Japan
Smart Community Alliance

JSCA 国際標準化 WG　成果報告書　第２号

# JSCA

## スマートグリッド・セキュリティ研究会
## 成果報告書

JSCA 国際標準化 WG

2017

**【要旨】**

スマートグリッドにおける情報セキュリティの重要性の認識が高まりつつある。スマートグリッド・セキュリティ各主要規格は、網羅的かつ膨大な施策体系から成り立っており、まったく予備知識を持たない状態で、全体像を把握することは困難である。情報セキュリティ系技術者の支援を受け、予備知識を習得することにより、情報セキュリティに関する知見を有する電力系技術者数を増やしていくことが重要である。

このような背景から、主要セキュリティ規格に関して、電力系技術者が全体像を把握・理解することを目的とする。

さらには IEC の主要規格案に対してコメント作成し、日本提案に繋げることも目的とする。

目次

## 1. はじめに

「スマートグリッドのセキュリティの重要性が注目を集めており、国際標準化動向についても感心が高まっています。現状、複数の組織により複数の規格が並行して議論されているため、電力システムに従事する立場としては、それら複数の規格の関係性を理解した上で、総合的かつ抜けの無い対策を打てるようにしたいと考えています。

そのような背景から、

(i) スマートグリッドに関係するセキュリティ規格の全体俯瞰

(ii) 各規格の開発従事者による概要説明

(iii) 国内外電力会社の対応状況

等、前提知識に関する共通理解を得た上で、JSCA として今後の対応方法を議論する予定です。」

これは、2014 年 3 月 6 日に開催した「スマートグリッド情報セキュリティ国際規格に関するワークショップ」案内の冒頭の文章であり、ワークショップが開催された 2014 年の状況をよく表している。JSCA 国際標準化 WG では、このワークショップを発端として、2016 年 2 月 3 日までの約 2 年間、スマートグリッド情報セキュリティに関する勉強会・研究会を開催、活動を実施した。本レポートでは、その 2 年間の活動状況を報告する。

## 2. 活動スケジュール

スマートグリッド・セキュリティ勉強会は、2014 年 12 月 17 日に、JSCA 国際標準化 WG 配下の勉強会として発足し、第 1 回会合を開催。2015 年 7 月からは名称を研究会に改め、2016 年 2 月まで、約 2 年間活動を行った。

勉強会／研究会としての活動は、(1) 既存のセキュリティに関する規格の読解・理解、(2) スマートグリッド・セキュリティに関する規格、ISO/IEC 27019 へのコメント対応、の２種類の活動から成っている。(1)(2)の活動スケジュール、及び、本活動にとってマイルストーンとなる ISO/IEC 27019 検討スケジュールを下記に示す。

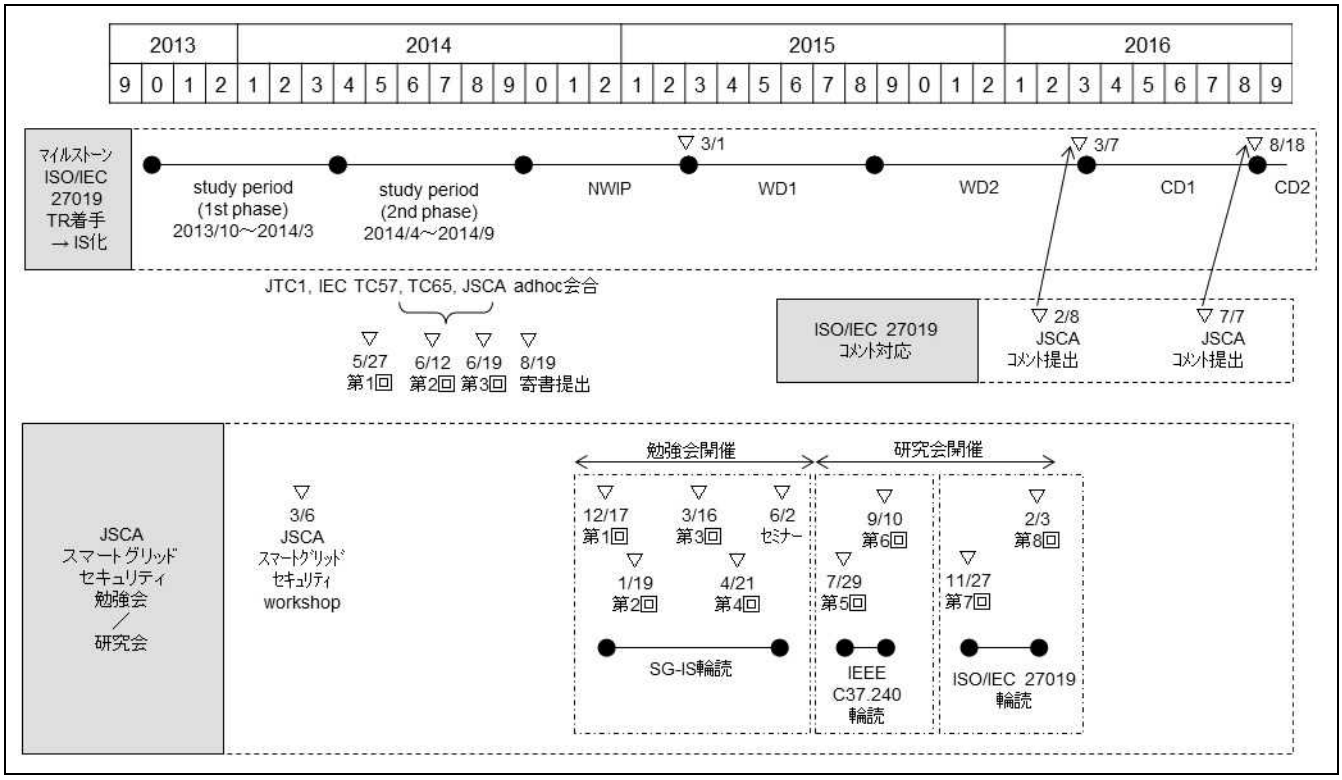


図 1　スマートグリッド・セキュリティ勉強会／研究会　活動実績

## 3. 活動前史

～　「スマートグリッド情報セキュリティ国際規格に関するワークショップ」

JSCA 国際標準化 WG の活動として、「スマートグリッドのセキュリティに関する検討を行いたい」、という声は活動の当初から上がっていた。2013 年夏頃の JSCA 国際標準化 WG 幹事社会議で、セキュリティに関する SWG を立ち上げることが正式決定し、活動内容的に、いきなり何か規格原案を提案するのではなく、まず、セキュリティ国際規格に関する状況把握から始める必要があったため、SWG ではなく、「勉強会」として立ち上げることとなった。

スマートグリッド・セキュリティに関する国際規格は、主要なものだけでも、

(1) JTC1/SC27/WG1 による、ISO/IEC 27000 シリーズ

(2) IEC TC57/WG15 による、IEC 62351 シリーズ

(3) IEC TC65/WG10 による、IEC 62443 シリーズ

がある。地域ごとの活動（規格化動向）としては、

欧州：CEN/CENELEC/ETSI SG-CG（Smart Grid Coordination Group）による報告書
Smart Grid Information Security (SGIS)

米国：NIST SGIP による NISTIR 7268
NERC による NERC CIP (Critical Infrastructure Protection)

等がある。更に国際規格を検討していく上で、国内・海外の電力会社によるセキュリティ対策の実施状況の把握も必要となる。

国内有識者（JTC1/SC27、IEC TC57、IEC TC65 の国内幹事及びセキュリティ規格関係エキスパート）と数回の打合せを行った結果、上記内容を前提情報として把握しておく必要がある、との結論に達した。また勉強会開催にあたり、何をすべきかのコンセンサスを得る必要があった。

以上のような背景から、初回会合はセミナー的なものではなく、参加型のワークショップとして開催することとし、2014 年 3 月 6 日、「スマートグリッド情報セキュリティ国際規格に関するワークショップ」を開催した（プログラムは次頁のとおり）。

表１　2014年3月6日開催、「スマートグリッド情報セキュリティ国際規格に関するワークショップ」プログラム

| No. | 時間 | 内容 | 発表者 |
|---|---|---|---|
| 1 | 15:00～15:20<br>（20分） | 開会の挨拶<br>本日の主旨の説明<br>スマートグリッドに関する規格の全体の関係について | 事務局（NEDO）<br>三島　久典（日立）<br>JSCA国際標準化WG幹事社委員 |
| 2 | 15:20～15:50<br>（30分） | 米国規格化の動向（NISTIR 7628, NERC CIP）<br>欧州規格化の動向（SG-CG） | 芹澤　善積（電中研）<br>IEC TC57/WG10, WG15国際委員 |
| 3 | 15:50～16:10<br>（20分） | IEC TC57/WG15動向<br>IEC 62351概要紹介 | 上林　達（東芝）<br>IEC TC57/WG15エキスパート |
| 4 | 16:10～16:30<br>（20分） | IEC TC65動向<br>IEC 62443概要紹介 | 武部　達明（横河電機）<br>IEC TC65/WG10国内幹事 |
| 5 | 16:30～16:40<br>（10分） | CSSC（技術研究組合制御システムセキュリティセンター）活動紹介 | 佐藤 明男（三菱総研）<br>CSSC事務局 |
| 6 | 16:40～17:00<br>（20分） | JTC1/SC27動向<br>ISO/IEC 27019概要紹介 | 山下　真（富士通）<br>ISO/IEC JTC1/SC27/WG1国内幹事 |
| 7 | 17:00～17:20<br>（20分） | 電力会社のセキュリティ対策状況（国内、海外） | 芹澤　善積（電中研）<br>IEC TC57/WG10, WG15国際委員 |
| 8 | 17:20～17:50<br>（30分） | オープンディスカッション<br>(1) 既存電力システムに対し何をすべきか？（15分）<br>(2) 標準化活動としてやるべきことは？（15分） | モデレータ<br>三島　久典（日立） |
| 9 | 17:50～18:00<br>（10分） | closing | 三島　久典（日立） |

ワークショップには44名が参加。プログラム最後のオープンディスカッションで、

・スマートグリッド・セキュリティに関する各主要規格は、網羅的なセキュリティ施策体系から成り立っており、情報セキュリティに関して予備知識を持たない電力系の技術者にとっては、全体像の把握が困難。しかし、実際に当該規格を必要とするのは電力系技術者であるため、電力系技術者が主要規格の全体像を把握・理解することが不可欠。

・情報セキュリティに関する知見を有する電力系技術者の絶対数を増やす必要あり。

等の意見があり、勉強会を設立、活動を開始することとなった。

## 4. スマートグリッド・セキュリティ勉強会／研究会　活動実績

図１．活動実績で示したとおり、スマートグリッド・セキュリティ勉強会／研究会の活動内容は、

(1) 既存セキュリティ規格の内容把握（規格文書読解）

・Smart Grid Information Security (SGIS)

・IEEE C37.240

・ISO/IEC 27019

(2) ISO/IEC 27019 コメント対応

の２項目から成る。それぞれの活動状況を説明する。

### 4.1 既存セキュリティ規格の内容把握

(1) Smart Grid Information Security (SGIS)

2014 年の時点で、JTC1, IEC のスマートグリッド・セキュリティに関する主要規格の内容については、各国内委員会メンバーが把握していた。また、地域活動によるセキュリティドキュメントについても、米国 NIST Cyber Security Group による NISTIR 7628 については、仮訳が存在していた。当時、CEN/CENELEC/ETSI の Smart Grid Coordination Group (SG-CG) が Smart Grid Reference Architecture を公表、その中で紹介されていた Smart Grid Architecture Model (SGAM) がスマートグリッド規格開発のための共通モデルとして着目され始めていた。同じく SG-CG が公表したセキュリティ規格に関するレポート、SG-CG/M490/H_ Smart Grid Information Security についても今後主要ドキュメントと目される可能性が高く、また 2014 年の時点では仮訳も存在しなかったため、勉強会で最初に内容検討を行うドキュメントとして採用することとした。当該ドキュメントは、2012 年 11 月に第１版が公表されていたが、勉強会の開始時点、2014 年 12 月にちょうど第２版が公表され、内容も大幅に拡充されていたため（頁数がほぼ倍となっていた)、勉強会では第２版を使用した。SGIS 第２版の目次は下記のとおりである。

表 2　SGIS 目次

7 European Set of Recommendation
8 Applied Information Security on Smart Grid Use Cases
9 Privacy Protection
10 SGIS Framework (Former SGIS Toolbox)
11 Conclusion
Annex A - Additional Information on DER control use case
Annex B - Overview on Privacy Enhanced Technologies for Smart Metering
Annex C - Overview on Document Status of investigated Standards
Annex D - Detailed Description of the SGIS Framework Steps
Annex E - References

＜概要＞

スマートグリッドのサイバーセキュリティ及びデータ保護・プライバシーについてのガイダンス。各章の内容（要約）は下記のとおり。

「5 SGIS Key Element」

３つの鍵となる要素は、(1) SGAM、(2) SGIS-SL（セキュリティレベル）、(3) selected use case、
であり、どのようにセキュリティレベルを設定し、どのように規格を適用するか、の一連の流れを説明している。レベルの設定の仕方（系統の範囲の広さで考える）が独特。

「6 Smart Grid Set of Security Standards」

既存規格の概略説明。

・requirement standard（what：要求項目）
・solution standard（how：施策）

に分けて、(1)概要, (2)規格審議の状況、(3)（スマートグリッドのセキュリティ規格として見る場合の）ギャップ、を分析。

「7 European Set of Recommendation」

ENISA と EC SGTF WG2 がまとめた、”list of security measures for Smart Grid” の紹介。Domains overview に対し、SGIS の検討結果として、Situational Awareness（状況認識）と Liability（責任）を追加。

「8 Applied Information Security on Smart Grid Use Cases」

４つのユースケース、

・Transmission Substation

・Distribution Control Room
・Consumer Demand Management
・Distributed Energy Resources (DER) Control
について、実際にセキュリティレベルを特定している点がユニーク。

「9 Privacy Protection」
かなりページを費やしており(21頁。全体の約４分の１の頁数)、本ドキュメントの目玉。スマートメーターとEV充電を例にとり、スマートメーターについては5カ国(仏、独、蘭、英、瑞典)の状況を紹介。
9.2 Impact Assessment では、セキュリティとプライバシーでは、そもそもの対象及びリスク評価が異なること(故に、セキュリティのリスク分析ツールは直接的には使えない)、9.3 Analysis of Emerging Privacy Technologies では様々なデータ保護技術が紹介されている。
GDPR (General Data Protection Regulation) は、下記に仮訳あり。
http://www.soumu.go.jp/main_content/000196316.pdf

「10 SGIS Framework (SGIS Toolbox)、Annex D 詳細」
リスク分析～セキュリティレベル設定～施策検討の一連の流れの説明。

「Annex B Privacy Enhanced Technologies for Smart Metering」
データ保護技術の紹介(9.3 の詳細)

以上の流れを理解した上で、11 Conclusion, 4 Executive Summary を読むと腑に落ちるようになっている。

内容読解は、これらを11チームで分担し、各チームが担当部分の内容を理解、説明(プレゼン形式は自由だが、日本語全訳ではなく内容解説とすること)、という形態で進めていった。
「今後、主要ドキュメントになると目され、かつ、当時日本語訳が存在しない」という理由で本ドキュメントを読解対象として選択したが、セキュリティ・プライバシーガイドラインとして、かなりよくできたドキュメントであり、特に、
(1) 「6 Smart Grid Set of Security Standards」で、セキュリティ規格として、
・requirement standard (what：要求項目)
・solution standard (how：施策)
の２種類があり、それぞれについて既存規格を網羅、概略説明が成されていること。
(2) 「9 Privacy Protection」で、プライバシーに関する詳細説明があること

等の特徴があり、勉強会の一番初めのドキュメントとしては非常に有用であった。

SGIS の読解終了の時点（2015 年 3 月）で、スマートグリッド・セキュリティ勉強会メンバーに対し活動継続の意向確認を行い、結果、活動は継続、2015 年度は「研究会」として活動することとなった。

(2) IEEE C37.240

セキュリティに関するほとんどの規格が、所謂、セキュリティ・マネジメント規格[1] であるのに対し、SGIS の「6　Smart Grid Set of Security Standards」で紹介されていた IEEE のドキュメント、

・IEEE C37.240: Cyber Security requirements for Substation Automation, Protection and Control Systems

・IEEE 1686: Intelligent Electronic Devices (IED) Cyber Security Capabilities

の 2 つは、実際に電力システムで必要となる要求項目を定義しているドキュメントとして紹介されていたため、電力事業者におけるセキュリティ施策検討の参考として、C37.240 を本ドキュメントの 2 番目の読解ドキュメントの対象とした。

IEEE C37.240 の目次は以下のとおりである。

表 3　IEEE C37.240 目次

| |
|---|
| 1. Overview |
| 2. Normative reference |
| 3. Acronyms and abbreviations |
| 4. Use of this standard |
| 5. Description of cybersecurity |
| 6. Cybersecurity requirements |

頁数は全体で 24 頁であり、内容的には 5. 6. がメインの記述となっている。

＜概要＞

システム稼動のために必要となるデータには、静的なものと動的なものがあり、

・静的／動的データの不正な改変

・データの不正参照

等によってシステム動作上の不具合が生じる。よって、

・いかにして不正が行われないようにするか？

・不正が行われたことをどのように検出するか？

[1] セキュリティ施策が網羅的に成されているかどうかの「管理（マネジメント)」を行うための規格。

の観点から、変電所内機器運用で必要となるICTシステムのセキュリティ要求項目を整理した内容となっている。

頁数が少ないため、「6. Cybersecurity requirements」を３チームに分けて、読解を行った。内容に関して各チームから、

・実用面については考える必要があるが、今回かなり深く読み込んだことにより、システムに組み入れる場合の検討が容易になると考えられる。
・今回内容を把握したことにより、今後、ドキュメント改訂の場合も容易に提案可能と考えられる。

等のコメントがあった。

(3) ISO/IEC 27019

図１　活動状況で示したとおり、ISO/IEC 27019の規格化が2013年から進行しており、その都度内容を確認してコメント対応を行っていたが、2015年後半のWD2対応で内容精査が必要となったため、あらためて、読解対象とした。

ISO/IEC 27019 Information Technology - Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industryの目次立ては以下のとおりである。

表４　ISO/IEC 27019 目次

| |
|---|
| 0 Introduction |
| 1 Scope |
| 2 Normative references |
| 3 Terms and definitions |
| 4 Energy utility specific ISMS requirements |
| 5 Information security policies |
| 6 Organization of information security |
| 7 Human resource security |
| 8 Asset management |
| 9 Access control |
| 10 Cryptography |
| 11 Physical and environmental security |
| 12 Operations security |
| 13 Communications security |
| 14 System acquisition, development and maintenance |
| 15 Supplier relationships |

16 Information security incident management
17 Information security aspects of business continuity management
18 Compliance
Annex A (Informative) Additional implementation guidance
Bibliographic references

＜概要＞

ISO/IEC 27019 は分野別規格[2] として開発されたものであり、タイトルの「based on ISO/IEC 27002」のとおり、ISO/IEC 27002 に対して、エネルギー事業特有の要件を追加したものとなっている。よって目次立ては、ISO/IEC 27002 を完全に踏襲しており、追加がある項目については、

「Control 6.1.6 from ISO/IEC 27002:2005 is augmented as follows:」

の後に、

ENR - 6.1.6 Identification of risks related to external parties

のように追加項目が記載されており、また、追加項目が無い場合は、

5 Security policy

No additional information specific to the energy utility domain.

のような記載となっている。よって、27019 単体では不十分であり、ISO/IEC 27002 も合わせて参照していく必要がある。

読解は 5 章以降を 1 チーム約 2 章ずつ、計 9 チームで行った。内容に関して各チームから、

・全体に過不足が無い感じだが、何点か重要な追加項目あり。例えば、
「危機、緊急時の要件を契約で定義する」旨の記述等。
・新技術（data diode 等）への言及があり、参考となった。

等のコメントがあった。

4.2 ISO/IEC 27019 対応

(1) ISO/IEC TR27019 study period 対応

ISO/IEC TR 27019[3] は、タイトルの「specific to the energy utility industry」が示すとおり、エネルギー業界向けプロセス制御システムに特化したセキュリティ管理ガイド

[2] 各事業分野個別のセキュリティ施策を記載した規格
[3] ISO/IEC TR 27019:2013, Information technology -- Security techniques -- Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

ラインであり、27000 シリーズの中で「分野別規格」と呼ばれるものの一つである。分野別規格としては他に、27011 電気通信業界向け（for telecommunications organizations)、TR27015 金融サービス向け（for financial services)、27017 クラウドサービス向け（for cloud services)等がある。

TR27019 は 2013 年 7 月に発行されたが、その直後ドイツから IS 化へのファストトラック提案があった。これは、IEC の適合性認定の参照ドキュメントとして、TR（技術報告書）ではなく、IS（国際規格）である必要があり、TR27019 をスマートグリッド分野でのセキュリティ管理参照ドキュメントとすることを意図したものである。ドイツからのファストトラック提案に対しては拙速ということで反対意見が多く、2013 年 10 月～2014 年 9 月の 1 年間の study period を設けて、TR27019 の精査を行い、その後改めて NWIP（新業務項目提案）とすることが決議された。

国内では study period の第 1 フェーズ（2013 年 10 月～2014 年 3 月）の間は、TR27019 の直接の検討母体である JTC1/SC27/WG1 と、技術的に関係の深い IEC TC57/WG15、IEC TC65/WG10 がリエゾンで検討を始めた。しかし、2014 年 3 月 6 日に開催したワークショップの準備で JTC1、IEC 関係者と議論を重ねた結果、組織的対応が必要、とのコンセンサスに至り、上記 3WG＋JSCA、経済産業省（オブザーバ）による ad hoc 会議を開催、study period 第 2 フェーズ（2014 年 4 月～9 月）に対応することとなった。

Ad hoc 会議は、2014 年 5 月 27 日，6 月 12 日，6 月 19 日 の 3 回開催され、study period 終了時の日本寄書（8 月 19 日）提出には、JSCA 国際標準化 WG もコメントを提出した。

(2) ISO/IEC 27019 コメント対応

Study period 終了時の投票では結局 IS が可決となった。これを受けて、2015 年 3 月から、ISO/IEC 27019 の WD1（working draft: 作業原案）が開始された（図 1 を参照)。Ad hoc 会議はそのまま体制を維持し、共同で 27019 コメント対応を行うこととなった。JSCA も、スマートグリッド･セキュリティ勉強会メンバー限定、かつ、WD2 及び CD1 フェーズ限定で、情報処理学会情報規格調査会より 27019 ドラフト参照の許諾を受け、WD2、CD1 のコメントに対応した。

WD2 フェーズ（2016 年 3 月 7 日コメント提出）では、10 項目を提出した（内訳：editorial 1 件、general 5 件、technical 4 件)。また、CD1 フェーズ（2016 年 8 月 18 日コメント提出）では、3 項目を提出した（editorial 3 件)。コメントはそれぞれ日本コメントとして採択、かつ、各ドラフトの comment resolution でも採択された。

2016 年 10 月 25 日の SC27/WG1 会合（国際）において、CD1 から DIS（国際規格案）に移行することが確認された。これ以降は ISO の管理下となるため、JSCA としては対応を終了した。

## 5. 活動成果

スマートグリッド勉強会／研究会の２年間の活動を通じて得られた成果は主に以下の 2 点である。

(i) スマートグリッド・セキュリティに関する主要規格の内容理解

スマートグリッド・セキュリティに関する主要規格、(a) SGIS、(b) IEEE C37.240、(c) ISO/IEC 27019、の内容を詳細に理解することができた。勉強会／研究会メンバーは電力系エンジニアであり、情報セキュリティに関するエンジニアは含まれていなかったが、今回の活動を通じて、スマートグリッド・セキュリティ規格に精通する技術者が 50 名強養成されたことは、国際競争力の強化につながったと考えられる。

(ii) 情報セキュリティ国際標準化活動との連携体制確立

ISO/IEC 27019 へのコメント対応を通じて､規格作成の実務作業に参画することができた。審議中ドラフトへのコメント提出が今回初となる勉強会／研究会メンバーも多く、限られた期間の中で期日までに内容を精査し、必要な対応を取る緊張感を体験できたことは、貴重と考えられる。また、情報セキュリティ国際標準化活動との連携体制を確立することができ、IEC の外の活動であっても提案動向を注視する必要あり、という認識が醸成されたことも、国際競争力という点では大きい。

## 6. まとめ　～　今後の方向性

### 6.1 スマートグリッド・セキュリティ研究会活動について

スマートグリッド・セキュリティ研究会の今後の活動については、

- 主要規格読解については、既に必要と思えるものを網羅しているため、これ以上は行わない。
- 27019 審議他への対応について、活動継続を希望する者は各自当該国内委員会に参画して活動を継続する。
- JISC スマートグリッド戦略専門委員会策定「18 の注力すべき領域」の一つとして「セキュリティ:情報セキュリティ(グリッド側)／EMS を含むユーザ側セキュリティ」があり、JSCA としても検討の場が必要となる可能性あり。

等の理由から、2016 年度の時点で、研究会としての体制そのものは維持、ただし、活動そのものは休止とした。

## 6.2 スマートグリッド・セキュリティ研究の方向性　～　電力システム概略モデルの確立

セキュリティ施策検討は脆弱性分析から始まるが、そのためには電力システムの概略モデルが必要となる。具体的内容としては、不正操作（外部／内部ネットワーク経由、機器への直接接続）の可能性を検討するための、ネットワーク接続図、及び各機器の概略図（操作用機器接続ポートの有無)、等をはじめとして、要するに ISO/IEC 27002 の管理領域として列挙されている項目の中で、技術的対策に該当するもの、

・通信セキュリティ
・運用セキュリティ
・物理的及び環境的セキュリティ

を分析するための、概略モデルが必要となる。

本件に関しては、既存電力システムに対する理解が不可欠であり、かつ、情報系ネットワークに関する理解も不可欠となる。特に、個別電力会社の現行システムではなく、複数電力会社に対して共通的に適用可能なものである必要があり、検討にあたっては、電力系・情報系双方のエンジニアの協力が不可欠となる。

## Annex 1.　研究会委員名簿

主査

| | |
|---|---|
| 株式会社日立製作所 | 三島　久典 |

メンバー

| | |
|---|---|
| 株式会社エナリス | 森　文高 |
| 沖電気工業株式会社 | 千村　保文 |
| 沖電気工業株式会社 | 猪熊　基博 |
| 沖電気工業株式会社 | 八百　健嗣 |
| 関西電力株式会社 | 村上　和宏 |
| 関西電力株式会社 | 和田　哲史 |
| 関西電力株式会社 | 久保田　泉 |
| 関西電力株式会社 | 中川　浩孝 |
| 関西電力株式会社 | 篠崎　隆志 |
| 関西電力株式会社 | 稲井　学 |
| 株式会社建設技術研究所 | 檜山　浩孝 |
| 株式会社建設技術研究所 | 山本　大樹 |
| 株式会社 GS ユアサ | 今泉　博文 |
| 清水建設株式会社 | 佐藤　和浩 |
| 清水建設株式会社 | 廣瀬　啓一 |
| 住友電気工業株式会社 | 久田　俊哉 |
| 中部電力株式会社 | 音川　淳 |
| 中部電力株式会社 | 野村　英生 |
| 千代田化工建設株式会社 | 白井　城太郎 |
| 千代田化工建設株式会社 | 沼田　諒平 |
| 千代田化工建設株式会社 | 伊藤　史剛 |
| 株式会社デンソー | 小田　享史 |
| 株式会社デンソー | 松本　隆 |
| 株式会社東芝 | 林　秀樹 |
| 株式会社東芝 | 神竹　孝至 |
| 株式会社東芝 | 松下　達之 |
| 日本アイ・ビー・エム株式会社 | 池田　一昭 |
| 日本アイ・ビー・エム株式会社 | 石橋　正章 |
| 日本アイ・ビー・エム株式会社 | 梅田　浩之 |
| 日本アイ・ビー・エム株式会社 | 伊藤　健太郎 |
| 日本アイ・ビー・エム株式会社 | 石原　寛紀 |
| パナソニック株式会社 | 荒牧　隆 |

| | |
|---|---|
| パナソニック株式会社 | 岡田　幸夫 |
| パナソニック株式会社 | 福田　尚弘 |
| パナソニック株式会社 | 中兼　晴香 |
| パナソニック株式会社 | 山本　雅一 |
| パナソニック株式会社 | 馬場　彩子 |
| 株式会社日立製作所 | 三島　久典 |
| 株式会社日立製作所 | 前田　浩 |
| 株式会社日立製作所 | 吉澤　孔明 |
| 株式会社日立製作所 | 長塚　明郎 |
| 富士通株式会社 | 山田　勇 |
| 三菱電機株式会社 | 小川　雅晴 |
| 三菱電機株式会社 | 小島　康弘 |
| 三菱電機株式会社 | 高篠　麻果 |
| 三菱電機株式会社 | 米田　健 |
| 三菱電機株式会社 | 小林　信博 |
| 三菱電機株式会社 | 村上　ユミコ |
| 三菱電機株式会社 | 山口　晃由 |
| 三菱電機株式会社 | 小倉　博行 |
| 三菱電機株式会社 | 平井　肇 |
| 横河電機株式会社 | 武部　達明 |
| 株式会社明電舎 | 挾間　洋平 |
| 株式会社明電舎 | 伊藤　憲一 |
| 株式会社明電舎 | 奥野　義道 |
| 株式会社明電舎 | 新井　裕 |

オブザーバー

| | |
|---|---|
| 経済産業省 | 高桑　淳、中川　幸成、土田　悦道、馬場　彩子 |
| JTC1/SC27/WG1（国内） | 山下　真 |
| 一般財団法人　電力中央研究所 | 芹澤　善積、嶋田　丈裕 |
| 国際標準化 WG 座長（同志社大学） | 合田　忠弘 |

事務局

| | |
|---|---|
| JSCA 事務局（NEDO　スマートコミュニティ部） | 桜井　孝史、澤　　貢、豊岡　友裕、佐藤　謙一 |

## Annex 2.　開催実績

2014年12月に「スマートグリッド･セキュリティ国際規格に関する勉強会」として設立。2015年4月に「スマートグリッド・セキュリティ研究会」として活動開始。

表5　2014年度活動実績

| 回、開催日 | 活動内容 |
|---|---|
| 第1回<br>2014年12月17日 | ・本勉強会の進め方について（目的、進め方）<br>・ISO/IEC 27000ファミリー規格と情報セキュリティについての講演・質疑 |
| 第2回<br>2015年1月19日 | ・IEC 62443についての講演・質疑<br>・ CEN/CENELEC/ETSI-SGIS Smart Grid Coordination Group, SG-CG/M490/H_ Smart Grid Information Security, 2014-12の輪読分担 |
| 第3回<br>2015年3月16日 | ・CEN/CENELEC/ETSI-SGISの輪読 |

表6　2015年度活動実績

| 回、開催日 | 活動内容 |
|---|---|
| 第4回<br>2015年4月21日 | ・CEN/CENELEC/ETSI-SGISの輪読 |
| セミナー<br>2015年6月2日 | ・JSCA会員向け「スマートグリッド・セキュリティ国際規格に関するセミナー」を開催<br>・SG-CG/M490/H_ Smart Grid Information Securityについて発表 |
| 第5回<br>2015年7月29日 | ・2015度の活動計画<br>・IEEE C37.240の概要説明及び輪読分担 |
| 第6回<br>2015年9月10日 | ・IEEE C37.240輪読 |
| 第7回<br>2015年11月27日 | ・ISO/IEC TR27019の概要説明及び輪読分担 |
| 第8回<br>2016年2月3日 | ・ISO/IEC 2ndWD 27019輪読<br>・今年度活動まとめ<br>・今後の活動について |

## Annex 3.　スマートグリッド・セキュリティ関連国際規格　審議概況

以下の３つの委員会が検討の中心となっている。

表７　スマートグリッド・セキュリティ関連国際規格　審議概況（2017 年時点）

| 委員会 | 主テーマ | 主要規格 | 現在の状況 | 主要メンバー |
|---|---|---|---|---|
| JTC1/SC27 | ・情報セキュリティ・マネジメント規格を中心とする。（情報システムセキュリティ）<br>・分野別マネジメント規格を検討中。（スマートグリッドも対象） | ISO/IEC 27000 シリーズ | ISO/IEC 27019 DIS 2017 後半に FDIS、2018 発行予定。 | ICT 系ベンダー<br>認証事業者 |
| IEC TC65/WG10 | ・工業用プロセス計測制御（制御システムセキュリティ）<br>・ISA99（国際計測制御学会）が規格原案を作成。<br>・国内では CSMS を推進中。 | IEC 62443 シリーズ | 27019 への対応（JTC1 とのリエゾン）<br>62443 リバイズ | 工業・産業計測機器系ベンダー |
| IEC TC57/WG15 | ・TC57 の範囲（61850 に代表される変電所自動化）のセキュリティ。 | IEC 62351 シリーズ | 27019 への対応（JTC1 とのリエゾン）<br>62351 のリバイズ | 電力系事業者、研究所、ベンダー |

## Annex 4.　セキュリティ入門

１．セキュリティ（security）とは何か？

(1) 定義：　対象・システムを脅威（主に人為的・作為的脅威）から守ること

注 1. この場合の脅威は、主に人為的脅威（作為的脅威）を対象とする。

表８　自然災害との違い

| | 自然災害 | 人為的脅威 |
|---|---|---|
| 発生頻度 | 偶発的確率分布に従う（ポアソン分布、正規分布） | 確率分布に従わない |
| 被害を受ける箇所 | 特に規則性無し | 特定箇所、ピンポイント |
| 被害の発生原因 | 外部から | 外部だけでなく、内部からも |

注 2. 信頼性（reliability）、安全性（safety）とは異なる（別の文脈で考える）。

(2) Security chain　←　セキュリティを検討する際の基本的な考え方

「鎖を引っ張ると、一番弱い部分が切れる」

⇒　システム全体を見渡したとき、一番弱い部分から破られる。

（これを「security chain」と呼ぶ）

したがって、「セキュリティ施策」とは、「何かを強くする」、というよりも、

「穴を埋める（脆弱性をつぶす）。

弱い部分に施策を施し、全体のレベルをある一定レベル以上にする」

という表現・考え方の方が適切。それ故、セキュリティレベルを示す表現は、

・あるレベルのセキュリティは実現できている（セキュリティレベルの設定）

・それ以上の脅威については、破られる可能性あり（万能ではない）

という言い方になる。

(3) セキュリティ検討の構成要素

インシデント v.s. 対応レベル

（発生する事象に対し、どのレベルまでの対応をしておくか）

A．インシデント管理

（日々発生する）様々な脅威事例とその対策に関する情報収集

・SOC（security operation center）

・IRT（incident response team）の相互連携

等の組織的対応。

B．対応レベル

対応レベル　＝　Σ（頻度×影響度×コスト）≧（実現したいセキュリティレベル）

・頻度：脅威の発生頻度

・影響度：不具合が生じた場合の被害の波及範囲、回復時間

・コスト：施策のコスト

２．ISO/IEC 27002 の管理領域（clause）

システム全体を網羅的に見る、ということが重要。網羅的＝もれなく見るのは難しい。

⇒　ISO/IEC 27002 で、「管理領域」として整理されている。（まずここが出発点）

表 9　ISO/IEC 27002 の 14 個の管理領域

| | |
|---|---|
| 5 | 情報セキュリティのための方針群（Information security policies） |
| 6 | 情報セキュリティのための組織（Organization of information security） |
| 7 | 人的資源のセキュリティ（Human resource security） |
| 8 | 資産の管理（Asset management） |
| 9 | アクセス制御（Access control） |
| 10 | 暗号（Cryptography） |

| |
|---|
| 11　物理的及び環境的セキュリティ（Physical and environmental security） |
| 12　運用セキュリティ（Operations security） |
| 13　通信セキュリティ（Communications security） |
| 14　システムの取得、開発及び保守（System acquisition, development and maintenance） |
| 15　供給者関係（Supplier relationships） |
| 16　情報セキュリティインシデント管理（Information security incident management） |
| 17　事業継続管理における情報セキュリティの側面<br>（Information security aspects of business continuity management） |
| 18　遵守（Compliance） |

これらを、管理的対策（組織的、人的）、技術的対策（技術的、物理的）で整理すると、下表のようになる（『情報セキュリティ教本　改訂版』、IPA、2009、を元に作成）。

表 10　管理的対策と技術的対策

| | | |
|---|---|---|
| 管理的対策 | 組織的 | 5　情報セキュリティのための方針群 |
| | | 6　情報セキュリティのための組織 |
| | | 8　資産の管理 |
| | | 14　システムの取得、開発及び保守 |
| | | 15　供給者関係 |
| | | 16　情報セキュリティインシデント管理 |
| | | 17　事業継続管理における情報セキュリティの側面 |
| | | 18　遵守 |
| | 人的 | 7　人的資源のセキュリティ |
| 技術的対策 | | 9　アクセス制御 |
| | | 10　暗号 |
| | | 11　物理的及び環境的セキュリティ |
| | | 12　運用セキュリティ |
| | | 13　通信セキュリティ |

3．［考察］ISO/IEC 27002「管理領域」を実際の電力システムに当てはめるとどうなるか（以下、主語は「電力事業者」。「電力事業者として○○はあるか？」の考察を行う。）

(1) 管理的対策・組織的

「5　情報セキュリティのための方針群」

・管理ポリシーと管理施策はあるか？（組織としての管理方針全般）

⇒

・「資産」：ものと情報の列挙・分類し、重要性のクラス分け・ランク付けを行い、
それぞれ、守る（どのように・どのレベルで）／守らない、等を整理する。
・これらセキュリティ資産の管理体制・管理ポリシー（要するに何をどうするかの方針）を決める。

(2) 管理的対策・人的： 人的要素に関する施策
・組織への入場・退場管理、セキュリティ教育
・アクセス権限（場所、装置、情報）の考え方の整理

(3) 技術的対策（← ほとんどの人が「セキュリティ」と聞いて連想する内容）
**※検討のためには電力システムの概略モデル（全体概要図）が必要。**
（所謂ネットワークセキュリティに関する項目（不正アクセス対応、ファイアウォール、ウイルス対策、等のキーワード以前に、根本的なキーワードを列挙する）

・ネットワーク：アクセス制御だけでなく、本人性認証（正当な者からのアクセスかどうか）が不可分。外部からのアクセスだけでなく、内部からのアクセスもチェック要。
・暗号：データ秘匿、デジタル署名（本人性、データの非改竄保証）
注：暗号化された状態でも改竄は可能（全文解読が必須ではない）
・ソフトウェア管理：ウィルス・ワクチン
パッチ管理（不具合対策モジュール、バージョンアップの正当性（コードサイニング））
・認証：機器の認証
正当な人からのアクセスかどうか、の他に、
正当な端末、正当な機器を使用してアクセスされたものかどうか？（不正接続対策）

注
・セキュリティホールは、対策した部分を破られることよりも、脆弱性対策を放置した不注意によるセキュリティホールが残っているケースがほとんど。よって、基本とされる脆弱性対策は、網羅的にきちんとやる必要あり。
・セキュリティ的に弱いのは、技術的対策ではなく、管理的対策（組織的・人的）の方。

４．「プライバシー」について

・AMI に関しては、電力供給機能維持・使用量計測以上に、「顧客データ利用」という観点からプライバシーの扱いを検討しておく必要がある。
・プライバシー対応の困難性： （日本では）法思想的なバックボーンが弱い。
欧・米では「個人の権利」との関係で、プライバシーの扱いが法思想的に確立している。

（かつ、欧と米では考え方が異なる。）

⇒　方針決めが難しい、ということを認識しておいて欲しい。

CEN/CENELEC/ETSI SGIS 及び NISTIR 7268 等ではプライバシーに関する記述あり。

５．電力系システム特有の検討項目（情報系システムとの相違）

(1) 物理的・物質的特性に基づく動作が発生するシステム

情報システムの場合の脅威は、基本的にデータに関する脅威であり、システムの不具合によって人体に直接脅威を及ぼすようなことはほとんど無い。しかし、電力システムの場合は人体への危険（感電、熱等）が伴う。

また、情報システムの場合、止めようと思った場合、すぐ止めることができるが、装置（メカ）はすぐには止まらない（動作上の危険)。

(2) 故障の発生頻度

情報システム・機器は、製品ライフサイクル及び減価償却の関係で、４年でほぼ入れ替えとなる。一方、電力システムは、使用年数が長い。

⇒　経年劣化の問題。及び、電力システム系機器と、制御システム（情報系システム）のライフサイクルの相違により、不整合が発生する。

## Annex 5. 参考文献


1) CEN-CENELEC-ETSI Smart Grid Coordination Group, SG-CG/M490/H_ Smart Grid Information Security, 2014/12

2) IEEE Power and Energy Society, IEEE Std C37.240™ - 2014 IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems, 2014/12/10

3) ISO/IEC TR27019 Information technology - Security techniques - Information Security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry, First edition, 2013/07/15

4) ISO/IEC 27002:2013(E) Information technology - Security techniques - Code of practice for information security controls, Second edition, 2013/10/01

5) 独立行政法人　情報処理推進機構、『情報セキュリティ教本　改訂版』、2009/03/27 改訂版第１刷発行

6) 株式会社　日本総合研究所、『平成 25 年度 次世代電力システムに関する電力保安調査報告書』、2014/02

7) スマートメーター制度検討会セキュリティ検討ワーキンググループ、『スマートメーター制度検討会セキュリティ検討ワーキンググループ　報告書』、2015/07

JSCA 国際標準化 WG　成果報告書　第2号
スマートグリッド・セキュリティ研究会成果報告書
2017 年 6 月 8 日（平成 29 年 6 月 8 日）発行

---

＜事務局＞
〒212-8554 神奈川県川崎市幸区大宮町 1310
ミューザ川崎セントラルタワー18F　NEDO 内
TEL：044-520-5269　FAX：044-520-5263
smart-japan@ml.nedo.go.jp

Japan
Smart Community Alliance

定価　1,000 円（税込）