北米におけるスマートグリッド・セキュリティの取組

伊藤 聡*, 山中 晋爾、駒野 雄一 (株式会社 東芝 研究開発センター)

Security Efforts for Smart Grid in North America

Satoshi Ito, Shinji Yamanaka、Yuichi Komano (TOSHIBA Corporation R&D Center)

はじめに

近年「スマートグリッド」という言葉が一般に広く認識されるようになってきた。スマートグリッドとは発電から送電・配電にいたる電力系統や制御機器を情報ネットワーク化することであり、電力需給を監視・最適化を可能とする次世代送電網として期待されている。

一方、このような社会インフラ機器の情報ネットワーク化は新たなサイバー攻撃等の情報セキュリティ上のリスクをもたらすことになる。例えば、系統制御システムの乗っ取り、虚偽の制御情報による系統混乱、DDos(Distributed Denial of Service)攻撃によるサービス妨害・停止といった攻撃はライフラインの維持にとって重大な事態を招く可能性がある。

また、スマートメータを介した需要家の電力使用量等の個人情報の流出によるプライバシ侵害の懸念も大きな問題として指摘されている。本稿ではスマートグリッドにおける情報セキュリティの課題、米国の取組の概要、その取組の１つであるプライバシ保護につて概説する。

１章 スマートグリッドの情報セキュリティ課題

1.1 海外インシデント事例

社会インフラシステムにおけるインシデント事例はその性格上、公表されにくい側面があるが、現実には少なからず発生している。以下に海外で発生した典型的な事例を示す。

①上下水道監視制御システムの不正操作（2000）[(1)]

Maroochy 市（オーストラリア）の上下水道監視制御システムに元契約作業員が無線リンクから侵入し、46 件にのぼる不正なリモート操作を行い、アラームの無効化、通信妨害、ポンプの起動停止によって 100 万リットル近くの未処理汚水が周辺に放流された。

②原発監視制御システムのウィルス感染（2003）[(2)]

米国 Davis Besse 原子力発電所の監視制御システムが大量の攻撃用パケットを撒き散らす「Slammer」と呼ばれるコンピュータ・ウィルスに感染。同発電所のセーフティシステムとプロセス用コンピュータが数時間アクセス不能の事態となった。

③スマートメータのセキュリティホール(2010)[(3)]

米国 InGuardians Inc の調査により、米国で普及を進めているスマートメータに深刻なセキュリティホールが発見されたと報告された。この報告では不正侵入によりメータ管理を横取りし、プログラムを変更することで他人の電力料金を変更する操作が可能であることが指摘された。

④監視制御（SCADA）システムを狙った STUXNET（2009～）

トロイの木馬型ウィルスで制御システムが使うデータベースへのアクセスと管理下にあるコントローラへの悪意のあるコードを書き込み可能。Windows の脆弱性を利用して USB メモリ、ネットワーク経由 、ファイル共有経由など複数の侵入経路を持ち、多数の感染例が報告されている。

1.2 情報セキュリティ上の特徴

システムの情報セキュリティを策定する場合、具体的なシステム構成に基づき、①保護資産の特定、②脅威の洗い出し、③リスク評価、④対策立案の手順で分析・検討というプロセスで実施するのが一般的である。しかし、スマートグリッドのような大規模システムでは網羅的な分析・対策策定が困難であり、大きな課題となっている。以下に。北米におけるスマートグリッドのセキュリティ検討上で考慮すべき特徴を示す。

①所有者／権限の異なる電力サブシステムが連携

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

②需要家サイドの情報を需給制御にフィードバック

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

③新しいサービス事業者と連携

第３者の事業者が提供する省エネサービス等との連携が期待されているが、まだビジネスプロセスが固まっていない

©2011 IEE Japan

状況で、データのアクセス管理が複雑となる。

④商用ネットワーク／無線ネットワークの利用

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

⑤リアルタイム性、信頼性、端末機器のリソース制約

電力系統の監視制御はリアルタイム性・信頼性が要求されるためベストエフォートでは許されない処理が多い。さらに電力系統の末端にあるエネルギ機器では耐熱性、コストの面から CPU 性能、メモリサイズなどの計算機リソースに制約がある。

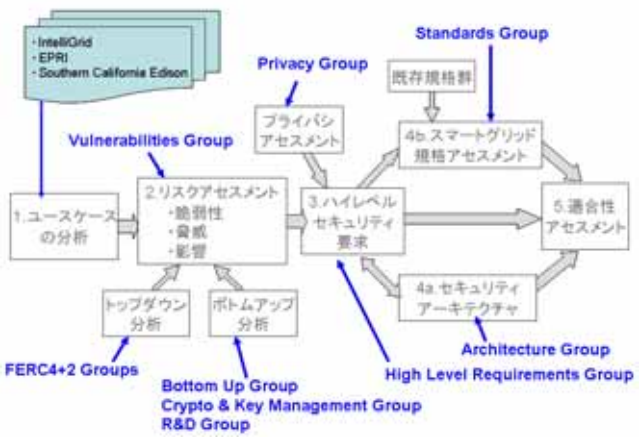
２章 米国 NIST の取組

2.1 NIST SGIP CSWG の取組

米国では NIST（National Institute of Standards and Technology）を中心としてスマートグリッド関連機器の Interoperability 確保の検討を行っており、2009 年４月から活動が本格化している。情報セキュリティについては CSCTG（Cyber Security Coordination Task Group）が設置され、検討方針と要求事項の作成を開始、2009 年９月には NIST IR 7628 Draft Ver1.0 が発行された。

2009 年秋からは第２フェーズとして、関連業界の代表で構成される NIST SGIP(Smart Grid Interoperability Panel)が設置され、CSCTG は 2010 年１月に SGIP 傘下の CSWG(Cyber Security Working Group)として活動を継続している。

CSWG の主要な目的の１つは、スマートグリッドに必要な情報セキュリティ要件を明らかにし、既存の規格や技術とのギャップを抽出することにある。CSWG は現在、関連分野の専門家が 400 名以上参画し、オープンな議論とその結果をガイドラインとして文書化する活動を進めている。図１に CSWG のアプローチを表したプロセスフローを示す。実際には図１にある各作業項目をベースに９つのサブグループを設置し、それぞれの課題を検討している。



2.2 NIST IR 7628

2010 年 8 月に NIST IR 7628(Guidelines for Smart Grid Cyber Security)[(4)]が発行された。この文章の主な目的は、①スマートグリッドの情報セキュリティを扱う団体へのガイダンスの提供と②スマートグリッドに適合した情報セキュリティ要件の策定に利用された分析プロセスに関する背景情報の提供であり、表１に示す６つの分野に分けた詳細な分析を行っている。

表１スマートグリッドを構成する６分野

略称	分野名
AMI	Advanced Metering Infrastructure （高度計量インフラストラクチャ）
DGM	Distribution Grid Management （配電網管理 ※系統側の分散電源等を含む）
ES	Electric Storage （エネルギー貯蔵 ※需要家側の分散電源等を含む）
ET	Electric Transportation （電気自動車・交通）
HAN/BAN	Home Area Network/Business Area Network （ホームエリアネットワーク/ビジネスエリアネットワーク）
WASA	Wide Area Situational Awareness （広域状況把握）

現在 本文書は次の３部構成となっている。

Vol.1 ： Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements
Vol.2：Privacy and the Smart Grid
Vol.3：Supportive Analyses and References

Vol.1 ではスマートグリッドの全体をブロックダイアグラムで表現した Logical Reference Model をベースに 22 種類の論理的インターフェースを定義し、それぞれに対して、19 分類（計 192 項目）のセキュリティ要件の適用の必要性の有無が定義されている。同時にセキュリティの３要素である C.I.A（Confidentiality, Integrity, Availability）に関するランク付けと暗号技術と鍵管理の課題についてもこの分冊で触れている。

Vol.2 はプライバシ問題を取り扱っており、次章で詳述する。

Vol.3 は一連の補足的な分析結果や参考情報についてまとめられており、情報セキュリティ研究者にとっても有用な情報が提供されている。具体的には①脆弱性のクラス分類、②ボトムアップ分析、③研究開発テーマ、④関連規格のレビューの方針、⑤セキュリティ検討のキーとなるユースケースが掲載されている。

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

©2011 IEE Japan

３章 プライバシに関する課題

前章で述べたCSWGにおいてもプライバシは大きな課題として取り上げられており、NIST IR 7628 Vol.2 がこの課題にのみに割かれている。本章では、プライバシの問題について述べる。

3.1 メータデータのプライバシ

スマートグリッドにおける重要なプライバシ情報として、スマートメータや HEMS(Home Energy Management System)から収集される各家庭のユーザ情報（単位時間当たりの電力使用量等）がある。例えば、ユーザ情報に含まれる「電力利用状況」からは、家庭内のユーザの　生活行動パターンや家庭内設備（例：在宅の有無や電気自動車の所有など）をオンラインで推定することが可能である。(図２参照)

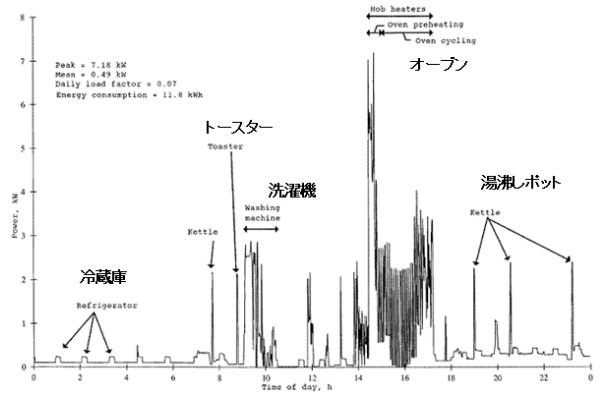


図２　電力利用状況グラフ（NIST IR 7628 Vol.2 より引用）

具体的には表２に示すようなプライバシに係わる情報が、スマートグリッドを介して得られる可能性がある。

表２：スマートグリッドで入手でき得る情報

（NIST IR 7628 Vol.2 より引用）

Name(氏名･法人名)	Party responsible for the account
Address(住所)	Location where service is being taken
Account Number (アカウント番号)	Unique identifier for the account
Meter reading (電力計測値)	kWh energy consumption recorded at 15–60 (or shorter) minute intervals during the current billing cycle
Current bill (使用料金)	Current amount due on the account
Billing history (支払い履歴)	Past meter reads and bills, including history of late payments/failure to pay, if any
Home area network (ホームネットワーク情報)	Networked in-home electrical appliances and devices
Lifestyle (ライフスタイル)	When the home is occupied and unoccupied, when occupants are awake and asleep, how much various appliances are used
Distributed resources (分散電源の状況)	The presence of on-site generation and/or storage devices, operational status, net supply to or consumption from the grid, usage patterns
Meter IP (IPアドレス)	The Internet Protocol address for the meter, if applicable
Service provider (サービスプロバイダ情報)	Identity of the party supplying this account (relevant only in retail access markets)

これらの情報は通常は電気料金の管理や省エネサービスのために用いられるものであるが、ユーザが望まない別の行為に悪用される可能性があり、以下のような事例が指摘されている。

①詐欺行為

データの操作により他の場所や他の電気自動車が消費したように見せかける。

②個人挙動パターンや利用機器の特定

スマートメータやホームオートメーションのデータから特定の機器を利用を追跡できる。また電気の利用データから、屋内のどこで、いつどんな機器が使われているかがわかる。これにより、家電メーカはこの情報を用いて製品の信頼性や保証期間などの設定に利用したり、ターゲット広告などのマーケティングに利用する。

③リアルタイムでのリモート監視

リアルタイムでモニタリングすることで、在宅の有無、住人の行動（歩いている、寝ている等）の情報を得る、

④スマートグリッド以外の商用目的での使用

個人のエネルギの消費履歴から導出されるライフスタイルの属性情報は広い分野の製品、サービスベンダ等に有用な情報となる。ベンダは属性情報を購入し、ターゲットを選定、商品を望まない人に対してもセールスを行う。

3.2 スマートグリッド プライバシ保護への取組。

わが国おいては「私生活をみだりに明かされない権利」との判例により事実上プライバシ権が認められているものであるが、近年、IT の観点で「自己に関する情報の提供時期、範囲、方式を自ら決定できる権利」と解釈して取り扱うケースが出てきている。いずれにしてもプライバシ侵害の有無は主観的な要素が大きいため、機械処理可能な明確な判定基準を設定するのが困難である。そのためスマートグリッドにおいても現在、技術開発とともに制度面の整備の必要性が指摘されている。制度面については,基本的には OECD(経済協力開発機構)が制定した８原則（①収集制限の原則、②データ内容の原則、③目的明確化の原則、④利用制限の原則、⑤安全保護の原則、⑥公開の原則、⑦個人参加の原則、⑧責任の原則）がベースとすることがコンセンサスとなっているが、米国の場合、州ごとのプライバシ標準と連邦政府による標準が存在しているためこれらとの調整も必要になると考えられる。

一般に個人情報を応用したサービスを行う場合、情報を集めておいて、サービス内容を充実させていく手法の適用が困難である。これは事前に使用目的を特定すること必要であり、さらに第三者へ新たに情報の提供を行うには本人の同意が必要であることから、それらの合意形成に多大なコストがかかるためである。今後、迅速、低コストで合意形成プロセスを確立することが制度設計の１つのポイントとなると考えられる。

©2011 IEE Japan

４章 プライバシ保護技術

前章でプライバシ保護に関する制度面の整備について述べたが、一方でこれらを実現するための IT 技術開発も重要である。プライバシ保護技術というとき、一般には仮想 ID 等用いた匿名技術や暗号化通信等の要素技術が思い浮かぶが、スマートグリッドでは全体システムを志向する場合が多い。そこで、ここではメータデータを中心的に扱う AMI（Advanced Metering Infrastructure）システムとしてのセキュリティを考える。図３に AMI システムの典型例を示す。AMI システムではスマートメータが計測したデータは AMI ネットワークを介して MDMS（Meter Data Management System）に蓄積される。MDMS は他のサーバやクライアントさらには他のサービスからの要求に応じて情報を提供する。

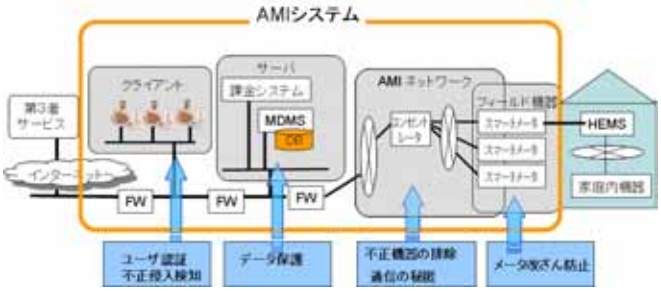


図３ AMI システムにおけるデータ保護

図３では AMI システムをセキュリティの観点で以下の４つの領域に分け、それぞれの領域でメータデータを保護に最低限必要な対策を示している、

- **フィールド機器**：スマートメータではメータの改ざんを防ぐために、ハードウェア/ソフトウェアの耐タンパ化が必要となる。特にスマートメータは HEMS とのインターフェースとなり得るため、細心の注意が求められる。
- **AMI ネットワーク**：無線メッシュ型通信を含めた様々な構成が想定されるため、機器認証による不正機器の排除と盗聴を防ぐための通信の秘匿化が必要となる。
- **サーバ**：MDMS では多数のユーザのデータを扱うため、強固な保護の仕組みが必要であり、外部からの不正アクセスはもとより内部不正者からの対策も必要となる。
- **クライアント**：内部ユーザのみを許可するユーザ認証とともに、マルウェアや外部からの不正侵入の防止を徹底する必要がある。

AMI システム全体として抜けのないように上記各領域のセキュリティ対策を全てに施すことがポイントとなる。また、各機器へのアクセス等のログを記録することはインシデントが発生した場合の原因把握・改善を図る上で重要であるとともに、抑制力としても有効である。

おわりに、

本稿ではスマートグリッドに関するセキュリティの取組について、プライバシ保護を中心に解説した。プライバシについては制度面、技術面の両面からのアプローチが必要であるが、これらは全てシステムの開発者、運用者の倫理に負うところが大であり、組織としてのセキュリティ管理の実践が今後ますます求められると考えられる。

文　献

(1)http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_briefing.pdf

(2) http://www.securityfocus.com/news/6767

(3)http://www.sfexaminer.com/economy/ap-exclusive-smart-meters-plagued-with-serious-security-holes-that-threaten-power-grid-89279997

(4)http://csrc.nist.gov/publications/PubsNISTIRs.html

©2011 IEE Japan