オープンでスマートなキャンパス施設の実現に向けての提言

東大グリーン ICT プロジェクト

【概要】

キャンパス施設を構成するすべてのハードウェアとソフトウェアが、共通のオープンな技術仕様に基づいて相互接続し、相互にかつ自由・自律的に連携協調動作可能な環境を実現することで、(1) 持続的なイノベーションと、(2) 継続的・効率的・低コストの運用、(3) 安全な継続的運用、さらに、(4) 地球環境対策に資する運用、を同時に一つの共通インフラで実現することを目指した、スマートなシステムの設計・構築と運営を実現しなければならない。 すなわち、これまでの、物理レイヤからアプリケーションレイヤまでの機能が独立した独自技術を用いた各サブシステムから構成される「垂直統合型のサイロ型システム(あるいは ストーブ&パイプ型システム)」を、すべてのサブシステムに共通するオープンな技術を用いて相互接続し連携動作することが可能な**『相互接続性を最重要要求条件』**とする「水平協調型のプラットフォーム型システム」へと、移行させることがキャンパス施設のスマート化であり、キャンパス施設の**長期的観点からのライフタイムコスト**[1] の削減と高機能化と運用の継続性の実現に寄与・貢献する。相互接続性を最重要条件とするキャンパス施設においては、**「外部システム・外部機器との接続」を前提にした、『セキュリティー・バイ・デザイン(Security-by-Design)』**の考え方に従った、すべての ハードウェア・ソフトウェアに関するサイバーセキュリティー対策の実装が必須条件とされる方向を目指さなければならない [2]。

オープン化とスマート化は、キャンパス施設を構成するすべてのハードウェアとソフトウェアに関して実現されるだけではなく、これらの調達手順と運用手順のオープン化とスマート化を実現するとともに、現在の「ベンダー主導」の設計・実装・運用・管理手順を、「オーナー主導・ユーザ主導」[3] あるいは ユーザとベンダーが密接にシステムの技術仕様を定義する Dev-Ops[4]と呼ばれる状況へ変革することで、より小さなコストで迅速かつ容易に、キャンパス施設の高度化・効率化・安定化を実現することが可能となる [5]。 「ベンダー主導」の状況を、「オーナー主導・ユーザ主導」に変化させるためには、発注者(施主)組

---

[1] 短期的利益を最大化することで、結果的には長期的利益を損なうような、長期的責任を放棄・無視したプロジェクト企画とコスト評価ならびに予算運用は、組織にとって不利益となる場合が多い。「振り逃げ禁止」の原則を適用すべきである。

[2] このような考え方は、内閣府が提言している「科学技術イノベーション総合戦略 2016」、2016 年 1 月に閣議決定された「第 5 期科学技術基本計画」においては、Society 5.0 と定義されており、すべてのシステムが IT/ICT 技術によってオンライン化・オープン化・スマート化され、相互接続された自律的統合システムとして連携協調・協働動作を、十分なサイバーセキュリティー対策とともに実現し、創造的な新機能を実現することが、我が国の今後の戦略的施策・方向性と明言されている。

[3] ベンダーへの「丸投げ禁止！」

[4] 開発(Development)と運用(Operating)を組み合わせた混成語で、開発担当者と運用担当者が連携・協力する開発手法をさす。

[5] 常に小さなコストで実現可能とは言えないが、特にライフタイムコストという観点からはより小さなコストとなることが少なくない。

織の担当者の知見と経験値の向上が必要となり、この実現に資する「発注者側のスキル向上」が実現されなければならない。**あるいは、発注者側の意思の具現化を支援することが可能な事業者あるいは組織を活用することも、有効な方法であろう[6]。**発注者側の知見の充実と向上によって、発注者側と受注者側の間での、適切な緊張感をもって、切磋琢磨と連携が実現される環境を確立しなければならないと考える。

1. IT 業界における 技術及びシステム構造のオープン化

各計算機ベンダーが開発した独自技術を用いた個別システムとしてのシステム構築と運用を前提としたメインフレーム型のコンピュータシステムは、まず、その接続機器の多様性と自由度の獲得・確保のために共通のオープン技術規格が制定され、その技術仕様に従ったさまざまな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。その後、コンピュータ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実質的な相互接続を実現する通信プロトコル（具体的には TCP/IP）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、さらに ネットワーク化することが可能となった。その過程においては、相互接続性の確認が精力的に行われた。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の障壁が激減されることとになり、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、維持性、持続性に関するコストと、システムを構成する各モジュール（ソフトウェアとハードウェアの両方）のコストの継続的かつ大幅な削減が継続されるとともに、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)品質の向上に貢献することになった。 これは、モジュール性を持ったオープン技術仕様の利用を、機器およびシステムの調達者・運用者が行ったことが原因であるととらえることができる。

すなわち、技術とシステム構造のオープン化によって、特に、**システムのオーナーおよびユーザ**にとって、以下の恩恵がもたらされたと解釈することができよう。

(1) ライフタイムコストの削減
  (a) 初期導入コスト
  (b) 運用コスト
    ① 機能のアップデート・追加(改修を含む)
    ② モジュールの入れ替え(代替機の可能性が制限)
    ③ システム運用のネットワーク化と最適化
(2) 新機能追加の可能性・実現性の向上

各ベンダーの独自技術を用いた旧来の IT システムにおいては、システムの構築と

[6] 成功事例としては、Plantec 社によるキューデンインフォコム社・QTnet 社の「データセンター福岡空港」が挙げられる。

運用・改修改善・高機能化に必要なコストが大きくなるのみならず、新機能の導入のための制限が存在し、新機能の導入が不可能な場合も少なくなかった。

ベンダーに共通なオープン技術の適用・導入によって、納品ベンダーでは導入が難しい(苦手な)新機能を、少ないコストで、かつ短い時間での実現(Agility)が可能となった。 すなわち、システムの設計・実装および運用の自由度を向上させることの可能性・実現性が向上し、特にシステムの所有者・運用者の意思を反映することが可能となる。

(3) システム統合の可能性・実現性の向上

特定のベンダーが提供する独自技術を用いず、ベンダーに共通なオープン技術を用いることで、それまでは、独立に運用されていたシステムを相互接続し、統合化および連携協働の実現性への困難度が軽減されることとなる。これまで、個別に稼働していたシステムを、相互接続し連携動作させることで、システムの効率化の実現と、新機能・革新的機能の実現が、今後の方向性と認識されている[7]。

一方、ベンダーにとっては、技術とシステム構造のオープン化によって、以下の恩恵がもたらされたと解釈することができよう。

利益率の高いシステムへ移行することで、既存システムによる事業を継続した時の利益率の低下[8] を防ぐことができる。 新しい付加価値を産まない事業・産業は、コストダウンによる利益率の向上のみとなり、結果的・長期的には、衰退せざるをえないというのが一般的である。これまで、相互接続できなかったシステムとの相互接続・連携協働動作により、新しい付加価値を持った利益率の高い新事業の実現可能性への挑戦が可能な状況を作りだした。

現在の、キャンパス施設の設計・実装・構築・運用・保全・管理に関する事業・産業である建築業界およびプラント業界は、オープン化以前の IT 業界に等しい状況にあると考えなければならないのではないだろうか。

---

[7] 「第 5 期科学技術基本計画」においては、「自ら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作りを強化する」という、ICT/IT 技術を用いた超スマート社会(Society 5.0)の実現が提言されている。

[8] 研究開発・生産システムの効率化によって、利益率の向上は実現可能ではあるが、大きな利益率の向上を期待することは容易ではないのが一般的であろう。

2. 建築・設備業界の発展・飛躍に向けた考え方と方向性

IT 業界が実現した、システムの「オープン化」と「スマート化」を、建築・設備業界で実現・展開することで、キャンパス施設のオーナーのみならずベンダー企業に対しても、総合的で継続的な恩恵がもたらさなければならない。

2.1 設備および設備システムに関する課題

以下に、現在のキャンパス設備ならびに設備システムが抱える課題を整理する。

(1) 調達システムに関する透明性の不足・欠如

① システム構造

システムを構成するサブシステムがブラックボックス化されることで、結果的に、施主側の要望実現に関する自由度が制限されることになっている。

② コスト構造

サブシステムのコストがブラックボックス化され、発注者を含まない、受注側企業間での相対でのコスト構造が形成され、コスト構造の透明化が阻害され、結果的に、サブシステムの提供可能業者間での競争環境の形成が阻害されている。

(2) ベンダーロックイン と 提供機能の制限

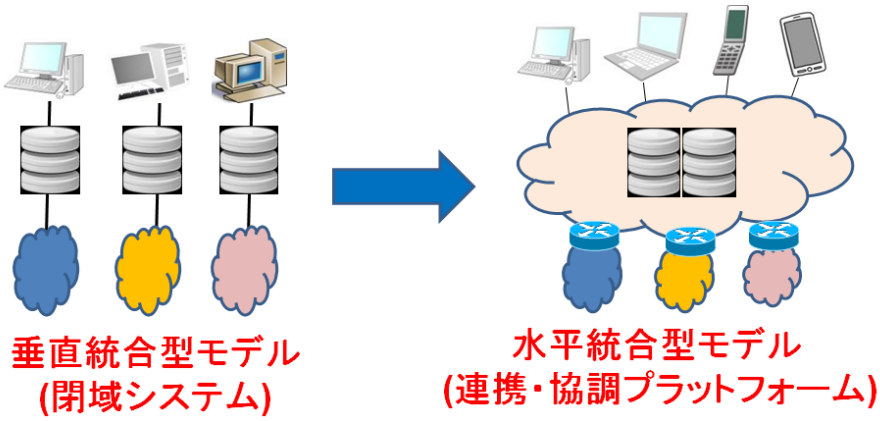
オープン技術が利用可能とされているにも関わらず、実質上は オープン技術の利用・適用が、事実上、困難(あるいは不可能)となっており、大幅な初期コストの増加が誘導され、特定のベンダーへのロックイン状況から抜け出すことが容易ではない状況が作り出されている事例が多い。具体的には、共通のオープン技術を用いた相互接続環境の実現は不可能ではないが、大きなコストを請求・要求される場合や、基本機能以外の機能に関する相互接続性は保証できない場合、あるいは、導入システムに対する正常・安定運用の保証しない場合(e.g., 『オープン化は可能だけど動作保証はできません』と脅迫される)などが、発生しているのが実状である。 その結果、事実上・実践的な「相互接続性」実現が阻害されるとともに、他のベンダーの機器・ソフトウェアの導入が阻害されているとともに、先端機能・新機能の導入に関する障壁(コストと運用制限)が大きく、事実上阻害されている状況が少なくない。

(3) システムのネットワーク化・統合化への制限

Industry4.0(第 4 次産業革命)や Society5.0 で 提唱されている、さまざまシステムの相互接続・相互連携・連携協働は、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である。このネットワーク化・統合化は、自キャンパス内の施設に限ったものではなく、自キャンパス以外の施設との相互接続・連携協働を、

意図したものである[9]。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。

しかしながら、相互接続に伴うシステムの動作保証の問題、サイバー セキュリティーを含むセキュリティー(安全性)の問題、相互接続に必要な費用の問題などを理由に、システムのネットワーク化・統合化への制限が提示されることになったり、あるいは、導入したシステムが独自技術を用いているために、相互接続することが事実上不可能となっている場合などが存在している。



(4) セキュリティー

システムがクローズドな独立運用を前提としている場合が少なくない。すなわち、物理的セキュリティーによって、外部からの攻撃への対処をしているので、安全であると、主張される場合が少なくない。そのため、当該システムを、他のシステムと相互接続する場合には、システムの安全稼働・正常稼働を保証することは不可能といわれることが多い。

また、他のシステムとの相互接続を行わないことを前提に、システムの設計・実装・構築・運用・保全が行われている場合が多く、基本的なセキュリティー対策が考慮・実装されていない場合も少なくないのが実状である。

2.2 注意が必要なビジネス慣習の例

以下に、キャンパス施設の所有者側が、キャンパス施設の新設や改修などの際に、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独自技術によるロックイン型ベンダーによる反応・対応の例を以下に挙げる。

---

[9] Plantec 社(www.plantec.co.jp)での事例では、外部設備との協調連携を IT システムの連携による物流の管理・制御の統合化と高度化によって、必要な在庫容量を大幅に削減した物流倉庫・物流システムの提案・受注・施工が存在する[3]。

(1) オープン技術を用いることでも、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。
(＊) 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。
(＊) 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。
(＊) 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 対応方針

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した。

(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)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」コンサル事業者の利用するなどして、実現されるべきである。 「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
設備の発注に際しては、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)

可能な限り、システムを構成するすべてのサブシステムに対するコスト構造がオープン化され、発注側に透明化されることを提案の必須条件に盛り込むべきである。これによって、受注内部でのブラックボックス化された相対での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。調達にあたっては、外部システムとの接続(ネットワーク化)の可能性を前提として、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とシステム運用の考え方が適用されなければならない[1][2]。少なくとも、以下のような項目が、セキュリティー機能の具体的項目として、盛り込まれるべきである。

(i) 物理・セキュリティー
(ii) サイバー・セキュリティー
(iii) エネルギー・セキュリティー

事例： 東北福祉大キャンパス[9]、 三井不動産 日本橋再開発

(6) 既存のオープンプロトコルの現状 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。

(i) 相互接続に伴うシステムの動作保証
(ii) 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
(iii) 相互接続に必要な費用

このような項目に配慮しつつ、キャンパス設備全体のオープン化とネットワーク化(相互接続化)を順次推進する方向性を包含した戦略的で計画的な実行計画が提案されるようにするべきである。

このような、考え方に従って、推進されている先端的で先駆的な事例(東京工業大

学[8]、大手センタービル[9]、東京大 工学部 2 号館[6])が、既に、いくつか存在している。

(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[10]。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[11]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。

(8) 電力・エネルギー自由化への対応

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 法的・商的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ことになる[12]。

(9) キャンパス施設の エコ・システム化

キャンパス施設を 1 つの プラットフォームとして捉え、以下の 4 つの機能を同時に実現するような検討と提案を推奨すべきである。

(ア) 省エネ・節電

---

10 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。

11 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。

12 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。 E.ON, https://www.eon.com/en.html)を 意識したシステム設計を行う必要がある

(イ) BCP(危機管理)
(ウ) 効率化・品質向上
(エ) 新機能導入 (システムのオープン化が必須条件)

2.2 事例紹介(BCP: Best Current Practice)

以下、GUTP(東大グルーンICTプロジェクト, www.gutp.jp)参加組織の事例を紹介する。

(1) 東京大学 [4][5][6][7]

2008 年から工学部 2 号館を実証実験棟として、IEEE1888 を適用したオープンなエネルギー管理システムを構築、2011 年東日本大震災後には、ピークで約 40%, 総量で約 30%の節電を実現した。全学施策としては 5 つの主要キャンパスの電力使用量のオンライン見える化システムを構築、ピークで約 30%、総量で約 20%の節電を実現した。工学部においては、各研究教育棟の電力使用量の見える化システムを構築、継続運用が行われている。

(2) 東京工業大学 「エネ・スワロー」 [8]

全面を太陽光パネルに、多様な蓄電池システムを持った 大岡山キャンパスに新設された、EEI 棟(環境エネルギーイノベーション棟)は、IEEE1888 を導入することで、個別の独自技術を用いて稼働する 研究装置・設備の統合的管理・制御システムを構築、ビル全体の統合的エネルギー管理制御が実現された。IEEE1888 を用いた総合エネルギー管理制御システムは、大岡山キャンパス全体に展開される。

(3) 理化学研究所

理化学研究所の和光キャンパスにおける省エネ対策の一環で、キャンパス全体と約 30 の研究棟の電力使用量のリアルタイム監視を見える化は、オープン技術である IEEE1888 を用いて実現され実稼働している。 既存のシステムにデータ収集のための機器を設置、オープンなデータベース・ストーレッジ・セントリックなシステムが構築された。

(4) 東京 大手センタービル (竹中工務店) [9]

既往の中央監視システムを、VPN を介してクラウドと接続し、クラウド上の基盤を使って、ポータルサイトやエネルギーの見える化システムなどを実現した。実現においては、IEEE1888 や MQTT などのオープン技術を活用することで、アプリケーションの更新性を高め、クラウド使うことで保守性についても向上を図った。複数ビルの接続も実現しており、ビル間でのエネルギー比較も実現している。

(5) 東北福祉大学 [10]

都市ガスと電力系統(東北電力)、さらに 太陽光パネルの 3 系統のエネルギー供給源を統合化・多重化したエネルギーセンターが、NEDO の補助事業として行われた。 2011 年 3 月の東日本大震災に際しては、都市ガスの運用が継続されたた

め、キャンパスへの ガス・コジェネレーションによる 電力と熱の供給が継続され、避難施設として、近隣市民の収容を行った。

(6) セントレア空港

将来の拡張性とロングライフコストの削減の観点から、BACnet を用いた施設となっている。G7 伊勢志摩サミット(2016 年 5 月)では、空港施設のサイバーセキュリティー対策が、緊急かつ重要な業務であることが認識された。

(7) 千葉大学・木更津工業高等専門学校 植物工場 [11]

統合型環境制御システムとして、「統合環境コアシステム」と多数の「インテリジェントコントローラ」から構成され、IEEE1888 を適用して、多様な独自技術を用いたベンダーの植物工場で利用する機器を相互接続し、データはコアシステムにストレージされ、オープンインターフェースを用いてアプリケーションが動作する構成で、マルチベンダー環境での統合管理制御システムが構築された。

(8) 静岡大学 [12],[13]

静岡大学が展開する 2 つのメインキャンパスである 浜松キャンパスと静岡キャンパスの電力消費量をリアルタイムに WEB を用いて告知する PANDRA SYSTEM (http://pandora.ipc.shizuoka.ac.jp/eco.cgi) は、GUTP で国際標準化に成功した IEEE1888 技術を用いて実現されており、現在でも継続稼働中である。

(9) 静岡県 浜松市 施設管理 [14]

浜松市が所有する 4 つ公共施設(図書館、福祉交流センター、水泳場)を IEEE1888 を活用して、マルチベンダー環境で構成される既存施設のオンライン統合管理を実現、初期費用を概ね 4 年で回収するモデルで運用されている(2013 年 4 月に採択)

(10) 日本橋ダイヤビルディング(三菱倉庫)

歴史的建物の外観を保存した「災害に強い環境配慮型オフィスビル」を実現するために、ビル内のエネルギー消費状況のリアルタイム管理と、外部環境(交通や気象)の情報をオンライン化・見える化を行った。

(11) (株)カメガヤ ドラッグストア

関東に展開されている 40 を超える店舗(Fit Care DEPOT)の消費電力量の遠隔統合管理システムを IEEE1888 を用いて構築、本社オフィスから、全店舗の稼働情報がリアルタイムに監視可能となった。

(12) 岩谷産業(株) 中央研究所 (尼崎) [14][15]

次世代のエネルギー供給システムである水素を用いたエネルギーシステムの導入とともに、IEEE1888 を用いたオープン BEMS を導入し、所内で使用するエネルギーの「見える化」を行っている。使用するエネルギーは、水素、LP ガス、太陽光、電気の 4 つである。実験で使用した水素は回収して燃料電池により発電を行い、所内で再利用されている。

(13) セイコー プレシジョン社 タイ工場

セイコーソリューションズ(株) は、国内のグループ会社の工場とタイのセイコープレシジョン社において IEEE1888 を用いた GreenTalk を利用し、様々な技術

を用いて稼働している既存システムを、オープンにネットワーク化・統合管理化することで、エネルギーの見える化と制御を行い、電力の削減に成功している。タイの工場では 空調電力を 20%､グループ会社の工場では 26%の空調電力の削減に成功している。

【参照文献・サイト】

[1] 日本データセンター協会､「データセンター セキュリティ ガイドブック 2015 年度版」､ http://www.jdcc.or.jp/pdf/DC_Security_Guidebook_2015.pdf

[2] 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、で http://www.igcj.jp/meetings/concept-for-security.pdf

[3] ビジネスブレイクスルー IT ライブ 239､「建築業界に対する Breakthrough – ビジネスからみた建築への改革-- 」、2016 年 10 月.

[4] 東京大学 TSCP 室、http://www.tscp.u-tokyo.ac.jp/

[5] 平井明成､「5－2 大学施設」、特集『電力不足とその対策』, pp57-60, vol.58-5, No.714, 電設技術、平成 24 年 5 月号

[6] 東大グリーン ICT プロジェクト、https://www.gutp.jp/

[7] 江崎、落合、「Internet by Design に基づいたスマートビル・スマートキャンパスの設計と実装 ―IEEE1888 を用いた実装･プラクティス･展開―」､情報処理学会 デジタル･プラクティス, Vol.5, No.3, 2014 年 7 月.

[8] 東京工業大学 環境エネルギーイノベーション棟、 http://www.nttdata-bizsys.co.jp/case/eco/eneswallow/tokyotech.html

[9] 大手センタービル : http://www.otecenter.tokyo/

[10] 東北福祉大学 エネルギーセンター、https://tfu.ac.jp/energy/index.html

[11] 栗本育三郎、”IEEE1888 を用いた植物工場統合型環境制御システム”、特集「モノのインターネット(IoT)」、オーム社 OHM, Vol.201, No.3, pp.26-27, 2014 年 3 月.

[12] 峰野博史、“Green by ICT による静岡大学スマートキャンパス化への取り組み”、大阪大学サイバーメディア フォーラム, No.12, pp.5-10, 2011 年 9 月.

[13] 静岡大学 「先駆的スマートキャンパスの実現に向けて」、2016 年 2 月. http://www.mirai-kougaku.jp/eco/pages/160212.php

[14] 静岡県 浜松市 4 施設の統合オンライン管理、2013 年 4 月. http://www.nttdatacs.co.jp/news/20130426.html

[15] http://www.iwatani.co.jp/jpn/r_and_d/

[16] 中島、高橋、牧野、落合、江崎、”ユーザイニシアティブ型グリーン ICT システム ―IEEE1888 によるエネルギーネストミックス型ビルの見える化―”, 電子情報通信学会 知的環境とセンサーネットワーク研究会 ポスター展示、信学技報、Vol.114, No.65, ASN2014-12, pp.43-44, 2014 年 5 月.

[17] セイコー ソリューションズ社事例、 http://www.seiko-sst.co.th/jp/greentalk-introduce.php

http://www.seiko-sol.co.jp/products/greentalk/greentalk_case/

【付録 1】「基本となる 10 の考え」[1]

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」 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[13]。 「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。

---

[13] 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。

【執筆者】

・執筆責任者

東京大学 大学院 情報理工学系研究科 教授　江崎 浩 (GUTP 代表)
東京都環境公社 環境科学研究所 主任研究員 藤原 孝行

・執筆チーム

東京大学 大学院 情報理工学系研究科 講師 落合 秀也
首都大学東京 都市環境学部 客員教授 山本 康友
(株)竹中工務店 情報システムエンジニアリング本部 粕谷 貴司
NTT データカスタマーサービス(株)
ファシリティーエンジニアリング事業部 部長 松下 浩之
シニアコーディネータ　笹沼 逸樹
LonMark Japan 理事長 富田 俊郎
シムックス(株) 代表取締役 社長 中島 高英
(株) ディー・エス・アイ 代表　豊田 隆志
豊田 SI 技術士事務所 所長 豊田 武二
(株) 三菱総合研究所 政策・公共部門
政策・公共部門 副部門長 中村秀治、
社会 ICT 事業本部　吉田薫

以上