特　集　エネルギーに関するサイバーセキュリティの現状と対応

Society 5.0の実現に向けた セキュリティーのあり方とエネルギー分野での展望

Security for Society 5.0 Era and Its Development in Energy Industry

江　崎　　浩*
Horoshi Esaki

概要

Society 5.0は，「第5期科学技術基本計画」において，第4次産業革命に続く，すべての社会・産業システムがオンライン化・ネットワーク化した「超スマート社会」を実現するインフラとされている[1]．基本計画の中では，エネルギーシステムに代表される最重要インフラにおけるサイバーセキュリティー対策が最重要課題として提起されており，2020年に向けてその対応を完了するべきとされている．本論文では，具体的には，どのような前提条件において，どのような考え方で対策を企画・設計・実装・運用すれば，効率化や高機能化・高度化に関する持続的なイノベーションを実現するに資するセキュリティー対策が実行可能なのかを「インターネット・バイ・デザイン」[2]の考え方に立脚して議論する．

1．ネットワーク化を前提とした「超スマート社会」

1.1　ネットワークのネットワーク化

内閣府が作成した「科学技術イノベーション総合戦略2015」[3]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，ポスト第4次産業革命と位置付けられるSociety 5.0の実現が提唱された．

> 「自らの大きな変化を起こし大変革時代を先導していくことを目指し，非連続なイノベーションを生み出すための取組を進める．さらにICTの進化やネットワーク化といった大きな時代の潮流を取り込んだ『超スマート社会』を未来社会の姿として共有し，こうした社会において新しい価値やサービスが次々と創出され，人々に豊かさをもたらすための仕組みつくりを強化する」

Society5.0の実現には，すべての社会・産業システムが，オンライン化され，さらにこれらがネットワーク化（相互接続）され，連携・協調・協働することで，システム全体の効率化や高機能化・高度化だけではなく，非連続なイノベーションを創出するプラットフォームが実現されなければならない．まさに，ネットワーク化された各産業セグメントのシステムのネットワーク化であり，拡張・拡大されたあるいは進化したインターネット[注1)]と捉えることができよう．

1.2　システムのオープン化

メインフレーム型のコンピュータシステムには，周辺機器の接続に関する多様性と自由度を獲得・確保するために共通のオープン技術規格が制定され，特定のベンダーにロックインされない多様な周辺機器の導入・利用が実現された．この方向性は，計算機の基本ソフトウェアであるオペレーティングシステムとコンピュータの相互接続を実現する通信プロトコルが，オープン化・共通化されることで，さまざまなハードウェアを同じソフトウェアを用いて利用し，さらに，ネットワーク化することに成功した．その結果，ベンダー間での競争環境が形成されるとともに，新しいハードウェアやソフトウェアの導入障壁が激減されることになり，持続的な新機能の導入（すなわちイノベーティブな機器・サービスの実現）と，システムの拡張性，柔軟性，維持性，接続性に関するコスト，システムを構成する各モジュールのコストの継続的かつ大幅な削減が継続されることになった．さらに，システムを構成する各モジュールの入れ替え可能性の担保による機器提供の継続性という観点でのBCP（Business Continuation Plan）品質の向上にも貢献することになった．すなわち，(1) 持続的なイノベーション，(2) 継続的・効率的・低コスト[注2)]での運用，(3) システムの継続的運用，の3つの機能を同時に実現したと捉えることができる．このようなエコシステム（後に

*東京大学大学院情報理工学系研究科創造情報学専攻教授
〒113-8656 東京都文京区本郷7-3-1
E-mail：hiroshi@wide.ad.jp

注1）インターネットは，ネットワークのネットワーク（Network of Networks）と言われている．
注2）ライフタイムコストの削減は，(1) 初期導入，(2) 運用保守保全（機能のアップデート・追加・改修，モジュールの入れ替え，システムのネットワーク化），の両方で期待される．

詳述）の実現は，モジュール性を持ったオープンな技術仕様の利用を，機器およびシステムのユーザ（調達者・運用者）が，勇気を持って実践したことに起因していると捉えなければならない．システムのオープン化によって，ユーザ（Operator）とベンダー（Developer）が密接にシステムの技術仕様を定義するDev-Opsと呼ばれる状況に変革することで，より小さいコストで迅速かつ容易に，システムの高度化・高機能化・安定化（継続運用）を実現することが可能となる．

1.3 セキュリティーに対する考え方

セキュリティーは「誰かが解決してくれるもの」ではなく，「関係するすべてのステークホルダ間による協調・協働」[注3)]によって実現されるものであるということも念頭に置く必要がある．「まずは自助，次に共助，最後に公助」の考え方で，「共助」においては，機器・ソフトウェア提供者，サービス提供者，サービス利用者にまたがる垂直方向の関係者と，提供者間および利用者間での水平方向の関係者の両軸での「共助」を実現することが重要である．セキュリティーの重要性が認識されているからこそ，以下のような状況が散見されるのも現実である．

＊多くの企業や組織において，セキュリティーポリシーが厳しすぎ，創造的な活動が，結果的に阻害されてしまっている
＊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，対策を怠っている場合が少なくない

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」**社会（Society 5.0）にとって，結果的に，とても危険な考え方となってしまう．この傾向は，IoT（Internet of Things）のような，これからインターネットに新しく接続されることになる産業において顕著である．また，**「閉じていれば安全」**の考え方で構築されたシステムは，他のシステムと相互接続する時のセキュリティーリスクと運用者が意図しない状況[注4)]での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，統合化を不可能としてしまい，新しいビジネス構造の構築への障害となってしまう．その結果，ビジネスチャンスの喪失や市場競争力の低下につながってしまうリスクを持つことを認識しなければならない．**すなわち，システムを外部システムやインターネットとは接続しない運用形態においても，外部接続やインターネットへの接続を前提としたセキュリティー対策（“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セキュリティー対策となることを認識しなければならない．**

2．オープンでスマートなエネルギー施設の実現

2.1 Demand-Chain型マルチステークホルダ・エコ・システムへの進化

電力とエネルギーの自由化が進展しており，多様なエネルギーを多重的に利用することが可能なビジネス環境が確立されつつある．この環境においては，各事業所・施設におけるエネルギーの統合化・多重化，すなわち，エネルギーミックスの環境の構築が可能となり，長期・中期・短期のすべてのフェーズでのエネルギー系統の入れ替えが，エネルギーの供給側では可能となる．このような環境に，エネルギーの消費側，すなわち，設備・キャンパス[注5)]側が，利用するエネルギー系統の入れ替えが可能なシステムの実装が行われなければならない．このようなシステムが実装可能にできなければ，各系統に閉じたベンダーロックイン・プロバイダロックインの環境となってしまい，設計と実装の自由度が下がってしまうリスクを負うことになる[注6)]．

また，FIT（Feed-in Tariff；固定価格買取制度）は，単純な，エネルギーの買取りの段階から，VPP（Virtual Power Plant）の考え方が自立/自律型のエコ・エネルギーキャンパスへと進化する挑戦の段階に入りつつある．これまでの，送配電システムの統合化によるSupply-Chainの構築から，需要者を含むエコシステムへの進化である．いわゆる，DR（Demand Response）システムである．この需要者側のDemandに応じて，Supply-Chainの最適化を動的に行うシステムは，これまでの供給者主導によるPUSH型のSupply-Chainシステムから，需要者側主導によるPULL型のDemand-Chainシステムへの変革と捉えなければならない．すなわち，エネルギーの生産者・配送者・消費者のすべてのステークホルダが，オンライン化し，協働・協調動作を行わなければならない事業環境なのである．このような環境を想定した，エネルギー・エコ・システムにおけるセキュリティー対策が確立・実践されなければならない．

注3）「Collaborative Security by All Stakeholders」という概念が，ISOC（Internet Society, www.internetsociety.org）によって提唱されている．
注4）IT/ICT機器の小型化と携帯性向上に伴い，外部とは隔離したつもりになっているシステムにおいても，外部から持ち込まれたハードウェアやソフトウェアが，意図せずにあるいは意図的に接続されてしまうリスクが急激に増大している．
注5）キャンパスは，通常，大学のような学術的なキャンパスだけではなく，大きな工業団地やオフィス街も「キャンパス」と呼ぶ．
注6）ドイツにおいては，ガスと電力のプロバイダーによる実質的なロックイン現象が発生した．

2.2 注意が必要なビジネス慣習

多くの機器提供ベンダーは，顧客を他のベンダーに取られず，かつ継続的に顧客から利益を得るために独自技術を用いたベンダーロックインを実現させたい．以下に，機器提供ベンダーが，ベンダーロックインを維持・強化するために，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挙げる．

(1) オープン技術を用いることも，ご希望の要求は満足することができますが，弊社の技術・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セキュリティー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，セキュリティー対策が考えられていない場合が多い．

2.3 基本となる考え方

以下に，2.2に示した現状の課題に対処するための方針を示す．

(1) システムの運用・保全・管理のオープン化
施設の保全・運用などの企画を，設備の所有者側（発注側）で，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，自力もしくは「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．2.2（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である．

(2) ライフタイムコストの観点にた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」「入れ替え」などの，すべての発注の際に盛り込むべきである．

(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行うことが可能となる．

(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である．

(5) セキュリティー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ー対策の提示が，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である．

(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）オープン化およびネットワーク化・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・明文化すべきである．
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あるい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，以下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ーを含むセキュリティー（安全性）対策
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
IT技術・システムを用いた事業の実行・執行形態の変革が進行している．実際の物理システムでの実装を行う前に，コンピュータシステム（＝サイバー空間）において，精細なシミュレーションが行われ，実際の物理システムの詳細設計が完了したあとに，実際の実装が行われる形態である[注7)]．言わば，「サイバースペース・ファースト（Cyber Space First）」あるいは「ソフトウェア・ディファインド（Software Defined）」

でのシステム設計・実装である．建築・設備業界における「BIM First」あるいは「Computational Design」に相当する事業形態である．

さらに，ネットワークに接続され施設システムとの相互接続と相互連携が可能なオープン技術を用いた（相互接続性が担保された）センサーデバイスの設置，移動あるいは除去が容易になってきている．センサーを含むシステムが生成するデータの収集保存と処理，さらに制御は，仮想技術を積極的に利用したクラウド基盤[注8)]の積極的な利用が推奨される．クラウド基盤においては，ハードウェアの技術仕様に非依存な，仮想的な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．

次に，IGCJ（Internet Governance Conference Japan, www.igcj.jp）が提唱しているIoT時代の社会・産業インフラを想定した「基本となる10の考え」[4)]の中で，エネルギー分野の施設・システムに関係が深く，重要であると考えられるものを以下に列挙する．

(1) まずは自助，次に共助，最後に公助

自然災害対応のような非常時の対応と同様に，「自助・共助・公助」の考え方が根付くべきです．自助とは，ユーザー一人一人が自らの安全を守ること，備えること．共助とは，地域や業種業態ごとに助け合って安全を守ること，備えること．最後の公助とは，政府や公的機関がそれらを支援し，公共サービスの一環として安全を守ること，備えることです．「誰かが安全な環境を提供してくれる」ことを前提とすることは，現実的ではありませんし，かえってリスクを増大させることになります．

(2) 原理主義」ではなく「実践主義」で進める

最初から100%の安全性を目指すのでなく，個人・組織・社会全体が常にセキュリティー対策を見直し続け，変わり続けられるような規則になっていることが重要です．

(3) 強制する・制限するのではなく，活動の活力向上を応援する

非定型の活動を受け入れ，活動の活力向上を応援（encourage）することができる環境を提供するようなデザイン・実装を目指ことが重要です．なにかを「強制（enforce）」したり，「制限（restrict）」したりすることは，可能な限り避けるべきです．

(4)「過保護」はかえってリスクを増大させる

厳しすぎる規制は「安全である」という錯覚を生むだけで，実際には，その環境で活動する人・機器を，環境の変化に対して弱体化させてしまうことになります．たとえば外部から完全に切り離されたシステムではセキュリティーの対策は不要という誤解を生み，各機器が自らを守る術を身につける機会さえも奪ってしまいます．怖いのは，危険が迫っていても自らを守る術を持つことなく無防備な状態が続くことです．

(5) セキュリティー対策を品質向上のための投資と捉える

セキュリティー対策を，安心安全を確保するための品質の向上であると定義し，すべての機器などの製品において，その品質を向上すべく，それぞれの立場において「セキュリティー QC活動」を実施することにより，安心安全なインフラの構築が可能となります．企業・組織におけるセキュリティー対策の推進は，道徳や社会責任ではなく，それは，サービスの質を向上し，顧客やユーザの情報を守り，自らのビジネスの拡大のための投資であると捉えるべきでしょう．

(6) 経験と知見の「共有」を行う

インシデントの経験や知見は，外部の人や組織と共有すべきです．共有することにより，そのインシデントについて専門家を含む，より多くの人や組織に検討の機会が与えられるからです．同様の手口による被害を防ぐチャンスが与えられることは，非常に重要です[注9)]．「勇気を出して声をあげる」ことが，社会全体のセキュリティー対策に貢献すると考え，そのような勇気ある経験と知見の共有を評価すべきです．

(7) インシデントの経験者は，「被害者」として「保護・支援」する

インシデント被害者が経験と知識の共有をためらう理由の一つは，当事者に対して責任の所在や対策の不備を厳しく追及する世論にあります．攻撃者の手口は日々変化しており，十分と思われる対策をとっていても被害に遭う可能性はゼロではありません．私たちは，インシデント被害者が意図的に対策を怠っていたというようなケースを除いて，彼らを「保護・支援」するべきであり，また彼らが第三者と経験を共有する行為を賞賛すべきです．被害者を責

注7）コンピュータシステムの劇的で継続的な性能向上が，詳細かつ精密に実空間の物理システムをシミュレーション可能にした．実際に，GUTPのメンバー企業が関与した事業の事例としては，羽田空港駐車場におけるLED誘導灯システムの開発においては，Computational Design/Cyber Space Firstの形態で行われた．

注8）パブリッククラウドとプライベートクラウドが存在しており，利用可能である．

注9）内閣府「科学技術イノベーション総合戦略2016」P.10には，「業界内・業界間でのサイバー攻撃等の情報共有を共通化・自動化を実現する仕組みを構築し，さらに業種間を跨ぐ情報共有の環境整備に取り組む．これにより，イベント単位で短期間の設置も想定されるセキュリティーオペレーションセンター（Security Operation Center，以下「SOC」という）の整備促進や業界間のSOC整備の促進にもつながる」と記述されている．

めることには意味がありません．責めることで被害者のセキュリティー対策をするインセンティブが失われ，経験と知見が隠されてしまうことのほうが問題です．航空機の事故調査(次の事故を防ぐための調査や情報公開が重視され，そのために真実を明らかにする．悪者を探し，追求するためのものではない）に倣い，被害者を「保護・支援」し，再発を防ぐための調査にこそ力を注ぐべきですし，より多くの情報が調査のために利用可能にする状況を作り出すべきです．

3．まとめ

電力とエネルギーの自由化の進展と，エネルギーシステムのIT/ICTを用いたスマート化とネットワーク化は，これまでの基本的には個別に独立して運用されてきた基幹システム（電力においては 9 電力会社が構築運用してきた発送電システム）の管理制御システムの相互接続と連携・協働運用へと向かい，さらに，9 電力会社以外の多様な発送電システムとの相互接続，需要者施設との相互接続，多様なエネルギーシステムの相互接続へと向かう．インターネットが実現した,ネットワークのネットワーク化であり，プロバイダ（エネルギーの供給側）とユーザ（エネルギーの需要者）のネットワーク化，エコ・システム化である．すなわち,今後のエネルギーシステムは,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・保全されなければならず，適切で有効なセキュリティー対策が適用されなければならない．そのセキュリティー対策は,「まずは自助，次に共助，最後に公助」の原則のもと，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，すべての関係者（ステークホルダ）の間で連携・協調・協働しながら，すべ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と考えられる．このような，セキュリティー施策の確立と実践によって，エネルギー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を実現しなければならない．

参 考 文 献

1）閣議決定，第 5 期 科学技術基本計画，平成28年 1 月22日．
2）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．
3）内閣府，科学技術イノベーション総合戦略2016,平成28年 5 月24日．
4）江崎，中村 等，セキュリティーに対する考え方，第1.1版，2016年 7 月22日，
http://www.igcj.jp/meetings/concept-for-security.pdf