産業サイバーセキュリティ研究会　WG1　ビル SWG（第３回）　議事要旨

日時　：　平成 30 年 6 月 11 日（月）　14 時 00 分～15 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
日本電信電話株式会社
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．空調分野におけるサイバーセキュリティへの取り組みについて
２．ビルネットワークベンダからのビルセキュリティへの要求について
３．ガイドライン素案作成作業について
４．自由討議

要旨　：

１．空調分野におけるサイバーセキュリティへの取り組みについて

- ビルの空調機器メーカーだが、海外での事業比率が高く、海外の規制等の影響を受ける事業環境にある。
- 5～6 階建て程度のビルであれば簡易的な空調コントローラを入れる。こちらでは、遠隔監視にはダイヤルアップ回線の利用が多いが、一部ではインターネット回線も使われている。サービスマンが USB やLAN 経由でデータを取り出すこともあり、そこからウイルスに侵入される恐れもある。また、過去には取扱説明書で「お客様のほうでセキュリティを確保してください」と書いていた。以前のシステムは、安全なネットワーク環境で使われることが前提で、機器側は何もセキュリティ対策を実施していなかった。
- 状況が変わるきっかけは複数ある。まず、日本の国際空港でシステム障害のためにエアコンが止まることがあった。
- 欧州に関しては、GDPR は要注意で、欧州以外でも適用されるため、グローバルでやらないといけない。事故が起きた時の対応が悪いと最大で４%の制裁金が課されるので、売上高が２兆円ならば 800 億円取られる可能性が出てくる。NIS 指令も見落とされがちだが、欧州各国に情報セキュリティに関連する国内法の整備を要求しており、欧州の家電機器委員会の議論を見ていると機器メーカーにも波及する可能性がある。
- アメリカでは国防総省の調達基準で、ビル用マルチエアコンに対するセキュリティ対策要求が強化されてきている。まず 1 つが、BACnet DDC (Direct Digital Control)、LonWorks DDC 以外の通信プロトコルを認めないというもの。日本の空調機はみな独自の通信プロトコルを採用しており、中身をメーカーが握っているので、政府が手を出せずに困るというもの。一方、アメリカのセントラル方式の室内機・室外機は BACnet に対応しており、何かあったときには政府として制御可能であり、この方式でないと認めないと言われている。この基準は世界中の米軍基地に適用されるので、日本国内の米軍基地でも同様に影響が出る話しである。２つ目は、NIST 標準への適合の課題がある。SP800-171 では、サプライチェーンまで対応が必要と言及されている。FedRAMP、政府調達基準全般にこういう動きがあり、空調機の市場としては、学校・病院など政府調達の比重も高いため、今後、社内基準の整備を行う予定である。
- 中国については、今年 3 月の展示会でネットにつながる製品が出て来るなど、今はネットにつながら

ないと売れない状況である。一方で何かあったときにはメーカーが責任を取ることになるので、いろんな制裁を受けたり、ブランド力が低下したりする可能性ある。

- 現在ではセキュリティに対する認識をだいぶ高めている。空調機は重要インフラの構成要素であり、仮に原因が機器になくてもエアコンが止まって何か起これば責任を問われるリスクがある。このため、事故が起こったときに責任者に情報が集まって緊急対応が取れる体制を構築している。また、PDCA サイクルを確立し、設計基準や運用手順にセキュリティ要件を反映させている。空調部門のセキュリティ設計基準を作り、この春から開発に適用している。
- 対策としては、防御のための対策と防御が破られた後の対策がある。防御対策としては、使ってないポートの無効化、OS の保護対策、不要な通信が増えたときの警告など。破られた後の対策は、ローカルの手元操作を優先する優先順位設定や、ユーザーへ通知する機能の組み込みなどがある。また、確実に守りたい機器を置いてある部屋については、冗長構成とし、ネットワークにつながってないエアコンが温度センサなどで自動運転するようにもしている。
- JDCC のリファレンスガイドを元に考察も行った。従来はお客さん側の対策が大半だが、今後はいろんなリスクをお客さんにお知らせするのがメーカーの責任になると認識している。機器、クラウドの両方で基準に従った対策が必要であり、顧客、メーカーの両方が、それぞれ責任を持って取り組む必要あると全社で認識した。

２．ビルネットワークベンダからのビルセキュリティへの要求について

- グループでセキュリティのガイドラインを策定して、階層的にグループ会社、子会社、孫会社をガバナンスしている。これに基づいてグループ各社がそれぞれの規定やガイドライン、マニュアルを独自に作っている。グループ全体は大きい組織なので、各社が全く同じルールで運用すると上手く回らないところもあるため、サイバーセキュリティやフィジカル、マネージメントのシステムで、ここだけは共通的に守りましょう、というのを決めている。
- ビルのガイドライン作成に当たっては、単にガイドラインの文書を作るのではなくて、リスクアセスメントに基づいた運用を重視すべきである。近年のサイバー攻撃は次々と新しい脅威が発生し、攻撃者が優位な状況にある。例えばランサムウエアなどは 3 年前には想像もつかなかった。システムの現状、新しい脅威に含まれるリスク、攻撃を受けたときの被害予想、そして守れるのか守れないのか、運用を含めた対策について検討し、そのリスクアセスメントで得られた知見や結果をルールに反映させるという、定期的な更新のルーチンを回すのが重要である。
- ビルはマルウエアへの感染を考慮していない運用がされている。感染する前提でリスクを常々考える必要がある。
- 昨年、あるビルを対象にサイバーセキュリティのアセスメントを行い、課題を検討した。
- ビルセキュリティは IoT セキュリティの延長線上で見る必要がある。これまで主に見ていたのは、OA のセキュリティであり、例えば標的型攻撃で感染して、情報が外部漏洩するのを最大のリスクとしていた。これからは IoT の世界で、可用性に対する攻撃をもっと重視し、リスクアセスメントをしてリスクを減らしていかないといけない。

- 攻撃価値の高いビルも数多くあり、確信的に狙われると防ぐことは厳しいのが現状である。ホームページなどのインターネットにつながっているシステムは、日々いろんな国からポートスキャンされており、少しでも脆弱性があると乗っ取られる。ビルでもこれからは同じことが起こり得る。
- 実際のアセスメントを行った中で感じたビルセキュリティの課題が幾つかある。
- まず、ビルでは、BACnet などの IT では普段使わないプロトコルが使われており、暗号化もされていない。このため、既存のセキュリティ機器で守ることができず、また、それらの機器を無秩序に導入すると、必要な通信を阻害しビルシステムが動かなくなる。
- また、機器のライフスパンが他の IT 機器とは全く違う。一度使い出すと数年、数十年使うものもあり、しかも IT の世界だと頻繁に実施する OS の更新等が困難で、機器やシステムに手を入れることが出来ない。
- 更に、物理セキュリティの掛け方もビルの世界は固有である。普通のオフィスはセキュリティゾーンが設定されており、通りがかりに攻撃することは困難だが、ビルの場合はサイネージや部屋のカギは、少し工夫するとつなぐことが出来たりするので、もっと幅を広げて考えないと守れない。
- そして一番大きいところが、ビルシステム、機器のアセットマネジメントの問題である。ビル内に、どの種類の、どういう通信接続の機器が、どれだけ入っているか、全体で把握しているケースがなかなかない。各システムが縦割りで入っているが、全体を管理できていない。全体把握、アセットマネジメントした上でアセスメントしていくことが必要である。
- IT はここ数年、感染が前提で、感染したときにどう被害を出さないか、というオペレーションになってきている。一方、ビルは今のところ感染しない前提で作られており、例えばネットワークの設計が、ビル全体でフラットだったりする。配線統合などもやられているので設定を間違えると横のシステムにつながったりする。建築するときから通信についてしっかり考える必要がある。また、既存ビルでもアセットのアセスメントをしたうえで適切な設計を考えるのが有効である。
- また、アウトソースの活用も考えると良い。日々刻々と変化する攻撃手法を自力で監視するのは難しく、専門家の活用も 1 つの方策である。
- まとめると、アセスメントをきちんとする、日々ネットワークを監視して何が起こっているかを把握、業界全体でセキュリティにコストかけてバイデザインでやることが重要だと言える。

３．ガイドライン素案作成作業について

- ガイドラインの素案作成を効率化するため、少人数の作業グループにて作業を開始し、これまで 2 回開催している。まずはビルオーナー、ゼネコン、サブコンの一部メンバーを中心に作業しているが、ステークホルダーが広まったり狭まったりするので、その都度メンバーに声をかけることを考えている。
- 素案作成に向けた概念レベルでの整理としては、まずリスクを捉えたうえで、ポリシーレベル、対応策レベル、実装レベルという形で積み上げてブレイクダウンをしていく。また、ビルは設計から活動終えるまでのライフサイクルが非常に長い。リスクがライフサイクルのどの段階まで響くものなのか、それも視野に入れて整理を行っている。
- これまでも説明しているように、JDCC で 21 の管理策をまとめているので、これをスタートポイントとし、

これをベースにブレイクダウンを進めている。

- WG1 において、サイバー・フィジカル・セキュリティ対策フレームワークの原案を提案している。第一層、第二層、第三層とマルチレイヤーでアプローチをかけている。このアプローチはアメリカでも注目されており、パブコメでも、マルチステークホルダーに対応するアプローチが正しいという意見がアメリカから来ている。第一層は従来型の企業間のつながりであり、ISMS でそれぞれ確認できる世界である。発注先とメーカーの両方が存在し、マルチステークホルダーで見ていかないと IoT の機能の維持が管理できない。第二層は機器を含めて正にマルチステークホルダーの世界である。第三層はデータを自由に使うとなるとさらにステークホルダーの範囲が広がっていく。
- フレームワークを使って、ガイドラインの抜け漏れチェック等が出来ると考えている。現在の JDCC の 21 管理策に適用してみると、第二層の機能、つまり IoT の転写機能が充実していることが分かる。一方で、設計・発注などの組織の信頼性や、データの活用を射程に入れた場合のデータの区分管理などは、追加で必要ではないかと言える。
- 実際の作業としては、リスクポイントの洗い出しから始めている。例えばBA 装置の設置場所。BA 装置へのアクセス制御、フィールド機器や配線の保護という大枠に対して、個別のリスクを洗い出して、最終的なガイドラインの形にしていきたい。
- 今後の作業方針としては、まずライフサイクルごとにポリシーレベルで対策を整理する。現在、SWG の中で一番マルチステークホルダーの形状をとっているのはビル SWG であり、ステークホルダーについてどういう形で対策に関わっていくのか考える必要がある。ポリシーレベルで整理ができたら、さらに対応策までをガイドラインの共通編骨子としてまとめて、インデックスとして使える形とする。その上で実装に落とし込む。夏を目標にガイドラインの共通編骨子を示せるようにしたい。

４．自由討議

（１）空調におけるセキュリティ課題

- 空調と GDPR に関係があるのか。
- グローバル IP アドレスが個人情報となる可能性を懸念している。答えは出ておらず、リスクを否定出来ないので、個人情報として扱っている。
- 情報をどこで管理しているかが問題で、ヨーロッパ域外に行ったときのことを考えて管理する必要がある。
- 開示と公開の違いに留意が必要である。開示はチェック出来る資料を示せということで、公開ほどきつくない。
- 最初はオープンプロトコルを使いなさいということで、公開のニュアンスが強かった。
- NIST は開示したときにサイバーセキュリティをクリアランス出来るかを見ており、そこを守っていれば公開プロトコルでなくても大丈夫なはず。
- NIST と国防総省ではレベルが違う。NIST はそれで通じるが、DoD は最初はダメと言う話しだった。
- プロトコルの内容開示の要求と、NIST SP800 への準拠の要求は性格が異なる。NIST 標準に関しては、空調設備を役所に入れるとなると、役所自体が 53 に対応する話しになる可能性がある。設

計情報の一部をベンダが 171 で管理するのか、役所のビルで使うので役所として 53 で管理するのか、その辺が混じっている。

- やり過ぎないようにすること。やらなくて良いことまでやると、産業界にとってはマイナスとなる。

（２）買収先へのガイドラインの浸透

- 買収した会社にどうやってガイドラインを浸透させるのか。今まで関わってこなかった人達に、どのように共有しているのか。
- 海外買収の場合、買収されたというよりは、パートナーになったという認識が強く、言うことを聞かない。それぞれの国情や事業形態とすりあわせる泥臭いやり方が必要になる。
- 買収時の契約等でガバナンスを効かせるというよりは、コミュニケーションベースでやることが多い。

（３）ガイドラインの作りについて

- ガイドラインの作成で、ライフサイクルを考えて、設計、製造、竣工、運用の終わりまで考えているのは良い。
- 運用をやっている人の意見も取り入れて欲しい。運用者の視点でいろいろなチェックが必要である。
- ガイドラインに盛り込むべき個別の要求をどんどん寄せて欲しい。SWG メンバーは、経験上、こうすれば良いというのを沢山知っていると思うので、プラクティカルな対策とインシデントを沢山入れて欲しい。
- 作業グループは施主が発注するときに使うチェックリストを作るのがミッション。失敗経験などをインプットしてもらえると作業しやすいと思う。
- ガイドラインを実際に手に取るのは、現場の作業員か。現場で手に取れる感覚で分かりやすい物になると良いと思う。

（４）ガイドラインの 1 次的対象者

- ガイドラインは誰に見てもらうものか、誰に読んでもらいたいものなのか。お金を払うのはオーナーなので、オーナーが自分のビルで出来ていること、出来ていないことを確認するための物という考えがある。
- お金を払わないと誰もやらないし、コストも掛かることなので、オーナーが見るべき物だと思う。
- コストに見合ったインセンティブが必要で、一定の評価を与えるルールがあるとなお良い。一定の評価があるものが、テナントから選ばれる仕組みがないと、オーナーは一生懸命やらないだろう。
- オーナー以外だと、誰がガイドラインを見るか。
- 全員見ることになるが、一次的にはオーナーだと思う。オーナーがリスクに気がつけばお金を出すと思う。
- あまりお金が掛かると浸透しないと思う。常にインセンティブを考えないといけない。
- 最後は、所有者、貸主として、施設を守っていくガイドラインという位置づけか。
- その位置づけで良いと思うが、お金のかかることは採用してもらえないのは同じ。
- 国と民間で要求レベルが違うのと同じように、所有者のステークホルダーに合った物を作り、ソリューションを提供しないといけない。施主はどういう制度があるとお金を出す気になるか、有効な基準を実現

するための「何か」を知りたい。

（５ａ）個別の要求について（システムの作り）

・ オーナーの立場からは、外との出口だけはしっかり守るが、建物の中のプロトコルはオープンで、全てのシステムがフラットな方がありがたい。ビルに固有の素数 ID を持たせ、管理サーバにも素数 ID を持たせ、そのかけ算の暗号としてやりとりすれば、今のコンピュータの能力では破れない。外の通信は安全に出来る。

（５ｂ）個別の要求について（攻撃パターン）

・ リソースを知らない間にマイニングに使われたり、情報を少しずつ抜かれたりしているというケースもある。

（５ｃ）個別の要求について（機器管理）

・ アセットマネジメントとして、機器１つ１つの種類、型番、IP アドレス、設置場所が分からなかったりする。テンプレートがあって、管理すべき項目が明らかであれば分かりやすい。

（５ｄ）個別の要求について（ログの管理）

・ 最近は突然止まるのではなく、じわじわ止まる。ログの保存期間が足りずに遡れないこともある。どのくらいのログが適切か分からない。
・ ビルシステムのログデータは誰が管理するものか。
・ 契約時に施主として指定する問題である。最終施工図面を要求するのも、どのデータを取るか指定するのも、最初の契約時に施主が要求する必要がある。取ったデータをサードパーティに渡すかどうかは施主が判断すること。
・ ビルのログをどこまで取るかは重要。今は機器のオン、オフくらいで、誰が作業したかは入っておらず、サイバー攻撃への対応が出来るレベルではない。かといって、何でもログを取るとすごく重くなり、保存先の問題も出てくる。ベンダと目安について相談する必要がある。
・ IT の世界では、このくらいのログが必要という蓄積がある。その業界がどうやってキャッチアップして行くかという話であり、実装の制約や秘匿上の条件などを関係者でまとめるのが良い。
・ ログの話しは、ベンダの立場からは、捨てる基準がないので、全部残すことになっており、コスト負担の問題にもなっている。
・ ログに関して、法務省のページでは公衆通信の記録は 90 日間と言っている。参考に出来ると良い。
・ 現実に 90 日で可能というのは良い情報だと思う。

（５ｅ）個別の要求について（要員の管理）

・ 人の認証も重要である。多くの業者が管理室に出入りしており、人を特定して、その人の資格情報や操作記録等を個人レベルで管理出来る必要がある。単独の自治体や民間では難しいが、将来

的にはやらないといけない。

- パーソナルクリアランスが一番難しいハードルだと思う。プライバシー問題に踏み込まないためには、人を特定せず、行動と結果を紐付けるようなやり方を考える必要があり、そういう研究もされている。課題への解決策は 1 つではない。
- サプライチェーン上、パーソナルクリアランスは必要だが、管理ルールよりは、チェックシーケンス、プロセスをどうするかということになる。やり過ぎると、個人情報保護法やGDPRの問題になるので、やり過ぎないように。
- 最近は画像認識の技術が上がってきており、行動分析により変な行動を見つけ出すのは十分可能になってきている。個人特定が難しくても、こういう技術を積極的に取り入れると良い。

（５ｆ）個別の要求について（古い機器への対応）

- セキュリティの棚卸しをすると古い機器が大量に見つかる。改造での対応はコストが高く、多くの場合は運用でカバーすることになるが、単独のオーナーでは解決出来ない問題である。業界としての取り組みや、何らかのプラクティスが共有されると良い。
- 現実に相当古い機器を使っており、それをやめようというガイドラインは作れない。運用として守るなら、こういう体制で守りましょうとなる。新築ならば古い機器は使うなとなる。
- 古い機器については、1 つの機器の中でもマルチステークホルダーになっているという問題もある。社内のガイドラインとしては、社内の IT、商品・サービス、生産レイヤーに分けている。

（５ｇ）個別の要求について（インセンティブの例）

- インセンティブの話しだが、セキュリティのレベルによって保険などで差が付くのは分かりやすい例で、差別化に使えると思う。

（６）まとめ

- 基本的に施主側に対しての視点からのドキュメント作りを行う。
- 中身はステークホルダー全体が読めるものとする。
- 短期の対策と長期の対策も区別して整理する。
- メンバー各位の経験的な提案があれば積極的に事務局に寄せて欲しい。ガイドラインに入れられるものは、入れるようにしていく。今はここが危ないから気をつけるべき、という非常にプラクティカルな物が作れると思う。

（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