2019年6月10日発行（毎月1回10日発行）第39巻第6号　通巻429号

ISSN 0910-0350

電気設備学会誌

The Journal of the Institute of Electrical Installation Engineers of Japan

特　　集：最先端の電気設備技術動向
支部だより/連載FAQ/賛助会員の声/本会記事

論文誌（新着）：https://www.jstage.jst.go.jp/browse/tieiej/list/-char/ja

学会ホームページ　https://www.ieiej.or.jp

Vol.39　2019

No. 6

一般社団法人　電気設備学会

Society5.0を支えるデータ共通基盤とエネルギーインフラ

Data Sharing Platform for Society 5.0 and Future Energy Infrastructure

江崎　浩*

キーワード：Society5.0，データ連携基盤，サイバーセキュリティ，オープン化，SDGs

1．概要

Society5.0は，「第5期科学技術基本計画」において，全ての社会・産業システムがデジタル化・ネットワーク化されている，第4次産業革命に続く社会インフラと定義されている。基本計画では，エネルギーインフラを含む重要な社会インフラの内外におけるサプライチェーンでのデータ共有と，その実現に必須となるサイバーセキュリティ対策が最重要課題として提起されており，2020年の東京オリンピック・パラリンピックの実施に向けてその対応を完了すべきと明記されている。本稿では，データセンターやエネルギーグリッドのような重要社会インフラにおいて，どのような前提条件を設定し，どのような考え方で具体策を企画・設計・実装・運用すれば，効率化・高機能化・高度化に関する持続的なイノベーションを実現することができるのかという課題に関する議論を行う。

2．デジタル化とネットワーク化を前提とした「超スマート社会」

2.1　ネットワークのネットワーク化

「科学技術イノベーション総合戦略2015」において「超スマート社会」の実現が提唱され，これに基づき2016年1月に閣議決定された「第5期科学技術基本計画」の中で，Society5.0の実現が提唱された。

Society5.0が目指す社会インフラは，全てのシステムが物理・サイバーの両面で相互接続され，各システムの所有・運営者だけではなく，システムの利用者(ユーザー)もデータの利用を可能とし，更にシステムの管理制御にも参画することが可能なシステム環境※1が提供されることで，デジタル技術を用いた社会・産業の持続可能な発展(SDGs：Sustainable Development Goals)を目指している。

※1　スマートメーターにおける宅内ユーザーが電力使用量のデータを取得可能にするためのB系は，宅内ユーザー(=消費者・ユーザー)が取得したデータを電力会社以外に利用可能とすることで，新しいデータの利用を可能とするために導入された。

例えば，エネルギーシステムにおけるSDGsは3E+S，すなわち，Energy Security，Economic Efficiency，Environment，＋Safetyを同時に実現することを意味する。これは，一つのインフラが四つの機能を同時に実現すると考えることもできるが，「スマートなインフラを構築することによって，一つの投資が四つの目的(=事業利益)によって償却(=Pay off)される」と捉えることもできる。“Multiple Pay Off”の考え方であり，利用の方法と目的を透明化(transparent)するというインターネット・バイ・デザイン(Internet-by-Design)の考え方である[1]。電力システムは，これまでウォータフォール型の発電側から消費側への一方向のシステムとなっていたが，今後は，再生可能エネルギーの発電と消費を組み合わせた(再生可能エネルギーやガスなどを含む)多様なエネルギー源の利用を可能とする前提「自家消費型システム」の積極的な導入を含めた双方向のネットワーク型電力システムへの改革を推進するための環境・制度の整備と拡充を目指すことになっている。

*東京大学大学院情報理工学系研究科教授

1963年1月生まれ，福岡県出身。1987年九州大学大学院修士課程修了。1987年～1998年㈱東芝。1998年～2000年東京大学大型計算機センター助教授，2000年～2005年東京大学大学院情報理工学系研究科准教授，2005年より現職(教授)。

2.2 データ連携に対する考え方

現実世界の全てのシステムの構造や動き・振舞いがデジタル世界で完全にコピー(Digital Twin)され，更に各システムがネットワーク化されることで，デジタル空間(サイバー空間)上に，全てのシステムが統合化可能なデジタルシステムが構築される。これまで，連携・協働することがなかったシステム間でのデジタルデータの共有が行われ，これまでにはできなかった連携・協働が可能となる。この新しい連携・協働によって，これまでにないインフラの効率化・高性能化・高機能化，更に新機能の創生・導入という「付加価値の創生」が実現される。このようなSociety5.0が目指す，「ビッグデータ」，「IoT(Internet of Things)」，更に「人工知能」が前提の社会・産業インフラの実現には，「Stove-and-Pipe」の構造が大きな障害となることが認識された。そこでSociety5.0では，これまでの「Stove-and-Pipe」と呼ばれる「垂直統合型のサイロ(silo)型のシステム・事業構造」を“De-Silo-ing”して，水平統合型若しくはマトリックス型の構造に移行(Migration)させることを目指している。内閣府では，水平統合型若しくはマトリックス型構造への移行による「データ連携基盤」の実現に向けた議論を行い，2018年4月にその結果を発表した(概要は3.3で記述)[2]。

経済産業省が2017年12月27日に設置した「産業サイバーセキュリティ研究会」では，Society5.0が目指す産業分野横断型の統合デジタル網を「バリュークリエーションネットワーク」と定義した。これまでの「サプライチェーン」は，現実世界の物理空間を意識した提供者側から消費者への一方向の一元的な構造を考えていた。しかし，Society5.0では，社会インフラが物理空間層，デジタル(サイバー)空間層，そしてこれを結びつける層の3層構造から構成され，更に各層内部での「モノとデータの」流れは一方向ではなく双方向のネットワークとなっており，この「モノとデータの」流れが価値(=バリュー，value)を創造すると定義した。

2.3 セキュリティに対する考え方[3]

セキュリティは，「誰かが解決してくれるもの」ではなく，「関係する全てのステークホルダ間による協調と協働」によって初めて実現されるものであるということを念頭に置く必要がある。しかし，次のような「危険で不適切な」状況が散見されているのが現実である。

「多くの企業や組織において，単に「閉じていれば安全」だと考え，対策を怠っている。」

これらは，「インターネットへの接続性の提供を前提とした」Society5.0が実現する社会にとって，結果的に非常に危険な考え方となってしまう。「閉じていれば安全」の考え方で構築・運用されるシステムは，他のシステムと相互接続するときのセキュリティリスクと運用者が「意図しない」状況での外部機器及び外部システムとの接続のリスクが非常に大きくなってしまい，結果的にシステムの統合コストの増加のみならず，統合化，すなわち他システムとのデータ連携を不可能としてしまい，新しいビジネス構造の構築の障害となってしまうだけではなく，サプライチェーンの効率化への大きな障害となってしまう。すなわち，外部システムやインターネットへの接続を前提としたサイバーセキュリティ対策(=“Security-by-Design”)を適用しておくことが，企業にとってのBCP(事業継続計画)と事業の成長戦略の観点からの「経営的なセキュリティ対策」となることを認識しなければならない。

産業分野ごとにサイバーセキュリティ対策の具体的施策の実現に向けた議論を行っている「産業サイバーセキュリティ研究会」(経済産業省)では，注力する産業分野として次の五つの産業分野が取り上げられている。

①ビル(エレベーター・エネルギー管理等)※2
②電力
③防衛産業
④自動車産業
⑤スマートホーム

本研究会での議論では，単独の事業者に閉じたサイバーセキュリティ対策だけではなく，「システム・施設の設計・構築・運用に関係する多数の事業者から構成されるサプライチェーン」に関するサイバーセキュリティ対策の実現が重要，かつ，大きな論点とされた。

※2 「ビル」には，社会産業を支える製品の製造を司る「工場(factory) 施設」を包含することが認識され，これがガイドラインでは明記されることなる。

3. オープンでスマートな施設の実現

3.1 注意が必要なビジネス慣習

ベンダロックインを維持するために，システムのオープン化を行わない方向に誘導する典型的なビジネス慣習の例を次に挙げる。

(1) オープン技術を用いることでご希望の要求を満足することができますが，当社の技術・製品によって同様のことが，より安いコストで実現可能です。

(注)ライフタイムコストでは，逆に大きなコスト負担となる場合が少なくない。

(2) ご希望の機能を提供することは「不可能」です。

(注)実は可能でも，不可能と主張される場合が少なくない。

(3) ご希望の要求を満足するための修正は不可能ではありませんが，

①このくらいの「大きな額の」，「システムの動作検証を含む」開発費用が発生しますので，この費用のご負担をお願いしなくてはなりません。

②修正に伴い，システムの維持管理に必要な保守費用がこのくらい「大きな額」増加することになります。

③納品したシステムとは，その構成が異なったものになってしまいますので，関連する部分に関する「契約時の動作保証」は不可能となります。

(4) セキュリティ面での問題が発生してしまいます。ご希望の修正を行った場合には，セキュア(安全な)稼働を保証することは不可能です。

(注)そもそも，セキュリティ対策が考えられていない場合が多い。

3.2 基本となる考え方※3

次に，3.1に示した現状の課題に対処するための方針を示す。

※3 電力9社による調達仕様の共通化(＋政府による実施の監視)によるコスト削減と，サイバーセキュリティ要件の必須化が制度化されることになった。

(1) システムの運用・保全・管理のオープン化

キャンパス施設の保全・運用などの企画を，キャンパス設備の所有者側(発注側)が自力で行うことが可能な環境を構築するのが理想である。そこで，実際の調達においては，企画の立案と実施管理は，自力若しくは「適切な」コンサル事業者を利用するなどして実現されるべきである。端的には，「丸投げ」の禁止である。

特に，運用管理の契約において，適切な措置を取れることを可能にするような条件を発注仕様書に明記することが重要である。3.1(3)で示したような課題が発生するリスクを軽減し，システム仕様のオープン化を実現するべき。

(2) ライフタイムコストの観点に立ったシステム仕様の検討と定義

導入時のコストだけではなく，ライフタイムコストの算出とその評価を考慮した提案システムの査定を行うために，ライフタイムコストの提示を調達の評価要件に盛り込むことが望ましい。この対応は，システムの「改修」，「追加」，「入替え」などの全ての発注の際に盛り込むべき。

(3) 調達のオープン化(透明性の確保)

受注内部でのブラックボックス化された契約関係がオープン化され，より健全な競争関係の構築と，提案システムの公正で公平な評価を可能にするべき。

(4) 技術のオープン化(透明性の確保)

将来の機能拡張・保全維持や他のシステムとの相互接続性の評価を行うとともに，その確保を行うために，各サブシステムが適用している技術仕様が発注側に提示・開示されることを提案の必須条件に盛り込むべき。

(5) セキュリティ機能の定義と明文化

安全対策，継続的・持続的運用(BCP：Business Continuity Plan)と保全に必要なセキュリティ対策の提示が「発注側に提示・開示される」ことを提案の必須条件に盛り込むべき。

(6) 既存システムと統合化

これまでは，独立に運用保全されてきたシステムを(透明に)オープン化及びネットワーク化・統合化することで，スマート化するという方向性を要求条件・仕様として明確化・明文化すべき。また，このようなシステムのネットワーク化・統合化は，既存の非オープンシステム若しくは既存のオープンシステムとの統合を実現させなければならないため，次のような項目への配慮が必要なことを明記すべきであると考える。

①相互接続に伴うシステムの動作保証

②サイバーセキュリティを含むセキュリティ

③相互接続に必要な費用

(7) IT化(クラウド・IoT)の積極的利用

オープン技術を用いた(相互接続性が担保された)センサデバイスの設置，移動若しくは除去が容易になってきている。センサを含むシステムが生成するデータの収集保存・処理・制御には，クラウド基盤の積極的な利用が推奨される。クラウド基盤では，ハードウエアの技術仕様に非依存な仮想的計算機環境となっており，経費支出の平滑化と削減が容易になるとともに，サイバーセキュリティの強化が低コストに実現される。

3.3 データ連携

2017年度から2018年度に「分野間データ連携基盤の整備に向けた方針」を提言する「データ連携基盤サブWG」での議論が行われた[2]。以下が，主な提言のポイントである。

（1） 十分なサイバーセキュリティ対策を前提とする

IoTで全てのヒトとモノがつながるSociety5.0では，サイバー攻撃の起点が増大するとともに，複雑につながるサプライチェーンを通じてサイバーリスクの範囲が拡大する。また，サイバー攻撃による影響がフィジカル空間まで達するリスクがある。データ流通市場の活性化が進み，大量のデータがグローバルサプライチェーンにおいて連携し，データの利用・再販が進むことを想定すると，ハイレベルなサイバーセキュリティ対策を備えた分野間データ連携基盤を構築することが重要である。

（2） 民間のデータセンターの活用

データセンターについては，その維持管理やサイバーセキュリティ対策に必要な人的リソースの継続的な確保が懸念される。また，最先端のICT技術の導入の観点からも，分野ごとのデータ連携基盤，分野間データ連携基盤は競争原理が働く民間企業が運営する最新のデータセンターを活用することが望ましい。

（3） 相互接続性の確保

既に，様々なシステムが稼働しているところであり，データフォーマット・語彙・メタデータ・APIなどを全面的に標準化ありきで進めるのではなく，相互接続性を優先し，変換機能など，技術的な解決手段によって，合理的に実現するべきである。民間等の独自のデータ提供サービス構築等を阻害することなく，できるところから連携を進めていることが重要である。また，ICT技術の進展に合わせて将来的な変更・アップグレードを前提とした考えの下で，柔軟なシステム構築を目指すべきである。

このような背景の下，内閣府・経済産業省・総務省・防衛省の連携による「クラウドサービスの安全性評価に関する検討会」が2018年10月に起動された。本検討会では，政府が調達するクラウド基盤の要求条件を決めることになる。さらに，この要求条件は，重要インフラに適用する方針となっている※4。

※4 重要インフラには電力システムも含まれており，産業別サイバーセキュリティの基準とクラウド基盤の要求基準の両方が電気設備の技術基準として引用されることになる。

なお，この要求条件の中には，クラウドサービスを提供するデータセンターの施設に関するサイバーセキュリティ要件が必要であること，更にその要件は，経済産業省で作成する「ビルSWG」が作成するガイドライン，すなわち，GUTP(東大グリーンICTプロジェクト)及びJDCC(日本データセンター協会)が共同で作成した「施設に関するサイバーセキュリティレフェレンスガイド」に基づいたものとなる。

4. おわりに

Society5.0が目指す全ての産業・システムのデジタル化とネットワーク化によるスマート化は，これまでの基本的には個別に独立して運用されてきた施設・システムの相互接続と連携・協働運用へと向かう。すなわち，既存の垂直統合型のビジネス構造の創造的破壊である。さらに，今後の設備システムは，オープン化とネットワーク化を前提として，設計・実装・運用・保全が実現されなければならず，その結果，適切で有効なサイバーセキュリティ対策が適用されることが必須条件となる。そのセキュリティ対策は，「まずは自助，次に共助，最後に公助」の原則の下，結果的にリスクを増大させることになる「過保護」な施策を「勇気をもって」避け，「経験や知見の共有」を実現し，全ての関係者(ステークホルダ)の間で連携・協調・協働しながら，全ての関係者の活動の活力を応援・支援し，向上するに資する挑戦を安心して実行することに貢献する体制が確立・実践されなければならない。

このような，適切なセキュリティ施策の確立と実践によって，これまで個別に運用されてきていたシステム間でのデータ連携と，システム統合の実現によるシステムの「継続的イノベーション」と「安定した事業継続性」が実現されることになる。

参 考 文 献

1) 江崎：「インターネット・バイ・デザイン」，東京大学出版会，2016年6月
2) 内閣府：「分野間データ連携基盤の整備に向けた方針案」，平成30年4月4日， https：//www8.cao.go.jp/cstp/tyousakai/datarenkei/3kai/siryo1.pdf
3) 江崎，中村他：「セキュリティに対する考え方」，2016年7月，http：//www.igcj.jp/meetings/concept-for-security.pdf