産業サイバーセキュリティ研究会　WG1　ビル SWG（第 2 回）　議事要旨

日時　：　平成 30 年 4 月 16 日（月）　15 時 00 分～17 時 00 分

構成員　：

（座長）江崎　浩　東京大学　教授
松浦　知史　東京工業大学　准教授
アズビル株式会社
イーヒルズ株式会社
鹿島建設株式会社
株式会社九電工
株式会社きんでん
技術研究組合制御システムセキュリティセンター
セコム株式会社
ダイキン工業株式会社
株式会社竹中工務店
株式会社日建設計
日本生命保険相互会社
一般社団法人日本ビルヂング協会連合会
株式会社日立製作所
一般社団法人ビルディング・オートメーション協会
一般社団法人不動産協会
三井不動産株式会社
三菱地所株式会社
三菱電機株式会社
横浜市

（オブザーバー）
国土交通省（大臣官房官庁営繕部設備・環境課、土地・建設産業局建設業課、土地・建設産業局不動産業課、住宅局住宅生産課、総合政策局情報政策課）
内閣官房　東京オリンピック競技大会・東京パラリンピック競技大会推進本部事務局
内閣サイバーセキュリティセンター　情報統括グループ（オリパラチーム）
公益財団法人東京オリンピック・パラリンピック競技大会組織委員会
中部国際空港株式会社／中部国際空港施設サービス株式会社

議題　：

１．前回の議論の整理と今後の進め方について
２．発注者の立場からのビルセキュリティへの要求等について
３．建築設備設計の立場からのビルセキュリティへの要求等について
４．ビルシステムの立場からのビルセキュリティへの要求等について
５．自由討議

要旨　：

１．事務局（前回の議論の整理と今後の進め方について）

- 前回の議論で概ね意見が一致した部分として、全体の方向性や検討に当たっての論点等の整理結果について説明。
- JDCC の建物設備システムリファレンスガイドを出発点とした、ガイドライン作成に向けた議論及び詳細化の方法について説明。
- それぞれの論点に対応したガイドラインの使用法のイメージについて説明。

２．発注者の立場からのビルセキュリティへの要求等について

- 2020 年 1 月竣工予定で新市庁舎を建設中である。議会棟と行政棟で 6,300 人の職員が入居し、さらに 1、2 階の低層階には商業エリアが入る。
- 新市庁舎は、災害時の司令塔も兼ねており、サーバ室と危機管理部が入るとともに、10 日分の非常用電源や地域冷暖房の拠点としてコジェネも入れる。そのほか、エコロジーの観点から太陽光、燃料電池も導入し、個別空調や照明制御の IoT 活用、監視カメラや入退館の管理、外気温に対応したデマンドレスポンスを実現するクラウド BEMS の導入など、IoT 及びネットワークをフルに活用した施設となる。
- 一方、ビル設備への IoT 導入は、現時点では課題点も多い。ICT 設計者のスキルは十分ではなく、多種多様なメーカに渡る非常に多数の IoT 機器が設置されることになり、結果として非常に複雑なシステムとなる。市庁舎の場合、攻撃のターゲットになりやすい一方で、乗っ取り等の影響も非常に大きい。導入する IoT 機器のセキュリティに関する検査認証体制も未整備である。
- ビルシステムの調達の観点から見ると、自治体では設計・施工業者の調達と納入機器の調達が別々となる仕組みであり、また外部クラウド等との接続などもある。これに対し、ビルの IoT システムの設計ガイドや参照モデル、その中でのサイバーセキュリティ要件の規定、個別の IoT 機器のセキュリティ規定や相互接続のためのセキュリティ基準もない。竣工時の検査方法や管理更新などもセキュリティの観点から要検討である。発注者、運用者、委託先ともにセキュリティの経験値が低く、ビルに関するサイバーセキュリティについての性能評価が存在しない。このため、議会などへの客観的な説明も難しい状況にある。

３．建築設備設計の立場からのビルセキュリティへの要求等について

- 最近は、ビルの中で建築設備がネットワークにつながるようになってきており、IoT のようなデバイスレベルまでの接続が行われるなど、ネットワーク利用の幅も広がってきている。
- 一方、設計・施工体制としては、自動制御、BEMS、中央監視などは機械設備の担当者が、監視カメラやテレビ関係、インターネットなどは電気設備の担当者が、エレベータは建築意匠の担当者がそれぞれ設計するなど、個別バラバラに設計され、それぞれの発注図書に個別にインターネット接続の要求が書かれるような状況である。
- またセキュリティに関して現状どの程度配慮しているかについては、空調延長サービスなどで Web サーバを置く場合などはサーバ証明書を使った https 接続程度は提供しているが、インターネット接続のファイアウォールは基本的な設定のみ、監視カメラのパスワード設定は初期設定のままが多くて構築業者やメーカ任せの場合が多い。ウイルス対策も外部インターネットに接続せず、ビル内の LAN のみの場合は対策をしないこともある。OS のアップデートもアプリを含めた更新コストの関係もあり、古い OS のままということも多い。ネットワークも発注図書にバラバラに要求が書かれているため、用途毎にバラバラに引かれており、個々のネットワークの規模が小さいので、統合監視的な取り組みも出来てない。さらに現場のビル管理者は、電気主任技術者やボイラー技師等が一般的で、IT は専門外だったり、小規模ビルの場合には非常駐のケースも多い。
- メーカの対応としても、新しい試みへの抵抗感が多いように感じられる。システム構成の多くをマニュアル化しており、そこから外れる事項への抵抗が強い。
- 一方で海外では統合 BMS がポピュラーになってきている。ビルの監視を 1 台の PC で統合的に見ることができ、BI ツールとも連携した分析ができるなど、高度な利用が可能である。今後は日本でも徐々に普及してくるだろう。
- 2015 年に竣工し、世界一スマートなビルと言われている、オランダの The Edge と呼ばれるビルの事例も出てきている。28,000 個のセンサーが使われるなど、数多くの IoT が導入されており、業務システムとビル管理システムを融合したサービスを提供するなど、高度なスマート化を実現している。このような動きは他のビルにも広まってくると考えられる。
- このような将来のビルの設計・施工体制のあり方としては、それぞれ独立している各設備をネットワークが横串するような姿が考えられる。設計・施工の段階に通信や ICT の専門家が存在して、ネットワークにつながる各設備を横串で面倒をみていくような体制が必要と思っている。
- ビルシステムがますますネットワークにつながり、インターネットとシームレスにつながっていく中で、ビルシステムの設計・施工に関わる既存の技術者の ICT スキルアップと同時に、通信・ICT のスペシャリストのビル分野への参入の両方が望まれている。これらを一歩一歩着実にやるために、簡単なことでも効果が上げられる対策、１つ１つの対策を確実に行えるガイドラインが必要と考える。

４．ビルシステムの立場からのビルセキュリティへの要求等について

- 既存ビルの場合、クローズド環境がほとんどなので、サイバーからの侵入リスクよりもフィジカルからの侵入リスクの方が大きい。このためフィジカルからの標的型攻撃に対する多段防御が大事になる。この

際に、費用を考慮し、短時間でビルシステムへの防御対策を実施するには、クリティカルポイントを考慮して、対策順序を定義する必要がある。

- 実際に既存ビルにセキュリティアセスメントを行った事例を紹介する。対象は設備設計が終わった状態の新築ビルだが、システムは既に決定済みだったので、既存ビルへの後付対策と同じアプローチで、アセスメントと対策の実装を行った。
- 対策 1 は、リスク箇所の見える化と対策方法の立案として、現状把握によりリスク分析を実施した。自社ではセキュリティアセスメントの PDCA を回すサービスを提供しており、それを適用して、システム構成図や IP 機器の各種情報から、最新設備の設計図面を作り、現状とリスクポイントの見える化を行った。リスクアセスメント結果から、内部 IP ネットワークの対策場所や必要な設定等を明らかにし、さらにファームウェアの更新、定期診断などを継続実施できるようにした。
- 次に対策 2 で、物理セキュリティ対策として、L2 スイッチのポート使用制限などを提言した。対策 1 で特定したセキュリティインシデントについて JDCC の 21 項目の管理策を考慮して、対策のためのシステム導入と運用対策について案を企画した。
- 最後に対策 3 で、物理セキュリティを突破されて内部 IP ネットワークに侵入された場合の内部 IP ネットワークレベルでの対策を実施した。具体的には、許可した機器のみの接続、不正通信の検知・通知、許可したデータのみ通過、これらの機能を満たす L2 スイッチ製品を設置した。
- 例えば、内部攻撃の例として、ネットワークスイッチの空きポートに不正端末を挿入し、大量の不正パケットを送信してネットワーク負荷を増加させることで、監視カメラと監視端末は正常に動作しているが、システム全体は正常に動作出来ないようにすることがある。この場合、L2 スイッチを使って大量の不正パケットを遮断することが対策になるが、L2 スイッチはさらにマルウェア対策としても有効である。レイヤー2～4 でのマルウェアの動き（ポートスキャン、侵入、攻撃など）が分かれば、内部 IP ネットワークにおいても検知、遮断することが可能である。
- 現状のビル用 L2 スイッチは、IT 業界で普通に用いられているスイッチよりも機能が限られており、これを最新のスイッチに変えていくだけでも、マルウェア感染、DoS 攻撃マルウェア、ARP Spoofing 攻撃、アクセス制限／通信制限、ネットワーク盗聴、SMB 通信遮断、作業ミス対策など、幅広い内部 IP ネットワークでのインシデントに対応することが可能である。

５．自由討議

（１ａ）ビルシステムの現状（設計プロセス）

・ 最初から全体を意識して作ることができれば良いが、往々にして途中からあれも欲しいとなり、追加されることが多い。

（１ｂ）ビルシステムの現状（外部接続）

・ 各システムが縦割りでインターネットにつながっている。入り口も集約されてはいない。

・ 設計としては、インターネット接続を集約したいと思うが、現実にはそれぞれ別々の用途でインターネット回線につながっている。ファイアウォールの設定もばらばらである。

- ビルの入り口で光アクセス回線の 1Gbps 帯域をフルに使うことはないと思うので、入り口だけでも 1 つに集約できると良いと思う。
- ビル設計がネットワークを含めた効果的な提案を出来ていないのが現状である。

（１ｃ）ビルシステムの現状（図面管理）

- ビルシステムが IT 的にどうつながっているか、納入当初に図面を出してもらうと良い。ID/PW もせめて初期設定からは変えるべき。各部署が個別に発注している状況だとしても、誰かが全体絵図をトータルに見ていく必要がある。基礎的な取り組みを重ねていくだけで、レベルは上がると思う。

（１ｄ）ビルシステムの現状（コスト）

- IT の世界とビルの世界の乖離が大きい。同じ L2 スイッチでも両者のそれは大きく機能が違う。ビル設備を構築する人と IT ネットワークを構築する人への支払いコストも違っており、単純に IT の世界の人をビルの世界で働いてもらうとはならない。両者が寄り添えるポイントをどう見つけていくかが課題である。
- 概念論で語っても具体的に人月単価とかを出して議論しないと変わらない。適正なコストを共有できればと思う。
- 確かに難しいのはコスト対策である。ここはなかなか進まないのが現状である。

（１ｅ）ビルシステムの現状（損害賠償）

- インシデントによるテナントからの損害賠償、免責条件はどのような契約になっているのか。保険は利用しているのか。海外ではシステムベンダが損害を負うケースもあるが、誰が責任を持つのか。
- 現状は一般の損害保険の範囲で対応しており、サイバー攻撃による巨大な損害には対応できるようにはなってない。そういう意味では、セキュリティがしっかりしていることは、テナントにとっての選定基準になってくるかもしれない。間接的にはビルのバリューにつながる話である。
- 保険には入っていない。その代わり、テナントとの間で責任の分岐点を明確化しようとしている。例えばネット接続は、オーナーからは提供しておらず、テナント自身が ISP と直接契約する形にしている。
- 保険には入っていない。ただし、何か起きた時のために、セキュリティに関してここまでやっていたと主張できる材料が欲しい。保険もあると良いと思うが、保険料の算定根拠も分からず、全額払ってもらえるのか心配でもあり、導入はしていない。
- データセンターでは、電源や空調のトラブルでファシリティがダウンした事例の報告はあるが、サイバー攻撃でダウンした事例は聞いたことがない。サイバー攻撃対策の議論も行っているが、電源の強化、空調の強化が大事な状況であり、現状に合わせた対策の強化を行っている。

（１ｆ）ビルシステムの現状（自社の取り組み）

- 自社としてビルの管理をクラウドに移行し、そこでセキュリティを確保する方策の研究を始めている。
- ビルの管理に関しては ISMS に取り組んでおり、ビル設備の製品自体は JDCC ガイド、IoT 機器ガ

イドラインまでカバーできれば、それなりに安全性を確保できると考えている。

（２）ガイドの形態

- データセンターのセキュリティ対応策である、JDCC の 21 管理策ではビルにとっては十分ではないと考えている。JDCC のリファレンスガイドはデータセンター事業者を中心に、運用者の立場で作っているので、BA システムそのものの脆弱性に手を入れられておらず、実装まで踏み込めていない。この場では必要なメンバーがそろっているので、具体的な手法に踏み込んだ解決策を出していって欲しい。
- 実例も少し入れるようにしたい。
- JDCC の項目に加えて対策レベルでは IT の分からない人でも分かるようにして欲しい。
- 3000 坪だと相当な数が対象になる。既存物件で、大きな資本力もなく、3000 坪の普通の大きさの賃貸ビルの事業者が使える内容を意識して欲しい。
- 時間を掛けてでも、中途半端ではなく、使いやすいガイドにする必要がある。21 項目もどこまでやれば良いのか分からないということのないように。一般のオーナーでもコスト感が頭に浮かぶ必要がある。
- ビル全体のサプライチェーンを把握し、設計からメンテナンスまで、知見のある人が入ってくる構造にするのが大事。
- 本日発表してもらった新市庁舎調達のチェックリストは発注側の要求としてわかりやすい。
- 典型的な BA のシステム構成を定義し、普遍的なシナリオを数個用意して、その具体化シナリオについて、JDCC ガイドを元にしてまとめると良い。
- リスクアセスメントのための最低限のシナリオを入れる。本日発表してもらった L2 スイッチの話が使える。
- 設計段階でセキュリティを入れるには発注側にも知見が必要になる。主に大型ビルを作る時で、貸しビルではそこまで必要ではないかも知れない。
- セキュリティを進めるには 2 つの方策がある。①危機意識の醸成。②オーナーにプラスのインセンティブを与える。
- 危機意識の醸成に関しては、オリンピックがあてはまる。平昌でも激しい攻撃が来た。簡単な対策としては、今日の話から「安価な L2 スイッチを入れていない」ことのチェックなどが使えると思う。
- プラスのインセンティブに関しては、国交省とうまく協力出来ると良い。
- オリパラ施設と一般ビルとは分けた方が良い。
- 新築ビル用と既存ビル用はきれいに分けた方が良い。経営インパクトもある程度、桁のオーダーで分かるようにする。また掛けるコストと受容するリスクの関係も整理する。
- ビルのセキュリティにも星 1 つとか 3 つとかのレベルがあると良い。止まっても影響が少ないところ、止まるとまずいところなど、いろいろある。
- 指標は有効である。ただし、作るのは難しい。
- 中央省庁的には、NISC の統一基準も大事かと思う。特にオリパラ的にも大事である。
- 重要インフラはしっかりやり、それ以外はベストエフォートが全体の意識共有だと思う。まず重要インフラをしっかりとやると良い。整理としては、プラスのインセンティブと危機意識の醸成を含めて整理する。

・ まとめとしては、推進策は危機意識の醸成とプラスのインセンティブの 2 つで考える。既存ビルへのすぐにやるべき対策を整理する。調達を含めたガバナンスチェックリストがあると良い。

（３）ビルの区分の基準

・ ビルの分け方で、床面積に加えて、電力設備ガイドラインの区分などを補足条件にいれてはどうか。
・ 例えばオリパラ施設は区分 S、空港・駅などは区分 A、一般ビルはランドマークになるような 4 万坪以上が区分 A、これらは一定レベル以上の対策を強く推奨する。区分 B は横浜市役所が 4 万坪なので、1～2 万坪以上を大規模、それ以下の小さなビルは意識改革のためのガイドにする程度でどうか。

（４）ガイドの利用法

・ インセンティブの逆で、ビルが攻撃を受けたとき、テナントから損害賠償請求を受ける可能性もある。そのために、ここまで対策をしていると示せることが大事である。
・ オリパラ施設、空港・駅など、一般ビルはランドマークになるような 4 万坪以上の大型ビルについては、一定レベル以上の対策を強く推奨する。逆に小さなビルは意識改革のためのガイドにする程度で良いのでは。
・ クリティカルインフラはしっかりやり、それ以外はベストエフォートが全体の意識共有だと思う。まず重要インフラをしっかりとやると良い。整理としては、プラスのインセンティブと危機意識の醸成を含めて整理する。

（５ａ）ガイドの具体的内容（検知と初動対応）

・ 安全ということでは初動復帰の手段が大事。

（５ｂ）ガイドの具体的内容（アクセス管理）

・ ネットワークへの統合が時代の流れだが、ユーザの利便を考えると分けた方が良いという考えもある。全部混ぜると危ない。オペレーションのアクセス者数を絞るべきである。

（５ｃ）ガイドの具体的内容（ネットワーク）

・ 設計書にネットワークへの要件記述が入っていないというのも課題である。チェック方法を示せると良い。
・ ガイドには IT 制御やネットワークの基準を含んでいく必要がある。
・ ネットワークへの統合が時代の流れだが、ユーザの利便を考えると分けた方が良いという考えもある。全部混ぜると危ない。システム間の接続も細くするべき。
・ ネットワークの使い方は二極分化する。統合されたネットワークで使われるものと、製品毎に個々の回線を引くようなもの。こちらはビルの入り口がごちゃごちゃになるので、指針が欲しい。情報の出口も整理することが大事である。

（５ｄ）ガイドの具体的内容（図面管理）

・ BIM を納品させるべき。インベントリ管理とオペレーションツールを統合するようなものが、ビルにもあると良い。

（５ｅ）ガイドの具体的内容（ID 管理）

・ 名前付け、機器の ID 管理が大事である。統合管理にも、VLAN の管理にも、インシデントの評価にも名前付けは重要。地道で大変だが、参照モデルとして ID の付け方などを入れることは、中長期的にはかえって楽になるはず。

・ BIM 的な情報管理を作る。

（５ｆ）ガイドの具体的内容（体制）

・ トップとして CISO や調達 CEO をおくように要求を入れるべきである。

・ ビルオーナーとして対策を取ろうとしても知識がなく、ゼネコン、サブコン、設計事務所等の相談することになる。それらにベンダまでも含めて、検討出来る体制が必要である。

（以上）

お問合せ先
商務情報政策局　サイバーセキュリティ課
電話：03-3501-1253