産業サイバーセキュリティ研究会　WG1　ビル SWG（第 1 回）　議事要旨

日時　：　平成 30 年 2 月 28 日（水）　12 時 30 分～14 時 30 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
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．産業サイバーセキュリティ研究会 WG1 ビル SWG の設置について
２．ビルのサイバーセキュリティに関する問題認識について
３．「JDCC 建物設備システムリファレンススガイド」について
４．自由討議

要旨

１．事務局

- 産業サイバーセキュリティ研究会 WG1 ビル SWG の位置づけ等について説明。
- ビル分野のサイバーセキュリティを取り巻く現状について紹介。
- ビル SWG の設置について説明

２．ビルのサイバーセキュリティに関する問題認識について

- サイバーへの意識の低さが攻撃を招く。
- オフィスビルにとってリスクの高い攻撃は、空調乗っ取りによるサーバルーム温度上昇、電源乗っ取りによる全館停電、防災乗っ取りによる火災等の不検知、ビルシステムを踏み台とする外部への攻撃。
- ハード／ソフト面の課題はOSのバージョンアップ困難、スケジュール運行でアドホックな作業が困難、定期点検以外に止められないシステム、運用面の課題は現場係員のセキュリティ意識の低さ、IT+OT 要員の不足、設計から利用開始までの間のシステム陳腐化。
- 早急に取り組むべき課題は、建設中のセキュリティ対策、竣工時のシステム検査手法確立、これらの発注段階での仕様書の記述方法。
- サイバーセキュリティに取組む理由の１つは、海外との都市間競争を勝ち抜くこと。そのためには、システムだけでなく運用も重要で、きめ細かでしっかりとした運用は日本は得意なところ。ガイドラインとして対策レベルの目安を示し、システムと運用のバランスを示すことが重要ではないか。
- ガイドラインのあり方として、ビルの規模によるセキュリティ基準の違いを考慮すること、システム設計における設定基準を示すこと、運用における設定基準を示すこと。

３．「JDCC 建物設備システムリファレンススガイド」について

- JDCC ファシリティ・インフラ WG の活動として、「建物設備システムリファレンスガイド」を作成。現在第二版まで発行し、ビルオーナー、設計者、管理者、データセンター事業者などに幅広く活用されるものを意識して作成。
- 基本的問題意識として、従来のビル設備はクローズドシステムだったが、回線の低廉化やシステムの信頼性からクラウドへ移行してきている。一方で、セキュリティの無い、制御システム部分がそのまま上

位インターネットにつながっており、危険な状況。攻撃も高度化してきており、BA ネットワークへの侵入事例も出てきている。

- 建物設備システムのセキュリティ管理策として、21 項目を整理。物理的設計における管理策、構築時における管理策、運用時における管理策に大別し、それぞれの具体的なセキュリティ対策の例示を実施している。
- ビル内には攻撃にさらされやすい危険箇所も多く、可能な対策から実施するとともに、要員の意識向上を図ることが重要。

４．自由討議

（１）ビルに求められるサイバーセキュリティ対策の検討軸について

- システムの構築から運用まで、ライフサイクルに応じて複数の選択肢を選べるようにする。
- 運用に入ってからの時間軸の視点もある。攻撃は進化するので、後付けの対策も取り入れ可能な柔軟性を持たせる。運用としては、竣工から 10～20 年後の改修時期についても考慮する。
- 自社ビル（庁舎）とテナントビルの違いもある。使う人間と管理する人間が同一でないため、分けて考えるべき。自社ビルかテナントビルかによってビル設計にも違いが生じるので、求められるサイバーセキュリティ対策も変えるべき（テナントの場合、空調延長をインターネット経由でビル制御システムにリモートでリクエストするが、セキュリティ上の問題も考慮する必要が出る）。
- 新築ビルと既存ビルもある。既存ビルに対して後付けで機微のある部分を最低限カバー出来るよう、被害の影響とその対処法がわかれば業界として危機感が上がる。既存ビルに比重を置いて欲しい。

（２）設計／発注時点でセキュリティを組み込むことについて

- 設計（仕様）とテストの組み合わせについて、ディベロッパー、サブコン、機器メーカーのコミュニケーションが取れていることが重要。現状では、コミュニケーションはとれているが、セキュリティの話はほとんどされていない。ビッグオーナーでもセキュリティの知識がなく、相談する先がないので、施設をよく知っているベンダーやサブコンに相談にのってもらいたい状況。様々な検査の際、ゼネコンやサブコンが集まり方針を決めるということは実施しているので、そこでセキュリティの議論も出来ると良い。設計段階で仕様をセキュリティの観点からブレイクダウンし、細かいチェックができるように。
- ビルを建てるときの発注は、個別設備毎に専門分化しており、ネットワークの専門家が横串でチェックできる体制にない。相互にコミュニケーションがとられないまま、ベンダーがそれぞれの仕様でセキュリティのブラックボックスをあちこちにちりばめている。BA やネットワークの構成に対し、「ネットワークをどうセキュアにするか」という観点で、ビルオーナーが明示的に発注する概念がない。建築・現地・設計書を横串でつなぐ発注ジャンルが必要である（例：BA の中央監視を設計する際、ネットワークに関しては素人の機械設備担当が発注することになるので、自動制御メーカーの助言を得るべき）。

（３）ビルに求められるセキュリティ対策の位置づけ／あり方

- ビルのグレードを決めるようなものになると、テナントによるビルの選別にも係わってくるので、その点で

は慎重な議論が必要。

- 発注者の立場から見ると、通信分野の優先順位が低い。そこを強化するにはビルオーナー側のチェックが必要で、ビルオーナー側が持つべきガイドラインやチェックリストがあるとよい。オーナー側とテナント側のシステムがつながっていることによる考慮すべき項目、建築を伴う設備機器がある場合の調達時のチェックなどは、議論すべき事項である。
- ビルを守ることは、一つの街全体を守ることに等しい。全てを守ることは無理があり、本当に守らなければならないもの、クリティカルな部分がどこかを想定すべき。すべてのビルを対象にすることは難しいという点では、狙われやすい種類のビル（競技場、空港、データセンターなど）にとって参考になる指針にしてほしい。既存物件に関しては、追加的セキュリティ対策に、それなりのコストが掛かる。対策の優先順位が必要。
- オリパラに向けて、いつまでに何をすべきなのかを時間軸で示して欲しい。その際、対策の具体的な選択肢が示されると、実効性が上がる。
- 建築主と設計者がお互いに会話をするベースとなるガイドラインがあると良い。ガイドラインがないと、安価という観点だけでシステムを組みがち。また、既存のビルのセキュリティホールが判断できるものになってほしい。脆弱性がわかれば、それぞれ補強すればよく、経営判断で投資すればよい。ただしセキュリティホールの判断が難しいので、専門知識の養成も含めたガイドラインの使われ方が望ましい。
- セキュリティをコストではなくプラスアルファの価値としていきたい。BA 関連機器(ネットワーク、センサ、アクチュエータ等)の ID 管理体制を整備することでセキュリティに留まらない価値向上が期待出来（例えば、デジタルサイネージ、照明、スピーカー等を組み合わせ制御すれば、普段の便利さも、災害時の避難誘導の質も向上する。各部屋にある空調の温度変更の履歴をフィードバックさせる事で、ビル全体が学習し自然と最適な空調環境が実現される。）、周りを説得しやすくなる。ビルの新しい価値を考えて、IT の進化に伴ったスマートビルのあるべき姿を考えるのも裏のテーマとしてほしい。

(４)検討の進め方、その他内容へのコメント

- 電力のセキュリティガイドラインでは、プラントオーナーからでてくるセキュリティ要件が数十ページに対し、ブレイクダウンしてその対策を作ると数百ページの仕様になった。ビルでは紐解く規格が未策定なのが課題であり、JESC 電力が参考になると思う。必須項目と推奨項目があり、企業の体力に合わせて組み合わせることができる。
  - 一方、電力とビルでは、オーナー、テナントの意識が違うので、運用も異なるものとなる。ビル業界における ISAC を設立し情報共有を図ったり、SOC や CSIRT を(同一組織や特定地域における)複数のビルを跨いで共通して運用する方法も考えられる。サイバー攻撃が起こった時の BCP 上の問題も入れられるとよい。
- IT 関係の図面管理が重要。図面がないと、ウイルス感染の復旧に時間が掛かる。大規模ビルでは図面更新が義務付けられており、工事のたびに更新するが、IT 系の図面についてはよくわかっていない。小規模なビルでは竣工時の図面しか残っていない。機器のアクチュエータの ID 管理も確認すべき。そこからアクセス管理をして、次に一番守りたい部分はどこかを考えられる。BIM のように、配管、

配線等の情報を持つことと同様に、セキュリティ対策においても機器等の情報を管理すべき。

- セキュリティを高めたあとに、マネタイズができるのかという点についても議論すべき。

（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