することにより、セキュリティ確保に必要な作業およびコストを最小限にしようとしているとする指摘が数多く寄せられている。

図表 2.4-4　NERC CIP version 5 の構成（Draft）

標準	概要
CIP 002-5	リスクベースのアプローチによって重要資産を特定し、これに基づき重要サイバー資産を定める。
CIP 003-5	最小限のセキュリティ管理を確立して重要サイバー資産を保護するためのセキュリティに関する行動計画を策定・実施する。
CIP 004-5	重要サイバー資産へのアクセスを電子的・物理的に許可された人員に対して、必要なトレーニングを施し、セキュリティ意識を身につけさせる。
CIP 005-5	重要サイバー資産を取り囲む電子的なセキュリティ防衛線を特定し、防衛線上の全てのアクセスポイントを特定し保護する。
CIP 006-5	重要サイバー資産を物理的に保護するための行動計画を策定・実施する。
CIP 007-5	自らが定めた重要サイバー資産のセキュリティを確保するための手法、プロセス、手続きを定義する。
CIP 008-5	重要サイバー資産に関連するセキュリティインシデントを特定、分類、対処して報告をする。
CIP 009-5	重要サイバー資産に関する復旧計画を策定し、計画手順を確立し、技法に沿った復旧計画を行う。
CIP 010-5	重要サイバー資産の構成管理プロセスを特定し、不備を特定、分類、対処して報告をする。
CIP 011-5	重要サイバー資産を廃棄や再利用する際の情報取り出しに承認を行い、情報保護を行う。

（出所）NERC CIP verion 5 Draft（2013 年）

現在 FERC と NERC は信頼性規格の適用対象となる「重要インフラ」の適用範囲を明確化するべく議論を行っている。FERC の提案では、1,500MW を超える発電能力を有する単一施設にはサイバーセキュリティ規定が厳格に適用されるべきで、500kV 以上の全ての送電施設および 300kV 以上の特定の送電施設（他施設と多数の相互接続を行うハブとなる送電施設）は全てサイバーセキュリティ対策が必要な重要インフラであると提言している。

現在策定が進められている CIP Ver. 5 は、現行の CIP Ver.3 と比べて 2 個の標準が増え、合わせて合計 10 個のサイバーセキュリティ標準が存在する。また重要資産の特定方法についても、より均一で明確性が増した 17 の基準により特定する方法が規定されており、重要資産を特定する際の自由裁量の余地を制限することで、プロセスの一貫性と明確性を向上させる目的がある。

CIP Ver. 5 では下記のような電力システム（とその担い手）を想定し、8 つのリスク管理の視点と、BES Cyber System への影響尺度（Impact Rating）を提案している。

図表 2.4-5　CIP Ver.5 が想定する電力システムとリスク管理の視点

信頼性調整者	需給調整者	送電事業者	送電設備保有者	配電事業者	発電事業者	発電設備保有者	
	○	○	○	○	○	○	ダイナミックレスポンス
○	○	○	○	○	○	○	需給制御
	○				○	○	周波数変動制御
		○	○	○		○	電圧変動制御
○		○			○		Constraints制御
		○			○		監視
		○			○		復旧
○	○	○			○		警告
○	○	○	○		○	○	事業者間調整

視点1	CIP-004 個人と訓練
視点2	CIP-005 電気的セキュリティ
視点3	CIP-006 物理的セキュリティ
視点4	CIP-007 システムセキュリテイマネジメント
視点5	CIP-008 インシデント報告と対応計画
視点6	CIP-009 復旧計画
視点7	CIP-010 構成変更マネジメントと脆弱性アセス
視点8	CIP-011 情報保護

（出所）NERC CIP version.5 を基に日本総研作成

図表 2.4-6　CIP Ver.5 で定義された BES Cyber System への影響尺度

影響尺度		内容
高	1.1	信頼性調整者(Reliability Coordinator)の制御センター又はバックアップセンター
	1.2	総計3000MW以上を制御している又は2.3/2.6/2.9の資産を保有する需給制御者(Balancing Authority)の制御センター又はバックアップセンター
	1.3	2.2/2.4/2.5/2.7/2.8/2.9/2.10の資産を保有する送電事業者(Transmission Operator)の制御センター又はバックアップセンター
	1.4	2.1/2.3/2.6/2.9の資産を保有する発電事業者(Generator Operator)の制御センター又はバックアップセンター
中	2.1	有効電力容量1500MW以上の発電所
	2.2	無効電力1000MVAR以上の無効電力設備
	2.3	計画調整者(Planning Coordinator)や系統運用者(Transmission Planner)が1年以上の計画期間内に非信頼的影響の回避の必要を指摘した発電施設
	2.4	500kV以上の送電設備
	2.5	200kV以上500kV未満で3つ以上の変電所に接続している送電設備
	2.6	信頼性調整者や計画調整者、系統運用者が相互接続により信頼性を損ねると指摘した発電設備または送電設備
	2.7	核施設接続要件を満たす必要のある送電設備
	2.8	発電端で送電システムに接続する必要のある発電相互接続を提供する送電設備
	2.9	特別防御システム(Special Protection System)や是正・改善命令スキーム(Remedial Action Scheme)、自動開閉システム(Automated Switching System)
	2.10	300MW異常の自動負荷遮断を実現するためのシステムとその要素
	2.11	1500MW以上の発電事業者の制御センター又はバックアップセンター
	2.12	送電事業者の制御センター又はバックアップセンター
	2.13	総計1500MW以上を制御している需給制御事業者の制御センター又はバックアップセンター
低		制御センター、バックアップセンター、送電設備、変電所、復旧に必要なシステムおよび設備、配電事業者の保護システム

具体的な CIP のセキュリティ要件については巻末の付録に記載するが、CIP Ver.5 の特徴として、必要なセキュリティ要件とその確認方法が具体的かつ定量的に記述されていることが挙げられる。具体的なセキュリティ対策が実施されていることの確認方法として、例えば以下の基準が提示されている：

- サイバーセキュリティ・トレーニングプログラム
  - 四半期に 1 回の研修・啓発の開催を示す文書
  - 研修記録
- 接続取り消し
  - 権限剥奪認証の業務フロー又はサインオフフォーム
  - 権限剥奪者のアクセス不能を示すログ又は証拠
- 電気的セキュリティ境界
  - ネットワークにつながっているサイバー資産を特定したすべての ESP リスト
  - 許可された接続（上り／下り）のみを認証する接続ルールが明文化されていることが示されたルールリスト（ファイアーウォール、接続制御リスト）
  - 悪意のある通信を検出する手法（侵入探知システム、アプリケーションレイヤーファイヤーウォール）を記した文書
- 物理的セキュリティ計画
  - 物理的セキュリティ境界と物理的アクセスが 1 つ以上の手法によって管理されているということが記載された物理的セキュリティ計画
- 外部者制御プログラム
  - 来訪者に関する記録を 90 日間保存した文書
- 接続ポートとサービス
  - 適用される全サイバー資産やアクセスポイント上の全ての有効なポートに関する書類
  - ホスト型 FW（ソフトウェアとしての FW）や、特定ポートだけを接続し、他は接続拒否するアプライアンス（ネットワーク型 FW に相当）の環境設定ファイル
  - 物理的入出力ポートの保護の種類を示す書類
    - ✧ システム構成による論理的な保護
    - ✧ ポートロックや警告表示といった物理的な保護）
- セキュリティパッチ管理
  - パッチ設定の記録
    - ✧ パッチ設定日
    - ✧ ソフトウェアのバージョン
    - ✧ ソフトウェア登録日等についての自動パッチ管理ツールの情報
  - いつ、どのように脆弱性に対処したかを示す計画
  - 事業者が実行したセキュリティパッチや緩和を完了するまでの時間等の脆弱性緩和に対する行動記録

- 悪意のあるプログラムからの保護
  - 悪意のあるプログラムを検知・阻止・防止するためのプロセスの実行記録
    - ✧ アンチウィルス、システム強化、方針、等
  - 悪意のあるプログラムを検知するプロセスの反応記録
  - 悪意のあるプログラムを検知した時のこれらのプロセスの実行記録

NERC CIP が要求するこれらのサイバーセキュリティ対策要件は、「Mandatory Reliability Standards for Critical Infrastructure Protection, Order No. 706, 122 FERC 61,040」(2008)の項目 236、344、414、478、(550)、585、654 及び 689 によって、全て FERC に「Mandatory and Enforceable」(義務的かつ強制的) な要件として承認されている。

なお、要件に違反した場合は、FERC により所定の罰金が科せられる内容となっている。罰金額は違反要件を定める VRF (Violation Risk Factor) と実際の違反の程度の定める VSL (Violation Severity Level) に基づいて決定される。

図表 2.4-7　NERC CIP に違反した場合の罰金額

	Violation Severity Level							
Violation Risk Factor	Lower		Moderate		High		Severe	
	Range Limits		Range Limits		Range Limits		Range Limits	
	Low	High	Low	High	Low	High	Low	High
Lower	$1,000	$3,000	$2,000	$7,500	$3,000	$15,000	$5,000	$25,000
Medium	$2,000	$30,000	$4,000	$100,000	$6,000	$200,000	$10,000	$335,000
High	$4,000	$125,000	$8,000	$300,000	$12,000	$625,000	$20,000	$1,000,000

実際の罰金について、単位は「per day per violation」であり、違反の頻度（同じ要件一日違反の回数や違反の要件の数）と違反の期間（連続も、分散も）が罰金額の算定に関わってくる。但しあくまでも FERC が定めた罰金額算定のための基準であり、実際の運用においては、違反事業者の能力、違反時間帯、実際の状況、違反後の態度などにより調整される。具体的に考慮される項目は以下のとおり：

① 繰り返しの違反と違反者のコンプライアンス記録（初犯なら減免が可能）
② コンプライアンス指令の遵守失敗
③ 違反者による自首や自主的な改善措置
④ 違反調査中及び指示された是正・改善活動中違反者の協力態度・程度・質
⑤ 違反者のコンプライアンスプログラムの出席状況とパフォーマンス
⑥ 違反者により違反行為の隠蔽の企て
⑦ 意図的な違反行為
⑧ 酌量できる周囲環境

罰金以外の処罰について、「Remedial Actions」（是正・改善命令）や「Sanctions」（制裁）などの措置も在り得るとされている。要求される「Remedial Actions」の例としては以下が挙げられる：

① 運営・計画の基準や制限の明確化
② 特定のシステムに対する勉強・研究
③ 運営実践やガイドラインの定義
④ 監査テストなどを通じてデータ、実践や過程の確認
⑤ 個人のための特定する訓練
⑥ 明確な運営プランの開発

「Sanctions」の例としては、活動、機能や運営上の制限、主要違反者を記載する「reliability watch list」の作成などが推奨される。

2）NISTIR 7628

NIST のスマートグリッドセキュリティにおける主要取り組みの一つとして 2009 年 9 月には NISTIR 7628 (Guidelines for Smart Grid Cyber Security) Draft Ver. 1.0 が発行され、2010 年 8 月 1 正式版が発行された。NISTIR 7628 の主な目的は、①スマートグリッドの情報セキュリティを扱う団体へのガイダンスの提供と、②スマートグリッドに適合した情報セキュリティ要件の策定に利用された分析プロセスに関する背景情報の提供の 2 つで、Vol.1～Vol.3 の三分冊になっている。

図表 2.4-8　NISTIR 7628 概要

分冊	概要
Vol. 1: Smart Grid Cyber Security Strategy, Architecture and High-level Requirements	スマートグリッドの全体をブロックダイアグラムで表現した論理参照モデルをベースに22種類の論理的インターフェースを定義し、それぞれに対して、19分類（計192項目）のセキュリティ要件の適用の必要性の有無が定義されている。同時にセキュリティの3要素であるCIA（Confidentiality, Integrity, Availability）に関するランク付けと暗号技術と鍵管理の課題についてもこの分冊で触れている。
Vol. 2: Privacy and the Smart Grid	プライバシー問題を取り扱っている。
Vol. 3: Supportive Analyses and Reference	一連の補足的な分析結果や参考情報についてまとめられており、情報セキュリティ研究者にとっても有用な情報が提供されている。具体的には： ① 脆弱性のクラス分類 ② Bottom-up分析 ③ 研究開発テーマ ④ 関連規格のレビューの方針 ⑤ セキュリティ検討のキーとなるユースケース

（出所）NISTIR 7628 を基に日本総研作成

NISTIR 7628 はドラフト段階からスマートグリッドの情報セキュリティのガイドラインとして世界から注目されており、現在これに基づいた標準化活動も始まっている。

図表 2.4-9　NISTIR 7628 Vol.1 「スマートグリッド（SG）サイバーセキュリティ・ストラテジー、アーキテクチャ及びハイレベル要件」概要

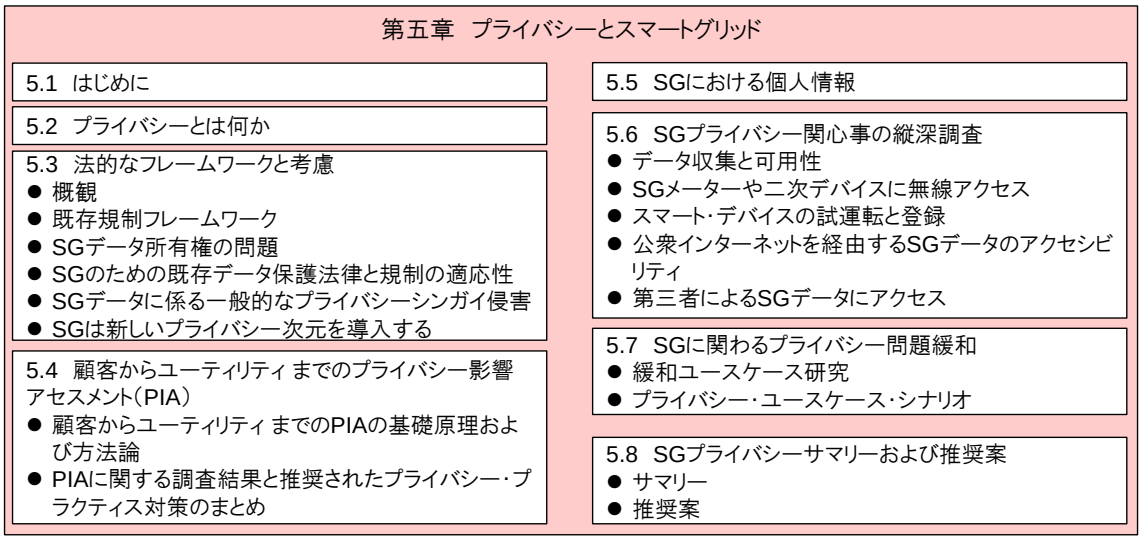
＊ 赤文字の箇所は、NIST SP 800-53に含まれない内容（スマートグリッドを意識した内容）

（出所）NISTIR 7628 を基に日本総研作成

分冊ごとの内容を見てみれば、NISTIR 7628 Vol.1 は、スマートグリッドに接続される機器・システムについて、基本対応方針・問題となるロジカル・アーキテクチャ及びインターフェース、セキュリティ要件の定義を行っている。

NISTIR 7628 で定義されているハイレベル・セキュリティ要件は前身である NIST SP 800-53 に含まれる各要件だけではなく、SG のため特定する管理策も含む。

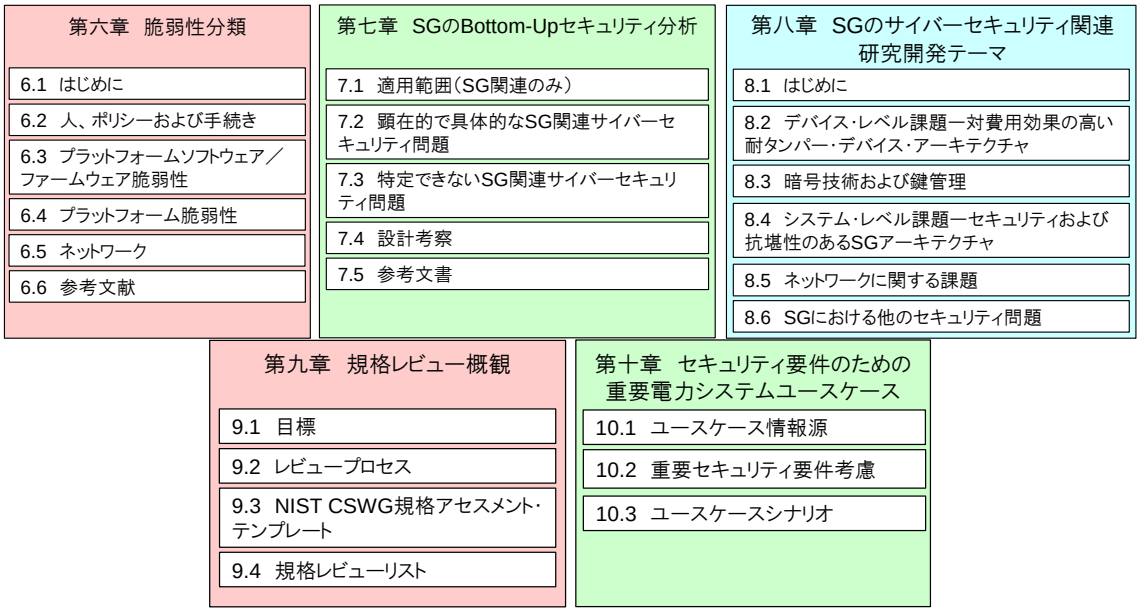
図表 2.4-10　NISTIR 7628 Vol.2 「プライバシーとスマートグリッド」概要



（出所）NISTIR 7628 を基に日本総研作成

NISTIR 7628 Vol.2 はスマートグリッドに接続される一般家庭のプライバシー問題の評価について、論点及び見解を提示している。また NISTIR 7628 Vol.3 では、Vol.1、2 を補完する内容として、スマートグリッドシステムの脆弱性分類、最先端の研究開発のテーマ、また重要電力システムユースケース等を記載している。

図表 2.4-11　NISTIR 7628 Vol.3 「補完的な分析と参考資料」概要

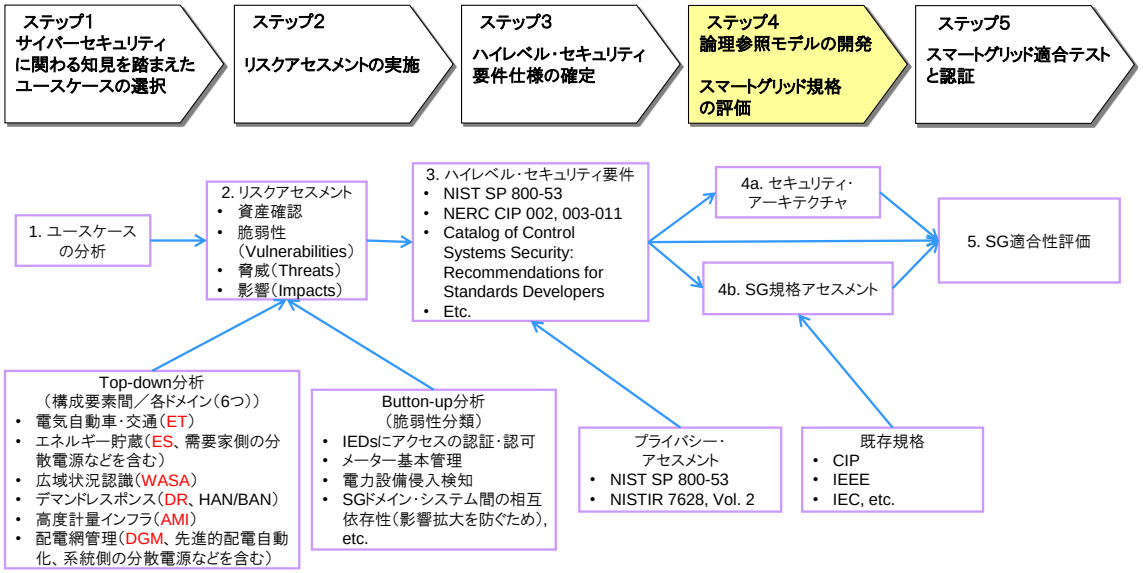


（出所）NISTIR 7628 を基に日本総研作成

NISTIR 7628 は、ユースケースの選択、論理参照モデルの開発、スマートグリッド規格の評価及び、スマートグリッド一致性のテストと認証といった一連のステップを踏んで作成された。また、NIST は各ステップを各作業項目として担当するサブグループを設置し、それぞれの課題を検討している。具体的な分担は以下のとおりである：

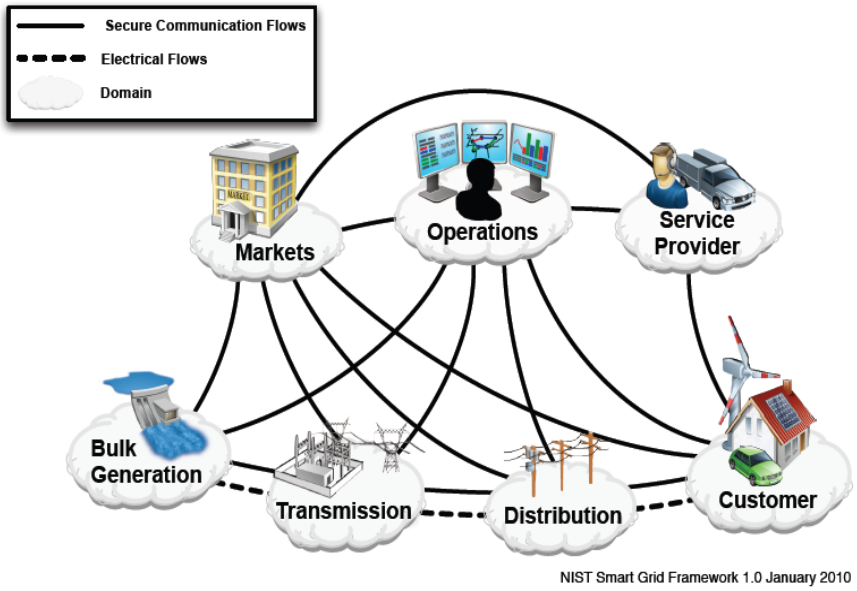
ユースケースの分析：IntelliGrid、EPRI（電力研究所）、Southern California Edison (SCE Corp)
Top-down 分析：FERC4+2 Groups
Button-up 分析 : Bottom-up Group、Crypto & Key Management Group、R&D Group
リスクアセスメント：Vulnerabilities Group
プライバシーアセスメント：Privacy Group
ハイレベル・セキュリティ要件：High Level Requirements Group
セキュリティ・アーキテクチャ：Architecture Group
SG 規格アセスメント：Standards Group

図表 2.4-12　NISTIR 7628 Vol.3 「補完的な分析と参考資料」概要



具体的な分析に入る前に、NISTIR 7628 は先ずスマートグリッド概念モデルを作り、電力事業者が携わっている発電、送電、配電といった 7 つのドメインと、それぞれのドメインの間における安全な通信と電力の流れを想定している。

図表 2.4-13　論理参照モデルの開発－スマートグリッドの概念モデル



（出所）NISTIR 7628

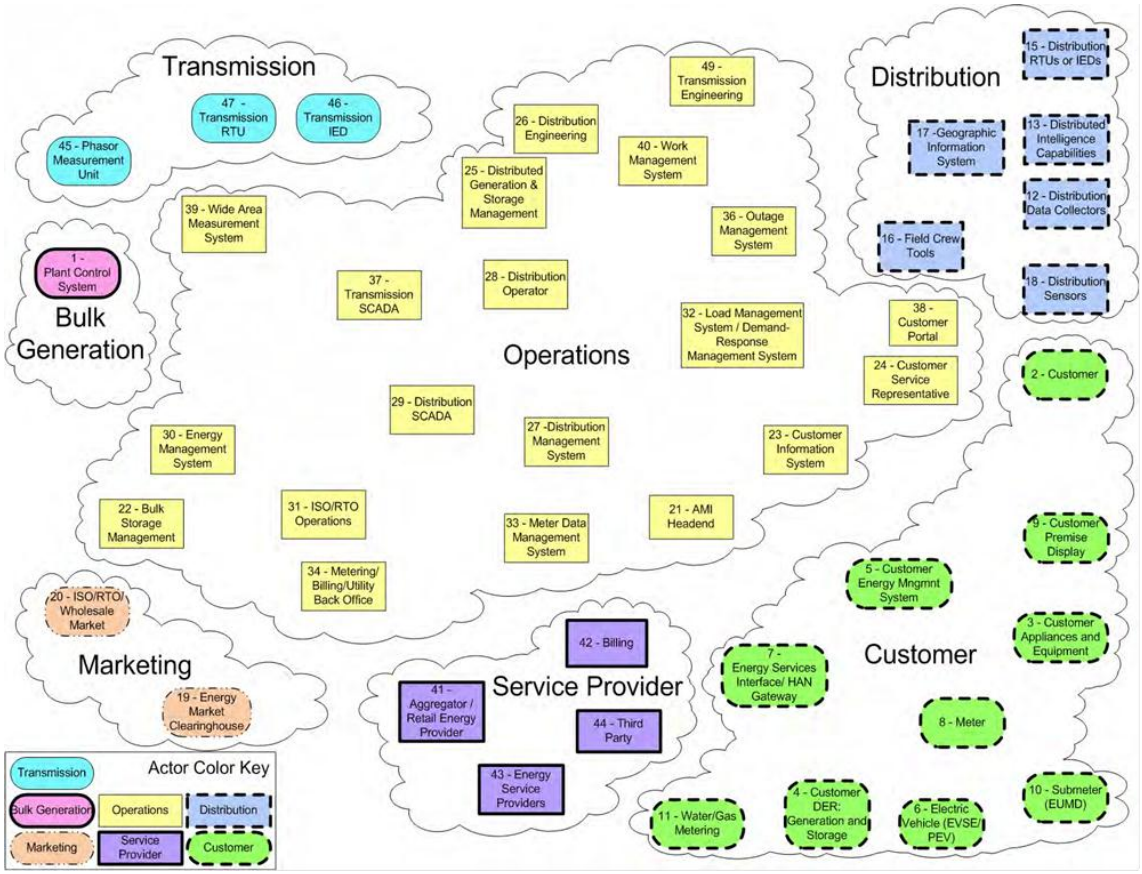
図表 2.4-14　NIST スマートグリッド概念モデルの 7 つのドメイン

日本の電気事業の構造を考慮して整理	
電力事業者	• 発電（Bulk Generation） • 送電（Transmission） • 配電（Distribution） • 運用（Operations）
サービス事業者 （新事業分野）	• 取引所（Markets） • サービス･プロバイダ（Service Provider）
需要家 （家庭）	• 顧客（Customer）

（出所）NISTIR 7628 を基に日本総研作成

スマートグリッドに接続する事業主体として 7 つのドメインを設定し、それらをさらに細分化し、46 のアクター（需要家、需要機器、事業者）を想定している。

図表 2.4-15　論理参照モデルの開発－アクターの定義

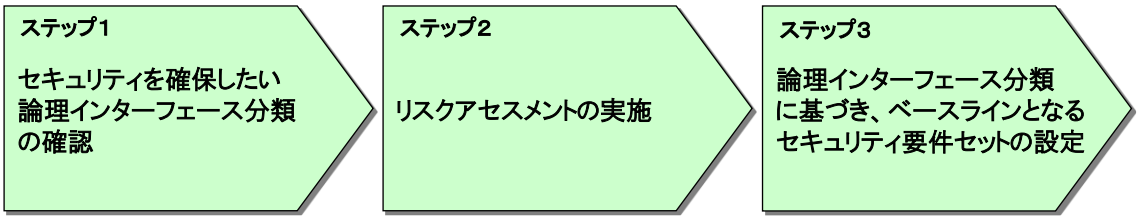


（出所）NISTIR 7628

そして、NIST では、46 のアクターの間で、スマートグリッドシステム（ドメイン）内及び相互間のデータ交換等に用いられるインターフェースを 137 種に整理し、これらのインターフェースを 22 カテゴリにセキュリティ上の特徴で分類し、各インターフェース間の通信に関するリスク評価を行っている（詳細は巻末の付録を参照）。

NISTIR 7628 によるスマートグリッドの保安方法は、論理インターフェース分類の確認、リスクアセスメントの実施及びベースラインセキュリティ要件の設定の３つのステップで実現される。

図表 2.4-16　NISTIR 7628 によるスマートグリッド保安の方法



（出所）NISTIR 7628 を基に日本総研作成

また、NISTIR 7628 のスマートグリッドセキュリティにかかわる機密性、完全性、可用性（CIA: Confidentiality, Integrity, Availability）を定義し、特徴定めている。各 CIA は、低（Limited）、中（Serious）および高（Severe/Catastrophic）の 3 つの潜在的な影響レベルに分けている。

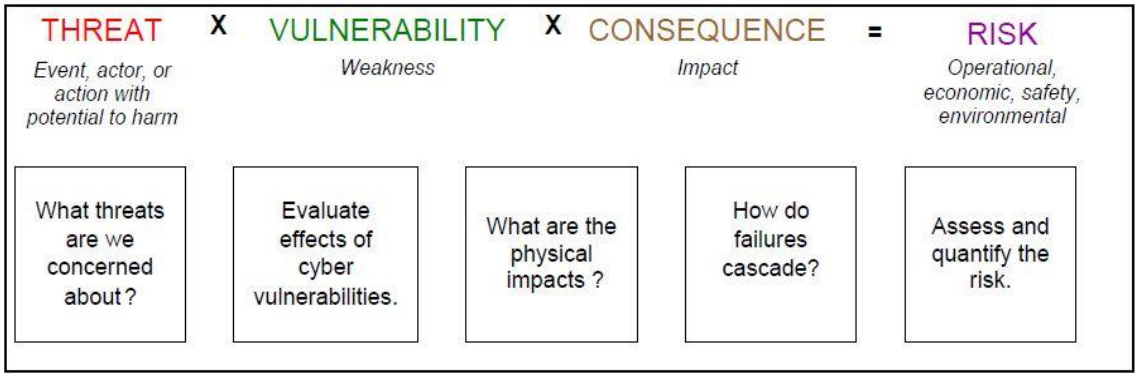
図表 2.4-17　NISTIR 7628 による CIA の定義・特徴

セキュリティ目標	定義	特徴
機密性 （Confidentiality）	個人プライバシーと専有情報の保護方法を含む承認される情報アクセス／公開を制限する。	● 機密性の重要度は前に三つのセキュリティ目標の中に最も低いが、近年顧客情報がオンラインでも利用できるようになるため重要性はますます高まっている。 ● 例としては： ➢ 顧客情報保護 ➢ 電力市場情報保護 ➢ 会社総合情報保護（e.g.従業員名簿、内部戦略計画など） ● 機密性の損失は不正な情報漏えい
完全性 （Integrity）	不正情報改ざん・破壊を防ぎ、否認防止と情報真正性を確保する。	● 完全性の例としては ➢ 無許可のデータ修正ができない ➢ データ源は認証される ➢ データに伴うタイムスタンプは認識・認証される ➢ データ品質は認識・認証される ● 完全性の損失は許可のない修正や情報の破壊である
可用性 （Availability）	タイムリー・信頼できる情報アクセス及び情報利用を確保する。	● 電力システムの信頼性にとって一番重要なセキュリティ目標。 ● 可用性に関わる待ち時間はシステム／デバイスによって違う： ➢ 保護継電のためには4ミリ秒以下 ➢ 送電広域状況認識・監視のためには秒以下 ➢ 変電所とフィーダー遠隔SCADAデータのために数秒以下 ➢ ノンクリティカル装置とマーケット価格情報監視のために数分以下 ➢ メーター検針及び長期マーケット価格情報のために数時間以下 ➢ 電力品質情報等の長期データのために数日／数週間／数月間以下 ● 可用性の損失は情報／情報システムにアクセス／利用における妨害である

（出所）NISTIR 7628 を基に日本総研作成

ステップ 2 のリスクアセスメントを実施するとき、NISTIR 7628 のリスク共通モデルを使い、リスクを脅威、脆弱性及びインパクトの３つに分けて分析すると推奨される。また、スマートグリッドに抱える脆弱性に対応可能なセキュリティ要件カテゴリは付録 5(3)を参考。各セキュリティ要件が対応できるインターフェースは付録 5(4)に説明する。

図表 2.4-18　NISTIR 7628 で用いられるリスク評価モデル



（出所）NIST IR 7628 を基に日本総研作成

2.5 欧州の電力インフラにおけるサイバーセキュリティ対策

2.5.1 欧州の電力インフラにおけるサイバーセキュリティ対策の考え方

欧州では、スマートグリッドの実現を見据えたサイバーセキュリティ対策について検討が進められている。以下に欧州におけるスマートグリッドのセキュリティ対策の考え方を示す。

- 所有者／権限の異なる個別の電力システムが連携することに留意する

発電・送電・配電が独立した事業者で運営されており、セキュリティポリシーが不統一である。さらに、セキュリティ対策が施されていないレガシー機器が多数存在する。

- 需要家サイドの情報を需給制御にフィードバックする状況を想定する

ホームネットワークなど電力会社の管理が困難な機器との接続が想定され、十分なセキュリティ管理が期待できない。また需要家自身が攻撃者になり得る可能性も否定できない。

- 電力システムがエネルギーサービス事業者と連携する状況を想定する

第三者のエネルギーサービス提供事業者が提供する省エネサービス等とでン力システムが連携することが期待されているが、エネルギーサービス提供事業者のビジネスプロセスが固まっていない状況で、データのアクセス管理が複雑となる可能性がある。

- 商用ネットワーク／無線ネットワークの利用拡大に備える

マルウェア、DDoS 攻撃、不正アクセスなどインターネットで発生する脅威はすべて想定する必要がある。

- 電力システムのリアルタイム性や端末機器のリソース制約を考慮する

電力システムの監視制御はリアルタイム性・信頼性が要求されているため、ベストエフォート処理が許されない場面も多い。さらに電力系統の末端に位置するエネルギー機器では耐熱性やコスト制約から、十分な CPU 性能、メモリサイズを確保できない可能性も考慮する必要がある。

なお、特に重点的に対策が検討されている分野として、事務処理系ネットワークやリモートメンテナンス回線から制御系ネットワークへサイバー攻撃が拡大する可能性である。このような事態を想定し、制御システム内部への侵入は避けられないとの認識に立って、内部での対策の必要性が認識されている。ただし対策コストとの兼ね合いがあるため、どこまでを義務化すべきかについてはさらなる検討が必要とされている。

2.5.2 欧州の電力インフラに対するサイバーセキュリティ対策の経緯

欧州では、他地域と比べてスマートグリッドの導入が先行しており、スマートグリッドの標準策定に関わる様々な組織が存在するが、スマートグリッドにおけるサイバーセキュリティを注目し、そして取り組んでいるのは主にここ５年間のことである。

これまでのところ、欧州委員会（EC：European Commision）がスマートグリッドの標準化に関する様々な指令（Directive）を出しているが、セキュリティに係る指令においては、具体的な施策について提示された例は少なく、大きな方向性が提示されたに留まっている[1]。

欧州委員会は 2011 年 3 月 1 日に M/490「Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment」というマンデート[2]を発表し、セキュリティ問題について、「欧州のエネルギー市場の継続的改善と、安定した発電市場を形成するためには、安全かつ健全なエネルギーネットワークが必須である。それを実現するために関連情報及び通信ネットワークの保安は必要不可欠である。また、データ・システムのセキュリティを維持し、需要家・端末ユーザーの権益及び市民としての基本的権利・自由を尊重することが重要である。」との見解を示した。

これまでのところ、スマートグリッドの電力保安に係る主要な指令として、以下の指令がなされている。

- **Directive 2008/114/EC**「on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection」（欧州重要インフラの識別及び指定とそれらの保護の必要性評価）

  Directive 2008/114/EC では、EU 加盟国に対して、電力システムにおける重要インフラ（ECIs）[3]の識別を要請している。加えて、下記の３項目を加盟国に命じている。

  ① 万が一の際の ECIs の稼動停止によって影響が及びかねない EU 加盟国に対して、各 ECI の存在を知らせること

---

1 その一因は、欧州連合（EU）が巨大かつ複雑な組織で、サイバーセキュリティ対策のような敏感（センシティブ）な問題に対する意思決定が困難なためと指摘されている。

2 Mandate：すべての利害関係者のコンセンサスに基づいて、限られた期間内に開発するという EU 加盟国と欧州標準化団体との合意によって管理される。

3 ECIs：European Critical Infrastructure。定義は「assets or systems essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, located in member states, where disruption or destruction of these assets or systems would have a significant impact on at least two member states」。即ち、本指令では、稼動停止した際に二つ以上の EU 加盟国に影響を与えかねない資産やシステムの識別を要請していることを意味する。該当する ECIs の例としては、発電所や送電インフラなどが含まれる。

② 各 ECI の所有者／運営者に対して、その資産／システムが ECIs に該当することを通知すること
③ 各 ECI のために運営者セキュリティ計画（OSPs：Operator Security Plans）を策定し、セキュリティ SLOs（Security Liaison Officers）を任命すること

- **Directive 2009/72/EC**「concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC」（電力セクターの内部市場に関する共通ルールの指令（Directive 2003/54/EC の廃止を含む））

  Directive 2009/72/EC の 17 章「Assets, equipment, staff and identity」（送電システムの資産、設備、人員）において、「送電システム運営者は IT システムや設備、物理的な施設・建物及びセキュリティ・アクセス・システムを垂直的統合企業（vertically integrated undertaking）の一部と共有してはならない。また、IT システムや設備、セキュリティ・アクセス・システムの構築のために同一のコンサルタントや外部委託先を使うことも禁止する。」という内容の IT システム・資産保安に関わる指令を通知した。

EC のスマートグリッドに関するセキュリティ関連のマンデート（Mandate）の内容は下記のとおりである。

- **EU Mandate M/490**「Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment」

  「持続可能な最先端スマートグリッド情報システム（SGIS：Smart Grid Information Security）、データ保護・プライバシー（DPP : Data Protection and Privacy）に対する技術的及び組織的なニーズに対応すること」及び「送配電ネットワークなどの重要インフラ及び他の関連資産内（ビル、充電スタンドから最終末端まで）を対象とする安全なスマートグリッド情報通信システムを通じて、スマートグリッドサービスの提供を可能にすること」という２つの目標を念頭に制定された指令である。情報セキュリティ及びプライバシーに関する指令は下記のとおりである。

  - ✧ スマートメータ（SM）から安全にデータを収集するためのデータセキュリティメカニズム、暗号化及び干渉防止機能を含む適切な標準と方針
  - ✧ 様々なインターフェース及びシステム全体におけるデータプライバシー及びセキュリティ上のリスクを含むスマートグリッド内のリスク評価のための標準
  - ✧ 調達メカニズム、プロトコル及び技術ソリューションが、その内容に拠らず（agnostic）、同じアウトプットをエンドユーザーに提供できるスマートグリッドサービスのための標準。(サービスの例としてはユーザー認証、デジタル署名や暗号化などを含む)
  - ✧ 最新のセキュリティ技術を活用しており、リソースが制限された端末機器を含むスマートグリッドにおける全ての機器に適用出来る認証のためのメカニズム
  - ✧ セキュリティレベルとロバスト性の確認を行うためのスマートグリッド関連データの取り扱いに関する標準

- **EU Mandate M/441**「Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability」

  本指令の主な目標は、各種のユーティリティーメータ（水道、ガス、電力、熱を含む）の相互運用性の実現するための欧州標準作成の推進である。スマートメーターの導入により、顧客はリアルタイムで自らのエネルギー消費を認識することができ、エネルギー事業者も時々刻々の需要の変化をデータとして取得できる。スマートメーターに係るセキュリティに関する項目としては、「安全（セキュア）なデータ交換」が挙げられている。また、遠隔検針、

メーターシステムと通信を行う組織・機関との間の双方向通信や遠隔開閉機能に関するセキュリティが重要であることも指摘されている。

このほか、正式な指令やマンデートの他に、様々な電力分野セキュリティ関連の「Communication」や推奨（Recommendation）もある。代表的な文書は下記のとおりである。

- **COM(2006) 786**「Communication from the Commission on a European Programme for Critical Infrastructure Protection (EPCIP)」

  本文書では、ICT とエネルギー分野の相互依存の重要性について指摘している。また、2008 年を目途に ICT 分野と電力ネットワーク間の横断的な相互依存を検討課題とする CIP 専門グループを設立するという指示を出した。

- **COM(2009) 149**「Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Rigions on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"」

  本文書では、大規模サイバー攻撃や妨害を受ける際の EU の重要情報インフラ（スマートグリッド以外を含む）を保護するための準備、安全対策及び被害からの回復を重視することを呼びかけ、行動計画を策定するように奨めている。その一環として 2010 年を目途に通信ネットワーク及び情報システムのセキュリティ・復元問題に注力する専門グループの設立について提案している。

- **COM(2010) 245**「Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Rigions - A Digital Agenda for Europe」

  本文書では、EU の重要情報インフラ保安について、今後の検討課題が「Digital Agenda」として説明されている。

- **COM(2011) 163**「Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Rigions on Critical Information Infrastructure Protection - 'Achievements and next steps: towards global cyber-security'」

  本文書では、EU のサイバーセキュリティ（スマートグリッド以外を含む）における成果を紹介するとともに、今後の方向性を説明している。

- **COM(2011) 202**「Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Rigions - Smart Grids: from innovation to deployment」

  本文書では、スマートグリッドの展開・配置及びセキュリティ対策の方向性について言及している。また、そのための技術基準開発、データ保護の確保などに言及している。さらに、スマートグリッドの情報セキュリティ及び回復力の評価や、関連国際の連携をサポートするためのハイ・レベル・ステークホルダーにより構成されるグループの設立について提言している。

- **2012/148/EU**「Commission Recommendation of 9 March 2012, on preparations for the roll-out of smart metering systems」

  本文書中の Article 27 に、「ネットワーク操作員がセキュリティリスクを確認すること、またスマートメーターシステムの十分なセキュリティ・復元力レベルを確保するための適切なセキュリティ対策の整備することについて加盟国が保証すべきである。その目標を達成するために、ネットワーク操作員は、各国の権限のある当局及び市民社会組織（civil society organisations）の協力を得ながら、既存の標準、ガイドライン及びスキームの適用を図ることが重要である。その際、欧州ネットワーク情報セキュリティ庁（ENISA : European Network and Information Security Agency）によって開発された関連ガイドラインを参考すべきである。また適切な既存の参考文献が存在しない場合には、新たに対策を開発するべきである。」と言及されている。

EU のスマートグリッドのサイバーセキュリティ対策では、上位となる EU 指令を踏まえつつ、各 EU 加盟国が独自に有する規制と、各研究・タスクフォースグループの提言・推奨施策を参考としながら、各国のプレイヤー（発電、送電、小売業者等）が各々の役割に応じた対策を実施するという構造になっている。

近年では、スマートメーターとスマートグリッドの急速な普及に伴い、欧州委員会では「適切な標準・規制を策定する前にスマートグリッドが整備されてしまえば、後追いで対策を実施することになり、その対策には多大なコストが発生する恐れがある」と認識しており、様々なタスクフォースと協働し、セキュリティ対策に取り組んでいる。

提言しているタスクフォースは主に以下のようである：

- 欧州委員会が設立した European Smart Grid Task Force Expert Group (EG) 2
  - ✧ データ取扱、データセキュリティ及びデータ保護に対する提言を行

う。

- CEN/CENELEC/ETSI Joint Working Group (JWG)（活動期間：2010.年7月から2011年3月まで。現在はCEN/CENELEC/ETSI Smart Grid Coordination Group (SG-CG)に発展）
  - スマートグリッドにおける共通アーキテクチャ、セキュリティ及びプライバシー問題について検討・提言を行う。
- DG CONNECT's Ad-Hoc EG on Smart Grid Security
  - スマートグリッドのための通信ネットワーク及び情報システムのセキュリティ・復元対策について検討・提言を行う。

その他には、以下の関係組織が、サイバーセキュリティを含むスマートグリッドの標準化を進めている。

- ヨーロッパ：
  - CEN (European Committee for Standardization、欧州標準化委員会)
  - CENELEC (European Committee for Electrotechnical Standardization、欧州電気標準化委員会)
  - ETSI (European Telecommunications Standards Institute、欧州電気通信標準化機構)
  - EC(European Commission、欧州委員会)
- イギリス：
  - UK HMG IA (UK Government's National Technical Authority for Information Assurance)
  - CPNI (Centre for the Protection of the National Infrastructure、英国国家インフラ防護センター)
- フランス：
  - CIGRÉ (Council on Large Electric Systems)
- ドイツ：
  - Germany's BSI (Federal Office for Information Security、ドイツ連邦情報セキュリティ庁)
- オランダ：
  - ✓ Netbeheer Nederland

さらに、各国の取組みの支援、橋渡しを行う組織として、ネットワーク情報セキュリティに関する情報、ベストプラクティスの共有、欧州委員会や各加盟国に提言を行う担当機関として、欧州ネットワーク情報セキュリティ庁（ENISA）が設置されており、電力・スマートグリッドシステムを含む制御システムのサイバーセキュリティも所管している。具体的な活動としては米国を含めた海外の事例についての調査・分析等の実施、それらに基づくサイバーセキュリティ関連の推奨施策の提言を行っている。

国ごとの取組みについては原則的に各国の政府が責任を持ち、独自の方法で重要インフラ制御システムの情報セキュリティ強化に取り組んでいる。例えば、施策推進の中心は、英国、スウェーデンのように重要インフラ防護の所管省庁である場合や、ドイツのように情報セキュリティの所管省庁である場合がある。英国やドイツでは制御システムセキュリティに関する基準・ガイドを政府が直接作成しているが、オランダでは政府から独立した民間の機関に作成を委託している。

また、EU-US Energy Council という組織が組成されており（2009 年 11 月）、EU は米国と緊密に連携し、スマートグリッドのサイバーセキュリティ関連研究・対策を協働している。

3. 我が国のこれまでのサイバーセキュリティに対する取り組み

我が国では、内閣官房情報セキュリティセンター(NISC)や情報処理推進機構(IPA)、JPCERT コーディネーションセンター（JPCERT/CC）といった各機関で様々なサイバーセキュリティ対策の取り組みがなされている。

3.1. 情報セキュリティ基本計画

2005 年 4 月に内閣官房に NISC が設置され、同年 5 月に高度情報通信ネットワーク社会推進戦略本部（IT 戦略本部）に情報セキュリティ政策会議がそれぞれ設置された。情報セキュリティ政策会議では、情報セキュリティ基本計画を 3 次にわたり、包括的な中長期計画として策定している。

第 1 次計画においては、情報通信技術の利活用を通じた経済の持続的発展とより良い国民生活の実現、それにより発生する脅威からの安全保障という国家目標の中に位置づけるとともに、情報セキュリティ問題に対する足元を固める観点から、顕在化した問題への対処療法的な対応から事前対策の取組への転換を推進した。また、政府機関、重要インフラ事業者や企業等の各主体について、縦割り構造の中でそれぞれが独自の対応に終始する状態から、自らの責任を自覚しながら、それぞれの立場に応じた適切な役割分担を果たす枠組みを立上げた。

第 2 次計画では､従来の事前対策の取組を引き続き着実に推進するとともに、万が一の事態においても迅速な対応等を進めることで、事業継続性を確保するという「事故前提社会」における事後対応力の強化が行われた。

これらの取組を継続しつつ、国民を守る情報セキュリティ戦略においては、サイバー空間に係る全ての脅威に対する対応力を世界最高水準に高めることを目標とし、海外における大規模サイバー攻撃事態の発生等の環境変化に対応し、その対処体制の整備や平素からの情報収集・共有体制の構築・強化等の安全保障・危機管理の観点からの取組が進められてきている。

そして 2013 年 6 月 10 日の情報セキュリティ政策会議において、我が国の情報セキュリティ政策に関する新たな国家戦略となるサイバーセキュリティ戦略をとりまとめ、従来の情報セキュリティ確保のための取組はもとより、広くサイバー空間に係る取組を推進する必要性と取組姿勢を明確にした。

本戦略に基づく最初の年次計画である「サイバーセキュリティ 2013」では、これまでとは次元を変えた取り組みとして、重要インフラ事業者の対策として以下のようなものが挙げられている。

重要インフラ事業者における対策（カッコ内は担当）

【新たな「行動計画」の策定】

（ア）新たな「行動計画」の策定（内閣官房及び重要インフラ所管省庁）

【リスク評価手法に基づく対策の重点化】

（イ）「安全基準等」策定方針及び重要インフラ分野における「安全基準等」の継続的改善（内閣官房及び重要インフラ所管省庁）

（ウ）「安全基準等」の整備浸透状況調査（内閣官房及び重要インフラ所管省庁）
（エ）共通脅威分析の実施（内閣官房）
（オ）リスク・コミュニケーションの充実（内閣官房及び重要インフラ所管省庁）

【情報共有体制の深化・拡充】
（カ）「セプターカウンシル」の活動支援（内閣官房）
（キ）共有すべき情報の整理（内閣官房）
（ク）第 2 次行動計画の情報連絡・情報提供に関する実施細目に基づく情報共有の推進（内閣官房）
（ケ）実施細目に基づく情報共有に係るルールの改善等（重要インフラ所管省庁）
（コ）セプターの強化及び訓練（内閣官房及び重要インフラ所管省庁）
（サ）「サイバー情報共有イニシアティブ（J-CSIP）」の強化（経済産業省）
（シ）情報通信分野における事業者との官民連携の推進（総務省）

【重要インフラ障害に対する連携対応能力の強化】
（ス）分野横断的演習の実施（内閣官房及び重要インフラ所管省庁）
（セ）個別分野におけるサイバー演習（総務省及び経済産業省）

【評価・認証の導入等におけるサプライチェーンリスクへの対応強化】
（ソ）サイバー攻撃（インシデント）対応調整支援（経済産業省）
（タ）重要インフラで使用される情報システムのセキュリティ・信頼性向上のための支援体制の整備（経済産業省）
（チ）重要インフラ事業者に対するソフトウェアや制御システム等の脆弱性関連情報の優先提供及び情報セキュリティ関連情報マネジメントの支援等（経済産業省）
（ツ）制御システムに関するインシデントや脆弱性への対応のための連携体制の構築（経済産業省）
（テ）制御システムにおけるセキュリティマネジメントシステム適合性評価スキームの確立支援（経済産業省）
（ト）制御機器等の評価・認証スキームの確立支援（経済産業省）
（ナ）制御システムセキュリティの国際標準に基づく評価・認証機関設立（経済産業省）
（ニ）制御システムセキュリティ評価・認証の国際相互承認（経済産業省）
（ヌ）制御システムセキュリティ評価・認証の利活用に向けた検討（経済産業省）
（ネ）ソフトウェア、情報システムの信頼性向上（経済産業省）

【訓練等による対処態勢の強化】
（ノ）大規模サイバー攻撃事態等発生時の初動対処に係る訓練の実施等（内閣官房及び関係府省庁）

【人材の育成・普及啓発】

（ハ）重要インフラ事業者における人材育成の促進（内閣官房及び重要インフラ所管省庁）
（ヒ）広報公聴活動の充実（内閣官房）

【国際連携の推進】

（フ）重要インフラ分野での国際連携推進（内閣官房、総務省、経済産業省及び重要インフラ所管省庁）

【個別分野における取組の強化】

（ヘ）電気通信システムの安全・信頼性確保（総務省）
（ホ）重要無線通信妨害対策の強化（総務省）

【その他】

（マ）社会的に重要な情報システムについての情報セキュリティ強化（経済産業省）

3.2. サイバーセキュリティリスクに対する認識

サイバーセキュリティリスクを体系的に把握するため、IPA が脆弱性対策情報データベースを 2007 年 4 月 25 日から公開している。

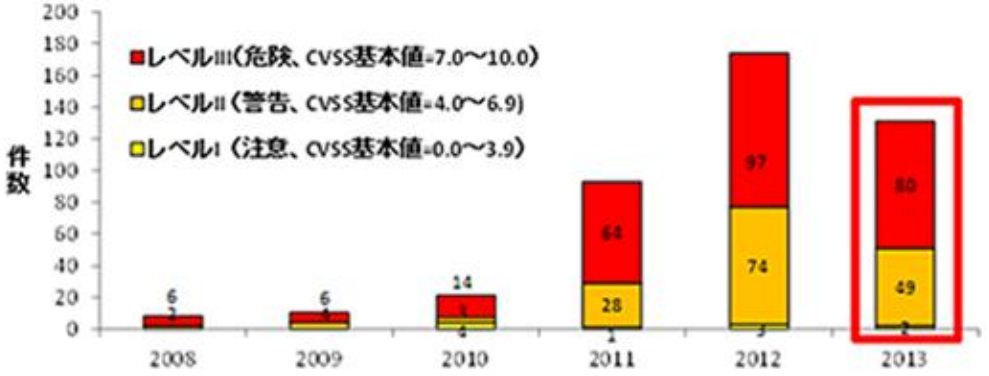
国内のソフトウェア開発者が公開した脆弱性対策情報と、IPA と JPCERT/CC が共同で運営している脆弱性対策情報ポータルサイト JVN（脆弱性対策情報ポータルサイト）で公表した脆弱性対策情報に加えて、米 NIST の脆弱性データベース NVD が公開したソフトウェアの脆弱性対策情報を集約・翻訳して、脆弱性対策データベース（JVN iPedia http://jvndb.jvn.jp/ ）を公開し、現在の登録件数は累計 43, 000 件を超えている。

図表 3.2-1　JVNiPedia の登録件数の四半期別推移

（出所）IPA ホームページ

2008 年度以降には、SCADA に関する脆弱性情報についても JVN　iPedia で公開するようになり、制御システムのサイバーセキュリティリスクについても報告されるようになった。

図表 3.2-2　産業用制御システムのソフトウェアの脆弱性の深刻度別件数



（出所）IPA ホームページ

最近では産業用制御システムに関するソフトウェアの脆弱性対策情報の登録が多くなっている。2013 年は 131 件が登録されており、2013 年末までの登録累計は 437 件になる。131 件の登録のうち 80 件が深刻度の高いレベル III の脆弱性となっており、年々、産業制御システムに関して報告される脆弱性の数、及び深刻度が増している状況と言える。

CVSS とは、脆弱性の基本評価基準の数値を基に I, II, III の 3 段階とした共通脆弱性評価システムで、数値が大きいほど深刻度が高い。

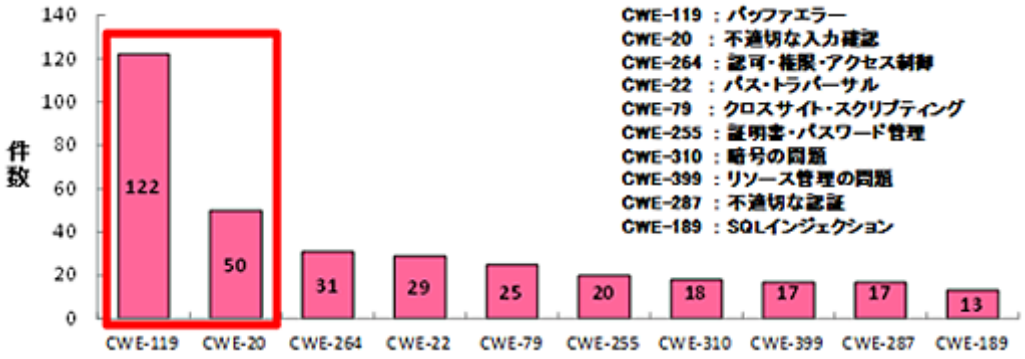
レベル III　リモートからシステムを完全に制御されるような場合や大部分の情報が漏えいするような脅威

レベル II　一部の情報が漏えいするような場合やサービス停止につながるような脅威

レベル I　攻撃する為の条件が複雑な場合やレベル II に該当するが再現性が低い脅威

また産業用制御システムに関するソフトウェアの脆弱性対策情報をタイプ別に分類した件数からは、任意コードの実行などの重大な脅威につながる CWE-119（バッファエラー）の件数が 122 件となっている。

図表 3.2-3　産業制御システムを構成するソフトウェアの脆弱性の種類別件数



（出所）IPA ホームページ

CWE とは、ソフトウェアにおけるセキュリティ上の弱点（脆弱性）の種類を識別するための共通の基準で、SQL インジェクション、クロスサイト・スクリプティング、バッファオーバーフローなど多種多様にわたるソフトウェアの脆弱性を識別するための、脆弱性の種類（脆弱性タイプ）を定義している。

3.3. 重要インフラの行動計画

3.1 で整理した「情報セキュリティ基本計画」に基づき、日本国内でサイバーセキュリティ被害が起こった場合を想定して、NISC では重要インフラとして電気通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流の 10 分野を特定し、情報セキュリティ対策に係る行動計画を作成している。

2005 年　　第一次「重要インフラの情報セキュリティ対策に係る行動計画」
2009 年　　第二次「重要インフラの情報セキュリティ対策に係る行動計画」
2014 年　　第三次「重要インフラの情報セキュリティ対策に係る行動計画」

3.4. 情報共有体制の確立

NISC では官民での情報セキュリティに関する情報を共有するために、情報共有・分析機能であるセプター（CEPTOAR）を上記 10 分野に対して以下の 15 機関を設置している。

1)電気通信分野
- T-CEPTOAR（日本データ通信協会テレコム・アイザック推進会議）
- ケーブルテレビ CEPTOAR（日本ケーブルテレビ連盟）
- 放送 CEPTOAR（日本民間放送連盟）

2)金融分野
- 金融 CEPTOAR 連絡協議会（全国銀行協会）
- 銀行等 CEPTOAR（全国銀行協会事務システム部）
- 証券 CEPTOAR（日本証券業協会ＩＴ管理部）
- 生命保険 CEPTOAR（生命保険協会総務部コンプライアンス統括 G）

損害保険 CEPTOAR（日本損害保険協会業務企画部共同システム開発室）

3)航空分野

航空分野における CEPTOAR（国土交通省航空局安全企画課）

4)鉄道分野

鉄道 CEPTOAR（国土交通省鉄道局危機管理室）

5)電力分野

電力 CEPTOAR（電気事業連合会情報通信部）

6)ガス分野

GAS CEPTOAR（日本ガス協会保安技術グループ）

7)政府・行政サービス分野

自治体 CEPTOAR（地方自治情報センター自治体セキュリティ支援室）

8)医療分野

医療 CEPTOAR（厚生労働省医政局研究開発振興課医療技術情報推進室）

9)水道分野

水道 CEPTOAR（日本水道協会総務部総務課）

10)物流分野

物流 CEPTOAR（日本物流団体連合会）

図表 3.2-4　10 分野 15 機関のセプター一覧

重要インフラ分野	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
事業の範囲	電気通信	放送		銀行等	証券	生命保険	損害保険	航空	鉄道	電力	ガス	地方公共団体	医療	水道	物流
名称	T-CEPTOAR	ケーブルテレビ CEPTOAR	放送 CEPTOAR	金融CEPTOAR連絡協議会 銀行等 CEPTOAR	証券 CEPTOAR	生命保険 CEPTOAR	損害保険 CEPTOAR	航空分野における CEPTOAR	鉄道 CEPTAOR	電力 CEPTOAR	GAS CEPTOAR	自治体 CEPTOAR	医療 CEPTOAR	水道 CEPTOAR	物流 CEPTOAR
事務局	一般財団法人日本データ通信協会 テレコム・アイザック推進会議	一般社団法人日本ケーブルテレビ連盟	一般社団法人日本民間放送連盟	一般社団法人全国銀行協会 事務システム部	日本証券業協会 IT管理部	社団法人生命保険協会 総務部コンプライアンス統括グループ	一般社団法人日本損害保険協会 業務企画部共同システム開発室	国土交通省 航空局 安全企画課	国土交通省 鉄道局 危機管理室	電気事業連合会 情報通信部	一般社団法人日本ガス協会 保安技術グループ	財団法人地方自治情報センター 自治体セキュリティ支援室	厚生労働省 医政局研究開発振興課医療技術情報推進室	社団法人日本水道協会 総務部総務課	一般社団法人日本物流団体連合会
構成員（内訳）	27社・団体 （固定系のネットワークインフラを設置する電気通信事業者、アクセス系の電気通信事業者、ISP事業者、携帯電話事業者等）	246社 （一般社団法人日本ケーブルテレビ連盟の正会員ケーブルテレビ事業者）	194社・団体 （日本放送協会、地上系民間基幹放送事業者、一般社団法人日本民間放送連盟）	1,561社 （銀行、信用金庫、信用組合、労金、商工中金、農協等）	253社 8機関 （証券会社、取引所等証券関係機関）	43社 （社団法人生命保険協会の定款に定める社員および特別会員）	29社（含むオブザーバー3社） （情報システム委員会参加会社）	2グループ 3機関 （航空運送事業者、定期航空協会及び官庁（航空局・気象庁））	22社1団体 1機関 （鉄道事業者22社、1団体及び官庁（鉄道局））	12社2機関 （一般電気事業者、日本原電(株)、電源開発(株)、電気事業連合会、電力中央研究所）	10社 （主要な一般都市ガス事業者10社）	47都道府県 1,742市区町村	1グループ 2機関 （医療機関、日本医師会（情報共有機能）、保健医療福祉情報システム工業会（情報分析機能））	8水道事業体 （会員水道事業体のうち会長都市並びに地方支部長都市） [補足] 障害の内容によって、構成員を通じ、全国の日本水道協会の会員水道事業体(1,350事業体)への情報を提供。	16社6団体 （物流事業者）
緊急窓口	2007年4月より運用開始	2012年12月より運用開始	2007年4月より運用開始										2008年4月より運用開始		
情報の取扱いルール	2007年 1月制定	2012年 11月制定	2007年 3月制定	2007年 3月制定	2007年 3月制定	2007年 3月制定	2007年 3月制定	2007年 3月制定	2007年 3月制定	2006年 9月制定	2007年 3月制定	2007年 3月制定	2008年 3月制定	2008年 3月制定	2008年 3月制定
情報と連絡手段	障害事例情報等 メール、電話、FAX	障害事例情報等 メール、電話	障害事例情報等 メール、電話、FAX、WEB	障害事例情報等 メール、電話、WEB	障害事例情報等 メール、電話、FAX、WEB	障害事例情報等 メール、電話	障害事例情報等 メール、電話	障害事例情報等 メール、電話	障害事例情報等 メール、電話	脆弱性に関する情報等 メール、電話、携帯電話、FAX、電子会議室、TV会議、会議体	障害事例情報等 メール、電話、携帯電話、FAX	障害事例情報等 メール、電話、WEB	障害事例情報等 メール、電話、携帯電話、衛星電話、FAX	障害事例情報等 メール、電話、携帯電話、衛星電話、FAX	障害事例情報等 メール、電話

（出所）NISC「セプターの活動状況の把握について」（2011 年 6 月）

これらの各分野を超えた情報共有を図るために、各セプターにより構成される「セプターカウンシル」を創設している。

更に、各セプター及び重要インフラ所管省庁との「縦の情報共有」体制の強化を通じた重要インフラ防護能力の維持・向上のために、情報連絡・情報提供

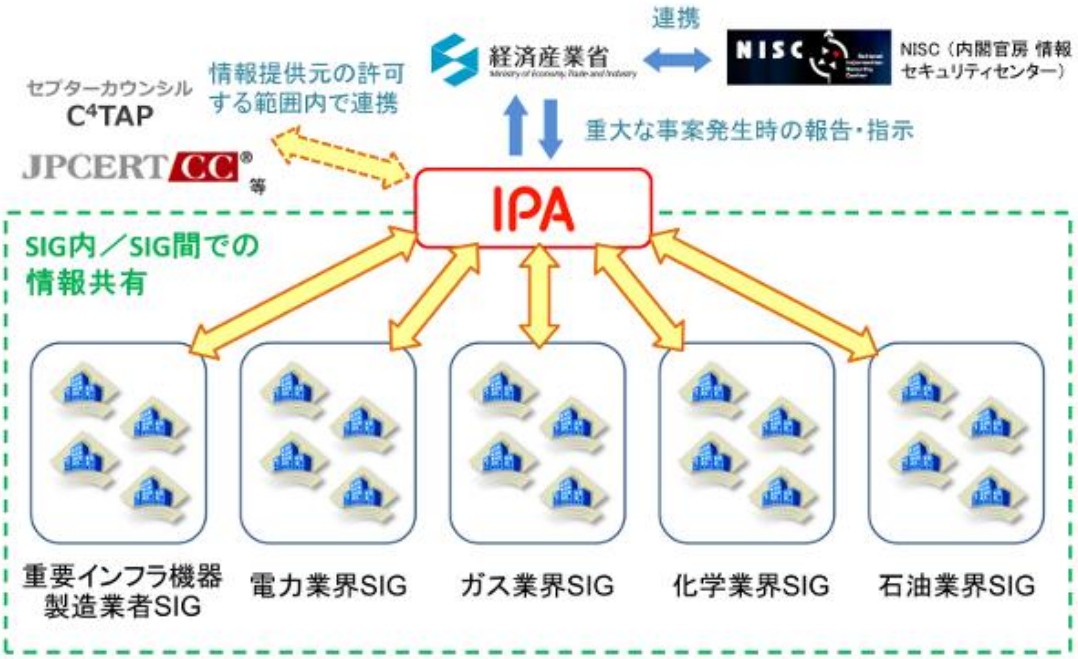
の手順に基づく「セプター訓練」をして実施している。

また 2011 年 10 月に経済産業省の協力のもとに、IPA がサイバー攻撃による被害拡大防止のため、重要インフラで利用される機器の製造業者を中心に、サイバー情報共有イニシアティブである J-CSIP を発足させた。

J-CSIP は現在、全 5 業界 45 の参加組織による情報共有体制を確立し、サイバー攻撃に関する情報共有を通して、参加組織における以下のような防御力の向上を図っている。

①類似攻撃の早期検知と障害の回復
②攻撃に対する防御の実施
③今後想定される攻撃への対策検討

図表 3.2-5　サイバー情報共有イニシアティブ（J-CSIP）体制図



（出所）IPA ホームページ

3.5. 制御システムのセキュリティマネジメントに関する取り組み

2009 年には、JPCERT/CC が「制御システムセキュリティガイドライン、標準、及び認証への取り組みに関する分析」をまとめ、各国の制御システムのセキュリティガイドラインや標準、認証について報告を行っている。

こうした動きを受けて、CSSC では制御システムセキュリティに特化した認証規格の推進を行っており、制御システムの汎用的な国際標準として IEC62443 を選択している。その理由としては、lEC62443 が制御システムセキュリティの全レイヤ/プレイヤーをカバーした規格であり、先行する事業者向けセキュリティマネジメント認証の CSMS や装置ベンダー向けの機器認証の EDSA といった規格が IEC62443 に採用される方向にあるためである。

3.6. 制御システム機器のリスクへの対応

JPCERT/CC では、制御システム製品のベンダー向けに情報共有コミュニティ「制御システムベンダーセキュリティ情報共有タスクフォース（当時名称)」を 2009 年に発足させている。2010 年度からは、制御システムベンダに限らず、制御システムに携わる方を対象に参加者を募集し、制御機器のサイバーセキュリティリスクを共有している。また制御システムの技術的な観点から「国内の制御システムにおける汎用通信プロトコルの利用状況およびセキュリティへの取り組み状況に関する調査」や「制御系プロトコルに関する調査研究」といった報告書を作成し、プロトコル等の対策を提言している。

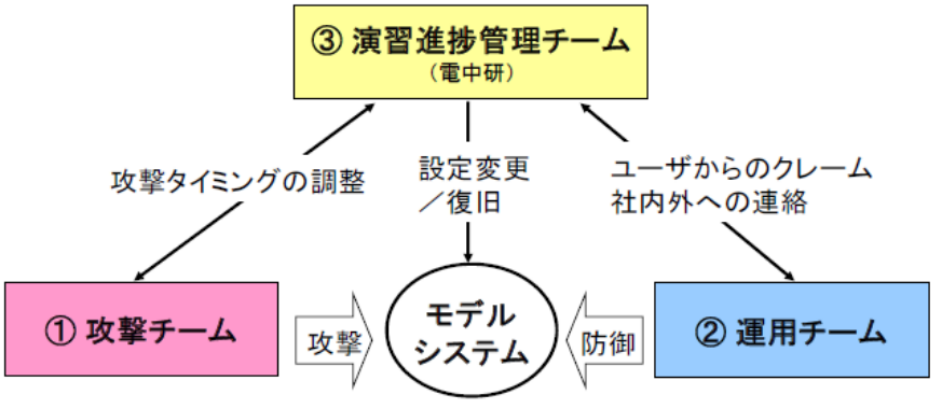
3.7. 電力システムを対象としたサイバーセキュリティ演習

2012 年 3 月に技術研究組合制御システムセキュリティセンター（CSSC）が設立され、宮城県多賀城市にサイバー演習拠点と、東京に研究センターが稼動している。

CSSC では制御セキュリティテストベッド（CSS-Base6）として、7 種類の模擬システム（排水・下水プラント、ビル制御システム、組立プラント、火力発電所訓練シミュレータ、ガスプラント、スマートシテイ、化学プラント）を稼働させており、サイバーセキュリティ演習の実施している。

また電力中央研究所では、電力システムにおける一般業務系システムを対象としたサイバーセキュリティ演習を実施している。本演習には電力会社および関係会社のサイバーセキュリティ担当者が傘下しており、演習用モデルシステム上でサイバー攻撃を実際に体験することができる。具体的には、電力中央研究所が攻撃および進捗管理を行い、演習参加者は運用チーム（防御側）として参加する。

図表 3.2-6　サイバーセキュリティ演習実施体制



（出所）重要インフラ情報セキュリティフォーラム 2009
「電力分野におけるサイバーテロ演習」

演習シナリオは、攻撃の状況想定・前提条件（攻撃目的、侵入経路、攻撃対象、攻撃の種類）等を規定する。また攻撃の網羅性を確保するためケースを設定し、ケースの範囲内での具体的な攻撃手法は攻撃者が自由に選択する。更に、限られた時間内で様々な攻撃を経験するため前提条件（不正端末が接続されていた等）や促進ルール（ユーザーID、パスワードの開示等）を適用している。

3.8. サイバーセキュリティリスクに関する海外動向調査

サイバーセキュリティリスクの被害が実際に起きている海外動向を把握するために、IPA ではウェブページ上に制御システムのセキュリティのページを設置し、米国と欧州の制御システム担当機関の公開文書を翻訳して公開している。

- 米国国土安全保障省(DHS)の産業制御システムセキュリティ担当機関である ICS-CERT から公開された注目すべき文書の抄訳を掲載。
- 欧州ネットワーク情報セキュリティ庁（ENISA）が発行する制御システムに関する公開文書から注目すべき文書の抄訳を掲載。

また IPA 独自でも調査報告書をまとめ、制御システムのセキュリティについて提言を行っている。

- 「重要インフラの制御システムセキュリティと IT サービス継続性に関する調査」（2008 年度）
- 「組込みソフトウェアエンジニアリング標準に関する調査」（2008 年度）
- 「制御システムセキュリティの推進施策に関する調査報告書」（2009 年度）

3.9. 個別業界におけるサイバーセキュリティ対策

3.9.1.金融業界の取り組み

金融業会においては、公益財団法人金融情報システムセンター（FISC）が業界横断的なサイバーセキュリティ対策を自主的な活動として進めている。

金融システムにおいては、クローズドに構成されている基幹システムと、通常のインターネット回線を使用したインターネットサービスが緊密に連携して動作するため、基幹システムにおける外部接続点においては DMZ や F/W の設置を徹底している。また DMZ や F/W の設置を徹底していても、悪意ある犯罪者は何らかの手段により必ず侵入してくるとの前提の下、入口対策もさることながら、出口対策（中から外への情報発信の検知・遮断等）の強化も進めている点が特徴である。対策が進む特に欧米の金融機関を参考に、日本の金融機関におけるサイバーセキュリティ対策も Prevention（防護）から、Detect（検知）&Response（対策）へと切り替わりつつある。

図表 3.9-1　FISC が提言するサイバーセキュリティ対策

対策	予防	検知・防御
入口対策	● OS のサービスパック最新化 ● OS、汎用ソフトウェアのセキュリティパッチ適用 ● マルウェア対策ソフトのパターンファイル更新	● ファイアーウォール ● マルウェア対策ソフトの導入 ● IDS/IPS の導入とシグネチャ[4]の更新 ● スパムメールフィルタの導入とブラックリストの更新[5]
内部対策	● OS やデータベースの ID、パスワードの適切な管理、パスワードの変更管理 ● エラーログを含む、アクセスログの取得と定期的な分析 ● OS やデータベースの最小特権機能の導入 ● 起動プロセスの制限 ● ファイルの暗号化 ● データベースの暗号化	● 振舞い検知型マルウェア対策ソフトの導入 ● 特定コマンドの実行監視[6] ● ポリシーベースのデータベースアクセス監視[7]
出口対策	● 通信ログ、イベントログの取得と定期的な分析	● IDS/IPS の導入とシグネチャの更新 ● 次世代ファイアーウォール

（出所）金融情報システム No.325（2013 冬）「金融機関におけるサイバー攻撃への体制整備について」を基に日本総研作成

[4] 攻撃や不正アクセスの特徴を定義したデータで送受信されるトラフィックとシグネチャを比較することで、不正侵入や外部への不正通信を検知・遮断する。

[5] 現在のメールシステムでは、送信経路が記録されるため,発信されたサーバーを特定することができる。ブラックリストとはスパムメールの発信元として知られているサーバーや発信元を偽装するためにメールの中継を行うサーバーの IP アドレスを列記したもので、ブラックリストを受信メールサーバに登録することで、該当サーバーからのメール受信を遮断することができる。

[6] 管理者権限への変更などマルウェアの活動過程で不正に実行される特定のコマンドを監視する。

[7] 予め業務プログラムが使用する SQL 文をポリシーとして登録し、「SELECT*」文など不正プログラムが情報窃取のために発行するような SQL 文を監視して、DB へのアクセスを遮断する。

また、資金余力のある金融機関本体は十分な対策が出来るが、中小の金融機関や関連会社や協力会社といった外部委託先はサイバーセキュリティ対策が万全でないことも多く、FISC においても対応が議論されている（具体的には、中小金融機関によるサイバーディフェンス・ソリューションの共同購入やメンバーシップ制組織の設立などが検討されている模様）。

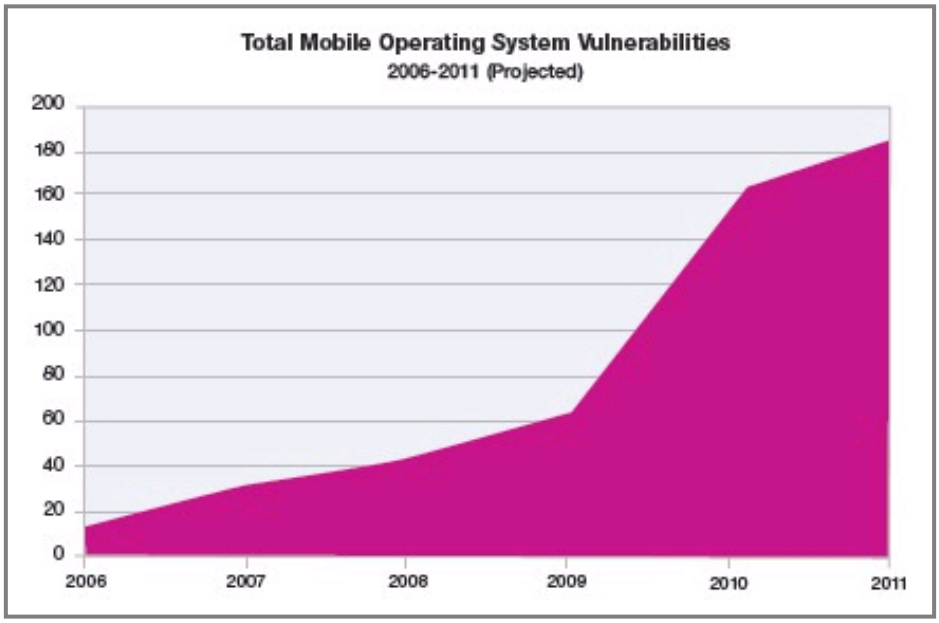
個別の金融機関の対策では、大手行であれば必ず組織内 CSIRT（Cyber Security Incident Response Team）という組織横断のサイバーセキュリティ部門が設置されており、当該部門が組織横断的にサイバーセキュリティ対策の啓発や、実際の被害発生時の対策等を実施している。

FISC の業界横断的な取り組みとしては、NISC 金融セクターにおいて情報共有体制の構築が図られており、同セクターにおいて年 1 回のサイバーセキュリティ対策演習が実施されているものの、参加者が限定的であり業界全体のセキュリティレベルを底上げするような活動には至っていないと認識されている。

3.9.2.情報通信業界の取り組み

情報通信業界では、デジタルデバイスの普及とともに、サイバー攻撃の対象も従来の Server や PC から SmartPhone、タブレット急速にシフトしてきている。CNCERT の発表によると、2013 年にウイルスに感染したスマートフォンの数は世界で 800 万台以上に上り、それらから 1,600 個以上の悪意のあるコードが検出されたとされる。

図表 3.9-2　モバイル端末で報告され脆弱性の推移（世界）



（出所）米 IBM「2011 年中期セキュリティ動向の調査報告」

情報通信業界では、攻撃対象の多様化とともに、攻撃手段も巧妙かつ複雑に進化してきている。このような脅威に速やかに対応し、業界全体のセキュリティ対策の水準を向上させていくためには、電力業界においてもインフラ事業者、制御系システム事業者等を問わず、脅威の進化と対策の継続性を啓蒙する活動や、啓蒙コストを個別事業者任せにせず業界や国として準備することが有用であろう。また、米国では電力システムに対するサイバー攻撃が増加していることは既に述べたとおりだが、攻撃者はこれまで情報通信業界に対して攻撃を行ってきた者と同一である可能性もあり、通信事業者が有する攻撃源の共有も有効な対策の一つとして考えられる（具体的には、IP アドレスや ISP 情報、Keyboard 情報、Character 情報（文字情報）等の情報を取集し、攻撃者やその特性を限定し、攻撃リスクに対する予防ときめ細やかな対策等が想定される)。

既に情報通信業界においては、送信元ブラックリストや対策チューニングなど情報共有、対策技術の研究開発、法制度改定や緊急避難時の解釈の取り扱い、業界横断でのサイバー演習の実施など業界横断的な取り組みや、当該活動に対する国費活用などを積極的に進めてきており、このような経験を有する通信業界との分野横断的な取り組みの拡充は、今後、電力業界にとっても大いに参考になるだろう。

また現在導入が進むスマートメーターにおいては、通信事業者が提供する通信回線がスマートメーターデータの通信ネットワークとして活用される。スマートメーターのセキュリティ機能の実現には、メーターそのものの防護だけでなく、電気事業者とメーターの間の通信機能を提供する通信事業者の取り組みも必要となる。このためには、メーターのセキュリティ機能の同定と検証、通信事業者が提供するスマートメーター用のサービスのあり方、さらには責任分担のあり方、データ保護のあり方を検討される必要がある。この点でも、通信事業者との連携はさらに強化されるべきである。

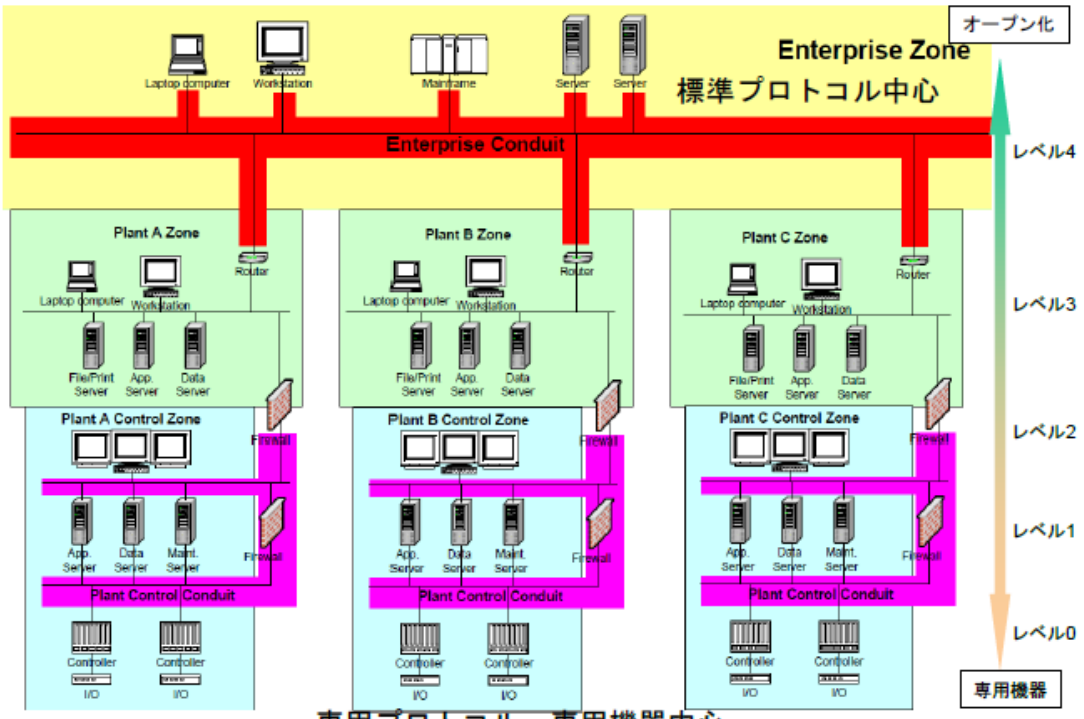
3.9.3.プラント産業の取り組み

汎用ＯＳ・アプリケーションの導入に伴うサイバーセキュリティリスクの増加に着目し、「たとえクローズドなネットワークであっても、接続点がある限り、外部からの侵入がある」という前提になった各種の対策を検討してきている。

（1）プラント産業全般のサイバーセキュリティ対策

制御システムのネットワークの対策として、接続点における DMZ の設置、侵入後に重要なシステムまでの到達を許さない多段構成（多層防御戦略)、マルウェア等の感染拡大を防ぐためのネットワーク構成などが検討されてきている。

図表 3.9-3　制御システムにおける多層防御戦略の概念図



（出所）ISA「An Overview of ISA99」（2007 年 10 月）

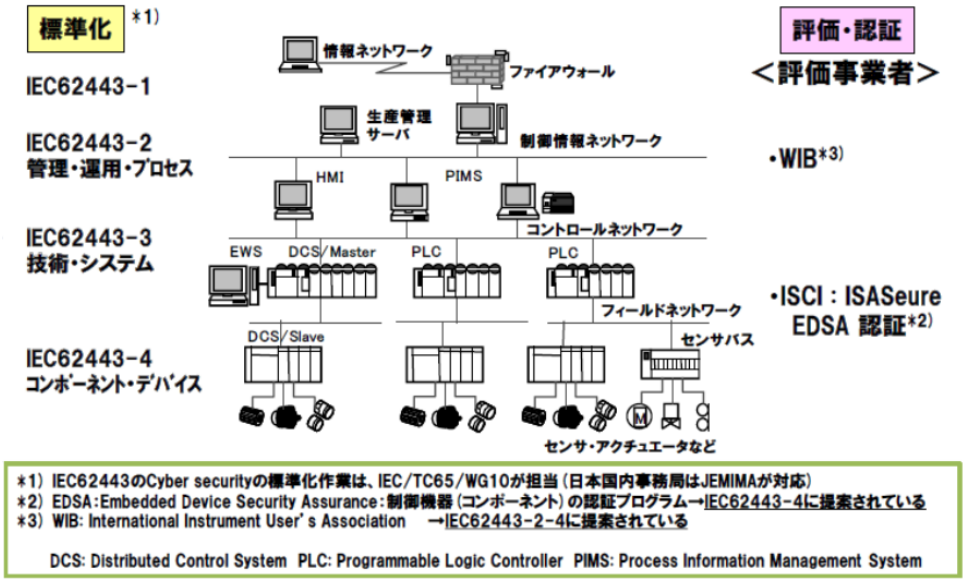
また、工場内で稼動するプログラムを認証されたものだけを動作させるホワイトリスト方式を採用しているケースもある。工作機械メーカーのアマダでは、当初はウィルスソフトを導入してサイバーセキュリティ対策を行おうとしていたが、ウィルススキャン時のＣＰＵ負荷が大きいために工程内のパソコンが誤作動してしまった。そこでホワイトリスト方式を採用した。

さらにUSBメモリにウィルススキャン機能を組み込んで感染を防ぐケースもある。コンピューター周辺機器メーカーのバッファローでは 2010 年に工場内へウイルスが侵入した。これは外部から持ち込まれた USB メモリにウイルスが入っていたことが原因だった。そこで、USB メモリに強固なセキュリティ機能を組み込み、万が一 USB メモリにウイルスが入っていても、そのセキュリティ機能がブロックし被害を食い止める対策を行っている。

（２）汎用制御システムの標準規格 IEC62443

IEC62443 は制御システムセキュリティの全レイヤ/プレイヤーを網羅した規格となっており、先行する EDSA（Embedded Device Security Assurance）認証や WIB（Working-party on Instrument Behaviour）などが IEC62443 に採用される方向となっている。

図表 3.9-4　制御システムにおけるセキュリティに関する規格

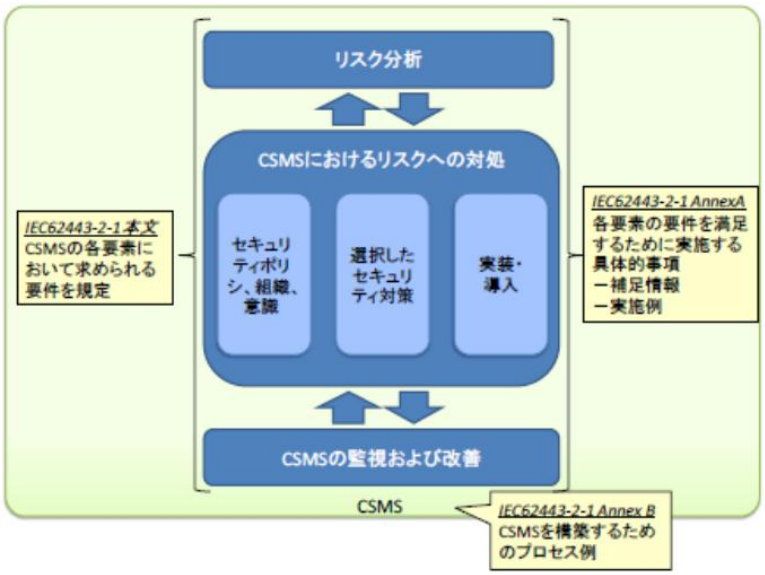


（出所）ICEC「CSSC EDSA 認証」（2013）

（３）CSMS(Cyber Security Management System)認証規格

EDSA は装置ベンダー向けで米国が先行しているが、事業・運用者向けの IEC62443- 2 をベースとした CSMS 認証は ISMS の制御システム版と考えられており、国内ではこちらが先行しており、JIPDEC（一般財団法人日本情報経済社会推進協会）が推進している。

図表 3.9-5　CSMS 認証の概要

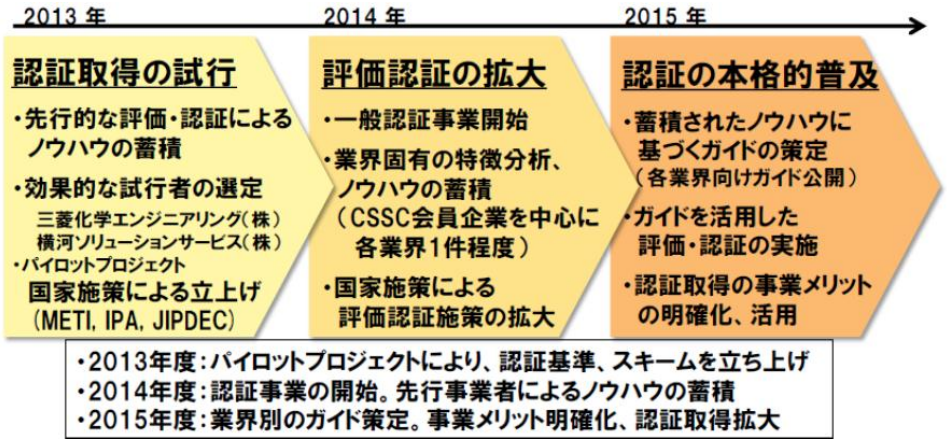


（出所）IPA「制御システムにおけるセキュリティマネジメントシステムの構築に向けた解説書」

CSMS は、リスク分析とリスクへの対処、監視及び改善のマネジメントサイクルになっており、リスクを識別し、リスクをアセスメントしてから対策を行うことが求められている。また、セキュリティポリシーの策定や組織体制の構築といったことも求められる。

2013 年には CSMS 認証を取得するために 2 社（化学系エンジニアリング、制御・計測システム保守ベンダー）が試行をしている。

図表 3.9-6　CSMS の認証の普及見通し



（出所）ICEC「CSSC EDSA 認証」（2013）

4. 我が国の電力システムに求められるサイバーセキュリティの在り方

4.1. 諸外国・他産業の取り組みから得られた示唆

以上に述べた調査結果から得られた示唆は次のとおりである。

1）米国におけるサイバーセキュリティ対策

米国では早くから重要インフラにおけるサイバーセキュリティ対策の重要性を認識しており、国家を挙げた対策を実施してきている。当初は電力事業者の任意団体として発足し、北米大停電以降、電力供給の信頼性確保に向けた業界横断的な取り組みを主導し、2007 年以降に ERO として電力システムに対するサイバーセキュリティ標準（NERC CIP）を策定してきている NERC の取り組みは、我が国の今後の電力システムの保安対策を考えるうえで重要な示唆を与えてくれる。

NERC が単独ではなく、FERC 及び DOE と連携してサイバーセキュリティ対策の水準を向上させている事例は、我が国においても電力セクターのサイバーセキュリティ対策に責任を持つ公的な機関が必要なことを示唆している。

また NERC CIP では、事業者の裁量が大きかった Ver.3 から、個別システムに対する具体的なセキュリティ要件と基準を明示した Ver.5 の発効が議論されているように、事業者への強制力が働く仕組みへと変わりつつある。我が国においても、電力の安定供給を維持し続けるうえで重要な施設を有する事業者に対しては、ある程度の強制力を持った規格やガイドラインの施行が有効なのではないか。

2）欧州におけるサイバーセキュリティ対策

欧州では、各国の取組みの支援や橋渡しを行う組織として、またネットワーク情報セキュリティに関する情報、ベストプラクティスの共有、欧州委員会や各加盟国に提言を行う担当機関として、欧州ネットワーク情報セキュリティ庁（ENISA）が設置されており、電力・スマートグリッドシステムを含む制御システムのサイバーセキュリティを所管している。具体的な活動としては米国を含めた海外の事例についての調査・分析等の実施、それらに基づくサイバーセキュリティ関連の推奨施策の提言を行っており、このような海外事例をベンチマークして、統一的な推奨施策の提言を行っている点は我が国にとっても参考になる。

スマートグリッドのサイバーセキュリティ対策について本格的な検討を開始したのはここ５年のことであるが、その問題意識の背景にはスマートメーター・スマートグリッドの急速な普及があり、後追いでの対策を防ぐために、セキュリティ対策についても標準が必要とされている。特に特に重点的に対策が検討されている分野として、事務処理系ネットワークやリモートメンテナンス

回線から制御系ネットワークへサイバー攻撃が拡大することが挙げられている。このような事態を想定し、制御システム内部への侵入は避けられないとの認識に立って、内部での対策の必要性が認識されている。ただし対策コストとの兼ね合いがあるため、どこまでを義務化すべきかについてはさらなる検討が必要とされている。

なお、各ＥＵ加盟国においては、原則的に各国の政府が責任を持ち、独自の方法で重要インフラ制御システムの情報セキュリティ強化に取り組んでいる。例えば、施策推進の中心は、英国、スウェーデンのように重要インフラ防護の所管省庁である場合や、ドイツのように情報セキュリティの所管省庁である場合がある。英国やドイツでは制御システムセキュリティに関する基準・ガイドを政府が直接作成しているが、オランダでは政府から独立した民間の機関に作成を委託している

3）我が国の他産業におけるサイバーセキュリティ対策

本調査では、比較的サイバーセキュリティ対策が進んでいると考えられる金融業界、情報通信業界、プラント業界を対象に、そのサイバーセキュリティ対策をベンチマークした。

金融業界では、通常のインターネットサービスと基幹システム間においてデータ交換を行う外部接続点においてセキュリティ対策が徹底されていたが、そのうえで攻撃者は内部に必ず侵入するとの想定に基づき、内部対策や出口対策（振舞検知型マルウェア対策ソフトの導入、特定コマンドの実行監視、ポリシーベースのデータベースアクセス監視、IDS/IPS の導入とシグネチャの更新、次世代ファイアーウォールの導入等）が検討されていた。対策により外部からの侵入に対する防御は万全であるとの認識から一歩進め、「外部からの侵入は必ずある」との前提に立った対策立案は、今後、複雑かつ巧妙化する攻撃に曝されるであろう電力システムのサイバーセキュリティ対策を考えるうえで有用である。

情報通信業界では、複雑かつ巧妙化する攻撃手段に対して様々な対策を講じてきており、エンドユーザーへ転嫁できない各種の対策コストの負担についても先行して様々な議論や取り組みを積み重ねてきた実績がある。送信元ブラックリストや対策チューニングなど情報共有、対策技術の研究開発、法制度改定や緊急避難時の解釈の取り扱い、業界横断でのサイバー演習の実施など業界横断的な取り組みや、当該活動に対する国費活用方法など参考にすべき取り組みは多い。また今後、導入が進むスマートメーターにおいては通信事業者が提供する通信ネットワークを活用する比率も増加するため、責任分界に関する議論や安全性確保の取り組みも協働で進めていく必要があり、今後ますますの連携が必要となろう。

プラント産業においては、汎用ＯＳ・アプリケーションの導入に伴うサイバーセキュリティリスクの増加に早くから着目し、「たとえクローズドなネットワークであっても、接続点がある限り、外部からの侵入がある」という前提になった各種の対策を検討してきている。具体的には、制御システムのネットワークの対策として、接続点における DMZ の設置、侵入後に重要なシステムまでの到達を許さない多段構成（多層防御戦略）、マルウェア等の感染拡大を防ぐためのネットワーク構成などが検討されてきている。また USB メモリに対するウィルススキャン機能の導入、工場内で稼動するプログラムを認証されたものだけを動作させるホワイトリスト方式の導入なども具体的な対策として参考になる。

4.2. 我が国の電力システムのサイバーセキュリティに関する評価

本調査では、電気事業連合会を通じて一般電気事業者の協力を得て、複数社へのヒアリングおよび全 10 社へのアンケート調査を実施した。これらの調査に基づき我が国の電力システムの構成と現状のサイバーセキュリティに関する評価を行ったところ、概ね次のようなものであった。

電力制御システムに対する一般電気事業者各社のサイバーセキュリティポリシーは、電力業界（10 の一般電気事業者）の自主的な取り組みとして策定・運用されている電気事業連合会ガイドラインに則って、全社ポリシーあるいは部門ポリシーを策定し構築されている（スマートメーター等については NIST 等のガイドラインを参考に対策を実施・検討）

発電所監視制御システム等を含む電力制御システムは、出来る限り外部との接続点を限定したクローズドなネットワーク構成とし、物理的隔離と侵入防御（守衛等による入退所管理）、記録媒体の持ち込み制限、下請け等の要員管理などの対策を行っている。外部とネットワーク接続がある場合にも、ファイアーウォール等による通信経路・方向の限定、リモートメンテナンス回線の極小化、接続先を認証して必要時のみ外部接続する運用等を行っており、外部からの侵入を防ぐ対策を行っている。

また電中研や CSSC が主催するサイバーセキュリティ演習等への参加を通じて、定期的にサイバー攻撃に対する防御策に対する練度も向上させるとともに、サイバーセキュリティに対する定期的な意識啓発も行っている。

これらの取り組みにより、これまで運転制御に影響のあるセキュリティインシデントは発生しておらず、セキュリティ対策としては一定の評価ができる。

4.3. 電力システムのサイバーセキュリティ確保に向けた検討の視点

本調査でも既に述べたように、世界では Stuxnet のように、クローズドなネットワーク環境下においても可搬記録媒体等を通じて発電所内部へのマルウェアの侵入を許した事例などがある。また米国等では、リモートメンテナンス回線下で Windows SQL Server のアプリケーションプログラムを立ち上げた際に外部から脆弱性を攻撃された事例や、発電所を退職した人員が、退職後のアクセス権限抹消までのタイムラグを利用して発電所内部のシステムに侵入を試みた事例などが報告されている。また米国では電力システム関連施設への不正アクセスが多数、報告されており、その攻撃方法も巧妙かつ複雑化している。このように、サイバー攻撃の手段は多様化しており、未知のウイルス・マルウェア等への対策、汎用アプリケーション・ＯＳの脆弱性への対処、要員管理・アクセス権限管理の徹底等の個別対策が望まれるが、すべての電力制御システムに適用可能な確立した技術はないことから、コスト面・レスポンス面・運用面で支障のない範囲で対策を計画的に実施することが重要となる。

またより上位の「セキュリティ対策の考え方」という視点に立てば、従来の「クローズドなネットワーク構成（＝外部からの通信ネットワークを介した侵入は不可能)」という見地から、「クローズドであっても侵入はあり得る」という見地に立った対策へと切り替える必要があろう。既に制御システムのセキュリティ対策では、このような考え方に基づき、接続点での侵入検知・防御、あらかじめ登録されたアプリケーションやコマンドしか実行できないホワイトリスト方式、たとえ侵入を許しても、重要度の高いシステムに到達することを防ぐ多層防御などが検討されており、電力システムのセキュリティにとっても参考になる取り組みが多い。但しこれらのセキュリティ対策を可用性が極めて重要な電力システムに適用する場合、機能追加やネットワーク構成の変更に伴うコスト増、作業プロセスの刷新に伴う運用への影響、応答時間に与える影響等、検証すべき点は多い。そのため当面は現在の対策を一歩進め、F/W や GW における異常なアクセスを検知する仕組みを導入するなど、進化する攻撃手段に備える対策が重要となる。

さらに、サイバー攻撃の脅威は日々進化しており、より巧妙かつ複雑に進化しているため、現状の個々のリスクについて認識をすれば対策として十分ということはなく、増加するリスクに対してどのように都度認識できるようにするのかという包括的な視点での検討が、持続的な対策として有効であると考えられる。そのためには、個別の技術的な対策もさることながら、最新のサイバーインシデントやセキュリティ対策にキャッチアップし、それらに対するリスクアナリシスを通じて、対策の必要性ならびに対策が必要な場合の個別対策立案、事後評価を行うためのサイバーセキュリティリスクのマネジメントシステムを確立することが望ましい。既に日本では CSMS のパイロット認証が始まっており、2016 年度から第三者認証がスタートする見込み。電力システムにおいても、これらを参考にしたマネジメントがなされることが望ましい。

当面の運用においては、事業者ごとに、ネットワークに接続しているシステムに対して、システムの導入時・変更時、ネットワーク接続時にリスクアナリシスを行うことが推奨される。なおその際、すぐさま第三者認証を取得することは難しいと考えられるため、リスクアナリシスを通じて必要な対策が実施済みであることを、各事業者が必要な記録の保管を通じて促すことが有効である。その際、各事業者間において、システム構成やセキュリティポリシーが異なることを鑑み、具体的なマネジメントサイクルについては各社に委ねることが現実的な対応として考えられる。

業界横断的な取り組みとして、既に各社の情報セキュリティ担当者が集う会議体が存在しており、加えて CSSC や電中研のサイバーセキュリティ研修が実施されていることから、業界横断的な取り組みについては十分に実施されてきていると考えられる。しかし今後は、スマートメーターの導入や新規参入者の増加に伴い、電力システムにおいてもインターネット回線を介した情報交換の頻度が増加すると考えられることから、情報通信業界等、異分野のサイバーセキュリティ担当者との意見交換を促進する「場」の創出を進めていくことが有用であろう。また世界的に電力システムに対するサイバー攻撃が増加する中、サイバーセキュリティリスクに関する最新情報を共有するために、サイバーセキュリティ情報に関する専門機関（JPCERT、IPA）との連携も有用だろう。

また、今後は電源の多様化の流れに伴う再生可能エネルギーの導入が考えられる。代表的なものとして太陽光発電、風力発電が挙げられるが、これらは日照や風況により時々刻々と変化する電源であるため、適切に出力変動に対処しなければ、系統の周波数の乱れを引き起こし、安定的な電力供給に影響を及ぼす可能性もあるため、再生可能エネルギー等の出力等の情報を踏まえた需給調整はより一層重要なものとなる。また、電力システム改革の進展に伴い、多様な事業者が一般電気事業者の運用する制御系システムに連系し電力の安定供給を実現することも考えられるため、電力システム改革の進展を踏まえた対応も検討していく必要がある。現在は一般電気事業者の自主的な取り組みとして電気事業連合会のガイドラインが存在するが、米国の NERC CIP、NIST SP 800 シリーズ、NISTIR 7628 等の統一的な基準・ガイドラインを参考に我が国の電力システムに対する統一的な基準・ガイドラインを検討することも有用だろう。

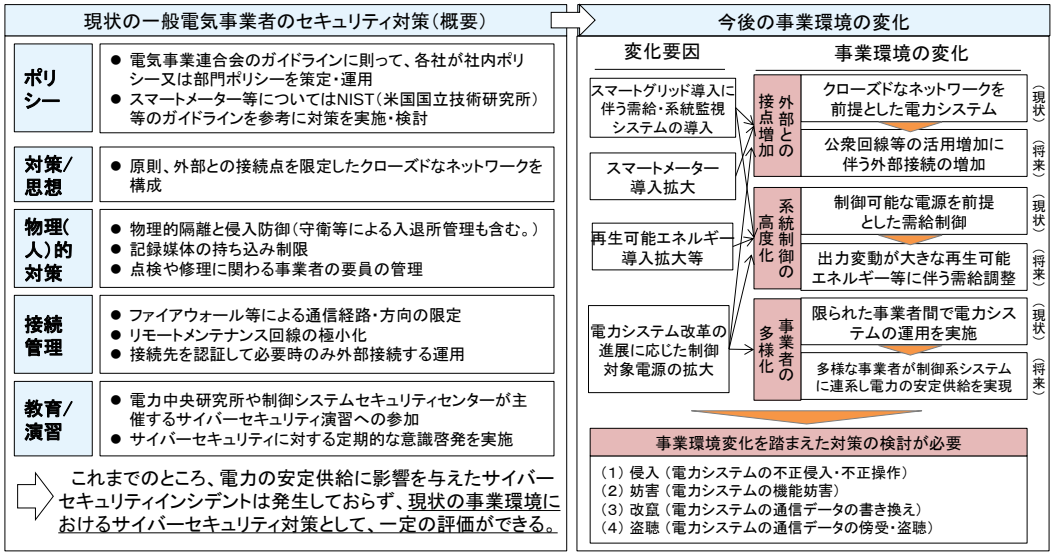
また導入が進められているスマートメーターはその通信システムは、①メーターによるデータ取得、②通信回線による送配電事業者のサーバーへのデータの送付、③送配電事業者から小売事業者のサーバーへのデータの受渡しの 3 つが一体となって機能するものとなっている。スマートメーターの脆弱性を利用したサイバーアタックによって、大規模な停電が引き起こされることは(発電所監視制御システム等と比べて)相対的に少ないと考えられるが、自動開閉機能を持つスマートメーターについては、一戸単位で開閉操作を行うことも可能であるため、不正操作ができないようにするセキュリティ対策が必要である。例え

ば米国では、スマートメーターの赤外線ポートから検針データの閲覧や書き換え等を行う被害事例が報告されており、その対策としてスマートメーターのサイバーセキュリティについても十分な検討が行われている。その中では境界の保護(DHS2-8-7 項)の理論的解釈事項として、電力会社の自動検針インフラシステムに対するサイバーセキュリティのリスクを最小限に抑え、かつ、不正アクセスを可能な限り避けるため、AMI ネットワーク（A ルート）と、不特定多数の接続が期待される HAN などスマートグリッドアプリケーションネットワーク（B ルート）の間では、物理的インターフェースを含む境界間の保護やシステムやセキュリティ領域の分離を行うことも検討されている。

我が国においても、スマートコミュニティアライアンス（JSCA）に設置されたスマートハウス・ビル標準・事業促進検討会において、平成 25 年 5 月に、「HEMS-スマートメーター（B ルート） 運用ガイドライン」をとりまとめている。この中で、スマートメーターB ルートの開通においては、システム面、保守運用面において十分なセキュリティ強度を有するべきであるとして、A/B ルートの分離等、セキュリティについての基本要件を定めている （詳細は付録 8 参照） 。また、A ルートに関しては、現在、各電力会社が構築を進めているところであり、ネットワーク仕様に沿ったセキュリティ対策が検討されている。

スマートメーターは日本全国で数千万個という単位で導入されるインフラであるため、全ての設置台数に対して万全な保安の確保を求めることは現実的ではない。そのため、スマートメーターのサイバーセキュリティ対策についても、他の電力制御システムと同様に、適切なリスクアナリシスを通じて、十分なセキュリティ対策が実施されることが期待される。またスマートメーターは、検定有効期間が１０年であり、設置後長期間使用される可能性が高いことを考慮すると、導入済みのスマートメーターのサイバーセキュリティ対策を確保していくための施策についても検討が必要であろう。

図表 4.3-1　現状の電力システムのセキュリティ対策と将来におけるリスク



（出所） 日本総研作成

4.3.1.電力分野のサイバーセキュリティ対策について考慮すべき事項

セキュリティ対策を構成する要素として、機密性・完全性・可用性の三要素が挙げられるが、電力システムは運用の大原則として、供給と需要の同時同量を図っていくことが必要となるため、セキュリティ対策に当たっては、安全性を第一としつつも、可用性を過度に妨げないことを考慮することが重要である。

また電力制御システムのサイバーセキュリティ対策を検討する上では、電力会社のみに議論が偏ることがあるが、特に将来的な技術的な対策については、ベンダー等の電力業界の他のプレイヤーとの協働が必要である。従って、一義的な責任は電力会社としつつも、電力システムに関連する様々な事業者のセキュリティ対策を一様に向上させていくことで、経済・社会的な重要インフラである電力供給システムの安全性・安定性を確保する仕組みを構築することが重要である。

さらに電力インフラの公共性を考慮すると、サイバーセキュリティリスクへの追加的な対策に伴うコストの負担について、その目的に応じて電力会社単独で負担すべき範囲、業界全体で負担、若しくは国費を活用して負担すべき範囲など、適切なコスト負担も考慮事項と言える。

4.3.2.具体的なサイバーセキュリティ対策

以上の視点を踏まえ、電力システムにおける現状のサイバーセキュリティ対策のさらなる高度化及び今後の事業環境の変化を踏まえながら実施を検討するべき事柄としてとして以下を提言する。

①リスクマネジメントシステムの確立

現在の電力システムにおいて主要な役割を果たしている一般電気事業者が、リスクアナリシスを通じてネットワーク接続点を有する重要資産を分析し、その記録を保管するなどマネジメントシステムを確立することが重要である。

また、電力制御システムにおける汎用 OS・プロトコルの普及、外部接続機会の増加によって、調達する機器やシステム自体のサイバーセキュリティリスクについても配慮が必要となる。

現在、CSMS のパイロット認証が進められているが、このような取り組みを参考としつつ、電力業界全体において、サプライチェーンリスクへ対応できる体制を整えていく必要がある。

- 一般電気事業者・新規参入者
  - サプライチェーンリスクを考慮した調達・廃棄プロセスの管理
- 政府機関
  - 電力システム分野における認証導入の検討
- ベンダー（機器メーカー・ソフトウェアベンダー）
  - 電力システム向けに納入する機器・ソフトウェアのサプライチェーンにおけるセキュリティチェックの徹底

特にスマートメーターは日本全国で数千万個という単位で導入されるインフラであるため、先にも述べたように全ての設置台数に対して万全な保安の確保を求めることは現実的ではないが、他の電力制御システムと同様に、適切なリスクアナリシスを通じて、十分なセキュリティ対策が実施されることが期待される。

②外部接続点の対策徹底

既に述べたように、電力システムにおける外部接続点の増加や、電力システムに対するサイバー攻撃の増加を考慮すると、これまでのクローズドなネットワークという前提から、「外部侵入はあり得る」という立場に立った高度な対策が必要である。そのために不正な通信の監視・検知及び侵入防御の多段構成等の対策が求められる。

③業界横断的な情報共有

一般電気事業者や将来的な新規参入事業者が、通信事業者と連携してサイバーセキュリティ対策を一層進めていくことが必要である。

- 電気事業者、通信事業者双方に共通する共通脅威の分析
  - 送信元ブラックリストの共有等
- 電気事業者、通信事業者間のリスク・コミュニケーションの機会拡充

- 対策チューニング等
- 分野横断的演習の実施
  - スマートメーター通信ネットワーク等を対象としたサイバーセキュリティ演習の共同開催等

④セキュリティ人材の訓練・育成

経済産業省や電気事業連合会のような業界団体が、一般電気事業者のみならず、新規参入を予定している事業者に対しても、自社のみならず社会的にも影響を与え得る経営課題として、サイバーセキュリティ対策の重要性を認識させる意識啓発活動を図っていくことが必要である。

またこのような意識啓発の結果、一般電気事業者や新規参入事業者の自社内において、電力システムのサイバーセキュリティに従事する人材の動機付け・位置づけ向上を図ることも重要である。

また近年のサイバー攻撃の進化を踏まえると、入口対策から内部対策、出口対策へのサイバーセキュリティ対策の重点を移していくことになると考えられる。そのためには、サイバーセキュリティ対策の導入のみならず、運用時におけるサイバー攻撃の早期発見や、インシデント発生時の迅速対応・早期復旧にも対応できる高度なサイバーセキュリティ人材の訓練・育成を行うことが重要である。この取り組みのためには、一般電気事業者や新規参入事業者が自社内で育成プログラム等を開発・運用する他、経済産業省等の政府組織がセキュリティ人材育成に対する支援を行っていくことも有効である。

⑤電力分野のサイバーセキュリティガイドラインの策定等

一般電気事業者は、一般電気事業者等により構成される電気事業連合会の自主的なガイドラインによって電力保安対策が図られてきた。今後の事業環境の変化を踏まえ、米国の NERC CIP、NIST SP 800 シリーズ、NISTIR 7628 等の基準・ガイドラインを参考にして、電力システムに対して統一的なガイドライン（日本版ＣＩＰ）を策定・運用していくことが望ましい。既に米国や欧州では、電力市場に参入する事業者に対する統一的なガイドラインが策定・運用されており、我が国においても同様の取り組みが有効と考えられる。

ガイドラインが含むべき項目は今後検討が必要になるが、本委員会に参加した委員意見から、以下のような内容を含むべきとされた。なお対象となる事業者の事業内容・事業規模に応じて、現実的に遵守することが可能な対策を検討することも重要である。

図表 4.4-1　電力分野のサイバーセキュリティガイドラインが含むべき内容

項目	概要
リスクアナリシス	リスクアナリシスを通じた重要資産の特定
対策立案	資産の重要度に応じたサイバーセキュリティ対策の立案
個別対策	電力システムの物理的保護
	電力システムの電子的接続点の保護
	サプライチェーンリスクへの対処
人材育成	サイバーセキュリティ対策に資する人材育成・教育計画
危機管理	サイバーインシデントへの対応手順

（出所）日本総研作成

ガイドラインの対象となる事業者は、一般電気事業者が運用する制御系システムに連系して安定供給を実現するための電源等を有する事業者が考えられるが、具体的には今後の事業環境を踏まえながら検討を行うことが必要である。

さらに、ガイドラインの実効性を高めるための運用の仕組みについても、米国と類似したものにすることも考えられるが、我が国における実行性の担保や新たに電力制御システムに連系する新規参入事業者の存在も考慮して十分に検討を行う必要がある。

おわりに

本調査では、電力システムを取り巻く事業環境の変化、サイバー攻撃の複雑化・巧妙化を受け、次世代の電力システムにおいて求められるサイバーセキュリティ対策のあり方を検討した。

我が国の電力システムでは、一般電気事業者におけるサイバーセキュリティ対策によって、これまでのところ電力の安定供給を脅かすような事故は発生しておらず、一般電気事業者の取り組みは一定の評価はできる。

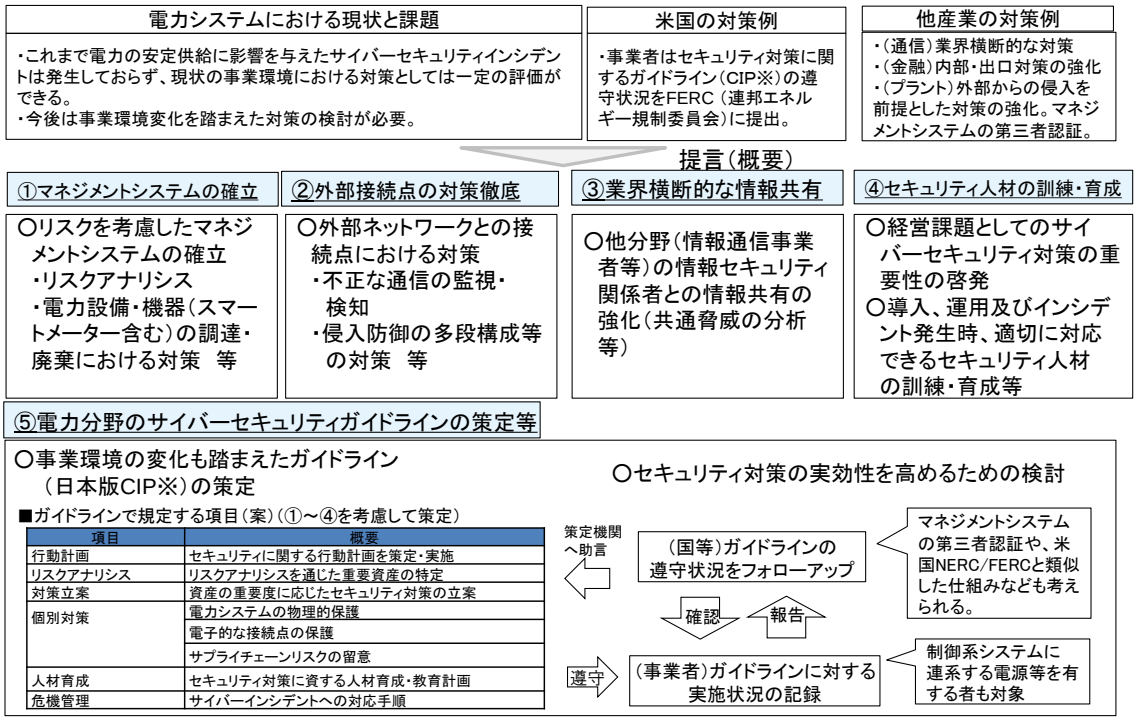
他方、諸外国では、電力システムに対するサイバー攻撃の増加を考慮して、サイバーセキュリティ対策を強化すべく、ガイドラインの運用や内容の拡充を図っているところ。また日本国内の他産業（通信・金融・プラント）においても、進化するサイバー攻撃に対応して、業界横断での取り組みや、サイバー攻撃によるシステム内部への侵入を前提とした内部対策・出口対策への重点を移しつつある状況が明らかになった。

このような状況を踏まえ、我が国の電力システムにおいても、以下の対策が必要となるという結論に至った。

①マネジメントシステムの確立
②外部接続点の対策徹底
③業界横断的な情報共有
④セキュリティ人材の訓練・育成
⑤電力分野のサイバーセキュリティガイドラインの策定等

なお、本調査は、サイバーセキュリティガイドラインについては具体的な内容及び対象となる事業者、その運用方法は詳細の検討はされていないが、今後、必要に応じてその具体的な検討がなされ、社会的・経済的に重要なインフラである電力システムに必要な電力保安が確保されることが重要である。
本調査を踏まえて、重要インフラを担う電気事業者はもとより関係者が適切な措置を講じていくことが望ましい。

図表 5-1　本調査のまとめ



※CIP：NERC（北米電力信頼度協会）が作成するガイドライン（Cyber-security Critical Infrastructure Protection）

（出所）日本総研作成

略語集

A:

ARRA	American Recovery and Reinvestment Act 米国再生・再投資法
AMI	Advanced Metering Infrastructure SM 等を含むスマートグリッドの基盤通信インフラ

B:

BES	Bulk Electric System 大規模電力システム

C:

CEN	Comité Européen de Normalisation 欧州標準化機構
CENELEC	European Committee for Electrotechnical Standardization 欧州電気標準化機構
CEPTOAR	Capability for Engineering of Protection, Technical Operation, Analysis and Response 情報共有・分析機能、「セプター」と呼ぶ
CIA	Confidentiality, Integrity, Availability セキュリティの 3 要素（機密性、完全性、可用性）
CIP	Critical Infrastructure Protection 重要インフラ保護基準
CIPC	Critical Infrastructure Protection Commission 重要インフラ保護委員会
CNCERT	National Computer Network Emergency Response Technical Team / Coordination Center of China 中国の National CSIRT
CPNI	Centre for the Protection of the National Infrastructure 英国国家インフラ保護センター
CPU	Central Processing Unit 中央演算装置
CSCTG	Cyber Security Coordination Task Group NIST の SG 関連機器の情報セキュリティ検討グループ
CSMS	Cyber Security Management System 事業者向けセキュリティマネジメントシステム
CSSC	Control System Security Center 技術研究組合制御システムセキュリティセンター
CSWG	Cyber Security Working Group SGIP の傘下にある CSCTG の後継グループ
CVSS	Common Vulnerability Scoring System 共通脆弱性評価システム
CWE	Common Weakness Enumeration ソフトウェアの脆弱性の共通識別基準

D:

DDoS	Distributed Denial of Service 協調分散型 DoS 攻撃
DHS	Department of Homeland Security 米国国土安全保障省
DMZ	Demilitarized Zone 組織内ネットワークとインターネットの間に設置されている 隔離されたネットワーク領域
DNS	Domain Name System インターネット上でドメイン名を管理・運用するシステム
DOC	Department of Commerce 米国商務省
DoS	Denial of Service ICT サービスの提供を不能にするサイバー攻撃
DOE	Department of Energy 米国エネルギー省
DPP	Data Protection and Privacy データ保護・プライバシー

E:

EC	European Commission 欧州委員会
ECIs	European Critical Infrastructures EC 加盟国に影響を与える重要インフラ
EDSA	Embedded Device Security Assurance 組込み機器のセキュリティ認証規格
EG	Expert Group エキスパートグループ
EISA	Energy Independence and Security Act エネルギー自給・安全保障法
ENISA	European Network and Information Security Agency 欧州ネットワーク情報セキュリティ庁
EPRI	Electric Power Research Institute 米国電力研究所
ERO	Electric Reliability Organization 電力信頼性機関
ESOs	European Standardisation Organizations 欧州規格作成機関
ESP	Electronic Security Perimeter 電力セキュリティ境界
ETSI	European Telecommunications Standards Institute 欧州電気通信標準化機構
EU	European Union 欧州連合

F:

FERC	Federal Energy Regulatory Commission 米国連邦エネルギー規制委員会
FISC	Center for Financial Industry Information Systems 金融情報システムセンター
FW (F/W)	Fire Wall ファイアーウォール

G:

GW	Gateway ゲートウェイ

H:

HAN	Home Area Network ホームエリアネットワーク
HEMS	Home Energy Management System 家庭内エネルギー管理システム

I:

ICEC	Instrument & Control Engineering Conference 計測制御技術会議
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team 米国　産業制御システムサイバー緊急対応チーム
ICT	Information Communicatin Technology 情報通信技術
IDS	Intrusion Detection System 侵入検知システム
IEC	International Electrotechnical Commission 国際電気標準会議
IEEE	Institute of Electrical and Electronics Engineers 米国電気電子学会
INL	Idaho National Laboratory アイダホ国立研究所
IPA	Information-technology Promotion Agency 情報処理推進機構
IPS	Intrusion Prevention System 侵入保護システム
ISA	International Society of Automation 国際計測制御学会
ISMS	Information Security Management System 情報セキュリティマネジメントシステム
ISP	Internet Service Provider インターネット・サービス・プロバイダー
IT	Information Technology 情報技術

J:

J-CSIP	Initiative for Cyber Security Information sharing Partnership of Japan サイバー情報共有イニシアティブ
JIPDEC	Japan Institute for Promotion of Digital Economy and Community 日本情報経済社会推進協会
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center JPCERT コーディネーションセンター
JSCA	Japan Smart Community Alliance 日本スマートコミュニティアライアンス
JVN	Japan Vulnerability Notes IPA の脆弱性対策情報ポータルサイト
JWG	Joint Working Group 連携ワーキンググループ

N:

NARUC	National Association of Regulatory Utility Commissioners 全米公益事業規制委員協会
NERC	North American Electric Reliability Council 北米電力信頼度協議会
NESCO	National Electric Sector Cybersecurity Organization 米国電力セクター・サイバーセキュリティー機構
NESCOR	National Electric Sector Cybersecurity Organization Resource 米国電力セクター・サイバーセキュリティー機構リソース
NIPP	National Infrastructure Protection Plan 国家インフラ防護計画
NISC	National Information Security Center 内閣官房情報セキュリティセンター
NIST	National Institute of Standards and Technology 国立標準技術研究所
NSTB	National SCADA Test Bed 米国監視制御システム試験ベッド
NVD	National Vulnerability Database 米 NIST の脆弱性データベース

O:

OE	Office of Electricity Delivery and Energy Reliability 電力信頼性局
OS	Operating System オペレーティングシステム
OSPs	Operator Security Plans EU 加盟国の運営者セキュリティ計画

R:

RISI	Repository of Industrial Security Incidents サイバーセキュリティインシデントのデータベース

S:

SCADA	Supervisory Control and Data Acquisition 監視制御システム
SG	Smart Grid スマートグリッド
SG-CG	Smart Grid Coordination Group スマートグリッド合同グループ
SGIP	Smart Grid Interoperability Panel スマートグリッド相互運用性パネル
SGIS	Smart Grid Information Security スマートグリッド情報セキュリティ
SGTF	Smart Grid Task Force スマートグリッド・タスクフォース
SM	Smart Meter スマートメーター
SLOs	Security Liaison Officers セキュリティ連絡役員
SQL	Structured Query Language データの定義や操作をするデータベース言語

U:

UCAIug	Utility Communication Architecture International Users Group 電力会社、機器ベンダ等の国際ユーザーグループ
USB	Universal Serial Bus 情報機器に周辺機器を接続するためのシリアルバス規格

V:

VRF	Violation Risk Factor
VSL	Violation Severity Level

W:

WIB	Working-party on Instrument Behaviour 欧州石油メジャーが中心の機器セキュリティ調達要件

付録１ 検討委員名簿

本事業では下記の委員からなる「次世代電力システムに関する電力保安調査委員会」を設立し、全 5 回の委員会を開催して検討を進めた。

（委員長）

新　誠一	電気通信大学　情報理工学研究科　教授

（委員長代理）

小林　偉昭	技術研究組合　制御システムセキュリティセンター 専務理事

（委員）

浦谷　嘉一	電気事業連合会　情報通信部　副部長
金野　千里	独立行政法人　情報処理推進機構　技術本部 セキュリティセンター 情報セキュリティ技術ラボラトリー　ラボラトリー長
真田　教志	NTT コミュニケーションズ株式会社　第三営業本部 営業推進部門　部長
新野　昭夫	GE 富士電機メーター株式会社　マーケット開発部 部長
芹澤　善積	一般財団法人　電力中央研究所　システム技術研究所 副所長
中野　利彦	株式会社日立製作所　インフラシステム社 制御セキュリティセンタ　センタ長
名和　利男	株式会社サイバーディフェンス研究所　情報分析部 理事
宮地　利雄	一般社団法人　JPCERT コーディネーションセンター 理事
吉松　健三	技術研究組合　制御システムセキュリティセンター 研究開発部

※敬称略、委員は五十音順、所属等は委員会開催時

付録 2 委員会開催実績

第 1 回
日時：平成 25 年 10 月 21 日 10:00 ~ 12:00
場所：株式会社日本総合研究所 13 階 131 会議室
議事：検討内容の確認、電力システムの構成とセキュリティ対策の概要
電力会社への確認事項

第 2 回
日時：平成 25 年 11 月 19 日 10:00 ~ 12:00
場所：株式会社日本総合研究所 13 階 131 会議室
議事：電力会社の電力システム構成とセキュリティ対策のヒアリング結果
電力システムの将来像

第 3 回
日時：平成 25 年 12 月 24 日 10:00 ~ 12:00
場所：株式会社日本総合研究所 13 階 131 会議室
議事：諸外国における電力インフラに対するサイバー攻撃の状況
最新のサイバー攻撃トレンドおよび対策の内容
米国の電力インフラサイバーセキュリティ規格・ガイドライン
日本における電力インフラに対する提言の方向性

第 4 回
日時：平成 26 年 1 月 23 日 10:00 ~ 12:00
場所：株式会社日本総合研究所 13 階 131 会議室
議事：電力会社のサイバーセキュリティに関するアンケート結果
他産業のサイバーセキュリティ対策（金融業界、情報通信業界）

第 5 回
日時：平成 26 年 2 月 13 日 10:00 ~ 12:00
場所：株式会社日本総合研究所 13 階 131 会議室
議事：報告書（案）審議

付録 3 諸外国のサイバーインシデント事例

図表付録 3-1　スマートメーターを対象としたサイバー攻撃事例

項目		詳細
発生年月		2009年（2012年4月に報告された）
発生場所		米国
インシデント種別	意図的／非意図的	意図的
	外部／内部	外部
脆弱性		不明
対象システム		スマートメーター
経緯・概要		攻撃者はインターネット上見つかったツールを利用し、メータ管理を横取りし、プログラムを変更することで電力消費記録設定を改ざんした。その深刻なセキュリティホールは米国InGuardians Incの調査により発見された。
影響		その会社のスマートメーターを配置した領域内同じようなインシデントは広がっていた。

図表付録 3-2　アクセス権限管理の不備によるサイバー攻撃未遂事件

項目		詳細
発生年月		2009年3月
発生場所		米テキサス州Energy Future Holdings社
インシデント種別	意図的／非意図的	意図的
	外部／内部	外部
脆弱性		アクセス権限管理プロセス
対象システム		業務システム
経緯・概要		Energy Future Holdings社の元社員であったDon Chul Shinは、解雇された当日、無効になる前のVPNアクセスを使い、重要データの消去及び自らのYahooアカウントへの無断共有を図ったことが露見し、当局に逮捕された。同社員がComnanche Peak原子炉の制御モデル設計を担当していたこと、及びVPN接続中にエンジニアリンググループに対して発電機の出力上昇による影響を確認していたことから、需給予測システムだけでなく、さらなるサイバー攻撃の可能性もあるとされた。
影響		需給予測システムに対するサイバー攻撃を意図していたが、未遂に終わる

図表付録 3-3　フィッシングメールを起点としたアクセス権限獲得

項目		詳細
発生年月		2007年4月
発生場所		米国（エネルギー会社：匿名）
インシデント種別	意図的／非意図的	意図的
	外部／内部	外部
脆弱性		Windows DNS（Domain Name System）
対象システム		会社システム経由でSCADAシステムへ
経緯・概要		攻撃者は当該企業に勤務する社員に福利厚生関連に偽造したEメールを送り、添付した.chmファイルを開くと、サーバーに感染し、Windows DNSの脆弱性を利用して攻撃者に対して当該社員のPCアクセス権限を獲得する。具体的には、社内NW内でランダムに生成したアカウントでのアクセスを複数回試行し、Primary Domain Controllerを管理下に置く。
影響		SCADAシステムにアクセス可能なPCも感染した状況で発見され、（未遂であったが）SCADAのコントロールも可能な状況であった。

図表付録 3-4　原発監視制御システムのワーム感染

項目		詳細
発生年月		2003年1月
発生場所		米国Davis-Besse原子力発電所
インシデント種別	意図的／非意図的	非意図的
	外部／内部	外部からのウイルス感染（SQL Slammerワーム　※類似事例が2003年前後に多数、発生）
脆弱性		外部接続用の回線管理、パッチ管理、要員管理
対象システム		原子力発電所の内部NW/サーバー、SPDS（Safety Parameter Display System）
経緯・概要		発電事業者（First Energy Nuclear社）のNWとDavis-Besse発電所の所内NWは様々なアクセス制御ポリシーを備えるF/Wを介して接続することができたが、通常はF/Wの1434 portを閉じた状態でなければ、UDPによるデータの送受信が制限される仕様となっていた。所内のサーバー上で動くアプリケーションを開発していたFEN社のSEが作業のためT1ラインと呼ばれる専用線を開通させたところ、上記のF/Wをバイパスしてしまい、接続したFEN社のサーバー経由でSQL Slammerワームが感染し、発電所内監視制御システムにおける1434 portを開いていた全てのサーバーにランダムにアクセスを繰り返し、大量の攻撃用パケットを撒き散らす事態となり、データオーバーロードを引き起こした。
影響		Davis-Besse原子力発電所の内部ネットワークでデータオーバーロードが生じ、その影響でSPDS（Safety Parameter Display System）が5時間、プロセスコンピュータが6時間停止した。（プラント制御・保護機能に影響がなかったので、甚大な被害にはならなかった）

図表付録 3-5　ウラン濃縮施設の遠心分離機の Stuxnet 感染

項目		詳細
発生年月		2010年11月
発生場所		イラン・ナタンツウラン原子力プラントの濃縮施設
インシデント種別	意図的／非意図的	意図的
	外部／内部	外部
脆弱性		a combination of vulnerabilities (一つの脆弱性だけではなく、様々なホール（Windows OS, Siemens PLCなど）を利用された結果)
対象システム		遠心分離機制御システムのSCADAシステム
経緯・概要		Stuxnet （Microsoft Windowsコンピュータワーム）はコンピュータ（PLCを制御するWinCC/PCS7（Siemens社製DCS）など）を乗っ取ったり、PLCに侵入したりした後、周波数を断続的に変化させるが、これに応じて遠心分離機の回転数も大幅に増減した。その結果、遠心分離機に過大な負担がかかり、破損に至った。
影響		ウラン濃縮施設の遠心分離機がコンピュウィルスに感染。約8,400台の遠心分離機がすべて停止した。

付録 4　諸外国のサイバーセキュリティガイドライン

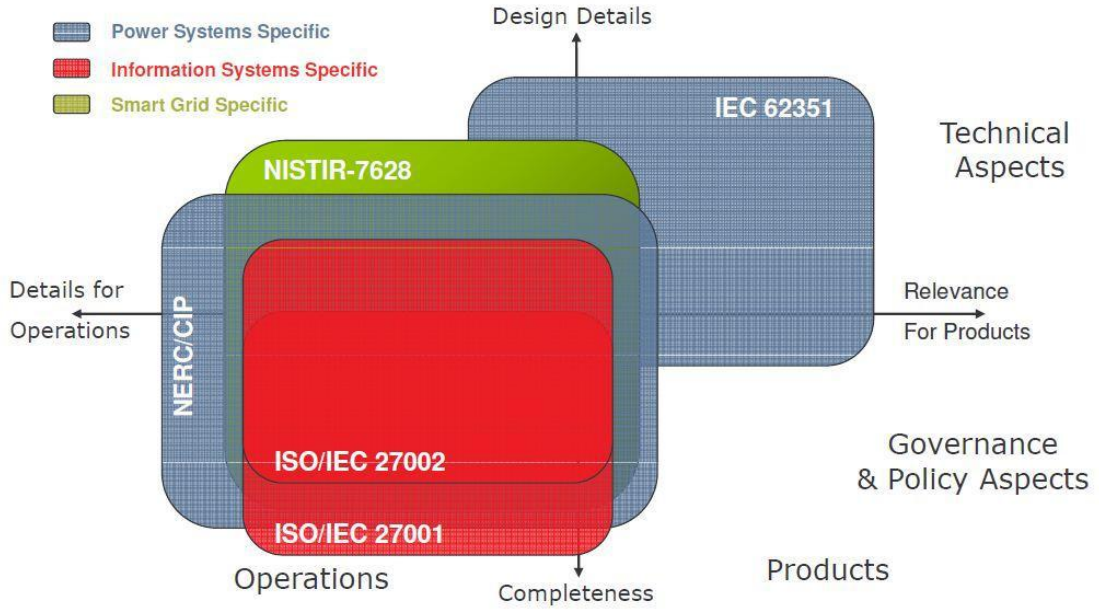
図表付録 4-1　諸外国のサイバーセキュリティガイドライン一覧

規格・ガイドライン	発行団体	出版年	国
CIP ver.3 001-2, 002-3～009-3(現行)／CIP ver.5 002-5～009-5, 010-1, 011-1(将来)	North American Electric Reliability Corporation (NERC)	2009 年／2013 年（更新中）	米国
Guidelines for Smart Grid Cyber Security Vol.1-3（NISTIR 7628）（2013 年　Revision1 のドラフトも参照）	National Institute of Standards and Technology (NIST)	2010 年（Rev.1 は 2014 年春にリリース予定）	米国
Guide to Industrial Control Systems (ICS) Security　(NIST SP 800-82, Revision 1)	NIST	2013 年 (Rev.2 は NIST SP 800-53, Rev.4 に対応し、2014 年春にリリース予定)	米国
Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53, Revision 4)	NIST	2013 年（更新中）	米国
ISO/IEC 27000-series (ISMS Family of Standards)	ISO/IEC	2009 年～（更新中）	国際
IEC62443 Industrial communication networks - Network and system security（以前の ISA99） 1-1～1-4(共通・全般), 2-1～2-4(管理・運用・プロセス), 3-1～3-3(技術・システム), 4-1～4-2(部品・デバイス)	The International Society of Automation (ISA)	作成中（2007 年～）	米国／国際
IEC62351 Power systems management and associated information exchange – Data and communications security, Parts 1-8 (Parts 9-11 も)	International Electrotechnical Commission (IEC)	2007 年（更新中）	国際
ISO/IEC 15408 Information technology – Security techniques - Evaluation criteria for IT security	International Organization for Standardization (ISO)/IEC	2009 年～（更新中）	国際
Catalog of Control Systems Security: Recommendations for Standards Developers	U.S. Department of Homeland Security (DHS)	2011 年	米国
Cyber Security Procurement Language for Control Systems	DHS	2008 年	米国

System Protection Profile – Industrial Control Systems	NIST	2004 年	米国
Process control and SCADA security - Good practice guidelines	Centre for the Protection of National Infrastructure (CPNI)	2008 年 日本語版もあり	英国
21 steps to Improve Cyber Security of SCADA Networks	U.S. Department of Energy (DOE)	2002 年	米国
IEEE 1686-2007, IEEE Standard for Substation Intelligent Electronic Devices (IED) Cyber Security Capabilities	Institute of Electrical and Electronics Engineers (IEEE)	2007 年	国際
Security Profile for Advanced Metering Infrastructure, Version 2.1	Advanced Security Acceleration Project (ASAP)	2012 年	米国
UtilityAMI 2008 Home Area Network System Requirements Specification	UCA International Users Group	2008 年	米国
AMI System Security Requirements	ASAP	2008 年	米国

各ガイドラインの位置付けは下表のとおり。

図表付録 4-2　スマートグリッド情報セキュリティ



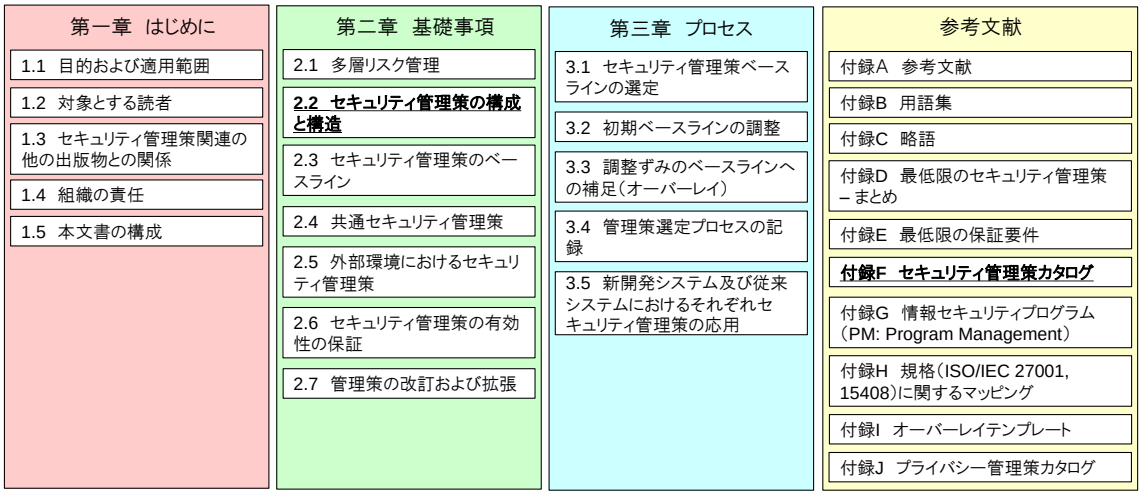
出所：CEN-CENELEC-ETSI SGCG「Smart Grid Information Security」

付録 5 米国の電力システムのサイバーセキュリティに関する主要ガイドライン
(1)NIST

1) NIST SP 800-53 Rev.4

NIST-SP 800-53 ではアメリカ政府のコンピュータシステムのための運営管理上及び技術上の管理策の構成と構造について詳しく述べている。また、ベースラインの選定から管理策(18 の種類)の応用までの実践プロセスを明示する。

図表付録 5-1 NIST SP 800-53 Rev.4 概要



図表付録 5-2 NIST SP 800-53 におけるセキュリティ管理策分類

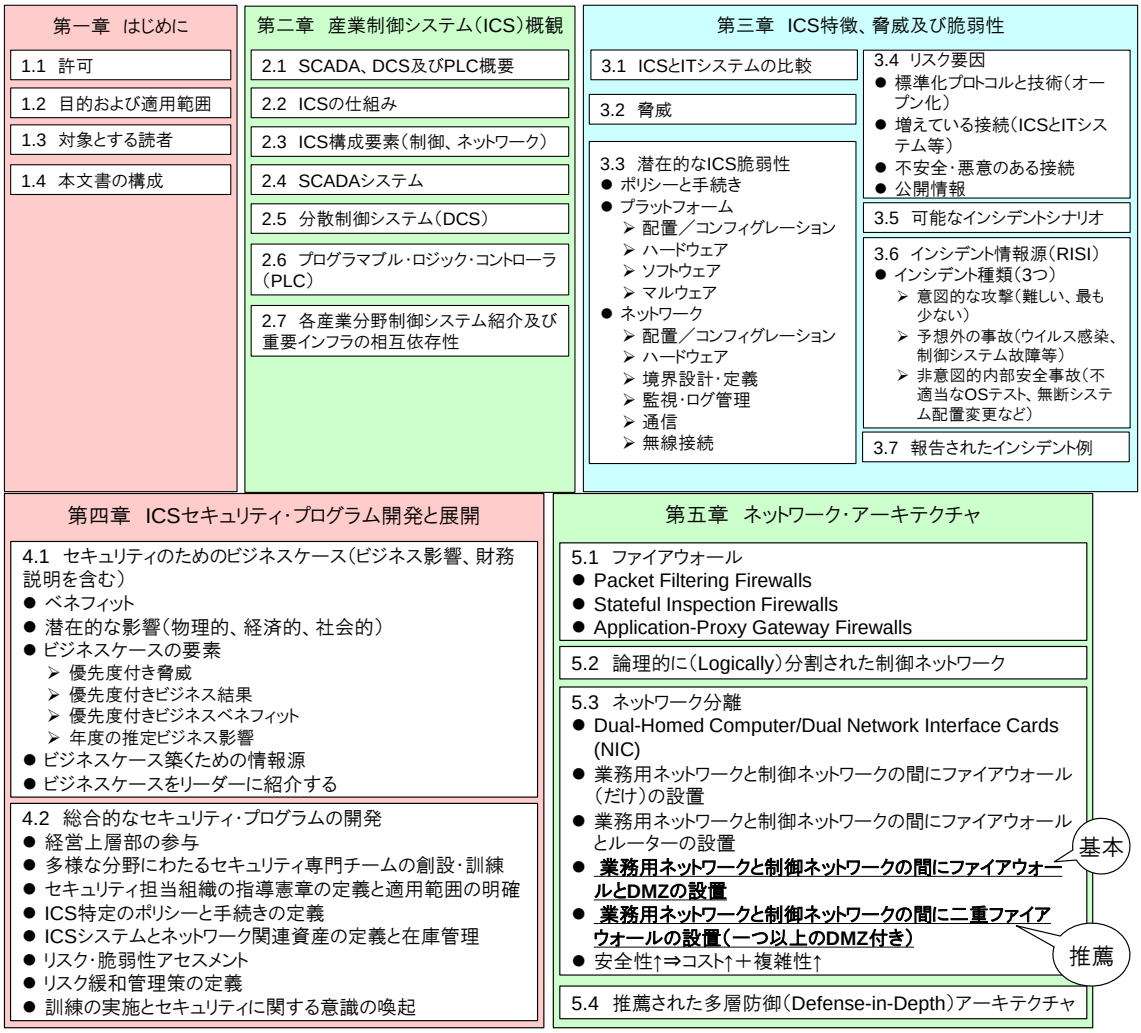
管理策分類	略語	説明
アクセス制御 (Access Control)	AC	The process of granting or denying specific requests for obtaining and using information and related information processing services for physical access to areas within the information system environment.
意識向上およびトレーニング (Awareness and Training)	AT	Policies and procedures to ensure that all information system users are given appropriate security training relative to their usage of the system and that accurate training records are maintained.
監査および責任追跡性 (Audit and Accountability)	AU	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
セキュリティ評価と運用認可・承認 (Security Assessment and Authorization)	CA	Assurance that the specified controls are implemented correctly, operating as intended, and producing the desired outcome.
構成管理 (Configuration Management)	CM	Policies and procedures for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system

		implementation.
緊急時対応計画 （Contingency Planning）	CP	Policies and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.
識別および認証 （Identification and Authentication）	IA	The process of verifying the identity of a user, process, or device, through the use of specific credentials (e.g., passwords, tokens, biometrics), as a prerequisite for granting access to resources in an IT system.
インシデント対応 （Incident Response）	IR	Policies and procedures pertaining to incident response training, testing, handling, monitoring, reporting, and support services.
保守 （Maintenance）	MA	Policies and procedures to manage all maintenance aspects of an information system.
記録媒体の保護 （Media Protection）	MP	Policies and procedures to ensure secure handling of media. Controls cover access, labeling, storage, transport, sanitization, destruction, and disposal.
物理的および環境的な保護 （Physical and Environmental Protection）	PE	Policies and procedures addressing physical, transmission, and display access control as well as environmental controls for conditioning (e.g., temperature, humidity) and emergency provisions (e.g., shutdown, power, lighting, fire protection).
計画 （Planning）	PL	Development and maintenance of a plan to address information system security by performing assessments, specifying and implementing security controls, assigning security levels, and responding to incidents.
人的セキュリティ （Personnel Security）	PS	Policies and procedures for personnel position categorization, screening, transfer, penalty, and termination; also addresses third-party personnel security.
リスクアセスメント （Risk Assessment）	RA	The process of identifying risks to operations, assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact.
システムおよびサービスの調達 （System and Services Acquisition）	SA	Allocation of resources for information system security to be maintained throughout the systems life cycle and the development of acquisition policies based on risk assessment results including requirements, design criteria, test procedures, and associated documentation.
システムおよび通信の保護 （System and Communications Protection）	SC	Mechanisms for protecting both system and data transmission components.
システムおよび情報の完全性 （System and Information Integrity）	SI	Policies and procedures to protect information systems and their data from design flaws and data modification using functionality verification, data integrity checking, intrusion detection, malicious code detection, and security alert and advisory controls
プログラム・マネジメント （Program Management）	PM	Provides security controls at the organizational rather than the information-system level.

2）NIST SP 800-82 Rev.1

NIST SP 800-82 では、産業制御システム（ICS）の特徴を考慮したガイドラインを示している。このガイド文書には必須の要件や監査は含まれていないが、制御システムに特化した唯一のアメリカ政府の公式文書である。

図表付録 5-3　NIST SP 800-82 Rev.1 概要（1）



NIST SP 800-82 では、ICS が直面している脅威や脆弱性などのリスク要素は詳しく分析される。また、技術的な対策だけではなく、ビジネス現場に近い管理・運営面に係る対策・考え方も多く紹介している。さらに、ICS セキュリティの重要な一環としたネットワーク構造と対策について詳しく分析する。

図表付録 5-4　NIST SP 800-82 Rev.1 概要（2）

※ICSセキュリティ管理策の名称はNIST SP 800-53のITセキュリティ管理策と対応している

NIST SP 800-53 と同じく、NIST SP 800-82 は、アクセス制限、不法利用防犯やシステム回復等五つの目標を目指し、ICS に特化した 18 種類のセキュリティ管理策を提案している。

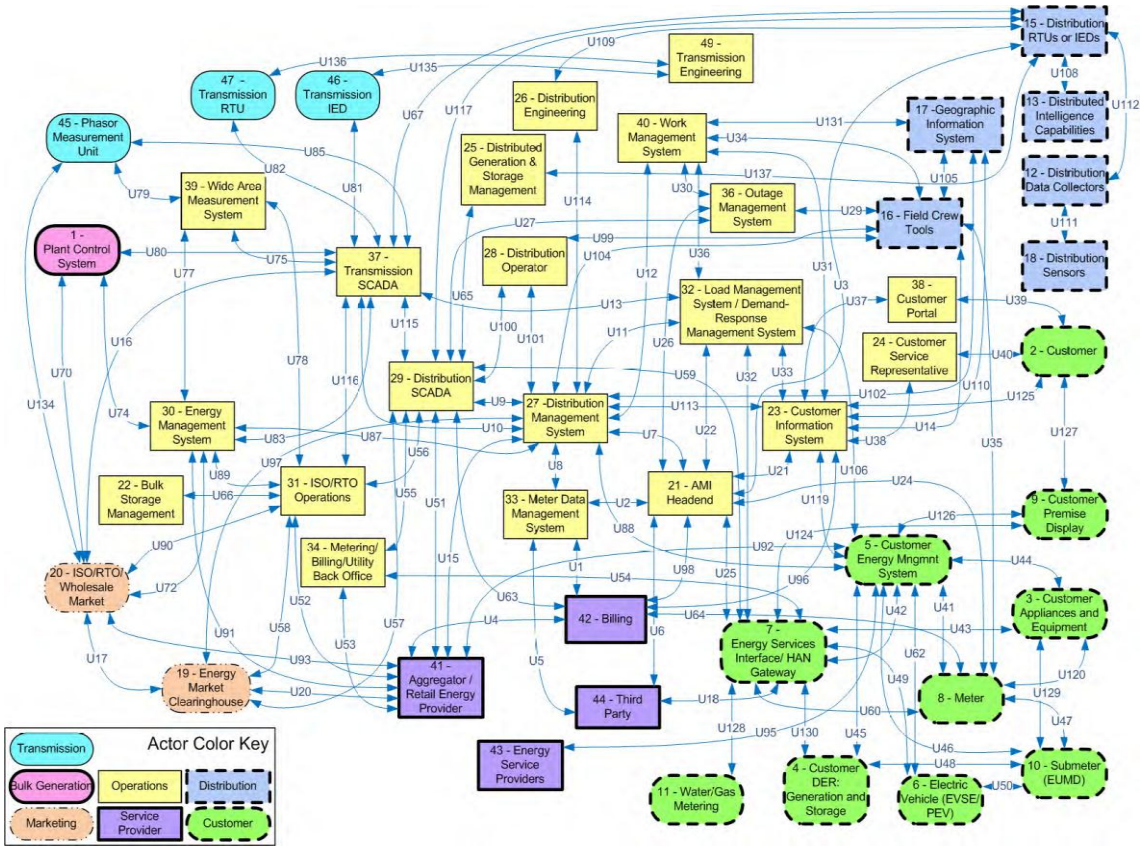
図表付録 5-5　ICS セキュリティ管理策実行の目標

目標	具体対策
ICSネットワークへの**ロジカルアクセスとネットワーク活動**の制限	• **ファイアウォール付きDMZネットワークアーキテクチャの構築** • **ICSは多層ネットワーク・トポロジー利用すべき**
ICSネットワークと設備への**物理的なアクセス**の制限	• **物理的なアクセス・コントロール（ロック、カード認証、警備など）の組み合わせは利用すべき**
個別ICSコンポーネントの**不法利用**の防犯	• セキュリティ・パッチの配置 • 利用されていないポートとサービスを無効にする • ICSユーザーの権限の制限 • 監査証跡の追跡と監視 • アンチウィルスソフトやファイル整合性チェック・ソフトなどのようなセキュリティ要件を使う
悪条件下の機能維持	• 各重要コンポーネントが冗長カウンターパートを持つことを確保する • 一つのコンポーネントは問題になっても、ICSや他のネットワークで無用なトラヒックの発生したり、どこか他の問題を引き起こしたり（連鎖イベントなど）をしないようにする
インシデント後のシステム回復	• インシデント対応プラン（インシデント発生後システムが速やかに回復できることを確保する）

3）NISTIR 7628

NIST IR 7628 では、論理インターフェースを具体的に定義することによって、リスク評価及び対策を明確化している。

図表付録 5-6　論理参照モデルの開発－アクター間の論理参照モデル



図表付録 5-7　論理参照モデルの開発－論理インターフェース分類（22 種類）

No.	論理インターフェース分類	例
1	制御システムと**高可用性**、また**計算能力と帯域幅**の両方、またはいずれか一方で**制限がある**設備の間のインターフェース	• Between transmission SCADA (Supervisory Control and Data Acquisition) and substation equipment • Between distribution SCADA and high priority substation and pole-top equipment • Between SCADA and distributed control system (DCS) within a power plant
2	制御システムと**非高可用性**だが、**計算能力と帯域幅**の両方、またはいずれか一方**上制限がある**設備の間のインターフェース	• Between distribution SCADA and lower priority pole-top equipment • Between pole-top IEDs (Intelligent Electronic Device) and other pole-top IEDs
3	制御システムと**高可用性**、また**計算能力や帯域幅上制限がない**設備の間のインターフェース	• Between transmission SCADA and substation automation systems
4	制御システムと**非高可用性**、また**計算能力や帯域幅上制限もない**設備の間のインターフェース	• Between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs
5	**同じ組織内部**の制御システムの間のインターフェース	• Multiple data management systems (DMS) belonging to the same utility

		• Between subsystems within DCS and ancillary control systems within a power plant
6	**別の組織**の制御システムの間のインターフェース	• Between an RTO (Regional Transmission Operator)/ISO (Independent System Operator) EMS (Energy Management System) and a utility energy management system • Between a Generation and Transmission (G&T) SCADA and a distribution CO-OP SCADA; • Between a transmission EMS and a distribution DMS in different utilities; • Between an EMS/SCADA and a power plant DCS.
7	共通管理機関下の**事務系システム**の間のインターフェース	• Between a Customer Information System (CIS) and a Meter Data Management System (MDMS)
8	違う管理機関下の**事務系システム**の間のインターフェース	• Between a third-party billing system and a utility MDMS
9	B2B 関係で繋がっている**金融やマーケットのシステム**の間のインターフェース	• Between a Retail aggregator and an Energy Clearinghouse
10	**制御システム**と**非制御／事務系システム**の間のインターフェース	• Between a Work Management System (WMS) and a Geographic Information System (GIS) • Between a DMS and a CIS; • Between anOMS and the advanced metering infrastructure (AMI) headend system • Between an outage management system (OMS) and a work management system (WMS).
11	環境パラメータを測定するための**センサーとセンサーネットワーク**（普通はアナログ測定器付き簡単なセンサーデバイス）の間のインターフェース	• Between a temperature sensor on a transformer and its receiver
12	**センサーネットワーク**と**制御システム**の間のインターフェース	• Between a sensor receiver and the substation master
13	**AMI ネットワークを利用するシステム**の間のインターフェース	• Between MDMS and meters • Between LMS (Load Management System)/DRMS and Customer EMS
14	**可用性の高い AMI ネットワークを利用するシステム**の間のインターフェース	• Between MDMS and meters • Between LMS/DRMS (Distribution Resource Management System) and Customer DER • Between DMS Applications and Customer DER (Distributed Energy Resource) • Between DMS Applications and distribution automation (DA) Field Equipment
15	HAN(Home Area Network)、BAN (Building Area Network)や NAN (Neighborhood Area Network)などの**顧客側のネットワークを利用するシステム**の間のインターフェース	• Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER equipment • Between Energy Service Interface (ESI) and PEVs (Plug-in Electric Vehicle)
16	**外部システムと顧客側**の間に	• Between Third Party and HAN Gateway • Between energy service provider (ESP) and DER

		• Between Customer and CIS Web site
17	**システムと現地スタッフのノートパソコン／設備**の間のインターフェース	• Between field crews and GIS • Between field crews and substation equipment • Between field crews and CIS; • Between field crews and OMS; • Between field crews and WMS; • Between field crews and corporate marketing systems
18	**測定装置の間**のインターフェース	• Between sub-meter to meter • Between PEV meter and Energy Service Provider (ESP) • Between MDMS and meters (via the AMI headend); • Between customer EMS and meters; • Between field crew tools and meters; • Between customer DER and submeters; • Between electric vehicles and submeters.
19	**運営決定サポートシステム**の間のインターフェース	• Between wide area measurement system (WAMS) and ISO/RTO
20	**エンジニア／保守システムと制御設備**の間のインターフェース	• Between engineering and substation relaying equipment for relay settings • Between engineering and pole-top equipment for maintenance • Within power plants
21	保守およびサービスのための**制御システム**とそのシステムを構築する**ベンダ**の間のインターフェース	• Between SCADA system and its vendor
22	セキュリティ／ネットワーク／システム管理操作台と全てのネットワーク及びシステムの間のインターフェース	• Between a security console and network routers, firewalls, computer systems, and network nodes(**論理参照モデルには含まれない**)

各インターフェース分類に対応する CI&A（機密性、完全性、可用性）レベルは下表で示すとおりである。

図表付録 5-8　論理インターフェース分類別の CIA 影響レベル

論理I/F分類	C:機密性	I:完全性	A:可用性
1	低	高	高
2	低	高	中
3	低	高	高
4	低	高	中
5	低	高	高
6	低	高	中
7	高	中	低
8	高	中	低
9	低	中	中
10	低	高	中
11	低	中	中
12	低	中	中
13	高	高	低
14	高	高	高
15	低	中	中
16	高	中	低
17	低	高	中
18	低	高	低
19	低	高	中
20	低	高	中
21	低	高	低
22	高	高	高

(2)NERC CIP Ver.5 のセキュリティ要件と基準例

NERC CIP Ver.5 の 10 の標準の中に、CIP 004-5 から CIP 011-5 までには重要サイバー資産保安について具体的な対策が提言されている。

CIP-004-5:Cyber Security ― Personnel & Training		
R1 サイバーセキュリティ・トレーニングプログラム		
適用システム	**要件**	**基準例**
・高度の影響のある BES サイバーシステム ・中度の影響のある BES サイバーシステム	BES サイバーシステムにアクセスする社員に対するサイバーセキュリティ研修・啓発の**四半期**に 1 回の開催	**四半期**に 1 回の研修・啓発の開催を示す文書
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS ・ルーティング対応した外部接続を伴う中度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS	**以下の項目を含む研修の実施:** ・サイバーセキュリティ方針 ・物理的アクセス制御 ・電子アクセス制御 ・来訪者制御プログラム ・BES サイバーシステム情報の取り扱いと保管 ・サイバーセキュリティインシデントと対応計画 ・BES サイバーシステムの復旧計画 ・サイバーセキュリティインシデントへの反応 ・サイバーセキュリティリスク	研修教材
	電子アクセスや物理的アクセスの許可前の研修の実施	研修記録
	15 ヶ月に 1 回の研修の実施	個々人の研修記録
R2 個人リスクアセスメントプログラム		
適用システム	**要件**	**基準例**
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS ・ルーティング対応した外部接続を伴う中度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS	ID 確認プロセス	ID 確認プロセスに関する文書
	個人リスク評価として**過去 7 年間の犯罪歴**を確認するプロセス	個人リスク評価として**過去 7 年間の犯罪履歴**を確認するプロセスに関する文書
	アクセス許可のための**犯罪歴評価の基準**やプロセス	アクセス許可のための**犯罪歴評価の基準**やプロセスに関する文書
	契約者やサービスベンダの社員のリスク評価の認証に関する基準やプロセス	契約者やサービスベンダの社員のリスク評価の認証に

		関する基準やプロセスを定めた文書
	アクセス許可を有する個人のリスク評価を保障するプロセス	アクセス許可を有する個人のリスク評価を保障するプロセスに関する文書
R3 接続マネジメントプログラム		
適用システム	**要件**	**基準例**
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS ・ルーティング対応した外部接続を伴う中度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS	電子アクセス、物理的アクセス、BES サイバーシステム情報の指定保管場所へのアクセスに関する許可プロセス	電子アクセスや物理的アクセス、BES サイバーシステム情報の指定保管場所へのアクセスに関する文書
	電子アクセスと物理的アクセス許可を有する人物の四半期ごとの認証	アクセス者リストとアクセス権保有者の認証
	電子アクセスに関して **15 ヶ月**ごとに、①ユーザーアカウント、②アカウントグループ、③役割分類、④権限、の各項目が正しいあるいは必要性が認められることを認証	アカウントリスト、グループや役割ごとの権限、アカウント設定、設定の正しさと必要性の確認、を記載した文書
	BES サイバーシステム情報の指定保存場所へのアクセスが正しく、事業者の決定が適切であったことの認証	BES サイバーシステム情報の許可リスト、権限付与、事業者の決定が適切であったことの認証に関する文書、を含むレビュー文書
R4 接続取り消し		
適用システム	**要件**	**基準例**
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS ・ルーティング対応した外部接続を伴う中度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS	物理的アクセスや相互遠隔アクセス権の剥奪プロセスと **24 時間**以内の権限剥奪の実行プロセス	・権限剥奪認証の業務フロー又はサインオフフォーム ・権限剥奪者のアクセス不能を示すログ又は証拠
	退職や異動に伴い個人のアクセスが不要になる場合の個人アカウントへの電子アクセス権と物理的アクセスの**翌日中**の剥奪	・理論的かつ物理的アクセスのレビューを示す業務フロー又はサインオンフォーム ・個人がアクセスできないことを示すログなどの証拠
	期間満了に伴う BES サイバーシステム情報の指定保管場所への個人アクセス権剥奪の**翌日中**の実施	指定場所への物理的アクセス権又は BES サイバーシステム情報を含むサイバーシステムへのアクセス権が**翌日中**に剥奪されたことを示す書類
・高度の影響のある BES サイバーシステムとそれ	期間満了に伴う個人の非共有ユーザーアカウントの剥奪の **30 日**以内の実施	**30 日**以内にアクセス権剥奪が実行されたことを示す業

に関連する EACMS		務フロー又はサインオフフォーム
	期間満了や退職・異動に伴うユーザーに知られている共有アカウントのパスワード変更の 30 日以内の実施	期間満了や退職・異動から 30 日以内にパスワードのリセットが実施されたことを示す業務フロー又はサインオフフォーム

CIP-005-5：Cyber Security ― Electronic Security Perimeter(s)

R1 電気的セキュリティ境界

適用システム	要件	基準例
・高度の影響のある BES サイバーシステムとそれに関連する PCA ・中度の影響のある BES サイバーシステムとそれに関連する PCA	ルーティング対応プロトコル経由でネットワークにつながっているすべての適用可能なサイバー資産の限定された ESP での管理	ルーティング対応プロトコル経由でつながっている適用可能なサイバー資産を特定したすべての ESP リスト
・高度の影響のある BES サイバーシステムとそれに関連する PCA ・ルーティング対応した外部接続を伴う中度の影響のある BES サイバーシステムとそれに関連する PCA	ルーティング対応したすべての外部接続の特定された EAP を通した接続	ルーティング対応したすべての外部通信経路と特定の EAP に関する図表
・高度の影響のある BES サイバーシステムのための EAP ・中度の影響のある BES サイバーシステムのための EAP	上り・下り接続許可要求とその他の接続の拒絶	許可された接続のみ認証されたり各々の接続ルールの理由が明文化されていることが示されたルールリスト（ファイアーウォール、接続制御リスト）
・ダイアルアップ接続を伴う高度の影響のある BES サイバーシステムとそれに関連する PCA ・ダイアルアップ接続を伴う中度の影響のある BES サイバーシステムとそれに関連する PCA	適用可能なサイバー資産とのダイヤルアップ接続時の技術的合理性の証明	事業者がどのように各々のダイヤルアップ接続の接続証明を与えているかを記載した文章
・高度の影響のある BES サイバーシステムのための EAP ・コントロールセンターに	上り・下り接続の悪意のある通信を検出するための 1 つ以上の手法の保有	悪意のある通信検出手法（侵入探知システム、アプリケーションレイヤーファイヤーウォール）を記した文章

おける中度の影響のある BES サイバーシステムのための EAP		
R2 相互遠隔接続マネジメント		
適用システム	**要件**	**基準例**
・高度の影響のある BES サイバーシステムとそれに関連する PCA ・ルーティング対応した外部接続を伴う中度の影響のある BES サイバーシステムとそれに関連する PCA	相互遠隔接続を行うサイバー資産が直接的せつなサイバー資産に接続しないような相互システムの運用	ネットワーク図又は設計文書
	すべての相互遠隔接続セッションに対して、暗号化の実施	暗号化の開始・終了場所の詳細を記した設計文書
	すべての相互遠隔接続セッションに対するマルチファクター証明の要求	証明要素の詳細(パスワード・PINs、トークン・デジタル認証・スマートカード、指紋認証・虹彩スキャン・その他生態認証)を記した設計文書
CIP-006-5：Cyber Security ― Physical Security of BES Cyber Systems		
R1 物理的セキュリティ計画		
適用システム	**要件**	**基準例**
・ルーティング対応した外部接続を伴う中度の影響のある BES サイバーシステム ・PACS とそれに関連する高度の影響のある BES サイバーシステム又はルーティング対応した外部接続を伴う中度の影響のある BES サイバーシステム	物理的アクセス制限の運用規則又は手続き規則の定義	運用規則又は手続き規則が記された文書
ルーティング対応した外部接続を伴う中度の影響のある BES サイバーシステムとそれに関連する EACMS と PCA	物理的アクセス許可を持つ個人にだけ適用可能な物理的セキュリティ境界への物理的アクセスを許可する規則の運用	・物理的セキュリティ境界と物理的アクセスが 1 つ以上の手法によって管理されているということが記載された物理的セキュリティ計画 ・物理的アクセスが許可された人物にだけに制限されていることを証明できる文書
高度の影響のある BES サイバーシステムとそれに関連する EACMS と	物理的セキュリティ境界内への物理的アクセスを許可された個人にだけ許容することを 2 つ以上の管理での実現	・物理的セキュリティ境界と物理的アクセスが 1 つ以上の手法によって管理されて

PCA		**いるということが記載された物理的セキュリティ計画** ・物理的アクセスが許可された人物にだけに制限されていることを証明できる文書
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PCA ・ルーティング対応した外部接続を伴う中度の影響のある BES サイバーシステムとそれに関連する EACMS と PCA	物理的セキュリティ境界内への許可されない物理的アクセスの監視	物理的セキュリティ境界内への許可されない物理的アクセスの監視の制御を記した文書
	物理的セキュリティ境界内への許可されない物理的アクセスの探知に対する **15 分以内**のアラームやアラートの発信	・物理的セキュリティ境界内への許可されない物理的アクセスの探知に対してアラームやアラートを発信することを記した物理的セキュリティ計画 ・BES サイバーセキュリティインシデント対応プランで特定したようにアラームやアラートが発信したことを示す証拠
PACS とそれに関連する高度の影響のある BES サイバーシステム又はルーティング対応した外部接続を伴う中度の影響のある BES サイバーシステム	物理的アクセス制御システムの監視	PACS への許可されない物理的アクセス監視を記した文書
	物理的アクセス制御システムへの許可されない物理的アクセスの探知に対する **15 分以内**のアラームやアラート発信	・物理的アクセス制御システムへの許可されない物理的アクセスの探知に対してアラームやアラートを発信することを記した物理的セキュリティ計画 ・BES サイバーセキュリティインシデント対応プランで特定したようにアラームやアラートが発信したことを示す証拠
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PCA ・ルーティング対応した外部接続を伴う中度の影響のある BES サイバーシステムとそれに関連する EACMS と PCA	物理的セキュリティ境界内への物理的アクセスを許可された人物の入室記録	・物理的セキュリティ境界内への物理的入室に関する記録を定めた物理的セキュリティ計画 ・物理的セキュリティ境界内への入室者や入室日時などを記した記録
	物理的アクセスに関する記録の **90 日間**の保存	物理的セキュリティ境界内への入室者や入室日時などを記した記録
R2 外部者制御プログラム		

適用システム	要件	基準例
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PCA ・ルーティング対応した外部接続を伴う中度の影響のある BES サイバーシステムとそれに関連する EACMS と PCA	物理的セキュリティ境界内への来訪者の入室時のアクセス許可を受けた社員の同伴	・来訪者の物理的セキュリティ境界内への入室時は許可を受けた社員との同伴を定めた来訪者管理プログラム ・来訪者記録など実行プロセスなどを記した文書
	来訪者の物理的セキュリティ境界内への入退室記録（日時、氏名、来訪目的を含む）やマニュアル	・来訪者の物理的セキュリティ境界内への入室時は許可を受けた社員との同伴を定めた来訪者管理プログラム ・来訪者記録など実行プロセスなどを記した文書
	来訪者に関する記録の **90 日間**の保存	少なくとも **90 日間**保持されている記録
R3 物理的接続制御システムメンテナンスおよびテストプログラム		
適用システム	**要件**	**基準例**
・PACS とそれに関連する高度の影響のある BES サイバーシステムとルーティング対応した外部接続を伴う中度の影響のある BES サイバーシステム ・物理的境界に設置したハードウェアとデバイスとそれに関連する高度の影響のある BES サイバーシステムとルーティング対応した外部接続を伴う中度の影響のある BES サイバーシステム	物理的アクセス制御システムの訓練と維持と物理的セキュリティ境界に設置されたハードウェアやデバイスの **24 ヵ月**ごとの動作確認	物理的アクセス制御システムの訓練と維持および物理的セキュリティ境界に設置されたハードウェアやデバイスの **24 ヵ月**ごとの動作確認を記したプログラムと訓練・メンテナンス記録
CIP-007-5：Cyber Security ― System Security Management		
R1 接続ポートとサービス		
適用システム	**要件**	**基準例**
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA ・ルーティング対応した外部接続を伴う中度の影響のある BES サイバ	技術的に実行可能で有効な論理ネットワークにアクセスするポートを決定することが事業者に求められる。 動的ポートを扱うために必要となるポート範囲やサービスを決定することも含まれる。	・適用される全サイバー資産やアクセスポイント上の全ての有効なポートに関する書類が求められる ・サイバー資産上の応答ポート一覧例

ーシステムとそれに関連する EACMS と PACS と PCA	論理ポートを無効にしたり、制限したりする設備を持たない機器の場合、これらのポートはオープンとみなされ、そういった設備が必要となる。	- 機器環境設定ファイル -（設定）出力コマンド　例：netstat - オープンポートのネットワークスキャン、他 **・ホスト型 FW（ソフトウェアとしての FW）や、特定ポートだけを接続し、他は接続拒否するアプライアンス（ネットワーク型 FW に相当）の環境設定ファイル**
・高度の影響のある BES サイバーシステム ・コントロールセンターにおける中度の影響のある BES サイバーシステム	ネットワーク接続や操作卓、可搬媒体に使われている物理的入出力ポートの不必要な使用に対する保護	**物理的入出力ポートの保護の種類を示す書類** **-システム構成による論理的な保護** **-ポートロックや警告表示といった物理的な保護**
R2　セキュリティパッチ管理		
適用システム	**要件**	**基準例**
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA ・中度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA	適用されるサイバー資産へのパッチ管理プロセス（監視、評価、導入）	BES サイバーシステム、又はサイバー資産基盤毎の ・パッチ管理プロセスに関する書類 ・監視対象書類、一覧
	2.1 で定義された監視対象を最後に評価してから最低 **35 日以内**に、リリースされたセキュリティパッチの妥当性について評価する	書類上の監視対象向けに公開されたセキュリティパッチの事業者に代わって、**35 日毎**に、評価を実施、委託する
	2.2 で定義された適用可能なパッチは、**35 日以内**に評価を完了し、以下を行う -パッチの適用 -最新の緩和計画の立案 -既存の緩和計画の更新 緩和計画には、セキュリティパッチや緩和を完了するまでの時間といった脆弱性の緩和に対処するための事業者による計画された行動を含む	**・パッチ設定の記録** - パッチ設定日、ソフトウェアのバージョン、ソフトウェア登録日等についての自動パッチ管理ツールの情報） **・いつ、どのように脆弱性に対処したかを示す計画** -事業者が実行したセキュリティパッチや緩和を完了するまでの時間といった脆弱性緩和に対する行動記録
	・シニアマネージャーか権限を委譲されたものによって 2.3 で立案・更新した緩和計画について、計画で示された時間内に実行される	緩和実施記録

	・2.3 で示した計画が更新されたり、時間枠が拡張された場合は、シニアマネージャー又は権限を委譲された者に承認されている	
R3 悪意のあるプログラムからの保護		
適用システム	**要件**	**基準例**
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS ・中度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS	悪意のあるプログラムを阻止、検知、防止するための方法を展開する	**事業者によるこれらのプロセスの実行記録** - アンチウィルス - システム強化 - 方針、等
	検知した悪意のあるプログラムの脅威を緩和する	・悪意のあるプログラムを検知するプロセスの反応記録 ・悪意のあるプログラムを検知した時のこれらのプロセスの実行記録
	・3.1 で定義した(ウイルスの)シグネチャやパターンを使用する方法は、それらの更新するプロセスを持つ ・プロセスではシグネチャやパターンを試験、設定しなければならない	**シグネチャやパターンの更新を使っているプロセスを示す書類**
R4 セキュリティイベント監視		
適用システム	**要件**	**基準例**
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA ・中度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA	・サイバーセキュリティインシデントの同定と事後調査のために、BES サイバーシステムレベル、又はサイバー資産レベル(サイバー資産機能毎)のイベントを記録する ・最低限以下のイベントを記録する -成功したログイン攻撃の検知 -失敗したアクセス攻撃や失敗したログイン攻撃の検知 -悪意のあるプログラムの検知	・BES サイバーシステムが検知することの出来るイベントや、出力イベントをログとして残るように設定されたシステムが出力するリスト、又は紙 ・リストには、求められているイベント種類が含まれていなければならない
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA ・ルーティング対応した外部接続を伴う中度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA	・事業者が警告を必要と決めたセキュリティイベントに対する警告出力 ・最低限以下のイベントに対する(サイバー資産又は BES サイバーセキュリティシステム機能毎に)警告 -4.1 に示した悪意のあるプログラムの検知に対して -4.1 に示した失敗イベントログの検知に対して	・事業者が警告を必要と決めたセキュリティイベントをシステムから出力したリスト、又は紙 ・警告がどのように設定されているかを示すリスト
	技術的に実現可能な場合は、4.1 で示された適用されるイベントログを(CIP の例外的	・イベントログの保持プロセスの書類

	な慣習を除いた）連続 **90 日間**保持する	・**90 日以上**のログ保持設定記録の紙、又はシステム出力
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PCA	サイバーセキュリティインシデントが検知されていないと確認されてから **15 日以内**に、記録されたイベントの要約やサンプルの再調査を事業者が決定している	・再調査を記述した書類 ・再調査で発見した事象 ・再調査を行った日付
R5 システムアクセス制御		
適用システム	**要件**	**基準例**
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA ・コントロールセンターにおける中度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA ・ルーティング対応した外部接続を伴う中度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA	技術的に実行可能な場合、利用者の相互アクセスの認証実行方法	**どのようなアクセスが認証されるかを示した書類**
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA ・中度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA	全ての把握している使用可能なデフォルト又は他の初期アカウントの種類を特定し、目録を作る -システム毎 -システム群毎 -場所毎 -システム種類毎	BES サイバーシステムで使われる利用可能又は初期アカウントを示すアカウント種類別のアカウントリスト
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA ・ルーティング対応した外部接続を伴う中度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA	共有アカウントにアクセスする権限を持った個人の特定	・共有アカウントリスト ・共有アカウントにアクセス権限を持つ個人のリスト
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と	サイバー資産機能毎に把握している初期パスワードの変更	・新しく稼働させた機器のパスワード変更手順 ・システムマニュアルの書類

PACS と PCA ・中度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA		・疑似ランダム生成され、機器毎にユニークな初期ベンダパスワードを示したベンダ書類
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA ・ルーティング対応した外部接続を伴う中度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA	利用者相互アクセスがパスワード認証のみの場合の、技術的・手続き的なパスワード設定値の強制 ・パスワード長さ **8文字**より小さいか、サイバー資産が提供する最大長さ ・最低限のパスワード複雑さ **3 つ未満**の文字種類（大文字、小文字、数字、アルファベット以外）か、サイバー資産が提供する最大複雑さ	システムが強制する長さや複雑さといったパスワード設定値のシステム出力レポート、又はシステムスクリーン表示
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA ・コントロールセンターにおける中度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA	技術的に実現可能な場合、利用者相互アクセスがパスワード認証のみの場合の、技術的・手続き的なパスワード変更や少なくとも**15 か月に 1 回**のパスワード変更義務の強制	・パスワード変更をシステムが強制する周期性に関するシステム出力レポート、又はシステムスクリーン表示 ・手続きに従うことが記された書類を参照する証明
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA ・ルーティング対応した外部接続を伴う中度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA	技術的に実現可能な場合、 ・不正認証試行の回数制限 ・不正認証を試みた場合の警告表示	・アカウントロックの設定値の書類 ・決定されているログイン失敗数に達した後に、どのようにシステムが利用者に通知するかの警告設定のルール
CIP-008-5：Cyber Security ― Incident Reporting and Response Planning		
R1 サイバーセキュリティインシデント対応計画仕様		
適用システム	**要件**	**基準例**
・高度の影響のある BES サイバーシステム ・中度の影響のある BES サイバーシステム	サイバーセキュリティインシデントを識別し、分類し、対応するための1つ以上のプロセス	サイバーセキュリティインシデントを識別、分類、対応するプロセスが含まれた日付のあるサイバーセキュリティインシデント対応計画
	・法律で禁止されている場合を除いて、識別	サイバーセキュリティインシ

	されたサイバーセキュリティインシデントが報告義務がある、又は電力業界情報共有・分析センター(ES-ISAC)へ通知するものかどうかを決定する1つ以上のプロセス ・ただの準備通告かもしれない ES-ISAC への最初の通知は、報告義務のあるサイバーセキュリティインシデントと決定してから 1 時間を超えない	デントが報告義務のあるものか決定したり、ES-ISAC へ最初に通知の書類を決定するための指針や閾値を提供する、日付のあるサイバーセキュリティインシデント対応計画
	サイバーセキュリティインシデント対応グループや個人の役割と権限	監視や報告、開始、書類作成等のサイバーセキュリティインシデント対応グループや個人の役割や権限を規定した日付のあるサイバーセキュリティインシデント対応プロセスや手続き
	サイバーセキュリティインシデント用の事故取扱手順	事故封じ込めや根絶、回復／事故解決といった事故取扱に対処するための日付のあるセキュリティインシデント対応プロセスや手続き

R2 サイバーセキュリティインシデント対応計画の導入とテスト		
適用システム	要件	基準例
・高度の影響のある BES サイバーシステム ・中度の影響のある BES サイバーシステム	最低 15 か月に 1 回のサイバーセキュリティインシデント対応計画のテスト ・実際の報告義務のあるサイバーセキュリティインシデントへの対応によって ・報告義務のあるサイバーセキュリティインシデント等についての紙のドリルや机上訓練によって ・報告義務のあるサイバーセキュリティインシデント運用訓練によって	・テストの要約、ノートやログ、テストで起きた伝達を編集した訓練ー学習報告を日付のある証拠として ・訓練に基づいた討論や運用を含む訓練の種類
	・報告義務のあるサイバーセキュリティインシデントへ対応や報告訓練を行う際の R1 に基づいたサイバーセキュリティインシデント対応計画の利用 ・インシデントや訓練へ対応した際に発生した計画との逸脱の書類	インシデント報告書、ログ、インシデント対応プロセス中に付けたノート、インシデントや訓練へ対応した際に発生した計画との逸脱について追跡調査した書類
	報告義務のあるサイバーセキュリティインシデントの記録保持	セキュリティログ、捜査報告書、e-mail、返信用紙又はチェックシート、フォレンシック分析結果、回復記録、過去に報告義務のあったサイバ

		ーセキュリティインシデントに関するインシデント調査ノートのような書類
R3 サイバーセキュリティインシデント対応計画のレビューと改訂、伝達		
適用システム	**要件**	**基準例**
・高度の影響のある BES サイバーシステム ・中度の影響のある BES サイバーシステム	サイバーセキュリティインシデント対応計画のテスト、又は報告義務のあるサイバーセキュリティインシデント対応完了後 **90 日以上**遅れないこと ・学んだレッスンや学んだレッスンの欠席者の文書 ・計画に関連して学んだ文書化されたレッスンに基づいたサイバーセキュリティインシデント対応計画の改訂 ・計画に関連して学んだ文書化されたレッスンに基づいて改訂されたサイバーセキュリティインシデント対応計画で決められた役割について、個人・グループへの通知	・過去のインシデントレビューミーティングメモやサイバーセキュリティインシデント対応計画のテストや実際の報告義務のあるサイバーセキュリティインシデント対応に関する学習したレッスンを示す追跡報告書を日付のある文書又はレッスンで学習していないことを示す日付のある文書 ・日付があり、改訂された学習されたレッスンに基づいて変えたサイバーセキュリティインシデント対応計画 ・計画更新配布の証拠 - e-mail - 米国郵政公社又は他の郵便サービス - 電子配布システム - 訓練書名シート
	役割や権限変更後、サイバーセキュリティインシデント対応のために事業者が決定したグループ・個人、又は技術が計画実行能力に及ぼす影響を **60 日以内**に ・サイバーセキュリティインシデント対応計画を改訂する ・改訂されたサイバーセキュリティインシデント対応計画上の決められた役割を持つ個人やグループへ通知する	役割や権限、対応者、技術等の変化について記載された、日付があり改訂されたサイバーセキュリティインシデント対応計画 ・計画更新配布の証拠 -e-mail -米国郵政公社又は他の郵便サービス -電子配布システム -訓練書名シート
CIP-009-5：Cyber Security ― Recovery Plans for BES Cyber Systems		
R1 復旧計画仕様		
適用システム	**要件**	**基準例**
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と	復旧計画の実施条件	復旧計画を実施するために定義された条件が言語化された 1 つ又はそれ以上の計

PACS ・中度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS		画
	対応者の役割と権限	対応者の役割と権限の定義が言語化されている1つ又はそれ以上の復旧計画
	1つ又はそれ以上の BES サイバーシステムが機能的に回復するために必要な情報バックアップと格納のプロセス	BES サイバーシステムを機能的に回復するのに必要な情報のバックアップと格納のための個別のプロセスの文書化
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS ・コントロールセンターにおける中度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS	1.3 のバックアッププロセスが成功して完了したことを検証し、バックアップ失敗への対処のための1つ又はそれ以上のプロセス	バックアッププロセスが成功して完了したことを確認するためと、バックアップが失敗した場合の対処時のログ、ワークフロー他の文書
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS ・中度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS	・復旧計画を実行させる起点となるサイバーセキュリティインシデントの原因を決定する1つ又はそれ以上のサイバー資産機能毎のデータ保存プロセス ・データ保存が回復を妨げたり制限していない	CD 保存や回復前のデータミラーリングといったデータ保存手順
R2 復旧計画の導入とテスト		
適用システム	**要件**	**基準例**
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS ・コントロールセンターにおける中度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS	少なくとも **15 か月に 1 回**は、要件 R1 を参照した復旧計画をテストする ・実際の事故から回復する際に ・紙のドリルや机上訓練で ・運用訓練で	・最低 **15 か月に 1 回**実施する復旧計画のテスト（実際の事故からの回復や神のドリルや机上訓練、運用訓練）についての日付のある証拠 ・紙のドリルや完全な運用訓練については、ミーティング通知、議事録、他の訓練で分かったことの記録が証拠になる
	BES サイバーシステムを機能的に回復するために使われる情報の代表的なサンプルを、現在の設定に使えるか適合しているか	使いやすさ（サンプルテープの読み込み、テープ内容の拾い読み）や、適合性（バッ

	を確認するために、少なくとも **15 か月に 1 回**テストする BES サイバーシステムを機能的に回復するために使われる情報を包含している実際の復旧計画が、このテストの代わりになる	クアップ媒体内容や現在の設定間のマニュアル又は自動比較項目)をテストするための基準に基づいた運用ログ又はテスト結果
・高度の影響のある BES サイバーシステム	最低限 **36 か月に 1 回**は、復旧計画の運用訓練を通して、要件 R1を参照した復旧計画をテストする 実際の回復対応は運用訓練の代替になる可能性がある	・運用訓練が **36 か月に1回**に行われ、事業代表者環境へ回復されていることを示している ・実際の回復対応が発生して **36 か月以内**に、復旧計画を実行している
R3 復旧計画のレビューと改訂、伝達		
適用システム	**要件**	**基準例**
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS ・コントロールセンターにおける中度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS	復旧計画テスト又は実際の回復完了後、**90 日以内**に ・復旧計画テストや実際の回復に関連して学んだ知識の文書化するのと学んだ知識が無かったことの文書化 ・計画に関連して学んだ文書化された知識に基づいた復旧計画の改訂 ・学んで文書化した知識に基づいて改訂された復旧計画上の決められた役割を人員やグループへ通知	・復旧計画テストや実際の事故回復での識別された不備や学んだ知識に関する日付のある文書、あるいは学んだ知識が無かったことを示した日付のある文書 ・学んだ知識に基づいた改訂が示された日付のある復旧計画 ・計画更新配布の証拠 -e-mail -米国郵政公社又は他の郵便サービス -電子配布システム -訓練書名シート
	事業者が決定する、復旧計画の実行能力への影響がある役割と権限、対応者や技術の変更後 **60 日以内**に ・復旧計画の更新 ・改訂した復旧計画上の決められた役割を人員、グループへ通知	・役割や権限、対応者、技術等の変化があった場合の日付のある改訂された復旧計画 ・計画更新配布の証拠 - e-mail - 米国郵政公社又は他の郵便サービス - 電子配布システム - 訓練書名シート
CIP-010-1：Cyber Security-Configuration Change Management and Vulnerability		
R1 構成変更管理		
適用システム	**要件**	**基準例**

・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA ・中度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA	個々の又はグループ毎に以下の項目を含む基本構成 ・OS(バージョンを含む)や個別の OS を持たないファームウェア ・意図的に導入した商用利用、又はオープンソースソフトウェア(バージョンを含む) ・導入したカスタムソフトウェア ・論理ネットワークのアクセスポート等 ・適用したセキュリティパッチ	・個別又はグループ単位のサイバー資産毎の、基本構成に必要とされる項目を定義した一覧表 ・個別又はグループ単位のサイバー資産毎の、基本構成上必要とされる項目資産管理システムの記録
	既存の基本構成から逸脱した変更に関する承認と書類	・変更要求記録と、管理システムの関連する電子認証の変更権限に関する変更 ・要件に合わせて実行された変更文書
	既存の基本構成から逸脱した変更をする場合、変更してから **30 日以内**に必要とされる基本構成を改訂する	変更が実施されてから **30 日以内**である、日付のある改訂された構成書類
	既存の構成管理から逸脱した変更をする場合、 ・変更前に、変更によって影響を受ける CIP005 と 007 で要求されるサイバーセキュリティ管理を決定する ・変更に従い、要件 1.4.1 で決定したサイバーセキュリティ管理が悪影響が無いか検証する ・検証結果を文書化する	日付のあるテスト結果に基づいて検証、テストされたサイバーセキュリティ管理のリスト
・高度の影響のある BES サイバーシステム	技術的に可能な場合、既存の構成管理から逸脱した変更をする場合、 ・生産環境への何らかの変更を導入する前に、テスト環境での変更テスト又は、悪影響を最低限に抑えたテスト ・テスト結果と、テスト環境が使われた場合、本番環境との違いの文書化	成功したテスト結果やテスト環境との違いのリストに従ってテストされたサイバーセキュリティ管理のリスト
R2 構成監視		
適用システム	**要件**	**基準例**
・高度の影響のある BES サイバーシステムと関連する EACMS と PCA	最低 **35 日に 1 回**は、R1.1 で示した基本設定の変化を監視する 検知した未承認の変更を文書化し、調査する	未承認変更を検知した調査記録に沿って、設定を監視しているシステムからのログ
R2 構成監視		
適用システム	**要件**	**基準例**
・高度の影響のある BES	最低**15 か月に 1 回**は、書類上、又は実際の	・評価方法等に従って BES

サイバーシステムと関連する EACMS と PACS と PCA ・中度の影響のある BES サイバーシステムと関連する EACMS と PACS と PCA	脆弱性評価を行う	サイバーシステムの管理状況の評価を(15 か月以内に)実施した日付のある書類リスト ・評価の日付と、評価を実施した時のツールの出力結果の書類リスト
・高度の影響のある BES サイバーシステム	技術的に実現可能な場合、最低 36 か月に 1 回 ・テスト環境を使うか、又は本番環境で基本構成のモデルを用意して、悪影響を最小にした方法で、実際の脆弱性評価を行う ・テスト結果とテスト環境を使った場合には本番環境との違いの文書化	(36 か月以内に実施された)日付のある評価結果と、評価実施に使用したツールの出力結果、テスト環境と本番環境の違いのリスト
・高度の影響のある BES サイバーシステムと関連する EACMS と PCA	新しく適用可能なサイバー資産を本番環境に追加する前に、サイバー資産の脆弱性評価を行う(CIP が定義する例外的な環境や、基本構成にとって同じ種類のサイバー資産の場合を除く)	新しいサイバー資産を発注する前に実施された日付のある評価結果と評価実施に使用したツールの出力結果のリスト
・高度の影響のある BES サイバーシステムと関連する EACMS と PACS と PCA ・中度の影響のある BES サイバーシステムと関連する EACMS と PACS と PCA	R3.1,3.2,3.3 に従って実施した評価結果と、評価で指摘された修正又は脆弱性緩和の行動計画(実施日、実施状況)の文書化	再調査又は、評価結果の文書化リスト -実施項目リスト -実施計画の予想完了日 -実施項目ごとの実施状況記録(状況確認打ち合わせ議事録や作業指示システムの更新結果、実施項目を追跡した一覧表)

CIP-011-1:Cyber Security ― Information Protection

R1 情報保護

適用システム	要件	基準例
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS ・中度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS	BES サイバーシステム情報の定義に合った情報を特定する方法	・BES サイバーシステム情報を主体の情報保護プログラムから特定する文書化された方法 ・主体の情報保護プログラムで指定されたように、ラベルや分類等の BES サイバーシステム情報を特定する情報表示 ・BES サイバーシステム情報等を認識するのに十分な知識を全職員に与える訓練

		資料 ・BES サイバーシステム情報を主体の情報保護プログラムで収納するよう指定した電気的・物理的場所
	BES サイバーシステム情報の保護や安全に取り扱うための手続き（格納、搬送、理容等）	・格納や搬送時の安全、BES サイバーシステム情報の利用といった保護や安全に取り扱うための手続き ・BES サイバーシステム情報が主体の書類手続きと一致した方法で取り扱うことを示した記録
R1 情報保護		
適用システム	**要件**	**基準例**
・高度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA ・中度の影響のある BES サイバーシステムとそれに関連する EACMS と PACS と PCA	適用されるサイバー資産の再利用に先立って、事業者がサイバー資産情報格納媒体から BES サイバーシステム情報の未承認取り出しを防ぐために行う行為	・BES サイバーシステム情報を未承認で取り出すことから守るために、除去や取り除き、破壊などのような機密性を下げる行為を追跡した記録 ・暗号化や、物理的なセキュリティ防御線の維持、BES サイバーシステム情報の未承認取り出しを防ぐために使われる他の方法のといった行為を追跡した記録
	BES サイバーシステム情報を含むサイバー資産の廃棄に先立って、事業者がサイバー資産情報格納媒体から BES サイバーシステム情報の未承認取り出しを防ぐために行う行為	・サイバー資産の廃棄の前に、情報格納媒体が壊されたことを示した記録 ・サイバー資産の廃棄の前に、BES サイバーシステム情報の未承認取り出しを防ぐ行為の記録

BES：Bulk Electronics System（大規模電力システム）
EACMS：Electronics Access Control or Monitoring Systems（監視制御システム）
EAP：Electronic Access Point（電子アクセスポイント）
PACS：Physical Access Control Systems（物理的なアクセス制御システム）
PCA：Protected Cyber Assets（保護されたサイバー資産（コンピューター、ネットワークなど））

また、以下で CIP 008-5～CIP 011-5 に対応する違反厳重程度（VSL：Violation Severity Levels、処罰を決めるとき重要な要因の一つである）の定義・説明を整理し、示す。

Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
		Lower VSL	Moderate VSL	High VSL	Severe VSL
長期計画	低い	N/A	N/A	役割や権限が定められていない計画 又は 事故取扱手続が明記されていない計画	事故を識別、分類、対応する1つ以上のプロセスのある計画を作っていない 又は 計画はあるが、報告義務のある事故を識別する1つ以上のプロセスが含まれていない 又は 事故識別後**1時間以内**の ES-ISAC への予備通知が明記されていない
運用計画リアルタイム運用	低い	**15 か月以内**に計画のテストがされていないが、テスト間隔が **16 か月**を超えていない	**16 か月以内**に計画のテストがされていないが、テスト間隔が **17 か月**を超えていない	**17 か月以内**に計画のテストがされていないが、テスト間隔が **18 か月**を超えていない 又は テストまたは報告義務のある事故が起こった時に、計画との逸脱を文書化していない	**19 か月**のテスト間隔内で計画のテストが行われていない 又は 事故関連の記録を保持していない
運用評価	低い	事故やテストから **120 日以内**であるが、**90 日以内**に改訂した計画に定めた役割を関係者に通知していない	事故やテストから **120 日以内**であるが、学習した知見を文書化してから **90 日以内**に計画を改訂していない 又は 事故やテストから **120 日以内**に改訂したが関係者に通知していない 又は 計画実行能力に	事故やテストから **120 日以内**であるが、**90 日以内**に学習した知見や学習されなかった知見を文書化していない 又は 事故やテストから **120 日以内**に学習された知見を文書化したものに基づいて計画を改訂していない	事故やテストから **120 日以内**に学習した知見や学習されなかった知見を文書化していない

			影響のある変化があって 90 日未満だが、60 日以内に計画を改訂も通知もしていない	又は 計画実行能力に影響のある変化があって 90 日以内に計画を改訂も通知もしていない	
Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
		Lower VSL	Moderate VSL	High VSL	Severe VSL
長期計画	中程度	N/A	事業者は復旧計画を持つが、1.2～1.5 の要件のどれか1つが定められていない	事業者は復旧計画を持つが、1.2～1.5 の要件のどれか2つが定められていない	復旧計画を持っていない 又は 復旧計画を持つが、要件 1.1 の起動条件を定めていない 又は 復旧計画を持つが、1.2～1.5 の要件の3つ以上定められてない
運用計画リアルタイム運用	低い	前回テスト時に何等かの不備が見つかり、評価され、収集されたにも関わらず、要件 2.1 に従って、前回から 16 か月は超えていないが、15 か月以内に復旧計画をテストしていない 又は 要件 2.2 に従って･･･15,16 か月 又は 要件 2.3 に従って･･･36,37 か月	前回テスト時に何等かの不備が見つかり、評価され、収集されたにも関わらず、前回から 17 か月は超えていないが、16 か月以内に復旧計画をテストしていない 又は 要件 2.2 に従って･･･16,17 か月 又は 要件 2.3 に従って･･･37,38 か月	前回テスト時に何等かの不備が見つかり、評価され、収集されたにも関わらず、要件 2.1 に従って、前回から 18 か月は超えていないが、17 か月以内に復旧計画をテストしていない 又は 要件 2.2 に従って･･･17,18 か月 又は 要件 2.3 に従って･･･38,39 か月	要件 2.1 に従って、18 か月以内に復旧計画をテストしていない 又は ●テストは実施、不備識別のみ／●テストは実施、不備の識別、評価、収集をしていない 又は 要件 2.2 に従って･･･18 か月 又は、●／● 要件 2.3 に従って･･･39 か月 又は、●／●
運用評価	低い	復旧計画改訂後、210 日を超えていないが、90 日以内に役割を関係者に通知していない	復旧計画テスト、又は実際の回復から 210 日を超えていないが、90 日以内に、学んだ知見で計画を改訂していない	復旧計画テスト、又は実際の回復から 210 日を超えていないが、90 日以内に、学んだ知見や学んでいない知見について文	復旧計画テスト、又は実際の回復から 210 日以内に、学んだ知見や学んでいない知見について文書化し

			又は **復旧計画改訂後**、**120 日以内**に役割を通知していない 又は 役割・権限、対応者、技術が変更時に **90 日**を超えていないが、**60 日以内**に計画の改訂又は関係者に通知していない	**書化していない** 又は **120 日以内**に、学んだ知見で**計画を改訂していない** 又は 役割・権限、対応者、技術が変更時に **90 日以内**に計画の改訂又は関係者に通知していない	**ていない**
Time Horizon	**VRF**	**Violation Severity Levels (CIP-010-1)**			
		Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
運用計画	中程度	R1.1.1～1.1.5 の内、**4つ**まで構成変更管理プロセスとして 導入、文書化している 又は **5 つ**全て導入、文書化しているが、**不備の識別**のみ 又は **5 つ**全て導入、文書化しているが、**不備の識別、評価、収集は未実施** 又は 1.4.1 と 1.4.2 のステップに従って不備の識別のみ 又は 1.4.1 と 1.4.2 のステップに従っているが、不備の検知、評価、収集は未実施	R1.1.1～1.1.5 の内、**3 つ** 又は **4 つ**導入、文書化しているが、不備の識別のみ 又は **5 つ**全て導入、文書化しているが、**不備の識別、評価、収集は未実施** 又は CIP005、007 の基本構成管理のセキュリティ管理プロセスはあるが、不備の識別のみ 又は プロセスはあるが、不備の識別、評価、収集はしていない	R1.1.1～1.1.5 の内、**2 つ** 又は **3 つ**導入、文書化しているが、**不備の識別**のみ 又は **3 つ**導入、文書化しているが、**不備の識別、評価、収集は未実施** 又は 基本構成管理の変更についての認証、文書化のプロセスはあるが、不備の識別のみ 又は プロセスはあるが、不備の識別、評価、収集は未実施 又は 変更から **30 日以内**に基本構成の改訂をしていない 又は しているが不備の識別のみ 又は しているが、不備の識別、評価、収集は未実施	構成変更管理プロセスとして **導入、文書化していない** 又は R1.1.1～1.1.5 の内、**1 つ** 又は **2 つ以下**導入、文書化しているが、**不備の識別**のみ 又は **5 つ**全て導入、文書化しているが、**不備の識別、評価、収集はしていない** 又は 基本構成管理の変更の認証、文書化のプロセスがない 又は 変更から **30 日以内**に基本構成の改訂するプロセスがない 又は CIP005、007 の基本構成管理のセキュリティ管理プロセスがない 又は

				又は CIP005、007 のプロセスはあるが不備の検知のみ 又は CIP005、007 のプロセスはあるが不備の識別、評価、収集は未実施 又は 変更テストのプロセスはあるが不備の識別のみ 又は 変更テストのプロセスはあるが不備の識別、評価、収集は未実施 又は テスト結果の文書化プロセスはあるが不備の識別のみ 又は テスト結果の文書化プロセスはあるが不備の識別、評価、収集は未実施	プロセスがあるが、変更の検証や文書化はしていない 又は 変更時のテストプロセスがない 又は テストを文書化するプロセスがない
運用計画	中程度	N/A	N/A	N/A	検知した基本構成を未承認の変更を監視、調査、35 日以内の文書化のプロセスが無い 又は プロセスはあるが、不備の識別のみ 又は プロセスはあるが、不備の識別、評価、収集は未実施
長期計画 運用計画	中程度	文書化した BES サイバーシステムの脆弱性評価プロセスを持つが、前回実施後 18 か月以内だが 15 か月以内に評価を	文書化した BES サイバーシステムの脆弱性評価プロセスを持つが、前回実施後 21 か月以内だが 18 か月以内に評価を	文書化した BES サイバーシステムの脆弱性評価プロセスを持つが、前回実施後 24 か月以内だが 21 か月以内に評価を	文書化した BES サイバーシステムの脆弱性評価プロセスを持っていない 又は 文書化した BES

		実施していない 又は 文書化した**適用可能なシステム**の脆弱性評価プロセスを持つが、前回実施後 **39 か月以内**だが **36 か月以内**に評価を実施していない	実施していない 又は 文書化した**適用可能なシステム**の脆弱性評価プロセスを持つが、前回実施後 **42 か月以内**だが **39 か月以内**に評価を実施していない	実施していない 又は 文書化した**適用可能なシステム**の脆弱性評価プロセスを持つが、前回実施後 **45 か月以内**だが **42 か月以内**に評価を実施していない	**サイバーシステム**の脆弱性評価プロセスを持つが、前回実施後 **24 か月以内**に評価を実施していない 又は 文書化した**適用可能なシステム**の脆弱性評価プロセスを持つが、前回実施後 **45 か月以内**に評価を実施していない 又は BES サイバーシステムの評価プロセスはあるが、既存の構成管理のモデルで実施していない 又は 適用可能なシステムの評価プロセスはあるが文書化していない
Time Horizon	**VRF**	**Violation Severity Levels (CIP-010-1)**			
		Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
運用計画	**中程度**	N/A		**事業者が** BES **サイバーシステム情報保護プログラムを導入しているプログラムには、**BES **サイバーシステム情報とその不備を識別するが、不備を評価したり正すのではない1つ以上の方法が記されている** **又は** **システム情報は識別するが、不備を識別、評価正すことが無い情報保護プログラムを導入** **又は**	**事業者が書類を保有していない、または** BES **サイバーシステム情報保護プログラムを導入**

				システム情報を保護、安全に取扱い、不備を識別するが、不備を評価、正すことが無い情報保護プログラムを導入 又は システム情報を保護、安全に取扱うが、不備を識別、評価正すことが無い情報保護プログラムを導入	
運用計画	低い	N/A	事業者はいつ以上の文書化されたプロセスを導入するが、それは BES サイバー資産からの BES サイバーシステム情報を未承認で取り出すことを防ぐことに関する再利用のためのプロセスは含まない	事業者はいつ以上の文書化されたプロセスを導入するが、それは BES サイバー資産からの BES サイバーシステム情報を未承認で取り出すことを防ぐことに関する**廃棄や媒体破壊**のプロセスは含まない	事業者は文書化された導入されたどんなプロセスも持たない

VRF：Violation Risk Factors
VSL：Violations Severity Levels

(3)NISTIR 7628 によるスマートグリッドの脆弱性分類

NISTIR 7628 はスマートグリッドにおける脆弱性のハイレベルな分類を行い、適用できるセキュリティ要件も提示している。

脆弱性分類			Smart Grid Security Requirements Families																	
			SG.AC	SG.AT	SG.AU	SG.CM	SG.CP	SG.IA	SG.IR	SG.ID	SG.MP	SG.PS	SG.PE	SG.PL	SG.CA	SG.PM	SG.SC	SG.SI	SG.SA	SG.MA
People, Policy & Procedure	Training	Insufficiently Trained Personnel		●			●		●							●				
		Inadequate Security Training and Awareness Program		●			●		●							●				
	Policy & Procedure	Insufficient Identity Validation, Background Checks	●					●				●	●			●				●
		Inadequate Security Policy	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●
		Inadequate Privacy Policy													●	●				
		Inadequate Patch Management Process	●			●	●	●	●							●		●	●	
		Inadequate Change and Configuration Management														●			●	
		Unnecessary System Access	●			●		●			●	●	●			●				
	Risk Management	Inadequate Periodic Security Audits			●											●				
		Inadequate Security Oversight by Management		●	●							●	●		●	●				
		Inadequate Continuity of Operations or Disaster Recovery Plan					●							●	●	●				
		Inadequate Risk Assessment Process														●				
		Inadequate Incident Response Process				●			●				●	●		●				
Platform Software/Firmware Vulnerabilities	Software Development	Code Quality Vulnerability		●								●				●	●	●	●	●
		Authentication Vulnerability	●	●		●										●		●	●	●
		Authorization Vulnerability	●	●		●										●		●	●	●
		Cryptographic Vulnerability		●												●			●	●
		Environmental Vulnerability	●	●				●				●				●	●		●	●
		Error Handling Vulnerability		●												●		●	●	●
		General Logic Error		●												●			●	●
		Business logic Vulnerability																		
		Input and Output Validation		●												●		●	●	●
		Logging and Auditing Vulnerability		●				●								●			●	●
		Password Management Vulnerability	●	●				●								●			●	●

		Path Vulnerability		●												●			●	●
		Protocol Errors		●												●			●	●
		Range and Type Error Vulnerability		●												●			●	●
Platform Software/Firmware Vulnerabilities	Software Development	Sensitive Data Protection Vulnerability		●						●						●			●	●
		Session Management Vulnerability		●												●			●	●
		Concurrency, Synchronization and Timing Vulnerability		●												●			●	●
		Insufficient Safeguards for Mobile Code		●												●			●	●
		Buffer Overflow		●												●			●	●
		Mishandling of Undefined, Poorly Defined, or "Illegal" Conditions		●												●			●	●
		Use of Insecure Protocols		●												●	●		●	●
		Weaknesses that Affect Files and Directories		●												●			●	●
	API Usage & Implementation	API Abuse		●												●			●	●
		Use of Dangerous API		●												●			●	●
Platform Vulnerabilities	Design	Use of Inadequate Security Architectures and Designs	●	●	●		●	●	●			●		●		●	●	●	●	●
		Lack of External or Peer Review for Security Design	●	●	●		●	●	●			●		●		●	●	●	●	●
	Implementation	Whitelisting			●	●														●
		File Integrity Monitoring								●	●							●	●	●
		Inadequate Malware Protection		●	●		●		●					●			●	●	●	
		Installed Security Capabilities Not Enabled by Default	●	●	●	●		●						●			●	●	●	
		Absent or Deficient Equipment Implementation Guidelines	●	●	●	●		●						●		●	●		●	
	Operational	Lack of Prompt Security Patches from Software Vendors			●		●		●								●	●	●	
		Unneeded Services Running		●	●	●								●			●	●	●	
		Insufficient Log Management	●	●	●	●	●	●	●		●			●			●	●	●	
	Poorly configured security equipment	Inadequate Anomaly Tracking	●	●	●		●	●	●			●	●	●			●	●	●	
Network	Network	Inadequate Integrity Checking				●									●	●		●	●	●
		Inadequate Network Segregation				●									●		●	●	●	●
		Inappropriate Protocol Selection				●									●	●	●	●	●	●
		Weaknesses in Authentication Process or Authentication Keys				●													●	●
		Insufficient	●			●		●				●	●		●	●				●

		Redundancy																		
		Physical Access to the Device	●			●		●				●	●		●	●			●	●

(4)NISTIR 7628 によるスマートグリッドセキュリティ要件の適用範囲

ここでスマートグリッドのための 197 のハイレベルなセキュリティ要件を詳述し、22 の論理インターフェース分類に対応付けられている。

セキュリティ要件グループ	Serial No.	SG サイバーセキュリティ要件名	論理インターフェース分類における適用性																						
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Access Control (SG.AC)	SG.AC-5	InformationFlow Enforcement																						
	SG.AC-6	Separation of Duties	Applies at moderate and high impact levels																					
	SG.AC-8	Unsuccessful Login Attempts	Applies at all impact levels																					
	SG.AC-10	Previous Logon Notification																						
	SG.AC-11	Concurrent Session Control																						
	SG.AC-12	Session Lock							H	H									L				L	H
	SG.AC-13	Remote Session Termination																	M		M			
	SG.AC-14	Permitted Actions without Identification or Authentication	H	H	H	H	H	H	M	M	M	H			H	H	M	M	H	H		H	H	H
	SG.AC-16	Wireless Access Restrictions	Applies at all impact levels																					
	SG.AC-18	Use of External Information Control Systems	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																					
	SG.AC-19	Control System Access Restrictions	Applies at all impact levels																					
	SG.AC-20	Publicly Accessible Content	Applies at all impact levels																					
	SG.AC-21	Passwords	Applies at all impact levels																					
Awareness and Training (SG.AT)	SG.AT-5	Contact with Security Groups and Associations																						
	SG.AT-6	Security Responsibility Training	Applies at all impact levels																					
Audit and Accountability (SG.AU)	SG.AU-4	Audit Storage Capacity	Applies at all impact levels																					
	SG.AU-5	Response to Audit Processing Failures	Applies at all impact levels with additional requirement enhancements at high impact level																					
	SG.AU-7	Audit Reduction and Report Generation	Applies at moderate and high impact levels																					
	SG.AU-8	Time Stamps	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																					
	SG.AU-11	Conduct and Frequency of Audits	Applies at all impact levels																					
	SG.AU-12	Auditor Qualification	Applies at all impact levels																					
	SG.AU-13	Audit Tools	Applies at all impact levels																					
	SG.AU-14	Security Policy Compliance	Applies at all impact levels																					
	SG.AU-15	Audit Generation	Applies at all impact levels																					
	SG.AU-16	Non-Repudiation							M	M	M				H	H		M				H	H	H
Security Assessment and Authorization (SG.CA)	SG.CA-1	Security Assessment and Authorization Policy and Procedures	Applies at all impact levels																					
	SG.CA-2	Security Assessments	Applies at all impact levels																					
	SG.CA-3	Continuous Improvement	Applies at all impact levels																					
	SG.CA-5	Security Authorization to Operate	Applies at all impact levels																					
	SG.CA-6	Continuous Monitoring	Applies at all impact levels																					
Configuration Management (SG.CM)	SG.CM-7	Configuration for Least Functionality	Applies at all impact levels																					
	SG.CM-8	Component Inventory	Applies at all impact levels																					
	SG.CM-11	Configuration Management Plan	Applies at all impact levels																					
Continuity of Operations (SG.CP)	SG.CP-1	Continuity of Operations Policy and Procedures	Applies at all impact levels																					
	SG.CP-4	Continuity of Operations Training	Applies at all impact levels																					
	SG.CP-7	Alternate Storage Sites	Applies at moderate and high impact levels with additional requirement enhancements at moderate and high impact levels																					
	SG.CP-8	Alternate Telecommunication Services	Applies at moderate and high impact levels with additional requirement enhancements at moderate and high impact levels																					
	SG.CP-9	Alternate Control Center	Applies at moderate and high impact levels with additional requirement enhancements at moderate and high impact levels																					

	SG.CP-11	Fail-Safe Response	Applies at high impact levels
Identification and Authentication (SG.IA)	SG.IA-1	Identification and Authentication Policy and Procedures	Applies at all impact levels
	SG.IA-2	Identifier Management	Applies at all impact levels
	SG.IA-5	Device Identification and Authentication	H H H H M M M H H H H
	SG.IA-6	Authenticator Feedback	L L L L L L H H L L H H L H L L L L H
Information and Document Management (SG.ID)	SG.ID-1	Information and Document Management Policy and Procedures	Applies at all impact levels
	SG.ID-4	Information Exchange	Applies at all impact levels
	SG.ID-5	Automated Labeling	
Incident Response (SG.IR)	SG.IR-1	Incident Response Policy and Procedures	Applies at all impact levels
	SG.IR-3	Incident Response Training	Applies at all impact levels
	SG.IR-4	Incident Response Testing and Exercises	Applies at all impact levels
	SG.IR-5	Incident Handling	Applies at all impact levels
	SG.IR-6	Incident Monitoring	Applies at all impact levels
	SG.IR-7	Incident Reporting	Applies at all impact levels
	SG.IR-10	Smart Grid Information System Backup	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels
Smart Grid Information System Development and Maintenance (SG.MA)	SG.MA-1	Smart Grid Information System Maintenance Policy and Procedures	Applies at all impact levels
	SG.MA-2	Legacy Smart Grid Information System Updates	Applies at all impact levels
	SG.MA-3	Smart Grid Information System Maintenance	Applies at all impact levels with additional requirement enhancements at high impact levels
	SG.MA-4	Maintenance Tools	Applies at all impact levels
	SG.MA-5	Maintenance Personnel	Applies at all impact levels
	SG.MA-6	Remote Maintenance	Applies at all impact levels with additional requirement enhancements at high impact levels
Media Protection (SG.MP)	SG.MP-1	Media Protection Policy and Procedures	Applies at all impact levels
	SG.MP-3	Media Marking	Applies at moderate and high impact levels
	SG.MP-4	Media Storage	Applies at all impact levels
	SG.MP-5	Media Transport	Applies at all impact levels
Physical and Environmental Security (SG.PE)	SG.PE-8	Emergency Shutoff Protection	Applies at all impact levels
	SG.PE-9	Emergency Power	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels
	SG.PE-10	Delivery and Removal	Applies at all impact levels
	SG.PE-11	Alternate Work Site	Applies at all impact levels
	SG.PE-12	Location of Smart Grid Information System Assets	Applies at all impact levels with additional requirement enhancements at high impact level
Planning (SG.PL)	SG.PL-1	Strategic Planning Policy and Procedures	Applies at all impact levels
	SG.PL-2	Smart Grid Information System Security Plan	Applies at all impact levels
	SG.PL-3	Rules of Behavior	Applies at all impact levels
	SG.PL-4	Privacy Impact Assessment	Applies at all impact levels
Security Program Management (SG.PM)	SG.PM-2	Security Program Plan	Applies at all impact levels
	SG.PM-3	Senior Management Authority	Applies at all impact levels
	SG.PM-4	Security Architecture	Applies at all impact levels
	SG.PM-5	Risk Management Strategy	Applies at all impact levels
	SG.PM-6	Security Authorization to Operate Process	Applies at all impact levels
	SG.PM-7	Mission/Business Process Definition	Applies at all impact levels
Personnel Security (SG.PS)	SG.PS-6	Access Agreements	Applies at all impact levels
	SG.PS-8	Personnel Accountability	Applies at all impact levels
	SG.PS-9	Personnel Roles	Applies at all impact levels
Risk Management and Assessment	SG.RA-3	Security Impact Level	Applies at all impact levels

(SG.RA)			
	SG.SA-1	Smart Grid Information System and Services Acquisition Policy and Procedures	Applies at all impact levels
	SG.SA-2	Security Policies for Contractors and Third Parties	Applies at all impact levels
	SG.SA-3	Life-Cycle Support	Applies at all impact levels
	SG.SA-4	Acquisitions	Applies at all impact levels
	SG.SA-5	Smart Grid Information System Documentation	Applies at all impact levels
Smart Grid Information System and Services Acquisition (SG.SA)	SG.SA-6	Software License Usage Restrictions	Applies at all impact levels
	SG.SA-7	User-Installed Software	Applies at all impact levels
	SG.SA-8	Security Engineering Principles	Applies at all impact levels
	SG.SA-9	Developer Configuration Management	Applies at all impact levels
	SG.SA-10	Developer Security Testing	Applies at all impact levels
	SG.SA-11	Supply Chain Protection	Applies at all impact levels
Smart Grid Information System and Information Integrity (SG.SI)	SG.SI-1	System and Information Integrity Policy and Procedures	Applies at all impact levels
	SG.SI-5	Security Alerts and Advisories	Applies at all impact levels
	SG.SI-7	Software and Information Integrity	H H H H H H M M M H M H H M M H
	SG.SI-9	Error Handling	Applies at all impact levels
Smart Grid Information System and Communication Protection (SG.SC)	SG.SC-2	Communications Partitioning	
	SG.SC-3	Security Function Isolation	H H H H M M H H H M M H
	SG.SC-4	Information Remnants	
	SG.SC-5	Denial-of-Service Protection	H M H M M M M M M H M H
	SG.SC-6	Resource Priority	H H H
	SG.SC-8	Communication Integrity	H H H H H H M M M H M M H H M M H H H H H
	SG.SC-9	Communication Confidentiality	H H H H H
	SG.SC-10	Trusted Path	
	SG.SC-11	Cryptographic Key Establishment and Management	Applies at all impact levels with additional requirement enhancements at high impact levels
	SG.SC-12	Use of Validated Cryptography	Applies at all impact levels
	SG.SC-13	Collaborative Computing	Applies at all impact levels
	SG.SC-14	Transmission of Security Parameters	
	SG.SC-15	Public Key Infrastructure Certificates	Applies at all impact levels
	SG.SC-16	Mobile Code	Applies at moderate and high impact levels
	SG.SC-17	Voice-Over Internet Protocol	
	SG.SC-20	Message Authenticity	Applies at all impact levels
	SG.SC-21	Secure Name/Address Resolution Service	Applies at all impact levels
	SG.SC-22	Fail in Known State	Applies at moderate and high impact levels
	SG.SC-23	Thin Nodes	
	SG.SC-24	Honeypots	
	SG.SC-25	Operating System-Independent Applications	
	SG.SC-26	Confidentiality of Information at Rest	H H H H H H
	SG.SC-27	Heterogeneity	
	SG.SC-28	Virtualization Technique	
	SG.SC-29	Application Partitioning	H H H H H H H H H H H H H H H H
	SG.SC-30	Information System Partitioning	Applies at moderate and high impact levels

(5)CIP、NIST SP 800-53 及び NISTIR 7628 のセキュリティ要件比較

セキュリティ要件の内容を比較すると、CIP ver.2 よりも NIST のガイドラインの方が適用範囲が広い。既存の電力システムについては CIP、スマートグリッドにおけるサイバーセキュリティ対策のためには、NISTIR 7628 を参照する構造であると考えられる。また、NISTIR 7628 の管理策はさらに GRC、UTR 及び CTR の三種類で分けられる。其々の定義は以下のとおりである：

GRC: Common Governance, Risk, and Compliance (GRC) Requirements;（組織レベル、具体的な論理インターフェース分類や SG 情報システムにより補足の必要も）
UTR: Unique Technical Requirements;（一つ以上の論理インターフェース分類に通用、全部ではなく）
CTR(C): Common Technical Requirements, Confidentiality;（22 の論理インターフェース分類に通用する）
CTR(I): Common Technical Requirements, Integrity;
CTR(A): Common Technical Requirements, Availability.（実際に存在しない）

Smart Grid Cyber Security Requirement Category	NISTIR 7628 Number	Smart Grid Cyber Security Requirement Name	Category	NIST SP 800-53 (R3) Number	Control Name	NERC CIPS (1-9) May 2009
Access Control (SG.AC)	SG.AC-1	Access Control Policy and Procedures	GRC	AC-1	Access Control Policy and Procedures	CIP 003-2 (R1, R1.1, R1.3, R5, R5.3)
	SG.AC-2	Remote Access Policy and Procedures	GRC	AC-17	Remote Access	CIP005-2 (R1, R1.1, R1.2, R2, R2.3, R2.4)
	SG.AC-3	Account Management	GRC	AC-2	Account Management	CIP 003-2 (R5, R5.1, R5.2, R5.3) CIP 004-2 (R4, R4.1, R4.2) CIP 005-2 (R2.5) CIP 007-2 (R5, R5.1, R5.2)
	SG.AC-4	Access Enforcement	GRC	AC-3	Access Enforcement	CIP 004-2 (R4) CIP 005-2 (R2, R2.1-R2.4)
	SG.AC-	Information	UTR	AC-4	Information	—

	5	Flow Enforcement			Flow Enforcement	
	SG.AC-6	Separation of Duties	CTR(I)	AC-5	Separation of Duties	—
	SG.AC-7	Least Privilege	CTR(I)	AC-6	Least Privilege	CIP 007-2 (R5.1)
	SG.AC-8	Unsuccessful Login Attempts	CTR(I)	AC-7	Unsuccessful Login Attempts	—
	SG.AC-9	Smart Grid Information System Use Notification	CTR(I)	AC-8	System Use Notification	CIP 005-2 (R2.6)
	SG.AC-10	Previous Logon Notification	UTR	AC-9	Previous Logon (Access) Notification	—
	SG.AC-11	Concurrent Session Control	UTR	AC-10	Concurrent Session Control	—
	SG.AC-12	Session Lock	UTR	AC-11	Session Lock	—
	SG.AC-13	Remote Session Termination	UTR	—	—	—
	SG.AC-14	Permitted Actions without Identification or Authentication	UTR	AC-14	Permitted Actions without Identification or Authentication	—
	SG.AC-15	Remote Access	UTR	AC-17	Remote Access	CIP 005-2 (R2, R3, R3.1, R3.2)
	SG.AC-16	Wireless Access Restrictions	CTR(C)	—	—	—

	SG.AC-17	Access Control for Portable and Mobile Devices	CTR(C)	AC-19	Access Control for Mobile Devices	CIP 005-2 (R2.4, R5, R5.1)
	SG.AC-18	Use of External Information Control Systems	GRC	SC-7	Boundary Protection	—
	SG.AC-19	Control System Access Restrictions	GRC	—	—	—
	SG.AC-20	Publicly Accessible Content	GRC	—	—	—
	SG.AC-21	Passwords	CTR(I)	—	—	—
Awareness and Training (SG.AT)	SG.AT-1	Awareness and Training Policy and Procedures	GRC	AT-1	Security Awareness and Training Policy and Procedures	CIP 004-2 (R1, R2)
	SG.AT-2	Security Awareness	GRC	AT-2	Security Awareness	CIP 004-2 (R1)
	SG.AT-3	Security Training	GRC	AT-3	Security Training	CIP 004-2 (R2)
	SG.AT-4	Security Awareness and Training Records	GRC	AT-4	Security Training Records	CIP 004-2 (R2.3)
	SG.AT-5	Contact with Security Groups and Associations	GRC	AT-5	Contact with Security Groups and Associations	—
	SG.AT-6	Security Responsibility Training	GRC	—	—	—
	SG.AT-7	Planning Process Training	GRC	—	—	CIP 004-2 (R2)
Audit and Accountability (SG.AU)	SG.AU-1	Audit and Accountability Policy and	GRC	AU-1	Audit and Accountability Policy and	CIP 003-2 (R1, R1.1, R1.3)

		Procedures			Procedures	
	SG.AU-2	Auditable Events	CTR(I)	AU-2	Auditable Events	CIP 005-2 (R1, R1.1, R1.3) CIP 007-2 (R5.1.2, R5.2.3, R6.1, R6.3)
				AU-13	Monitoring for Information Disclosure	
	SG.AU-3	Content of Audit Records	CTR(I)	AU-3	Content of Audit Records	CIP 007-3 (R5.1.2)
	SG.AU-4	Audit Storage Capacity	CTR(I)	AU-4	Audit Storage Capacity	—
	SG.AU-5	Response to Audit Processing Failures	GRC	AU-5	Response to Audit Processing Failures	—
	SG.AU-6	Audit Monitoring, Analysis, and Reporting	GRC	AU-6	Audit Monitoring, Analysis, and Reporting	CIP 007-2 (R5.1.2) CIP 007-2 (R6.5)
	SG.AU-7	Audit Reduction and Report Generation	GRC	AU-7	Audit Reduction and Report Generation	—
	SG.AU-8	Time Stamps	GRC	AU-8	Time Stamps	—
	SG.AU-9	Protection of Audit Information	GRC	AU-9	Protection of Audit Information	CIP 003-2 (R4)
	SG.AU-10	Audit Record Retention	GRC	AU-11	Audit Record Retention	CIP 005-2 (R5.3) CIP 007-2 (R5.1.2, R6.4) CIP 008-2 (R2)
	SG.AU-11	Conduct and Frequency of Audits	GRC	AU-1	Audit and Accountability Policy and	—

					Procedures	
	SG.AU-12	Auditor Qualification	GRC	—	—	—
	SG.AU-13	Audit Tools	GRC	AU-7	Audit Reduction and Report Generation	—
	SG.AU-14	Security Policy Compliance	GRC	CA-1	Security Assessment and Authorization Policies and Procedures	—
	SG.AU-15	Audit Generation	CTR(I)	AU-12	Audit Generation	—
	SG.AU-16	Non-Repudiation	UTR	AU-10	Non-Repudiation	—
Security Assessment and Authorization (SG.CA)	SG.CA-1	Security Assessment and Authorization Policy and Procedures	GRC	CA-1	Security Assessment and Authorization Policies and Procedures	—
	SG.CA-2	Security Assessments	GRC	CA-2	Security Assessments	—
	SG.CA-3	Continuous Improvement	GRC	—	—	—
	SG.CA-4	Smart Grid Information System Connections	GRC	CA-3	Information System Connection	CIP 005-2 (R2)
	SG.CA-5	Security Authorization to Operate	GRC	CA-6	Security Authorization	—
				PM-10	Security Authorization Process	
	SG.CA-6	Continuous Monitoring	GRC	CA-7	Continuous Monitoring	—
Configuration Management (SG.CM)	SG.CM-1	Configuration Management Policy and Procedures	GRC	CM-1	Configuration Management Policy and Procedures	CIP 003-2 (R6)
	SG.CM-	Baseline	GRC	CM-2	Baseline	CIP 007-2

	2	Configuration			Configuration	(R9)
	SG.CM-3	Configuration Change Control	GRC	CM-3	Configuration Change Control	CIP 003-2 (R6)
				SA-10	Developer Configuration Management	
	SG.CM-4	Monitoring Configuration Changes	GRC	CM-4	Security Impact Analysis	CIP 003-2 (R6)
				SA-10	Developer Configuration Management	
	SG.CM-5	Access Restrictions for Configuration Change	GRC	CM-5	Access Restrictions for Change	CIP 003-2 (R6)
	SG.CM-6	Configuration Settings	GRC	CM-6	Configuration Settings	CIP 003-2 (R6) CIP 005 (R2.2)
	SG.CM-7	Configuration for Least Functionality	CTR(I)	CM-7	Least Functionality	—
	SG.CM-8	Component Inventory	CTR(I)	CM-8	Information System Component Inventory	—
	SG.CM-9	Addition, Removal, and Disposal of Equipment	GRC	MP-6	Media Sanitization	CIP 003-2 (R6)
	SG.CM-10	Factory Default Settings Management	GRC	—	—	CIP 005-2 (R4.4)
	SG.CM-11	Configuration Management Plan	GRC	CM-9	Configuration Management Plan	—
Continuity of Operations (SG.CP)	SG.CP-1	Continuity of Operations Policy and Procedures	GRC	CP-1	Contingency Planning Policy and Procedures	—
	SG.CP-2	Continuity of Operations Plan	GRC	CP-1	Contingency Planning Policy and	CIP 008-2 (R1) CIP 009-2

					Procedures	(R1)
	SG.CP-3	Continuity of Operations Roles and Responsibilities	GRC	CP-2	Contingency Plan	CIP 009-2 (R1.1, R1.2)
	SG.CP-4	Continuity of Operations Training	GRC	—	—	—
	SG.CP-5	Continuity of Operations Plan Testing	GRC	CP-4	Contingency Plan Testing and Exercises	CIP 008-2 (R1.6) CIP 009-2 (R2, R5)
	SG.CP-6	Continuity of Operations Plan Update	GRC	—	—	CIP 009-2 (R4, R5)
	SG.CP-7	Alternate Storage Sites	GRC	CP-6	Alternate Storage Sites	—
	SG.CP-8	Alternate Telecommunication Services	GRC	CP-8	Telecommunications Services	—
	SG.CP-9	Alternate Control Center	GRC	CP-7	Alternate Processing Site	—
				CP-8	Telecommunications Services	—
	SG.CP-10	Smart Grid Information System Recovery and Reconstitution	GRC	CP-10	Information System Recovery and Reconstitution	CIP 009-2 (R4)
	SG.CP-11	Fail-Safe Response	GRC	—	—	—
Identification and Authentication (SG.IA)	SG.IA-1	Identification and Authentication Policy and Procedures	GRC	IA-1	Identification and Authentication Policy and Procedures	—
	SG.IA-2	Identifier Management	GRC	IA-4	Identifier Management	—
	SG.IA-3	Authenticator Management	GRC	IA-5	Authenticator Management	CIP 007-2 (R5, R5.1, R5.2, R5.3)
	SG.IA-4	User Identification and	UTR	IA-2	User Identification and	CIP 003-2 (R1, R1.1, R1.3)

		Authentication			Authentication	
	SG.IA-5	Device Identification and Authentication	UTR	IA-3	Device Identification and Authentication	—
	SG.IA-6	Authenticator Feedback	UTR	IA-6	Authenticator Feedback	—
Information and Document Management (SG.ID)	SG.ID-1	Information and Document Management Policy and Procedures	GRC	—	—	—
	SG.ID-2	Information and Document Retention	GRC			CIP 006-2 (R7)
	SG.ID-3	Information Handling	GRC	MP-1	Media Protection Policy and Procedures	CIP 003-2 (R4.1)
	SG.ID-4	Information Exchange	GRC	—	—	—
	SG.ID-5	Automated Labeling	GRC	—	—	—
Incident Response (SG.IR)	SG.IR-1	Incident Response Policy and Procedures	GRC	IR-1	Incident Response Policy and Procedures	—
	SG.IR-2	Incident Response Roles and Responsibilities	GRC	IR-1	Incident Response Policy and Procedures	CIP 008-2 (Rr1.2) CIP 009-2 (R1.2)
	SG.IR-3	Incident Response Training	GRC	IR-2	Incident Response Training	—
	SG.IR-4	Incident Response Testing and Exercises	GRC	IR-3	Incident Response Testing and Exercises	—
	SG.IR-5	Incident Handling	GRC	IR-4	Incident Handling	—
	SG.IR-6	Incident Monitoring	GRC	IR-5	Incident Monitoring	—
	SG.IR-7	Incident Reporting	GRC	IR-6	Incident Reporting	—
	SG.IR-8	Incident Response Investigation and	GRC	PE-6	Monitoring Physical Access	CIP 008-2 (R1, R1.2-R1.5)

		Analysis				
	SG.IR-9	Corrective Action	GRC	—	—	CIP 008-2 (R1.4) CIP 009-2 (R3)
	SG.IR-10	Smart Grid Information System Backup	GRC	CP-9	Information System Backup	—
	SG.IR-11	Coordination of Emergency Response	GRC	—	—	CIP 008-2 (R1.3)
Smart Grid Information System Development and Maintenance (SG.MA)	SG.MA-1	Smart Grid Information System Maintenance Policy and Procedures	GRC	MA-1	System Maintenance Policy and Procedures	—
	SG.MA-2	Legacy Smart Grid Information System Updates	GRC	—	—	—
	SG.MA-3	Smart Grid Information System Maintenance	GRC	PL-6	Security-Related Activity Planning	—
				MA-2	Controlled Maintenance	
	SG.MA-4	Maintenance Tools	GRC	MA-3	Maintenance Tools	—
	SG.MA-5	Maintenance Personnel	GRC	MA-5	Maintenance Personnel	—
	SG.MA-6	Remote Maintenance	GRC	MA-4	Non-Local Maintenance	—
	SG.MA-7	Timely Maintenance	GRC	MA-6	Timely Maintenance	CIP 009-2 (R4)
Media Protection (SG.MP)	SG.MP-1	Media Protection Policy and Procedures	GRC	MP-1	Media Protection Policy and Procedures	—
	SG.MP-2	Media Sensitivity Level	GRC	RA-2	Security Categorization	CIP 003-2 (R4, R4.2)
	SG.MP-3	Media Marking	GRC	MP-3	Media Marking	—
	SG.MP-4	Media Storage	GRC	MP-4	Media Storage	—
	SG.MP-5	Media Transport	GRC	MP-5	Media Transport	—
	SG.MP-6	Media Sanitization and Disposal	GRC	MP-6	Media Sanitization	CIP 007-2 (R7, R7.1, R7.2, R7.3)

Physical and Environmental Security (SG.PE)	SG.PE-1	Physical and Environmental Security Policy and Procedures	GRC	PE-1	Physical and Environmental Protection Policy and Procedures	CIP 006-2 (R1, R2)
	SG.PE-2	Physical Access Authorizations	GRC	PE-2	Physical Access Authorizations	CIP 004-2 (R4)
	SG.PE-3	Physical Access	GRC	PE-3	Physical Access Control	CIP 006-2 (R2)
				PE-4	Access Control for Transmission Medium	
				PE-5	Access Control for Output Devices	
	SG.PE-4	Monitoring Physical Access	GRC	PE-6	Monitoring Physical Access	CIP 006-2 (R5)
	SG.PE-5	Visitor Control	GRC	PE-7	Visitor Control	CIP 006-2 (R1.4)
	SG.PE-6	Visitor Records	GRC	PE-8	Access Records	CIP 006-2 (R1.4, R6)
	SG.PE-7	Physical Access Log Retention	GRC	—	—	CIP 006-2 (R7)
	SG.PE-8	Emergency Shutoff Protection	GRC	PE-10	Emergency Shutoff	—
	SG.PE-9	Emergency Power	GRC	PE-11	Emergency Power	—
	SG.PE-10	Delivery and Removal	GRC	PE-16	Delivery and Removal	—
	SG.PE-11	Alternate Work Site	GRC	PE-17	Alternate Work Site	—
	SG.PE-12	Location of Smart Grid Information System Assets	GRC	PE-18	Location of Information System Components	—
Planning (SG.PL)	SG.PL-1	Strategic Planning Policy and Procedures	GRC	PL-1	Security Planning and Procedures	—
	SG.PL-2	Smart Grid Information System Security	GRC	PL-2	System Security Plan	—

		Plan				
	SG.PL-3	Rules of Behavior	GRC	PL-4	Rules of Behavior	—
	SG.PL-4	Privacy Impact Assessment	GRC	PL-5	Privacy Impact Assessment	—
	SG.PL-5	Security-Related Activity Planning	GRC	PL-6	Security-Related Activity Planning	CIP 002-2 (R1)
Security Program Management (SG.PM)	SG.PM-1	Security Policy and Procedures	GRC	AC-1	Access Control Policy and Procedures	CIP 003-2 (R1, R1.1, R1.3, R5, R5.3)
	SG.PM-2	Security Program Plan	GRC	PM-1	Information Security Program Plan	—
	SG.PM-3	Senior Management Authority	GRC	PM-2	Senior Information Security Officer	—
	SG.PM-4	Security Architecture	GRC	PM-7	Enterprise Architecture	—
	SG.PM-5	Risk Management Strategy	GRC	PM-9	Risk Management Strategy	—
	SG.PM-6	Security Authorization to Operate Process	GRC	PM-10	Security Authorization Process	—
	SG.PM-7	Mission/Business Process Definition	GRC	PM-11	Mission/Business Process Definition	—
	SG.PM-8	Management Accountability	GRC	PM-1	Information Security Program Plan	CIP 003-2 (R2, R3)
Personnel Security (SG.PS)	SG.PS-1	Personnel Security Policy and Procedures	GRC	PS-1	Personnel Security Policy and Procedures	CIP 004-2 (R3)
	SG.PS-2	Position Categorization	GRC	PS-2	Position Categorization	CIP 004-2 (R3)
	SG.PS-3	Personnel Screening	GRC	PS-3	Personnel Screening	CIP 004-2 (R3)
	SG.PS-4	Personnel Termination	GRC	PS-4	Personnel Termination	CIP 004-2 (R4.2) CIP 004-2 (R5.2.3)
	SG.PS-5	Personnel Transfer	GRC	PS-5	Personnel Transfer	CIP 004-2 (R4.1, R4.2)
	SG.PS-6	Access	GRC	PS-6	Access	

		Agreements			Agreements	
	SG.PS-7	Contractor and Third-Party Personnel Security	GRC	PS-7	Third-Party Personnel Security	CIP 004-2 (R3.3)
	SG.PS-8	Personnel Accountability	GRC	PS-8	Personnel Sanctions	—
	SG.PS-9	Personnel Roles	GRC	—	—	—
Risk Management and Assessment (SG.RA)	SG.RA-1	Risk Assessment Policy and Procedures	GRC	RA-1	Risk Assessment Policy and Procedures	CIP 002-2 (R1, R1.1, R1.2, R4) CIP 003-2 (R1, R4.2)
	SG.RA-2	Risk Management Plan	GRC	PM-9	Risk Management Strategy	CIP 003-2 (R4, R4.1, R4.2)
	SG.RA-3	Security Impact Level	GRC	RA-2	Security Categorization	
	SG.RA-4	Risk Assessment	GRC	RA-3	Risk Assessment	CIP 002-2 (R1.2)
	SG.RA-5	Risk Assessment Update	GRC	RA-3	Risk Assessment	CIP 002-2 (R4)
	SG.RA-6	Vulnerability Assessment and Awareness	GRC	RA-5	Vulnerability Scanning	CIP 005-2 (R4, R4.2, R4.3, R4.4) CIP 007-2 (R8)
Smart Grid Information System and Services Acquisition (SG.SA)	SG.SA-1	Smart Grid Information System and Services Acquisition Policy and Procedures	GRC	SA-1	System and Services Acquisition Policy and Procedures	—
	SG.SA-2	Security Policies for Contractors and Third Parties	GRC	—	—	—
	SG.SA-3	Life-Cycle Support	GRC	SA-3	Life-Cycle Support	—
	SG.SA-4	Acquisitions	GRC	SA-4	Acquisitions	—
	SG.SA-5	Smart Grid Information System Documentation	GRC	SA-5	Information System Documentation	—
	SG.SA-6	Software	GRC	SA-6	Software	—

		License Usage Restrictions			Usage Restrictions	
	SG.SA-7	User-Installed Software	GRC	SA-7	User-Installed Software	—
	SG.SA-8	Security Engineering Principles	GRC	SA-8	Security Engineering Principles	—
				SA-13	Trustworthiness	
	SG.SA-9	Developer Configuration Management	GRC	SA-10	Developer Configuration Management	—
	SG.SA-10	Developer Security Testing	CTR(I)	SA-11	Developer Security Testing	—
	SG.SA-11	Supply Chain Protection	GRC	SA-12	Supply Chain Protection	—
Smart Grid Information System and Communication Protection (SG.SC)	SG.SC-1	System and Communication Protection Policy and Procedures	GRC	SC-1	System and Communication Protection Policy and Procedures	CIP 003-2 (R1, R1.1, R1.3)
	SG.SC-2	Communications Partitioning	UTR	—	—	—
	SG.SC-3	Security Function Isolation	UTR	SC-3	Security Function Isolation	—
	SG.SC-4	Information Remnants	UTR	SC-4	Information in Shared Resources	—
	SG.SC-5	Denial-of-Service Protection	UTR	SC-5	Denial-of-Service Protection	—
	SG.SC-6	Resource Priority	UTR	SC-6	Resource Priority	—
	SG.SC-7	Boundary Protection	UTR	SC-7	Boundary Protection	CIP 005-2 (R1, R1.1, R1.2, R1.3, R1.4, R1.6, R2, R2.1-R2.4, R5, R5.1)
	SG.SC-8	Communication Integrity	UTR	SC-8	Transmission Integrity	—
	SG.SC-9	Communication Confidentiality	UTR	SC-9	Transmission Confidentiality	—

	SG.SC-10	Trusted Path	UTR	SC-11	Trusted Path	—
	SG.SC-11	Cryptographic Key Establishment and Management	CTR(C)	SC-12	Cryptographic Key Establishment and Management	—
	SG.SC-12	Use of Validated Cryptography	CTR(C)	SC-13	Use of Cryptography	—
	SG.SC-13	Collaborative Computing	GRC	SC-15	Collaborative Computing Devices	—
	SG.SC-14	Transmission of Security Parameters	UTR	SC-16	Transmission of Security Attributes	—
	SG.SC-15	Public Key Infrastructure Certificates	CTR(C)	SC-17	Public Key Infrastructure Certificates	—
	SG.SC-16	Mobile Code	CTR(C)	SC-18	Mobile Code	—
	SG.SC-17	Voice-Over Internet Protocol	UTR	SC-19	Voice Over Internet Protocol	—
	SG.SC-18	System Connections	CTR(C)	CA-3	Information System Connections	CIP 005-2 (R2, R2.2-R2.4)
	SG.SC-19	Security Roles	CTR(I)	SA-9	External Information System Services	CIP 003-2 (R5)

	SG.SC-20	Message Authenticity	CTR(I)	SC-8	Transmission Integrity	—
	SG.SC-21	Secure Name/Address Resolution Service	CTR(I)	SC-20	Secure Name/Address Resolution Service (Authoritative Source)	—
	SG.SC-22	Fail in Known State	CTR(I)	SC-24	Fail in Known State	—
	SG.SC-23	Thin Nodes	UTR	SC-25	Thin Nodes	—
	SG.SC-24	Honeypots	UTR	SC-26	Honeypots	—
	SG.SC-25	Operating System-Independent Applications	UTR	SC-27	Operating System-Independent Applications	—
	SG.SC-26	Confidentiality of Information at Rest	UTR	SC-28	Confidentiality of Information at Rest	—
	SG.SC-27	Heterogeneity	UTR	SC-29	Heterogeneity	—
	SG.SC-28	Virtualization Technique	UTR	SC-30	Virtualization Technique	—
	SG.SC-29	Application Partitioning	UTR	—	—	—
	SG.SC-30	Information System Partitioning	CTR(I)	SC-32	Information Systems Partitioning	—
Smart Grid Information System and Information Integrity (SG.SI)	SG.SI-1	System and Information Integrity Policy and Procedures	GRC	SI-1	System and Information Integrity Policy and Procedures	—
	SG.SI-2	Flaw Remediation	CTR(I)	SI-2	Flaw Remediation	CIP 007-2 (R3, R3.1, R3.2)
	SG.SI-3	Malicious Code and	GRC	SI-3	Malicious Code	CIP 007-2 (R4, R4.1,

		Spam Protection			Protection	R4.2)
				SI-8	Spam Protection	CIP 007-2 (R4)
	SG.SI-4	Smart Grid Information System Monitoring Tools and Techniques	GRC	SI-4	Information System Monitoring	CIP 007-2 (R6)
	SG.SI-5	Security Alerts and Advisories	GRC	SI-5	Security Alerts, Advisories, and Directives	—
	SG.SI-6	Security Functionality Verification	GRC	SI-6	Security Functionality Verification	CIP 007-2 (R1)
	SG.SI-7	Software and Information Integrity	UTR	SI-7	Software and Information Integrity	—
	SG.SI-8	Information Input Validation	CTR(I)	SI-10	Information Input Validation	CIP 003-2 (R5) CIP 007-2 (R, R5.1, R5.2)
	SG.SI-9	Error Handling	CTR(I)	SI-11	Error Handling	—

付録 6　欧州の主要タスクフォースの取り組み

(1)欧州スマートグリッド・タスクフォース・エキスパートグループ 2 (SGTF EG2: European Smart Grid Task Force Expert Group 2)

欧州のエネルギー供給サイドでは、EU 範囲のスマートグリッドの導入をサポート・促進するために、欧州委員会のガス＆エネルギー局内に「スマートグリッド・タスクフォース」(SGTF）を設立した（2009 年 11 月)。SGTF は第 3 次エネルギーパッケージ（TEP：Third Energy Package）におけるスマートグリッドの実現に向けて、総合的なビジョン（規制、技術）を提供する。また、SGTF は重要問題に関する規制機関と被規制側の事業者・エンドユーザー間の合意を目指している。重要問題の例としては、コスト／ベネフィットの評価、関連リスク、必要なインセンティブなどが挙げられている。

SGTF はステアリングコミティの下に、当初は３つのエキスパートグループ（EG）が置かれた。EG1 が「スマートグリッドとスマートメーターの機能（Functionalities)」、EG2 が「データセキュリティ、データハンドリング、データプロテクションのための規制勧告」、EG3 が「スマートグリッド展開に関わる関係者の役割と責任」といったテーマを担当している（スマートメーターセキュリティ・デプライバシー分析も行う)。その後、ガスに関連するスマートグリッド分野をテーマとする EG4 も設立された。各 EG は EC によって召集され、ENISA が所管している。

スマートグリッドに直接関わっている EG2 の具体的な目標・使命は以下のとおりである。

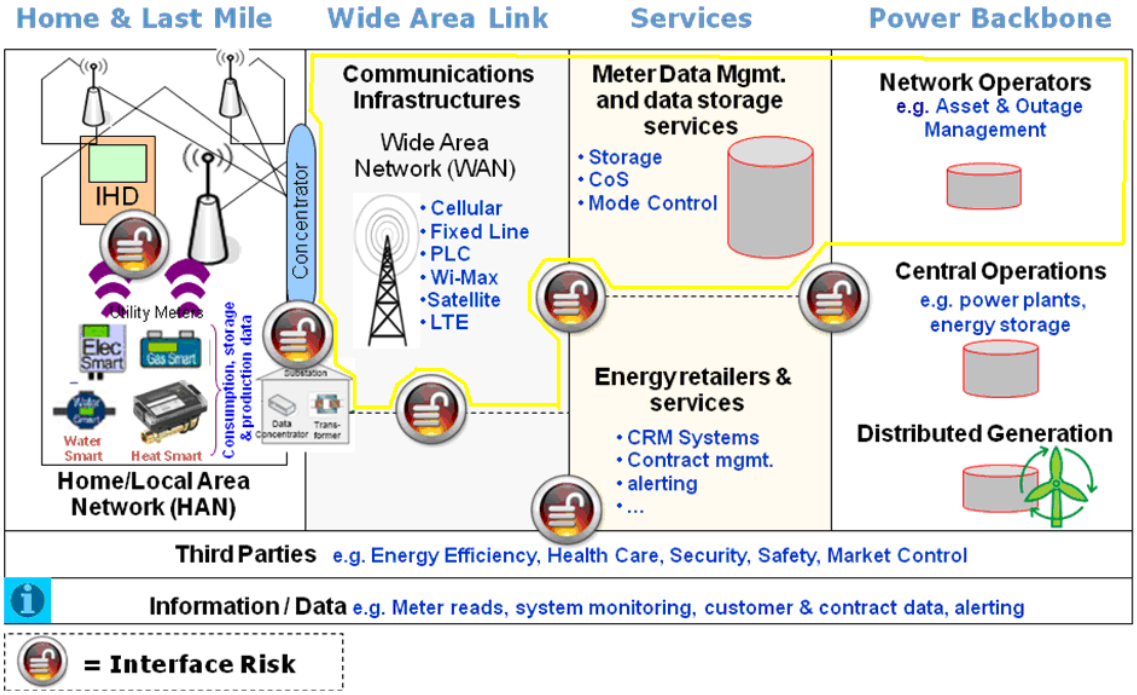
- スマートグリッドにおけるベネフィット及び顧客の関心事項の確認
- データ保護、プライバシー及びそれぞれの執行に係る欧州の法規制の確認
- データ取り扱い、安全及びデータ保護における可能なリスクの確認
- データの所有者及びアクセス権利の確認
- データ保護のための責任組織及び執行メカニズムの確認
- データ活用を促進するためのフレームワークの開発
- 顧客、市民及び政治家に対してスマートグリッド・コミュニケーションのベネフィットに関する推奨

成果物の例としては、EG2 は 2011 年 2 月に「‘Regulatory recommendations for data safety, data handling and data protection」（データ安全、データ取扱及びデータ保護のための規制勧告）というレポートを発表している。

その中間報告書が概観するスマートグリッドのアーキテクチャ概念図に示されているように、スマートメーターネットワークにおける様々なインターフェースにおいて、サイバーセキュリティリスクが集中すると指摘されている。
上記の分析に基づいて、SGTF の EG2 中間報告書はスマートグリッドに関わ

るデータセキュリティに関して、ESO(欧州標準化機構）がスマートグリッド・インタフェースのセキュリティをカバーする新しい標準を更新・拡張・開発するべきと勧告している。また、スマートグリッドの End to End のセキュリティとプライバシー保護を設計するに当たり、適切な暗号方式（対称鍵暗号(e.g. AES)、あるいは非対称暗号(e.g. RSA, ECC 暗号, etc.)）評価のうえ選択しなければならないとされている。

図表付録 6-1　スマートグリッドのアーキテクチャ概念図



出所：SGTF EG2「Regulatory Recommendations for Data Safty, Data Handling and Data Protection」報告書を基に日本総研作成

なお、EG2 に関与する組織は下記のとおり。

- ネットワーク・情報セキュリティ（NIS：Network and Information Security ）、重要情報インフラ保護（CCIP：Critical Information Infrastructure Protection）及びエネルギー分野の加盟国の当局
- ICT 産業及び業界団体
- サイバーセキュリティ標準の経験・知見を持つ組織
- 発電事業者及び業界団体
- 配電及び送電ネットワーク運用者及び業界団体
- 自動化・制御システム及び関連技術のサプライヤー（ベンダ）
- エネルギー貿易事業者

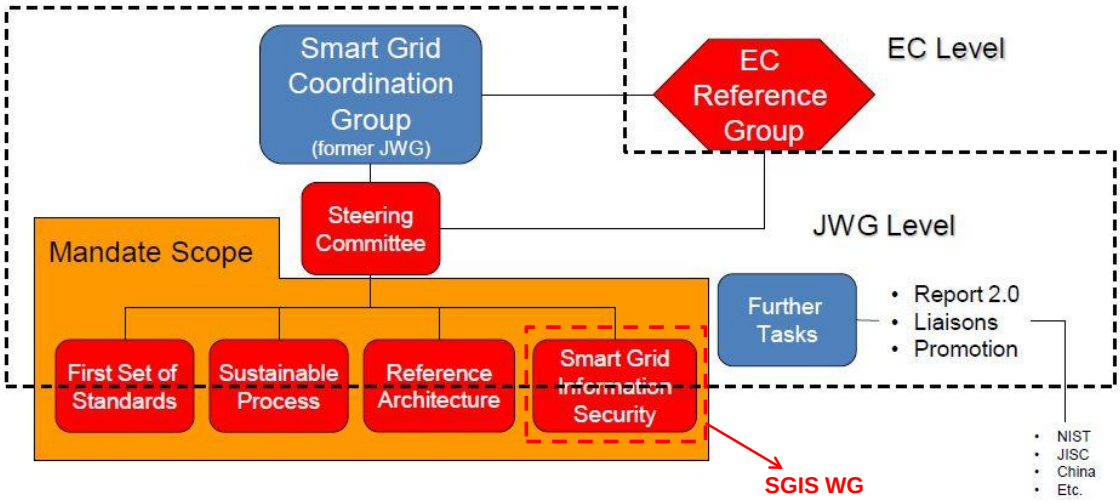
(2)CEN/CENELEC/ETSI Smart Grid Coordination Group (SG-CG) (CEN/CENELEC/ETSI Joint Working Group (JWG))

SGTF はスマートグリッドの展開・配置を成功させるための新たな標準開発の重要性及び既存の標準の修正・改善の必要性を提言している。また、そのグループの専門家は、ＥＵに様々な標準策定機構が存在することにより、不整合・矛盾を有する標準が策定されるリスクも指摘している。その結果、SGTF EG1 はスマートグリッド標準を作るための CEN/CENELEC/ETSI 連立グループを設立する必要性があるという結論を出した。その結果、CEN/CENELEC/ETSI Joint Working Group (JWG)が設立された（活動期間は 2010 年 6 月から 2011 年 3 月まで)。成果物として、スマートグリッド全体の標準化に関する報告書「Final report of CEN/CENELEC/ETSI JWG on standards for smart grids」が提出されている。

前述のとおり、欧州委員会（EC）は M/490 の中で ESO に対して、ESO がスマートグリッド領域における継続的な標準強化・開発、横断的な整合性・一貫性の維持、及び継続したイノベーションの促進を可能にさせるフレームワークの開発を要請している。そして、M/490 に対する ESO の回答として、CEN/CENELEC/ETSI Smart Grids Coordination Group (SG-CG)が設立された。新組織は、以前の JWG とほぼ同一のメンバーにより構成された。SG-CG の下にも実際下記の通り 4 つのワーキンググループ（WG：Working Groups）がある

① Reference architecture WG.
② First set of standards WG.
③ Sustainable processes WG.
④ Security WG

図表付録 6-2　SG-CG 構成



（出所）フィンランド CLEEN 社「D1.3.1 Smart Standardization Analysis, Ver. 2」を基に日本総研作成

その中の１つである Security WG（SGIS WG）はスマートグリッドのセキュリティに関わるグループである。

SGIS WG は数多くの CI&A (Confidentiality, Integrity and Availability)、信頼性（Reliability）／回復力（Resiliency)、プライバシー及び相互運用性基準をベースとした重要セキュリティ要件を定義する。また、多層セキュリティレベルの策定によりスマートグリッドの構成インフラの識別、スマートグリッドセキュリティ関連国際標準のリバイス、ヨーロッパにおける既存の規制や標準の間のギャップや差異の識別、資産分類、リスク評価及び前述のギャップと他要件を埋めるためのツールや方法論の定義にも関与している。

(3)欧州委員会通信ネットワーク・コンテンツ・技術総局 (DG CONNECT：Directorate General of Communications Networks, Content and Technology)のスマートグリッドセキュリティにおける経験的専門グループ（Ad-Hoc EG on Smart Grid Security）

2010 年に、ENISA のサポートにより、欧州委員会は１つの専門グループを立ち上げた。そのグループの名前は「DG CONNECT's Ad-Hoc EG on Smart Grid Security」である。使命／任務は以下のとおりである：

- EU レベルの関連政策の確認及び議論（アウトプットとしては COM(2011) 163、COM(2011) 202 などがある）
- 電力業界と ICT 業界を取りまとめ、関連機関による議論・作業を通じて、スマートグリッドのための ICT セキュリティ及び被害からの回復力に関する重要性について認識を向上させること
- EU が取るべきアクションの優先度の確認
- セキュリティ及び回復力を確保するための EU レベルの提言の定義
- スマートメーターの要素の確認（例としては、スマート家電、スマートメーター、スマート配電、スマート（ローカル）発電、スマート送電がある）
- 重要ストラテジー、ハイレベル要件定義
- 上記の取り組みを通じた意思決定者の意識向上

スマートグリッドセキュリティにおいて、Ad-Hoc EG の主要取り組みとしては、「Programme of Work」が定義され、下記の 4 つの主要領域（Area)、12 のワークパッケージ（WP）に注力（2010 年 11 月から 2012 年 5 月まで）

- Area 1. リスク、脅威及び脆弱性
  - WP 1.1　すべての関連スマートグリッド資産の認識及び分類
  - WP 1.2　関連資産（Relevant Asset）のためのアタッチ（attatch）／脅威分類基準の開発
  - WP 1.3　関連資産のための対策分類基準の開発
  - WP 1.4　関連資産のためのハイ・レベル・セキュリティリスク評価方法

論の開発

- Area 2. 要件及び技術
  - WP 2.1　セキュリティ要件
  - WP 2.2　有効的なセキュリティ対策を包含するためのスマートグリッド要件の拡張
  - WP 2.3　データセキュリティ対策を取り入れるためのスマートグリッド通信プロトコル及びインフラの研究
  - WP 2.4　公共調達

- Area 3. 情報及び知識共有
  - WP 3.1　加盟国（MS）及び関連有力な組織の間の横断的な連合・同盟関係を発展させること

- Area 4. 意識、教育及び訓練
  - WP 4.1　戦略的なリーダーのためのハイレベル会議
  - WP 4.2　データセキュリティにおける利害関係者の意識向上のための促進活動
  - WP 4.3　エネルギー産業におけるサイバーセキュリティの高度人材の育成

(4)欧州ネットワーク情報セキュリティ庁 (ENISA:European Network and Information Security Agency)

欧州ネットワーク情報セキュリティ庁（ENISA）は欧州におけるデジタル社会の健全な発展と情報セキュリティ向上に貢献するため、2004 年に設立された EU の専門機関である。主たる役割は、欧州の各国政府に重要インフラセキュリティを含むサイバーセキュリティに関する助言と支援を提供することであり、EU 各国の情報セキュリティ担当当局、特に各国の CERT（Computer Emergency Response Team）を支援する。

当初設置目的としては、欧州連合、欧州委員会の各機関および欧州各国のネットワーク情報セキュリティ問題に対する予防、対策および緊急対応の能力を向上することであった。また、ネットワーク情報セキュリティ障害に関わる案件について、規則 460/2004（ENISA 設置規則）で定められた権限で欧州委員会、欧州各国に対し、支援と助言を提供している。さらに、ネットワーク及び情報セキュリティにおける法制度整備・改訂のための技術面での予備検討について、欧州委員会の要請に応じて支援リスクの評価・検討のためのフレームワーク策定、リスク管理機能向上を支援している。

ENISA の組織構造は以下のとおりである。

- 経営会議（Management Board）は加盟国、欧州委員会及び利害関係者の

代表により構成される。
- 利害関係者グループ（PSG：Permanent Stakeholders' Group）は 30 名の欧州全域からの高水準専門家によって構成されている。それぞれの所属する利害関係組織は ICT 産業、ICT ユーザー組織及びネットワーク・情報セキュリティ領域の学術機関を含む。

主要任務は以下のとおりである。

- 欧州委員会と欧州各国に対して以下について助言と支援を提供：
  - ✧ 情報セキュリティ
  - ✧ システム製品のセキュリティ問題についての政府と産業界の意思疎通
- 欧州レベルの最新かつ緊急な（電力通信ネットワークの CI&A に影響する恐れを有する）リスクを分析するための情報セキュリティのインシデントとリスクに関するデータの収集、分析結果の加盟国・EC への提供
- ネットワーク及び情報セキュリティ問題に対する予防、発見及びレスポンス方法論の開発における EC と加盟国の協力・提携の促進
- 脅威への対処能力強化のためのリスクアセスメントとリスク管理手法、防止管理対策の発展・奨励
- 注意喚起と関係者間の連携のための関連産業における官民連携の展開
- EC と加盟国が産業界へハードウェア及びソフトウェア製品におけるセキュリティ関連問題に関する協力
- ネットワーク及び情報セキュリティにおける製品・サービスのための標準開発のフォロー
- EC へネットワーク及び情報セキュリティ領域の研究及びリスク防止に関するアドバイス
- ネットワーク及び情報セキュリティ対策の国際連携
- 活動範囲内で目標に準じる独自の結論、方向性勧告、アドバイス
- 最低限の監査フレームワークの設定
- 内部市場の十分な透明性レベルの実現に貢献

ENISA における具体的な活動例としては、複数年度にまたがる長期的な活動である「多年度テーマプログラム（MTP22）」と、一年間試験的に新しい活動を行う「準備活動（PA23）」がある。PA は活動期間終了後に MTP と位置付けるべきかどうかの見極めが行われる。

また、CIIP プログラムと回復力向上にも取り組んでいる。重要情報インフラ基盤（CIIP：Critical Information Infrastructure Protection）に対する脅威は現実に起こり得るとの認識に基づき、以下のような課題を提起している。

- グローバルな課題としての取り組み
- 官民連携が不十分

- サイバーセキュリティ戦略策定の必要性
- 情報共有促進
- ガイダンスの不足、経験も不足 等々

欧州連合(EU)の各国に対しての共通脅威としては通信が対象となっている。この対応として、準備と防護、検出と対応、被害低減と回復、国際連携が CIIP のアクション計画を策定している。2008 年は準備期間で、2009 年に被害低減に向けたギャップの洗い出し、グッドプラクティス、ガイドラインの作成等を実施し、2010 に勧告、演習、具体的な準備等を推進し、ENISA 第二段階のような対応を開始するとしている。具体的にはメンバー国間での信頼を確立する動きや、すべての重要インフラに影響を与える通信に対する演習を実施する計画である。なお、EU は、2010 年 11 月 4 日に「Cyber Europe 2010」と称し、全 EU 加盟国 27 ヵ国と EFTA（欧州自由貿易連合：European Fair Trade Association）加盟国 3 ヵ国が参加して、初の汎欧州レベルでのサイバー攻撃に備えた演習を実施した。

CII(Critical Information Infrastructure)におけるセキュリティと回復力は最大の重要課題であり、ENISA の役割がより強くなってきている。

なお、ENISA の取り組みの主要成果物は下記のとおりである。

- 「Protecting Industrial Control Systems, Recommendations for Europe and Member States,」（産業制御システム保護：欧州及び加盟国への勧告）（2011 年 12 月）
- 「Smart Grid Security, Recommendations for Europe and Member States」（スマートグリッドセキュリティ：欧州及び加盟国への勧告）（2012 年 7 月）
- 「Appropriate Security Measures for Smart Grids – Guidelines to Access the Sophistication of Security Measure Implementation」（スマートグリッドのための適切なセキュリティ対策：セキュリティ対策実装の高度化知識アクセスのためのガイドライン）（2012 年 12 月）

(5)英国国家インフラ防護センター (CPNI：Centre for the Protection of the National Infrastructure)

英国国家インフラ保護センター（CPNI）は、2007 年に情報局保安部（MI5：Military Intelligence, Section 5）の一部と国家インフラストラクチャー安全調整局（NISCC：National Infrastructure Security Co-ordination Centre）、国家セキュリティ顧問局（NSAC：National Security Advice Centre）を併合して作られた英国政府内の専門組織である。省庁横断の組織であり、英国の様々な政府機関、産業界、大学からの人材で構成されている。

主な任務は、テロリズムやその他の脅威に対する国のインフラの脆弱性を低減する目的で、電力・スマートグリッドを含む重要インフラのセキュリティ（情報通信、人的、物理的セキュリティも含む）に関する総合的なアドバイスを政府機関および民間部門へ与えるもので、セキュリティのガイドの作成・公開、対面での伝達など様々な方法で行われる。アドバイスは高度な専門性と情報に基づくもので、他の政府機関、大学、民間の研究プロジェクトの後援もしており、また様々な分野の専門家との情報交換も行っている。

CPNI が行っている研究プロジェクトは、情報エレクトロニクス分野と物理的・人的セキュリティ分野の両方がある。情報エレクトロニクス分野はSCADA・プロセス制御システムの相互依存性と次世代ネットワークに関するものであり、具体的にはシステムセキュリティエンジニアリング、脆弱性の発見と対策、リアルタイムなマルウェアの特定、ネットワーク犯罪調査、相互依存性のモデリングおよび認証である。物理的・人的セキュリティ分野の研究領域は、ヒューマンファクター、電子工学と制御システム（自動車、センサネット、SCADA)、防弾・対爆、物理的防御手段、およびスキャニング・検出技術（爆発物、武器、生物・化学・放射性物質）である。

(6)ドイツ連邦情報セキュリティ庁
(BSI:Federal Office for Information Security)

ドイツ情報セキュリティ庁（BSI）は内務省の下部組織である。1986 年に中央暗号庁がコンピュータセキュリティを所管したことから始まり、情報セキュリティニーズの高まりを受け、1989 年中央 IT セキュリティ庁へ改組後、1990 年に BSI となった。

BSI はサイバーセキュリティ全般を所管しており、以下に関する IT の脆弱性の分析と防護手段の開発を行っている。

- ソフトウェアと重要インフラセキュリティ
- ネットワークセキュリティ（連邦 CERT 運営、IT situation center、IT 危機管理センター、早期警戒システム）
- 暗号技術、RFID27 や生体認証などの新技術

これらには､IT に関するリスクと脅威に関する情報の提供と IT セキュリティ試験、IT システムのアセスメント、電力業界を含む各種産業との連携も含まれる。また、E-SCSIE（European SCADA and Control Systems Information Exchange）との連携、政府とユーザーと大学関係者の情報交換、インシデント情報の共有などを実施している。

電力システムを含む重要インフラ防御については、重要インフラ防護国家戦略､情報インフラ防護計画（NPSI)､重要インフラ防御実施計画（UP KRITIS)､が内務省によって定められ公開されている。これらによると、重要インフラ防御に関する連邦政府としての対策は、内務省のもとで BSI、住民保護災害支援庁（BBK)、連邦刑事局（BKA)、連邦技術支援局（THW）がそれぞれの担当分野を取りまとめている。BSI の取組みは国内の情報セキュリティを確保する一環として重要インフラに関する情報セキュリティに取り組んでいる。主要活動としては、サイバーセキュリティに関するガイドライン・ツールの開発、セキュリティ基準の策定、推奨プラクティス集の公開、自己評価ツールの配布を実施している。

(7)サイバーセキュリティ及びサイバー犯罪における欧州連合・米国 WG
(EU-US Working Group（WG）on Cyber-security and Cybercrime)

サイバーセキュリティ及びサイバー犯罪における欧州連合・アメリカワーキンググループ（EU-US Working Group （WG） on Cyber-security and Cybercrime）は 2010 年 11 月 20 日にリスボンで行った EU-アメリカサミットの背景で設立された。主要目標としてはセキュリティ及び自由社会の繁栄にとってまずまず重要となるグローバルネットワークに対して新たな脅威の対応である。

EU-US WG は成立から一年以内の進展及びいくつかの重点領域について説明した。それぞれの進展は以下のとおりである。

- 2012 年までの EU-US 合同サイバーインシデント演習を端緒とする協力プログラムを通じ、グローバルに共同でインシデント・マネジメント・レスポンス能力を向上させる。
- 幅広いコミットメントを通じ、民間分野・産業界の協同で優良実践の共有、ボットネットとの戦い、産業制御システム及びスマートグリッド（水処理や発電など）の保安、インターネットの回復力・安定性向上などの重要問題の解決に携わる。
- 迅速な合同意識向上活動、大西洋範囲の情報共有を行う。

また、スマートグリッドセキュリティに係る活動について、現状調査、既存イニシアティブ、選考試験、優良実践及び ICT リスク、プライバシーとセキュリティ手法の比較分析を行う。また、EU 側からのインプットは以下のとおりである。

- 加盟国レベル（オランダ、ドイツ、イギリス、スウェーデンなど）及び欧州レベルにおける産業用制御システム及び ICT 分野・エネルギー分野の相互依存性に関する調査結果（ENISA）
- 欧州パブリックとプライベート両方の利害関係者によって構成され、DG CONNECT に調整される、マートグリッドにおける通信ネッワーク及び情報システムのセキュリティ・回復に関する専門グループの活動内容

アメリカ側からのインプットは以下のとおりである。

- 発達した自発的なセキュリティ標準受理のための国際範囲での官民協働の経験
- 官民連携の制御システムセキュリティ対策の実現するための方法論・メカニズム

このような連携により期待されるアウトプットとしては下記の成果物がある。

- 制御システム／スマートグリッド優先領域における EU 及びアメリカのエンゲージメント戦略
- 産業用制御システムとスマートグリッドのサイバーセキュリティにおけるEUとアメリカ官民エンゲージメントのための行動計画。
- 既存産業用制御システムの共同組織の分析
- 自発的な参与のためのベスト・プラクティスの強調

付録 7　欧州スマートグリッドのサイバーセキュリティに関する提言・施策

(1)欧州スマートグリッド・タスクフォース・エキスパートグループ 2(SGTF EG2)提案

SGTF EG2 が「データセキュリティ、データハンドリング、データプロテクションのための規制勧告」(「Regulatory Recommendations for Data Safty, Data Handling and Data Protection」) の報告書（2011 年 2 月 16 日公表）をまとめている。そこでは、以下に示すように 13 個のインタフェースリスク上のリスクが示され、スマートグリッドに関わるデータセキュリティに対して新たな標準化が必要であると勧告している。SGTF が示したインターフェースは、メーターから IHD（In-Home Display)、HAN から LAN、LAN から WAN などのインターフェースを挙げ、タイプと扱われるデータ等が示されている。137 のインターフェースを示した NIST のような細分化は行われていないが、米国と同様の考え方に基づくものと見られる。

① スマートメーター～In-Home Display

２つのデバイス間の物理的インターフェースのリスク。個人データ漏洩、プリペイメント情報、メーター計量情報、価格情報、料金情報などの偽装の危険が存在する。ファームウェアのアップグレードに関わるリスクも存在する。

② HAN（Home Area Network）～LAN（Local Area Network）

需要家ネットワークから外部への物理的インターフェースのリスク。PLC 及び無線メッシュを使用して LAN に繋げると、多くのメーターが可視化されることで、データセキュリティに大きなリスクが発生する。メーター計量情報、ロードプロファイル情報、アラーム情報などが偽装されるリスクが存在する。ロードプロファイルの技術情報にも漏洩リスクがある。

③ LAN～WAN（Wide Area Networks）

変電所（サブステーション）/地域データコンセントレータとバックホールデバイス、または PLC コンセントレータ間の IP ブリッジに存在するリスク。家庭からのデータ移動と他の消費者データの結合によって、より高度なレベルのリスクが発生する。スマートメータシステムにおいては、ローカルなデータコンセントレータと長距離のバックホールとのインタフェースリスクである。メーター計量情報、ロードプロファイル情報、アラーム情報に偽装のリスクがあり、メーター読出し、ロードプロファイル、アラームなどの技術情報データ漏えいのリスクがある。

④ WAN～ヘッドエンド/データコレクタ

バックホールデータデバイスからバックエンドシステムへのリンクに存在する物理インタフェースリスク。ヘッドエンドシステムがメーターに直接通信する場合には、そこにもリスクが存在する。メーター計量情報、ロードプロファイル情報、アラーム情報などが偽装されるリスクが存在する。

⑤　WAN～中央データコレクタ

メーターあるいはコンセントレータから中央データコレクタへの物理インターフェースに存在するリスク。メーター計量情報、ロードプロファイル情報、アラーム情報などが偽装されるリスクが存在する。

⑥　LAN/WAN/ DC（Domain Controller）～ネットワーク管理者

変電所モニタリングに際して、データコレクタからのデータサービスインタフェースに存在するリスク。ネットワークモニタリングの技術データが漏洩し、メーター計量情報、アラーム情報などに偽装のリスクが存在する。

⑦　LAN/WAN/ DC～配電事業者（DSO：Distribution System Operators）

消費者への電力料金請求とその他の付加サービス用に提供されるデータサービスインタフェースに存在するリスク。メーター計量情報、ロードプロファイル情報、アラーム情報などが偽装されるリスクが存在する。

⑧　家庭用分散電源～配電事業者

負荷マネジメント用の逆潮電力提供量計測とバックホールネットワークの間の物理インターフェースに存在するリスク。メーター計量情報、ロードプロファイル情報、アラーム情報などが偽装されるリスクが存在する。ネットワークモニタリングの技術情報が脅威にさらされる。

⑨　家庭用分散電源～配電事業者

逆潮電力提供量計測とバックホールネットワークの間の物理インターフェースに存在するリスク。消費者請求データが脅威にさらされ、メーター計量情報、ロードプロファイル情報、アラーム情報などが偽装されるリスクが存在する。

⑩　電力小売事業者～サードパーティ

付加的サービスのために電力小売業者から外注される(例えばプリペイドサービス）ことによるリスク。メーター計量情報、ロードプロファイル情報、アラーム情報などが偽装されるリスクが存在する。

⑪　HAN～サードパーティ

エネルギーサービスに関わる(発電業者、送配電業者とは異なる）サードパーティ業者へ家庭からデータが提供されることに存在するリスク。メーター読出し情報、ロードプロファイル情報などが偽装されるリスクが存在する。

⑫　家庭用分散電源～サードパーティ

家庭用分散電源のアグリゲーション(集成)・サービスに伴うリスク。メーター読出し情報、ロードプロファイル情報などが偽装されるリスクが存在する。

⑬　メータ～無線メッシュ

トポロジーに依存したネットワークに存在するリスク。データインスタレーションとインスタレーション時の料金ダウンロードに伴って、メーター読出し情報、ロードプロファイル情報、料金データなどが偽装されるリスクが存在する。

また、他の２つの報告書「Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection: Recommendation to the European Commission」（2011 年 11 月）及び「Cyber Security of the Smart Grids – Summary Report」を含め、重要な勧告・提言は以下のとおりである：

- SMとSGのデータ保護／プライバシーアセスメント及びEU範囲の詳細な関連標準はEU現有のプライバシー及びデータ保護フレームワークだけを用いて実現できるか、もしくは追加の法的枠組みが必要なのかについて更なる作業が必要
- ESOs（CEN、CENELEC及びETSI）は、協定したデータプライバシー及びセキュリティ原則をSG製品及びソリューションの設計中核として強制すべき
- ESOsは欧州基準を基づきSGインターフェースにおける新たなセキュリティ標準を更新・拡張・開発すべき
- 最も適切で、利用可能な暗号方式（AES, RSA, ECCなど）を評価するために更なる作業が必要：
  - ✧ 認証期間（非対称暗号に必要）の創立・運営を可能にさせるビジネスモデルが研究調査中である
  - ✧ 多国間の鍵管理・鍵管理の責任者に関する調査
- ESOsのJWGは新たな標準化活動する前にEG2の勧告及び関連書類をレビューすべき
- ESOsは欧州レベルの鍵管理を考慮しながら、暗号方式の現状の査定、関連技術基準枠組み内一番適切な技術の明示をすべき
- 通信技術やプロトコルにかかわらず、すべての加盟国は同じ鍵管理の共通モデル及びセキュリティ・プライバシー方針（市場実情により手加減が必要だが）を採用すべき
- SMだけでなく、SGにおける他のデバイス（一旦消費データを転送すれば）にもセキュリティ及びプライバシー方針が必要
- 銀行やカード決済などの業界の経験を踏まえながら、欧州標準制定の基礎としてハイレベルのデータ取扱い方針を確定

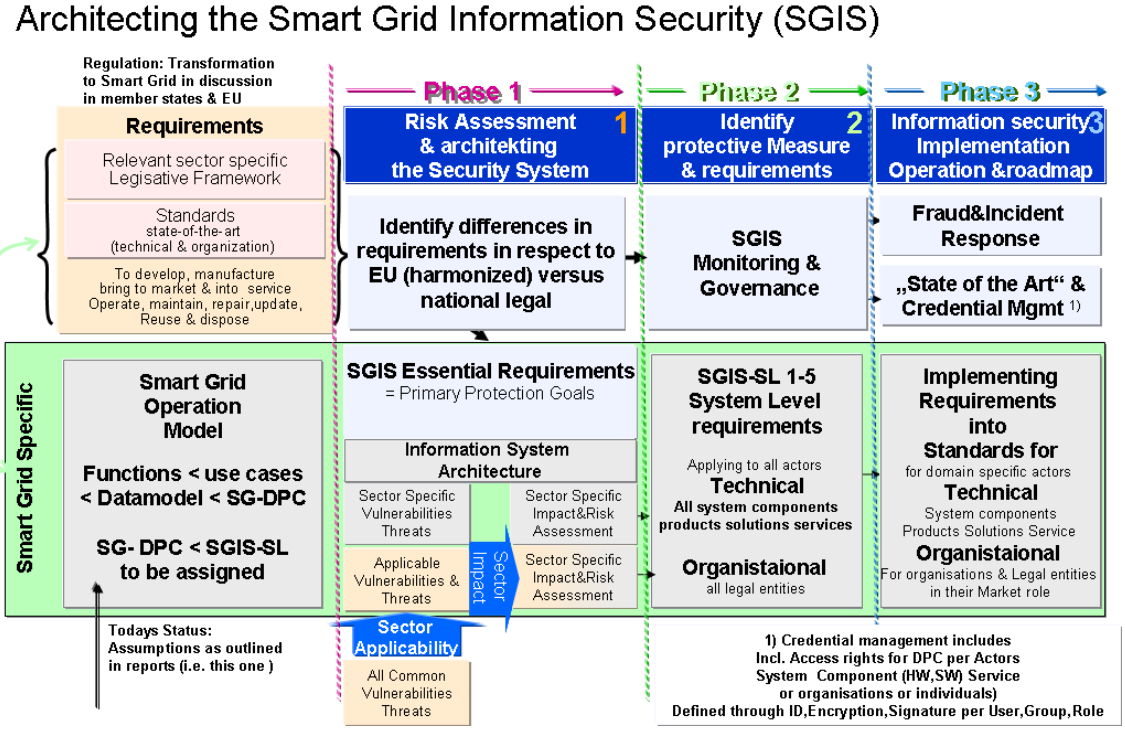
(2)CEN/CENELEC/ETSI SG-CG（元 CEN/CENELEC/ETSI JWG)による提案

①「Standards for Smart Grids」

CEN/CELEC/ETSI JWG の最終報告書「Standards for Smart Grids」（2011 年 6 月）は様々な標準面（参照アーキテクチャ、通信インターフェース、発電、送電、配電、スマートメーターなどを含む）で標準化向けの提言をされている。その中に、情報セキュリティ面のスマートグリッド標準化のために、複数の提言・勧告がなされている。

- 参照アーキテクチャに関する勧告：
  - Ref-4: セキュリティアーキテクチャ：欧州委員会 SGTF EG2 の成果物（報告書など）を踏まえ、 可能な限り適合性評価（Conformity Assessment）アプローチを考慮しながらセキュリティアーキテクチャを開発する。
- スマートグリッド情報セキュリティに係る標準化向けの勧告：
  - リスクアセスメント及びセキュリティシステムの構築
  - 保護措置及び用件の確認
  - 情報セキュリティ実施運用及びロードマップ
  - ISec-1: あらゆる関連標準の中にシステムレベルの情報セキュリティ用件がカバーされることを確保する。

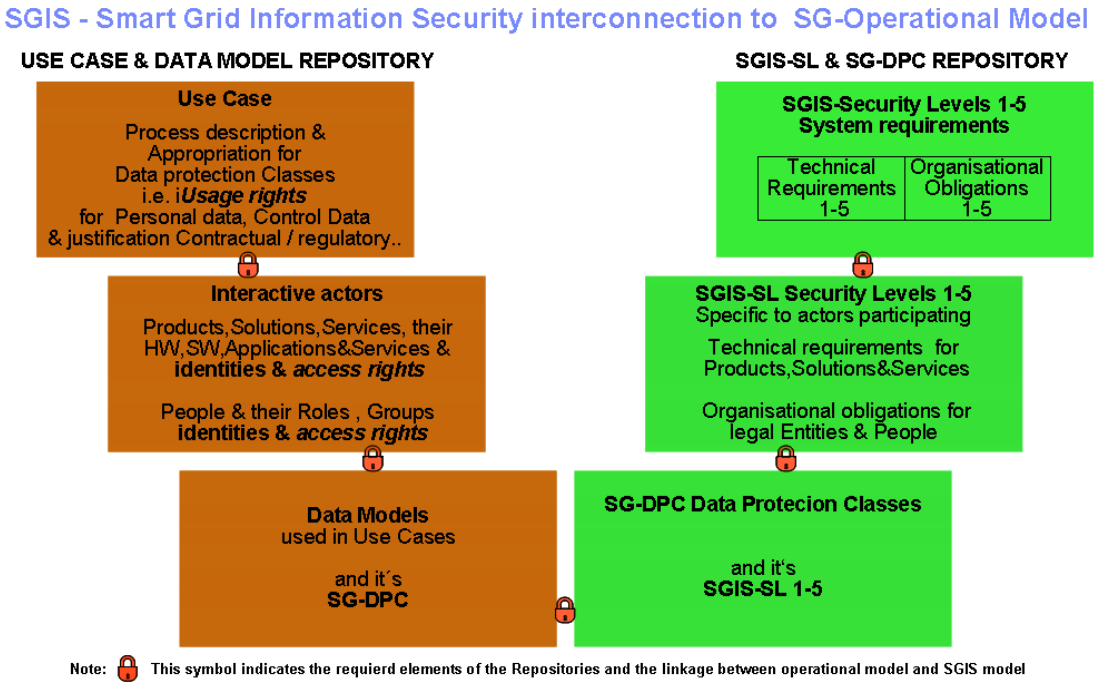
図表付録 7-1　スマートグリッド情報セキュリティのモデリングから実行までのプロセス



出所：CEN/CELEC/ETSI JWG の「Standards for Smart Grids」報告書を基に日本総研作成

- ISec-2: スマートグリッド機能及びユースケースと SGIS 及びデータ保護／プライバシー（DPP：Data pProtection　/ Privacy 要件とのバンディング。
  - ✓ 下図は上記のようなユースケースと UML データモデルレポジトリ、SG-DPC（Data Protection Classes：データ保護クラス）及び SGIS-SL（Security Level：セキュリティレベル）のレポジトリの間の相互リンクプロセス及び相互接続のプロセスについて説明する。

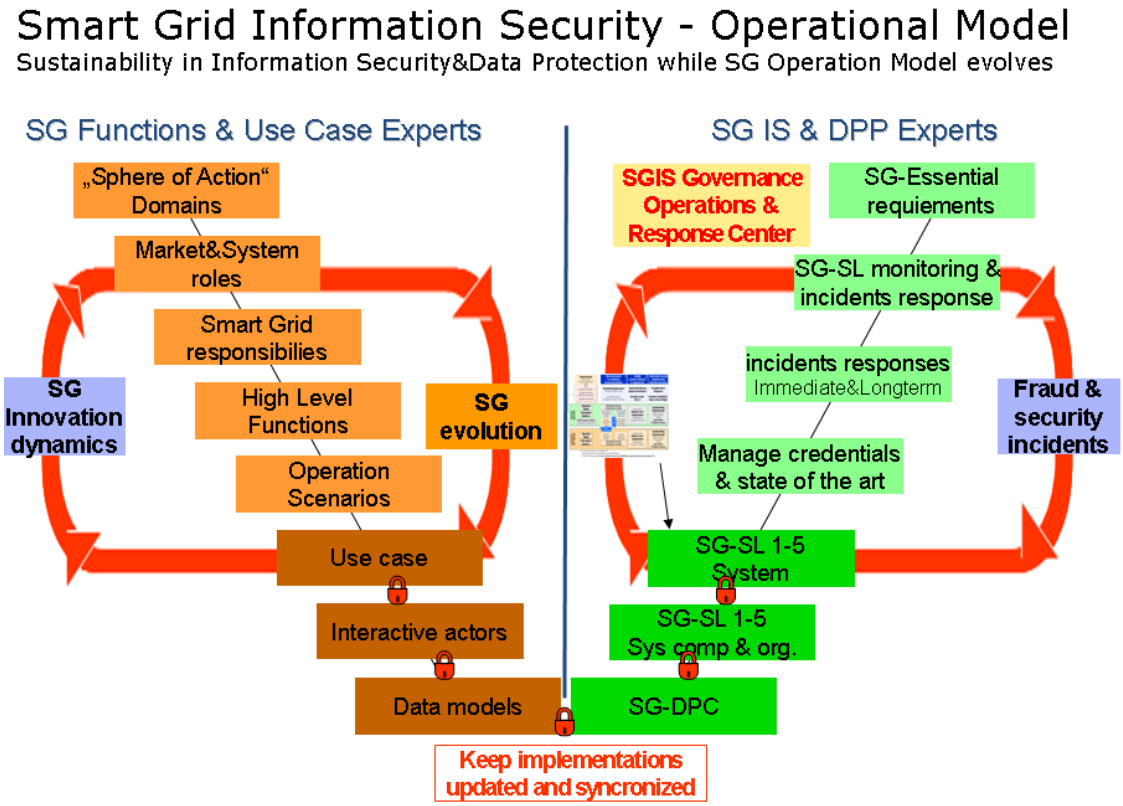
図表付録 7-2　ユースケース及びデータモデルと SG-DPC 及び SGIS-SL



出所：CEN/CELEC/ETSI JWG の「Standards for Smart Grids」報告書を基に日本総研作成

- ISec-3: SGIS-SL 及び SG-DPP 改善及び同期要件：
- ISec-4: ESO は SGIS と DPP のモデリング、また SGIS-SL と SG-DPC のリポジトリをサポートするための IT ツールの提供

図表付録 7-3　スマートグリッド運用モデル全体



出所：CEN/CELEC/ETSI JWG の「Standards for Smart Grids」報告書を基に日本総研作成

②「Smart Grid Information Security」

CEN/CELEC/ETSI JWG の「Standards for Smart Grids」報告書に記載された内容に従い、次代の CEN/CELEC/ETSI SG-CG は「Smart Grid Information Security」という報告書（2012 年 11 月）を公表し、前述のいくつかの勧告・提言に対応した。

まず、スマートグリッド情報セキュリティのセキュリティレベル（SGIS-SL：SGIS Security Levels）を具体的に定義した。その目標は電力グリッドの運用と情報セキュリティの間の架け橋になることである。

図表付録 7-4　SGIS-SL 説明

セキュリティ レベル	セキュリティ レベル名	欧州電力網安定性シナリオ セキュリティレベル例
5	Highly Critical	Assets whose disruption could lead to a **power loss** above **10 GW** **Pan European** Incident
4	Critical	Assets whose disruption could lead to a power loss from above **1 GW to 10 GW** **European / Country** Incident
3	High	Assets whose disruption could lead to a power loss from above **100 MW to 1 GW** **Country / Regional** Incident
2	Medium	Assets whose disruption could lead to a power loss from **1 MW to 100 MW** **Regional / Town** Incident
1	Low	Assets whose disruption could lead to a power loss **under 1 MW** **Town / Neighborhood** Incident

出所：CEN/CENELEC/ETSI SG-CG「Smart Grid Information Security」を基に日本総研作成

また、スマートグリッドデータ保護クラス（SG-DPC：Smart Grid Data Protection classes ）についても詳しく説明する。情報資産があこそセキュリティリスク評価が始まる。スマートグリッドサービス、すなわち共通ユースケース、いくつかのドメイン／ゾーンにわたるため、データモデルは様々な場所において所有者が違っている多様な情報システムをカバーしないといけない。それで、データモデルの分類およびタッグが推奨される。その分類こそはスマートグリッドデータ保護クラス（SG-DPC）であり、それぞれのユースケース及びシステム構成要素のための標準を選択するための適切な SGIS-SL の確認をサポートする。

二種類の SG-DPC は図表 5-8 に示すとおりである。両方とも任意の情報モデル／資産に適用できる。また、情報の CI&A（機密性(Confidentiality)、完全性（Integrity）および可用性（Availability)、責任追跡性（Accountability)、否認防止（Non-repudiation）及び信頼性（Reliability）などのプロパティの保全の必要がある。

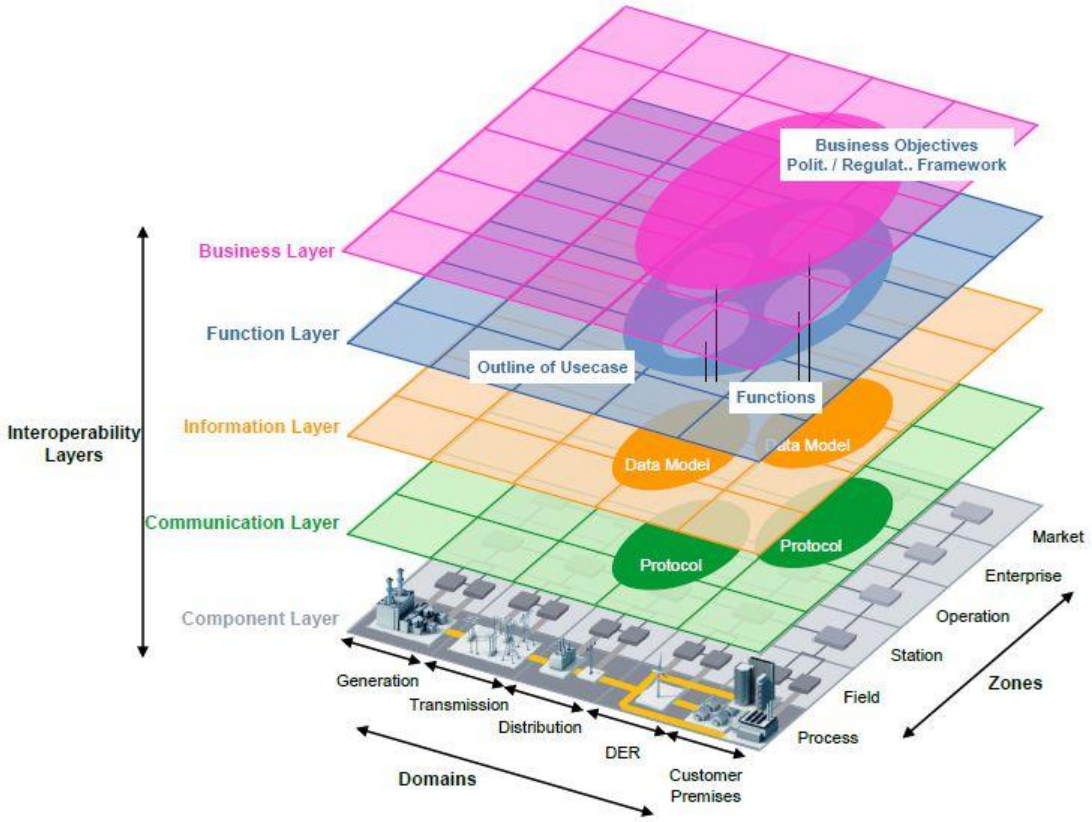
図表付録 7-5　SG-DPC 説明

SG-DPC 1 Personal Information
Sensitive Personal Information
Personal Information
De-personalized Pseudonym zed Personal information
No Personal information

SG-DPC 2 System Information
System Data (i.e. Firmware), Configuration Data, Customer Credentials, Private & Public Keys, Roles /Actor IDs
Governance & Reporting Information, Logging and Audit Information
Audit & Log required information
Information to administrate remotely
Information to operate remotely (Control signals)
Business Information
Measurement data

出所：CEN/CENELEC/ETSI SG-CG「Smart Grid Information Security」を基に日本総研作成

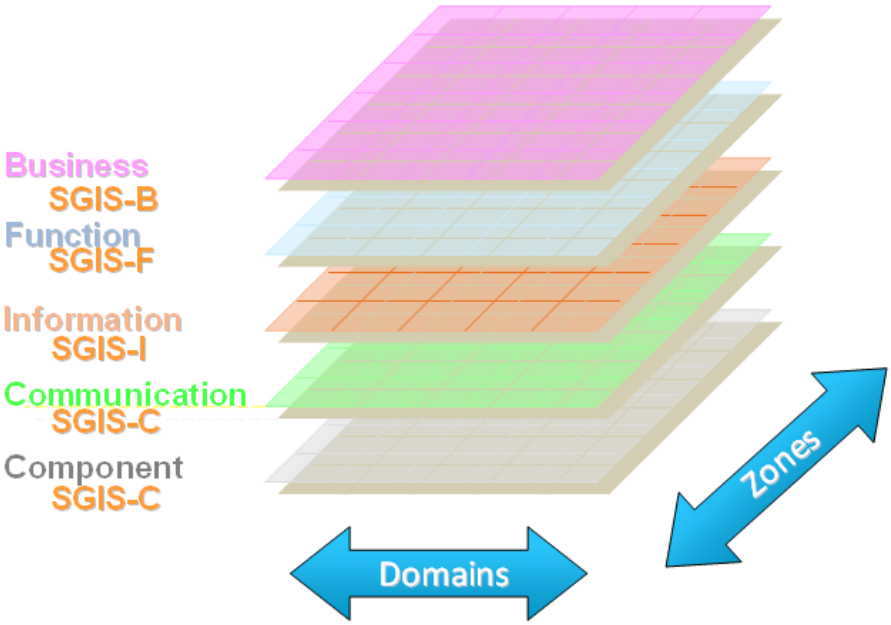
図表付録 7-6　SGAM レイヤ



出所：CEN/CENELEC/ETSI SG-CG「Smart Grid Information Security」を基に日本総研作成

新たに提言されたモデルとして、スマートグリッドアーキテクチャモデル（SGAM：Smart Grid Architecture Model）がある。そのドメインは発電、送電、配電、分散型エネルギー資源（DER：Distributed Energy Resource）、需要家機器（Customer Premise）の 5 つから構成される。またゾーンはマーケット、エンタープライズ、運用、ステーション、フィールドおよびプロセスの 6 つを含む。それらを踏まえ、さらに上から下までビジネス層、ファンクション（機能）層、情報層、通信層、コンポーネント（構成要素）層の 5 つの相互運用レイヤが定義される。

図表付録 7-7　各レイヤにおけるセキュリティ・ビュー

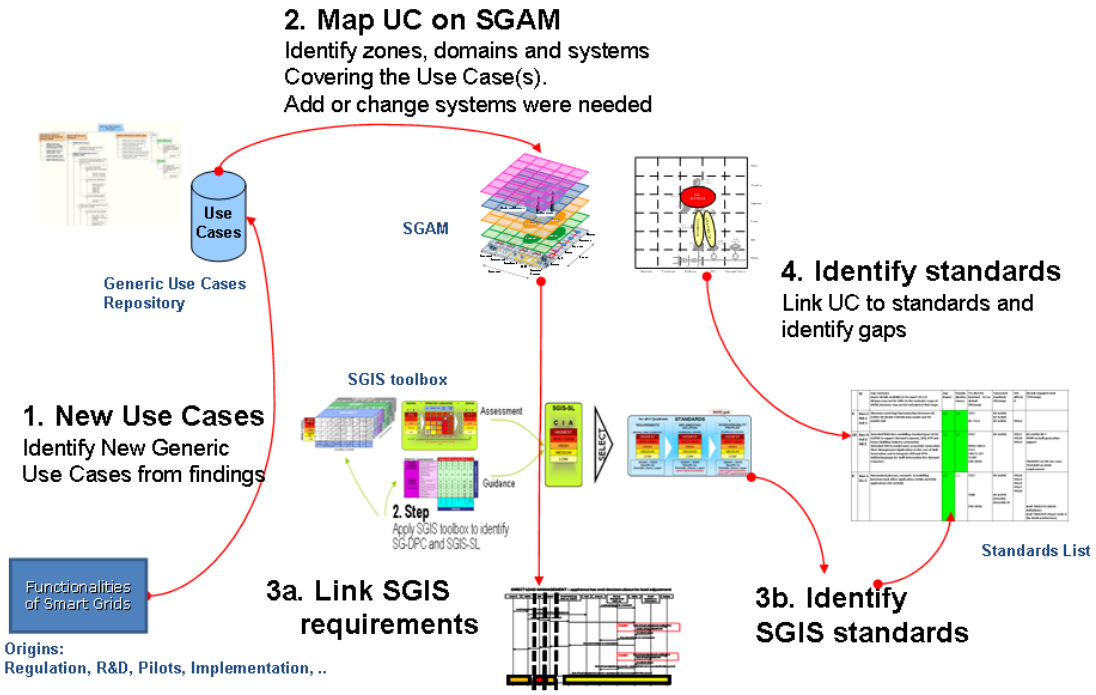


出所：CEN/CENELEC/ETSI SG-CG「Smart Grid Information Security」を基に日本総研作成

このモデルに基づき、特定の資産に対する適切なサイバーセキュリティ対策を立案するためのツールも公開されている（SGIS ツールボックス）。

SGIS ツールボックスは、スマートグリッドユースケースの利害関係者にユースケースにおけるセキュリティニーズを確認するための簡単かつ実用な方法を提供するものである。ツールボックスを用いて、ユースケースの機能及びその機能を遂行するための情報を踏まえ、SGAM をドリルダウン（Drill Down）し、ユースケースがあるべきドメイン、ゾーン及びレイヤを確認する。そして、ユースケースの SGAM 上へマッピングしり。

図表付録 7-8　スマートグリッドユースケース共通フレームワークにおける SGIS ツールボックス説明



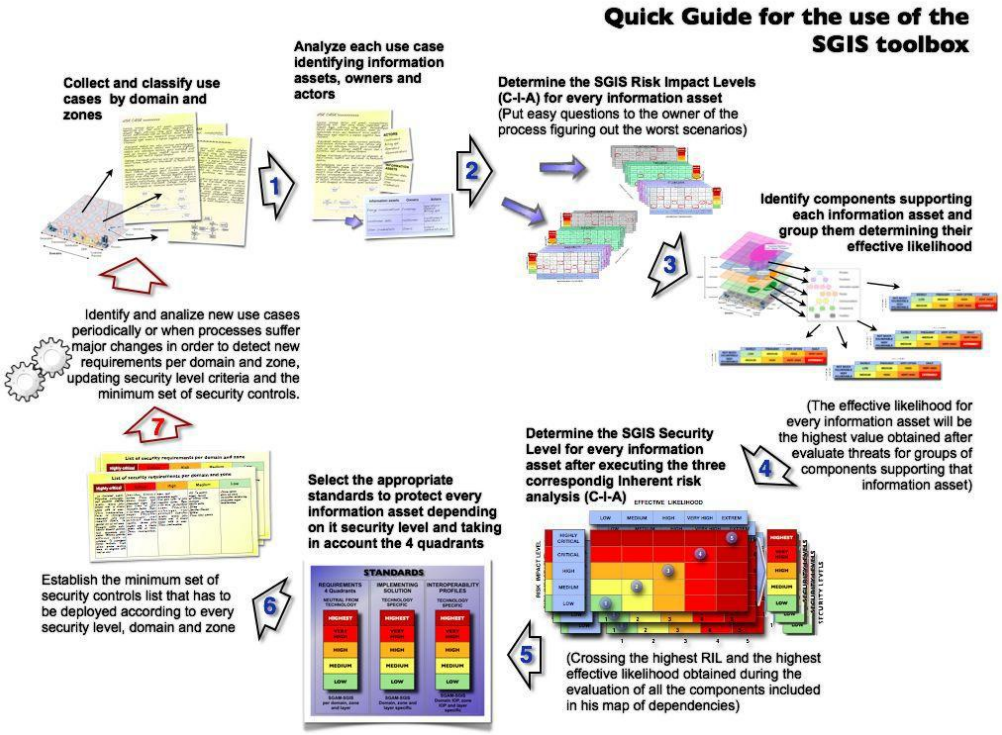
出所：CEN/CENELEC/ETSI SG-CG「Smart Grid Information Security」を基に日本総研作成

レイヤごとのセキュリティ・ビュー、あるいはリスクアセスメントの結果を用いることによって、相互に関係がある各ドメイン／ゾーンが特定され、当該セルに対して要求される SGIS セキュリティレベル（SGIS-SL）を確認することが可能となる。

さらに、特定したセルの SGIS-SL に基づき、NISTIR-7628 のセキュリティガイドラインや、SG-CG/FSS（First Set of Standards Ver. 2.0、2012 年 11 月）のセキュリティ標準リスト[8]（9.3 章に記載）を参考し、セキュリティ要件及びその要件を実現できる標準を特定することが可能となる。

[8] ISO/IEC 27001、ISO/IEC 27002、IEC 62351、NERC/CIP（米国標準）および NISTIR 7628 を参照して策定された標準リスト

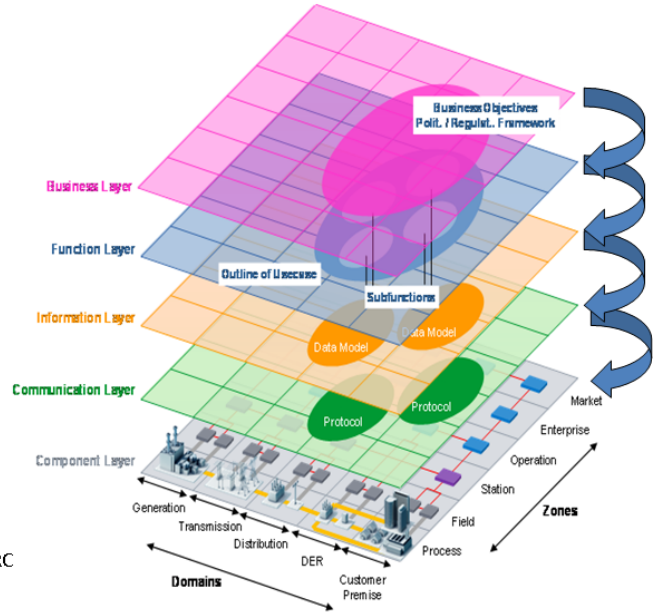
図表付録 7-9　SGIS ツールボックス使用クイックガイド



出所：CEN/CENELEC/ETSI SG-CG「Smart Grid Information Security」を基に日本総研作成

図表付録 7-10　SGAM を用いてユースケースのマッピング

- SGAM defined by European Smart Grid Coordination Group (SG-CG)
- Security consideration in each cell and thus for each interface in the cube → Security views per layer
- Identification of existing security standards (requirements and solutions)
- Identifying gaps for which further standardization work has to be done
- Provide potential improvements for existing standards (current focus lies on ISO 27001, ISO 27002, IEC 62351 which were mapped against security requirements from NERC CIP and NIST IR 7628)



出所：CEN/CENELEC/ETSI SG-CG「Smart Grid Information Security」を基に日本総研作成

なお、本報告書の結論の要点としては以下のとおりである：

- SGIS の基礎となる標準は現在用意されている。
- SGIS のニーズとともに標準が適切に進化するために努力し続けなければならない。その目標を達成するために、SGIS ツールボックスは重要なツールと考えられ、更なる開発及び保守も必要である。
- スマートグリッドの導入時や、認証された命令をスマートグリッド構成要素に発信する時に、常にスマートグリッド重要インフラが公衆ネットワークに接続するリスクについて慎重に検討すべき。
- ヨーロッパにおけるアメリカ ICS-CERT のような組織を設立する必要性が確認される。インシデント管理のサポート、スマートグリッドシステム及び情報セキュリティインシデントにおける情報提供、それぞれに対するレスポンスなどをその組織に委任すべき。

(3)DG CONNECT's Ad-Hoc EG on Smart Grid Security による提案

DG CONNECT's Ad-Hoc EG on Smart Grid Security の報告書は EC の内部資料として公表されなかったが、外部発表資料によりそのグループの活動を通じて下記のいくつかの方面で出された結論、勧告及び推奨を記載する。

- 教育（エネルギー産業におけるサイバーセキュリティ高度人材）
  - ✧ 次世代スマートグリッドインフラを運営できるよく訓練された積極的で前向きで決断力があるオペレーターが不足している。
  - ✧ そのチャレンジを直面するために最新のエンジニア及び ICT に係る教育科目が必要である。

- リスクアセスメント
  - ✧ ICT 分野と電力安全分野の専門家がスマートグリッドセキュリティの設計強化のために協働すべきである。
  - ✧ 有効なセキュリティ対策セットを確認するために、全面的なリスクアセスメントの実行が必要である。シナリオが進化するとともに定期的な再アセスメントが必要である。

- リスクマネジメント
  - ✧ スマートグリッドのための ICT のセキュリティおよび回復性を強化するためにハイレベル・セキュリティ要件の定義が必要である。
  - ✧ セキュリティ特性（機密性、完全性及び可用性）をベースにし、「検知、レスポンス、復旧」（Detection, Response and Resillience）という次元に沿ってセキュリティ要件を完遂する。

- インシデント管理
  - ✧ インシデントの対応及びスマートグリッド（電力網）へのサイバー攻撃により発生する危機の管理を担当する政府機関を指定し、委任する。
  - ✧ サイバーセキュリティのための欧州範囲の戦略策定が必要である

- （公共）調達
  - ✧ プライベートとパブリック両方の資産所有者、ベンダ及び規制者と連携し、スマートグリッド構成要素及びサービスにおける基本レベルのセキュリティのため共通な調達制度や標準のいずれか、または両方を確立する必要がある。

- 経済的刺激の必要性
  - ✧ スマートグリッドに投資する時に関連産業界がサイバーセキュリティを遂行するための経済的刺激を考慮する必要がある。

- 規制フレームワークの改定

- ✧ サイバーセキュリティは電力会社の安全プロセスに統合されなければならない。
- ✧ 政策立案者は規制団体と協働し、標準、セキュリティガイドライン及びコンプライアンス・メカニズムを確立しないといけない。
- ✧ 規制を厳しくした結果、逆効果を起こしかねない規制は避けるべきである。

➢ **セキュリティ及び認証標準**
- ✧ EU 範囲のセキュリティ標準との調和が必要である。

➢ **情報共有**
- ✧ 各分野及び政府間の情報共有、また脆弱性と攻撃者に関する通信及び保安はベンダやエンドユーザーにとって重要である。

➢ **スマートメーターだけでなく、産業制御システムの基本的なサイバーセキュリティにおける中核的な問題の確認.**
- ✧ 情報（システム制御）の完全性及び真正性を確保できる政策が必要である。
- ✧ 制御信号の「バリュー・チェーン」全体にわたる可用性（Availability）、完全性及び真正性は保証される必要がある。

➢ **異なるセキュリティ対策レベル**
- ✧ スマートグリッドインフラの健全性及び回復性の双方に配慮を加えるために、異なっているアーキテクチャ・レイヤに順応する異なるセキュリティ対策レベルが必要である。

➢ **スマートグリッドのサイバーセキュリティ及び回復性向上のための優良実践**
- ✧ スマートグリッドの配置・展開の導入段階からサイバーセキュリティ対策を実施するために、勧告・推奨及び必須要件のベースラインが必要である。
- ✧ 産業自動化制御システム（ICAS：Industrial Automation and Control Systems）及び監視制御とデータ収集（SCADA：Supervisory Control And Data Acquisition）システムのサイバーセキュリティ改竄を防ぐためにガイドライン及び勧告・推奨が必要である。

➢ **サイバーセキュリティに対する C-レベル・アウェアネス**
- ✧ 電力組織／オペレーターの中の意思決定者のサイバーセキュリティに対する認識・意識・アウェアネスを向上させる必要がある。

➢ **セキュリティのための研究開発**
- ✧ End to End のエネルギー供給の責任者とする一連の関連組織のリスク

マネジメント、復旧及び情報セキュリティ上の研究

- ✧ エネルギー供給の End to End の復旧強化及び高度システムベースの罰則・罰金による不正抑制のための政策の有効性に関する研究

- ➢ **サイバーセキュリティ問題はグローバル範囲のため、レスポンスもグローバルにならないといけない**

(4)欧州ネットワーク情報セキュリティ庁(ENISA)による提案

①「Smart Grid Security - Recommendations for Europe and Member States」

ENISA では、スマートグリッドにおけるサイバーセキュリティの重要性を踏まえ、調査研究をはじめ、様々な活動を行っている。その一環として、ENISA ではスマートグリッド関係者を集め、オープンディスカッションの場を設けた。目的は、スマートグリッドのサイバーセキュリティに関する懸念を洗い出し、各加盟国、欧州全体、および国際社会の取組みを認識し、支援することである。成果物として、「Smart Grid Security - Recommendations for Europe and Member States」(「スマートグリッド―欧州及び加盟国向けの推奨・勧告」)を公表する。

本調査では第 1 段階として情報収集、第 2 段階として収集した情報の分析と取りまとめ、推奨施策の勧告を行った。なお、情報収集は、ガイドラインや報告書などの各種資料の調査のデスクワークのほか、オープンディスカッション、アンケートおよびインタビューにより関係者の意見を広く集めた。

調査結果として、100 に及ぶ知見が取りまとめられ(3 章)、これらの知見を基に、スマートグリッドのセキュリティ強化のための 10 の推奨施策を勧告している(4 章)。

図表付録 7-11　ENISA 報告書「Smart Grid Security」の開発方法

出所：ENISA「Smart Grid Security」報告書を基に日本総研作成

デスクワークを基づき研究調査(Desktop Research)の概要は下記のとおりである：

- 230 以上の文書が分析される：
  - ✧ 知名度の高い出版物：技術報告書、専門書籍、優良実践、標準、論文
  - ✧ 他の技術文書：白書、製品／サービス、シーツなど
  - ✧ 最新の情報：フォーラム、メールリスト、ツイッタ、ブログなど

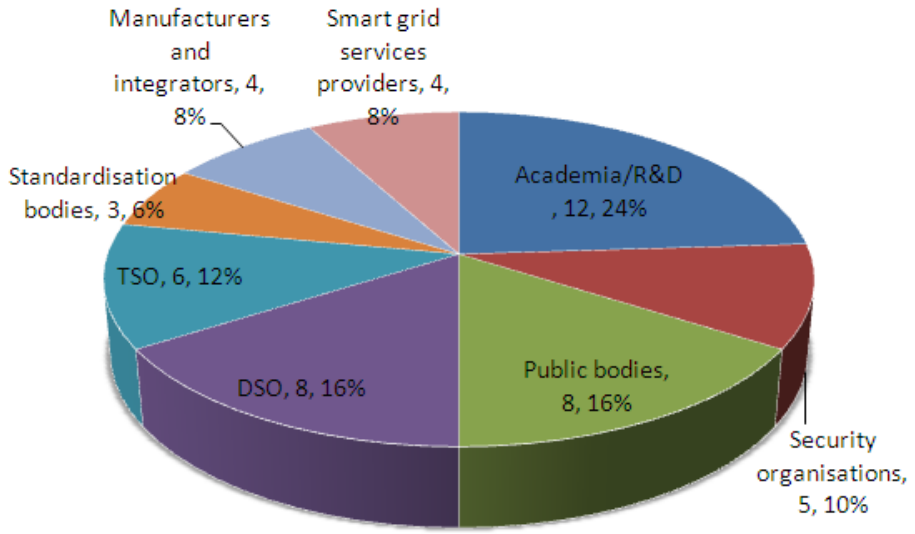
また、アンケート調査及びインタビュー(Survey and Interviews)の概要は

下記のとおりである：

- 304 名の専門家と連絡を取った
- 専門家は以下のようなカテゴリーで分けられる：
  - メーカー及び SIers（Manufacturers and Integrators）
  - セキュリティツール及びサービスのプロバイダー（Security tools and services providers、すなわちベンダ）
  - 配電システムオペレーター（DSO）
  - 送電システムオペレーター（TSO）
  - 発電所（Power generation）
  - スマートグリッドサービスプロバイダー（Smart Grid services provider 、e.g. マーケター）
  - 学術及び研究開発機関（Academia and R&D）
  - 出版団体（Public bodies）
  - 標準化団体（Standardisation bodies）

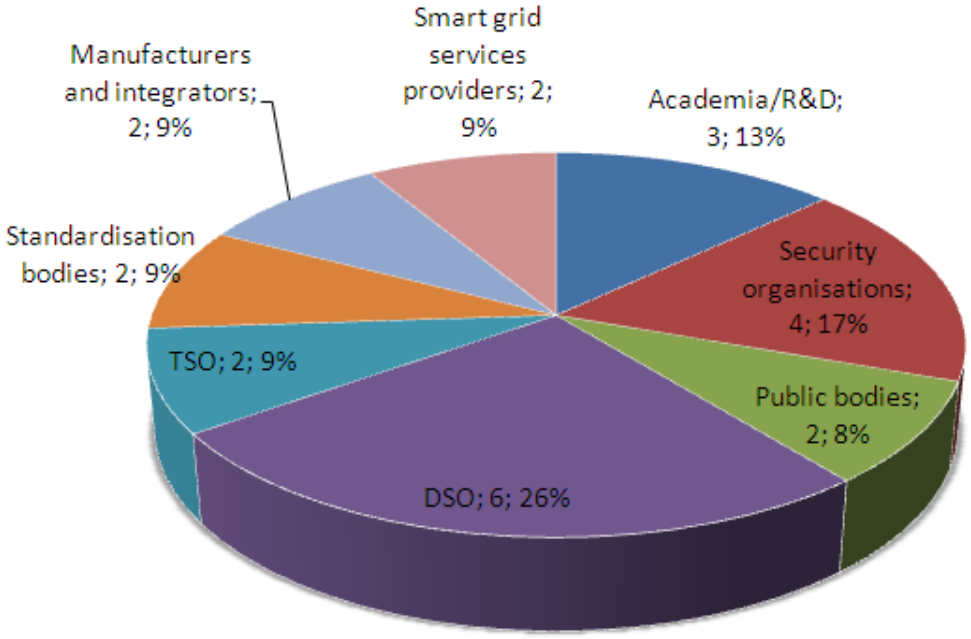
その中に 50 名参与者がアンケートを回答し、23 名参与者がインタビューを受けたといわれる（各内訳は下図表のとおり）。

図表付録 7-12　アンケート回答者の専門家カテゴリーにおける内訳



出所：ENISA「Smart Grid Security」報告書を基に日本総研作成

図表付録 7-13　インタビュー参加者の専門家カテゴリーにおける内訳



出所：ENISA「Smart Grid Security」報告書を基に日本総研作成

この報告書の本編は 7 のメイン章に分けられ、目次は以下のとおりである：

① 概要
② はじめに
  ✓ スマートグリットにおけるサイバーセキュリティ
  ✓ 背景
  ✓ 調査の目的
  ✓ 調査の方法
  ✓ 本報告書について
③ 調査より得られた主な知見
④ 推奨施策
⑤ 結論
⑥ 参考資料
⑦ 略語一覧

また、今回調査研究の結果にかかわる具体的な情報（デスクワークの調査研究のアウトプット詳細や専門家から得た生データの分析など）を収納する 5 つの付録添付ファイルもある：

① 付録Ⅰ：スマートグリッドの概念とICTへの依存
② 付録Ⅱ：スマートグリッドのセキュリティ面
③ 付録Ⅲ：アンケートおよびインタビューの分析
④ 付録Ⅳ：スマートグリッドセキュリティ関連の標準、ガイドライン、規制文書
⑤ 付録Ⅴ：スマートグリッドセキュリティ関連のイニシアティブ

その中に、添付資料１（付録 I）及び添付資料２（付録 II）はデスクワークの調査研究段階の主要結果の代表物である。特に添付資料２の中に、ENISAは大量の情報に基づき、スマートグリッドにおける脅威とそれらの分類されたクラス（技術、会社イメージ及び情報管理、法律、社会面及び人的倫理問題、組織的な問題、国際関係／政治問題、マーケティング／経済的／金融的な問題、環境問題）を分析・整理し、詳しく紹介している。

本編の 3 章に紹介している 100 程度の調査より得られた主な知見は下記のとおり。

- スマートグリッドのセキュリティにおける最大の課題
- スマートグリッドビジネスケース
- スマートグリッドの基本構成
- スマートグリッドの実証実験とサイバーセキュリティ
- セキュアなスマートグリッドの基本要件
- スマートグリッドにおけるサイバーセキュリティ上の課題
- サイバーセキュリティに関する現行のスマートグリッド・イニシアチブ
- スマートグリッドのリスク評価
- 認証制度と国指定の認証機関の役割
- スマートグリッドにおけるサイバーセキュリティ評価
- サイバー攻撃への対応
- スマートグリッドセキュリティ分野における調査研究
- 産業制御システムの推奨セキュリティ施策（ENISA 報告書）

代表的な知見（問題点に対する指摘など）の詳細は以下のとおりである。

- 標準参照アーキテクチャが欠如している
- サイバーセキュリティとプライバシーは分けて議論している
- サイバーセキュリティは ICS-SCADA 及びスマートグリッドのパイロット及び大規模配置・展開する際に、主要な問題とされていない
- 具体的なアセスメント方法論が必要である
- 統一される欧州範囲セキュリティ認証プロセスが欠如している
- オペレーター、メーカー及び需要家の意識向上・訓練が必要である
- セキュリティに係る努力はスマートメーターだけにフォーカスではなく、サブステーション自動化、マイクログリッド、SCADAや遠隔通信ネット

ワークなどにも必要とされる。

- ICS-SCADA、スマートグリッドサイバーセキュリティおよびプライバシーイニシアチブにおける取りまとめる実体が必要である
- インシデント管理上の規制が必要である
- 大規模サイバーセキュリティインシデントに対応できる欧州の実体が必要である
- サイバーセキュリティ、プライバシーおよび不正防止がスマートグリッドの成功にとって非常に重要である
- 深層防御のコンセプトが重要である
- エンドユーザー・プロパティの集積化＋頻繁な ICT 使用＋インターネット及び公衆ネットワークの利用により、攻撃暴露リスクが高まる（Attack Exposure）
- 信頼性（Reliability）および回復性（Resiliency）はスマートグリッドビジネスケースにおいて重要な問題である。
- スマートグリッドの定義の欠如：需要家側管理などを含むべきか否か
- 需要家内のインフラは DSO や他のサービスプロバイダーのコントロール外であるため、セキュリティについて頑健性が求められる
- 専門知識及び予算の不足はサイバーセキュリティが棄却される根本的な原因になりかねない
- いくつかの技術上の課題が存在する：
  - ✧ レガシーシステムの統合
  - ✧ デバイス保安
  - ✧ 活動監視
- 存在しない／不完全な規制はセキュリティ問題になる（例：メーターのロールアウトが早すぎる問題やガス・熱及び電力統合によって生じるリスクなど）
- DSO と TSO は、自身の活動範囲において強制的なリスク評価を行うべき
- 国指定の認証機関（NCAs : National Certification Authorities）はスマートグリッド関連製品および関連組織に対するセキュリティを認証すべき
- スマートグリッド技術が未熟であるため、現在の標準で活用されているセキュリティ認証は負担になりかねない
- サイバーセキュリティは頑健性、信頼性および回復性を基に評価すべき
- 不遵守を防ぐために規制圧力が必要である
- 敏感な（秘密）情報が漏洩しない限りにおいて、セキュリティガイドラインへの遵守／不遵守に対する調査結果の公表が必要である。
- TSO および DSO 常にインシデント対応力の向上が必要である。
- DSO および TSO はサイバーインシデントの検知を担当すべき（IRRIS FP7 project）
- オペレーターのサイバーインシデント報告を義務化にするべき
- ＥＵ全体として大規模サイバーセキュリティ事故対応を担当する機関の必要性について議論が必要

- コンピュータ緊急対応チーム（CERTs：Computer Emergency Response Team）がインシデント管理を行うべき

これらの議論に基づき、4 章で下記のとおり十の推奨施策・勧告が提案される：

推奨施策 1：規制の枠組み・政治的枠組みの改善（R1: Improve the regulatory and policy framework on SG cyber security）
推奨施策 2：スマートグリッドのサイバーセキュリティ関連イニシアティブを取りまとめるのために、官民パートナーシップ（PPP）機関の設立促進（R2: Creation of a PPP entity to coordinate smart grid cyber security initiatives）
推奨施策 3：認識向上・訓練イニシアティブの促進（R3: Awareness rising and training）
推奨施策 4：知識の共有・発信イニシアティブの促進（R4: Dissemination and knowledge sharing）
推奨施策 5：最低基準・対策・ガイダンスの策定（R5: Develop a minimum set of reference standards, measures & guidelines）
推奨施策 6：製品・組織向けセキュリティ認証制度の確立促進（R6: Promote the development of security certification schemes）
推奨施策 7：テストベッド・セキュリティ評価手法の開発促進（R7: Foster the creation of test beds and security assessments）
推奨施策 8：電力網に影響を及ぼす欧州規模のサイバーインシデントに対応するための戦略の見直し（R8: Refine strategies to coordinate large scale pan-European cyber incidents）
推奨施策 9：電力網に影響を及ぼすサイバーセキュリティ問題に関する、CERT への協力要請（アドバイザー参加要請）（R9: Involve CERTS to play an advisory role）
推奨施策 10：既存の研究開発プロジェクトを活用し、スマートグリッド研究開発の促進（R10: Foster R&D in SG cyber security leveraging existing research programs）

②「Appropriate security measures for smart grids – Guidelines to access the sophistication of security measure implementation」

ENISA が「Smart Grid Security」報告書を発表した後、さらなる調査を行い、スマートグリッドの施設及びサービスのセキュリティ及び回復性を向上させるために、スマートグリッドサイバーセキュリティ対策のの確立に取り組んだ。成果物としては「Appropriate security measures for smart grids - Guidelines to access the sophistication of security measure implementation」である。

その技術文書は「Smart Grid Security」と違い、最低限（かつ適切な）セキュリティ対策セットの確立を通じてスマートグリッドの利害関係者へサイバーセキュリティサービスの最低水準を改善できるガイダンスを提供する。提案される 38 のセキュリティ対策は 10 のドメイン及び 3 のソフィスティケーション・レベルで分けられる。通用でき、広範囲で採用されることが可能なスマートグリッド問題に対応するアプローチを実現するために、それらの対策を策定する間に ENISA は常に「スマートグリッド界の様々な利害関係者の合意及び協力」を求める。そのような利害関係者の種類は下記のとおりである：

- 規制及び政策制定者
- スマートグリッド・オペレーター
- 標準化機構（e.g. ETSI、NIST、IEC、ISO など）
- セキュリティソリューションプロバイダー
- スマートグリッド製造者
- 学術及び研究開発機関
- スマートグリッドサイバーセキュリティに係る加盟国の公共団体

対策開発の方法として、最初の段階で大規模なデスクワークの研究調査を通じてスマートグリッドセキュリティ実践に係る既存のフレームワーク及び標準の現状調査を行う。同時に、スマートグリッドの実際のオペレーターと共にリスクアセスメントを行う。その後、コンプライアンスベースではなく、リスクベースでバースラインとなる適切な対策を抽出する。さらに、各対策に対して 3 の実施ソフィスティケーション・レベルの設定し、其々の調整・対応を説明する。

デスクワークのとき選ばれた重要文書は下記の通りである：

- NISTIR 7628: Guidelines for Smart Grid Cyber Security
- ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management
- ISO/IEC DIS 27036-2: Information technology - Security techniques - Information security for supplier relationships, Part 2: Requirements

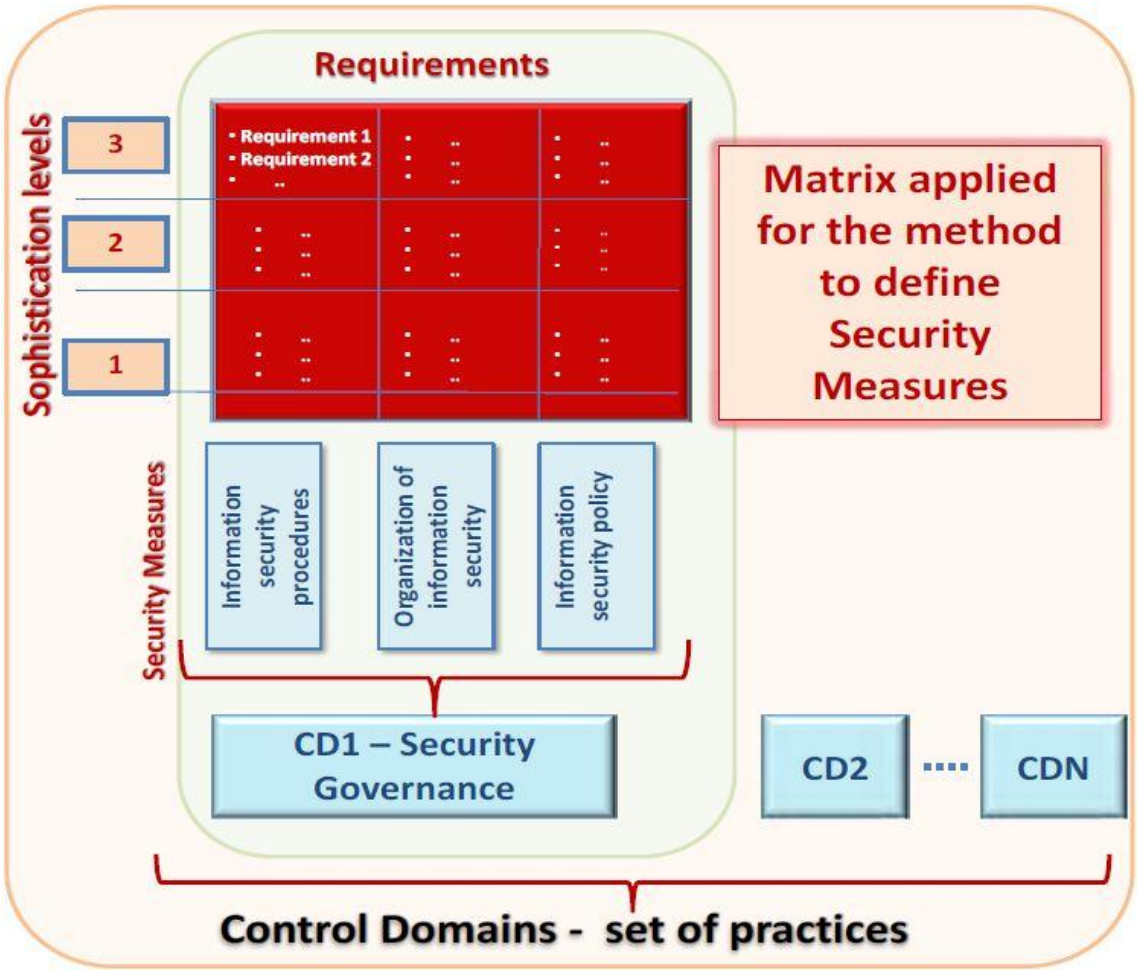
- ISO/IEC 27011: Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- NERC CIP
- IEC 62443: Technical Specification - Industrial Communication Networks - Network and System Security
- IEC 62351: Power Systems Management and Associated Information Exchange – Data And Communications Security
- ISO/IEC TR (Technical Report) 27019: Information technology - Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry
- BDEW (Bundesverband der Energie- und Wasserwirtschaft) - White Paper Requirements for Secure Control and Telecommunication Systems

報告書の各章の概観は下記のとおりである：

- 1 章－はじめに：スマートグリッドコンテクスト及び本調査の動機が紹介される。また、本調査に使われる専門用語及び方法論も説明する。
- 2 章－適切なセキュリティ対策：スマートグリッドセキュリティのための具体的なセキュリティ対策の開発プロセスが紹介された。また、スマートグリッドコンテクストを踏まえ、抽出されたドメイン及び其々に適切な関連セキュリティ対策についても説明する。
- 3 章―ソフィスティケーション・レベル：確認されたセキュリティ対策のリスト及び各ドメインのために定義されるソフィスティケーション・レベルで分類されたエビデンスが紹介される。
- 4 章－適切なセキュリティ対策のカタログ：定義されたセキュリティ対策をまとめる表が含まれる。
- 5 章－ISO/IEC-27002、NISTIR-7628 及び ISO/IEC TR 27019 へのマッピング：定義されたセキュリティ対策と ISO/IEC-27002、NISTIR-7628 及び ISO/IEC TR 27019 標準の関係を示す表が含まれる。

下記のマトリクスにドメイン及びソフィスティケーション・レベルにより SG セキュリティ対策の整理型を示す。

図表付録 7-14　対策開発方法の概念モデル



出所：ENISA「Appropriate security measures for smart grids」報告書を基に日本総研作成

「Appropriate security measures for smart grids」報告書は 10 のドメインにおける具体的なセキュリティ対策からプラクティスまで詳しく紹介される。

① セキュリティガバナンス及びリスク管理（Security governance and risk management）
- ✓ **説明**：このドメインにおけるセキュリティ対策はスマートグリッド利害関係者のセキュリティポリシーと一致する適切な実行を促すために策定される。
- ✓ **コントロール目標**：プロバイダーはスマートグリッドセキュリティを指導・コントロールするセキュリティ管理プログラムの確立・維持する。そのプログラムは戦略的な方向性を提供したり、目標の実現、スマートグリッドシステム及び構成要素におけるサイバーセキュリティリスクの十分説明、責任を持って組織リソースの利用を確保したり、セキュリティプログラムの成敗を監視したりする。また、そのプログラムは内部リスクだけでなく、適切に ICT 及びエネルギーサプライチェーンからのリスクも確認すべきである。

② 第三者管理（Management of third parties）
- ✓ 説明：このドメインのセキュリティ対策は第三者にかかわるものであり、スマートグリッド・オペレーターが本当で持続可能なスマートグリッドへの統合を支えるためである。
- ✓ **コントロール目標**：プロバイダーはセキュリティ関連問題におけるスマートグリッドバリューチェーンに参入したスマートグリッドの利害関係者との合意を含む第三者管理プログラムを確立る。その合意にもサプライチェーンを考慮すべきである。

③ スマートグリッドのコンポーネント／システム及びのためのライフサイクル・プロセス及び操作手順の保安（Secure lifecycle process for smart grid components/systems and operating procedures）
- ✓ **説明**：このドメインに含まれる活動や手続きはスマートグリッド構成要素及びシステムのライフサイクル（運用、環境設定、保守及び廃棄）保安にかかわる。それで、このドメインのセキュリティ対策はスマートグリッド情報システムやコンポーネントの適切な環境設定、また変更管理手続きなどを考えなければならない。
- ✓ **コントロール目標**：プロバイダーはスマートグリッド構成要素／システム及び手続の計画、要件定義、開発、配置・展開、環境設定、運用及び廃棄の一連を含むライフサイクル保安プロセスを確立・維持する。

④ 個人の安全、意識及び訓練（Personal security, awareness and training）
- ✓ **説明**：このドメインのセキュリティ対策は、スマートグリッドにおける信頼できる運営を行うため、スマートグリッドを運営する組織の従業員が十分な訓練を受けることを確保する。

- ✓ **コントロール目標**：プロバイダーはすべての関連利害関係者のサイバーセキュリティをサポートしたり、電力セクター間のセキュリティ情報の相互交換及びスマートグリッドバリューチェーンの情報セキュリティ専門家を育成したりするための個人セキュリティ、意識及び訓練プログラムを確立・維持する。

⑤ インシデント・レスポンス及び情報知識共有（Incident response and Information knowledge sharing）

- ✓ **説明**：このドメインは潜在的な妨害やインシデントに有効的なレスポンスができるために、スマートグリッドに影響可能な脅威、脆弱性及びインシデントをカバーする。
- ✓ **コントロール目標**：プロバイダーは損害を有効的に含んでサイバー事件の予防、解決及び事件からの復旧、また内部・外部実体のためのサイバーセキュリティ情報共有を許すインシデント・レスポンス及び情報・知識共有プロセスを確立・維持する。

⑥ 監査・会計（Audit and accountability）

- ✓ **説明**：このドメインがエネルギー及びスマートグリッドに特化した法定基準及び組織政策に対するコンプライアンスを確認するために、監査・会計ポリシー及び関連規制の実施をカバーする。
- ✓ **コントロール目標**：プロバイダーは　スマートグリッドシステム及び構成要素における十分な記録能力（Log Capability）を可能にさせ、分析のための貴重な記録データを提供できる監査・会計プロセスを確立・維持する。

⑦ 運営の連続性（Continuity of operations）

- ✓ **説明**：このドメインのセキュリティ対策は災害、脅威及び意外な事件を含む幅広い状況の中にスマートグリッドの基本機能を確保する。
- ✓ **コントロール目標**：プロバイダーは正常システム運用が妨害される事件においてもスマートグリッド情報システムの運営を続ける／再開させることが可能のような運営プロセスの連続性を確立・維持する。

⑧ 物理的セキュリティ保護（Physical security）

- ✓ **説明**：このドメインはスマートグリッド資産のための物理保護要件をカバーする。
- ✓ **コントロール目標**：プロバイダーは権限がある人しかスマートグリッド情報システムにアクセスできないことを確保できる物理的セキュリティプログラムを確立・維持する。

⑨ 情報システムセキュリティ（Information systems security）（ドラフトの時には、「アクセス管理」である）

- ✓ **説明**：このドメインはファイアーウォール、ウイルス対策ソフトウェ

ア、侵入検知などの様々な技術を用いてスマートグリッド情報システムに管理された情報を保護するための要件定義をカバーする。

- ✓ **コントロール目標**：プロバイダーは権限を授けられた実体しかスマートグリッド情報システム及び構成要素には論理的にアクセスできなく、またそれらの情報が確実に保護される情報システムセキュリティコントロールを確立・維持する。

⑩ ネットワークセキュリティ（Network security）

- ✓ **説明**：このドメインはスマートグリッド情報システムと、ビジネス用及び産業用ネットワークの間のセグメンテーションの間に設置される通信チャネルを保護するための要件設計・実施をカバーする。
- ✓ **コントロール目標**：プロバイダーはセキュリティコントロールが迂回されないような安全なネットワーク工学プログラムを確立・維持する。

各確認されたセキュリティ対策は異なるソフィスティケーション・レベルで実施することができる。セキュリティ・プラクティスの有効実施をチェックするために、各レベルにはデザイン及び提供すべきエビデンスの妥当性を評価するためのプラクティスが含まれる。それらのレベルの説明は下記図表のとおりである：

図表付録 7-15　ソフィスティケーション・レベルの説明

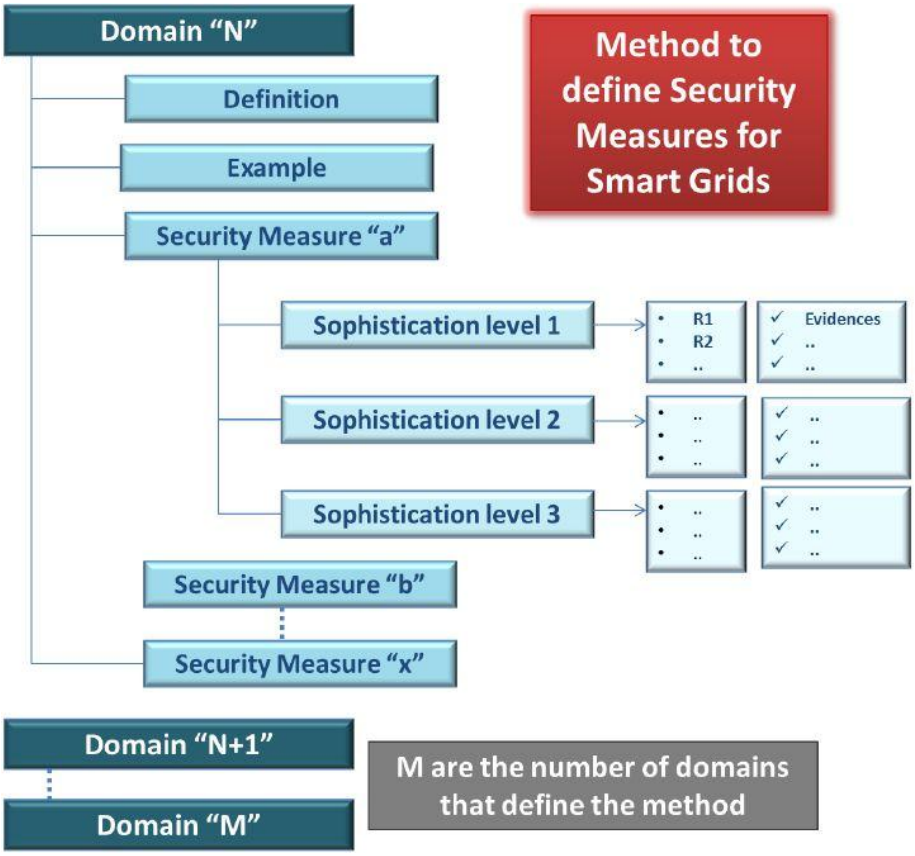
ソフィスティケーション ・レベル	説明
1	セキュリティ対策は早い段階で実行される（事前ではなく）。セキュリティ目標はある程度達成される。
2	セキュリティ対策は産業標準にしたがって組織の大部分で実行される。セキュリティ目標は達成され、有効性は時々（ad-hoc）調べられる。
3	セキュリティ対策はアドバンスド方法で実行され、連続的に監視／テストされている。定期的にそれらのセキュリティ対策を構造ベースにレビューし、またビジネス目標をサポートする必要であれば、最適可能な方式で更新する。演習及びテストは対策有効性検証のために計画される。

出所：ENISA「Appropriate security measures for smart grids」報告書を基に日本総研作成

図表付録 7-16 はスマートグリッドセキュリティ対策を定義するための共通方法の概観である。ソフィスティケーション・レベルはそれぞれ独立して各ドメインに当てる。結果として、スマートグリッドプロバイダーは異なるドメインにより異なるソフィスティケーション評価を受けかねない。ある組織に適用できるソフィスティケーション・レベルはその組織の規模や提供されるサービスなどの組織特性次第であるという認識は重要である。例えば、5 人しかいないプ

ロバイダーのために、業界最善実践標準と提携するセキュリティポリシーや人事のための文書化された正式な手続きは必要ではないとされている。

図表付録 7-16　スマートグリッドセキュリティ対策を定義するための共通方法概観



出所：ENISA「Appropriate security measures for smart grids」報告書を基に日本総研作成

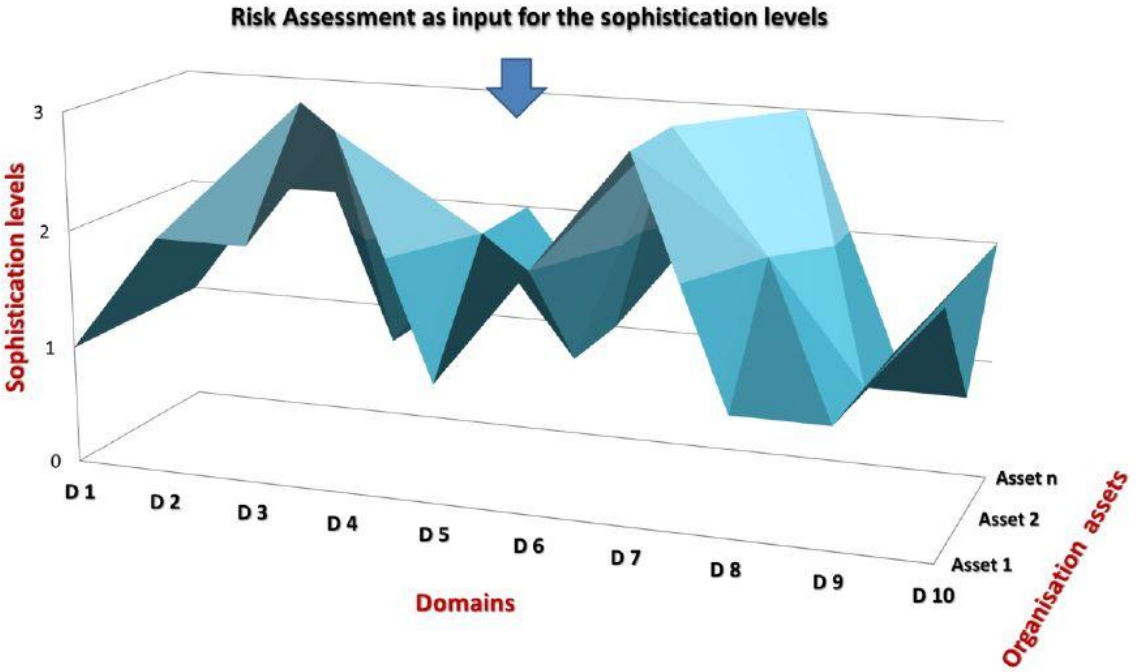
報告書「Appropriate security measures for smart grids」に定義されるセキュリティ対策と NISTIR-7628 に提供されるセキュリティ要件の関係は付録に示される。

また、補足として、ENISA はリスクアセスメントの対策決定における役割について下記の通りで説明する：

- リスクアセスメントは　スマートグリッドシステム設計者がリスク値を決める前に、最低限容認度のために閾値を設定すること、またスコープ内の資産のためのリスクアセスメントを実施することを可能にさせる。そのため、リスクアセスメントは一つの重要予備段階であり、　スマートグリッド組織に必要とされるソフィスティケーション・レベルによってリスクレベルを決める前に、各組織にどんなリスクレベルが適切／受入れ可能なのかについて理解するために実施すべきである。次表の通りに、リスクア

セスメントはソフィスティケーション・レベルを決めるとき有用なインプットという位置づけである。

図表付録 7-17　ソフィスティケーション・レベル決定における役割



出所：ENISA「Appropriate security measures for smart grids」報告書を基に日本総研作成

したがって、組織はリスクアセスメントの結果を考えて有効的に利用した上で具体的なコントロール、対策及びソフィスティケーション・レベルを選択すべきである。そうすれば、提案されるスマートグリッドセキュリティ対策は、セキュリティマネジャーがどこのセキュリティに注目すべきか、また彼らの各組織内のセキュリティ対策優先度について決めることができるようで適切なベンチマークと考えられる。

(5)その他のガイドライン

欧州範囲で系統的なスマートグリッドサイバーセキュリティ関連の標準・ガイドライン・規制がまだ存在していないが、加盟国の国内の基準としていくつかある。代表的なのは以下のとおりである：

名前	Privacy and Security of the Advanced Metering Infrastructure
種類	ガイドライン（ベストプラクティス）
グループ／イニシアティブ／組織	Netbeheer Nederland Privacy and Security Working Group
状態	最終（バージョン1.5）
発行年月	2009年9月
対象となる読者	
メーカーやSIer	1
セキュリティツール及びサービスプロバイダー（ベンダ）	2
配電システムオペレーター(DSO)	2
送電システムオペレーター（TSO）	1
小売エネルギー業者	0
学術・研究開発機関	0
対象になる産業	全産業通用
関係地域	オランダ

名前	VGB R175. IT security for generating plants
種類	ガイドライン（優良実践）
グループ／イニシアティブ／組織	VGB Group
状態	最終
発行年月	2006年5月
対象となる読者	
メーカーやSIer	1
セキュリティツール及びサービスプロバイダー（ベンダ）	2
配電システムオペレーター(DSO)	0
送電システムオペレーター（TSO）	2
小売エネルギー業者	0
対象になる産業	発電
関係地域	ドイツ

名前	Managing Information Security in an Electric Utility
種類	ガイドライン（技術報告書）
グループ／イニシアティブ／組織	CIGRE, JWG D2/B3/C2-01 Security for Information Systems and Intranets in Electric Power Systems
状態	最終
発行年月	2005年9月
対象となる読者	
メーカーやSIer	1
セキュリティツール及びサービスプロバイダー（ベンダ）	2
配電システムオペレーター(DSO)	2
送電システムオペレーター（TSO）	2
小売エネルギー業者	1
学術・研究開発機関	0
対象になる産業	配電／送電
関係地域	フランス

（6）ENISA によりスマートグリッドにおける脅威とそれらの分類

ENISA は「Smart Grid Security：Recommendation for Europ and Member States」報告書の中に、スマートグリッドが直面している脅威を分析し、さらにそれらを以下の 7 つのクラスで分類する：

① 技術
② 会社イメージ及び情報管理
③ 法律、社会面及び人的倫理問題
④ 組織的な問題
⑤ 国際関係／政治問題
⑥ マーケティング／経済的／金融的な問題
⑦ 環境問題

脅威分類	
クラス	脅威
技術	Malware
	Non optimised processes
	Weak innovation
	Manipulation of device's internal electronics
	Physical manipulation of devices' subcomponents
	Removable component replacement
	Manipulation of home devices
	Unauthorised firmware replacement
	Compromised firmware update
	Escalation of privileges
	Sensible information interception
	Alteration of information in transit
	Traffic injection
	Sensible information theft
	Credentials discovery
	Partial denial of service
	General denial of service
	Breakdown
	Propaganda
	Disclosure of information
	Disinformation
会社イメージ及び情報管理	Low quality information for decision making
	Damage to Brand Image/reputation
	Rumour
	Bad patenting policies and procedures
	Weak knowledge of regulations
	Lack of comprehensive insurance coverage
	Unfavourable contractual agreements
法律、社会面及び人的倫理	Non compliance with national and international regulations
	Strike
	Sabotage
	Retention
	Faked sickness
	Incompetence

	Bribery
	Dishonest behaviour
	Employee unreliability
	Error
	Illicit action
	Panic
	Epidemics
	Penuries
組織的な問題	Weak internal controls
	Not respected management
	Procedures are not followed
	Illness
	Badly controlled outsourcing
	Low morals
	Labour accidents
国際関係／政治	War
	Terrorism
	Regional conflict
	Organised crime
	Kidnapping
	Government corruption
	Mass psychoses
	Group anarchy
	Riots
マーケティング／経済的／金融的な問題	Volatile market
	Product/service boycott
	Unsuccessful merger/acquisition
	Bad product/service performance
	Non adapted product
	Unsatisfied client
	Bad strategic decisions
	Client dependence
	High competition
	Interrupted production
	Negative Return on Investment (ROI)
	Debt
	Low capital
	Demands of shareholders
	Untrustworthy financial sources
	Slowdown in economic growth
	Fraud
	Insufficient resources
環境	Natural catastrophe
	Pollution
	Nuclear catastrophe
	Biological disaster
	Chemical disaster
	Radio-electric incident

(7)ENISA が提案する 10 の推奨施策・勧告詳細

ENISA が提案する 10 の推奨施策・勧告詳細は下記の通りである：

- 推奨施策・勧告 1. 欧州委員会（EC）及び加盟国（MS）の監督当局はスマートグリッドサイバーセキュリティにおける国及・EU レベルの規制の枠組み・政治的枠組みの改善に取り組むイニシアティブを担当すべきである。

  - 重要側面：
    - 明確な書類及び規制の開発
    - SG のための汎欧州サイバーセキュリティ戦略の基本原則、チャレンジ、目標及びニーズの定義
  - 規制の枠組みに求められるのは以下のとおりである：
    - プライバシーと共にサイバーセキュリティを検討すること
    - 現時点 SG 配置・展開のためのセキュリティ目標の定義（e.g. スマートメーターのロールアウト）
    - 強制的なリスクアセスメント
    - 製品及び組織のためのセキュリティ認証
    - 従わない会社のための規制的な圧力（罰金など）
    - コンプライアンスの結果の公表
    - サイバーセキュリティインシデントの報告

- 推奨施策・勧告 2：ENISA 及び加盟国の協力を得ながら、EC はスマートグリッドのサイバーセキュリティ関連イニシアティブを取りまとめるのために、官民パートナーシップ（PPP）機関の設立を促進すべきである。

  - 重要側面：
    - 全ての SG サイバーセキュリティ・プライバシー問題に携わるイニシアティブの EU レベルの唯一の中央協調存在（Central Coordinating Entity）
    - EU 及び加盟国の官民連携
    - SG サイバーセキュリティにおけるグローバル視野を持つ EU 及び加盟国のイニシアティブ（SGIS、DG CONNECT's ad-hoc EG, …）
  - 目標:
    - 重複の作業を避ける。
    - タスクフォース及びワークグループの間の交流を促進する。
    - 現有の／将来のイニシアティブのための明確かつ統一のストラテジーを定義する。
    - 加盟国及び欧州のイニシアティブ間の協働を確認する。
    - 進行中の取り組みを広く周知する。
    - 技術用語の共通辞書の作成
    - 利益代表管理

- 推奨施策・勧告 3：ENISA 及び EC は認識向上・訓練イニシアティブを促

進すべきである。

- 推奨施策・勧告 4：EC 及び加盟国は ENISA の協力を得ながら、知識の共有・発信イニシアティブを促進すべきである。

  - 重要側面：
    - EU 連携実体の傘下
    - 加盟国及び EU によって促進される
    - 電力網オペレータ、電力サービスプロバイダー、メーカー及び最終消費者を対象とする。
    - 積極的に学術／研究開発に参入すること
  - 目標：
    - C-レベルスタッフの認識向上
    - 安全的なデバイスやアプリの作成についてメーカーのための訓練
    - オペレーター向けのセキュリティ及び電力網の復旧に影響しかねない脅威及びリスクに関する訓練
    - 最終消費者及びサービスプロバイダーのための不正防止、プライバシーなどにかかわる認識向上・訓練
    - サイバー・セキュリティ・イニシアチブにおける DSO／TSO のリーダーシップの強化
    - 既存イニシアティブは自分の取り組みを広く知れ渡らすことを促進する
    - CERT の関与を含んで DSO 及び TSO のための知識共有プラットフォーム創立の分析（推奨施策・勧告 9 に参考）

- 推奨施策・勧告 5：EC は ENISA、加盟国及び民間団体の協力を得ながら、既存標準及びガイドラインに基づき最低限対策セットを策定すべきである。

  - 重要側面：
    - MS の協力を得ながら、EU にリードされる。
    - 進行中のイニシアティブ（e.g. SGIS WG, DG CONNECT's ad-hoc EG）及び利害関係者の個々の経験を活用する。
    - 強制的なセキュリティアセスメントの基準を設定すべきである。ベンダ及び電力網運営者の為の欧州認証制度の確立をサポートする。
  - 最低限標準及びガイドラインセット：
    - 共通参照アーキテクチャ
    - 参照リスクアセスメント方法論（推奨施策・勧告 1 に参考）
    - ISA99 や WIB ベンダのための要件などの既存イニシアティブを活用して作成される SG システムのための技術要件（推奨施策・勧告 6 に参考）
    - ISO 27K シリーズ、ISA99 及び NIST IR 7628 を活用して作成されるセキュリティ管理ガイドライン
    - 頑丈な HAN/IAN/BAN を実装するためのガイドライン

- 推奨施策・勧告 6：EC 及び MS の監査当局はコンポーネント・製品・組織

向けセキュリティ認証制度の確立を促進すべきである

- 重要側面：
  - EU の公共機関によって推進される
  - 対象製品及び組織のセキュリティ
  - 推奨施策・勧告 5 に従って作られた標準セット及び CC、ISA99 及び ISO 27K のような既存イニシアティブを活用する
- 目標：
  - 加盟国にわたるセキュリティ及び復旧要件を調和させる。
  - 汎欧州の最低限監査可能なコントロールセットの基準を確立する（e.g. 認証されたサービスプロバイダーなら比較しやすい、製品認証を通じて製品のセキュリティレベルに係る情報を手に入れる、安全管理における電力網運営者認証を通じて比較用のベースラインが提供される…）
  - 国指定の認証機関（NCAs）は認証担保を担当する。

- 推奨施策・勧告 7：EC 及び加盟国の監査当局はテストベッド・セキュリティ評価手法の開発を促進すべきである。

- 重要側面：
  - 二つのタスクとも加盟国及び EU によって促進されるべきである。
  - テストベッド：基本的なセキュリティ原則（e.g. WIB ベンダのための要件）をベースに快速／素早いセキュリティテストを行うべきである。
  - セキュリティアセスメント：DSO、TSO 及び他のアクターにおける独自のセキュリティアセスメント及び侵入テストの実施を促進する
- 目標：
  - 認証制度が開発されるときにギャップを埋める。
  - もし準備できたら、テストベッドも委任される認証実行者になりえる。

- 推奨施策・勧告 8：EC 及び加盟国は ENISA の協力を得ながら、電力網に影響を及ぼす欧州規模のサイバーインシデントに対応するための戦略をさらに研究調査し、見直すべきである。

- 重要側面：
  - EC、ENISA 及び加盟国の監査当局は常にリードの役割を発揮すべきである。
  - 電力網利害関係者を巻き込む：発電所から顧客まで
  - 既存の多国籍電力組織（すなわち ENTSO、ACER など）、国の重要インフラ保安局、他の危機管理組織及び CERT も考慮すべきである。
- 目標：
  - 共同で大規模サイバーインシデントに対応する戦略の更なる研究・調査
  - 中央協調実体と分散的な電力網オペレーター自主協調団体の共存
  - 課題：アラームエスカレーション、政策決定（e.g. TSO を隔離する）、事

前確立されるインシデント対応手順、欧州電力網内部の相互依存性

- 推奨施策・勧告 9 : 加盟国の監査当局は CERT の協力を得ながら、電力網に影響を及ぼすサイバーセキュリティ問題に関する、CERT への協力（アドバイザー参加要請）を要請すべきである。

  - 重要側面：
    - EC 及び加盟国の監査当局はこのプロセスをリードすべきである。
    - 推奨施策・勧告 8 により定義された戦略と同調すべきである。
  - 目標：
    - 能力がある CERT は SG におけるのサイバーセキュリティ問題にも取り組むべきである。
    - 広範囲の重要インフラ（遠隔通信システム、陸上交通インフラなど）も直接に電力網に依存する。
    - 可能な大規模サイバーインシデントに対応するため、CERT は EU や加盟国レベルのところで標準の危機管理構造を提言すべきである。
    - どれでも正確な役割を更なる研究・調査すべきである。例として下記の通りである：
      1) 情報交換のための統一ポイント
      2) 貴重な情報の参照（e.g. 優良実践散布);
      3) 電力網のサイバーセキュリティ監視のための中心点
      4) 認識向上に取り組むリーダー
      5) サイバーセキュリティ認証における補助役

推奨施策 10 :（R10: Foster R&D in SG cyber security leveraging existing research programs）

- 推奨施策・勧告 10 : EC 及び加盟国の監査当局は学術・研究開発界の協力を得ながら、既存の研究開発プロジェクトを活用し、スマートグリッド研究開発を促進すべきである。

  - 重要側面:
    - FP7 及び Horizon 2020 の活用
  - 提案される研究課題：
    - SG の監視機能保護及び自動意思決定システム
    - 健全、安全、復旧可能なアーキテクチャ（e.g. 自己回復／グレースフルデグラデーション、暗号材料管理)
    - 信用、保証及びエンド・ツー・エンドセキュリティ（e.g. 依存性分析、ユーズケースモデリング）
    - 信頼システムのセキュリティ
    - サプライチェーン保護
    - クラウドにおけるスマートグリッド保安

✧ スマートグリッドサイバーセキュリティの法律／経済面 の課題
✧ Etc.

（8）ENISA によりスマートグリッドのためのセキュリティ対策

ENISA の「Appropriate security measures for smart grids – Guidelines to access the sophistication of security measure implementation」という文書の中で、定義された 10 のドメインに対してセキュリティ対策を制定している。

ドメイン	ID	セキュリティ対策	定義
セキュリティガバナンス及びリスク管理	SM 1.1	Information security policy	The provider should establish and maintain an appropriate information security policy
	SM 1.2	Organisation of information security	The provider should establish and maintain an appropriate structure of security roles and responsibilities
	SM 1.3	Information security procedures	The provider should establish and maintain an appropriate set of security procedures that supports the implementation of the security policy
	SM 1.4	Risk management framework	The provider should establish and maintain an appropriate risk management framework for risk assessment and risk treatment activities across the organisation which will take into account the complex operational environment
	SM 1.5	Risk assessment	The provider should establish and perform risk assessment activities to identify and evaluate the risk across the organisation at regular intervals
	SM 1.6	Risk treatment plan	The provider should establish and maintain an appropriate risk treatment plan in order to manage the risk across the organisation
第三者管理	SM 2.1	Third party agreements	The provider should establish and maintains appropriate third party agreements to preserve the integrity, confidentiality and availability of the information at the same level as the internal services when dealing with customers and third parties
	SM 2.2	Monitoring third parties services and validating solutions against predefined acceptance criteria	The provider should establish and maintain mechanisms in order to monitor the compliance of contractual obligations of information and services and validate solutions against predefined acceptance criteria
	SM 3.1	Security requirements (should be aligned with the M/490 SG-CG/SGIS Working Group recommendations) analysis and specification	The provider should identify and define beforehand the necessary security requirements for smart grid components and systems during the design and procurement

	SM 3.2	Inventory of smart grid components/systems	Using default configurations often leads to insecure and unnecessary open ports and exploitable services and applications running on hosts.
スマートグリッドのコンポーネント／システム及びのためのライフサイクル・プロセス及び操作手順の保安	SM 3.1	Security requirements (should be aligned with the M/490 SG-CG/SGIS Working Group recommendations) analysis and specification	The provider should identify and define beforehand the necessary security requirements for smart grid components and systems during the design and procurement
	SM 3.2	Inventory of smart grid components/systems	The provider should establish and maintain an inventory that represents the components and smart grid information systems
	SM 3.3	Secure configuration management of smart grid components/systems	The provider should ensure that the base security configuration of a smart grid’s components/systems is identified, set and maintained for every instance of that component/system
	SM 3.4	Maintenance of smart grid components/systems	The provider should establish and maintain activities for performing routine and preventive/corrective maintenance on the components and smart grid information systems
	SM 3.5	Software/firmware upgrade of smart grid components/systems	The provider should establish and maintain activities for software/firmware upgrade on the components and smart grid information systems
	SM 3.6	Disposal of smart grid components/systems	The provider should establish and maintain activities for the secure disposal of smart grid components and smart grid information systems
	SM 3.7	Security testing of smart grid components/systems	Security testing activities on the smart grid components/systems should be performed in order to verify its security
個人の安全、意識及び訓練	SM 4.1	Personnel screening	The provider should perform appropriate background checks on personnel (employees, contractors, and third-party users) if required for their duties and responsibilities
	SM 4.2	Personnel changes	The provider should establish and maintain an appropriate process for managing changes in personnel (employees, contractors, third-party users) or changes in their roles and responsibilities
	SM 4.3	Security and awareness program	The provider should establish and maintain a security awareness program across the organisation

	SM 4.4	Security training and certification of personnel	The provider should establish and maintain security training and personnel certification programmes, taking into account its needs based on their roles and responsibilities
インシデント・レスポンス及び情報知識共有	SM 5.1	Incident response capabilities	The provider should establish and maintain capabilities to respond against cyber security incidents
	SM 5.2	Vulnerability assessment	The provider should establish and maintain vulnerability assessment activities on the smart grid information systems
	SM 5.3	Vulnerability management	The provider should establish and maintain an appropriate vulnerability management plan in order to manage vulnerabilities on smart grid information systems
	SM 5.4	Contact with authorities and security interest groups	The provider should establish and maintain contacts with authorities and security interest groups to be aware of vulnerabilities and threats
監査・会計	SM 6.1	Auditing capabilities	The provider should establish and maintain auditing capabilities on the smart grid Information systems and components
	SM 6.2	Monitoring of smart grid information systems	The provider should establish and maintain monitoring activities on the smart grid Information systems and components
	SM 6.3	Protection of audit information	The provider should protect the audit information generated
運用の連続性	SM 7.1	Continuity of operations capabilities	The provider should establish and maintain capabilities to ensure essential functions after disruption events on smart grid Information systems
	SM 7.2	Essential communication services	The provider should establish, maintain and test essential/emergency communication services in case of major disasters
物理的セキュリティ保護	SM 8.1	Physical security	The provider should establish and maintain the appropriate physical security of the smart grid facilities/components/systems
	SM 8.2	Logging and monitoring physical access	The provider should establish and maintain capabilities for logging and monitoring the physical access to the smart grid facilities/components taking into account the criticality of the facility
	SM 8.3	Physical security on third party premises	The provider should protect equipment located outside of the organisations' own grounds or premises in areas that are the responsibility of other utilities against physical and environmental threats

情報システムセキュリティ	SM 9.1	Data security	The provider should implement security requirements in order to protect the information on smart grid information system
	SM 9.2	Account management	The provider should establish and maintain system/groups/user accounts on smart grid information systems
	SM 9.3	Logical access control	The provider should enforce logical access to authorized entities on smart grid information systems and security perimeters
	SM 9.4	Secure remote access	The provider should establish and maintain secure remote access where applicable to smart grid information systems
	SM 9.5	Information security on information systems	The provider should establish and maintain appropriate information security capabilities on information systems, to provide protection against malware, viruses and other common threats
	SM 9.6	Media handling	The provider should establish and maintain secure procedures for the access, storage, distribution, transport, sanitization, destruction and disposal of the media assets
ネットワークセキュリティ	SM 10.1	Secure network segregation	The provider should establish and maintain a segregated network for the smart grid information system
	SM 10.2	Secure network communications	The provider should establish and maintain secure communications across the segregated network

SM: Security Measure

(9)ENISA の SG セキュリティ対策が NISTIR 7628 のセキュリティ要件へのマッピング

各 ENISA のスマートグリッドのセキュリティ対策が対応する NISTIR 7628 のセキュリティ要件は下記のとおりである。

ドメイン	セキュリティ対策	NISTIR-7628の対応要件
セキュリティガバナンス及びリスク管理	Information security policy	SG.PM-1 Security Program Management SG.PM-3: Senior Management Authority
	Organisation of information security	SG.PM-1 Security Program Management SG.PM-3: Senior Management Authority SG.PM-8: Management Accountability SG.PM-19 Security Roles SG.AC-6: Separation of Duties
	Information security procedures	SG.PM-1 Security Policy and Procedures
	Risk management framework	SG.PM-5 Risk Management SG.RA-2 Risk Management Plan
	Risk assessment	SG.RA-1 Risk Assessment Policy and Procedures SG.RA-3: Security Impact Level SG.RA-4: Risk Assessment SG.RA-5: Risk Assessment Update
	Risk treatment plan	SG.RA-2 Risk Management Plan
第三者管理	Third party agreements	SG.AC-1: Access Control Policy and Procedures SG.CP-8: Alternate Telecommunication Services SG.CP-9: Alternate Control Center SG.PS-7 Contractor and Third-Party Personnel Security SG.PS-9: Personnel Roles SG.SA-2 Security Policy for Contractors and Third Parties SG.SA-4: Acquisitions
	Monitoring third parties services and validating solutions against predefined acceptance criteria	SG.AU-1 Audit and Accountability SG.AU-11: Conduct and Frequency of Audits
スマートグリッドのコンポーネント／システム及びのためのライフサイクル・プロセス及び操作手順の保安	Security requirements analysis and specification	SG.SA-8 Security Engineering Principles
	Inventory of smart grid components/systems	SG.CM-2: Baseline Configuration SG.CM-8: Component Inventory SG.ID-3: Information Handling SG.ID-5: Automated Labelling, SG.MP-2: Media Sensitivity Level SG.MP-3: Media Marking, SG.PL-3: Rules of Behaviour SG.PM-4: Security Architecture SG.PS-6: Access Agreements SG.RA-3: Security Impact Level
	Secure configuration	SG.CM-2 Baseline Configuration

	management of smart grid components/systems	SG.CM-3: Configuration Change Control SG.CM-4: Monitoring Configuration Changes SG.CM-5: Access Restrictions for Configuration Control SG.CM-6: Configuration Settings SG.CM-8 Component inventory SG.CM-10: Factory Default Settings Management SG.CM-11 Configuration Management Plan
	Maintenance of smart grid components/systems	SG.MA-1: Smart Grid Information System Maintenance Policy and Procedures SG.MA-3 Smart Grid information system maintenance SG. MA-4: Maintenance Tools SG.MA-6: Remote Maintenance SG.MA-7: Timely Maintenance SG.PL-5: Security-Related Activity Planning
	Software/firmware upgrade of smart grid components/systems	SG.SI-2 Flaw Remediation
	Disposal of smart grid components/systems	SG.CM-9 Addition, removal, and disposal of equipment SG.MA-3: Smart Grid Information System Maintenance SG.MP-6: Media Sanitization and Disposal
	Security testing of smart grid components/systems	SG.CM-2 Baseline Configuration SG.CA-2 Security Assessments SG.RA-6: Vulnerability Assessment and Awareness, SG.SA-3: Life-Cycle Support SG.SA-9: Developer Configuration Management SG.SA-10: Developer Security Testing SG.SI-6: Security Functionality Verification SG.SI-7: Software and Information Integrity
個人の安全、意識及び訓練	Personnel screening.	SG.PS-3 Personnel Screening
	Personnel changes	SG.AC-3: Account Management SG.PE-3: Physical Access SG.PS-4: Personnel Termination SG.PS-5: Personnel Transfer SG.SA-2: Security Policies for Contractors and Third Parties
	Security and awareness program	SG.AT-1 Awareness and Training Policy and Procedures SG.AT-2 Security awareness SG.AT-4: Security Awareness and Training Records
	Security training and certification of personnel	SG.AT-3 Security Training SG.AT-6: Security Responsibility Testing SG.CP-4: Continuity of Operations Training SG.PS-9: Personnel Roles
インシデント・レスポンス	Incident response	SG.IR-1 Incident Response Policy and

及び情報知識共有	capabilities	Procedures SG.IR-2 Incident Response Roles and Responsibilities SG.IR-3 Incident Response Training SG.IR-4 Incident Response Testing and Exercises SG.IR-5 Incident Handling SG.IR-6: Incident Monitoring SG.IR-7: Incident Reporting SG.IR-8: Incident Response Investigation and Analysis SG.IR-11: Coordination of Emergency Response
	Vulnerability assessment	SG.RA-4 Risk Assessment SG.RA-6 Vulnerability Assessment and Awareness SG.CA-6: Continuous Monitoring SG.SA-10: Developer Security Testing
	Vulnerability treatment	SG.SA-8 Security Engineering Principles SG.RA-6 Vulnerability Assessment and Awareness SG.SA-7: User-installed Software SG.SI-2: Flaw Remediation
	Contact with authorities and security interest groups	SG.AT-5 Contact with Security Groups and Associations SG.ID-4: Information Exchange SG.IR-9: Corrective Action
監査・会計	Auditing capabilities	SG.AU-1 Audit and Accountability Policy and Procedures SG.AU-2 Auditable Events SG.AU-3 Content of Audit Records SG.AU-4: Audit Storage Capacity SG.AU-11: Conduct and Frequency of Audits SG.AU-14: Security Policy Compliance SG.AU-15 Audit Generation
	Monitoring of smart grid information systems	SG.AU-2 Auditable events SG.AU-6 Audit Monitoring, Analysis, and Reporting SG.AU-5: Response to Audit Processing Failure SG.AU-7: Audit Reduction and Report Generation SG.CA-6: Continuous Monitoring SG.SC-7: Boundary Protection
	Protection of audit information	SG.AU-4 Audit Storage Capacity SG.AU-5 Response to Audit Processing Failures SG.AU-8: Time Stamps SG.AU-9 Protecting Audit Information SG.AU-10: Audit Record Retention SG.AU-16: Non-Repudiation
運用の連続性	Continuity of operations	SG.CP-1 Continuity of Operations Policy and

	capabilities	Procedures SG.CP-2 Continuity of Operations Plan SG.CP-3 Continuity of Operations Roles and Responsibilities SG.CP-4 Continuity of Operations Training SG.CP-5 Continuity of Operations Plan Testing SG.CP-6 Continuity of Operations Plan Update SG.CP-7 Alternate Storage Sites SG.CP-9: Alternate Control Center SG.CP-10: Smart Grid Information System Recovery and Reconstitution SG.PL-5: Security-Related Activity Planning
	Essential communication services	SG.CP-8 Alternate Telecommunication Services SG.CP-9 Alternate Control Center SG.CP-11 Fail-Safe Response SG.IR-11: Coordination of Emergency Response
物理的セキュリティ保護	Physical security	SG.PE-1: Physical and Environmental Security Policy and Procedures SG.PE-2 Physical Access Authorizations SG.PE-3: Physical Access SG.PE-8: Emergency Shutdown Protection SG.PE-9: Emergency Power SG.PE-12: Location of Smart Grid Information System Assets
	Logging and monitoring physical access	SG.PE-2: Physical Access Authorizations SG.PE-4: Monitoring Physical Access SG.PE-5: Visitor Control SG.PE-6: Visitor Records SG.PE-7: Physical Access Log Retention
	Physical security on third party premises	
情報システムセキュリティ	Data Security	SG.ID-3 Information Handling SG.ID-5 Automated Labelling
	Account management	SG.AC-1: Access Control Policy and Procedures SG.AC-3 Account Management SG.AC-4: Access Enforcement
	Logical access control	SG.AC-4 Access enforcement
	Secure remote access	SG.AC-2 Remote Access Policy and Procedure SG.AC-3: Account Management SG.AC-13: Remote Session Termination SG.AC-15 Remote Access SG.AC-16: Wireless Access Restrictions SG.SC-8: Communication Integrity SG.SC-9: Communication Confidentiality
	Information security on information systems	SG.SI-3 Malicious Code and Spam Protection SG.MA-4: Maintenance Tools SG.MA-6: Remote Maintenance

	Media handling	SG.MP-1 Media Protection Policy and Procedures SG.MP-2 Media Sensitivity Level SG.MP-3 Media Marking SG.MP-4 Media Storage SG.MP-5 Media Transport SG.MP-6 Media Sanitization and Disposal
ネットワークセキュリティ	Secure network segregation	SG.SC-7: Boundary Protection SG.SC-29: Application Partitioning
	Secure network communications	SG.AC-2: Remote Access Policy and Procedures SG.AC-4: Access Enforcement SG.AC-15: Remote Access SG.AC-17: Access Control for Portable and Mobile Devices SG.SC-2: Communications Partitioning SC.SC-7: Boundary Protection SG.SC-8: Communication Integrity SG.SC-9 Communication Confidentiality SG.SC-18: System Connections SG.SI-4: Smart Grid Information System Monitoring Tools and Techniques

付録 8　スマートメーターの A/B ルートの分離

電力会社が事業として独自に管理する A ルートのネットワークと異なり、B ルートはユーザーが主体のネットワークである。B ルートのユースケースとして、不特定の機器が比較的簡単に接続され、かつそれらの機器は、市場流通性を確保するため、相互接続性が確保される必要がある。

米国においては、UCAIug の AMI セキュリティプロファイルにおいて、境界の保護(DHS2-8-7 項の理論的解釈事項として、電力会社の自動検針インフラシステムに対するサイバーセキュリティのリスクを最小限に抑え、かつ、不正アクセスを可能な限り避けるため、AMI ネットワーク(A ルート)と、不特定多数の接続が期待される HAN などスマートグリッドアプリケーションネットワーク(B ルート)の間では、物理的インターフェースを含む境界間の保護やシステムやセキュリティ領域の分離が重要であると記載されている。

具体的な例として、同 DHS2-8-7 項のガイドラインに下記くだりが紹介されている。

The organization physically shall locate publicly accessible AMI system components to enforce segregation of subsystem data trafic with separete, physical network interfaces.

図表付録 8-1　UCAlug AMI セキュリティプロファイルによる
A/B ルートの分離の概念図

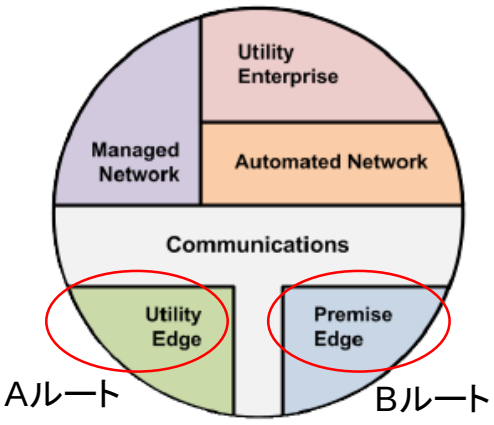


Figure 4: AMI Security Service Domains
AMIセキュリティー領域

（出所）UCAlug「SECURITY PROFILE FOR ADVANCED METERING INFRASTRUCTURE, Ver2.0 Oct 2010 release」

我が国においても、スマートコミュニティアライアンス（JSCA）に設置されたスマートハウス・ビル標準・事業促進検討会において、平成 25 年 5 月に、「HEMS-スマートメーター（B ルート） 運用ガイドライン」をとりまとめている。この中で、スマートメーターBルートの開通においては、システム面、保守運用面において十分なセキュリティ強度を有するべきであるとして、セキュリティについて、以下のような基本要件を定めている。

図表付録 8-2　我が国のスマートメーターBルートにおける
セキュリティの基本要件

7．セキュリティの基本要件

■ **スマートメーターBルートの開通においては、システム面、保守運用面において十分なセキュリティ強度を有するべきである。以下6項目によりセキュリティを担保する**

1. Bルート(宅内側)とAルート(AMI側)は、アイソレーションされた設計とする(図１)。アイソレーションの定義は、IPパケットの転送機能は持たせず、ネットワークドメインを分離することを意味する
2. スマートメーターとHEMSコントローラは１対１の接続形態とする
3. 公知な標準メディアが相互接続確認をサポートしている認証・暗号方式と組合せて適切なセキュリティを実施する
4. レイヤー２以下での暗号化処理は必須。暗号化処理方式はAES-128など、NIST等の公的な機関により長期に亘り十分な強度を有すると判断されるものを採用する
5. Bルートから他のドメインへIPルーティングで接続することは行わない
6. 悪意のあるIPパケット（コマンド）が宅内側から到達することを防ぐことを目的にECHONET Liteの対応コマンドを限定する

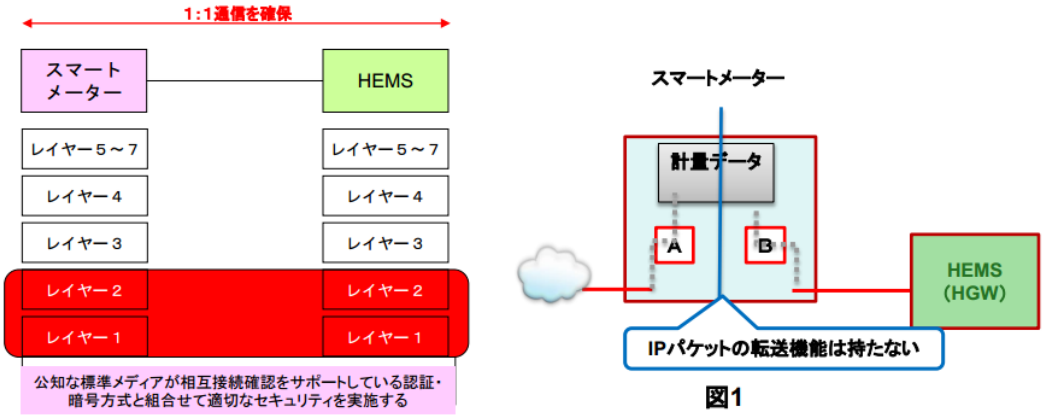


図1

（出所）JSCA スマートハウス・ビル標準・事業促進検討会
「HEMS-スマートメーター（B ルート）運用ガイドライン」