産業サイバーセキュリティ研究会　WG1　ビル SWG（第 12 回）　議事概要

日時　：　令和４年３月４日（金）９時 00 分～11 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
NTT グループ（株式会社 NTT ファシリティーズ）
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（欠席）
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（欠席）
一般社団法人ビルディング・オートメーション協会
株式会社日立製作所
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
ICSCoE２期ビルチーム有志

（オブザーバー）
国土交通省（総合政策局情報政策課サイバーセキュリティ対策室）
内閣サイバーセキュリティセンター（東京 2020G）（欠席）
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（欠席）
中部国際空港株式会社（欠席）
中部国際空港施設サービス株式会社

議題　：

１．各構成員より挨拶・1 年間の取組について報告
２．ガイドライン活用事例紹介
３．ガイドライン・個別編（空調編）の検討について
４．インシデントレスポンスの検討について
５．自由討議

要旨　：

1.　各構成員より挨拶・1 年間の取組について報告

・　顧客とのやり取りにセキュリティチェックシートがあるが、この 1 年間で増えたという感覚はない。ただし DX が推進されるなかで、自社提供システムと顧客システムの接続が増えてきている。
・　顧客との間でセキュリティ対策の話はかなり定常的に出てくる。
・　顧客からビルの設備ネットワークのセキュリティについての問い合わせが数件あり、ビル SWG で検討したチェックリストを使って話を進めている。
・　ビルのネットワークの接続状況について、チェックリストをもとにした確認作業を数ビルで実施した。
・　ガイドラインの活用は増えてきているとは思うが、現場の技術者の知識や理解度はまだ上がっていない。建設業界は慢性的に技術者不足が続いており、ビルシステムの試験に十分な時間が取れない。
・　設備面のチェックリストを作成し、数件のビルについてチェックを実施した。今後さらに対象ビルを広げていく予定である。
・　ビルシステムに不正端末が接続されたことを検知する仕組みを一部のビルに導入した。これまでは机上や実証実験レベルだったものが、実装できるレベルになってきた。
・　ビルにとどまらない公共空間の利活用やスマートシティ関連、ロボット利活用のときのビルの設定など、少し複合しているところについて、流れを作ってほしいという声が聞こえている。
・　最近は現場では、サイバー空間とフィジカル空間を融合したセキュリティについて言うことが多くなった。
・　見積もりの要件仕様にはまだサイバーセキュリティの要件は載ってきていない。新築でそういう取り組みへの浸透は薄い。
・　ロボットやセンサーをネットワークにしたときのセキュリティはこれからの課題になると思う。可用性の観点からビルの複雑化に伴う障害の増加も課題になっていくと思う。
・　最近はアクセス制限や物理的にネットワークを切り離すことで守るという意識から、認証されたメンバーに囲われた中で安全なコミュニケーションやデータ共有をするという形に変わってきている。

- 社内向けのビル制御システムに関する指針をブラッシュアップした。また、物件全てを対象に、チェックリストに基づく点検を実施した。ファイアウォールの設定を厳格に運用する取組や、それでも入られることを前提として検知する仕組みの導入を始めている。
- ビル建設の現場において工事や設計の段階のセキュリティ対策をガイドラインに基づいてチェックしているが、まだ何か壁を感じている。
- 最近は実際のプロジェクトにおいて顧客からガイドラインに従ってやっていきたいとか、設計書に反映して欲しいというリクエストを受けることが増えてきた。社内でチェックリストを作り、プライオリティをつけて着実に反映していくよう進めている。
- 取組の状況には温度差があるということで、かなりアクティブに行っているところ、あるいはまだマーケットの方が反応しておらず受身のところもある状況だと分かった。

２．自由討議

（１）トリアージについて

- インシデントレスポンスではトリアージが必要だが、実際にやるにはかなりの知識が必要で、BA システムや IT の知識、その経験も必要になる。
- BA 運用の現場はトリアージの知識はない。システムやネットワークセキュリティの会社は BA に詳しくないので、一緒になって高めていく必要がある。
- インシデントレスポンスにおける保全だが、粒度の問題として切り分けができると良い。末端のシステムはクリーンインストールして、最低限のコンフィグさえあれば原状復帰できるという考えもあるので、局所最適化されたパッケージングが進んでくると、現場の負担感は軽くなると思う。
- 機能安全の観点から設計で安全側に倒すようなアルゴリズムが予め入れてあれば、インシデント対応に反映させられると思う。
- ビルのコントローラもリブートすれば元に戻るのだが、個数が多いので、遠隔実施を考えないといけない。細かいパラメータの再調整の部分まで入れる仕組みを作れば、ビルの予防策として使えると思う。

（２）コミュニケーションと認証について

- BIM とか CAD などを共通のプラットフォームに載せて情報共有すると良いが、現場はまだエクセルとかで、そこに大きな乖離がある。本当は BIM を共有できると美しいが、その途中段階でも、今ある共有基盤に認証の枠組みを用いてデータ共有を実現すると、物事が進むようになると思う。多くのステークホルダーがいるビルでは、大手デベロッパが認証基準を示して、プロジェクトごとに関係者のアカウント管理をして、その中で業者同士のデータの引き継ぎが行えるようになると大きく前進する。
- インシデント対応の中でコミュニケーションの話しも大事である。

（３）現場意識の乖離について

・ ビルの現状との乖離は大きい。トリアージをするにはインシデントに気付く必要があるが、そのためのツールがビルのシステムに入っていない。BA 全体として IP を使っていても、全てが 1 つのネットワークにつながっているわけではなく、別々に細かなネットワークが多数存在している。IT の世界ではあたり前のものが、BA や OT の世界では乖離している。こうしたいという理想形があるが、そうできないという事情が広くあるのが現場の肌感覚であり、業界をあげて意識を変えていかないと難しい。
・ 関係者に問題意識を持ってもらうことは、非常に重要な仕事になると思う。経営サイドの必須条件として意識を持っていただくことも重要である。現場の意識の乖離については、ガイドラインとは別に議論をしないといけない。

（４）ロボットや他システムとの連携について

・ 最近、ビル業界で挙がっているユースケースとしてロボットがエレベーターと連携するというのがある。悪いことをやろうとすると、ロボットがセキュリティラインを越えて人に替わって情報を窃取することが考えられる。システム・オブ・システムで考えてリスクを見定める方向になっていけばと思う。
・ ビルでいろいろなロボットを試験的に使っているケースや、実証をしたいという話はある。ロボットでエレベーターを呼びたいという話になり、どのようにつなぐのかというと、インターネット経由でつなぐという話が無邪気に出てくる。
・ 自動運転車がビルの駐車場に入ってくるようになると、ビル側と通信をしないと駐車場に入れないという話が出てくる。今後 DX が進むと、ビルと外部との通信は必須なものになるので、少なくともビル内でしっかりと外部との通信ルールを決めておかないと危ないことになる。
・ 一時期はビルに安価なモニタリングセンサーが大量に付けられた時期があった。現在、BA にもいろいろな新しいものがつながってきているが、一般ビルほどそういうものを安易に導入する傾向がある。ビル SWG では、一般ビルに向けたリスク喚起のような提言も必要になるかと思う。

（５）エレベーターのセキュリティについて

・ エレベーター業界でもインターネット経由でロボットとつなぎたいという話が持ち上がっているが、ロボットを作っている相手メーカーの素性がわからない状況で繋ぐ必要があるケースが出てくることを懸念している。その点を踏まえて、エレベーターのセキュリティをどう担保するかという議論が始まろうとしている。
・ 海外では、エレベーターが Amazon のインターネットサービスとつながっているケースや、オープンネットワークとつながるケースが増えてきている。ISO でもエレベーターをどのようにセキュリティから守るかの基準策定が現在進行中である。
・ 昇降機個別でオープンネットワークからの操作を一定レベルで止めることや、ディフェンスするシステムを組んでいかないと防御はかなり難しいと思う。この辺のセキュリティ対策はこれから大きな課題になる。
・ 今までクローズドだったことを安全の理由にしていたエレベーターが変わりつつあるということだと思う。その際に認証の基盤をしっかりと埋め込みなさいという話で、ゼロトラストを含めた認証の話しが進むと健全な方向に向かうと思う。

- 認証後の振る舞いも考えないといけない。悪意をもってロボットがエレベーターを操作すると、ビルの交通量を遮断することも論理的には可能になるので、運用面も含めて議論をしないといけない。
- 一歩一歩最終ゴールを見据えて上手に業界に展開していただいて、今回空調でやったようなことをエレベーターでもぜひ進めていくということだと思う。
- こういった機会にエレベーターのチェックリストが加速できればいい。

（６）一般ビルでのインシデント対応について

- データセンター協会でインシデントレスポンスのガイドをまとめるにあたって、細かい議論や深い議論があって今のものになっていると思うが、一般のビルだとさらにシュリンクさせないといけない。
- どの段階で、何をもってインシデントと認識するのかという判断の課題がある。インシデントの予兆を捉えるために、通信のモニタリングや機器認証の議論は出たが、一般ビルに適用するのは厳しすぎる。その線引きについて、一般ビルによってもレベルがあると思うので、そういう議論が必要である。
- ビルの大きさによっても、インシデント対応をフルパッケージで内製化できるところと、そうではないところが存在しているのが悩ましい。大手はフルパワーでできるが、そうではないところをどうするのかという議論もやる必要がある。
- 何かがおかしいという状況が起きて、機器をメーカーに送って確認してもらったら、故障じゃなくてどうもサイバー攻撃だった、と後になってわかるケースが多いという話があり、検知が大きな課題になるという気がした。そういう点を含めて、どういうものをインシデントとして、特にサイバー攻撃として捉えるのかというところから、ビルではどうなのだろうという議論が必要だと思う。
- フルパワーでできないようなケースについても、中小ビルなどをクラウドで束ねて監視制御しているという話もあり、小さいビルなどはそういうところが束ねて面倒を見てあげることで、インシデントを捉えられるのではないかという議論にもできる気がした。
- 非常に細かいフルパッケージにすると取り組み意欲が湧きにくいので、ミニマムに出来るように、というのも考えている。
- ビルのサイバーセキュリティも大分進んで来ている一方で、大多数はユーザーもベンダーもそこまでは来ていないという認識が共有できたと思う。その対応をどうするかを考えて、ガイドラインの書きぶり、主張もシャープにしないといけない。

（７）FA との関連について

- 規模の話や DX の話しに関し、外との広がりのレベルとかも考慮して、マトリックスになると良いかと思う。FA の中で物理セキュリティもテーマになるので、このガイドラインともシームレスになるとありがたい。

（以上）