2010 年度
制御システムの情報セキュリティ動向に関する調査報告書

～アジアにおける制御システムセキュリティの取組み状況を調査～

2011 年 5 月

IPA 独立行政法人情報処理推進機構
セキュリティセンター

目次

序

1. はじめに

1.1 背景と目的

石油プラント、半導体製造工場や自動車製造工場等の産業用の制御システム（電力、交通や通信等の重要な社会インフラの制御システムも含む）は、今日、不正アクセスや情報漏えい等の様々な脅威に直面している。万が一、制御システムにトラブルが発生した場合、被害は甚大かつ広範囲になる可能性がある。

IPA は、2008 年度に米国[1]、2009 年度には米国及び欧州[2]において制御システムセキュリティに関する調査を行った。2010 年度は欧州と米国に続き、アジアにおける制御システムセキュリティへの取組みについて調査を行うとともに、スマートメータ周辺の制御システムに関わる新技術動向についても調査を行った。さらに、制御システムの研究・開発者や情報セキュリティ専門家などによる検討会を設置し、上記調査内容をもとに制御システムセキュリティについての課題整理とその検討を行った。

本報告書は、制御システムに関する組織や制御システムの情報セキュリティに関心を持つ人に対し、制御システムの情報セキュリティに関する調査・検討結果を伝え、制御システムの情報セキュリティを推進することを目的とする。

1.2 調査内容

本調査では、アジア各国における制御システムの脆弱性低減施策と、スマートメータ周辺の制御システムに関わる新技術のセキュリティ状況を把握するため、以下の調査・検討を行った。

■ アジアにおける制御システムの脆弱性低減施策（下記項目は昨年度調査と同様の観点）

(1) 脆弱性低減のためのガイドやツールなどの整備・活用状況

(2) 制御システム脆弱性の評価・検証のための手法

(3) 制御システムに関するセキュリティ障害事例データベース動向

(4) 制御システムの認証を取り巻く環境

■ スマートメータ周辺の制御システム動向に関する調査

(1) システム構成イメージ

(2) 構成要素に対するセキュリティ面での脅威・対策

(3) 技術動向、製品動向

[1]重要インフラの制御システムセキュリティと IT サービス継続に関する調査報告書
http://www.ipa.go.jp/security/fy20/reports/ics-sec/index.html

[2]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
http://www.ipa.go.jp/security/fy21/reports/ics_sec/index.html

1.3 用語および略語の定義

1.3.1 用語定義一覧

本報告書で使用する用語の意味を以下に定義する（図表 1-1）。

図表 1-1 用語定義一覧

用語	定　義
オープン化	本調査では、汎用製品の採用および標準プロトコルの採用の両方を含めて「オープン化」と呼ぶ。なお、上記のどちらか片方だけに限定して記述する場合は、「汎用製品の採用」、「標準プロトコルの採用」というように明確に区別して記述する。
制御システム	「制御システム」は、狭義と広義に分けて捉えることができる。 本調査では、特に言及が無い場合には狭義の意味で「制御システム」という表現を使用する。すなわち、センサやアクチュエータなどのフィールド機器、コントローラ、監視・制御用に用いるサーバやクライアント PC などをネットワークで接続した機器群(システム）をさすこととする。
SCADA	Supervisory Control And Data Acquisition の略称。 主に、地理的に分散した制御対象を広域ネットワーク経由で遠隔集中監視するシステムを SCADA システムと呼ぶが、日本では、PLC(Programmable Logic Controller）などの制御機器の監視を HMI(Human Machine Interface：マンマシンインタフェース）である汎用 PC 上で実行するためのソフトウェアを SCADA と呼ぶ場合が多い。 本調査では、制御システムのうち汎用製品、標準プロトコルが採用されているシステムをさすこととする。

1.3.2 略語一覧

本報告書で使用する略語は以下の通りである（図表 ）。

図表 1-2　略語一覧

略語	名称
AMI	Advanced Metering Infrastructure
AMR	Automatic Meter Reading
ANSI/ISA	American National Standards Institute / International Society of Automation
APT	Advanced Persistent Threats
ASEAN	Association of South - East Asian Nations
BEMS	Building Energy Management Systems
CAP	Certificate Authorising Participant
CC	Common Criteria

略語	名称
CCRA	Common Criteria Recognition Arrangement
CEMS	Community Energy Management Systems
CFATS	Chemical Facility Anti-Terrorism Standards
CNCERT/CC	National Computer Network Emergency Response Technical Team / Coordination Center of China
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DNP3	Distributed Network Protocol 3
DSO	Distribution System Operator
DoS	Denial of Service
EG2	Expert Group 2, EU Commission Task Force for Smart Grids
EGAT	Electricity Generating Authority of Thailand
EISA	Energy Independence and Security Act
ENISA	European Network and Information Security Agency
eSHIPS	e Smart House Information Platform Standardization Forum （“e”は、ecology, energy, electric , enjoy ・・・の略。）
ESMA	European Smart Metering Alliance
EU	European Union
GAO	U.S. Government Accountability Office
GB/T	中華人民共和国　推薦性国家標準
GB/Z	中華人民共和国　指導性技術文書
GB	中華人民共和国　国家標準(Guojia Biaozhun)
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HAN	Home Area Network
HEMS	Home Energy Management System
HMI	Human Machine Interface
ICS	Industrial Control Systems
ICSJWG	Industrial Control Systems Joint Working Group
IEC TC	International Electrotechnical Commission Technical Committee
IEC62443	Industrial communication networks - Network and system security
IEEE	The Institute of Electrical and Electronics Engineers, Inc.
IPA	Information-technology Promotion Agency, Japan 独立行政法人 情報処理推進機構
ISA	International Society of Automation
ISA-99	Industrial Automation and Control System Security
ISCI	ISA Security Compliance Institute
ISCS	Information Security Check Service
ITEI	Instrumentation Technology and Economy Institute P. R. China
JPCERT/CC	Japan Computer Emergency Response Team / Coordination Center 一般社団法人 JPCERT コーディネーションセンター

略語	名称
JVN	Japan Vulnerability Notes
KECS	Korea IT Security Evaluation and Certification Scheme
KEPCO	Korea Electric Power Corp
KISA	Korea Internet& security Agency
KrCERT/CC	Korea Computer Emergency Response Team / Coordination Center
M-bus	Message Bus
MIU	Meter Interface Unit
MOEA	Ministry for economic Affair
NIST	National Institute of Standards and Technology
OpenADE	Open Automatic Data Exchange (UCAIug OpenSG OpenADE Task Force)
OpenADR	Open Automated Demand Response (UCAIug OpenSG OpenADR Task Force)
OpenAMI	Open Advanced Metering Infrastructure (UCAIug OpenSG OpenAMI-Ent Task Force)
OpenHAN	Open Home Area Network (UCAIug OpenSG OpenHAN Task Force)
OpenSG	Open Smart Grid Technical Committee of the UCAIug
PLC	Programmable Logic Controller
PLC	Power Line Communication
PRIME	PoweRline Intelligent Metering Evolution
RISI	Repository of Industrial Security Incidents
SAC/TC124	TC of Industrial Process Measurement and Control of Standardization Administration of China
SCADA	Supervisory Control And Data Acquisition
SP	Special Publication
SUN	Smart Utility Network
TCP/IP	Transmission Control Protocol/Internet Protocol
TWACS	Two-Way Automatic Communications System
ThaiCERT	Thai Computer Emergency Response Team
UCAIug	Utility Communication Architecture International User Group
US-CERT	United States Computer Emergency Readiness Team
USB	Universal Serial Bus
WiMax	Worldwide Interoperability for Microwave Access

第 1 編　制御システムのセキュリティについて

2. 制御システムのセキュリティに係る現状

2.1　制御システムのインシデントの動向

2010 年に発見されたコンピュータウイルス Stuxnet など、制御系システムに対しても、近年セキュリティ面での脅威の拡大が見られる。

(1) 2009 年まで

米国国土安全保障省が運営している ICSJWG （Industrial Control Systems Joint Working Group）で報告された RISI（Repository of Industrial Security Incidents）の報告によれば、世界の制御システムインシデントの 2009 年までの累積総数は 162 件で、この内、2008 年は 10 件、2009 年は 18 件となっている[3]（図表 2-1）。

図表 2-1　世界の制御システムインシデント数の推移（1982-2009 年）

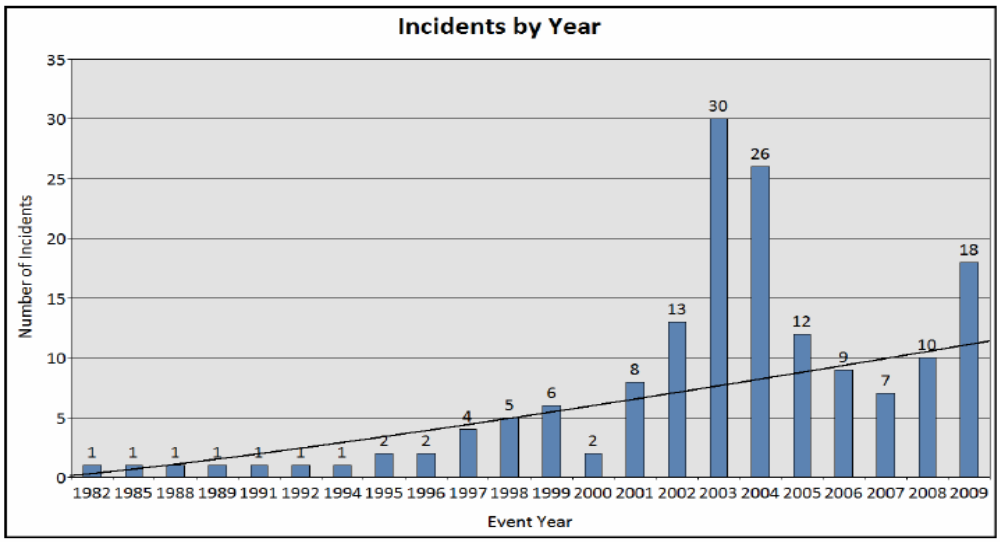


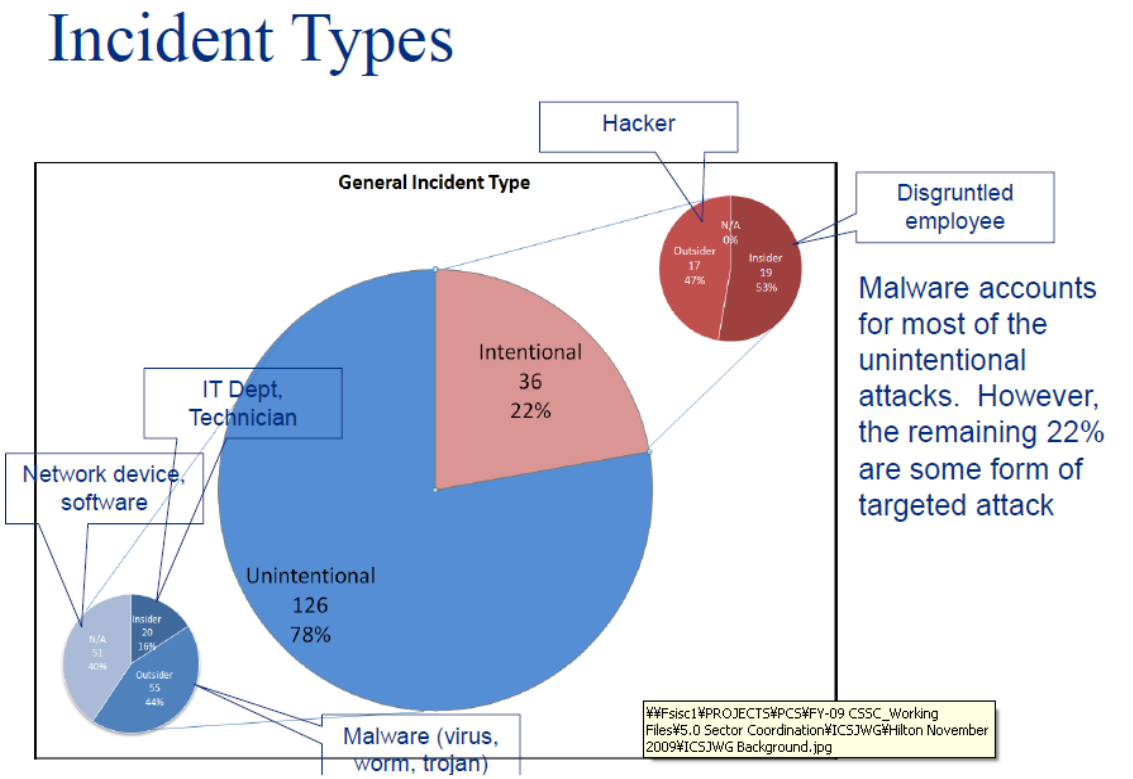
Figure 2-3: Incidents by Year

出典：ICSJWG プレゼン資料

162 件のうち 126 件(78%)は非意図的なマルウェアで、残りの 36 件(22%)が意図的なインシデントで、ある種の標的型攻撃である。36 件の意図的なインシデントの 17 件(47%)が外部からのハッカー攻撃で、19 件(53%)が内部からの攻撃である。126 件(78%)の非意図的なインシデントの 55 件がマルウェアによるインシデントである（図表 2-2）。

[3] What Went Wrong? A Study of Actual Industrial Cyber Security Incidents
http://www.us-cert.gov/control_systems/icsjwg/presentations/spring2010/02%20-%20Zach%20Tudor.pdf

図表 2-2　インシデントのタイプ分け(2009 年)



出典：ICSJWG プレゼン資料

(2)2010 年

2009 年までの累計では 55 件のマルウェアによるインシデントが報告されていたが、2010 年の報告では、60 件となっている。2010 年に起きた Stuxnet が衝撃的なマルウェアとして捉えられており、2010 年の報告でのインシデントの総数は 196 件と増加している。

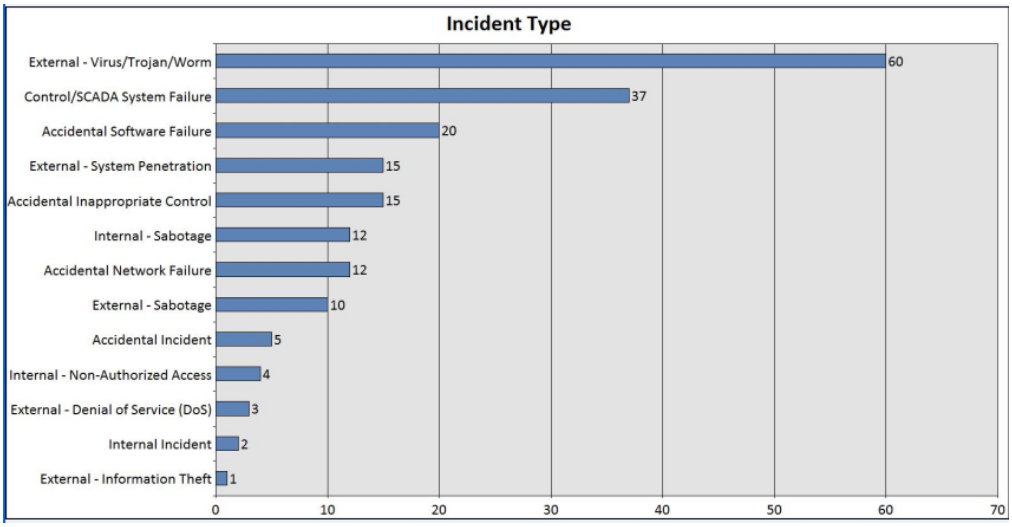
図表 2-3 は、インシデントのタイプごとの数を示し、図表 2-4 は、産業分野ごとのマルウェアによるインシデントの数を示している。[4]

2011 年 3 月に Security Incident Organization (SIO) による最新レポート“Report on Cyber Security Incidents and Trends Affecting Industrial Control Systems Resulting from Malware Infections”[5]が公開された。darkREADING 誌の記事によると、SCADA や産業制御システムのウイルス感染事件数は減少しているものの、実際には減っているというより、攻撃の巧妙化・ステルス化が進み、検知され難くなっているにすぎないと指摘している。

[4] Real DATA on Industrial Control Security from RISI “Real DATA on Industrial Control Security from RISIt:9pt;margin-top:22.5pt;width:425.2pt;height:241.6pt;z-index:2516331

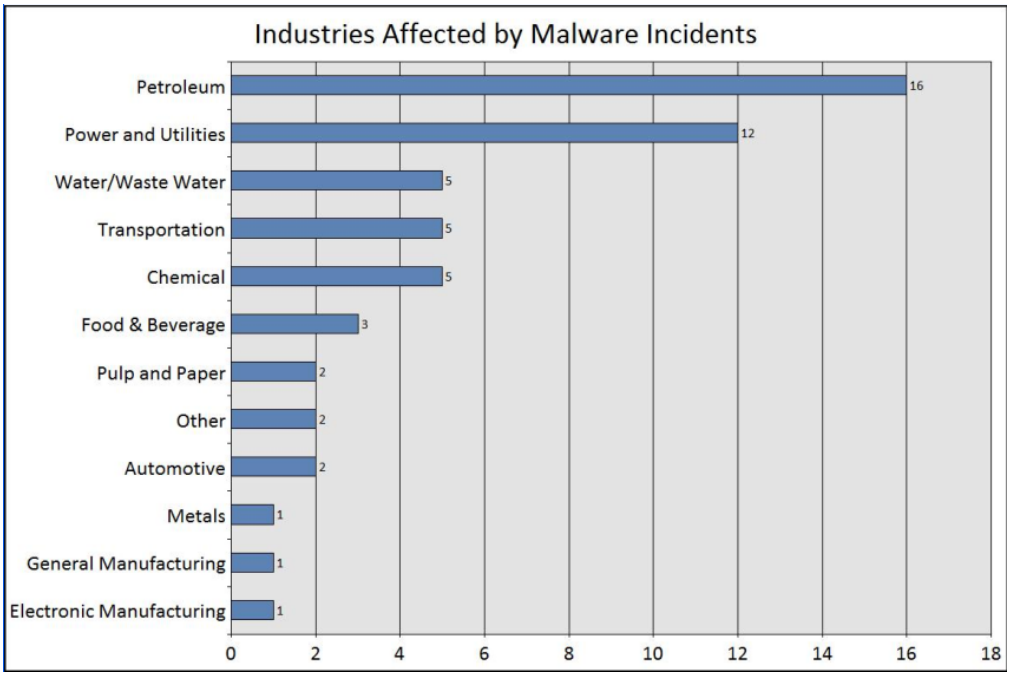
[5]http://www.sensorsmag.com/process-industries/news/security-incidents-organization-releases-annual-report-8230

図表 2-3　インシデントのタイプ分け(2010 年)



出典：RISI レポート

図表 2-4　産業分野ごとのマルウェアによるインシデントの数(2010 年)



出典：RISI レポート

2.2　具体的なインシデント例

ここでは、制御システムにおける具体的なインシデント事例をもとに、制御システムが直面している脅威と問題点について考察する。

2.2.1 Stuxnet の概要

制御システムにおける具体的なインシデント事例としては、2010 年 7 月に世界中で話題となったコンピュータウイルス Stuxnet が挙げられる。Stuxnet は、原子力発電所の制御システムに影響を及ぼしたのではないかと報道されている。なお、日本国内でも数件の検出事例が報告されているが、被害事例は報告されていない。

(1)Stuxnet の攻撃フロー

Stuxnet は以下のフローで一連の執拗な攻撃を行う。脆弱性を利用して情報系のシステムに感染し、拡散、潜伏、ウイルス機能強化を行いつつ（①～③)、攻撃目標である制御装置の制御システムへ侵入し、攻撃を実行する（④～⑤)。

① USB メモリやインターネットを通じた情報システムへのウイルス感染
② システムの脆弱性を利用することにより、権限昇格や、情報システム環境内部でウイルスの拡散などを実行
③ バックドアを作成し、外部の指令サーバ(C&C サーバ)と 80 番ポート（HTTP）を介して通信することにより、ウイルスの増強や新たなウイルスのダウンロードの実行
④ 組織内のネットワークを経由し、原子力システム等を制御する装置が配備してある制御システムへの侵入
⑤ 制御システム上にある装置に対する攻撃の実行

(2)Stuxnet の総合的な特徴

各機関が出しているレポートと IPA の解析結果[6]を総合的にまとめると以下である。

① 500K バイト以上のプログラムで、4000 弱の機能を持っている。
② 複雑であり、オブジェクト指向で開発されている。
③ 複数の未知の脆弱性(ゼロデイ)を利用している。
④ 2 つのルートキットを持ち、制御システムをターゲットとしている。
⑤ 作成者は、Windows について造詣が深いことが分かる。また、制御システムである WinCC/Step7 についても詳細を知っている。

2.2.2 Stuxnet 等の新しい攻撃の出現の背景

(1)社会インフラへの攻撃の広がり

従来の攻撃対象は、情報システムであり、そのシステム上にある資産や情報等を狙ったものであった。しかし、2.2.1 に述べたように、制御システムにおいてもインシデントが発生しており、制御システムについても、情報システムと同様にセキュリティ対策を実施する必要がある。

電力や鉄道等のような社会インフラは、制御システムを組み込んで実現されている。そのため、制御システムを攻撃されると社会インフラが影響を受け、社会全体が影響を受ける可能性がある。

[6] IPA テクニカルウォッチ:『新しいタイプの攻撃』に関するレポート
http://www.ipa.go.jp/about/technicalwatch/20101217.html

このように、社会インフラが攻撃者のターゲットとなったことに合わせて、防御側が守るべきシステム範囲も広がり、制御システムの関係者と連携した体制も必要となってきている。

(2)システム環境の変化

Stuxnet が出現するまでは、汎用製品や標準プロトコルで構成されている情報システムが攻撃対象であった。一方、IPA の調査報告[7]にもあるように欧米や日本の制御システムにおいても、図表 2-5 に示すように制御システムのオープン化（汎用製品や標準プロトコルの利用）が進展しており、システム環境に変化が起きている。

攻撃のターゲットが情報システムだけでなく制御システムに及ぶようになった要因として、従来は独自仕様を利用していた制御システムの環境が、徐々にオープンな仕様に変化してきていることが挙げられる。

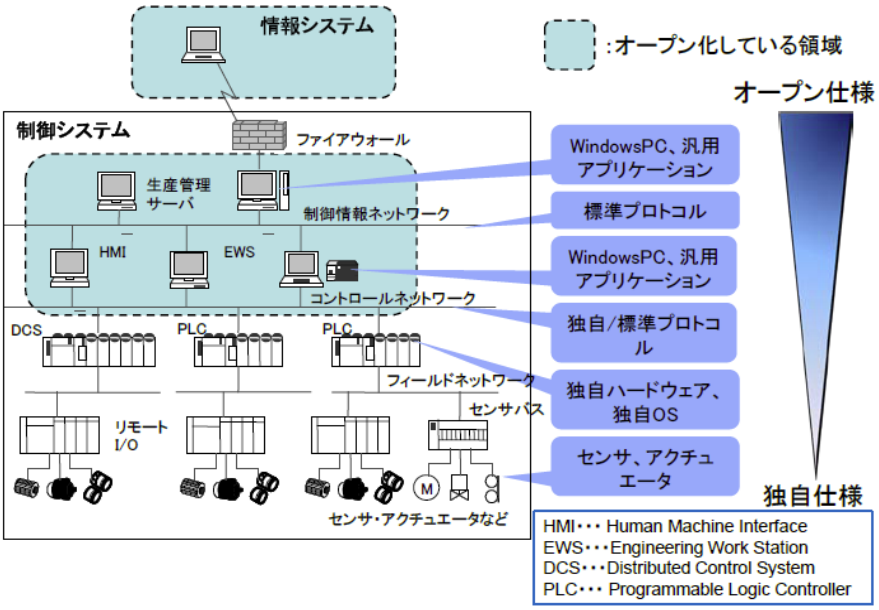
日本では、経済産業省がプラント設備に関して 234 社にアンケートを行った結果をまとめた資料[8]によると、制御システムにおけるサーバの 8 割以上、端末の 9 割近くが Windows 系を利用している。外部記憶装置については、サーバ・端末とも、USB を 7 割、CD/DVD リーダを 5 割程度保有している（図表 2-6）。また、サーバにおけるネットワーク接続ポートとしては、6 割がイーサネットを保有している。さらに、外部ネットワークとは 4 割弱が接続しており、接続先は、リモートメンテナンス回線が 5 割強、インターネットが 4 割である（図表 2-7）。また、社内情報システムとは半数以上が接続している。

このように、プラント設備での制御システムにおいては、汎用製品や標準プロトコルの利用が進みつつあることが示されている。

また、日本の制御システムに関しては、情報システムと制御システムを担当する部門が別である場合が多い。そのため、今回の Stuxnet のように情報システムと制御システムに跨って攻撃される場合を想定した脅威分析、システム設計や対処が実施困難な現状である。

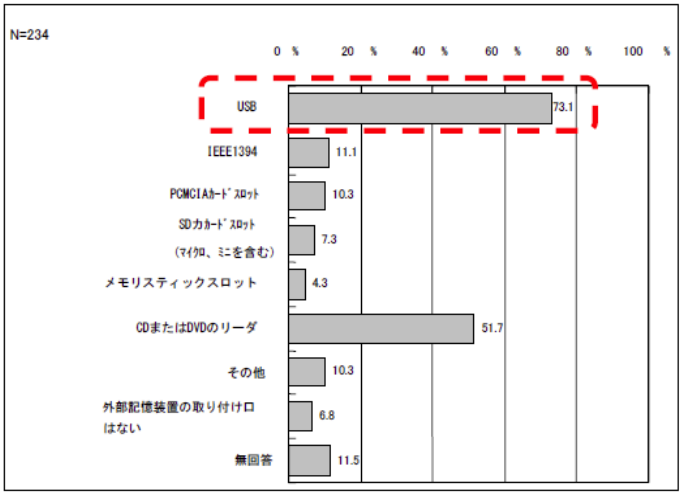
[7]制御システムセキュリティの推進施策に関する調査報告書
http://www.ipa.go.jp/security/fy21/reports/ics_sec/index.html
[8]「工業用装置等における汎用 IT 技術応用に起因する脅威と対策に関する実態調査事業」報告書
http://www.meti.go.jp/committee/kenkyukai/shoujo/cyber_security/001_06_01.pdf

図表 2-5　制御システムのオープン化：汎用製品＋標準プロトコル

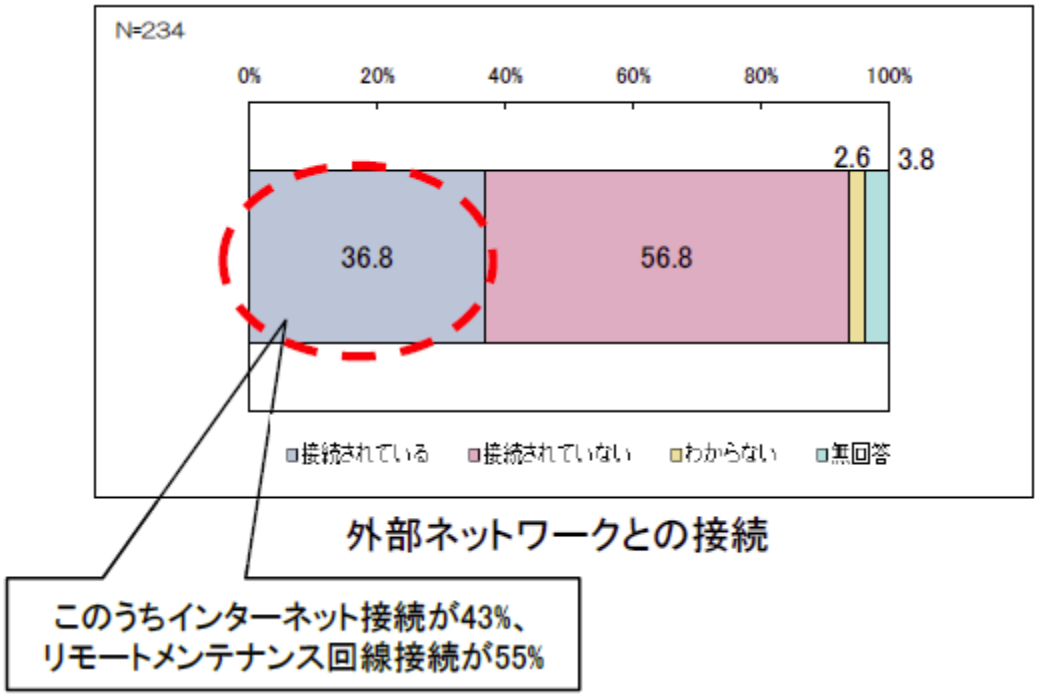


出典：IPA 作成資料

図表 2-6　プラント設備での外部メディアの取り付け口の有無



図表 2-7　外部ネットワークとの接続



2.2.3　Stuxnet 等のサイバー攻撃に関する各国の反応

Stuxnet によるサイバー攻撃は、汎用製品（Windows や Linux)や標準プロトコル(TCP/IP 等）の利用が拡大してオープン化が進んでいる制御システムへの初めての警告となる事例といわれている。

米国では DHS(Department of Homeland Security）が推進している ICS（産業用制御システム）へのサイバーセキュリティ対策強化活動のカンファレンス[9]で、Stuxnet についての報告がなされている。

EU では ENISA(European Network and Information Security Agency)において、Stuxnet を解析した結果をレポートとして報告しており、制御システムに対しての注意喚起[10]を行っている。

このように米国や EU では、産業用制御システムへのサイバー攻撃を見据えた上記のような対応が進んでいる。

2.2.4　新しいサイバー攻撃手法の分析と対応

Stuxnet のような、未知の脆弱性を悪用し、複数の既知の攻撃手法を組み合わせ、ソーシャルエンジニアリングにより特定企業や個人をねらい、対応が難しく執拗な攻撃が出現してきている。この新しいサイバー攻撃は 2010 年の春頃から海外では APT(Advanced

[9] http://www.us-cert.gov/control_systems/icsjwg/presentations.html
[10]http://www.enisa.europa.eu/media/press-releases/eu-agency-analysis-of-2018stuxnet2019-malware-a-paradigm-shift-in-threats-and-critical-information-infrastructure-protection-1

Persistent Threats)と呼ばれている。

(1)新しいサイバー攻撃手法の分析[11]

セキュリティベンダー等の各機関が出しているレポートや IPA での解析結果を踏まえると、以下に示すように、情報システムへの潜入等の「共通攻撃手法」と、特定システムへの攻撃や情報の窃取等の目標に応じた「個別攻撃手法」から構成される攻撃であると分析している。

「共通攻撃手法」

① インターネット(標的型メール攻撃、フィッシング、改ざんされた Web アクセス等）や USB メモリを経由した一般の情報システムへのウイルス感染
② システムの脆弱性を利用した権限昇格や、組織内ネットワークや組織内の USB メモリを使用する業務フローを利用した情報システム内部へのウイルスの拡散
③ バックドアを作成し、外部の指令サーバ(C&C サーバ)と通信することにより、ウイルスの増強や新たなウイルスのダウンロードの実行

※ウイルスの増強やダウンロードは以降④⑤の手順でも実行される可能性がある。

「個別攻撃手法」

④ 制御装置をコントロールする制御システムや、組織の重要情報(機密情報、個人情報など）を管理する基幹システムへの侵入
⑤ 制御システムの管理下にある装置や、基幹システムが保有する組織情報に対する攻撃（破壊、改ざん、情報窃取等）の実行

Stuxnet のケースでは、③において 80 番ポート(HTTP) 経由での通信が行われ、④⑤において、原子力設備を管理する制御システムへの侵入と、正常なコントロールへの攻撃がなされたものとみられている。

IPA では、このように「共通攻撃手法」と「個別攻撃手法」を持った攻撃は、制御システムや組織の情報システムにとって今後の深刻な脅威になるとの認識から、『新しいタイプの攻撃』と名称付けしている。

(2)対策の方向性

日本における制御システムは、一般に米国等と比較して、制御ネットワークが独立・分離されている事に加え、制御システムも今回悪用された制御システムの製品ベンダとは異なる製品が多く使用されていることから、直ちに、海外と同様の脅威が発生するとは限らない。日本における適切な対策を進めるためには、単に技術的な情報を海外から得るだけでは無く、日本の実情に応じた影響の分析と対策を実施することが重要である。

[11] IPA テクニカルウォッチ:『新しいタイプの攻撃』に関するレポート
http://www.ipa.go.jp/about/technicalwatch/20101217.html

「共通攻撃手法」への対策として、攻撃の上流である①、②に対しては、一般的には、

・USB メモリ利用など業務フローの見直し

・ソーシャルエンジニアリングを用いた攻撃を回避するためのユーザ教育

・情報システムの脆弱性対策

・アンチウイルス対策

などが挙げられる。しかし、ユーザの行動を完全にコントロールすることは困難であるだけでなく、Stuxnet でも使用されたゼロデイの脆弱性を突かれた攻撃に対しては、これらでは確実な効果を期待することはできなくなる。従って、①②の後に続く③を抑止することが、本質的で有効な対策になるものと考えられる。これを実現できれば、結果として深刻な脅威となる「個別攻撃手法」を回避することに繋がるからである。その対策としては、

・システム設計時におけるネットワーク設計（外部との隔離や接続ルートの明確化）

・外部との通信における接続先のフィルタリング

・外部との接続点における通信の監視、制御機構

などが挙げられる。

「個別攻撃手法」に対する対策は、対象が個別の制御システムや情報システムなど幅広い各種システムが攻撃対象となるため、個別のシステムごとに固有で検討していくことが必要となる。その対策の候補として、USB 等の利用に関するルール、ネットワーク構成、動作ソフトウェアの認証、アクセス制御などが挙げられる。

攻撃者は Windows や Linux に熟知しているだけでなく、制御システムについての知識も十分持っていると推測される。このような攻撃者に対応するためには、防御側でも制御システムを含む幅広い技術者の連携で対応していく必要がある。

2.3 その他の動向

2.3.1 SCADA (Supervisory Control and Data Acquisition) マーケット

調査会社の Frost & Sullivan によると 、「SCADA 市場は昨年の 46 億ドルから、2016 年には 70 億ドル近くまで成長する見込であり、産業界が世界の SCADA 市場で直面している主要な課題の 1 つは強化されたサイバーセキュリティを行うことで、SCADA ベンダの多くは TCP/IP ベースの SCADA ネットワークに対する特別な産業用ファイアウォールや VPN ソリューションの開発展開によってサイバー脅威のリスクへの対処に焦点を当ててきている」と指摘している[12]。

2.3.2 脆弱性の顕在化

(1)制御システムにおける脆弱性の報告事例

2010 年 9 月に中国で広く使われている制御システム(SCADA 等)ソフトに脆弱性が発見された。この事例では脆弱性の通報から対応までに遅れが出るなど、脆弱性関連情報の適切な流通に関しても、未だ問題が残る事が明らかとなった。

[12] http://www.informationweek.com/blog/main/archives/2010/12/scada_security.html

今後もセキュリティ研究者等によって新しい脆弱性が発見されていく事も考えられる。

(2)制御システムにおける脆弱性対策情報の登録状況

IPA では、米国の NVD(National Vulnerability Database) などから制御システムのソフトウェアに対する脆弱性情報の収集を進め、対策情報を脆弱性対策情報データベース JVNiPedia に蓄積して、対策の促進を支援している。2011 年 2 月現在、JVNiPedia では 2008 年分として 8 件、2009 年分は 9 件、2010 年分は 6 件、2011 年分(2 月 21 日現在)は 9 件、合計 32 件の制御システム用ソフトウェアに関する脆弱性対策情報を公開している。

このように制御システム用ソフトウェアの脆弱性が顕在化している。

3.制御システムの脆弱性低減に向けた取組み

本章では、今年度の調査の主目標であるアジア各国の制御システムの脆弱性低減に向けた取り組みについて、最新動向を記載する(3.3 節)。更に、米国、欧州そして日本については、追加情報を記載する。米国、欧州、日本における取組みの全体像については、2009 年度報告書「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」[13]を参照の事。

なお、世界各国の制御システムセキュリティへの取組み状況を本報告書最終頁の図表・付 2 に示す。

3.1 米国における取組み

3.1.1 脆弱性低減のためのガイドやツールなどの整備・活用に関する動向

(1)ICSJWG(Industrial Control Systems Joint Working Group) の活動

2010 年の春と秋に開催された ICSJWG のカンファレンス[14]から以下をまとめた。

(a) ICSJWG の概要

米国政府は、2009 年の秋から国土安全保障省(DHS)がファンディングをし、政府だけでなく、民間も巻き込んだ産業用制御システム(ICS: Industrial Control Systems)を対象に、情報セキュリティの普及・啓発を推進するための情報交換を行う場として ICSJWG (Industrial Control Systems Joint Working Group) を推進している。毎年春、秋の 2 回実施している。

ICSJWG は、DHS の制御システムセキュリティプログラム CSSP(Control Systems Security Program)という制御システムのセキュリティを推進するプログラムの一環で開催されている。参加しやすいように参加費は無料となっている。米国政府関係からの参加者だけでなく、産業界や大学などからも参加し、欧州やオーストラリアからの参加者も多かったが、アジア系からの参加はあまり見られなかった。参加者リストは公開されていない。

(b) ICSJWG の各 WG 活動と進捗状況の概要

以下の 6 つのサブグループ（情報共有 SG、ベンダ SG、能力開発 SG、R&D SG、ロードマップ SG、国際 SG）から構成されている。

① 情報共有 SG ：Information Sharing Subgroup

情報共有の環境整備。米国では重要インフラ分野は 17 ある。情報共有の簡易ポータル HSIN-CS(Homeland Security Information Network - Critical Sectors)は、重要インフラ分野での情報共有を支援するポータルである。このポータルには、次のような情報が提供されている。

・ICSJWG 関係者（ステークホルダ）による最新情報アナウンス
・ICSJWG 関係サイトへのリンク(ICS-CERT(Industrial Control Systems Cyber Emergency Response Team)、FEMA(Federal Emergency Management Agency) 等)や報告

[13] http://www.ipa.go.jp/security/fy21/reports/ics_sec/index.html
[14] ICSJWG : http://www.us-cert.gov/control_systems/icsjwg/index.html

・ICSJWG の活動報告等
・コミュニケーションや共同作業のツール提供
・各種情報提供
なお、情報共有 SG への参加には、ICSJWG のサブ WG のどれかに参加が必要である。

② ベンダ SG ：Vendor Subgroup
85 メンバ。脆弱性情報公開についての文書類(Vulnerability Disclosure Position Paper)をまとめている。

③ 能力開発 SG ：Workforce Development Subgroup
制御システムについて他のサブ WG との連携で教育やトレーニングなどのカリキュラムの整備の推進を予定している。制御システムのセキュリティエンジニアの育成についても言及していた。

④R&D SG ：Research and Development Subgroup
2011 年と 2012 年の活動計画を議論した。エネルギー分野が中心。以下がそこでの要求項目。
・テスト環境
・統合した遠隔アクセスのアプローチ
・装置の構成管理
・ICCP(Inter Control Center Protocol)ファイアウォール
・システムへのトラステドコンピュータとアンカー
・大量データセットのデータ分析と統合
・ID 管理とクレデンシャル(証明書) のライフサイクル
・内部脅威としての行動分析
・ICS IP スイート”OPSAID”の拡張利用
(OPSAID: Open PCS (Process Control System) Security Architecture for Interoperable Design)
・各種活動に役立つラボと R&D
・重要インフラ内での相互依存性

⑤ロードマップ SG：ICS Roadmap Development Subgroup
2010 年の春には、水・ダム・エネルギー・化学の 4 つの既存ロードマップの評価と業界横断的ロードマップ作成(2011 年目標)が説明された。秋の報告では、特に進展ないようであり、推進が難しいことが窺われた。

⑥国際 SG ：International Subgroup
40 メンバ。もっと参加者を増やしたいが、テレコンや対面会議は効率が悪いため、

HSIN(Homeland Security Information Network) の利用を検討していきたいとの報告があった。議論、提起されていた課題は以下である。

・各国の組織･コンタクトのリスト作成

・ICSJWG、CPNI(英国 Centre for Protection of National Infrastructure)、WIB(オランダ International Instrument Users' Association)・・・等の連携推進

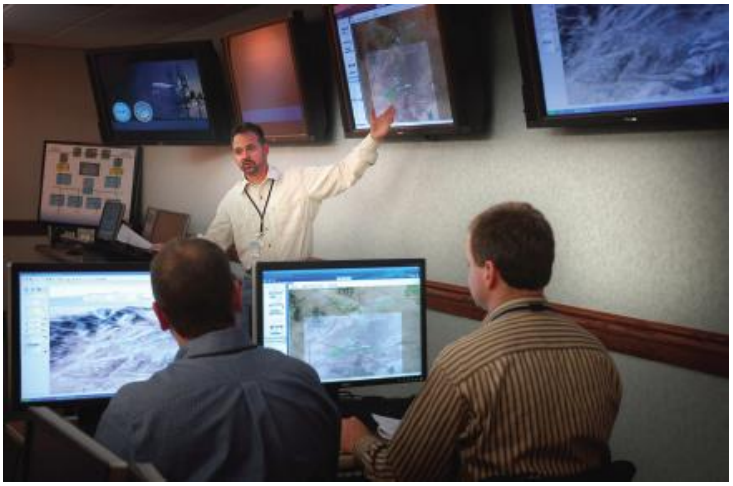
・グローバル SCM(Supply Chain Management) の視点から、米国だけでなく、その他の国での制御システムのセキュリティ対策推進の必要性

(2) ICS-CERT(Industrial Control Systems Cyber Emergency Response Team)

NCCIC(National Cybersecurity & Communication Integration Center: 国家サイバーセキュリティ・コミュニケーション統合センター) の配下の組織である。ICS(産業用制御システム) と重要インフラコミュニティへの貢献を目的としている。

(a) ICS-CERT の活動

図表 3-1 ICS-CERT の様子



出典：DHS ICS-CERT パンフレット

2010 年の活動成果として以下を挙げている[15]。

・13 のインシデント評価に参加

・32 のアラートとアドバイス発行

・4 つの ICS 分析レポート

・4 つの ICS デジタルメディア分析レポート

・週間ダイジェスト

技術分析では、マルウェアと組込みシステム分析、影響・重要度(Consequence) 分析、制御システム分析を実施。脆弱性管理では、協調しての開示、予想外の(Unanticipated) 開示を実施。オンサイトでの支援も実施。コミュニティへの認知度向上(Awareness)では、

[15] www.us-cert.gov/control_system

情報共有、インダストリでの会議参加(35 に参加)、ウェブサイトでの情報共有(サイバーセキュリティガイダンス、ベストプラクティス) を実施。

(b) セキュリティ研究と脆弱性開示事例

英国の制御システム開発企業 Invensys 社、セキュリティ専門企業 IOActive 社と ICS-CERT の 3 者の連携で脆弱性情報を責任ある手続きの下で開示することができたと言う事例紹介が ICSJWG カンファレンスであった。このような事例紹介をすることで、ほかの制御システム製品ベンダも脆弱性への対応に責任ある開示をするようになることが期待される。

対象の脆弱性 : Vulnerability Note VU#703189[16]

3.1.2 制御システム脆弱性の評価・検証に関する動向

(1)アイダホ国立研究所の制御システムセキュリティ教育プログラム

INL(Idaho National Laboratory : アイダホ国立研究所)の NSTB(ナショナル SCADA (Supervisory Control And Data Acquisition) テストベッド)プログラムには、トレイニング(訓練、教育)のコースがあり、制御システムの各種関係者へのセキュリティ教育を目的としている。エネルギー分野でのシステムを対象としているが、内容的には他の分野でも共用できる。3 つのコースが設定されていて、4 時間と 8 時間のコースは NERC(North American Electric Reliability Corporation)の教育継続クレジット(continuing education credits) に利用できる。トレーニングの概要は以下である。

a)初級 SCADA セキュリティ : 4 時間コース[17]

119 ページのパワーポイント教材が利用されている。

b)中級 SCADA セキュリティ: 8 時間コース[18]

218 ページのパワーポイント教材が利用されている。実際の SCADA ネットワークモデルを利用した実習もある。

c)上級 SCADA セキュリティレッド/ブルーチーム : 5 日間[19]

約 35 人をいくつかのチームに分けて、後半には攻撃・防御の実戦を経験することができる。

なお、INL への訪問時のヒアリングから、以下のことが分かった。

INL では重要インフラシステムのセキュリティを学習するために、学習者達がそれぞれ、ブルーチーム(守備側) とレッドチーム(攻撃側) に分かれ、実際に PC 上から攻撃等を行いながら、防御策あるいは攻撃者の視点について学ぶプログラムが実施されている。

プログラム終了後のブリーフィングでまとめられた意見に関しては、

・「何を守るべきか」を設定しない限り、ディフェンスは難しい

・自身のネットワークを誰がどのように使っているか等の熟知が必要である

・ハッキングはとても難しいが、フィッシングは意外と成功する

---

[16] Invensys Wonderware Archestra ConfigurationAccessComponent ActiveX control stack buffer overflow

[17] http://www.inl.gov/scada/training/d/4hr_introductory_scada_security.pdf

[18] http://www.inl.gov/scada/training/intermediate_scada.shtml

[19] http://www.inl.gov/scada/training/advanced_scada.shtml

などが挙げられているとのことで、セキュリティ分野から見ると、目新しい項目ではないが、実際の体験を通して、言葉の意味としてだけではなく実感する事で、経験と知識が身に付くものと推察された。本プログラムにおいては、ホワイトチームと呼ばれる攻撃側にも防御側にも手助けをする存在がおり、演習を「面白く」実施することも、学習意欲を促す結果につながっているのではないかと考えられる。

3.1.3 制御システムのセキュリティ障害事例データベースに関する動向

2010 年 4 月の ICSJWG カンファレンスで、制御システムについてのセキュリティインシデント(事件) のデータベースである RISI(Repository of Industrial Security Incidents)[20] の紹介があった。以下は、その講演での資料[21]に 基づいている。なお、2011 年の最新公開レポートに関しては、2.1(2)を参照の事。

(1)RISI の経緯

BCIT(ブリティッシュコロンビア大学)が ISID(Industrial Security Incidents Database)を、2001.1.1 に構築し、蓄積していた。2006 年に中止されたが、それを Byres 社が購入し、2008.1.1 より RISI としてサービスを開始した。2009 年に exida 社が Byres 社を買収し、Security Incidents Organization (SIO) というノンプロフィットの組織を立ち上げた。

内容は ISID のデータに 2006 年以降のインシデント情報を追加したものとなっている。

(2)制御システムのインシデントの推移

2009 年までには 162 件のセキュリティインシデントが蓄積されている。その情報の内容はインシデントごとに信頼度(4 段階)、インシデント種別などの以下の項目からなる：

- ・インシデントタイトル
- ・インシデント発生日
- ・報告の信頼度(確認した、未確認だが本当らしい、本当でなさそう、悪ふざけ)
- ・インシデント種別(事故、外部からのハッキング、ウイルス)
- ・産業分野(石油、パルプ、自動車・・・)
- ・エントリーポイント
- ・簡単な事象の説明
- ・影響を受けた装置、
- ・インパクト　　等

なお、セキュリティインシデントの推移(種別毎、産業毎) については、2.1 節を参照の事(図表 2-3、2-4)。

産業分野別の攻撃の数と攻撃の変化状況を図表 3-2 に示す。近年はライフライン系の攻撃が増加していることが窺われる。

---

[20] http://www.securityincidents.org/

[21] What Went Wrong? A Study of Actual Industrial Cyber Security Incidents
http://www.us-cert.gov/control_systems/icsjwg/presentations/spring2010/02%20-%20Zach%20Tudor.pdf

図表 3-2　　攻撃の変化状況

Industry Type	2000-2004	2005-2009	% Change
Water/Waste Water	3	14	367%
Power and Utilities	10	13	30%
Transportation	10	10	0
Food & Beverage	5	3	-40%
Petroleum	19	3	-84%
Chemical	8	1	-88%

(3)具体的なインシデント例

少し古いインシデントであるが、2010 年 4 月の ICSJWG カンファレンスで紹介されたインシデント事例(2 件)は以下である。

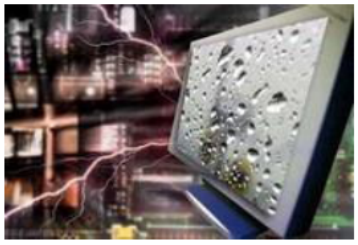
(a) ハッカーが水道システムのコンピュータに侵入

Risi

The Repository of Industrial Security Incidents
www.securityincidents.org

Hackers Penetrate Water System Computers

Date:	October 2006
Company:	Harrisburg Water System
Location:	Harrisburg, PA, USA
Industry:	Water & Wastewater
Incident Type:	Intentional - External - Hacker
Impact:	Unknown

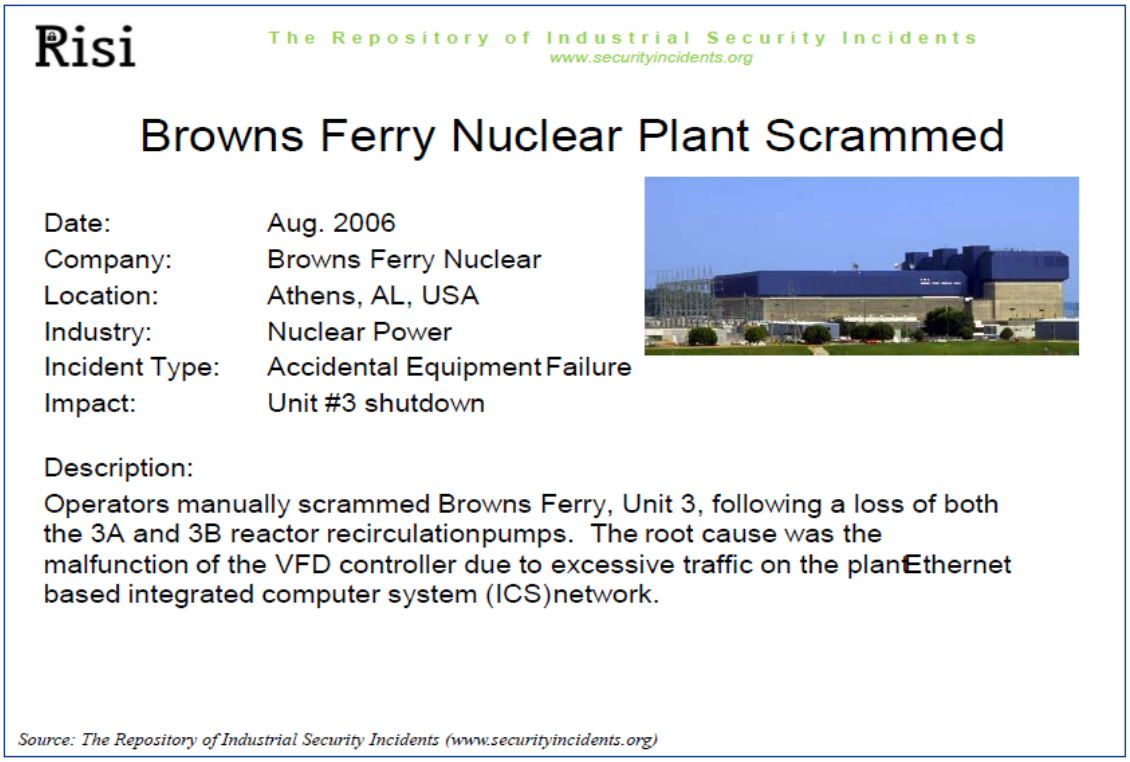


Description:
A foreign-based hacker used the internet to infiltrate the laptop (via internet) of an employee at the Harrisburg water system. The hacker used the employee's remote access as the entry point into the SCADA system and installed malware and spyware on a SCADA HMI computer.

Source: The Repository of Industrial Security Incidents (www.securityincidents.org)

出典：RISI 講演資料

(b) ブラウンズ・フェリー原子力発電所で原子炉緊急停止



出典：RISI 講演資料

3.1.4 制御システムの認証に関する動向

2010 年 10 月に開催された ICSJWG での講演および資料をベースとした報告とその情報から調査した、認証に関する動向について以下に説明する。

(1)事業者から製品調達時の認証についての事例報告

シェル、シェブロン(エネルギー(石油) 会社)の制御システム運用事業者から、セキュリティ製品を調達するときの認証についての事例報告がそれぞれあった。

① セキュリティ製品を開発しているベンダのプロセス(組織、製造、保守の 3 つのプロセス) を評価するもの

② セキュリティ製品の全体のセキュリティ、セキュリティ機能実装レベル、通信レベルのテストを評価するもの

これらいずれも、事業者、製品ベンダ、標準組織等の連携で推進されている。以下、その概要を説明する。

(a) セキュリティ製品調達時の要求規格(シェルの発表事例)

・シェル、デュポンや BP(British Petroleum) などがメンバである WIB[22](International Instrument Users' Association：http)が、制御システムのセキュリティ製品を調達

[22] http://www.wib.nl/

するときの要求規格を策定し、試行を開始した。
・ISO/IEC 15408 CC(Common Criteria)のような製品の細かなセキュリティ仕様に対する規格ではなく、製品を開発し提供するベンダの組織、製造、保守の3つのプロセスについて評価する規格で、23のプロセスに対しての要求規格からなる。
・セキュリティには従うべき標準が多数あるが、的確な標準がなく、ブレンドせざるを得ない。
・2010年4月時点で現在5社がグローバルサプライヤとして認定されている。
・事業者が多種多様のセキュリティ製品を調達する困難さを解決しようとする動きである。

(b) 製品の認証(シェブロン、セキュリティ標準機関ISCIとの合同発表事例)
ISA-99と呼ばれる制御システムのセキュリティ標準に準拠したかを評価するISASecure Embedded Device Security Assurance(EDSA)について紹介された。
・システム全体でのセキュリティ評価、製品実装レベルの評価、レイヤ4までの通信レベルのテストの3つの評価・認証
・通信レベルのテストとして、2010.5.30からCRT(Communication Robustness Test)をEDSA認証として開始。ISO/IEC61508のSIL(Security Integrity Level)認証と同様の位置づけ。
・EDSAは次の3つの階層から構成されている。
・SDSA(Software Development Security Assessment):システマティックセキュリティ評価で、ISO/IEC 61508、ISO/IEC 15408-1/3、OWASP CLASP等を参照している。
・FSA(Functional Security Assessment):実装レベルの評価で、ISA-99、NERC、NIST800-53、ISO/IEC 15408等を参照している。
・CRT(Communication Robustness Testing):レイヤ4までの通信レベルのテストで、プロトコルテストスイーツで5つのグループ分けになっている
・シェブロンは調達ドキュメントにISASecureを入れていると発表し、ベンダでの対応を期待している。

(a)、(b) ともに事業者が標準機関やベンダと一緒になってセキュリティ製品調達の要求レベルを規格とし、セキュリティレベルを確保しようとしている動きであり、日本の制御システム向けの装置を販売しているベンダに対しても重要な動きとなってくるものと考える。ただ、日本からの参加者からは、セキュリティは海外の事業者からの要求で対応しているが、国内の事業者は機能の数を要求してセキュリティ要求はまだという状況とのことであった。
なお、(a)に関する追加関連情報については 3.2.3(1)で、(b)に関する追加関連情報は以下の(2)で記述する。

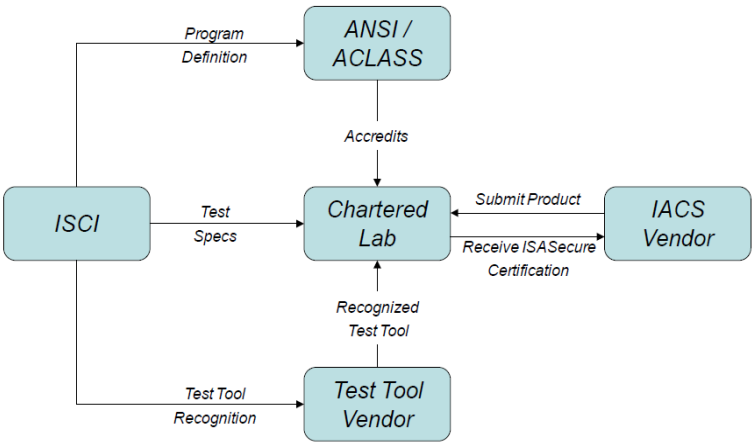
(2)ISCI(ISA Security Compliance Institute)の活動
前項で挙げた(1)(b)ISAに関して、公開情報など含め、活動を紹介する、
ISA Security Compliance Institute(ISCI)は、2007年にISAのASCI(Automation

Standards Compliance Institute)のもとに設立された。重要な制御システム製品のテスト(testing)と認証 (Certification)の規格化と手続き化が目的である。

現在のメンバには、シェブロン、Egemin、exida、エクソンモバイル、ハネウエル、Invensys、Mu Dynamics、Rockwell Automation、Siemens、横河、ISA99/ISCI Joint WG リエゾン等が参画している。

ISCI では、新たに ISASecure™ Embedded Device Security Assurance(EDSA：組込みデバイスセキュリティ保証)認証プログラムを開始した。図表 3-3 に示すようにテスト仕様を提示し、テストラボの公認(Accredit)やテストツールの承認(Recognition)などを実施している。ISO/IEC61508 機能安全規格の SIL(safety Integrity Level:安全度水準)と同様なものだと述べている。図表 3-4 に示すトレードマーク商標も用意しており、ウェブサイト[23]も公開している。

図表 3-3　　ISASecure プログラムの関係



図表 3-4　ISASecure 商標

ESDA の全体系を、図表 3-5 に示す。ESDA は、システム全体でのセキュリティ評価、製品実装レベルの評価、通信レベルのテストからなる以下の 3 つの階層からなる。

・SDSA: Software Development Security Assessment
　ライフサイクルでのセキュアなソフトウエアエンジニアリングで、ISO/IEC15408、ISO/IEC 61508 パート 3 等が参考規格となっている。

・FSA: Functional Security Assessment

[23] http://www.isasecure.org/

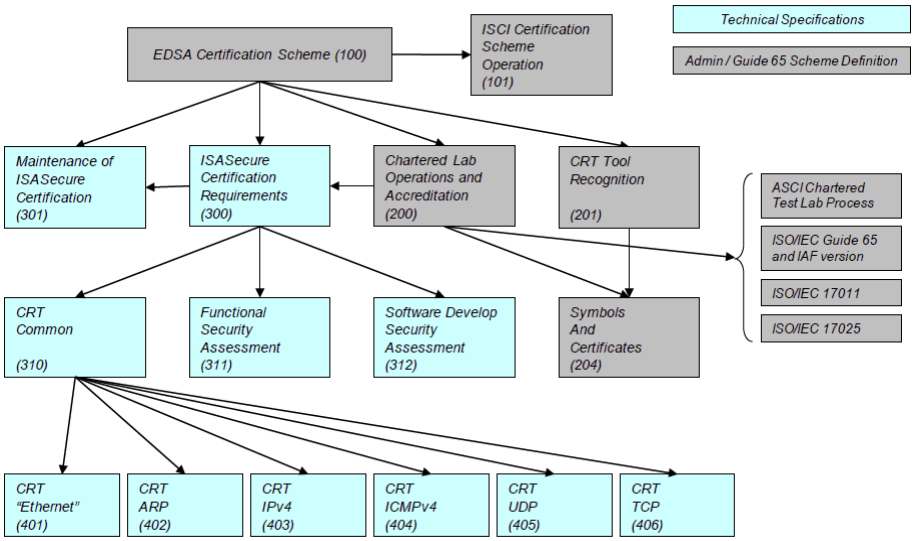
ISA99、NERC(North American Electric Reliability Council)の CIP-001-1 から CIP-001-9、NIST-800-53、NIST800-53 等の機能的なセキュリティ評価が参考規格となっている。

・CRT: Communication Robustness Tests

通信プロトコルの検証でイーサネット、ARP、IPv4、ICMPv4、UDP、TCP が現在対象となっている。拡張予定。

この通信分野では Wurldtech 社と協調していて、Achilles のレベル 1 テスト仕様と連携している。12 月にテスト製品が出荷される。さらに、exida 社は最初の公認テストラボに 2010 年 11 月になったと報告されている[24]。

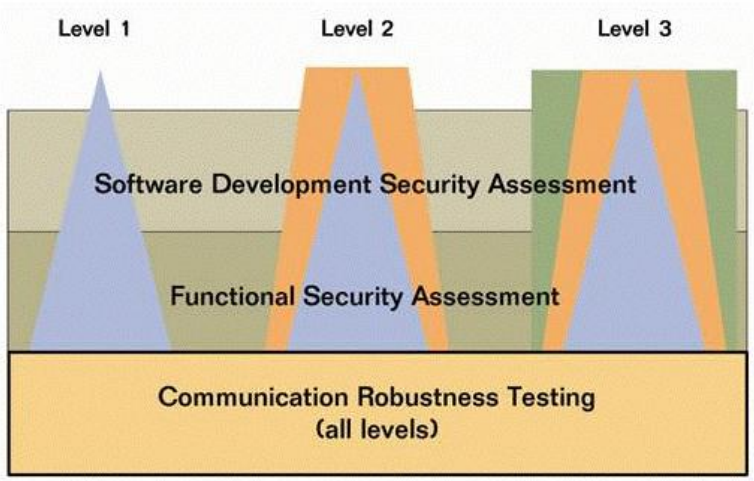
図表 3-5　ISASecure EDSA プログラムの全体系



また、ISASecure EDSA の認証のレベルは図表 3-6 に示す 3 段階となっている。CRT は各レベルに共通であるが、SDSA および FSA はレベルが上がるごとにの要件が追加されていく構造となっている。

[24]http://www.isasecure.org/News-Room/Press-Releases/Exida-is-first-certification-lab-to-achieve-ANSI-A.aspx

図表 3-6　ISASecure 認証レベル



3.2　欧州における取組み

3.2.1　脆弱性低減のためのガイドやツールなどの整備・活用に関する動向

(1)ENISA の進める CIIP プログラムとレジリエンシー

重要情報インフラ基盤 CIIP(Critical Information Infrastructure Protection)に対する脅威は現実のものとの認識で、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用意している。2008 年は準備期間で、2009 年に低減に向けての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 II のような対応を開始するとしている。具体的にはメンバ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」[25]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[26]でのサイバー攻撃に備えた演習を実施した。

特に通信事業に対して、Article13a の新しい対応を進めている。各国での通信インフラでの最低レベルを確保するための実装推奨や情報共用促進をするよう指導し、2011 年 5 月 15 日までに対応することを要求している。最低限のセキュリティレベルを確保すると言う

[25]ENISA:「CYBER EUROPE 2010 Exercise has started」
http://www.enisa.europa.eu/media/news-items/cyber-europe-2010-exercise-live〔Last visited on Jan.27, 2011〕
[26] ENISA:「Q&As on the first, pan-European Cyber Security Exercise 'CYBER EUROPE 2010'」
http://www.enisa.europa.eu/media/news-items/faqs-cyber-europe-2010-final〔Last visited on Jan.27, 2011〕

考え方を推進しており、通信としてはIPv6、DNSSecへの対応を推進している。
R&Dとしては、まず第1にクラウドコンピューティングを挙げ、リアルタイムでの検出や診断システム、無線ネットワーク、スマートグリッドとSCADA、センサネットワーク等の研究開発に力を入れていくことを挙げている。
CII(Critical Information Infrastructure)のセキュリティとレジリエンス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。

3.2.2 制御システム脆弱性の評価・検証に関する動向

CRITIS2010（CRITIS：Critical Information Infrastructure Security、重要情報インフラセキュリティ）における評価・検証に関係するトピックスを紹介する。

(1)エネルギー制御システムでのカスケード効果（あることが次々と影響を及ぼしていくこと）制御を実現する早期警報システム（Early Warning System）

スペインのマラガ大学より、遠隔地にある監視装置やアクチュエータ等の装置にセンサを設置し、センサと無線技術ZigBeeとISA100.11aを組み合わせた無線センサネットワーク（WSN: Wireless Sensor Network)から装置等の状況情報を収集するシステムの発表があった。
膨大なデータをSCADA(Supervisory Control And Data Acquisition：監視制御システム)センターにそのまま送るのではなく、何が発生したかを科学的に分析する技術と組み合わせ、状況の変化を分析し、その分析データをSCADAセンターに送ることにより遠隔地で発生している状況を早期に把握し、必要な警報や対処を実現する研究報告である。
今後遠隔地の多様な装置にセンサを取り付け、状況変動を監視するケースが増加するものと推測されるので、このような手法は有効になると考える。

(2)欧州SCADAセキュリティテストベッド

論文「Creating a European SCADA Security testbed」では、欧州は本来的に多国環境であるので、政策、財政、戦略的な考慮を参加国はしなければならない、と主張している。CERN（the European Organization for Nuclear Research）のような研究機関の検討によれば、欧州SCADAセキュリティテストベッドはうまく行く可能性が高いと述べている。

3.2.3 制御システムのセキュリティ障害事例データベースに関する動向

(1)オランダにおける取組み[27]

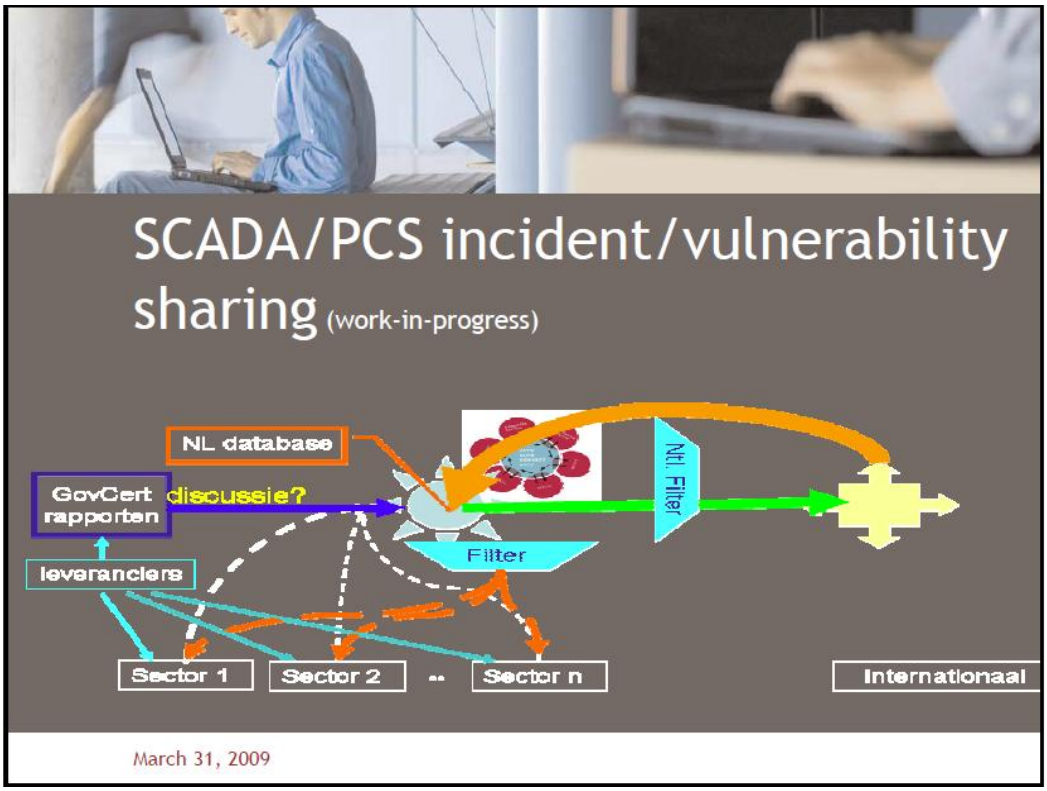
国内的にも国際的にも制御システムの重要性や緊急性の認識は高くなっているが、PCSのインシデント情報は、公開されない傾向が強くなっている。2006年にオランダ経済省の依頼でTNO(The Netherlands Organization for Applied Scientific Research) [28]とKEMA [29]が行

[27] http://cpni.nl/publications/PCS_brochure-UK.pdf
[28] http://www.tno.nl/ 欧州最大級のオランダの研究開発機関
[29] http://www.kema.com/about/Default.aspx 電力などエネルギー業界を専門とし、技術コンサルティングや各種安全・品質保証規格等の認証・認定サービスを提供する、オランダのグローバル企業

った調査でも、公開情報を見る限り殆ど報告されていない。顕在化したケースでも「機器の故障」「原因は不明」とされている場合が多い。

オランダでは、既存の官民セクタ横断的情報共有の仕組みである Cybercrime Information Exchange を通じ、PCS に関するインシデント情報もデータベース化し、共有する取り組みを試行している。このデータベースは GOVCERT.NL（オランダの国家 CERT）が管理しており、情報の共有は任意で、Exchange のメンバであれば誰でもアクセス可能としている。その構成イメージを、図表 3-7 に示す。

図表 3-7　オランダにおける制御システムのインシデント／脆弱性情報共有 DB の仕組み



出典：samen tegen cybercrime 公開資料[30]

3.2.4　制御システムの認証に関する動向

(1)WIB(International Instrument Users' Association)

1962 年にドイツの５つのプロセス産業事業者(現在のシェル等)が、プロセス装置のテストや結果の情報共有をするために集まったのが最初である。本部はオランダのハーグにある。

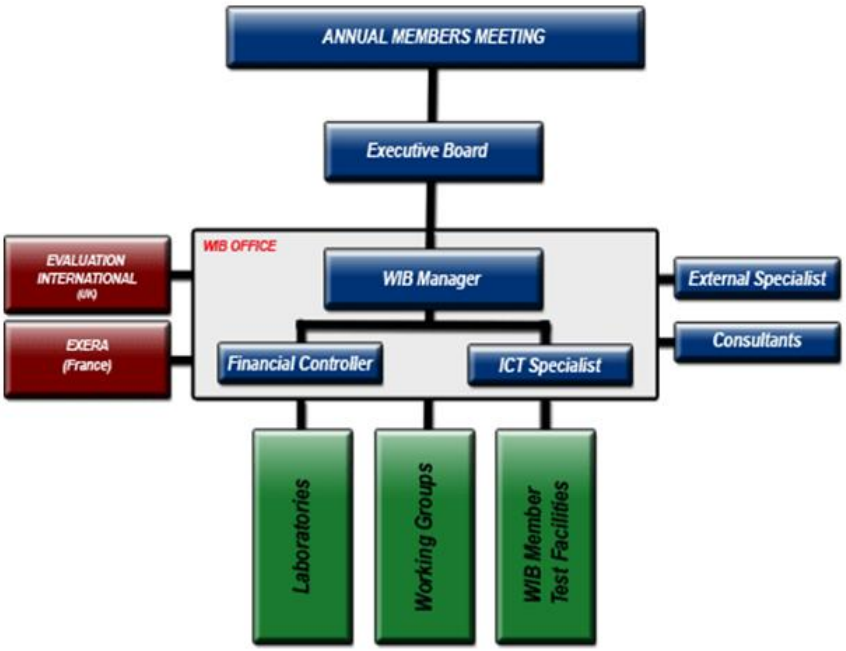
プロセス装置に対する事業者主体で、ベンダとの協調も進めている組織で、ベンダに対

[30]:http://ec.europa.eu/information_society/policy/nis/docs/vulnerabilities_workshop/s10_luijf_tno.pdf

するセキュリティ要件なども提案している。具体的なものとしては、2010 年 10 月に第 2 版[31]が発行されている。

図表 3-8 に WIB の機構図を示す。

図表 3-8　　WIB の機構図



3.3　アジア各国における取組み

国家間で統一されたセキュリティ施策に取り組む欧州や、世界的にも最も進んだセキュリティ対応として DHS を中心とする官側と民間事業者が連携して構築しようとしている米国等と比較すると、アジア地域の各国の施策には大きな疎密がみられる。アジアにおいては事業活動を行っている主要な制御システムベンダーは先進国の企業が多く、企業が実施する国際的なセキュリティ基準に依存している現状がある。各国の政府関係者は、政府間や企業間の組織的な連携が乏しい現状から鑑みて、官民で協力して総合的な対応が必要となる情報セキュリティへの対応に対し、懸念事項が少なくないと認識している。

アジアにおいては東アジア諸国、ASEAN 諸国、南アジア諸国のそれぞれにおいて、社会システム等の成熟した社会経済の発展した国家、急速に経済成長を遂げてきた国家と、未だに開発途上にある国家が混在した状況にある。

このようなアジア諸国の社会的経済的環境の違いを踏まえて、韓国、中国、タイを中心に取り上げて制御システムの情報セキュリティ動向を調査した。

3.3.1　韓国

[31]「Process Control Domain- Security Requirements for Vendors　Report: M2784-X-10」
http://www.wib.nl/reportindex/WIB_M2784_PCS_vendorsecurity_v2.pdf

2009 年 7 月に発生したインターネットにおける大規模な DDoS 攻撃(いわゆる 7.7 大乱)を契機に、韓国ではサイバーセキュリティ対策の見直しがなされ、サイバー部隊の新設など幾つかの対策がなされた。　韓国においては、韓国インターネット振興院(KISA：Korea Internet＆ Security Agency) が民間セクタにおける情報セキュリティ政策全般の実施に取り組んでいる。韓国においても制御システムは重要インフラ等で利用されており、制御システムのセキュリティに関して、官民で様々な取組みが行われている。

(1)脆弱性低減のためのガイドやツールなどの整備・活用に関する動向

韓国では、国家的な次元で制御システムにかかわるガイドラインを配布して保安水準の向上に努力している[32]。

重要インフラに関する主要な施設は、情報通信基盤保護法のうちの主要基盤施設として指定されており、毎年脆弱性の分析を実施し、保護対策を行っている。

脆弱性の分析手法としては情報セキュリティ安全診断制度（ISCS：Information Security Check Service）[33]などがある。

(2)制御システム脆弱性の評価・検証に関する動向

国家公共機関に納品する情報セキュリティ関連製品に対しては、CC(Common　Criteria)の評価や保安適合性の検証制度が実施されている。また、韓国独自の情報セキュリティ評価認証制度 KECS(Korea IT Security Evaluation and Certification Scheme) に沿った情報セキュリティ関連製品の評価を行っている。

韓国電力公社 KEPCO[34]においては、電力系の監視制御システムに HARRIS 社の製品[35]が使用されており[36]、規格は米国の ANSI/IEEEC37.1 が適用されている。KEPCO の次世代 SCADA(Supervisory Control And Data Acquisition) システムは IEC61850 を基準にデータベースサーバ処理とデータベースリアルタイム処理 に IEC61970 が使用されている[37]。また、分散制御システム DCS(Distributed Control System) に対するサイバー攻撃に対して、テストベッド等を使ってセキュリティプロトコルの検討を行っている[38]。

---

[32] 韓国世宗研究所・国家保安研究院へのヒアリングによる

[33] 例えば韓国インターネット振興院(KISA)の ISCS(Information Security Check Service for Strengthening the Stability　and Reliability of Information　Communication Service)
http://www.wseas.us/e-library/conferences/2005miami/papers/501-235.pdf

[34] 韓国電力公社　http://www.kepco.co.kr/eng/

[35] Harris Coopration　http://www.harris.com/

[36]"Power system and technical issues in South Korea"JK Park- 2001

[37] KEPCO Automation - Smart(KEPA-S)
https://www.kdn.com/home3/we/gs/WEGS_0303.jsp

[38] Security Protocols Against Cyber Attacks in the Distribution Automation System,LH Lim 他
IEEE, Transactions on Power Delivery Vol 25, No.1, Jan. 2010
プロトコルについては IEC TC57 WG15, IEC60870-5. ソウル近郊の龍仁市の明知大学にテストベッドを設置している。

現在韓国の上水道系においては、韓国政府は 2010 年 10 月「水産業育成戦略」を発表し政府主導により2020年までに8社の水企業を育成し水道の民営化推進を進めているが、現在、K-Water 社は、横河電機が協力して開発してきた HMI/SCADA Water-K software を使用している[39]。韓国で運用されている制御システムには、一般的に、ベンダが採用している国際標準が導入されている。制御システムの情報セキュリティ規格 ISA99 の委員会にも参加しており、2011 年春の ISA 会合の開催国となっている。ISA-99 が IEC/TC65 の IEC62443 に統合される方向にあることから、韓国はこの動向を視野に情報セキュリティへの注力を図ろうとしている[40]。

(3)制御システムのセキュリティ障害事例データベースに関する動向

制御系システムの情報セキュリティに関連する事故や事案などに対するデータベースは現在公式にはつくられていない。KRCERT/CC[41]などのデータベースに含まれて報告されている。

(4)制御システムの認証に関する動向

世界的な共通基準に基づく製品評価に関し、韓国は認証国(CAP:Certificate Authorizing Participant) として CC 承認アレンジメント(CCRA : CC Recognition Arrangement) に正式に加盟している。

制御系システムの情報セキュリティに特化した認証は、国としては実施していない。

3.3.2 中国

中国では Stuxnet の問題は関係機関や重要インフラ事業に関わる制御系システム関連企業などで深刻に受け止められた。Stuxnet を中国では“震動”と中国訳しているが、通常は「超級工廠病毒」と称している。つまり「めったにない超級クラスの工業関連のワーム」という受け止め方である。新華社通信では中国では業務に関係する 600 万台以上の個人コンピュータ、約 1,000 社の企業内コンピュータに Stuxnet の感染が見られたと報告されていた。

このような工業における制御システム(中国では「工業控制系統」という) の情報セキュリティの安全問題について、Stuxnet の問題によって初めて大規模な関心が集められたものである。

この問題について「工業網路安全形勢分析」(2011 年 1 月 11 日) などの分析が中国の制御システムの安全問題について概況を示している。そこでは 2003 年 1 月のスラマーワームの多量汚染事件、2005 年 8 月のダイムラー・クライスラー13 工場のワーム汚染による操業

[39] Korean Water Resources Corporation, STARDOM's OPC Communication with HMI/SCADA
[40] ISA では、委員会(committee)は ISA99、ガイドラインは、ISA-99 と称されている。
[41] KRCERT/CC の URL は http://www.krcert.or.kr/index.jsp

停止事件、2006 年 10 月のペンシルバニア州ハリスバーグの浄水場コンピュータシステム侵入事案などを引用しつつ、中国が直面する問題を指摘している。中国の制御システム系統(分散制御システム DCS、プログラムされたロジックコントロール PLC、プロセスコントロールシステム PCS 等）や SCADA などにおいては、オープンなシステムが使用されてきていることから、そこに内在する脆弱性を攻撃される脅威が増大してきていると述べている。

(1)脆弱性低減のためのガイドやツールなどの整備・活用に関する動向

制御システムおける情報セキュリティの役割の増大に伴い、システムメーカやベンダが準拠している国際的なセキュリティ基準などに依存しつつ、国家的なガイドやツールなどの整備を図ろうとしている。脆弱性低減のためのガイドやツールに関しては IEC62443 へ統合される ISA-99 と IEC/TC65 を参考としつつ、専門家は米国国土安全保障省のガイドライン[42]を照合することも強調している[43]。

(2)制御システム脆弱性の評価・検証に関する動向

北京亜控科技[44]の SCADA ソフト「Kingview 6.5.3」の脆弱性問題を一例として、中国では産業インフラ監視制御用の SCADA ソフトの脆弱性の検証とそのためのガイドラインの必要を認めているが、ANSI/ISA-99 Standards の要求をベースとして国際的な標準に沿った形での施策が考えられている。

(3)制御システムのセキュリティ障害事例データベースに関する動向

制御システムなどの事案のデータベースとしては「国家信息安全漏洞共享平台(国家情報セキュリティホール共有プラットフォーム)」(China National Vulnerability Database) [45]が置かれており「国家互連聯網(インターネット）応急中心」(国家計算機網絡応急技術協調中心）(CNCERT/CC) [46]の関係組織となっている。

これらは国務院の「工業と信息化部」の傘下組織であり、情報セキュリティに関しては「工業と信息化部」信息安全協調司[47]の監督下にある。

(4)制御システムの認証に関する動向

中国の工業用制御システムに関係する化学工業部門や情報セキュリティ産業などを担当する「工業と情報化部」では公安部や関係部門とともに情報セキュリティの認証と工業用制御システムの認証をカバーできる認証体系の構築を求めているが、現在のところ世界の動向を踏まえて関連する標準・規格を精査している段階であり、制御システムの情報セキュリティ

[42]化学工業反テロ基準(CFATS:: Chemical Facility Anti-Terrorism Standards)等を示している。なお 米国国土安全保障省のガイドラインは http://www.thinktec.org/UserFiles/File/S.%20McGurk.pdf P48 に記載がある
[43]工业网络安全形势分析
[44]北京亜控科技発展有限公司の URL は http://www.gkong.com/comm/user_vip_info.asp?id=52931
[45]http://www.cnvd.org.cn/
[46]http://www.cert.org.cn/
[47] http://xxaqs.miit.gov.cn/

に対応した認証システムの構築には至っていない。

(5)制御システムのセキュリティ標準・規格に関する動向

中国国内においては工業における制御システムの情報セキュリティを保護する国内の標準はまだできていない。公安部や関係部門は制御システムの情報セキュリティについて安全等級区分標準や保護の具体的方法などを制定すべく大きな関心を示している。

中国の工業における制御システムは長らく低い水準にあり、安全問題を含めて早急に高度化を図らねばならないとし、国としても『国家信息化安全標準化“十一五(第 11 次 5 カ年計画)”計画』で ICS の安全標準を作ることはその重点となっていると、「工業控制系統(ICS)的安全研究解析」(2011 年 1 月 5 日、e-works) で述べられている。

中国における制御システムの情報セキュリティに関しては政府も国際動向に大きな関心を示してきている。中国における製造設備などに関する国家標準規格としては GB(Guo jia Biao zhun:国家標準) がある。GB は国家の強制規格であり、GB/T は国家の勧奨規格である。また GB/Z は国家の指導的技術的な標準である。

制御システムの情報セキュリティに関しては、現在中国の強制的な規格である GB は制定されていない。

全国工業過程測量及び控制標準化技術委員会 SAC/124[48]は中国の国家規格の制定修正などを実施する機関であり、機械工業儀器儀表総合技術経済研究所(ITEI) [49]が事務局を務めている。国際的な規格の対応は全国工業過程測量及び控制標準化技術委員会 SAC/124 が対応を行っている。

中国では強制標準として「工業自動化製品安全要求」の中で 21 項目がある[50]。全国工業過程測量及び控制標準化技術委員会によれば工業用制御システムの情報システム標準は次のようなものがあるが[51]、2010 年 8 月時点で、一部は制定中である(図表 3-9) 。

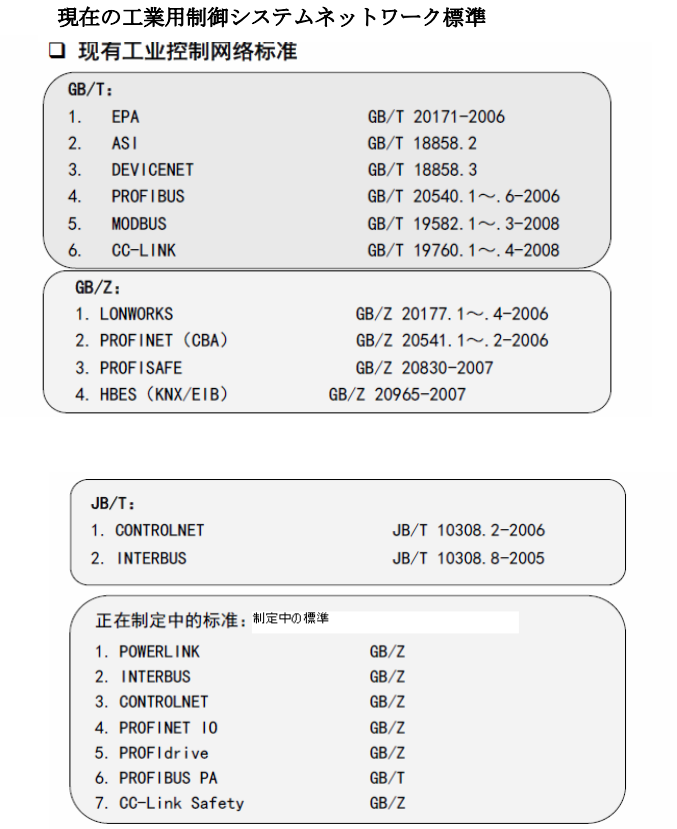
[48]http://www.tc124.com/

[49] 儀器儀表は器械計器の意

[50] 中国化工仪器网 http://www.chem17.com/News/Detail/8265.html

[51] 工业控制網路标准解析 2010 年 8 月 6 日

図表 3-9　中国の工業用制御システムの情報システム標準

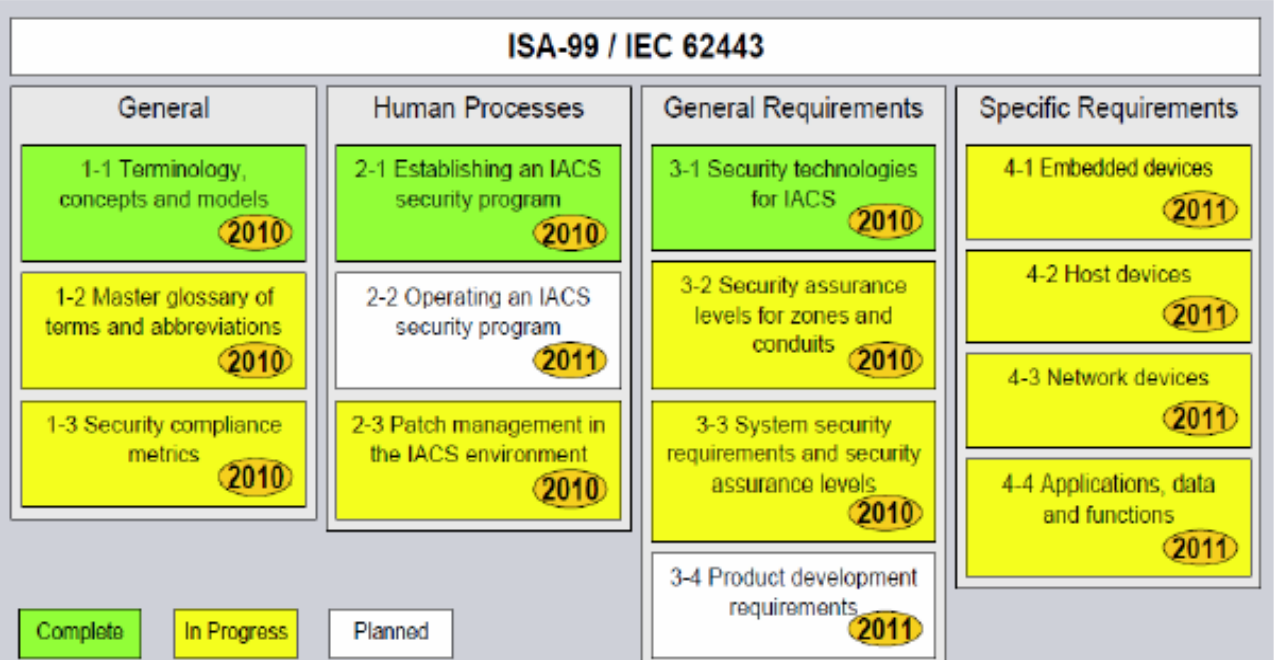


出典：工業控制網路標準解析

情報セキュリティの国際標準については、中国で何回かの国際会議を行っている。IEC62443 と ISA-99 の現在の状況について中国は図表 3-10 のように整理している。この図表に示されているように、中国は IEC62443 と ISA-99 の動きに関心を払っており、中国の制御システム情報セキュリティについては国際的標準の適用の検討を進めているものと推測される。

図表 3-10　IEC62443 及び ISA-99 の中国における整理

◆ 信息安全标准框架　（情報セキュリティ標準スキーム）



出典：工業控制網路標準解析

3.3.3　タイ

ThaiCERT の報告によれば，2008 年に ThaiCERT が取り扱った情報セキュリティのインシデントは全部で 276 件であり、その内 188 件（68%）がフィッシングであった（図表 3-11）[52]。20 件がポートスキャン・プローブ、43 件がマルウェア、22 件がハッキング・DDoS 攻撃などであった。これらの攻撃の内どれだけが重要インフラに対して行われた攻撃なのかは公表されていない。下に ThaiCERT[53]の公表している種類別のインシデント数の図表を示す。

[52]インシデントの発生対象システムは記載されてない
[53] ThaiCERT の URL は http://www.thaicert.org/

図表 3-11　近年 ThaiCERT の取り扱った種類別インシデント

Type of Incident / Year	Spam Mail	Port Scan and Probe	Malware	Phishing	Others (Hack, DDos etc.)
2001	66	38	34	-	12
2002	183	90	55	-	27
2003	31	170	171	-	17
2004	48	132	210	-	10
2005	24	56	307	20	46
2006	17	29	162	154	16
2007	0	7	38	262	35
2008	**3**	**20**	**43**	**188**	**22**

出典：APCERT 2008 Annual Report (http://www.apcert.org/documents/pdf/annualreport2008.pdf)

(1)脆弱性低減のためのガイドやツールなどの整備・活用に関する動向

システムメーカやベンダの国際的な基準等に依存しており、タイ独自のものは見当たらない。

(2)制御システム脆弱性の評価・検証に関する動向

制御システムの評価・検証については、国家は関与していない。

(3)制御システムのセキュリティ障害事例データベースに関する動向

制御系システムの情報セキュリティに関するインシデントなどのデータは ThaiCERT に報告されたものに含まれているが、それ専門のデータベースは公開されていない。

(4)制御システムの認証に関する動向

制御システムの認証については、国家は関与していない。

(5)ヒアリング結果

タイにおける「制御システムのセキュリティ動向」について、ヒアリングに応じたある有力な学識経験者は以下のように述べている。

①諸外国もそうであると思うが、タイにおいても重要インフラの管理者は、この問題についてオープンな議論を積極的に進めようとはしていない。政府もまた同様の態度である。

②インフラ管理者としては、制御システムをクローズドなシステムとして維持することで、そのセキュリティを維持したいと考えているからだと思われる。

③タイは技術的後進国であり、重要インフラの制御システムの多くは外国のシステムメーカやベンダからの輸入に依存している。

④従って、セキュリティに関わるガイド・ツールや標準化については、国がリードして政策を打ち出すというよりは、システムメーカやベンダが準拠している国際的な基準などに依存している。

3.3.4　アジア各国における取組みのまとめ

前節までのアジアにおける制御システムにおけるセキュリティ対応を大きな4つの視点に立って整理すると次のような特徴が挙げられる。

(1)脆弱性低減のためのガイドやツールなどの整備・活用に関する動向

アジアにおいてはガイド(基準) やツールや標準化については、国がリードして政策を打ち出すというよりは、海外の有力なシステムメーカやベンダが準拠している国際的な基準などに依存している現状にある。一部では国家的な次元で制御システムにかかわるガイドラインを配布して水準の向上を図る国(韓国)もあるが、制御システムおける情報セキュリティの役割の増大に伴い、システムメーカやベンダが準拠している国際的なセキュリティ基準などに依存しつつ、国家的なガイドやツールなどの整備を図ろうとする国(中国) などがある。脆弱性低減のためのガイドやツールに関してはIEC62443へ統合されるISA-99を参考としつつ、米国国土安全保障省のガイドライン[54]を照合する必要性の認識も高い。

制御システムおける情報セキュリティの役割の増大に伴い、システムメーカやベンダが準拠している国際的なセキュリティ基準などに依存しつつ、国家的なガイドやツールなどの整備を図ろうとしている。

(2)制御システム脆弱性の評価・検証に関する動向

脆弱性の分析評価・検証のための手法としては、不十分を認めつつも独自の情報セキュリティ安全診断制度(ISCS：Information Security Check Service)を実施している国もある(韓国)。研究開発機関を持ち、制御システム脆弱性の評価・検証のための手法開発に前向きに取り組む中国のような例のほか、小規模のテストベッドを保有し評価検証を行っている韓国の電力におけるケースも見られる。保有する情報セキュリティ安全診断制度と同時にそれぞれの国で事業展開している海外の有力なシステムメーカやベンダが準拠している国際的な脆弱性の評価・検証ツールを利用している現状が見られる。

(3)制御システムのセキュリティ障害事例データベースに関する動向

アジアにおいては各国のCERTがセキュリティ障害事例データベースの基礎として機能している。制御系システムの情報セキュリティに関連する事故や事案などに特化したデータベースは、欧州や米国の団体(例えばRISI)に存在するが、アジアの事案については殆ど含まれていない。またアジアの事案を多数含む障害事例データベースも現在見あたらない。韓国やシンガポール、タイ、台湾等々は欧州や米国の団体(例えばRISI)に障害事例を公開しデータベースに関わる動きも見られるが、一方CERT以外に公共安全や安全保障上の観点から国家脆弱性データベースを運用している中国などの例もある。

---

[54]化学工業反テロ基準(CFATS：Chemical Facility Anti-Terrorism Standards)等

(4)制御システムの認証に関する動向

アジアの主要国は制御システムの情報セキュリティ規格を策定している ISA99 委員会に参加しており、ISA-99 と統合される方向にある IEC/TC65 IEC62443 の動向にも留意している。

制御系システムの情報セキュリティについて、システムや製品に関する国としての情報セキュリティ評価認証制度は幾つかの国で実施されている。アジアにおいては統合される予定の ISA-99 と IEC62443 を適用する方向がみられ、国によってはそれぞれが国家規格として準用するケースも起こりうるものと考えられる。

3.4 日本における取組み

日本では、評価・検証のためのテストベッドや認証関係の活動では大きな変化はない。制御システムの脆弱性低減に向けた取組みとして、脆弱性低減のためのガイドやツールなどの整備・活用状況および制御システムに関するセキュリティ障害事例データベース動向について記載する。

3.4.1 脆弱性低減のためのガイドやツールなどの整備・活用状況

(1)サイバーセキュリティと経済　研究会

経済産業省では 2010 年 12 月に「サイバーセキュリティと経済　研究会」を開催した。この研究会[55]では、次の内容を目的としている。

「経済成長には IT が不可欠の基盤であり、IT の安全確保が経済成長の前提となるが、昨今のサイバー攻撃・情報漏えいでは、知的財産やライフラインを狙った事案や企業等の機密漏えいが多発している。IT の安全確保によって守るべき対象が経済活動や国民生活に直接かかわる分野へ質的に変化している。

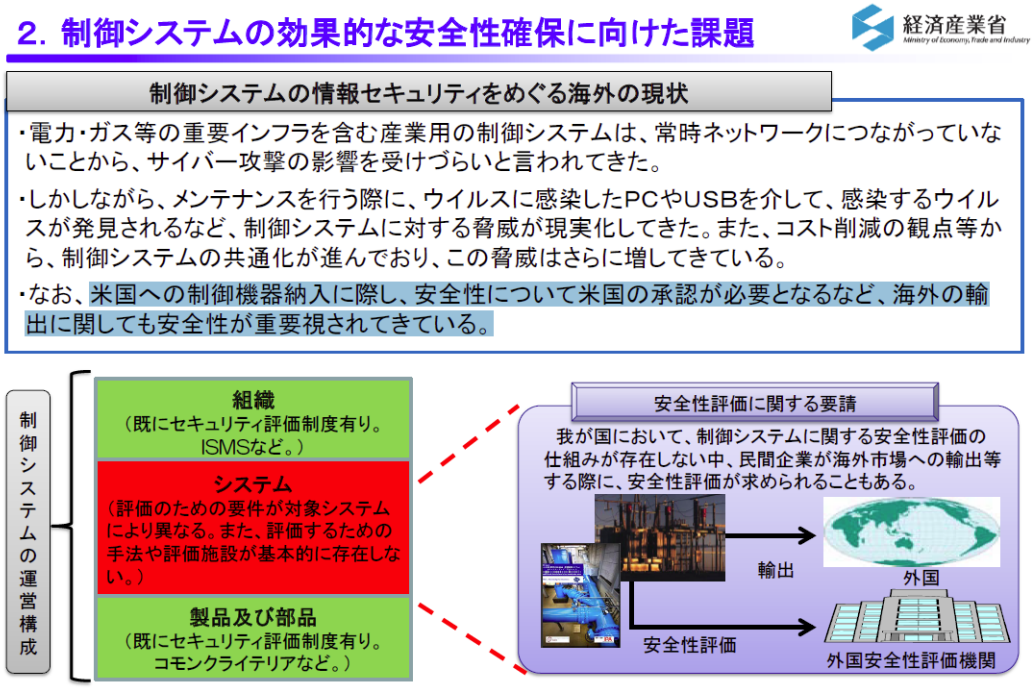
このため、経済成長・経済安全保障の観点から、必要な情報セキュリティ政策について検討し、まとめる。」

この研究会の場では、システムのメンテナンスを行う際に、ウイルスに感染した PC や USB を介して、感染するウイルスが発見されるなど、制御システムに対する脅威が現実化してきたことが議論されている。また、コスト削減の観点等から、制御システムの共通化が進んでおり、この脅威はさらに増してきている現状が紹介されている。さらに、米国への制御機器納入に際し、安全性について米国の承認が必要となるなど、海外の輸出に関しても安全性が重要視されてきているとも述べている。

検討項目の一つに「制御システムの安全性確保策について」が挙げられ、制御システムの効果的な安全性確保に向けた課題が図表 3-12 に示すように紹介されている。

[55] http://www.meti.go.jp/committee/kenkyukai/shoujo/cyber_security/001_haifu.html

図表 3-12　制御システムの効果的な安全性確保に向けた課題



課題と検討の方向性として、次の 4 点が提示されている。

①海外では、国による基準作成、検証設備運営、民間連携プロジェクト等模索中である。

②制御システムがオープンなネットワークに接続されたり、制御システムに共通の製品が使用されても安全に使えるよう、官民の役割分担を明確にした上で、システムの安全性評価の必要性を検討すべきではないか。

③制御システムに対するサイバー攻撃があった場合や新たな脆弱性が発見された場合、官民の役割分担やパートナーシップの枠組みやルール整備はどのようなものであるべきか。

④制御システムの脅威を経営者等に効果的に認識させるための方策はどのようなものであるべきか。

(2)独立行政法人情報処理推進機構(IPA)

IPA では社会インフラの安全性を確保し、国民生活、経済活動が円滑に営まれることを目標に、制御システムの脆弱性対策を促進及び普及・啓発活動を実施している。

(a) 2009 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」

制御システムのセキュリティに関する欧米等の取組みについて調査を行い、日本での推進施策についてまとめ、「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」[56]として 2010 年 5 月 31 日、IPA のウェブサイトで公開している。

調査の結果、24 時間 365 日停止しないことを最重要課題としている制御システムに対し

[56] http://www.ipa.go.jp/about/press/20100531_3.html

ても、信頼性を確保した上で、情報セキュリティを考慮する必要がでてきていることが明らかになった。この調査を基に報告書では、国内外の動向を記すとともに、我が国における制御システムの情報セキュリティ推進に向けた「制御システムセキュリティの信頼性とセキュリティへの取組み強化への提言」等の 5 つの提言をまとめている。

(b) IPA 重要インフラとスマートグリッドのセキュリティシンポジウム 2011[57]

2011 年 2 月 25 日に、制御システムに関する以下の講演会を開催した。

・重要インフラのセキュリティへの我が国の取り組み(内閣官房情報セキュリティセンター)
・セプターカウンシルの活動について(Telecom-ISAC)
・国内外のスマートグリッド実証実験について(新エネルギー・産業技術総合開発機構)
・スマートメータの動向(東芝東光メーターシステムズ株式会社)
・電気自動車の動向(日産自動車株式会社)
・スマートグリッドのセキュリティ動向調査結果の中間報告(IPA)

(c)「組込み・制御システム情報セキュリティ」セミナー[58]

制御システムに関する、情報セキュリティ上の脅威や対策を理解することを目的としているセミナーを 2010 年 6 月 30 日、7 月 22 日の両日で開催した。24 時間 365 日停止しないことを最重要課題としている制御システムにおいて、情報セキュリティを考えていくためのポイントを説明している。

(3)一般社団法人 JPCERT コーディネーションセンター (JPCERT/CC)

(a) 制御システムセキュリティカンファレンス 2011[59]

JPCERT/CC では、今後の制御システムにおける安全・安心な構築と運用に資するため、2011 年 2 月 10 日に「制御システムセキュリティカンファレンス 2011」を開催した。

(b) 日本版 SSAT (SCADA Self Assessment Tool) [60]

JPCERT/CC は、制御システム向けの簡便なセキュリティ自己評価ツール日本版 SSAT(SCADA Self Assessment Tool を 2011 年 2 月 28 日に公開した。

日本版 SSAT を利用することによって制御システムの構築と運用に関するセキュリティ上の問題項目を手軽に抽出でき、バランスの良いセキュリティ対策を行うことができる。また、邦訳版のグッド・プラクティス・ガイド「プロセス・制御と SCADA セキュリティ」と併用する事で、初心者にもより深い理解が可能である。

[57] http://www.ipa.go.jp/about/press/20110209.html
[58] http://www.ipa.go.jp/security/vuln/documents/201008_embsys_03.pdf
[59] http://www.jpcert.or.jp/ics/conference2011.html
[60] http://www.jpcert.or.jp/ics/ssat.html

3.4.2　制御システムに関するセキュリティ障害事例データベース動向

(1)脆弱性対策データベース[61]

IPA では、セキュリティのインシデント情報ではないが、米国の NVD などから制御システムのソフトウェアに対する脆弱性情報の収集を進め、対策情報を脆弱性対策情報データベース JVNiPedia に蓄積して、対策の促進を支援している。2011 年 2 月現在、JVNiPedia では 2008 年分として 8 件、2009 年分は 9 件、2010 年分は 6 件、2011 年分は 9 件、合計 32 件の制御システム用ソフトウェアに関する脆弱性対策情報を公開している。SCADA の脆弱性を含めた、JVNiPedia が蓄積している脆弱性関連情報量[62]は以下の図となる（図表 3-13）。制御系システムに関わるものは脆弱性対策情報全体に占める割合は小さいが、その社会インフラに対する影響を考えると、今後注視していく必要がある。

また、IPA と JPCERT/CC は共同で脆弱性の届出機関および脆弱性対策情報の公開に向けた作業を推進し、届け出られた脆弱性対策情報を脆弱性対策情報ポータルサイト JVN(Japan Vulnerability Notes）に蓄積し、公開している。この JVN でも制御システムのソフトウェアに対する脆弱性関連情報が公開されている。

図表 3-13　脆弱性対策データベース JVNiPedia の登録状況

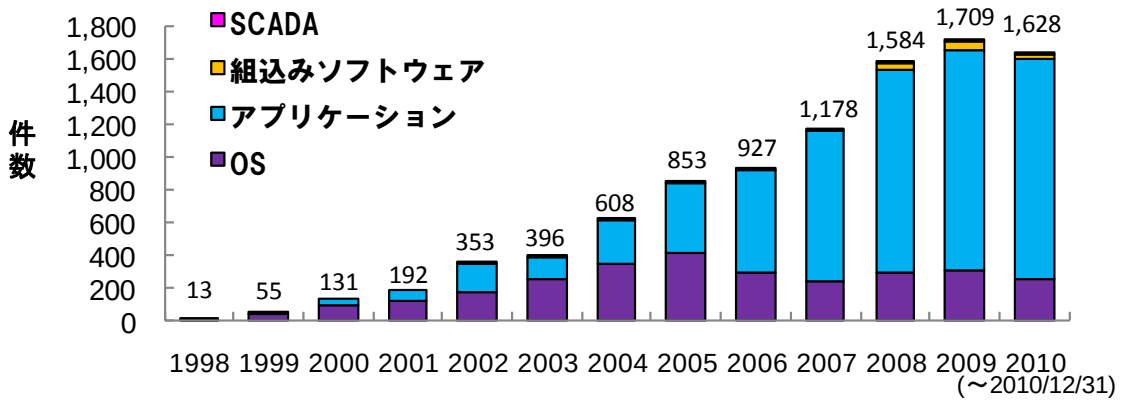


図6.脆弱性対策情報を公表した製品の種類別件数の公開年別推移

[61] http://jvn.jp/nav/jvn.html

[62] 脆弱性対策情報データベース JVN iPedia の登録状況[2010 年第 4 四半期(10 月～12 月)]
http://www.ipa.go.jp/security/vuln/report/JVNiPedia2010q4.html

第 2 編　スマートメータ周辺の制御システムについて

4.スマートメータ周辺の制御システムの動向

本章では、スマートメータおよびその周辺の制御システムの全体像、スマートメータと連携する各管理システム、およびその情報セキュリティについて説明する。本調査にあたって、特にアジア地域を中心にヒアリングで得られた情報や文献調査による詳細補足情報に関しては、付録 1 に記載しているので、参照されたい。

4.1 スマートメータ周辺の制御システム

IPA ではスマートグリッドといわれる新しい社会インフラの実現に向けて、セキュリティからの視点での今後の考慮すべき事項を明確にするための調査を実施した。

日経産業新聞 2010 年 12 月 20 日付の記事によれば、スマートグリッドを「知らない」が 6 割ということである。そこで IPA は、一般家庭や中小企業を主要対象としたスマートグリッド環境でのセキュリティの普及啓発を推進することにした。

本報告では、一般家庭や中小企業の需要家の環境をスマートハウス[63]と呼ぶことにする。スマートハウスは、情報技術を使って家庭の消費電力を制御する住宅であり、スマートグリッドを構成する最小単位ともなる。

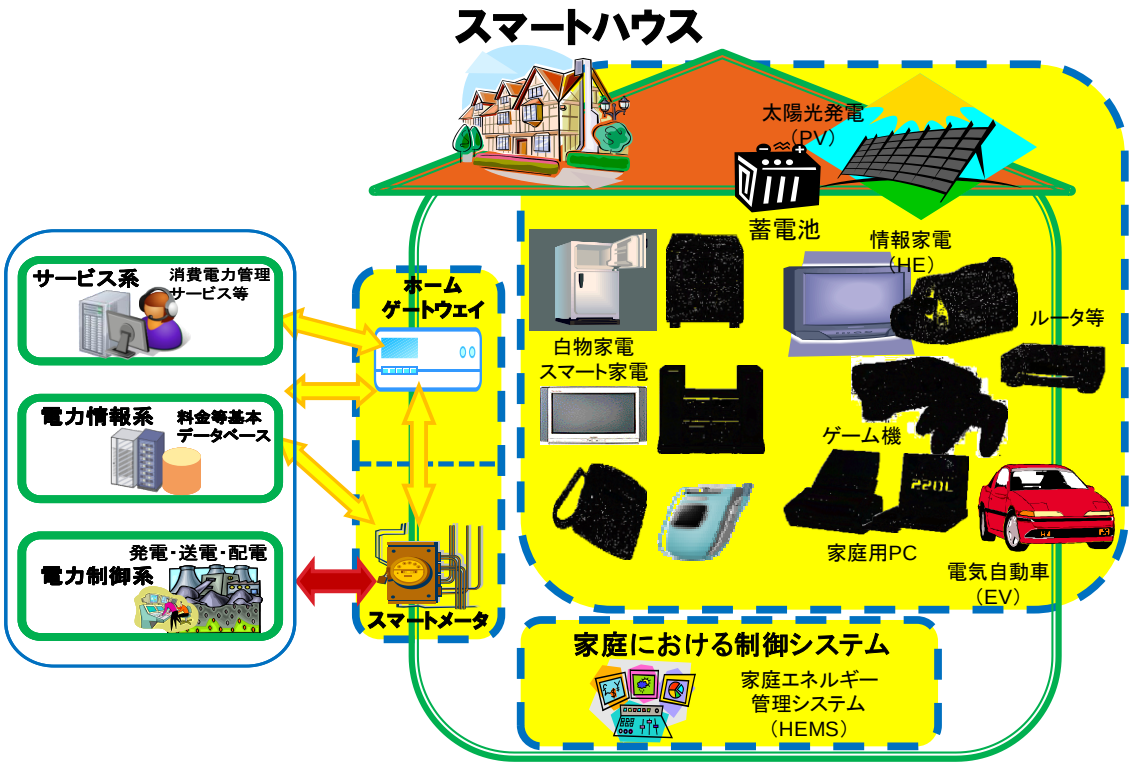
スマートグリッド環境でのスマートハウス(需要家)が外部(電力供給事業者等) との接点となる位置付けのものが、スマートメータとホームゲートウェイ(各種呼び方があり、サービスゲートウェイとも呼ばれる)である。

スマートメータやホームゲートウェイ(サービスゲートウェイ)とともにスマートハウスの中核的な構成要素に位置付けられる家庭エネルギー管理システム（Home Energy Management System：HEMS) も重要な構成要素となっている。HEMS は、CO_2 削減や省電力等家庭におけるエネルギーの利用状況の「見える化」によるエコ活動や、電力使用料金低減等の生活向上、太陽光発電等による家庭における電力の管理、電気自動車の充電情報管理などへの活用が期待される一般家庭向けの制御システムである。

上記の各構成要素は、図表 4-1 に示すような位置付けである。

[63] 賢く動く家電(ネットワーク情報家電)や蓄電を可能とする電気自動車や家庭用蓄電池など賢く需要マネジメントを実現する機器とそれをつなぐシステム(スマートハウス情報活用基盤整備フォーラム eSHIPS ホームページより: http://www.jipdec.or.jp/dupc/forum/eships/)。

図表 4-1　スマートハウスの各構成要素



IPA における検討から作成

また、一般家庭のほかにビルやオフィス、コミュニティ・地域への広がりに対する各種のエネルギー管理システム(EMS)も検討されている。HEMS(家庭エネルギー管理システム)、BEMS(ビルエネルギー管理システム)、CEMS(地域エネルギー管理システム)の概要を次に説明する。

4.1.1　エネルギー管理システムの概要

(1)HEMS(Home Energy Management System)の概要

HEMS(家庭エネルギー管理システム)は、CO_2削減や省電力等家庭におけるエネルギーの利用状況の「見える化」によるエコ活動や、電力使用料金低減等の生活向上、太陽光発電等による家庭における電力の管理、電気自動車の充電情報管理などへの活用を目的とした一般家庭向けのエネルギー管理システムである。家庭内の個々の家電機器の電力使用量やCO_2排出量の表示(見える化)、エアコン等の温度調節、照明器具の ON/OFF などの自動制御のほか、太陽光発電や今後導入が進むと考えられる電気自動車ともつながることで住宅全体のエネルギーの最適化を図るものであり、スマートグリッドの最小単位であるスマートハウスの中核的なシステムと位置付けられる。

HEMS 分野では、家電メーカなどが既に HEMS コントローラ等を商品化しており、電気使用量の見える化を核に新築住宅を中心に販売展開が行われているところである。

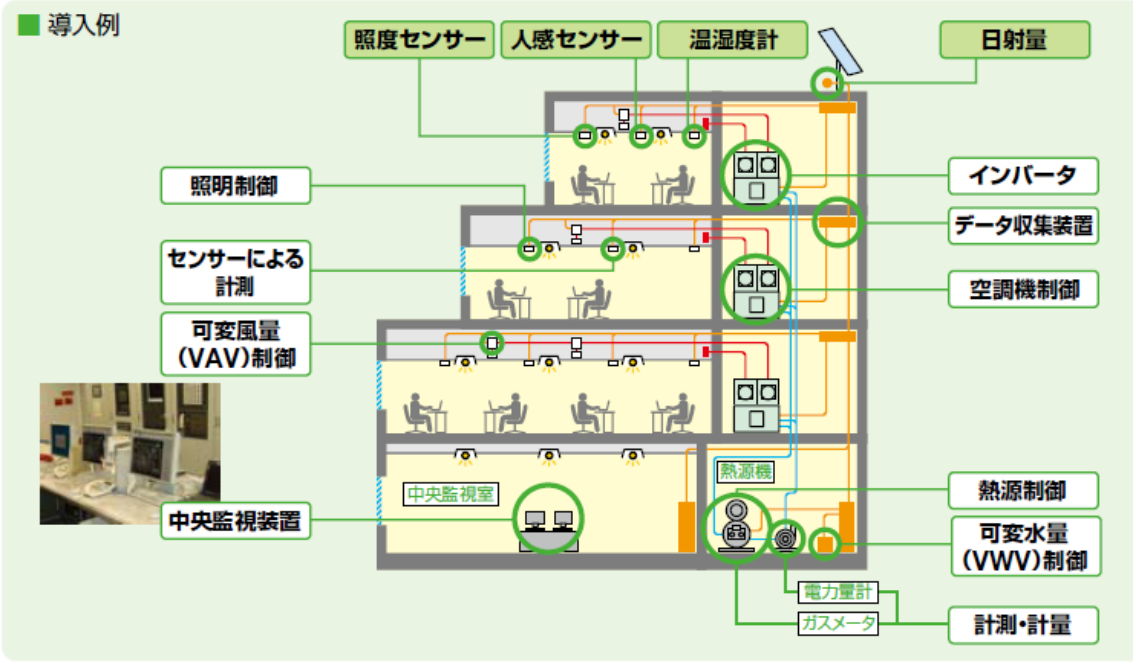
(2)BEMS(Building and Energy Management System) の概要

BEMS(ビルエネルギー管理システム) は、業務用ビル等において、室内環境・エネルギー使用状況を把握し、かつ、室内環境に応じた機器又は設備等の運転管理によってエネルギー消費量の削減を図るためのシステムをいい、計測・計量装置、制御装置、監視装置、データ保存・分析・診断装置などで構成される(NEDO BEMS 導入支援事業公募要領より) 。

ビルの電気消費量で多いのは、空調が 2 分の 1、照明その他で約 4 分の 1、コンセント周りの PC 等事務機器で 4 分の 1 とされる。ビルのマネジメントの観点からは、空調関係のデマンドコントロールが TCO (Total Cost of Ownership) 削減と CO_2 削減のバランスとしては最も効果的と考えられる。

空調のデマンドコントロールは、ビル内の人の存在、動きを人感センサなどにより感知し、温度設定やスイッチの開閉を管理するもので (図表 4-2)、いつどれくらいの温度設定にするかを設定できるアルゴリズムにより 30 分単位で従量化計算を行うプログラムなどが組み込まれる。

図表 4-2　BEMS 導入例



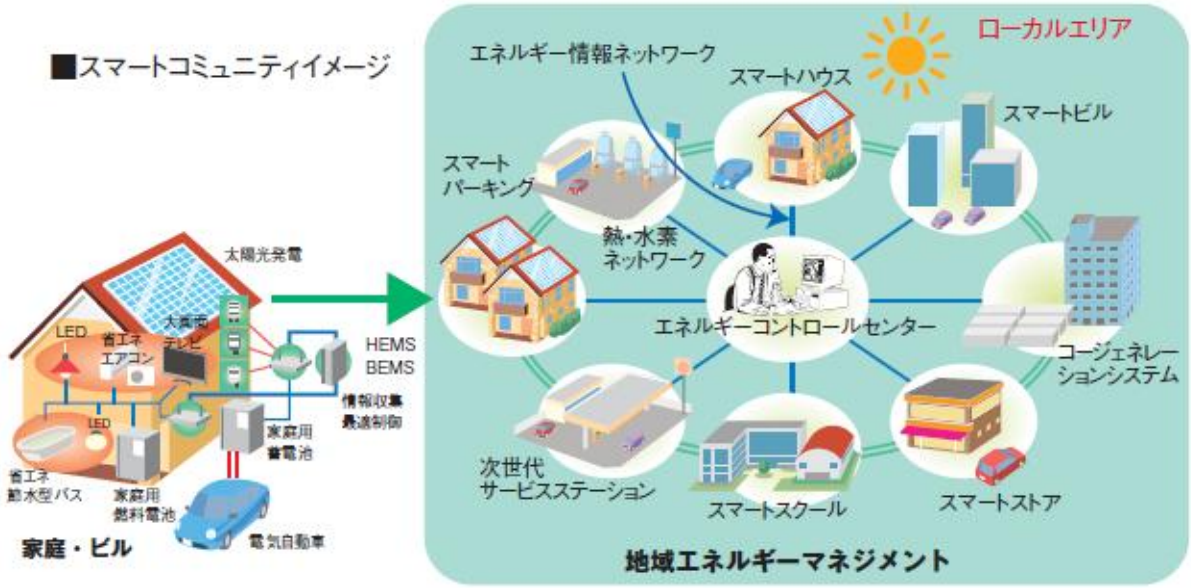
出典：NEDO BEMS 導入支援事業資料

経済産業省では、住宅・建築物高効率エネルギーシステム導入促進事業として、NEDO を通じて BEMS を導入する者に対する補助事業(BEMS 導入支援事業) を行っている。事業を開始した平成 14 年度から平成 21 年度までの合計採択件数は 490 件、補助金総額は 150 億円である。

(3)CEMS(Community Energy Management Systems) の概要

CEMS(地域エネルギー管理システム)は、HEMS、BEMS や電気自動車(EV:Electric Vehicle)及び充電インフラとの連携により、地域全体のエネルギー利用状況の集約・可視化、需要制御等を実現する地域エネルギー管理システムである(図 4-3 参照)。スマートハウスから地域全体でのエネルギーの利用効率向上を目指すスマートシティあるいはスマートコミュニティが構想されており、実証実験が進められている。スマートコミュニティは、エネルギー源に CO_2 削減を考慮した再生可能エネルギーを組合せて効率よく使うことで、環境への負荷をなくしつつ快適な生活を維持する社会インフラであり[64]、その中核を担うのが CEMS である。CEMS は、地域内に導入される HEMS、BEMS、EV および充電インフラとの連携により地域内のエネルギー利用と CO_2 排出の見える化の実現を目指している[65]。

図表 4-3　スマートコミュニティ　～　HEMS から CEMS へ



出典：NEDO 資料　“Think Green Innovation”より

4.2　スマートメータ及び連携する構成要素

4.2.1　スマートグリッドの概要とスマートメータ

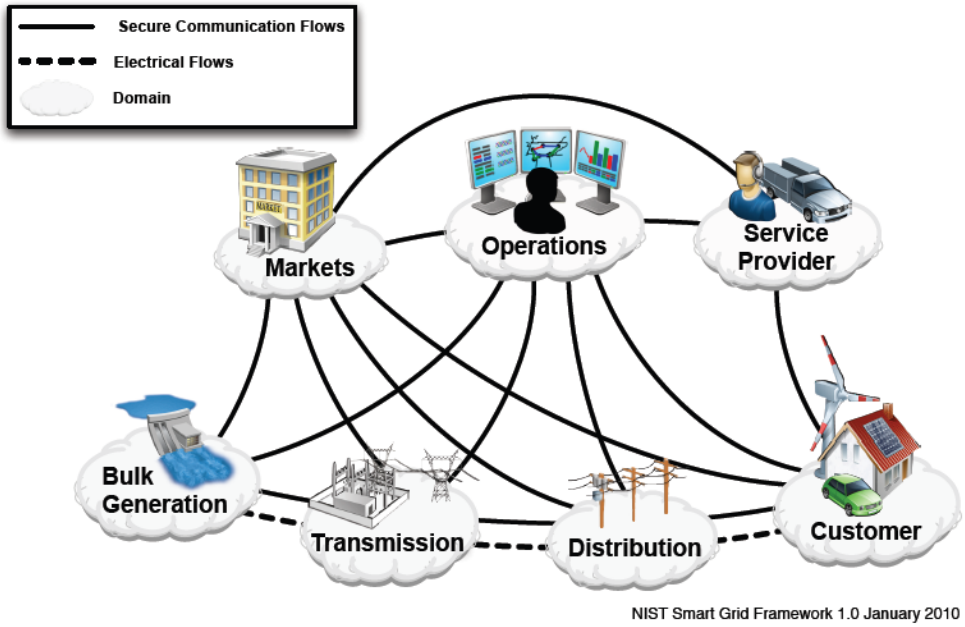
スマートグリッドとその重要コンポーネントであるスマートメータがエネルギー政策における重要課題として登場したのは、米国のブッシュ政権が 2007 年 12 月に法制化した「エネルギー自給・安全保障法(EISA:Energy Independence and Security Act of 2007) [66]がきっかけであった。エネルギー自給、温暖化対策などを打ち出した同法の第 13 章では、電力

[64] FOCUS NEDO　第 37 号世界に展開する　グリーンイノベーション，2010 年　4 月　発行より
[65] 次世代エネルギー・社会システム実証横浜スマートシティプロジェクト　マスタープラン
[66] http://en.wikipedia.org/wiki/Energy_Independence_and_Security_Act_of_2007

網システムの近代化を目指した、スマートグリッド及びスマートメータの普及が特記されている[67]。

EISA ではスマートグリッド推進政策の技術的担当部門として米国商務省標準技術研究所(NIST) が指名され、その後 NIST の主導下でスマートグリッド、スマートメータに関わる概念設計や技術標準化が進められてきた。NIST では、スマートグリッドについて 7 つのドメインを有する概念図を提起している(図表 4-4)。この図中においては、情報通信の流れが実線で、電力の流れが点線で示されている。

図表 4-4　NIST の定義するスマートグリッドの 7 つのドメイン



出典：　NIST Smart Grid Framework 1.0[68]

図表 4-4 の右下におかれているのが電力の需要家(Customer)であり、需要家と電力事業者を結ぶ窓口的機能を担うものとして図表 4-1 に示すようにスマートメータが位置づけられている。

我が国でも、平成22年5月から経済産業省が設置した「スマートメーター制度検討会」が発足し、スマートグリッドにスマートメータの制度検討が始められている[69]。同検討会では、狭義のスマートメータ概念として、「電力会社等の計量関係業務等に必要な双方向通信機能や遠隔開閉機能などを有したメータ」との定義を与え、広義には「狭義の概念に加えてエネルギー消費量などの「見える化」やホームエネルギー管理機能等も有したもの」との定

[67] http://www.ferc.gov/industries/electric/indus-act/smart-grid/eisa.pdf
[68] http://www.nist.gov/smartgrid/nistandsmartgrid.cfm
[69] 本報告書では原則「スマートメータ」と表記するが、「スマートメーター制度検討会」については検討会の名称に合わせて「スマートメーター」と表記する。

義を与えている。

以降、NISTの概念図や、我が国の「スマートメーター制度検討会」の検討内容を踏まえ、スマートメータおよび連携する構成要素とそのセキュリティに関する最新の動向を報告する。

4.2.2　スマートメータの概要

スマートグリッドにおいて電力供給事業者と需要家を結ぶ窓口に位置するものが電力計即ちスマートメータである。電力のほかにガスや水道もこれに準じた構成をなしている。スマートメータの概念、基本的な構造は以下の通りである。

スマートメータの概念

スマートメータについては遠隔自動検針・遠隔開閉・計測データ(使用電力量）の収集・発信などの機能を有する狭義の概念と、双方向の通信を有する家庭内機器通信ネットワーク・家庭内エネルギー管理用データの活用などを含む、将来のスマートメータ機能が考えられており、このような将来型スマートメータ概念を欧米では AMI(Advanced Metering Infrastructure)と呼んでいる。

スマートメータの構造

図表4-5に示すように、スマートメータは基本構成として①計量ボードを含む電力計量部、②開閉スイッチ部(図では2接点式遠隔遮断スイッチ／コントロールボード)、③通信ボードを含む通信部からなる。

図表 4-5　スマートメータの構造（例）

出典：GE エナジー「北米におけるスマートメータ導入状況のご紹介」第 3 回スマートメーター制度検討会

スマートメータが取り扱う情報としては、電力計量部で計測される電力量計量値、電圧、電流、周波数、電力、高調波(トランスデューサー機能)、異常値(停電、瞬停、フリッカ、欠相、電線接続状態監視)、計器情報(お客さま番号、契約内容(定格電流、時間帯など)、検定有効期限)、計量値バッファー、各種コントロールデータなどが挙げられる。現在日本では主として電力量計量値のみである[70]。

開閉器部は通信によって遠隔開閉が可能である。開閉器は海外では相線式が1Φ2Wのため1極切り(開閉器1個)であるが、日本は相線式が1Φ3Wのため2極切り(開閉器2個)である。接点は半導体ではなく、メカニカルなスイッチが使用されている。

通信部を構成する通信端末は有線の場合と無線の場合などがあり、使用メディアによって異なる。通信メディアはPLC(配電線搬送)と無線GPRS(一般携帯無線)に分けられ、近年はPLCが重要となってきている。PLCの規格にはPRIME(PoweRline Intelligent Metering Evolution)、G3、TWACS(Two-Way Automatic Communications System)などがあり、PRIMEはスペインの電力大手イベルドローラが、G3はフランスのEDF(Electricite de France)社が、TWACSは米国のPG&E(Pacific Gas and Electric Company)社及びSCE(Southern California Edison)社が採用している。通信に関しては、低圧から高圧まで信号を減衰させることなく電送でき、コストダウンを図る、いわゆるトランス越えが課題となっている。

一方、無線GPRS(一般携帯無線)としてはZigBee、WiMax、M-bus(ドイツ)などの規格があり、バッテリー駆動のガス、水道メータのための低消費電力化が課題となっている。

スマートメータメーカとしては先に挙げた電力量計量値、トランスデューサー機能関係、異常値検出、計器情報、計量値バッファー、各種コントロールデータなどの情報の取得を考えているが、電力会社は基本的には電力量計量値、管理のための契約内容(定格電流、時間帯など、検定有効期限など)に関する情報に関心を持っており、電力量計量値についてはリアルタイム値ではなく積算値を想定している。

欧米ではホームエネルギー機能等も含めた広義のスマートメータとしての情報の取得が方向づけられている一方、現在の日本においては、「スマートメーター検討会」において、狭義のスマートメータの範囲についての検討が進められている。

海外の動向

スマートメータ導入に至る背景やきっかけは各国それぞれの事情により異なっている。日本では、今後増大する再生可能エネルギーへの考慮や更なる高効率・高品質・高信頼度の電力供給システムの構築を目標として導入を進めている。一方、米国では、停電によって大きな社会的損失が生じているなど電力系統のリスクと不確実性の増大が背景にあり、また今後再生可能エネルギーの増大により、接続の考慮が必要になっていることがある。さらに、欧州では、再生可能エネルギーの増大に加えて、慢性的な盗電の発生、省エネルギーの推進という背景事情もあり、それらの課題への対策としてスマートメータの導入が進められている。

[70] 詳しくは「スマートメータの導入状況」(東光東芝メーターシステムズ(株)、スマートメーター制度検討会(第3回)配布資料参照)。

以下に欧米におけるスマートメータの導入状況を説明する[71]。（図表 4-6 参照）

(1)欧州

欧州各国ではスマートメータの導入が早い段階で進んでいる。現在、イタリア、スウェーデン、フィンランドの各国で 100%の普及率を誇り、他にもイギリス 40%、オランダ 30%、フランス 20%、ドイツ 10%の普及率となっている。

欧州では、「第 3 次 EU 電力自由化指令」（2009 年 7 月）でメータの経済的合理性及び費用対効果等について分析を行い、その結果が肯定的に評価される場合、2020 年までに需要家の少なくとも 80%に対してスマートメータを導入しなければならないと規定している[72]。これが後押しとなり、イギリス、フランスなどで 2020 年までに 100%の導入が見込まれている。

(2)米国

米国のスマートメータの導入は 40%と欧州の導入先行国に比べ遅くなっているが、増大する電力需要に伴う供給力不足の解消や送配電設備の投資抑制・老朽化による供給信頼度の低下を改善する観点から、デマンドレスポンスと組み合わせて導入を促進している。

ペンシルバニア州では、州法で今後 15 年以内にすべての需要家（約 600 万）に対しスマートメータの設置が義務付けられている。カリフォルニア州では複数の主要事業者が 2011～12 年までに数百万台の導入を計画している[73]。

[71] スマートメーター制度検討会配布資料をもとに整理。
[72] 「スマートメーターをめぐる現状と課題について」（電力・ガス事業部、スマートメーター制度検討会第 1 回配布資料）
[73] 出典は脚注 35 に同じ。

図表 4-6 欧米のスマートメータ導入状況

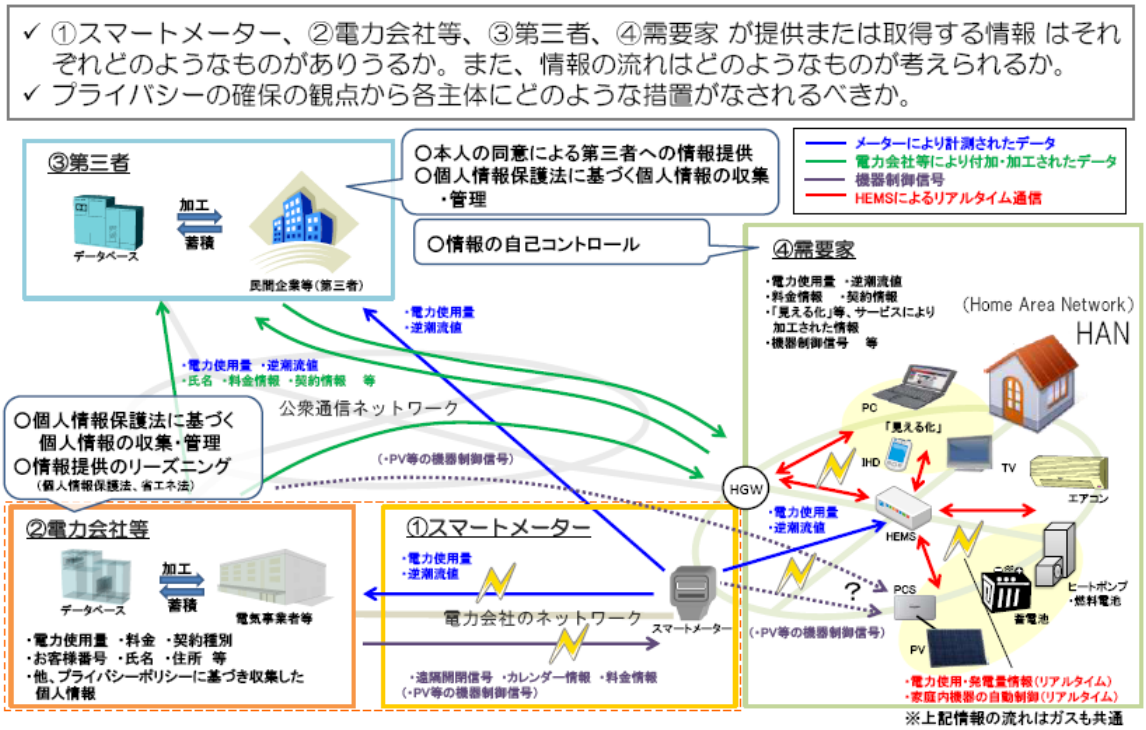
国	顧客数 （普及率）	スマートメータ導入に至る背景や検針頻度	スマートメータ導入のきっかけ等	各国のスマートメータ
イタリア （エネル社）	3300 万 （100%）	・検針頻度は年 1～2 回程度 ・盗電が社会問題 ・電力を輸入、需要抑制は重要課題	・2006 年 12 月電力ガス規制機関による「全低圧需要家にスマートメータを設置」義務化 ・ENEL は先行して導入	
スウェーデン （バッテンフォール社）	520 万 （100%）	・検針頻度は年 1 回程度 ・寒冷な気候、低廉な電気料金等により一人あたりの電力消費量が多い	・2003 年政府による「2009 年 7 月までに全ての需要家へ 1 ヶ月毎の検針を実施」義務化	
フィンランド （フォータム社）	200 万 （100%）	・検針頻度は年 1 回程度	・義務化されていないが、配電業者の運用効率向上や正確な計量などへの要請	
オランダ （ヌオン社）	754 万 （30%）	・比較的高い電気料金 ・政府は全世帯への設置に前向き（電力業界は消極的）	・規格でスマートメータとその機能を規定。 ・2008 年から全世帯へ設置を決定。	
ドイツ （Ｅ.ＯＮ社）	4400 万 （10%）	・検針頻度は年 1 回程度 ・住宅用は機械式 95%	・ドイツ系統運用者協会は国内向け AMR（Automatic Meter Reading）の導入が可能	
イギリス （セントリカ社、英ＥＤＦ社）	2600 万 （40%）	・検針頻度は 3 ヶ月に 1 回程度 ・CO2 削減目標への手段	・導入検討の主たる目的は気候変動対策（省エネ促進） ・電力消費量のディスプレイ配布を検討。	
フランス （仏 EDF 社）	3200 万 （20%）	・比較的高い電気料金	・規格でスマートメータとその機能を規定。 ・2008 年から全世帯へ設置を決定。	
アメリカ （PG&E 社, SCE 社, PPL 社）	13000 万 （40%）	・停電の削減 ・設備の最適化 ・１回／１月の検針	電力供給の広範囲化による検針の非効率	

4.2.3　スマートメータと HEMS の連携

経済産業省エネルギー庁のスマートメーター制度検討会では、スマートメータと HEMS（家庭エネルギー管理システム）との連携により、①遠隔検針（遠隔開閉）、②データを活用した需要家による省エネ・省 CO_2（見える化、経済的インセンティブ）、③系統安定化のための需要家側の機器の制御、などの機能が期待されるとしている[74]。

情報の流れから見たスマートメータと HEMS の位置関係は、図表 4-7 に示す通りである。スマートメータの導入による情報の流れと内容について整理したもので、右下図の HAN（家庭内ネットワーク：Home Area network）の中心に位置するのが HEMS である。また、スマートメータ以外の外部との通信の口として、ホームゲートウェイ（HGW）が位置づけられる。HGW は、第三者や電力会社と通信を行って高付加価値な電力管理サービスを提供するためのゲートウェイで、HEMS とも密接に連携することが考えられている。

図表 4-7　スマートメータの導入によって考え得る情報の流れと内容



出典：スマートメーター制度検討会第 7 回会合配布資料

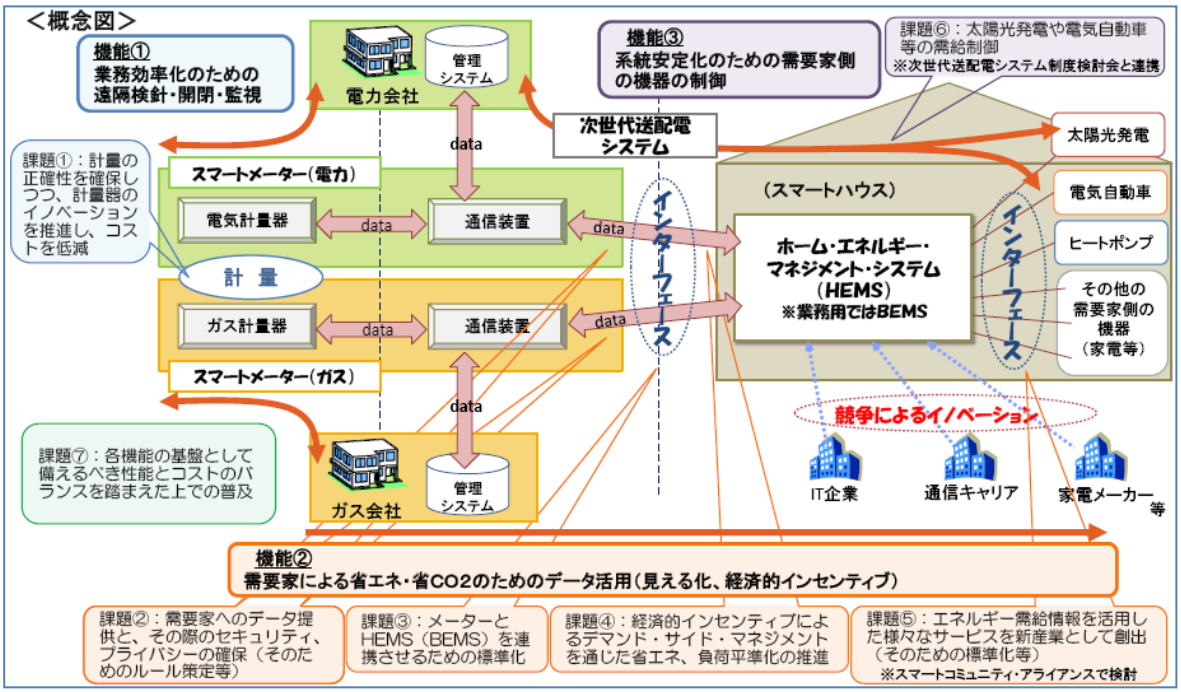
スマートメーター制度検討会では、将来のHEMS等のあり方によっては、広義のメータも考えられるとし、広義のメータのメリットとしては、HEMSを別途設置することなく、全ての需要家において、HANの構成やそれによる家庭内の機器制御等が可能となること等が期待されるとしている。しかし一方で、HEMS機能もメータに内包・一体化されるため、メータ設置後の技術進歩への対応が困難となることや、メータの装置更新のサイクルが、より速度の早い

[74] スマートメーター制度検討会第 1 回配布資料。http://www.meti.go.jp/committee/materials2/data/g100526aj.html

HEMS側の技術開発の制約になりかねないこと等、課題も存在する。また、現時点においては、機能追加にかかるコストの上昇によって、機器制御のニーズが無い需要家にまで過大な負担を求めることになることが懸念される。エネルギー基本計画においては「費用対効果等を十分考慮しつつ、2020年代の可能な限り早い時期に、原則全ての需要家にスマートメータの導入を目指す」とされており、スマートメータの導入・普及はそのスピードに合わせる必要がある。以上を踏まえると、当該期間においては、狭義のメータとし、広義のメータについては、需要家側の機器制御の必要性、HEMSのニーズ等を踏まえて将来時点において改めて検討するのが良いのではないか、との考え方を示している[75]。

スマートメーター制度検討会での議論の結論として、スマートメータとHEMS連携により期待される機能と課題を、図表4-8のように纏めている。検討会では、需要家へのデータ提供と、その際のセキュリティ、プライバシの確保（そのためのルール策定等）やメータとHEMSを連携させるための標準化、経済的インセンティブによるデマンド・サイド・マネジメントを通じた省エネ、負荷平準化の推進、太陽光発電や電気自動車等の需給制御、といった課題が挙げられている。

図表4-8　　スマートメータとHEMS連携により期待される機能と課題



出典：スマートメーターとエネルギーマネジメントシステムの連携により期待される機能と課題について（スマートメーター制度検討会第9回配布資料より）

4.2.4　スマートメータとホームゲートウェイの連携

[75] スマートメーター制度検討会第７回配布資料「スマートメーターの普及に係る論点等について」より。

ホームゲートウェイ(HGW) は、図表 4-1 および図表 4-7 に示すように、電力の管理を行うスマートメータ以外に、外部のサービス事業者や機能によっては電力会社との情報のやり取りをする接点となるゲートウェイで、スマートメータとの連携も検討されている。これによって、将来的にスマートハウスに各種のサービスを提供していくことが期待されている。

経済産業省が事務局を務める「スマートコミュニティ関連システムフォーラム」が平成 22 年 6 月にまとめた「スマートコミュニティフォーラムにおける論点と提案」において、HEMS に関連する内容としてスマートメータ/ホームサーバ及びホームネットワークに関する情報アーキテクチャの観点から見た課題が整理されている[76]。そこでは、ホームゲートウェイとして大きく分けて以下の 3 種類の可能性を挙げている。

① ホームサーバが家庭内のすべての機器をつなぐゲートウェイとなる可能性
　→ スマートメータがホームサーバにもつながる
② スマートメータが家庭内のすべての機器をつなぐゲートウェイとなる可能性
　→ スマートメータが将来高度化していく
③ スマートメータとホームサーバが共存する可能性
　→ 制御はスマートメータで、付加価値サービスはホームゲートウェイで

また、家庭内の電力情報の収集や機器管理を行うプレイヤーとして以下の複数の候補があり得るとしている。

・電力会社が行う場合
・ホームサーバ提供事業者(通信会社、家電メーカ、住宅メーカ、IT サービス事業者、他のエネルギー関連事業者) が行う場合等

4.2.5　スマートメータと家庭内ネットワーク HAN の連携

広義のスマートメータ、AMI(Advanced Metering Infrastructure)になると、ホームゲートウェイの機能を持ち、家庭内機器とリンクした HAN が構成される。情報収集及びエアコン等の簡単な機器制御も行う。機能として明確に記載されているもの以外にも、デマンドレスポンス機能・機器制御機能を含む場合がある[77]。

また、HAN(HEMS)側における通信方式については、ZigBee や Wi-Fi などの無線や PLC(Power Line Communication) などの有線が候補として検討されている。米国では、スマートメータとホームゲートウェイを ZigBee で接続する商品が市場に投入されている(EnergyHub 社 Dashboard など) 。この HAN 側通信機の設置方法や方式等については、スマートメーター制度検討会では以下のような点が指摘されているので抜粋する。(第 7 回会合における議論より)。

- HAN 側の通信機能については外付け方式で対応するとともに、HAN 側においてもメータからの通信に対応できる体制を整えてもらいたい。

[76] 「スマートコミュニティフォーラムにおける論点と提案」(スマートコミュニティ関連システムフォーラム、平成 22 年 6 月 15 日)
[77] 「スマートメーターの普及に係る論点等について」(資源エネルギー庁電力・ガス事業部、スマートメーター制度検討会(第 7 回)配付資料より)

- 現在、電力会社向けの無線を HAN 側にも振り分けることを検討中。同一の通信機を使うため、メータのコストダウンが可能となり、需要家側の追加負担も避けられる。外付け方式に絞ることでこうした可能性を狭める形にならないようにすべき。
- HAN 側の通信はユースケース・利用シーンを前提に考えるべき。例えば、引越し先でも同じ HEMS が使えるよう通信部分を標準化するなど、非効率を削除するよう検討すべき。
- HAN 側通信機の設置方法については、想定する導入数、需要家のニーズ、及び仕組み等が収斂していない段階において決めつけるべきではない。
- HAN 側の通信については、無線・有線の通信方式と、有線においてはジャックの形状を決めれば、問題ない。
- HAN 側の通信を無線・有線のどちらにするかはメータの設置場所によって大きく異なる。この点は HEMS 側と協力してできるものであり、特に無線の場合には周波数帯も含めて議論をすべき。
- 通信対象別に通信方式を選択するのではコストがかかる。同一の通信機で電力会社と HAN 側の両方へ情報を出すべき。その上で HAN 側用のチップの負担について議論をすべき。
- HAN 側通信機をどの程度普及させるのかが課題であり、相当数普及させるのであれば費用は料金回収で行うしかない。
- HAN 側通信機の費用負担を考える際に、料金で回収しないことを前提に外付けにすることが強調されているが、メータのコストという意味では通信も内蔵した方が安価になる。

そして、前述の「スマートコミュニティフォーラムにおける論点と提案」においてホームネットワークのオープン性と信頼性をどのようにして両立させるかという観点について、以下の点を指摘している。

･家電や住設機器同士のネットワークについては、ユーザの利便性を考えて特定企業の独自インタフェースとならないよう、インタフェースのオープン化が必要

･システムの信頼性を維持するためには、接続される機器によってシステムに不具合が生じないよう、機器に対する一定の規律が必要（例えば認証制度を設けるなど）

セキュリティに関連する課題については、ホームネットワークへの接続（伝送方式）について、インターネット型と特定用途優先型に分けてそれぞれの優位性と課題を示すなかで、以下のように指摘している。

① インターネット型(無差別伝送型)（一般道型）
- 既に普及したインターネットを利用して接続できることからコストパフォーマンスは高い
- ただし、セキュリティ、プライバシ面での課題あり

- エネルギーマネジメントに使う場合、通信品質（優先的な帯域の割当て、伝送遅延等）が保証されないため需給調整が出来ないリスクあり

② 特定用途優先型（伝送保証型）（優先レーン付きの高速道型）

- 通信品質、セキュリティ要件などが保証されることから信頼性・安全性は高い
- インターネットよりも高付加価値のサービスを受けることから、高コストとなる可能性あり
- エネルギーマネジメントに使う場合、通信キャリア毎に伝送保証の条件が異なったり、エネルギー会社が求める条件との食違いも想定されるため、整合を取る必要がある

4.2.6 スマートメータと外部ネットワーク WAN の連携

スマートメーター制度検討会では、需要家への情報提供を前提として、①遠隔検針・開閉等の最低限の双方向通信の機能を持った狭義のメータと②需要家機器制御機能等も有した広義のメータ（いわゆる AMI）の 2 通りが想定されている。需要家機器の制御については、電力会社が需給調整の観点から行うものと需要家が省エネ等の観点から行うものの 2 つが考えられるが、前者については、「社会的受容性を含めた実需や技術的な実現可能性、コスト等を踏まえ、将来における様々なツール（通信インフラ等）の中から最適な方法を検討していくことが必要」とし、また、後者については、通信ネットワークを含めた、「見える化」やエネルギーマネジメント機能の実現を目指す HEMS 等との連携・機能分担により実質的な対応は可能である、との認識が示されている。

資源エネルギー庁電力・ガス事業部がまとめた資料によると、当面（今後 10 年程度）双方向通信により目指す機能として以下を挙げている[78]。

○当面、遠隔検針や遠隔開閉、需要家及び電力会社等双方への電力等使用情報の提供といった機能を有するスマートメータの導入を目指すこととされたところである。

○上記を踏まえ、当面は上記の機能を有するスマートメータの導入を可能とするための双方向通信を目指すことが適当と考えられる。

○住宅用太陽光発電等の出力抑制については、上記の双方向通信が導入されていない段階では予め出力抑制日等のカレンダー情報を搭載した PCS（Power Conditioning System）による対応となる。上記の双方向通信が導入された後の段階においては、双方向通信を活用したカレンダー情報の書換えについても、機器の開発や実証試験[79]等を踏まえ検討を行っていくことが適当と考えられる。

[78]「双方向通信の導入に向けた課題について」（資源エネルギー庁電力・ガス事業部、平成 22 年 12 月 27 日）

[79] 次世代型双方向通信出力制御実証事業：通信による出力抑制や各種通信手段による検証（有線・無線）等について実証を行う。

また、双方向通信の実現に向けた課題として、以下が挙げられている。

(1)ラストワンマイル等を含めた通信インフラの整備

既存の電力系統等における通信インフラの有効活用や通信事業者の設備の活用など社会的コストの最小化を図ることが必要。また、通信方式の選択に当たっては、各一般電気事業者が通信システムの拡張性・信頼性、地域性等を考慮して最適な通信方式を選択していくことが必要。

(2)情報セキュリティの確保

電力ネットワークは電力の安定的供給を担う重要インフラであることや、個人情報の保護、情報セキュリティの確保のため、不正アクセス、情報漏えい等について、システム面、保守運用面等で十分な対策を講じていくことが必要。

(3)標準化

双方向通信による電力等使用情報の送受や、PCS のカレンダー情報の書き換えに向け通信プロトコルやデータフォーマット、通信機器のインタフェース等の標準化が必要。また、可能な限り国際標準化を目指すとともに、標準化によるセキュリティの脆弱性にも十分に考慮することが必要。

需要情報等の活用などで一般電気事業者以外にも参入の可能性のある分野（HEMS 等）の標準化を行う際には、関係者が広く参画できる体制を確保することが必要。

(4)社会的受容性の確保

HEMS 等により需要家自らが消費機器の制御をすることも可能であることから、需要家の社会的受容性の確保に向け、費用対効果も含めた周知等が必要。

双方向通信については、ZigBee など短距離無線技術によるソリューションと電力線通信(PLC) による有線ソリューションが提案されている。

ZigBee については、NIST が、2010 年 1 月 19 日に公表した「NIST スマートグリッドの相互運用性に関する規格のフレームワーク及びロードマップ(第 1 版)」において、25 の規格のひとつにホームエリアネットワーク(HAN) の機器の通信及び情報モデルとして ZigBee/HomePlug スマートエネルギー・プロファイル 2.0 が盛り込まれた。

また、HAN を、機器通信、測定及び制御を含む電力会社の先進計測システムに接続するための仕様として、OpenHAN が挙げられている[80]。

また、スマートグリッドを実現する通信企画の標準のひとつとして IEEE802.15.4g(SUN : Smart Utility Network) が取りきめられている。半径 100m～数 km の範囲において、複数の各ホームネットワークからの情報を電力会社やガス会社の情報収集局に集約し、双方向に制御できるため、スマートグリッド時代の無線ネットワークとして期待されている[81]。

[80]「次世代エネルギーシステムに係る国際標準化に向けて」(次世代エネルギーシステムに係る国際標準化に関する研究会、2010 年 1 月)

[81]「ICT から見たスマートグリッドの可能性」(科学技術政策研究所科学技術動向、2010 年 8 月号)

4.3 スマートハウスにおけるセキュリティ

4.3.1 スマートハウスに想定される脅威

需要家内部のリスクとしては、生活者の情報(ライフログ)が漏洩するリスクやHEMSで管理された家電機器がDDoS等の攻撃を直接受けて負荷に耐えられずに停止してしまうといったリスクなどが考えられる。セキュリティの観点からは、HANにおける通信路のセキュリティ、HEMSコントローラもしくはホームゲートウェイそのもののセキュリティに加え、エネルギー収支等の見える化につながる部分での情報収集のための機器間の通信データのセキュリティなどが挙げられる。

現在はネットワーク接続機能を持っていない冷蔵庫等の白物家電もがIP化され、インターネットにつながるようになり、そこに保護されていない書き込み可能メモリのような脆弱性があれば、脅威レベルが大きくなるため、より厳格なセキュリティ対応が必要となろう。

脅威の侵入口は複数考えられるが、HEMSコントローラなどにおいてファイアウォール機能を持つことにより主要な脅威を自動的に遮断し、家庭内の他の機器に影響が及ばないようにすることが重要である。

また、オフィスビルでは、BEMSにおけるクラウド活用の試みも見られ、クラウドの活用形態にも依存することになるが、エネルギー管理とクラウド化の観点からみたリスク対応も課題として挙げられる。

一方、セキュリティへの対応に関しては、ユーザが購入してネットワークにつないだ家電製品でリスクが顕在化した場合、脆弱性情報が既知か未知かを含めて、誰がどこまで責任を持つのかといった議論もある。

4.3.2 スマートメータ周辺のインタフェース上のリスク

スマートメータは計測器であると同時に通信機器であり、通信機器固有の脆弱性を有している。スマートメータを取り巻くシステム環境を考慮した場合、幾つかのインタフェースリスクが存在すると考えられる。

欧州のエネルギー供給サイドでは、欧州委員会のガス＆エネルギー局内にアドホック組織として「スマートグリッド・タスクフォース」(SGTF) が設立され、現在活動中である[82]。設立は2009年11月、存続予定機関は約20カ月であり、2011年夏頃まで活動が継続される予定である。SGTFはステアリングコミティの下に、三つのエキスパートグループ(EG) が置かれており、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」の報告書(全41ページ、2011 年2月16日公表) を纏めている[83]。そこでは、13 個のインタフェースリスクを抽出しており、今後の検討に有効と考えられる。以下

[82] http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm

[83] http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf

では、それを説明する。なお、付録 1.2 にも、本活動を記載しているので、参照の事。

① スマートメータから IHD(インハウスディスプレイ）へ

二つのデバイス間の物理的インタフェースのリスク。個人データ漏えい、プリペイメント情報、メータ計量情報、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 から LAN へ

需要家ネットワークから外部への物理的インタフェースのリスク。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 から WAN へ

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 からヘッドエンド/データコレクタへ

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 から中央データコレクタへ

メータ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フェースに存在するリスク。メータ計量情報、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）からネットワーク管理者へ

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えいし、メータ計量情報、アラーム情報などに偽装のリスクが存在する。

⑦ LAN/WAN/ DC から DSO(電力小売業者)へ

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 消費者による発電から配電ネットワークオペレータへ

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

タフェースに存在するリスク。メータ計量情報、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 消費者発電から電力小売り業者へ

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 電力小売り業者からサードパーティへ

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からサードパーティへ

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 消費者発電からサードパーティへ

分散型消費者発電のアグリゲーション(集成)・サービスに伴うリスク。メータ読出し情報、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 メータから無線メッシュへ

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。

4.3.3 各国におけるセキュリティへの取組み

スマートハウスに関連したセキュリティへの取組みは、想定している事業形態やサービス形態によって、米国、欧州、日本でそれぞれ異なる面を有している。

(1)米国

2010年9月、NISTが初めて発表したスマートグリッド・サイバーセキュリティに関するガイドライン(Guidelines for Smart Grid Cyber Security）では、ハイレベルな安全性要件、リスク評価の枠組み、個人住宅におけるプライバシ問題の評価、付加情報が示されている。同ガイドラインは137のインタフェースを特定し、共通あるいは類似する機能的特性および安全上の特性に基づき22のカテゴリに分類している。また、スマートグリッド全体または特定部分やそれに付随するインタフェースカテゴリに適用できる189のハイレベルの安全性要件を詳述している[84]。例えば、トランスミッションSCADAと変電設備の間、発電所(パワープラント）内のSCADAとDCS(Distributed Control System）の間、顧客情報システムと計

[84] NEDO 海外レポート No.1067, 2010.10.20

器情報管理システム間などのインタフェースが挙げられている[85]。

(2)欧州

欧州委員会のガス＆エネルギー局内にアドホック組織である「スマートグリッド・タスクフォース」(SGTF) のエキスパートグループが、データセキュリティを含む検討結果を報告書としてまとめ、2011 年2月に公表している[86]。同報告書では、4.3.2に示すように13個のインタフェース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が示したインタフェースは、メータからIHD(In-Home Display)、HANからLAN、LANからWANなどのインタフェースを挙げ、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。

(3)日本

スマートメーター制度検討会などでセキュリティを含めた議論が行われているが、欧米のようなガイドラインや勧告としてまとまったものはまだ出ておらず、欧米の動向を見据えつつ日本の事情に対応したセキュリティガイドラインの検討が行われているところである。例えば、スマートメーター制度検討会では、スマートメータ用情報ネットワークにおける主なセキュリティ要件として、ライフライン設備保護、個人・企業情報保護等の観点から、不正アクセス対策、なりすまし対策、盗聴・情報漏洩対策、改ざん対策、サービス停止対策が重要であるといった指摘がなされている。セキュリティ対策として暗号化や、端末認証・回線認証、閉域網(ユーザ毎に閉域性を確保した通信網) 構築等の複合的な対策が有効であり、日々変化するセキュリティ脅威に迅速に対応する為に、ネットワークセキュリティオペレーション体制の整備が重要とする意見も聞かれる[87]。

また、スマートハウスに係るマルチベンダ設備間インタフェース、スマートハウスに係るセキュリティガイドライン、スマートハウスに係る運用ガイドラインの策定などを進めているスマートハウス情報活用基盤整備フォーラム(eSHIPS) [88]では、データを保護するためのネットワークセキュリティや、個人情報の安全な管理手法の検討を行い、運用に関しては、個人情報を取り扱う事業者側の運用ルールや、サービスの精度を向上させて維持するための機器やサーバのシステム的な認証、および認証の制度などについて検討を行っている。

---

[85] 但し、この NIST のガイドラインに対して GAO は、連邦政府と州政府の不透明な所管の問題、消費者に対する説明、電力会社のセキュリティに対する取組、デバイスのセキュリティ対策、電力業界の情報交換メカニズム、サイバーセキュリティの評価方法など6つの課題を指摘している。(詳細は 4.4.1 項参照)

[86] http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf

[87] 「スマートメーターを繋ぐ情報ネットワークについて」(NTT 資料) スマートメーター制度検討会第 6 回会合

[88] http://www.jipdec.or.jp/dupc/forum/eships/

5. まとめ

5.1 調査分析結果を踏まえたまとめ

5.1.1 制御システムに対する脅威・対応等の現状

以下では、今年度、重点的に調査したアジアの制御システムについてのまとめと、2010年に顕在化した制御システムに対する脅威と脆弱性について述べる。なお、これまで調査してきた欧米と日本の追加情報に、アジアを加えたグローバルな制御システムに対する取組みを整理した図表を、付録2に示す。

(1)アジアの制御システムについて

アジアにおいては欧米に比べて社会経済文化等の現状の多様性が大きく、制御システムのセキュリティへの認識や対策について各国でバラつきがある。

① 脆弱性低減のためのガイドやツールなどの整備・活用状況

ガイドやツールについては、事業展開している海外の有力なシステムメーカやベンダが準拠している国際的な基準などに依存し、国がイニシアティブをとっているケースは少ない。国家的な次元でガイドラインを配布し水準の向上を志向する国もあるが、システムメーカやベンダが準拠している国際的な基準などに依存しつつ、国家的なガイドやツールなどの整備を図ろうとする方向が顕著である。特に米国政府の施策動向を参考とする動きが強い。

② 制御システム脆弱性の評価・検証のための手法

独自の情報セキュリティ安全診断制度の実施や、国の研究開発機関で脆弱性の評価・検証のための手法開発に取り組む国もあるが、アジアでは一般的に評価・検証のための手法は海外の有力なシステムメーカやベンダが準拠する国際的な脆弱性評価・検証ツールを利用している現状が見られる。

③ 制御システムに関するセキュリティ障害事例データベース動向

各国のCERTをセキュリティ障害事例データベースの基礎として利用している。また制御系システムの情報セキュリティに特化した欧米のデータベースを利用する方向も見られるが、アジアの事案を多数含む障害事例データベースも現在見あたらず、公共安全や安全保障上の観点から国家脆弱性データベースを運用している国もあり、独自に用意する国もある。

④ 制御システムの認証を取り巻く環境

制御系システムの情報セキュリティについてシステムや製品に関する国の情報セキュリティ評価認証制度を持つ国もある。アジアの主要国は制御システムの情報セキュリティ規格ISA99の委員会に参加しており、ISA-99とIEC/TC65のIEC62443とが統合される方向にある

動向に留意し、これを国家規格へ準用する方向も見られる。

(2)制御システムを狙った攻撃や制御ソフトの脆弱性の顕在化

これまでの制御システムでは、独自の作りこみやネットワーク的な遮断によって、サイバー攻撃による脅威が顕在化することは少なかった。しかし、2010 年 7 月に発見されたマルウェア（Stuxnet）は Windows のゼロデイの脆弱性や、シーメンス社の制御システムの特性等の詳細を熟知すると考えられる攻撃者による、極めて高度な作りこみがなされており、それによって制御システムが攻撃の対象となっている事が明らかとなった。特にこの攻撃では、オープンな情報系技術を利用したシステムをまず攻撃し、そこからシーメンス社のクローズドな制御機器に攻撃を行う事が特徴的である。

一方で 2010 年に中国で広く使われている SCADA ソフトに脆弱性が発見されたように、今後もセキュリティ研究者等によって新しい脆弱性が発見されていく事も考えられる。この事例では脆弱性の通報から対応までに遅れが出るなど、脆弱性関連情報の適切な流通に関しても、未だ問題が残る事が明らかとなった。

5.1.2　スマートメータ周辺の制御システムのセキュリティ動向

我が国においては資源エネルギー庁が 2010 年にスマートメータ制度検討会を開催するなど今後の利用を目指した様々な動きが見られる。スマートメータ周辺の制御システムのセキュリティに関しては次のような動向がある。

(1)スマートメータに関する日本と海外(特に欧米）の相違

スマートメータの導入について、現状では各国においてその目的に差異がみられる。例えば、米国では増大する電力需要に伴う供給力不足の解消や送配電設備の投資抑制・老朽化による供給信頼度の低下を改善する観点から、デマンドレスポンスと組み合わせて導入を促進しているとされる。一方、欧州では、盗電防止や実消費量に基づいた料金請求の実施に加えて、再生可能エネルギー推進の観点から導入が促進されている。日本は、今後増大する再生可能エネルギーへの考慮や更なる高効率・高品質・高信頼度の電力供給システムの構築を目標としている。

セキュリティ機能を持つスマートメータも開発が計画されており、新エネルギー・産業技術開発機構(NEDO）が米国で実施しているスマートグリッドの実証実験に導入・評価される予定である。電気利用率の見える化等を目的としたスマートメータの普及が進むと、これまでの情報ネットワーク等に電気使用量や金額、生活パターン等の新しい情報が現れる可能性がある。スマートメータを含めたこれらの情報を扱う機器やネットワークにおいては、適切なセキュリティ対策を施す必要がある。今後、これらの実験結果を見ながら、スマートメータに求められる要求仕様やセキュリティ機能を含めた標準化が検討されると考えられ、スマートメータを利用したサービスを含めて、セキュリティ課題と対策を検討する段階にあると言える。スマートメータのセキュリティを考える上では、それがスマート

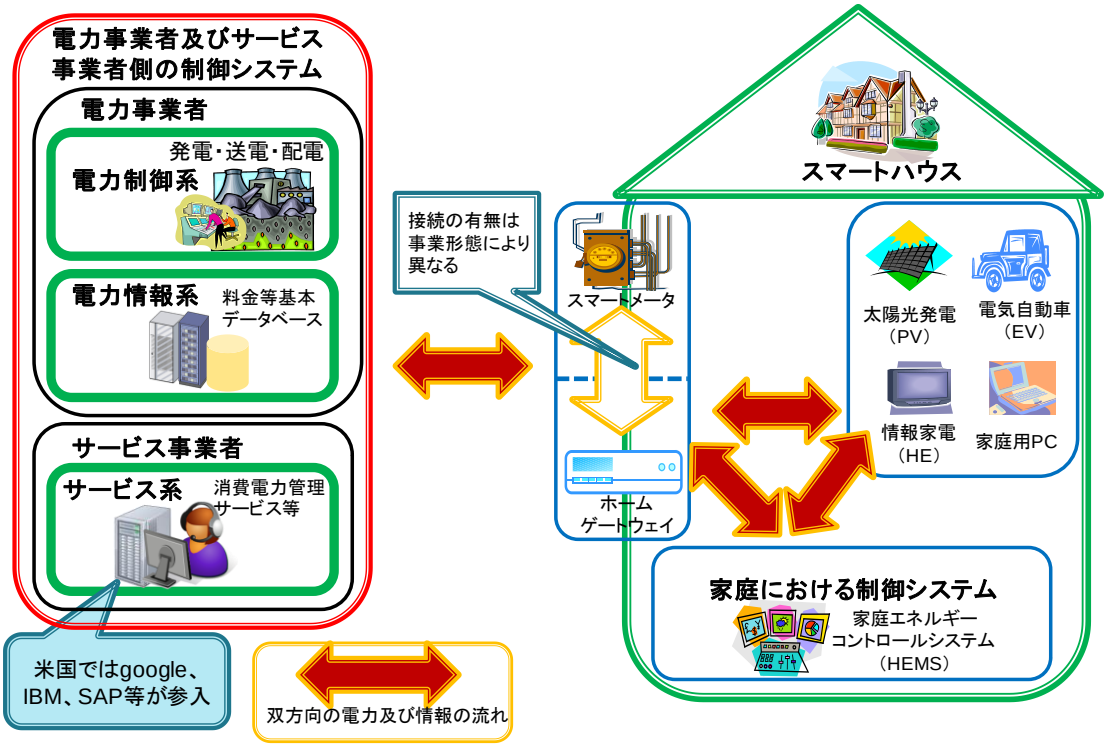
ハウス等のトータルシステムの中で、どのような位置付けとなるかを明確にする必要がある。そのため、スマートメータの位置付けとそのサービス形態について、様々なアプリケーションを明確化したアプローチが重要となるため、実証実験の成果を注視・分析していく事が必要である。

(2)家庭エネルギー制御システム(HEMS)の現状について

今回の調査では、スマートハウス側から見たスマートグリッドとの関係の概要を図表 5-1 にまとめた。スマートメータとサービスゲートウェイの関係は、電気関連事業者の構成やサービスの概要によって変化すると考えられるため、区分けしている。

この図におけるスマートグリッドが係わる制御システムは、「電力供給者及びサービス事業者側の制御システム」と「家庭における制御システム」の二つがあると考えられるが、今回は後者の「家庭における制御システム」(HEMS)にスポットを当てた。

図表 5-1 スマートグリッドにおけるスマートハウスの位置付け



IPA の検討により作成

電力供給の安定化および、CO_2 の削減や一般家庭の電気代削減に向けて、スマートメータや多種の家電と連携した HEMS を中心として、電力管理が行われると考えられる。今後、太陽光発電の普及や電気自動車のような大規模バッテリーを持つ機器が家庭に繋がる事で、家庭の余剰電力売却等による電力事業者への影響や、電力管理を実施する際の各家庭の課題が発生するであろう事が明らかとなった。

5.2 今後に向けて（提言）

5.2.1 制御システムに対するセキュリティ

(1)制御系システムのセキュリティ基準及び認証の検討

海外においては、米国では ISCI(ISA Security Compliance Institute)、欧州では WIB(International Instrument Userstute)、家庭の余剰電力売によって、セキュリティ基準の策定とそれを利用したテスト仕様や認証手法が具体化されつつある。欧米のインフラ事業者は、既にそれらの動向に注目しており、今後海外で制御システム製品を展開するためには、これらの基準や認証等への対応が必要になると考えられる。

これまでの調査から、制御システムの構成及びそこで発生する問題等に関して、地域特性が存在すると考えられるため、上記の組織で検討されているセキュリティ基準等を参考に、日本における制御システムのセキュリティ基準の検討が必要であると考えられる。また、日本国内の制御システムにセキュリティを組み込むだけでなく、海外に打って出るためのセキュリティについても、調査・検討を進める必要がある。日本において検討されたセキュリティ基準や認証等をベースに、海外の適切なカウンターパート等との連携のもとで、制御システム事業において、日本がリーダシップを取る事が求められる。

(2)制御システムにおける汎用製品や標準プロトコルの利用に伴う脅威の拡大

Stuxnet の発生は、制御システムのセキュリティ課題について注目を集める結果となった。事実、SCADA 系に対する投資も増えているとの報道もある。今後、制御システム全体として汎用製品や標準プロトコルの利用といったオープン化が浸透していくと、情報システムと同様の脅威も顕在化してくると考えられる。そのため、インフラ事業者と制御システム製品開発者にもセキュリティ関連情報を周知徹底していくことが必要である。IPA ではテクニカルウォッチ[89]等において、セキュリティインシデントに係る技術的な課題と対策について公開しているが、この中でもふれているように、システム設計の段階からシステム全体としてのセキュリティを検討する必要がある。また、制御システムの運用中だけではなく、システムの構築から保守までを含めたライフサイクル全体に対して、セキュリティ対策を検討していく必要がある。また、2010 年の四日市火力発電所による 0.07 秒の瞬時電圧低下による影響で明らかになったように、インタフェースやプロトコルだけでは無く、内部プロセスに関する脅威も併せて考慮する必要がある。

5.2.2 スマートメータ周辺の制御システムのセキュリティ

(1)HEMS のセキュリティ対策普及に向けた検討

今後、CO_2削減や省電力等のエコ活動や、電力使用料金低減等の生活向上、太陽光発電等による家庭における電力の管理、電気自動車の充電情報管理のような目的で、各家庭に家

[89] IPA テクニカルウォッチ『新しいタイプの攻撃』に関するレポート：http://www.ipa.go.jp/about/technicalwatch/20101217.html

庭エネルギー制御システム（HEMS）の導入が進むと考えられる。今後の課題として、HEMSと各機器における通信手段や取り扱う情報のデータフォーマット等に関して、標準化を進める必要がある。

HEMS は、電力使用量や接続機器情報のようにプライバシに係る情報や家庭内機器の制御機能を持つと考えられる。この際、在宅者の有無の確認に繋がるようなプライバシ情報の漏えいや、外部から家庭内機器を不正に制御される事を防ぐため、セキュリティ上の課題や対策を明確にした上で、HEMS と各機器の標準化に併せてセキュリティ要件を明確化する必要がある。

また、HEMS が普及する上では家庭内だけでコントロールを行うのでは無く、HEMS と外部サービスが連携して、利用者に有益な情報やサービスの提供が行われると考えられる。そのため、HEMS と外部が情報通信を行う際のセキュリティに関しては、サービス事業者においても共通の課題となると考えられるため、いくつかのサービスを想定したセキュリティ要件についても検討を進める必要がある。このような検討においては、様々な機器メーカやサービス事業者など、多種多様なプレイヤーの連携が不可欠であり、各種業界を横断的につなぐ必要がある。IPA では既に自動車や情報家電のセキュリティを検討する上で、今後ネットワーク化が進むと考えらえる電気自動車やデジタルテレビに関する有識者とのネットワークを有している。今後はこのような HEMS と係わる機器との連携も含めた検討をより一層進めていくことが求められる。

5.3 委員からのコメント等

本調査を進める上で、ご参画頂いた各委員から次のような意見が寄せられた。

(1)制御システムを含めた全体のセキュリティ

・制御システム・スマートグリッド両面において、改めて具体的な課題や関係性を網羅的に洗い出す必要がある。その中で、未対応な部分を明確にし、産官学のどこが対応をするのか、優先度の設定と共に検討する必要がある。

・制御システムやスマートグリッドの可用性についても意識する必要がある。運用上でのミスや、想定しない操作についても検討を進める必要がある。

・2010 年度にあった配電事故にあったように、高品質な環境下で動く事を前提に簡略化が進んだ事によって、過去には問題の無かった「品質のブレ」にシステムが対応できない事があるのではないか。システム構成等の全体的なセキュリティ課題だけでは無く、関連機器の内部プロセスについてのセキュリティ課題も併せて検討する必要がある。

・同じ制御システムとしても、プラント系の制御システムと HEMS のような制御システムには要件の違いがあると考えられる。その要件の整理・分析も必要がある。

(2)スマートメータ周辺のセキュリティに関して

・スマートハウスにおける構造やサービスによって、それに係るプレイヤーや利用される

プロトコルが変化する。セキュリティの詳細を明確にするには、具体的な場合分けを行い、誰がどこに気をつける必要があるかを検討する必要がある。
・今回の調査ではスマートメータ周辺機器に閉じているが、スマートハウスを利用する上では、電気自動車や情報家電等をつなぐ、複数のネットワークが組み合わされる。その中で、NEDO や IPA といった組織等のそれぞれの役割を整理する必要がある

6. 調査資料一覧

6.1 スマートメータ周辺の制御システム動向に関する主な文献

(1) WEIS2010

URL: http://weis2010.econinfosec.org/program.html

- “On the security economics of electricity metering,” Ross Anderson and Shailendra Fuloria Cambridge University Computer Laboratory
  http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.165.3425&rep=rep1&type=pdf

(2) Red Tiger Security

URL: http://www.redtigersecurity.com/

- NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses
  http://www.controlsystemsroadmap.net/pdfs/INL_Common_Vulnerabilties.pdf

(3) IOActive

URL: http://www.ioactive.com/

(4) Information Trust Institute-University of Illinois

URL: http://illinois.edu/

- “Exploring Convergence for SCADA Networks,” E. Heine, H. Khurana, and T. Yardley, Proceedings of the 2nd IEEE PES Innovative Smart Grid Technologies (ISGT 2011) Conference, Anaheim, California, Jan. 17-19, 2011
  http://www.iti.illinois.edu/sites/www.iti.illinois.edu/files/docs/tcip/2011_Heine_Khurana_Yardley_ISGT.pdf

(5) Department of Energy and Climate Change

URL: http://www.decc.gov.uk/

- Smart Metering Implementation Programme: Rollout Strategy, 27 July 2010
  http://www.decc.gov.uk/assets/decc/consultations/smart-meter-imp-prospectus/228-smart-metering-imp-rollout-strat.pdf
- Consumers’ views of Smart Metering Report by FDS International, 27 July 2010
  http://www.decc.gov.uk/assets/decc/consultations/smart-meter-imp-prospectus/227-consumer-views-smart-metering.pdf

(6) ELECTRIC LIGHT AND POWER

URL: http://www.elp.com/index.html

- In Smart Grid Security, the Details Matter, 2010-04-01
  http://www.elp.com/index/display/article-display/2632770661/articles/utility-automation-engineering-td/volume-15/Issue-4/Features/In-Smart-Grid-Security-the-Details-Matter.html
- Smart Grid Implementation Strategies for Success, 2010-11-01
  http://www.elp.com/index/display/article-display/9177842560/articles/electric-light-power/volume-88/issue-6/sections/smart-grid-implementation-strategies-for-success.html
- Interoperability-Bring Measurable Change to Utilities
  http://www.elp.com/index/display/article-display/0951968874/articles/electric-light-power/volume-88/issue-6/sections/interoperability-bring-measurable-change-to-utilities.html

(7) Insurance TECHNOLOGY

URL: http://www.insurancetech.com/

(8) Internet Engineering Task Force (IETF) Network Working Group

- Internet Protocols for the Smart Grid draft-baker-ietf-core-11, 2010-11-11
  http://datatracker.ietf.org/doc/draft-baker-ietf-core/?include_text=1

6.2 その他の参考文献

(1) 制御システムセキュリティ／Stuxnet 関係

- Quarterly Report on Cyber Security Incidents and Trends Affecting Industrial Control Systems. 3rd Quarter 2009, Repository of Industrial Security Incidents (RISI)
- Cybersecurity of Control System Networks, Robin Gandhi, William Mahoney, Ken Dick, University of Nebraska at Omah, at 2010 INDUSTRY DAY http://www.sameomaha.org/2010_Industry_Day/presentations/Training_Session_III_Gandhi_Mahoney_Dick.pdf
- Department of Homeland Security. Control Systems Security Program. Seán Paul McGurk. Director, Control Systems Security. National Cyber Security Division. U.S. Department of Homeland Security, www.thinktec.org/UserFiles/File/S.%20McGurk.pdf
- Control System Security Assessments, Marty Edwards Idaho National Laboratoryin 2008 Automation Summit A Users Conference, http://graphics8.nytimes.com/packages/pdf/science/NSTB.pdf
- "How Stuxnet Changed the World," Walt Sikora -VP, Security Solutions, ICSJWG 2010 Fall Conference, 26 October, 2010 http://www.us-cert.gov/control_systems/icsjwg/presentations/fall2010/Walter%20Sikora%20icsjwg-fall-2010.pdf
- "A Review of Selected Actual Control System Cyber Incidents" Joe Weiss, PE, CISM Applied Control Solutions, LLC, ICSJWG 2009 Fall Conference, November 4, 2009 https://secure.inl.gov/icsjwg-conference/Presentations/Weiss_ICSJWG_Fall_2009.pdf
- CS-CERT - 2010 YEAR IN REVIEW, ICS-CERT, January 2011 http://www.us-cert.gov/control_systems/pdf/ICS-CERT_2010_yir.pdf
- Control Systems Cyber Security Standards Support Activities, DHS National Cyber Security Division Control Systems Security Program, January 2009 http://www.inl.gov/technicalpublications/Documents/4192219.pdf
- Literature Review on Smart Grid Cyber Security, Collaborative Software Development Laboratory Department of Information and Computer Sciences University of Hawai, December 2010 http://csdl.ics.hawaii.edu/techreports/10-11/10-11.pdf
- NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses, Idaho National Laboratory, May 2010 http://www.controlsystemsroadmap.net/pdfs/INL_Common_Vulnerabilties.pdf

(2) スマートメータ／AMI 関連

- Intrusion Detection for Advanced Metering Infrastructures: Requirements and Architectural Directions," W. H. Sanders, and H. Khurana, in 2010 First IEEE International Conference on Smart Grid Communications, R. Berthier, 2010
  https://www.perform.csl.illinois.edu/Papers/USAN_papers/10BER01.pdf
- 2008 Assessment of Demand Response and Advanced Metering Staff Report, Federal Energy Regulatory Commission December 2008
  http://www.ferc.gov/legal/staff-reports/12-08-demand-response.pdf
- Electricity Grid Modernization, GAO, January 12, 2011
  http://www.gao.gov/products/GAO-11-117
- European Smart Metering Alliance Final Report, European Smart Metering Alliance (ESMA), January 2010
  http://ieea.erba.hu/ieea/page/Page.jsp?op=project_detail&prid=1564&side=downloadablefiles
- Smart Metering Financial Toolkit, Version 3.0, January 2010
  http://ieea.erba.hu/ieea/page/Page.jsp?op=project_detail&prid=1564&side=downloadablefiles
- Smart Metering Guide Energy Saving and the Customer Edition 2010, 16 November 2009
  http://ieea.erba.hu/ieea/page/Page.jsp?op=project_detail&prid=1564&side=downloadablefiles

(3) 標準関係

- NIST IR 7628, Guidelines for Smart Grid Cyber Security
  http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628
- Industrial Control System Security NIST SP 800-82, NIST Industrial Control System Cyber Security Workshop, 24 September 2010
  http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Sept2010-Workshop/NIST_ICS_workshop_Sep2010_SP800-82_briefing_Abrams.pdf
- NERC CIP-002 through CIP-009
- NIST SP800-53 Rev.0
- NIST SP800-53 Rev.1
- NIST SP800-53 Rev.2
- ISO/IEC 15408 (Common Criteria) ほか

(4) アジア関係（SCADA ASIA 2010 文献含む）

①韓国

- “Smart Grid Solution using Multiagent System,” Kang Dong Joo, Korea Electro-Technology Research Institute, 3 February, 2010
- Security Protocols Against Cyber Attacks in the Distribution Automation System, Lim, I.H.; Hong, S.; Choi, M.S.; Lee, S.J.; Kim, T.W.; Lee, S.W.; Ha, B.N.; NPTC, Myongji Univ., Yongin, South Korea http://ants.mju.ac.kr/publication/IEEE_TR.pdf
- Power System and Technical Issues in South Korea, Prof. Jong-Keun Park School of Electrical Eng, Seoul National University, http://oldsite.nautilus.org/archives/energy/grid/papers/jkpark.PDF
- Vulnerabilities in SCADA and Critical Infrastructure Systems, Rosslin John Robles , Min-kyu Choi1, Eun-suk Cho1, Seok-soo Kim1, Gil-cheol Park1, Sang-Soo Yeo, Department of Multimedia Engineering, Hannam University, in International Journal of Future Generation Communication and Networking http://www.sersc.org/journals/IJFGCN/vol1_no1/papers/14.pdf
- Assessment of the Vulnerabilities of SCADA, Control Systems and Critical Infrastructure Systems, Rosslin John Robles and Min-kyu Choi, Department of Multimedia Engineering, Hannam University, in International Journal of of Grid and Distributed Computing, Vol.2, No.2, June 2009 http://www.sersc.org/journals/IJGDC/vol2_no2/3.pdf

②タイ

- Implementation of a SCADA/EMS System in Metropolitan Electricity Authority Thailand, Wiwat Amornimit, Metropolitan Electricity Authority www.mea.or.th/internet/hdd/3-3.doc

③シンガポール

- “Update on Energy Efficiency Policies & Programmes in Singapore,” Energy Market Authority, 35th APEC EGEE&C Meeting Wellington, NZ, 4-5 Feb 10 http://www.apec-esis.org/www/UploadFile/5-%20Singapore's%20EE%20update.pdf
- An Intelligent Energy System Singapore’s Smart Grid Initiative, Eng Kiat Chan, Energy Market Authority, CEPSI 2010 http://www.cleantechinvestor.com/portal/smart-grid/5860-spotlight-on-singapore-smart-grid-city.html
- “Spotlight on Singapore: Smart Grid City,” in Cleantech magazine, July/August 2010, Cleantech Investor Ltd

http://www.cleantechinvestor.com/portal/smart-grid/5860-spotlight-on-singapore-smart-grid-city.html

④中国

- 工業控制網路標準解析（全国工業過程測量及び控制標準化技術委員会、機械工業儀器）2010 年 8 月 6 日
- 情報安全国家標準（信息安全共性技術国家工程研究センター作成）
  http://www.nercis.com.cn/standardv.jsp?id=66
- 中国標準化管理委員会資料
  http://www.sac.gov.cn
- 2010 年信息安全国家標準制修訂項目申報指南（全国信息安全標準化技術委員会）、2010 年 3 月 15 日
  http://www.tc260.org.cn/
- 機械工業儀器儀表総合技術経済研究所使用
  http://www.itei.cn/
- 国家信息化安全標準化“十一五（第 11 次 5 カ年計画）”計画

⑤台湾

-“Taiwan Power Company’s Work in Development in SCADA and Smart Grid,” Yang, Jin-Shyr, TPRI, Taipower, February 4, 2010
- “Green IT Activities and Situation in Taiwan,” Dr./Prof. Jenn-Hwan Tarng, Identification and Security Technology Center, Industrial Technology Research Institute, October 5, 2010
  http://www.greenit-pc.jp/activity/asia/file/chinese_taipei.pdf
- “Development of a Smart Power Meter for AMI Based on ZigBee Communication,” Shun-Yu Chan, Department of Electrical Engineering, I-Shou University/ Cheng-Shiu University, Taiwan
  http://ir.lib.ntust.edu.tw:8080/dspace/bitstream/987654321/14317/1/Smart%20Power%20Meter.pdf

(5)その他

- W32.Stuxnet Dossier, Symantec official blog, 30 Sep 2010
  http://www.symantec.com/connect/blogs/w32stuxnet-dossier

7. 図表一覧

＜付録部分＞

付録

付録 1.　米国・欧州・アジアのスマートメータについて

付録 1.1 米国の動向

1)　AMI の 3 段階導入

スマートメータについては将来の AMI(Advanced Metering Infrastructure)の実現に向けて次の 3 段階が考えられている。英文略称は Assessment of Demand Response Advanced Metering(FERC)による。

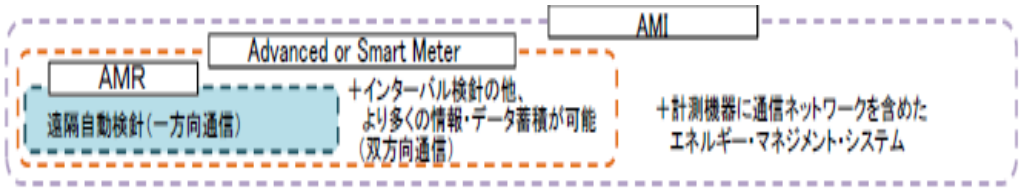
AMR(Automatic Meter Reading)　一方向通信での自動検針システム

AMM(Automatic Meter Management)　自動検針と計器管理・制御　双方向通信

AMI(Advanced Metering Infrastructure)　計器に通信ネットワークを含めたエネルギーマネジメントシステム

米国連邦エネルギー規制委員会の2008 Assessment of Demand Response and Advanced Metering Staff Report[90]によれば、さらにAMIにHANを付け加えた将来型AMIについても検討を行っている。この米国の3段階のステップを資源エネルギー庁は図表・付1-1を用いて説明している。

図表・付1-1　AMIの3段階導入[91]



出典：資源エネルギー庁第 6 回スマートメーター制度検討会「双方向通信の導入とスマートメータの機能について」

2)　NIST の AMI に対する考え方

米国政府の標準化機関である米国立標準技術研究所NISTはスマートグリッド・サイバー

[90] http://sites.energetics.com/MADRI/pdfs/ferc_12-08-demand-response.pdf
[91] 資源エネルギー庁第 6 回スマートメーター制度検討会「双方向通信の導入とスマートメータの機能について」

セキュリティに関するガイドラインに関してCyber Security Working Groupを設けて検討を進めてきた。NISTはThe Smart Grid Interoperability Panel – Cyber Security Working Groupが2010年9月に NISTIR 7628 「Guidelines for Smart Grid Cyber Security(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）」を発行した[92]。
Vol.1は、Smart Grid Cyber Security Strategy、Architecture、and High-Level Requirements、Vol.2は Privacy and the Smart Grid、Vol.3は、Supportive Analyses and Referencesの3部作で構成されている。

スマートメータに関わる部分は特にVol.3は、Supportive Analyses and ReferencesのLOGICAL ARCHITECTURE AND INTERFACES OF THE SMART GRID の項目に詳述されている。この付属F「スマートグリッドの理論上のアーキテクチャとインタフェース」ではAMIのロジックと構成網及び節点の説明を行っている。特に F.1 先進的計測インフラストラクチャ(AMI：Advanced metering infrastructure)の項で次のように説明を加えている。

「先進的計測インフラストラクチャ(AMI)」は、関連するシステムおよびデータ管理ソフトウェアを伴う通信ハードウエアとソフトウェアから構成されている。先進的計測インフラストラクチャ(AMI) は先進的計測機器と競争力のある小売業者やユーティリティ自身を含むユーティリティビジネスシステム(注、ガスや水道などの)間の双方向ネットワークをつくりあげる。先進的計測インフラストラクチャ(AMI) はリアルタイム(もしくは準リアルタイム) で電気機器の電力仕様料金を知らせ、ユーティリティの負荷低減を助けるものである。

AMI を導入したスマートグリッドの利用者の想定される電力情報ネットワークでは幾つかの節点がある。これをインタフェース(接続) と呼んでそれぞれの接続ごとに詳しい理論上の位置付けを行っている。図表・付 1-2、図表・付 1-3 にカテゴリ分けされた AMI 論理インタフェースを示す

[92] 概要についての紹介に「NIST がスマートグリッドのサイバーセキュリティに関する初のガイドラインを最終決定(米国)」NEDO海外レポートNo.1067(2010.10.20)がある。

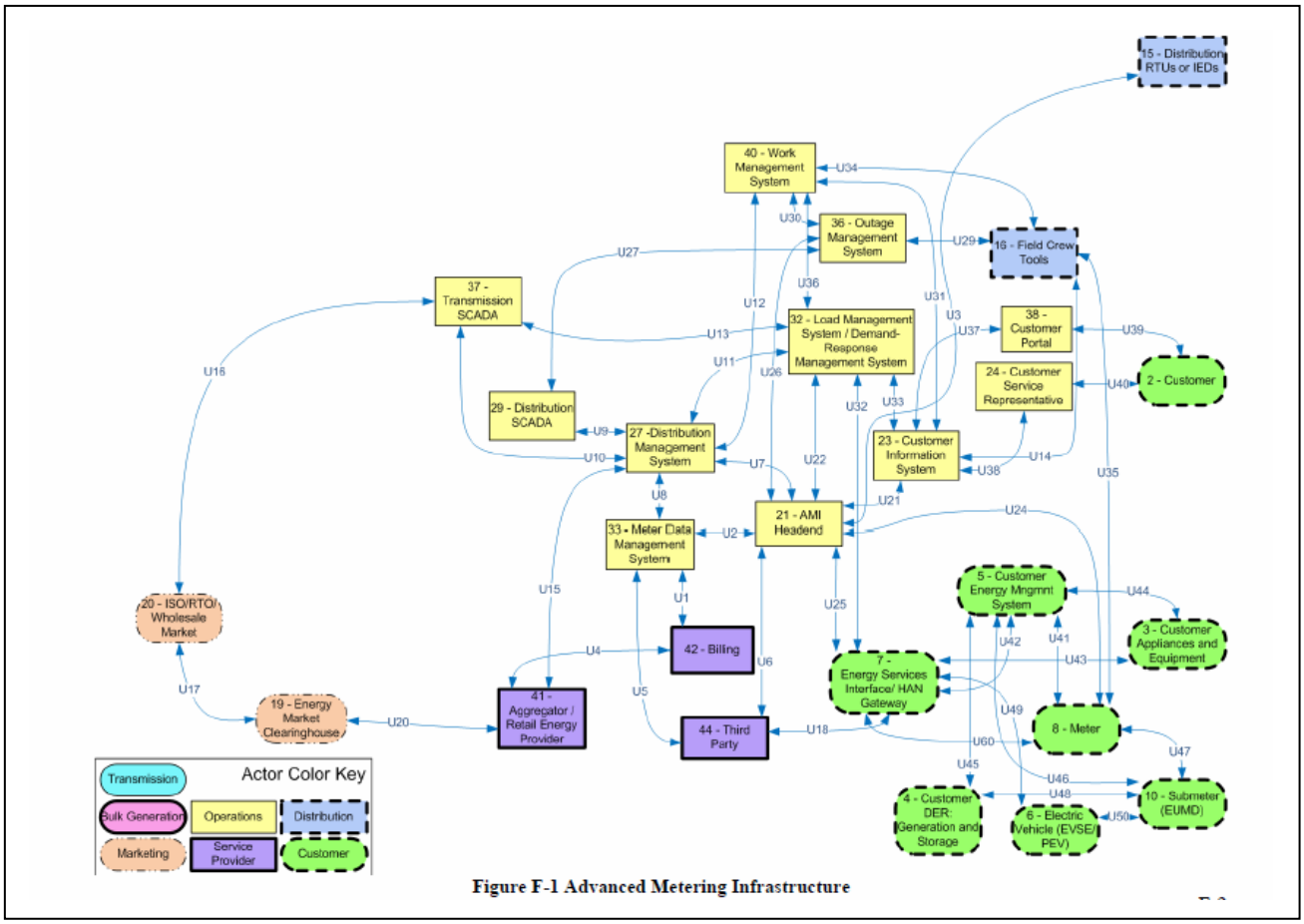
図表・付 1-2　F-1　論理インタフェースカテゴリによる AMI 論理インタフェース[93]

論理インタフェースカテゴリ		論理インタフェース（番号は図表・付 1-3 に対応）
1	コントロールシステムと、高可用性や計算機能を有し、およびまたは帯域幅が抑制された装置の間のインタフェース。例えば ・トランスミッション SCADA と変電設備の間 ・ディストリビューション SCADA と優先順位の高い変電とポールトップ設備の間 ・パワープラント内の SCADA と DCS の間	U3,U28
2	コントロールシステムと、高可用性がないが計算機能を有し、およびまたは帯域幅が抑制された装置の間のインタフェース。例えば ・ディストリビューション SCADA と低優先順位のポールトップ設備との間 ・ポールトップ IED とその他のポールトップ IED の間	
3	コントロールシステムと、高可用性を持つが計算機能や帯域幅制限のない装置とのインタフェース。例えば ・トランスミッション SCADA と自動変電システム	
4	コントロールシステムと、高可用性がなく、計算機能や帯域幅制限もない装置とのインタフェース。例えば ・ディストリビューション SCADA と、ディストリビューションポールトップ IED のため幹線ネットワークに接続された集積ノード	
5	同じ組織の中のコントロールシステム間のインタフェース。例えば ・同じ設備に属する複数の DMS システム ・DCS とパワープラント内の補助的なコントロールシステムの中のサブシステム間	U9,U27
6	異なる組織に存在するコントロールシステム間のインタフェース。例えば RTO/ISO EMS と諸設備エネルギー管理システム間	U7,U10,U13,U16
7	共通の管理権限に属すバックオフィスシステム間のインタフェース。例えば ・顧客情報システムとメータデータ管理システム間	U2,U22,U26,U31
8	共通の管理権限下に属さないバックオフィスシステム間のインタフェース。例えば ・サードパーティ製課金システムとメータデータ管理システム間	U1,U6,U15
9	金融や市場取引を通常含んだシステム間の B２B 接続を備えたインタフェース。例えば ・小売販売集合体と情報機関との間	U17,U20
10	コントロールシステムとノンコントロール／企業システム間のインタフェース。例えば ・労働管理システムと地理情報システム間	U12,U30,U33,U36

[93] NISTIR 7628「Guidelines for Smart Grid Cyber Security」Vol. 3, Supportive Analyses and References

11	環境パラメータ計測のためのセンサとセンサネットワーク間のインタフェースで、通常アナログ計測を備えた簡易なセンサが対象。例えば ・変圧器に備わっている温度計とその受信機間	None
12	センサネットワークとコントロールシステム間のインタフェース。例えば ・センサ受信機と変圧計測間	None
13	AMI ネットワークを使うシステム間のインタフェース。例えば ・MDMS とメータ間 ・LMS/DRMS と顧客 EMS 間	U8,U21,U25,U32
14	高可用性を備えた AMI ネットワークを使うシステム間のインタフェース。例えば ・MDMS とメータ間 ・LMS/DRMS と顧客 EMS 間 ・DMS アプリケーションと顧客 DER 間 ・DMS アプリケーションと DA フィールド設備	
15	以下を含む、顧客（住家、商業、工業上）サイトネットワークで使うシステム間のインタフェース。例えば ・顧客 EMS と顧客アプライアンス間 ・顧客 EMS と顧客 DER 間	U43,U44,U45,U49
16	外部のシステムと顧客サイトの間のインタフェース。例えば ・サードパーティと HAN ゲートウェイの間 ・ESP と DER の間 ・顧客と CIS ウェブサイトの間	U18,U19,U38,U39, U40
17	システムとモバイルフィールド作業員のラップトップ/装置の間のインタフェース。例えば ・領域群と GIS の間 ・領域群と変電施設の間	U14,U29,U34,U35
18	メータ機器間のインタフェース。例えば ・メータとサブメータ間 ・PEV メータとエネルギーサービス事業者との間	U24,U41,U46,U47, U50
19	操作決定支援システム間のインタフェース。例えば ・WAMS と ISO/RTO	None
20	エンジニアリングメンテナンスの システムとコントロール装置との間のインタフェース。例えば ・変電中継装置との間 ・メンテナンスのためのポールトップ装置の間 ・パワープラント内	U11
21	コントロールシステムとそのベンダの標準的な保守やサービスのためのインタフェース。例えば ・SCADA システムとその業者	U5,U132
22	セキュリティ/ネットワーク/システム管理コンソールと全てのネットワークやシステム間のインタフェース。例えば ・セキュリティコンソールとネットワークルータ、ファイアウォール、コンピュータシステム、そしてネットワークノードの間	None

図表・付 1-3　　AMI インタフェース



米国会計検査院 GAO(Government Accountability Office)は、米国立標準技術研究所(NIST)が 2010 年 9 月に初めて発行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ガイドラインに関して、以下の６つの課題を指摘した[94]。

(1)　連邦政府と州政府の不透明な所管の問題。

(2)　消費者に対するスマートグリッドの利点、コスト、リスク等の説明。

(3)　ユーティリティ企業(電力・ガス・水道など)が、セキュリティ全体への対応よりも、規制に合致しているかどうかを優先していること。

(4)　スマートグリッドシステムに使われるデバイス等にセキュリティ対策(イベントログの収集など）が組み込まれていないこと。

(5)　サイバーセキュリティやその他の問題について、電力業界が有効な情報交換メカニズムを有していないこと。

(6)　電力業界がサイバーセキュリティを評価するための評価手法を有していないこと。

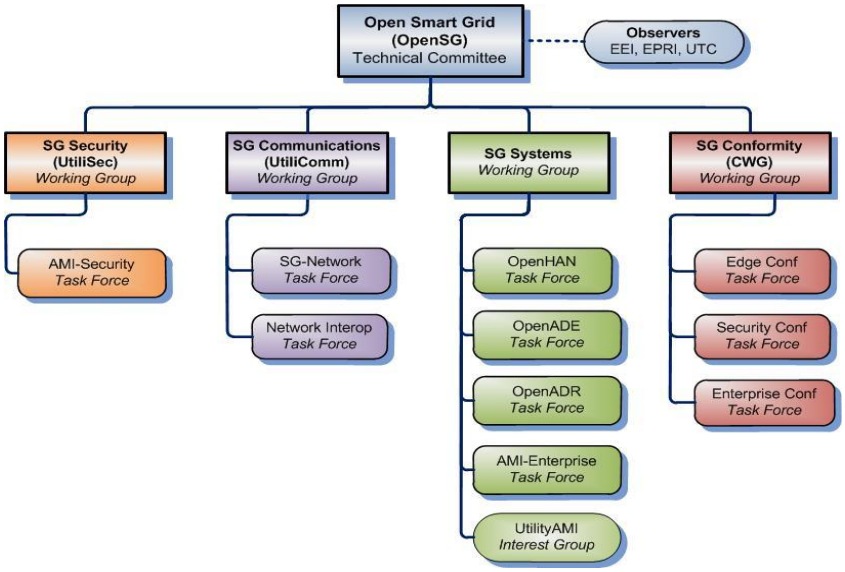
3)　オープンスマートグリッド

[94] Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed, GAO-11-117 January 12, 2011 http://www.gao.gov/products/GAO-11-117

46カ国の155社の電力会社・機器ベンダ等で構成される組織であるUCAIug(2002年6月設立。Utility Communication Architecture International User Group) はスマートグリッドの標準化を促進するために2009年に組織内にOpenSG(Open Smart Grid) 技術委員会を設立した。これがオープンスマートグリッドと呼ばれる動きで、図表・付1-4に組織体制を示す。ここでは電力会社と第三者との情報のやり取りや負荷制御等について、システム要件や制度及びベストプラクティスなどを検討するもので民間産業界が中心となって活動している。OpenHAN(Open Home Area Network)、OpenADE(Open Automated Date Exchange)、OpenADR(Open Automated Demand Response) などのタスクフォースを実施している。

SG Security Working Groupがセキュリティを扱っており、ここにはAMI-Security Task Forceが設置されている。

図表・付1-4　オープンスマートグリッドの組織体制



出典：Open Smart Grid Web ページ[95]

[95] http://osgug.ucaiug.org/org/default.aspx

付録 1.2　スマートメータを巡る近年の欧州の動向

本項では、EU の公式機関である「欧州スマートメータ・アライアンス」(ESMA) と、「欧州スマートグリッド・タスクフォース」(SGTF) の報告書を通じて、欧州におけるスマートメータを巡る最近の動向を紹介する。

1)ESMA の最終報告書に見る欧州の動向

欧州スマートメータアライアンス (ESMA) は、EU の政策執行機関である欧州委員会の下に設けられたアドホック (時限的) な下部機構である。制度的には、ESMA は欧州委員会エネルギー局の「インテリジェント・エネルギー・ヨーロッパ」の下に置かれていた。

ESMA は 2006 年 12 月にアドホック組織として発足し、3 年間にわたってスマートメータに関する幅広い調査検討活動を展開した。それらの調査研究に基づいて 2010 年 1 月に、ESMA は「最終報告書」、「フィナンシャル・ツールキット」、「スマートメータリングガイド」の 3 つの報告書を発表してその任を終えた[96]。この項では、主として ESMA の最終報告書に基づいて欧州のスマートメータを巡る状況を、本調査報告の趣旨と関連する勧告を中心として紹介する。

①スマートメータの特性と応用の定義

ESMA はスマートメータの特性を以下のように定義している。

・計測データの自動的な処理・移転・管理・利用
・メータの自動管理
・双方向データ通信
・消費者を含む関係者とそのシステムに有意かつ適時的な消費情報の提供
・エネルギー効率・エネルギー消費・エネルギーシステムの改善(発・送・配電及び末端利用) をサポートするサービスの提供

ESMA はスマートメータの応用を以下のように定義している。

・末端利用者と分散発電のエネルギー効率の監視と改善。消費者情報のフィードバック
・末端利用者のエネルギー管理
・料金設定(時間、最大需要、季節)
・エネルギー節約
・電力系統への需要対応、系統運用サポート、ピーク負荷制限
・スマートホーム、ホーム自動化、エネルギー企業による家電製品の遠隔制御
・遠隔開閉・負荷制御
・負荷分析、モデリング、予測
・決済と請求
・バーチャル発電プラント、再生可能発電、コジェネ
・エネルギー市場の競争と効率の改善
・発・送・配電企業による顧客サービス

[96] ESMA: http://ieea.erba.hu/ieea/page/Page.jsp?op=project_detail&prid=1564

・盗電検出
・国家機関などへの情報提供
・メータ管理
・送電ネットワークの状態評価
・電力の質の信頼性の監視
・プリペイメント
・周波数・電圧制御などの付加サービス
・停電分析と事前メンテナンス
・安全、安全保障、遠隔医療、地域的警報サービス

② カスタマー・フィードバック(見える化)

電力消費情報の顧客フィードバックを、ESMA は直接フィードバックと間接フィードバックに分類している。直接フィードバックでは、家庭内ディスプレイ(全家庭または個々の家電) を通じて、または事前支払いあるいは時間関連価格設定体系の一部として、リアルタイムに情報が最終消費者にフィードバックされる。間接フィードバックでは、最終消費者に届けられる以前に情報処理され、他のチャネル(ウェブサイト、E メール、頻度の高い請求書など)を通じて最終消費者に伝えられる。

カスタマー・フィードバック・システムについて、ESMA は以下の 6 点を勧告している。
・顧客は即時的かつ継続的にエネルギー消費について、光学的インハウスフィードバックデバイスによって知る必要がある。
・直接フィードバックが間接的フィードバックより効果的
・目標設定が伴うとフィードバックはさらに有効
・履歴フィードバックが比較的または規準的フィードバックより有効
・直接ディスプレイと詳細請求書の組み合わせが、間接的個人ウェブページより好まれる。
・インターネットは長期的データに基づいた分析やアドバイスと結びついた有用な追加的フィードバックを提供できる。

下の図表・付 1-5 は、カスタマー・フィードバックの伝達メディアについて、最終消費者がどのようなメディアを好むかについての国別の調査である。光学的スクリーン上での直接ディスプレイと詳細な請求の組み合わせが好まれることを示している。

「見える化」に関する上記の勧告に基づいたカスタマー・フィードバック・システムとして、ESMA 報告書は PowerPlayer を特筆して紹介している。(図表・付 1-6 及び図表・付 1-7 参照)

図表・付 1-5　スマートメータのフィードバック情報の受信手段に対する選好

国	ディスプレイ上の情報	詳細な請求書	個人別のウェブページ	電話サービス
フィンランド	68%	46%	34%	10%
ノルウェイ	54%	29%	32%	10%
スウェーデン	49%	28%	39%	5%
デンマーク	58%	29%	41%	10%
オランダ	39%	25%	23%	10%
フランス	57%	53%	28%	9%
ドイツ	61%	66%	32%	5%
英国	59%	61%	30%	20%
スペイン	50%	73%	29%	23%
ポルトガル	22%	32%	18%	5%
平均	55%	57%	30%	11%

出典:European Smart Metering Alliance Publishable Report[97]

図表・付 1-6　Powerplayer

出典:European Smart Metering Alliance Publishable Report

図表・付 1-7　iPhone 上の Powerplayer

出典:European Smart Metering Alliance Publishable Report

[97] http://ieea.erba.hu/ieea/page/Page.jsp?op=project_detail&prid=1564

③スマートメータ普及の技術的障害

スマートメータ普及のために克服すべき障害として、ESMA は法的障害、経済的障害、技術的障害、社会的障害の 4 点を指摘している。本調査報告の趣旨から、ここでは特に ESMA 最終報告書が指摘する技術的障害について紹介する。

・「インターオペラビリティの欠如」が、スマートメータの大規模採用を妨げている。主たる問題は、異なった製造者から提供されるシステムとデバイスの間のインターオペラビティを保証するオープンスタンダードの欠如である。適切な共通機能とオープンインタフェースの要請が、スマートメータとそのデータを利用したアプリケーションの市場を機能させる。

・現状のスマートメータには「モジュラー性が欠如」している。分散発電、需要対応、電力品質、顧客情報、エネルギー効率自動化などへの対応が、高コスト化している。

・「適切な標準化の欠如」した大規模なスマートメータ化は、サービスとアプリケーションの開発を妨げ、次世代のメータ交換まで 10 年間をロスすることになる。その反面、設計の貧弱な標準は開発のイノベーションを妨げる。

・「発・送電業者/配電業者/スマートメータ製造メーカ間の協力が弱体」である。特に AMR 技術とデータ通信について、協力関係と共通のアプローチとコンセンサスが必要である。また、異なったシステム間の統合が必要であるという意味で、マルチ・ユティリティの計量が重要となる。

④フィナンシャル・ツールキット

ESMA はその解散時に、最終報告書とは別にフィナンシャル・ツールキットを発表している[98]。このツールキットの主たる目的は、スマートメータ導入に関するコスト/ベネフィット分析を行うことであった。このツールキットでは、(1)現況の計量手法の継続、(2)改善された請求手法の導入、(3)リアルタイム・フィードバックの導入、(4)事前支払い手法の導入、(5)電力・ガスの統一計量化の 5 点を取り上げ、コスト/ベネフィットの詳細なモデリング分析を行っている。

⑤スマートメータリングガイド

ESMA はその解散時に、膨大なスマートメータリングガイド（151 ページ）を公表した[99]。この報告書は、スマートメータの導入と将来性を巡る 11 の課題について詳細に報告している。以下がこのガイドの指摘する諸課題である。

・なぜスマートメータか？
・スマートメータと顧客フィードバック
・スマートメータ―テクニカルオプション

[98] ESMA Smart Metering Financial Toolkit
http://ieea.erba.hu/ieea/page/Page.jsp?op=project_detail&prid=1564

[99] Smart Metering Guide Edition 2010
http://ieea.erba.hu/ieea/page/Page.jsp?op=project_detail&prid=1564

・スマートメータシステム―マルチ・ユティリティ課題
・スマートメータ―とスマートグリッド
・デマンド対応のためのスマートメータ・サービス
・スマートホームのためのスマートメータ・サービス
・ユーティリティとスマートメータ
・実証試験で得られたエネルギー節約効果
・メータリングの法規制と標準化
・スマートメータ・サービスのマーケティング

ESMA は、上記 11 個の課題について詳細な分析を行い、それぞれの課題について具体的な勧告を行っている。勧告の一例として「スマートホームのためのスマートメータ・サービス」を挙げるならば、ESMA は以下 4 点の勧告を行っている。
・スマートメータから HAN への消費データへのリアルタイムアクセスが提供されなければならない。
・スマートメータとスマートホームシステムとの間の通信プロトコルの一致。もし、共通のシステムが使用されないとすれば、スマートメータ LAN とスマートホーム HAN の結合を提供するハードウェアブリッジが用意されていることによってサポートされなければならない。
・コマーシャルベースの交渉が要請される。
・スマートホームデバイスにデータをパスするスマートメータ通信リンクを使用できる、承認済みのエージェントを保証しなければならない。通信サービスのコストをカバーするスマートメータデータプロトコルがスマートホームアプリケーションへとメッセージをパスできる機能があることを保証しなければならない。
⑥国別の進捗状況
ESMA の最終報告書[100]では、ヨーロッパ 24 カ国におけるスマートメータの進展状況を報告している。その内容についてはこの最終報告書の P.38 を参照の事。

2)欧州の SGTF におけるスマートメータセキュリティ分析の最新動向

一方、欧州のエネルギー供給サイドでは、欧州委員会のガス＆エネルギー局内にアドホック組織として「スマートグリッド・タスクフォース」(SGTF) が設立され、現在活動中である。設立は 2009 年 11 月、存続予定機関は約 20 カ月であり、2011 年夏頃まで活動が継続される予定である[101]。

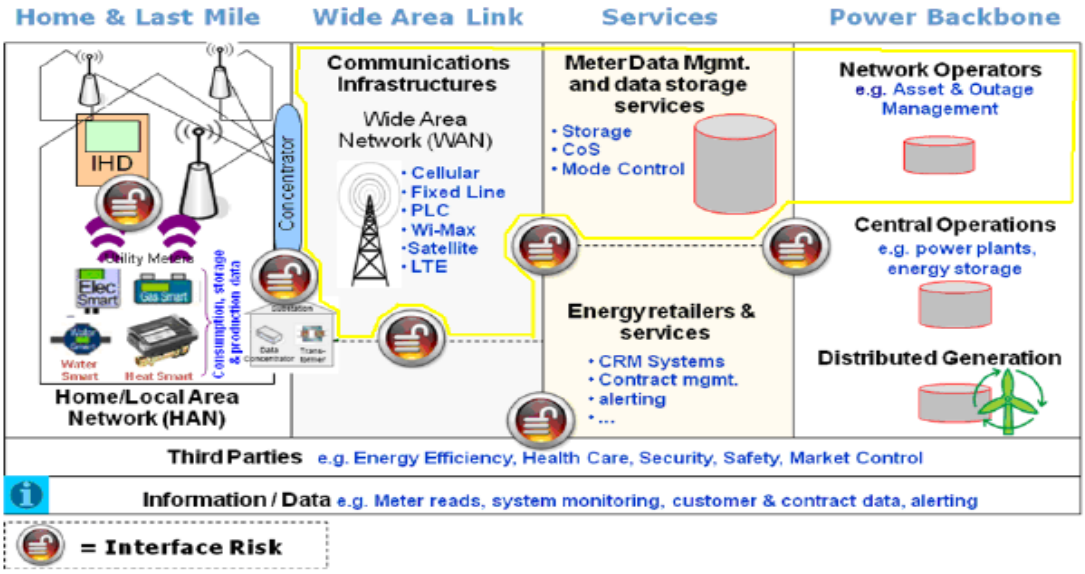
SGTF はステアリングコミティの下に、三つのエキスパートグループ(EG)が置かれている。EG1 が「スマートグリッドとスマートメータの機能(Functionalities)」、EG2 が「データセキュリティ、データハンドリング、データプロテクションのための規制勧告」、EG3 が「スマートグリッド展開に関わる関係者の役割と責任」である。本項では、本報告書の趣旨に

[100] http://ieea.erba.hu/ieea/page/Page.jsp?op=project_detail&prid=1564 <ESMA pubukishable report>
[101] http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm

最もよく関連する EG2 の報告書(全 41 ページ、2011 年 2 月 16 日公表）の「データセキュリティ」の部分について、その分析と勧告を概観する[102]。

EG2 中間報告書が概観するスマートメータのアーキテクチャ概念図は、図表・付 1-8 の通りであり､黄色の枠で囲まれている部分が､多くの EU 諸国において DSO(配電サービス業者）が担っている機能を示している。

図表・付 1-8　スマートメータのアーキテクチャ概念図とインタフェースリスク

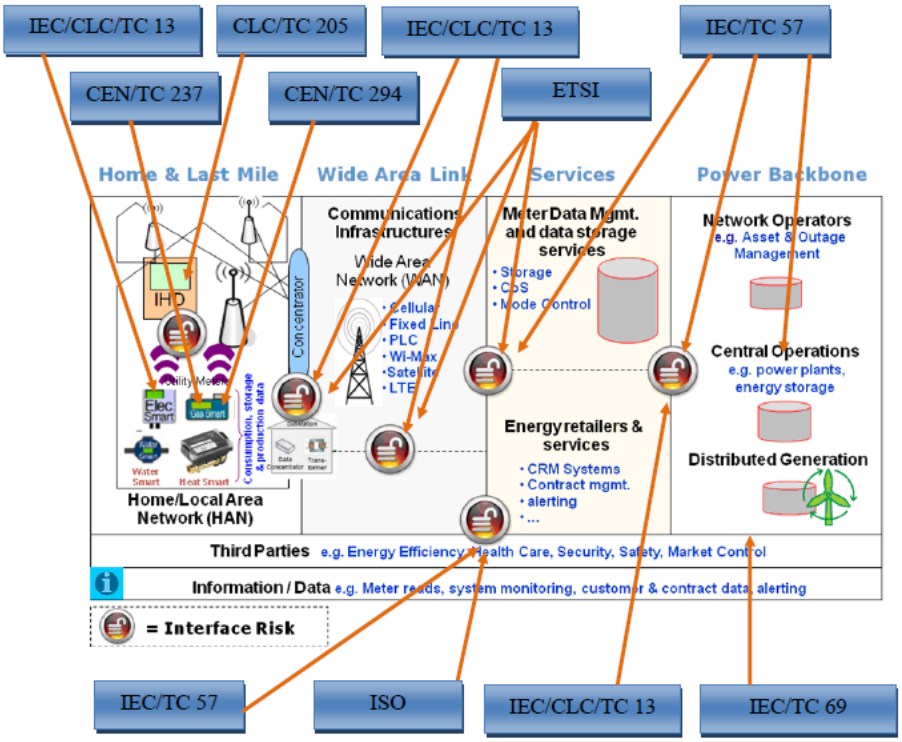


出典：SGTF EXPERT GROUP2 報告書[103]

上の図表・付 1-8 には 6 個の錠前が示されているが、EG2 中間報告書はこの部分にインタフェースリスクが集中するとしている。中間報告書では 13 個のインタフェースとそのリスクを示している(4.3.3 節参照)。さらに次に示す図表・付 1-9 では、各インタフェースリスクに関連する標準化に関わる委員会や組織が掲げられており、続く図表・付 1-10 では各種委員会や組織の責任分野が明確化されている。

[102] http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf
[103] http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf

図表・付 1-9　インタフェースリスクとそれに関連する欧州内の委員会と組織



出典：SGTF EXPERT GROUP2 報告書

図表・付 1-10　標準化委員会・組織とその責任分野

標準化委員会/組織	責任分野
IEC TC57	ESP(Energy Services Portal) システムのインタフェースと共通情報モデル
IEC TC13	電力メータと通信プロトコル
ISO	データセキュリティのビジネスプロセス
CEN TC 294	バッテリー駆動メータ通信
CEN TC 237	ガスメータ
ETSI M2M	通信
CLC/TC205	家電製品の家庭内自動化と通信プロトコル
IEC TC69	電気自動車
PCI-DSS	プリペイドカード産業

出典：SGTF EXPERT GROUP2 報告書

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、以下の勧告を行っている。

> このエキスパートグループは、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的側面を特にかつ暗示的にカバーする新しい標準化を、上記のリスト（本報告書の図表・付 1-10）に基づいて更新・拡張・開発する仕事を行わなければならないことを勧告する。
>
> スマートグリッドのエンド・ツゥ・エンドのセキュリティとプライバシ保護を設計するに際しては、最も適切な暗号プリミティブを明確に評価する仕事がもっとなされなければならないのは明確である。例えば、対称鍵暗号(例えば AES)、あるいは非対称暗号(例えば RSA や ECC 暗号)。暗号方式の選択は、信頼プロビジョニング、キー配布、キー防護、キー発生、キーパーソナライゼーション、キー廃棄やリタイアリング、キー更新にとって、大きな影響を持っている。
>
> (以下略)

付録 1.3　アジアの動向(スマートグリッド実証実験との関連で)

1)　韓国における実証実験

韓国の電力業界

電力自由化の一環として 2001 年、KEPCO (Korea Electric Power Corporation、韓国電力公社)の発電部門を韓国中部発電など 7 社 (原子力発電[104]1 社、火力 5 社[105]、送配電 1 社) に分社し、送配電設備を保有する KEPCO が民間を含めた発電事業者から電力を購入して顧客に供給している。発電部門は日本のような地域毎の電力会社と異なり、ソウル釜山で事業等という地域に限定されない事業形態をとっている。韓国の発電事業者が KEPCO に電力を卸売りする時は電力取引所で取引されており、電力取引所は送電線運用も行っている。電力小売り競争は配電ネットワークにオープンアクセスを導入し小口部門の自由化を図っている。スマートグリッドの導入では、この電力取引所が消費者主導のリアルタイム電気料金制度を構築する必要に迫られている。

スマートグリッドの技術開発戦略

韓国のスマートグリッドの技術開発戦略の動向は次のとおりである。2 月に知識経済部が大統領に「世界最初の国家単位のスマートグリッド構築ビジョン」を提言、3 月に「スマートグリッドロードマップ樹立推進委員会」を設立、5 月にスマートグリッド協会も発足した。2010 年 11 月には「スマートグリッド促進法案」、「リアルタイム電気料金制導入法案」、「内需創出･輸出産業化法案」などの関係法整備を伴う政策目標が発表されることになっているが現段階で詳細ははっきりしない。

政府が定めたスマートグリッドのロードマップによれば次の 3 段階のステップで実施される。(図表・付 1-11)

ステップ 1 はパイロットモデルで 2010-2013 年の期間で行われる。済州島のスマートグリッド実証実験である。

ステップ 2 はソウル市におけるスマートグリッドの構築で 2013-2020 年の期間を予定している。2015 年には統合したスマートグリッドのオペレーションを行い、2017 年には自動車のシステムを結合する。2020 年には AMI を完備させる。

ステップ 3 は国家全体に及ぼされたスマートグリッドの達成であり、2021-2030 年の期間を予定している。2021 年から自己修復機能を持った知能型グリッドを目指し、2025 年 12 月には東アジアにおける相互接続を目指す。2030 年には再生エネルギーの比率 11%を達成、電気自動車導入 20%を実現させる(国家の低炭素社会の実現という計画の中で、スマートグリッドのロードマップ達成は大きな役割を与えられている) 。

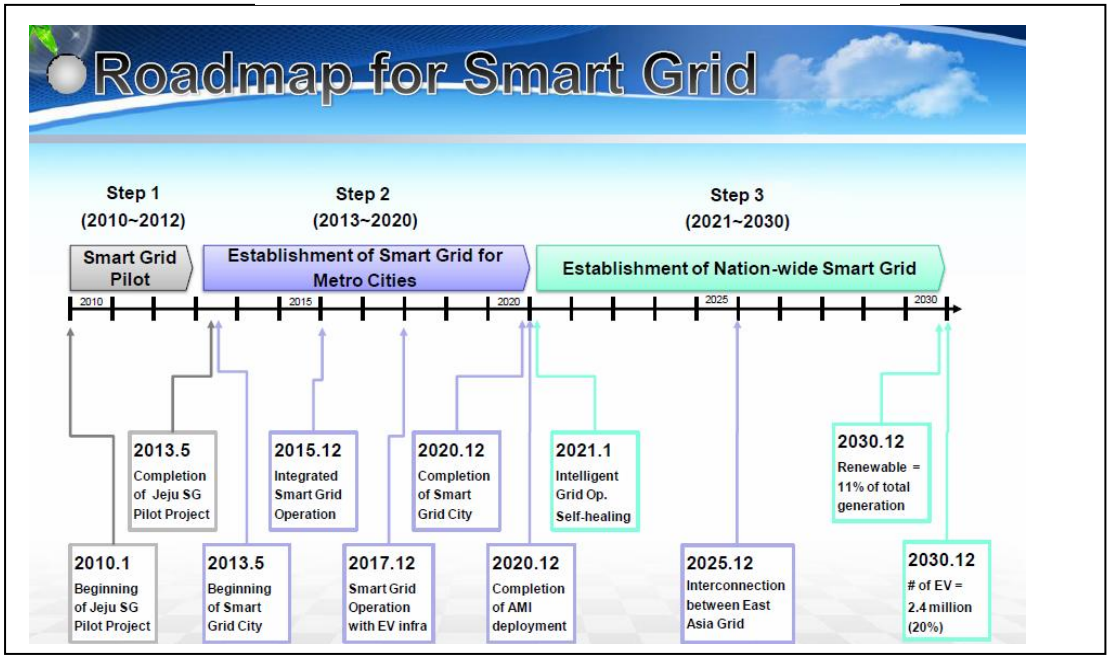
---

[104] 韓国水力原子力発電(KHNP)

[105] 韓国南部発電(KOSPO)、韓国中部発電(KOMIPO)、韓国東西発電(KOEWP)、韓国西部発電(KOWP)、韓国南東発電(KOSEP)

セキュリティに関する目標としては”セキュリティガイドライン”を整備し、スマートグリッドにあったセキュリティ体系を構築する。特にスマートグリッドのセキュリティに関わる標準と認証制度の構築については済州島のスマートグリッド実証実験段階で実験がなされようとしている[106]。

図表・付 1-11　スマートグリッドのロードマップ



出典：Dong Sub Kim” Smart Grid Pilot Project in Jeju Island and KEPCO の構築についてはている。スマートグ”

スマートグリッドのセキュリティガイドライン

韓国では米国立標準技術研究所(NIST) が昨年8月に発行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ガイドライン NISTIR 7628 “Guidelines for Smart Grid Cyber Security: Vol.3, Supportive Analyses and References”を基礎として検討している。しかしながら国情の違いなどを考慮した韓国版サイバーセキュリティに関するガイドラインの作成検討に着手している。この検討には関連専門研究者が関わっており2011年中には案が提出される見込みである[107]。

済州島のスマートグリッド実証プロジェクト

済州島の実証プロジェクトの主管は知識経済部[108]であり、韓国科学技術計画評価研究所

[106] SK テレコム等関係者に対するヒアリングによる

[107] 韓国電力研究院や SK テレコムなど通信事業者などの複数の専門家は、NIST のガイドラインは米韓の国情の違いなどからそのまま適用するには無理があり、できれば NIST ガイドラインをもとにして、日本などアジア諸国とベースが共通できるガイドラインを検討したいとの意見も聞かれた。

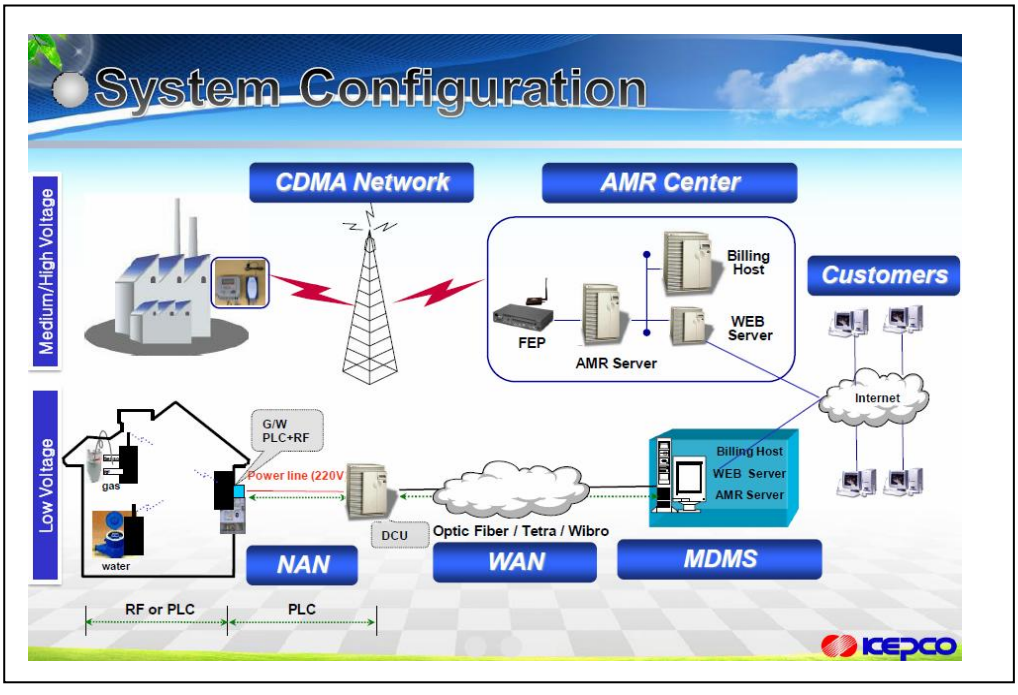
[108]知識経済部の URL は http://www.mke.go.kr/language/jap/index.jsp

KISTEP[109]が取り纏め、済州北東部の旧左邑につくられる。スマートグリッドのコンフィギュレーションを図表・付 1-12 に、全体概念を・付 1-13 に示す。

国家のスマートグリッドインフラを構築するという長期的な目標の下で、政府と民間事業者が Matching Fund 方式で濟州の旧左(Gujua)邑の一帯に実証実験基地を構築し Smart Grid 開発技術の開発を進め早期の実用化を図ることを狙っている。民間は多様な分野の約 168 の事業者が参加している。政府の出資は 696 億ウォン(約 52 億円）である。すなわち総事業費は 1392 億ウォン(約 104 億円）（推定)、需要家 3,000 世帯と 2 カ所の変電所等で構成され、風力発電などの小規模再生エネルギー電源、電気自動車充電器、家電製品、エネルギー情報ポータルシステム、ビルディング自動化システムなど、産業全般を網羅してスマートグリッド構築に取り組む。目標は 2011 年末までに電力 IT の新しい成果としての応用ソフトウェア開発、再生エネルギーの連結、発電制御システムなどインフラ中心の詳細設計を進め、電力 IT の 10 の研究成果の分析･実証、個別研究成果の試験、評価システム構築、実証対象製品と電力系統の相互運用検証、統合アーキテクチャ開発などの高度化設計過程を経て 2013 年中に完工する予定である。また、実証試験の成果をもとに海外市場進出も狙っている。

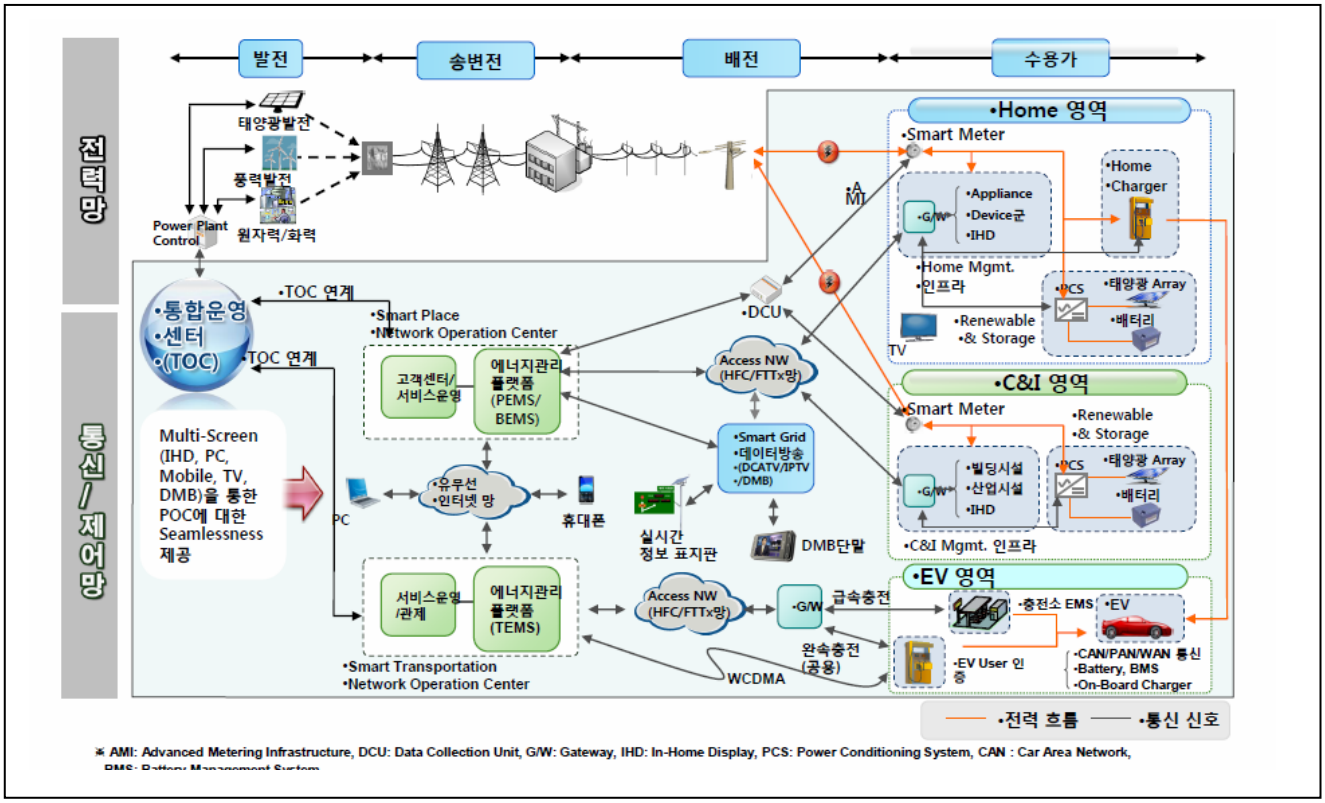
この団地では、リアルタイムの電気料金情報を家電製品に提供、知能型メーターを使用し経済的使用を支援する。再生電力関係では電気自動車用については、充電スタンドとバッテリー交換所の設置、家庭でも自動車電池充電できる設備を整備。風力、太陽光発電などの余剰電力を逆供給するシステムも設定されている。送電電力網は双方向の電力伝送で、故障時には自動復旧可能である。KEPCO が独自開発した高速 PLC 回線技術が使われる。

図表・付 1-12　スマートグリッドのコンフィグレーション



[109] 韓国科学技術計画評価研究所 KISTEP の URL は http://www.kistep.re.kr/eng/main.jsp

図表・付 1-13　韓国におけるスマートグリッドの全体概念



出典：KEPCO 資料（図表・付 1-12、13）

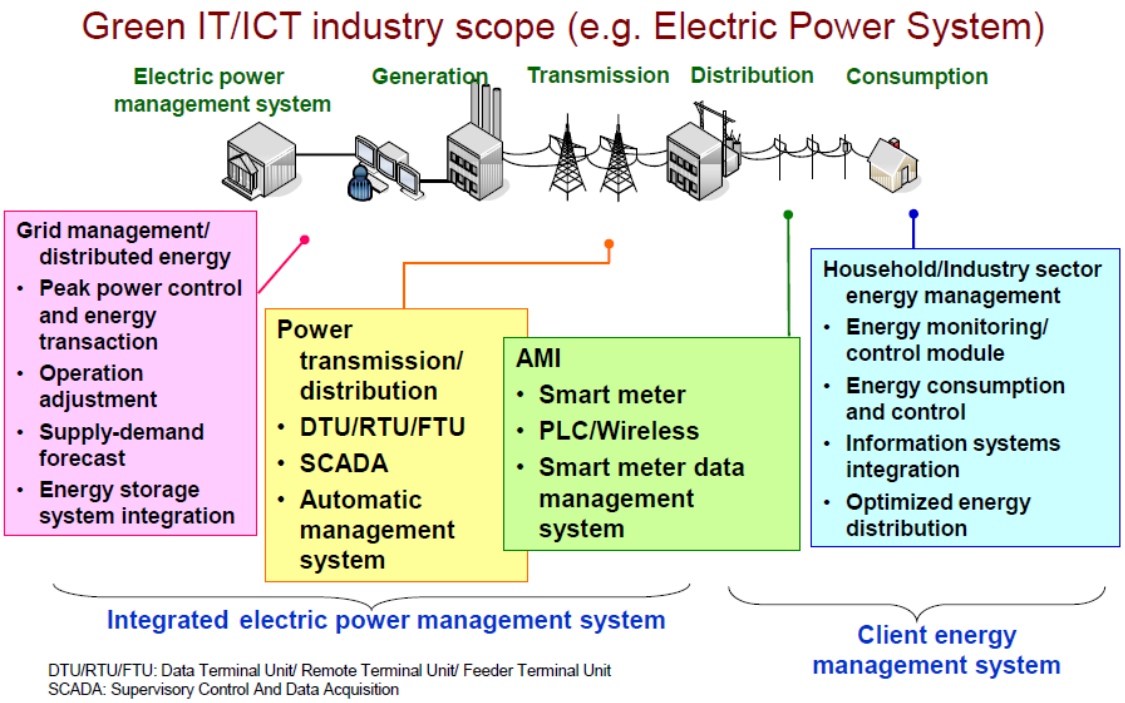
2)　台湾における実証実験（台湾電力資料）

台湾は 2009 年 4 月に MOEA（Ministry Of Economic Affair=経済部）が主催した「グリーンエネルギー開発戦略」によって、本格的なスマートグリッド開発計画を発足させた。計画の中心は太陽光発電、LED 照明、風力発電、バイオ燃料、燃料電池、グリーン ICT、低排ガス車などに置かれている。

台湾のリニューアブル電源は、2010 年 5 月時点で、設置済み風力発電タービンが 219 機、設置容量は 417MW である。PV は設置容量 7.3MW、在来型水力が 1937MW となっている。2025 年における目標値は、風力 3000MW、PV1000MW、バイオマス 1400MW である。以上のような目標を達成するために、スマートグリッド化が要請されている。

台湾におけるスマートグリッド･スマートメータ導入計画の概要を図表･付 1-14 に示す。

図表・付 1-14　台湾におけるグリーン IT/ICT 産業の範囲



出典：Dr./Prof. Jenn-Hwan Tarng "Green IT Activities and Situation in Taiwan" [110]

台湾の電力消費は産業用の高圧 220V と家庭用の 100V に 2 分されているが、総電力消費の 58%を占める高圧ユーザから AMI の導入を始めるというのが、スマートメータ計画の中心になっている台湾電力の方針である。台湾の高圧ユーザは約 2 万 4000 社に達するが、そのうち 1200 社のユーザについては 2010 年中にスマートメータを取り付け、残りの 2 万 3000 社については 2011 年と 2012 年で AMI 化を完了するとしている。また、低電圧ユーザについては、2012 年までに 1 万軒、2014 年までに 100 万軒、2015 年までには 500 万軒に AMI を普及させるとしている。なお、台湾の電力最終ユーザは計 600 万軒である。

スマートメータ本体については、電力計量チップとそのソフトウェア以外はすでに国産化されている。通信モジュール、電池、メータ情報管理システムなどは国内メーカによって開発・提供されている。

スマートグリッド末端部について、台湾電力は給電自動化と AMI を組み合わせた概念を提起している。

スマートグリッド化の核心部分である通信インフラとそのプロトコルについて、台湾電力は以下の 4 点を重要課題として指摘している。

①通信プロトコルの課題は、SCADA システムの統合、分散化した風力発電の情報プラットフォームの統合化、新しい国際プロトコル標準の影響を含む。

②台湾電力の通信プロトコルのガイドラインは、2006 年に公表され、スマートグリッドシ

[110] http://www.greenit-pc.jp/activity/asia/file/chinese_taipei.pdf

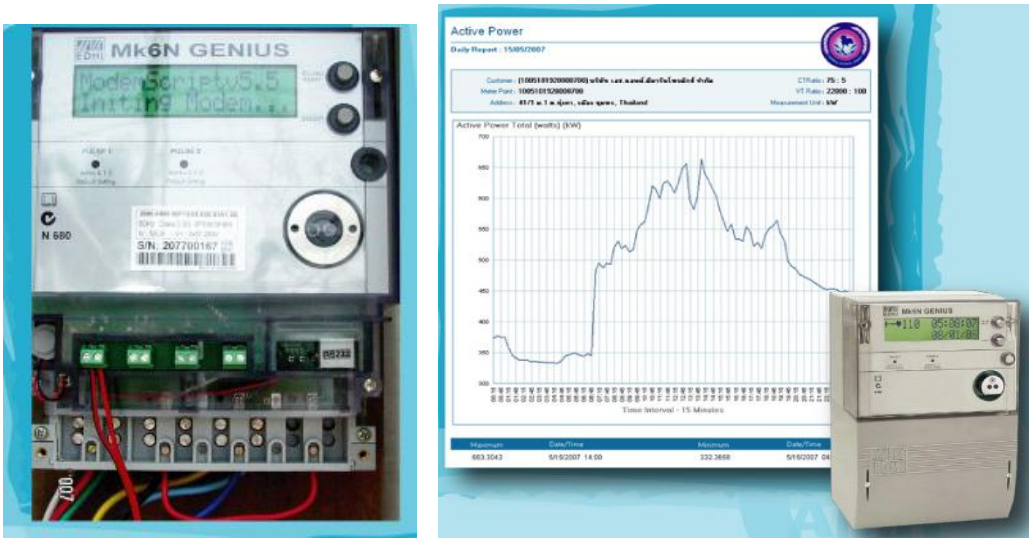
ステム上の通信プロトコル問題を取り扱う勧告と方向性を提供している。
③特定のシステム向けの通信プロトコル標準は TCP/IP 上の DNP3.0 あるいは IEC61850 にフォーカスされるだろう。
④系統システムにおける SCADA プロトコルの継続性が、通信の高速性よりも重要である。

この項は 2010 年の「SCADA Asia2010」における台湾電力の Yang Jin-Shyr 氏の報告、及び 2010 年の「Asia Green IT forum」における台湾交通大学の Tarng Jenn-Hwan の報告をベースとして作成したものである。

3)タイにおける実証実験

タイの電力供給事業は、発電を担当するタイ発電公社(EGAT)と、送配電を担当する MEA(首都圏電力公社＝首都圏を営業地域とする) 及び PEA(地方電力公社＝首都圏を除く全地域を営業地域とする) の 3 社で担われている。これら電力会社の中では PEA が最も積極的にスマートメータの導入を図っており(PEA のスマートメータ導入:AMR(Automatic Meter Reading＝自動検針)プロジェクト)(図・付 1-15)、その理由は、PEA の配電地域が広く地方に分散しており、検針と請求に膨大なコストを費やしているため、スマートメータ導入によって膨大な検針コストを縮小することが期待される[111]。

図表・付 1-15　現在実証中のタイ PEA のスマートメータと電力使用プロファイル



出典：　PEA 刊行のスマートメータ普及パンフレットより

PEA は以下の 6 点を AMR 導入のメリットとして指摘している[112]。

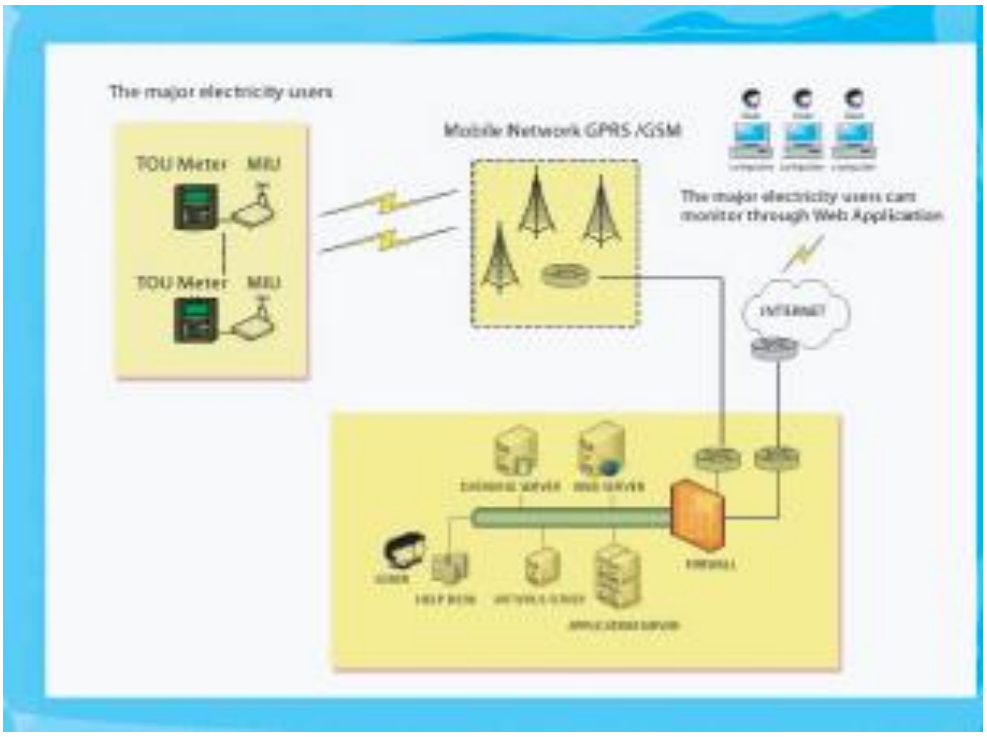
①人力検針のコスト削減
②電力ロス(漏電、盗電、配電網の故障) の検出
③電力使用量の詳細データを入手することによる需要家自身による節電
④AMR データに基づいた迅速な修理の手配
⑤請求される電力料金への需要家の信頼性向上
⑥ウェブ上での負荷プロファイルを確認することによる需要家による電力使用量管理
⑦インターネットを通じた電力料金支払い(E ペイメント)
⑧国全体の省エネ化

PEA の AMR 導入プロジェクトは 2005 年 5 月に取締役会で決定され、大きく 2 つのステッ

[111] チュラロンコーン大学工学部のエカチャイ准教授(タイ IEEE 会長)からのヒアリング、
[112] タイ地方電力公社(PEA)パンフレットによる

プを踏んで進行されることになっている。第 1 段階が大口需要家 3 万口に対するスマートメータの設置、第 2 段階が 100KVA または 30KW 以上の需要家への設置である。PEA の AMR 導入プロジェクトは、現在第一段階が進行中である。PEA の AMR 概念図を図表・付 1-16 に示す。

図表・付 1-16　PEA の AMR 概念図



出典：　PEA 刊行のスマートメータ普及パンフレットより

PEA は現在展開中の AMR によって以下 5 つのことが可能になると述べている。

①AMR による自動検針データの収集は 15 分間隔で行われ、MIU(Meter Interface Unit) を介して GPRS 無線によって中継基地に送信され、そこから有線で AMR サーバに送信される。送信された電力使用量データを AMR ソフトウェアが処理して、インターネット上にアップロードし、電子請求書の発行も行う。需要家は使用量や使用プロファイルをネット上で確認でき、E ペイメントで支払いをすることもできる。

②メータの故障や電気の違法な利用は自動的に AMR センターに通知され、管理者は直ちに対応することができる。

③封印されたメータが開けられた場合には、直ちに管理者に通知され、携帯電話などによって監督者が現場に急行できる。

④主な通信回線は GPRS 無線だが、バックアップとして GSM 無線も利用できる。

⑤需要家は AMR サーバ上のデータを用いて、需要家は一日、一週、一月、一年などの使用量の履歴を参照して比較することができる。タイ国 PGA 社のパンフレットによれば同社が

利用しているスマートメータは、EDMI 社製の大口ユーザ向け MK6N GENIUS である。EDMI 社は 1978 年にオーストラリアで設立され、その後シンガポール資本に買収されたスマートメータ専用メーカである。

実証実験で使用されているスマートメータの仕様を図表・付 1-17 に示す。

図表・付 1-17　スマートメータ MK6N GENIUS 仕様

計量精度	IEC62052-11 、 IEC62053-21(Class1) 、 IEC62053-22 (class 0.55) 、 IEC62052-23(class2)
計量モード	単相(3 回路)、3 相 3 線、3 相 4 線
通信オプション	*ANSI Type2 Optical Port (ANSI C12.18) 又は IEC62056-21 (IEC611-07) Optical FLAG Port *RS232(RTS/CTSI 及び DTR/DCD)　*RS485(2 又は 4 線マルチドロップ) *SCADA　*モデム(PSTN/GPRS/GSN/CDMA) *内部モデム電力供給　*MV90 コンパチブル *PPP/GPRS　*MODBUS *DNP3 *マスタ/スレーブ設定。マスタゲートウェイメータを通じて、31 スレーブメータにアクセス可能
ソフトウェア	ウインドウズ 98/ME/NT/2000/XP 上で走る EDMI 社製の EziView を、メータプログラミングとリーディングに使用。 EziView は後にメータにアップロードするために、料金プログラムと計量パラメータをオフラインでコンフィギュレーションできる。
アプリの拡張性	拡張可能
拡張例	*最大デマンドの割合を SMS(Short Message Service) にて送信 *請求期間中の平均電力ファクター *LCD メニューシステム *電磁タンパー検出 *電力ファクター制御拡張 *パルスアウトプットを通じた最大需要制御 *平均電圧・電流・アンバランスなど *電圧低下・上昇、停電 *電圧品質 *機器故障に際する SMS 又は GPRS(General Packet Radio Service) による警報送付 *個々のフェーズの VT フェイリュアの検出

出典：EDMI 社ホームページ[113]

2010 年 11 月 24-25 の両日に渡って、「スマートグリッド・スマートユティリティ・フォーラム 2010」と題する産学の会議が IEEE タイを中心として開かれた。この会議にはタイ国規制官庁(エネルギー規制委員会)、EGAT、PEA、MEA などの電力会社、学会などタイ国内からの参加者以外に、KEMA(スマートグリッド関連コンサルタント企業)、韓国電力公社(KEPCO)、GE エネルギーサービス、Echelon Asia、中国、オランダ、スウェーデン、英国、香港、シンガポールなどのユーティリティ企業や、コンサルタント企業が参加した[114]。

[113] http://www.edmi-meters.com/Default.aspx 及び http://www.wallaby-meters.com/downloads/Mk6N.pdf

[114] 会議のイニシアティブを取ったエカチャイ准教授は 2011 年も継続的に開く意向で日本の経験を取り入れるためにも、日本のユーティリティ企業、ベンダ、学会からの参加を求めている。

4)シンガポールにおける実証実験

シンガポールのインテリジェント・エネルギー・システム実証実験

シンガポールでは、エネルギー市場監督庁(EMA)の下で、発電会社 3 社、送配電会社 1 社、販売会社 1 社が設立され、その下に多数の小売会社が競争しており、アジアでは最も電力自由化が進展した国となっている。また、1 顧客当たりの平均停電時間が年間 1 分以下と、高い電力品質を実現している。

2009 年 11 月に EMA は「Intelligent Energy System＝IES」という名で、スマートグリッド実証実験を開始している。この実証試験の第 1 フェーズでは、4500 個のスマートグリッドが需要家に配布されが、その範囲は産業ユーザ、商業ユーザから住居にまで及んでいる。3.3 でも触れたが、フェーズ I（2010 年～2012 年)、フェーズ II（2012 年～2013 年）の 2 段階により「スマートメータ」「需要応答管理システム」「複数の電力源からの供給電力管理」の 3 分野に関する実証実験が行われる。

それぞれの実験概要は以下の通りである[115]。

●スマートメータ

通信機能のついた電気使用量の測定器「スマートメータ」を、光ファイバーケーブルや無線 LAN などの通信ネットワーク上に設置し、電力会社および利用者に電気の使用状況や送電量などの情報を知らせる双方向通信網システムを構築する。

●需要応答管理システム

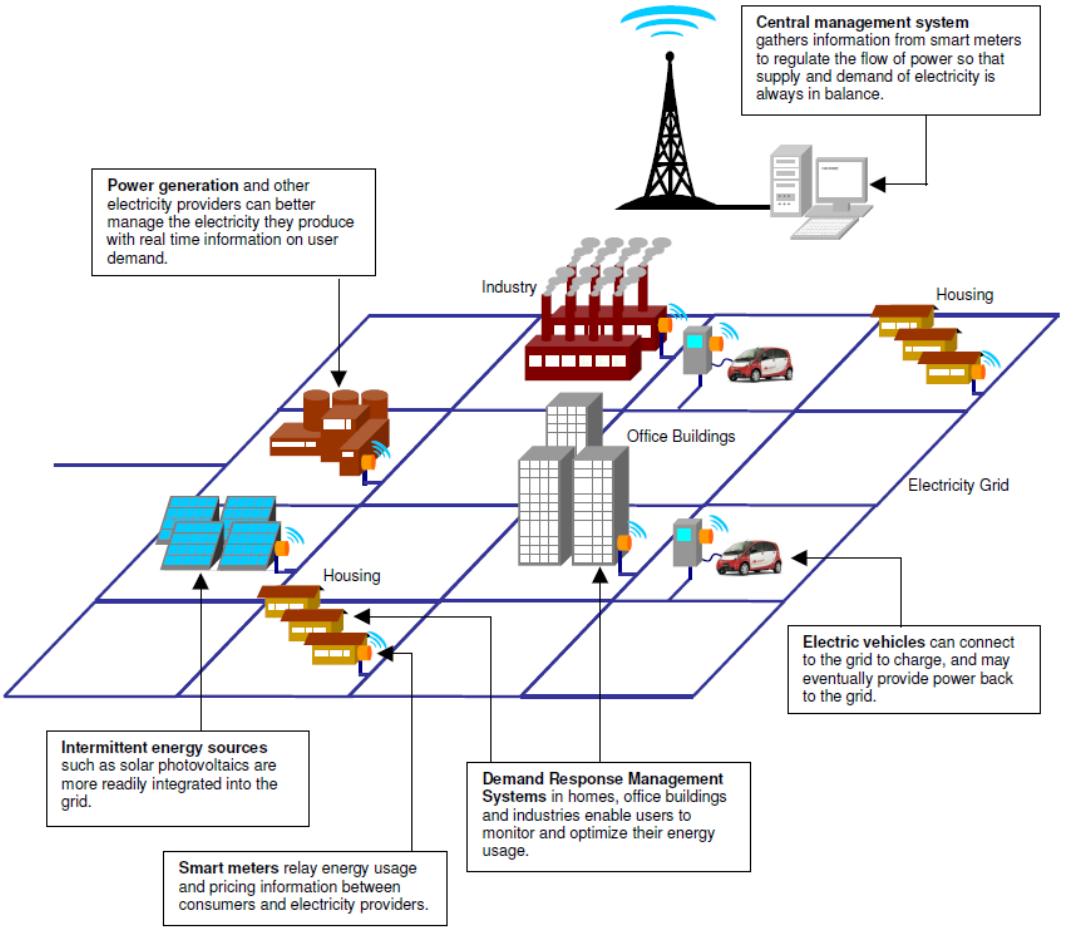
管理システムを家庭やオフィスに接続し、利用者が電気料金の変動に応じて電力消費量を監視･管理することができるようにする。利用者は電力消費量を最適化できる一方、電力会社は負荷変動を予測できコスト削減が可能となる。

●複数の電力源からの供給電力管理

ビルや一般の住居などへの設置も進んでいる太陽光発電システムや、熱と電気を効率よく利用できるコージェネレーションシステムなど、従来の発電所以外からスマートグリッドへ供給された複数の電力源からの電力を制御するシステムの実証実験を行う。電気自動車の充電による影響や、電力使用のピーク時には電気自動車に蓄電された電気を送電する可能性についても検証する。シンガポールのインテリジェントント・エネルギーシステムの概念図を図表・付 1-18 に示す。

[115] シンガポール経済開発庁 2010 年 1 月 15 日付プレスリリースより。
http://www.edb.gov.sg/edb/sg/jp_jp/index/news/articles/09.html

図表・付 1-18　シンガポールの IES 概念図



出典：Cleantech Investor ホームページより[116]

実証試験でテストされるのは、①適切な通信手段の選択(光ファイバーか Wi-Fi 無線か)、②電力使用のインフォームドデシジョンを需要家が下せる各種のアプリケーション、③より効率的な発送配電システムの構築、④PV や小規模コジェネなどの「プラグ&プレイ」による系統への取り込み、⑤小売業者の販売する最適商品選択への小規模需要家への情報提供などが挙げられている。

2009 年に最初にパイロット地域に選ばれた「マリンパレード&ウェストコースト地域」の 400 戸以上の住居では、電力使用量が宅内に設置されたディスプレイにリアルタイムで示され、時間別電力料金と組み合わされて、2.4%～3.9%のピーク電力使用量の低下がみられた。この結果、時間別料金性のインセンティブによって顧客の最適消費が実証されたとしている。

上の実験結果に基づいて、IES はオフピーク時に低価格電力を提供し電力使用の効率化を

[116] http://www.ema.gov.sg/media/news_pdfs/1260266179IES%20Press%20Release%20_Final_%20web.pdf

進めようとしている。事前プログラムされた自動デバイスとスマートメータアプリケーションによって、オフピーク時の電力利用を増加させる計画である。

IES 実証実験の下で、他にも幾つかの試みが行われている。

①ラオウビン島のインテリジェント・マイクロ・グリッド

シンガポールの東北部に位置する観光地であるパラオウビン島では、在来のディーゼル発電に代わって、再生可能エネルギーを中心的に使用するマイクロ・グリッド実証実験を行っている。この島での実証実験の中心は再生可能エネルギーの「プラグ&プレイ」型導入である。

②域的スマートグリッド国際協力

アジア太平洋経済協力会議(APEC) 参加国の一部は、この地域間のスマートグリッド化の調査を行う組織の樹立に動いており、シンガポールはその一国である。

③ERI@N　太陽光のグリッドへの統合

2010 年 6 月シンガポールの国立ナンヤン工科大学は、エネルギーリサーチインスティテュートを次世代エネルギー研究の COE(Center of Excellence) として設立した。この研究所の研究領域は、燃料電池、風力と潮力、蓄電デバイス、太陽電池、マイクロ・グリッド、スマートエネルギーであり、次世代エネルギー研究所の中心施設となることが期待されている。すでに ERI@N は、オーストラリア工科大学(オーストラリア)、連邦ポリテクニークローザンヌ(スイス)、ロンドンインペリアルカレッジ(英国)、ノルウェイ科学技術大学(ノルウェイ)、ケンブリッジ大学(英国)、ミュンヘン工科大学(ドイツ) と協力関係にある[117]。

[117]下記ウェブ資料による。
http://www.cleantechinvestor.com/portal/smart-grid/5860-spotlight-on-singapore-smart-grid-city.html
http://www3.ntu.edu.sg/erian/about_us.htm

付録 1.4　技術動向・製品動向・標準化動向の概況

(1)技術・製品動向

4.2.2 項で述べたようにスマートメータは、電力計量部、開閉器部、通信部から構成される。スマートメータの開発にあたっては、コストダウンのため、一体化・2 チップ(計測用、通信用）1 ボード化が図られる方向にある。通信は無線が主であり、特に ZigBee を中心とする方向だが、PLC も対応していく方向である[118]。

欧米を例に開発における課題を以下に挙げる。

① インターオペラビリティ

- 様々な要素（機器）が、異なるメーカであっても、すべてつながる仕組みづくり
- 様々なサプライヤーがメータにアクセス可能となる仕組みづくり
- ソフト配信による設定変更「interchangability」（インターチェンジャビィリティー）

② トランス(日本のポールトランス）の高機能化(インテリジェント化)

トランスにコンセントレータ機能(データ回収、記憶）と計測機能(電圧、電流の測定など)、電圧のコントロール機能、ステータス、イベント発生の伝達機能を持たせる。

③ 通信

欧米では無線特に ZigBee が主体。標準化・規格化とともにスマートメータの一体化の方向。(ZigBee、GPRS、 WiMax)

④ MDMS、EMS

Metering Data Management System(計器データの一次処理)

Energy Management System

今後、スマートメータと HEMS の関係がどうなっていくのかということも考慮する必要がある。広義の AMI がどうなっていくのか、明確に見えてきていないのが現状である。

以下に、スマートメータを構成する各部の技術動向と課題を述べる。

■ 開閉器

メカニカルな接点が入っており、半導体は使えない。メカニカルに動いているため、過電流に対して弱いといった課題がある。メータの規格として 2500 アンペアがあり、それをクリアできるものが少なく、コストも高い。大容量をどうするかも課題である。海外でも 200 アンペアまではあるが、それ以上はない。技術的にクリアすることは難しい。メータの外につけてそれを制御する形になることも考えられる。

■ 計量部

技術的な問題は計量という面ではない。ガス、水道メータの場合は電池駆動なので、寿命の問題がある。

[118] 東光東芝メーターシステムズ㈱資料及びヒアリングによる。

■ 通信

PLC はデータの取得率という意味では良いが、トランスをいかに越えるのか(トランス超え）が課題。特に日本や米国は柱状トランスに対してついている家、数が欧州に対して少ないので、コスト高になる。

米国などはメータの中に通信を入れている。日本は外に出そうとしている。ユニット式などで対応。欧州はメータとは別に取り外し通信ユニットがある。コストを安くするには、ワンボードにチップを載せてやる方が部材的には安いが、一概には言えない。

地域毎に無線と PLC が分かれることになれば、物量として変わってしまうのでコストに影響すると考えられる

■ その他

海外ではメータをいかに安くするかという観点から、入力と出力を隣同士並べているが、日本の場合、安全性を重視しており、入力と出力は左右に分かれている。すでにそういう配線になっているので、新しい配線にしようとしても作業できない。

〔欧米のスマートメータ製品例〕

● Enel 社(イタリア)

イタリア最大手の電力会社。2001 年からスマートメータの設置を始め 2005 年末まで 2700 万台を設置済。

ENEL ではインテリジェントメータ、PLC、GSM の組合せにより、遠隔自動エネルギーマネジメントを実現している。Enel 社のスマートメータを図表・付 1-19 に示す。

図表・付 1-19　ENEL のメータ

出典：Enel Sustainability Today

● PG&E 社(アメリカ)

カリフォルニア州北部及び中部地域で電気・ガスの供給を行っている。スマートメータの設置では米国で先行しており、2012 年までに 930 万台のスマートメータ導入計画を有する。展開されているのは GE 及び Landis + Gyr のスマートメータである(図・付 1-20 に Landis + Gyr 社のスマートメーターを示す)。しかし、顧客から高い電気料金やメータが発する電磁波による健康被害、さらに個人情報の漏えいに対する懸念などの不満が高まり、地元市議会が同年 8 月、スマートメータの設置を 1 年間禁止する条例を発令する事態に発展した。スマートメータ普及の観点から推移が注目されている[119]。

図表・付 1-20　PG&E のメータ

出典：Landis + Gyr 社 Product Specification Sheet より

[119] Wall Street Journal 日本語版(2010 年 9 月 10 日付)

(2)標準化の動向

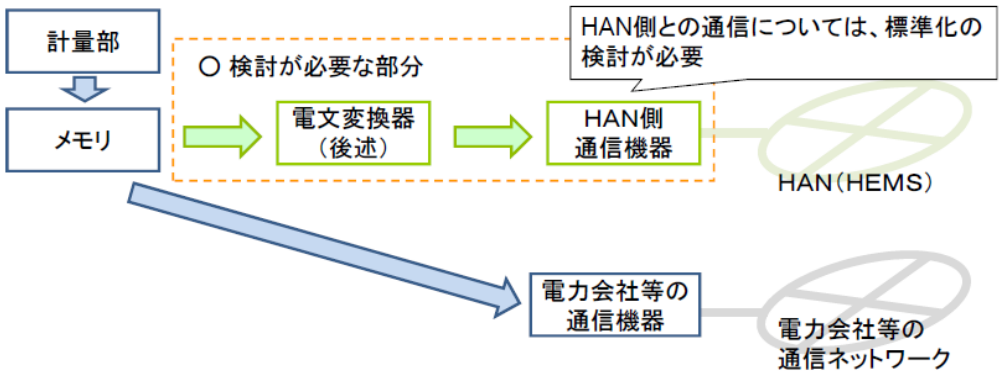
① セキュリティ

スマートグリッドのセキュリティについては、2010 年 9 月に NIST から「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(Guidelines for Smart Grid Cyber Security)」が発表された[120]。ガイドラインには、ハイレベルな安全性要件、リスク評価の枠組み、個人住宅におけるプライバシ問題の評価、付加情報が含まれている。また、HEMS のセキュリティに関しては、我が国では NIST がベースになるものと考えられるが、そこから何を選択するかについてはまだ検討段階にあり、明確な方向性は定まっていない。

② プロトコル

HEMS コントローラと個々の家電(スマート家電)間の通信や HEMS コントローラとスマートメータ間の通信プロトコルについては、欧米では ZigBee や Wi-Fi などの無線通信規格が取り上げられているが[121]、我が国においては何を使用するかまだ定まっておらず、機器への組み込みの容易性やアプリケーション、セキュリティなどの観点から実証実験等を通じて検討が行われているところである。(図表・付 1-21)

図表・付 1-21 HEMS 等の通信における標準化



出典：第 6 回スマートメーター制度検討会資料

スマートメーター制度検討会においては、通信方式については、有線方式と無線方式の 2 つが考えられ、技術的にはいずれも対応可能としながらも、有線方式については施工性や保守性(HEMS のゲートウェイが屋内に設置される場合)、無線方式については通信障害が発生しうるといった課題があると指摘している。(図表・付 1-22)

[120] http://www.nist.gov/public_affairs/releases/nist-finalizes-initial-set-of-smart-grid-cyber-security-guidelines.cfm
[121] スマートメーター制度検討会第 2 回会合配布資料参照。

図表・付 1-22　HAN（HEMS）側における代表的な通信方式

	Zigbee	Z-Wave	WiFi	Bluetooth	PLC	Ethernet
接続形態	無線	無線 (900MHz帯)	無線	無線	有線	有線
最大伝送速度	250 kbps (2.4GHz)	40 kbps	11-300 Mbps	1Mbps (Class1)	14-200 Mbps	10M -1Gbps
伝送距離	10 to 75m (通常 30m)	30m(見通し)	100m(屋内)	100m (Class 1)	300m	100m
標準化	IEEE 802.15.4	Z-Wave Alliance	IEEE 802.11	IEEE 802.15.1	IEEE 1901	IEEE 802.3
普及率	広く普及	広く普及	非常に高い	広く普及	広く普及 (日本は屋内通信のみ)	非常に高い
特徴	低コスト、低消費電力、長い電池寿命	家電の使用(ISM帯:2.4GHz)による影響無し	最も普及している高速無線方式。ノートPC等多くの機器に標準搭載	情報機器間の通信に広く利用されている	既存の家庭内電力線を利用可能。	高速通信で広く普及。通信の最も標準的なインタフェース

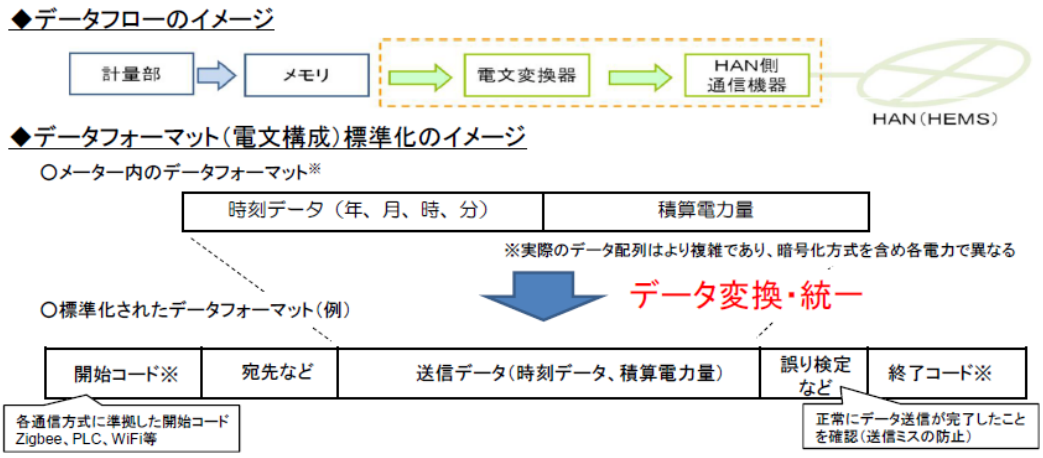
（出典：第2回スマートメーター制度検討会資料）

出典：第 2 回スマートメーター制度検討会資料

③　データフォーマット

取り扱う情報のデータフォーマット等に関しても標準化が求められる。スマートメーター制度検討会では、「現在の電子式メータにおけるデータフォーマット（電文構成）については、各社それぞれの取組により、セキュリティ対策も含め異なっており、標準化のみならず統一させることもコストや調整に要する時間を考慮すると容易ではないといえる。」としつつ、「ただし、HEMS 側における汎用性・利便性の確保のためには、HEMS への通信時には統一的なものに変換されることが望ましいのではないか。」としている。（図表・付 1-23）

図表・付 1-23　データフォーマットの標準化



出典：第 6 回スマートメーター制度検討会資料

図表・付2　制御システムセキュリティへの各国の取組み状況 ～4つの視点から～

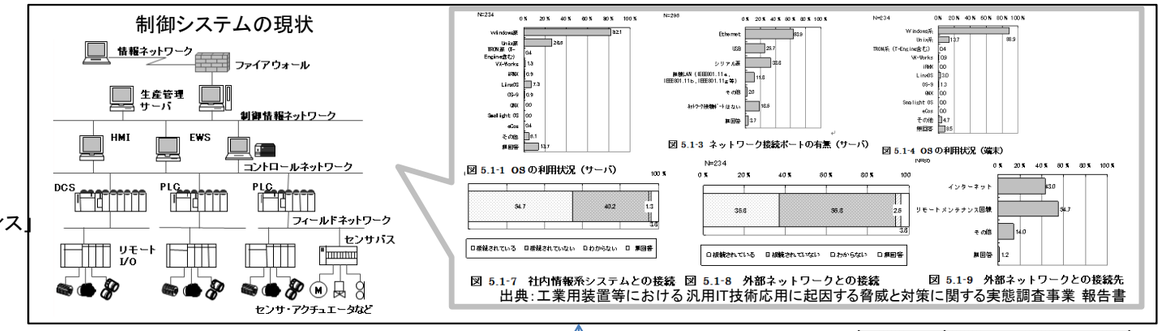


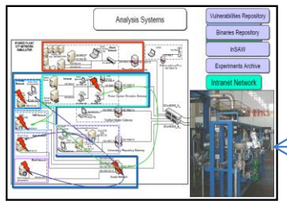
図 5.1-1 OSの利用状況（サーバ）　図 5.1-3 ネットワーク接続ポートの有無（サーバ）　図 5.1-4 OSの利用状況（端末）

図 5.1-7　社内情報系システムとの接続　図 5.1-8　外部ネットワークとの接続　図 5.1-9　外部ネットワークとの接続先

出典：工業用装置等における汎用IT技術応用に起因する脅威と対策に関する実態調査事業 報告書

NICC/TNOの「上水道分野用のSCADAセキュリティグッド・プラクティス」

IPSCのSCADAテストベッド



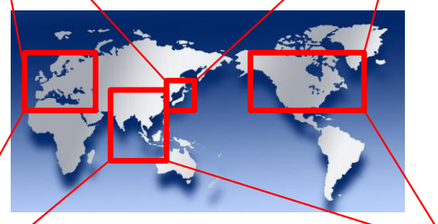
TNOのデータベース

Table 1: Categorisation of number of CI disruption events (number of events).

CI Sector	Cascade initiating	Cascade resulting	Independent	Total	Sample size
Education	0	3	1	4	4
Energy	146	76	388	609	590
Financial Services	1	26	33	60	60
Food	0	4	3	8	8
Government	2	40	26	68	67
Health	1	16	22	39	39
Industry	5	15	7	27	27
Internet	15	51	95	161	160
Postal Services	1	0	0	1	1
Telecom	69	125	114	308	295
Transport	19	128	276	423	422
Water	9	18	51	78	76
Total	268	501	1017	1786	1749

施策	欧州
ガイド・ツール	・推奨されるプラクティス集を公開（英国CPNI、オランダNICC/TNO水セクター向け） ・セキュリティ基準を策定（ドイツBSI standard 100-1 ～4） ・自己評価ツールを配布（英国CPNIのSSAT） ・情報共有の仕組みを整備（欧州のE-SCSIE、英国CPNIのSCSIE、スウェーデンSEMAのFIDI-SC）
評価・検証	・ヨーロピアンテストベッド取組みの一部としてIPSCではSCADAテストベッドを開設しセキュリティ検証を実施
データベース	・CPNIが制御システムセキュリティプログラムのひとつであるSCSIEを運営しており、インフラ運用者間での脆弱性情報共有カンファレンスを定期的に実施 ・制御機器ベンダーが脆弱性関連情報をユーザグループに直接通知、対策し、ユーザグループ内での解決を図る ・TNOがインシデント情報のデータベースを 構築
認証	・TUViTが複数の基準を顧客要件により組み合わせ、制御システムの監査・認証を実施

施策	日本
ガイド・ツール	・「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定に当たっての指針」（2007年6月 情報セキュリティ政策会議）などに基づき分野ごとに安全基準を設定 ・独自のツール類は少ない
評価・検証	・電力中央研究所で制御システムセキュリティの評価・検証を 行っているが、事業者または制御機器ベンダー内で共通的に利用可 能なセキュリティテスト環境は 見つからない
データベース	・JPCERT/CCが制御システムの脆弱性関連情報の収集、公開を実施。但し件数は少ない ・IPAが脆弱性対策情報DB(JVN iPedia)を運用
認証	・現状で特段の取組みは無い



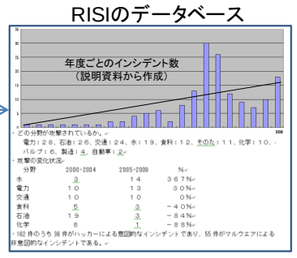
施策	アジア
ガイド・ツール	・情報セキュリティに関する安全基準を設けている国もあるが、国際的な標準に準拠するシステムや機器ベンダー企業の活動に委ねている。 ・独自のツール類を持つ国は少ない
評価・検証	・評価・検証の機能を果たす組織を持ったり、小規模の特化されたテストベッドを有する国もあるが、多くは独自の評価・検証を持たない。
データベース	・脆弱性データベースを保有している 国もあるが、各国のCERTが脆弱性情報の収集・公開を行っている。
認証	・国際的な標準IEC62443(ISA-99とIEC/TC65/WG10の組合)等に基づく認証を期待し、検討準備している 国が多い。独自の認証の制定と実施を 行うかについては方向が明確ではない。

施策	北米
ガイド・ツール	・推奨されるプラクティス集を公開（DHS/CSSP） ・セキュリティ基準を策定中（NISTのSP800-82およびISAのISA99, 100、NERCのCIP002～008） ・自己評価ツールを配布（DHS/CSSPのCS2SATおよびその後継のCSET） ・情報共有の仕組みを整備（2008年までPCSF、2009年よりCSJWG（HSINサービス開始））
評価・検証	・DOEがSCADAテストベッドを開設しセキュリティ技術の開発、検証を実施（INLのNSTBで検証実施）
データベース	・US-CERTが制御システムの脆弱性関連情報のデータベースを 持つが15～20件と少数 ・RISIが制御システムのセキュリティ事象データベースを運用 ・制御機器ベンダーが脆弱性関連情報をユーザグループに 直接通知、対策し、ユーザグループ 内での解決を図る
認証	・製品認証機関（米国MuDynamics社、カナダWurldtech社）による認証製品を 利用することで、一定のセキュリティレベルが担保されていることを確認、保証可能（ISCIでの検証サービス）

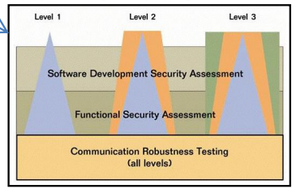
HSIN（Homeland Security Information Network）：制御システム関係者での情報共有ポータル

INLのNSTB

RISIのデータベース



ISCIの組込みデバイスセキュリティ保証（EDSA）の規格



お問い合わせ先

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

独立行政法人 情報処理推進機構セキュリティセンター

URL：http://www.ipa.go.jp/security/

〒１１３－６５９１ 東京都文京区本駒込２丁目２８番地８号

（文京グリーンコートセンターオフィス）

本報告書は以下のURLからダウンロード可能です。

URL： http://www.ipa.go.jp/security/fy22/reports/ics_sec/index.html