スマートグリッドに必要なセキュリティ対策
―安全・便利な送電網の構築に向けて―

昨今、再生可能エネルギーの導入促進、電力の有効活用のニーズを背景にスマートグリッド（次世代送電網）が注目されているが、スマートグリッドはネットワークを利用した通信を行うため、情報セキュリティ対策が欠かせない。本稿では、欧米のスマートグリッドにおけるセキュリティ対策を紹介するとともに、日本で必要となる対策について提言する。

スマートグリッドの目的

スマートグリッドは、送電網に情報通信技術を組み込むことによって、効率的な電力の供給および制御を実現する仕組みのことである。簡略化して次世代送電網と呼ばれることも多い。

スマートグリッドを構築する目的には国によって違いがある。日本では、CO_2排出削減のほか原子力発電の代替としても注目される太陽光発電など再生可能エネルギーに対応することが目的の１つである。政府は2020年度までに太陽光発電を2,800万kWにすることを目標にしているが、太陽光発電は電力供給や電力品質の不安定化が想定される。そのため経済産業省では2010年より、NRIセキュアテクノロジーズも参加する「次世代送配電系統最適制御技術実証事業」や「次世代型双方向通信出力制御実証事業」などにより対応を検討している。

一方、米国では老朽化した既存の送配電網の更新や、自動検針、電力使用開始・停止の遠隔操作などを目的としている。欧州の場合は、米国と同様の目的に加え、省エネおよびエネルギー有効活用の観点から、家庭での電力使用量の可視化や家電製品の遠隔制御などが主な目的になっている。

スマートグリッドのセキュリティリスク

従来、電力網のような制御システムは独自仕様の製品で構成され、隔離されたネットワーク上に構築されているため、外部からの攻撃に対しては安全であるといわれてきた。しかし、近年、制御システムにおけるセキュリティ事件は世界的に増加している（表１参照）。その理由として、システムが独自仕様から汎用的な仕様に置き換わったことや、隔離されたネットワークでの運用から、他のネットワークと接続された形態へと移行したことが挙げられる。

スマートグリッドも、汎用的なITの活用や電力会社（系統）と家庭間での相互接続が必須であり、不正アクセスや盗聴などのセキュリティリスクが高まる。

例えば、遠隔制御を逆手に取って、制御情報が流れる通信ネットワークが盗聴され、制御情報が改ざんされて大規模停電が起こされる恐れがある。また、電力使用量の可視化のためにネットワークを通じて収集・蓄積される個人情報が、盗聴や不正侵入によって盗ま

NRIセキュアテクノロジーズ
セキュリティコンサルティング部
主任セキュリティコンサルタント
上田直哉（うえだなおや）

専門は情報セキュリティ全般に関するコンサルティング

NRIセキュアテクノロジーズ
テクニカルコンサルティング部
副主任セキュリティコンサルタント
野口大輔（のぐちだいすけ）

専門はセキュリティ診断、制御システムセキュリティ

表1　制御システムにおけるセキュリティ事件の事例

事故の内容	発生国・発生年	原因	事故の経緯
鉄道の信号システムがウイルスに感染し運行が大幅に遅延	米国 2003年	アクセス制御の不備	感染原因は解明されていないが、2003年に流行したSobig（Sobig自体は現在流行しているZeusやSpyeyeのようにメール添付で感染する）が原因との報道がある。ネットワークの隔離が十分でなかったと推測され、オペレーターの端末が感染した結果、システムが感染したと考えられている。
原子力発電所の制御システムがワームに感染	米国 2003年	アクセス制御の不備	社内のPCがSlammer（Microsoft SQLServerの脆弱（ぜいじゃく）性を突いて感染を広げるワーム）に感染。社内OA系ネットワークと制御系の間のアクセス制御が甘く制御系も感染。
鉄道の切り替え機を不正に操作されあわや列車同士の接触事故という状況に	ポーランド 2008年	アクセス制御の不備	無線LANから侵入。鉄道の切り替え機までの間でアクセス制御がなかった。 14歳の少年によるいたずら目的の犯行。テレビリモコン型のコントローラを作り、切り替え機の制御を奪った。
国内制御系のウイルス被害	日本 2008年～	ウイルスが保存された端末・USBメモリーの持ち込み	自動車工場で、製造ラインに組み込まれているコンピュータ約50台がウイルスに感染。別の自動車工場では設備系コンピュータ約10台が感染。石油化学プラントではウイルス感染でシステムが完全に使えなくなり一時操業停止に追い込まれた。

れることも考えられる。

これらは、制御システムや情報システムが直面しているセキュリティリスクと同じである。重要インフラとして位置付けられる電力網は、サイバーテロの標的ともなり得ることから、スマートグリッドのセキュリティ対策は最重要課題である。そこで、スマートグリッドの取り組みが進んでいる欧米のセキュリティ対策を見ることによって、日本のスマートグリッドに適用すべきセキュリティ対策について考えてみたい。

米国のスマートグリッドセキュリティ

米国では、エネルギー省傘下の連邦エネルギー規制委員会（FERC）の監督下で、国立標準技術研究所（NIST）がスマートグリッドに関するセキュリティガイドラインを整備している。電力各社はこのガイドラインに基づいて必要なセキュリティ対策を実施することになる。

ここでは、筆者らが現地調査に訪れたカリフォルニア州におけるスマートグリッドのセキュリティ対策を紹介する。カリフォルニア州のスマートグリッドに実装されている主なセキュリティ対策は以下の６つである。

①検針ネットワークと制御ネットワークとの分離

スマートメーターとアクセスポイントを結ぶ検針ネットワーク（家庭で消費した電力量情報（検針情報）を送信）から制御ネットワ

ーク（送配電の制御情報を送信する）への不正アクセスを防ぐため、両ネットワークを分離している。

②スマートメーターと宅内環境の非接続

家庭内からの不正アクセスを防ぐため、スマートメーターと家庭内機器は接続されていない。

③プライベートネットワークの利用

検針ネットワーク、制御ネットワークともに、インターネットを代表とする公衆回線を使用していない。制御ネットワークには従来からの電力網を利用し、検針ネットワークは新たにスマートグリッドのために敷設したメッシュネットワーク（端末同士が通信することにより形成される網目状のネットワーク）を利用している。

④通信内容の暗号化

検針ネットワークでは、スマートメーターからアクセスポイントへの無線通信を盗聴される恐れがあるため、通信内容をすべて暗号化している。

⑤通信機器に認証を導入

スマートメーター、アクセスポイントともに信頼できる通信機器間での通信であることを担保するため、機器を認証する仕組みを導入している。認証方法には、データセンター側に設置する認証局サーバーを利用するPKI（公開鍵基盤）方式を採用している。

⑥ネットワークの冗長化

前述のように検針ネットワークはメッシュ形式で接続されており、これは冗長化を考慮したものでもある。このため、アクセスポイントの盗難や、送られるはずの情報が送られてこないなどの異常が発生した場合、その通信機器のみを切り離して別ルートで接続可能となっている。

以上のように、米国では「制御ネットワークに対する不正アクセス」を最大の脅威ととらえ、ネットワークへのセキュリティ対策を重点的に採用している。

欧州のスマートグリッドセキュリティ

欧州のスマートグリッドの特徴は、家庭での電力消費量の可視化を積極的に推進していることである。

筆者らは英国とフランスの２つのスマートグリッドプロジェクトを現地調査した。英国のLCNF（Low Carbon Networks Fund）が補助するUK Power Networks社の「Flexible Plug and Playプロジェクト」と、ERDF（フランス配電会社）が推進する「Linkyプロジェクト」（Linkyはスマートメーターの名称）である。

両プロジェクトはともにスマートメーター導入プロジェクトであり、プライバシー保護を重視したセキュリティ対策を取り入れている点が共通の特徴であった。電力使用量からその家庭のライフスタイルを推測できるため、個人の住所、氏名などの情報と一緒に管理する場合は、電力使用量はプライバシーデータ

として扱われている。

両プロジェクトではともに以下のセキュリティ対策が検討されていた。

①通信の暗号化と通信機器の認証

具体的なセキュリティ対策は米国と同様である。特に「Flexible Plug and Playプロジェクト」では米国カリフォルニア州の事例と全く同じネットワーク構成を採用していた。

②プライバシーデータの暗号化

スマートメーターなどの通信機器にはプライバシーデータが保存されているため、機器が盗難に遭ってデータが漏えいすることを想定して、通信機器上でデータをすべて暗号化している。

以上のように、欧州では「プライバシーデータの漏えい」を大きなリスクととらえ、制御ネットワークへの不正アクセス対策に加えて、データそのものに対するセキュリティ対策を実施している。

日本が取り組むべきセキュリティ対策

日本では、制御ネットワークと家庭間で相互に通信が行われることが想定され、家庭のプライバシーデータ（電力使用量）を活用することも検討されている。そのため、米国で重視されている「制御ネットワークに対する不正アクセス」と、欧州で重視されている「プライバシーデータの漏えい」の両方のリスクを考慮することが求められる。従って、日本では欧米で導入または検討されているセキュリティ対策を併せて取り込んでいく必要がある。

しかし、欧米と同様のセキュリティ対策をそのまま導入すれば安全というわけではない。現地調査の結果では、電力会社のオペレーターなど内部の権限者による不正や過失を防止する対策が不足していると思われた。また、スマートグリッドは情報通信技術が広く活用されることから、一般の情報システムと同様に、採用した製品に脆弱（ぜいじゃく）性が発見される可能性が高い。その場合の対応についても、欧米では十分に考慮されているとはいい難い。

このように、欧米のセキュリティ対策も現時点では不備がある。セキュリティ事故はまさにこのような小さな穴から発生してしまう。日本が安全なスマートグリッドを構築するためには、スマートグリッドを構成する機器と、機器間の通信の１つ１つについて、機能、取り扱う情報、データ保存の有無、利用技術などを明確化し、それぞれに対する個別のセキュリティリスクを洗い出した上で対策を検討していく必要がある。

昨今、情報システムのセキュリティ事故が後を絶たず、事後対応に追われる状況が続いている。事故を未然に防ぐためには、スマートグリッドの計画段階である今、セキュリティ確保に向けて官民が連携して知恵を絞ることが求められている。 ■