2012 年 9 月 11 日
独立行政法人情報処理推進機構（IPA）

ENISA Smart Grid Security – Recommendations for Europe and Member States
～【抜粋】推奨施策 6：スマートグリッド向けセキュリティ認証制度の確立～

本概要は、EU のサイバーセキュリティ担当機関 ENISA（European Network and Information Security Agency）が発行する調査報告書、“Smart Grid Security – Recommendations for Europe and Member States”の抄訳となります。内容の詳細につきましては、原文をご参照ください。（※本文中のリンク先は全て英文となります）
URL:http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations

1. ENISA 報告書 “Smart Grid Security – Recommendations for Europe and Member States”について

スマートグリッドは、ICT（Information Communication Technology）技術を活用し、電力の供給者と使用者の間で、需要と供給を管理し、経済的・効率的で質が高く、安全で持続的な電力の供給を可能にすることが期待されている。

しかし、コンピュータネットワークやシステム、インターネットといった ICT 技術への高い依存は、悪意あるサイバー攻撃により、壊滅的な打撃を被る可能性もある。ENISA では、スマートグリッドにおけるサイバーセキュリティの重要性を踏まえ、調査研究をはじめ、様々な活動を行っている。

その一環として、ENISA ではスマートグリッド関係者を集め、オープンディスカッションの場を設けた。目的は、スマートグリッドのサイバーセキュリティに関する懸念を洗い出し、各加盟国、欧州全体、および国際社会の取組みを認識し、支援することである。

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

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

これらの知見と推奨施策には、スマートグリッドを構成するシステム・機器のセキュリティ認証制度の必要性についても含まれており、CC(Common Criteria)、IEC 62443、ISA 62443 などのセキュリティ認証制度を基に、適切な評価・認証制度を確立することで、スマートグリッドに対するユーザの信頼性が向上し、スマートグリッド導入に促進に繋がるとしている。

以下に、「3 章：調査により得られた知見」と「4 章：推奨施策」より、関連個所を抜粋する。また、別紙に、報告書の内容一覧（目次）を添付する。

2. 報告書抜粋

（1）【3 章：調査より得られた主な知見】より抜粋

◆3.5 認証と国の認証機関の役割

◆3.5.1 国の認証機関の役割

多くの参加者が、**国指定の認証機関（NCAs：National Certification Authorities）が重要な役割を果たすと考えている。**例えば、以下のような役割が提案された：

1）スマートグリッドの重要な構成機器（特定の設定を含む）のセキュリティが十分に保たれていることを、事前に定めたプロテクション・プロファイルに従って確認し、保証する

2）スマートグリッド運用者の、組織的な面（プロセスや人に関わる面など）が、組織のセキュリティガバナンス戦略に沿っていることを証明する

◆3.5.2 欧州としてのセキュリティ評価制度と各国のセキュリティ評価制度

全 EU 加盟国を対象とする、欧州全体としてのセキュリティ評価制度を持つことについては、2 つの意見がある。1 つには、そうした取組みは欧州として行うべきであり、各国の認証機関によって個々に為されるべきではないと主張する専門家と、リスクと脅威レベルに伴う優先度は各国によって異なる可能性があるため、国家の安全保障問題として、各国が個別に取組むべきだと主張する専門家がいる。

◆3.5.3 機器ベースのセキュリティ認証制度の参考となる標準およびイニシアチブ

多くの専門家が CC を参考になる制度と見ている。その他には、FIPS 140 や PCI PTS（PCI PIN Transaction Security）の名が挙がった。また、**ISA 99 についても挙げられた**。英国の National Technical Authority for Information Assurance である英政府機関 CESG が、英国のスマートメータ機器の認定プロセスの設計を進めており、こちらも参考になると思われる。

◆3.5.4 スマートグリッドと CC

専門家によれば、CC は汎用的な認証制度である。従って、**スマートグリッド環境に適用する場合**、IC カード業界が JIL（joint interpretation library）を策定したのと同様に、**スマートグリッド独自のセキュリティ・プロファイルを含めるよう、拡張する必要がある**。

◆3.5.5 標準ベース、機器ベースの認証の代替案

ある専門家らによれば、**CC のような標準ベースの認証制度は、その煩雑さ故にメーカや SIer の負担となる可能性がある**。また、これから策定をしていく必要があり、長期間掛かる可能性もある。更に、スマートグリッド技術はこうした認証制度の導入にはまだ成熟度が足りないという意見もある。これらの理由から、

専門家からは、US National SCADA Test Bed Program で採用されているような、ホワイトボックステストやコード監査など、**もっと簡単にできる検証に基づく、より機動的な代替案の採用も提案された。この観点から、International Instrument Users‘ Association（WIB）のベンダ向け要件（現状 IEC 62443 と ISA 62443）も参考として挙げられた**。

◆3.5.6 スマートグリッド向けのセキュリティガバナンス認証

スマートグリッド向けのセキュリティガバナンス認証は、グリッドの運用者および必要関係者が統合的な ISMS を正しく導入できているか、チェックすべきである。そうした認証制度であれば、事業者やステークホルダーに対して、自身の取組みを測るためのベースライン（例：ベンチマークおよびセキュリティに対する姿勢の評価）を示すだけでなく、他事業者との比較も可能にする。**専門家からは、通信業界の事例のように、導入の参考にするには ISO 27000 シリーズが最適だという意見が挙がった。他に、ISA 99、NISTIR 7628 も挙がった。**

◆3.5.7 ガバナンス認証の代替案

専門家は、製品／機器の認証の場合と同様、**セキュリティ管理（ISO 27000 など）に最適という点だけに注視すべきでない**と主張する。併せて、脆弱性やセキュリティ上の問題がないか、**独立した配電事業者（DSO：Distribution System Operator）に対する第三者によるセキュリティ評価やペネトレーションテストを実施するよう、奨励すべき**である。

（2）【4 章：推奨施策】より抜粋

◆4.6 推奨施策 6：製品・組織向けセキュリティ認証制度の確立促進

◆4.6.1 概要

欧州委員会（EC）と加盟国（MS：Member States）の管轄機関は、**既存のイニシアチブ（CC、ISA 99、ISO 27000 など）を活用し、製品および組織のセキュリティ認証制度の確立を促進すること。**認証制度は、各加盟国のセキュリティおよびレジリエンシー要件に合致させるとともに、**欧州全体として監査の実施が可能な最低限の対策を定めていること。**また、認証を発行する権限を、国指定の認証機関（National Certification Authorities）に与えること。

◆4.6.2 目的

セキュリティレベルの向上とリスクの軽減により、認定・認証制度（accreditation & certification scheme）の導入が**スマートグリッドシステムおよびサービスに対するエンドユーザの信頼を向上させ、受け入れを加速してくれると期待される**。また、**認証を取得したサービスプロバイダはサービスの比較が容易になり、マ**

ーケティング戦略にも使えるようになる。製品の認証は、購入を検討している製品またはシステムのセキュリティレベルに関する情報をスマートグリッドの運用者やサービスプロバイダに提供し、特定のスマートグリッドに導入するのに十分なセキュリティが確保できているか、ライバル製品と比較してどうか、知ることを可能にする。同様に、**スマートグリッドのセキュリティガバナンスの認証では、グリッドの運用者および必要関係者が統合的な ISMS を正しく導入できているか、チェックすべきである。**そうした認証制度であれば、事業者やステークホルダーに対して、自身の取組みを測るためのベースライン（例：ベンチマークおよびセキュリティに対する姿勢の評価）を示すだけでなく、他事業者との比較も可能にする。

一方、今回の調査・分析において、**製品がセキュアかどうかを判定するためには、開発工程の評価とセキュリティ機能の検証が必要であることが明らかとなった。**前者は、設計のやり直しを避けるため、とりわけスマートグリッドのような産業環境といった**大規模ライフサイクルの場合はコストが高額になるため、効率性の観点から特に重要である**と考えられる。巧く確立された製品認証制度であれば、適切なセキュリティ評価要件を規定することで、両方の検証が行える。

本推奨施策では、**推奨施策 3 に示した標準を活用すべきである**（とりわけ、スマートグリッドシステムの技術的要件、および将来的なグリッドに携わる組織向けのセキュリティガバナンスガイドライン）。既に述べたように、**スマートグリッド向けの認証制度を確立するにあたっては、CC や ISO 27000 シリーズが最も名の挙がる標準である。しかし、どちらも直接スマートグリッドに適用することはできない。**CC は制御システムや他のスマートグリッド機器に特化したものではない。従って、制御システム環境に適用する場合には、IC カード業界が JIL（Joint Interpretation Library）を策定したように、スマートグリッド独自のセキュリティ要件に合うよう、拡張することが求められる。一方で、ISO 27000 シリーズを、通信業界による適用を参考に導入してはとの意見もある。

◆4.6.3 ステップ

- 機器や設定の再確認をリスクベースで行い、セキュリティ認証取得の対象とする機器を決定する
- スマートグリッド向けセキュリティ認証制度の検討にあたり、既存の標準やグッドプラクティスの適用の仕方について、過去の導入例（IC カード業界など）や事例（テストベッドなど）を分析する
- 製品セキュリティ認証制度、組織のセキュリティ認証制度を確立する
- 国指定の認証機関（NCAs：National Certification Authority）を、認証の発行機関として認定する
- 評価機関を認定する

以上

別紙:ENISA Smart Grid Security 内容一覧(目次)

※下線太字節が今回抜粋個所

Smart Grid Security - Recommendations for Europe and Member States