「スマートグリッドにおける電磁的セキュリティ特別調査専門委員会」
設立趣意書

１．背景・目的

地球温暖化や地下エネルギー資源の枯渇を防止する有力な方法として、太陽光発電システムや風力発電システム等のグリーン発電システムを配電網に接続する分散型電源の導入が国内外において積極的に進められている。スマートグリッドは、分散型電源による電力供給と消費者の電力需要を両面から効果的に制御し、電力の流れを最適化する送配電網であり、電力利用の効率性・快適性から国際的に注目されている。一方、スマートグリッドが社会基盤の 1 つとなる場合、スマートグリッドを構成する設備の故障・誤動作・性能低下等の不具合動作が及ぼす社会的リスクは極めて増大するため、近年、スマートグリッドに対するセキュリティ確保が重要な課題の１つとなっている。

スマートグリッドは、電力の供給と需要を記録管理するスマートメーターやそれらの情報を収集・管理するコンピュータや有線・無線通信機器等の設備またはシステムから構成される。これらの設備（センサ、コンピュータ、通信機器等）のセキュリティには、例えば、機器の不具合動作や機器が管理する情報の漏えい・改ざんがあり、これらを電磁現象で意図的に引き起こす「電磁現象を手段とするセキュリティ脅威」と「その対処」が、近年、先進各国のセキュリティ分野の研究で活発に行われている。

本「スマートグリッドにおける電磁的セキュリティ特別調査専門委員会」は、スマートグリッドに対する「電磁現象を手段とするセキュリティ脅威」と「その対処」に関する技術調査を実施し、スマートグリッドによる安心安全な電力利用社会基盤の構築に寄与することを設立の目的とする。

２．内外機関における調査活動

「スマートグリッド」に関しては、2010 年 1 月に NIST（米商務省標準技術研究所）が標準化に向けた枠組みを発表している。また、IEEE でも、2009 年 3 月にスマートグリッド関連システムの互換性の実現を目指す WG「P2030」を設立している。また、欧州では、2005 年に European Technology Platform Smart Grids (ETP Smart Grids)が設立され、Strategic Energy Technology Plan (SET Plan)を策定し、標準化のために、Joint Working Group on Smart Grids を 2010 年 5 月に設立している。さらに、これらの状勢と並行して、IEC（国際電気標準会議）でも、スマートグリッドに関する戦略グループ SG3 を 2008 年 11 月に設立し、IEC 版スマートグリッド標準化ロードマップ第 1 版を 2010 年 6 月に公開している。一方、国内では、スマートグリッドに関する組織として、経済産業省が次世代エネルギー・社会システム協議会を 2009 年 11 月に組織するとともに、次世代送配電システム制度検討会とスマートメーター制度検討会を 2010 年 5 月に設置している。また、NEDO（独立行政法人　新エネルギー・産業技術総合開発機構）も、企業・団体と経済産業省か

らなる官民協議会「スマートコミュニティ・アライアンス」を 2010 年 4 月に設立している。さらに、電気学会でも、「スマートグリッド特別研究グループ」を 2010 年 5 月に設置し、次世代エネルギーシステム構築の実現に向けて、進むべき方向性を探りつつ社会への情報発信を進めている。また、電気学会の電磁環境技術委員会の中に、「スマートグリッドと EMC 調査専門委員会」を 2011 年 4 月に設置し、スマートグリッドに関連する EMC 課題を検討して、2014 年 3 月に終了する予定である。

「情報セキュリティ」に関しては、情報・通信システム等のセキュリティ対策を強化する目的で，国際的基準である情報セキュリティマネジメントシステム(ISMS: Information Security Management System)が制定されており，日本においてもその適合性評価制度の運用が始まっている．ISMS では，物理的セキュリティとして，盗難・火事・水害等のほか，「電磁環境の管理に起因する脅威」への対応も要求している。この「電磁環境の管理に起因する脅威」には、機器からの電磁妨害波を用いた情報漏えい脅威と、意図的に機器に不具合動作を与える意図的電磁障害（I-EMI[1]: Intentional electromagnetic interference）脅威がある。具体的には、前者は、情報機器に対する TEMPEST[2] 的盗聴や暗号機器に対するサイドチャネル攻撃 [3]、後者は、機器のイミュニティ許容値を上回る高電力電磁環境(HPEM environments: High Power Electromagnetic environments)を意図的に生成する攻撃である。これらの脅威とその対処については、IEEE において 2003 年の「電磁両立性（EMC: electromagnetic compatibility）シンポジウム」以降、セッションとして取り上げられ、各種の研究が行われている。また、近年、ITU（国際電気通信連合)では、電磁環境に起因する情報漏えい脅威についてのガイドラインを発行しており、IEC（国際電気標準会議）および ITU（国際電気通信連合)では、HPEM（高電力電磁環境）に関するガイドラインの発行を行っている．さらに、電気学会でも、2007 年から 2010 年に「電磁波・情報セキュリティ技術調査専門委員会」を設立し、情報機器に対する電磁的セキュリティ脅威についての技術調査を実施し、情報セキュリティの観点から安心安全社会の構築に向けた情報発信を行っている。

備考：

1．I-EMI…機器の故障・誤動作・性能低下を目的として、高周波大電力電磁波を照射する攻撃をいう。兵器としては「e-bomb」などが存在する。

2．TEMPEST…情報機器が意図せずに放出している微弱な電磁波を受信し、情報再現（盗聴）する脅威に対する対策をいう。なお、TEMPEST は米国のコードネームであり、省略語ではない。

3．サイドチャネル攻撃…暗号機器の動作状況を様々な物理的手段で観察することにより、機器内部の秘匿情報を取得する攻撃をいう。

３．調査項目

以上のような趨勢に鑑み、本特別調査専門委員会では、以下の項目に関して現状と課題、研究開発の動向を調査検討する。

（1）　スマートグリッドにおける電磁的セキュリティ脅威
　① 実態調査、②文献等調査、③脅威分析
（2）　スマートグリッドにおける電磁的セキュリティ要求
　① 実態調査、②規格調査
（3）　スマートグリッドにおける電磁的セキュリティ対処
　① 実態調査、②文献等調査、③対処方法

４．予想される効果

本調査検討によって、スマートグリッドにおける電磁的セキュリティ脅威が明確になり、それに対応するための基礎資料を提供できる。

５．調査期間

平成 26 年（2014 年）4 月～平成 29 年（2017 年）3 月（3 箇年）

６．活動予定

委員会：４回／年

幹事会：２回／年

７．活動報告

調査結果は、技術報告としてまとめる。または、全国大会シンポジウムや学会誌などで発表する。

以上