産業サイバーセキュリティ研究会　WG1　ビル SWG（第 10 回）　議事要旨

日時　：　令和 2 年 2 月 13 日（木）10 時 00 分～12 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（欠席）
株式会社 NTT ファシリティーズ
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（欠席）、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（欠席）
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. ガイドラインの内容補足に向けた検討
2. インシデントレスポンスの検討
3. 空調編の検討
4. 国際連携に向けた検討
5. ビルサイバー推進体制についての検討
6. 自由討議

要旨　：

１．自由討議

（１）ガイドラインの内容補足に向けた検討（全般）

- ガイドラインの補足情報などを公開する場合には、攻撃のヒントにならないよう詳細度の調整が必要である。また初心者向けには啓発活動を継続し、セミナー等で啓発することも必要である。
- 外に出せない情報は出さないようにする。活動内容を WG メンバーに限定するためには、ISAC のようにメンバー限定で動くことができるように、ビル業界が自らの活動として実施する必要がある。今後のガイドライン等の検討を行う組織体制についても検討が必要であり、情報の取り扱いについても並行して検討を行う。
- 推進体制の他に、情報に TLP を設定することが考えられる。CSIRT 協議会においては、チャタムハウスルールを導入している。
- 文書はほとんど誰も読まないので、デモによる実演が手っ取り早い。
- 対策マップのイメージとして、リスクの大小や対策の数で濃淡をつけるのはよい整理方法である。軸の選び方も重要で、リスクがどこにあるのかがわかるのがよい。
- ガイドラインの補足については、できるだけ運用者・設計者にわかりやすいものとするべき。セキュリティ上の危険性について説明すると運用現場にも理解してもらえるので、運用上の穴、対策がわかるようなものがあるとよい。セキュリティの重要性がわかるとガイドラインを見てもらえるようになる。
- ガイドラインを使用して、顧客のビルのセキュリティチェックをしているが、本文と別紙のどれを参照すればよいのか判断に迷う。用語についても定義や説明が必要だし、事業者同士で情報交換ができる場があるとよい。
- 現場の人にとって、セキュリティはハードルが高い。セキュリティの専門家ではないベンダーの担当者にも参考になるような資料があるとよい。
- 初心者のサイバーセキュリティに対する理解を促進するために、被害・インシデントをビルに落とし込んだ資料があるとよい。ビルのサイバーセキュリティリスクを把握することができるチェックリストがあるとよい。

- BA 配下、配下外を含めてセンサーが増加している。センサーからクラウドに直接データを送信して、クラウドから BA にコマンドが送信されるケースもあるが、そのコマンドは信用していいのかという疑問がある。

（２）ガイドラインの内容補足に向けた検討（アップデート課題）

- ビル管理機器のアップデートは難しいが、ネットワーク構成の把握がベースとなる。アップデート後には、機器の動作を確認した後に本番運用をスタートさせるが、確認方法や手順等についてのノウハウの共有が必要だと思う。
- ビルネットワークは、基本的にはインターネットから隔離されているが、コントローラのアップデートをインターネット経由で実施するケースも出てくる。メーカーによる機器の検証は実施されているが、ネットワークに接続する前に検疫を実施するようにしたい。

（３）ガイドラインの内容補足に向けた検討（コスト課題）

- ビルのセキュリティ強化のためのコストが増加しているが、価格（賃料）に転嫁するしかない。製造業などはどうしているのか。
- コストアップは不可避であるが、メーカーは DX とセットで判断し、総合的に対応している。
- テナントの責任でセキュリティ対策を実施させるか、賃料を上げてビル側で対応するかということになる。業界としてのコンセンサスとするのであれば、賃料を上げざるを得ないということになるのではないか。

（４）ガイドラインの内容補足に向けた検討（人材育成課題）

- ビジネスとしてセキュリティチェックを実施できるようになると良い。調達の評価項目に必須項目と加点項目があるが、両者のウエイトは、どのようなファシリティを対象とする調達であるのかによって異なり、その判断ができる専門家の育成にはコストがかかる。
- 現状、IT 分野と OT 分野で、専門家のスキルの違いが大きすぎるという問題がある。ICSCoE や CSSC の活用を検討するべきで、国のアセットをもっと活用できないか。

（５）インシデントレスポンスの検討（検知、対応、手順）

- ビルの場合、単なる機器の故障なのか、インシデントによる不具合であるのかがわからないケースが多い。現状、故障対応マニュアルはあるが、サイバーインシデントかどうかの判断ができない。サイバー上の事象で注意するべき兆候は何かがわかるような、現場に即したインシデントレスポンスマニュアルができるとよい。
- インシデント対応について、まず防御、監視しつつ、検知しようという体制を考えているが、攻撃を受けた場合、ビル全体を停止して対応するべきなのかの判断が難しい。侵入された後にどのような手順で対応するべきか、答えがない。
- ビル制御など監視体制を組むことができないところに、既存のものにボルトオンする技術が開発されているが、プロトコルが対応しているか、システムに互換性があるかの確認が必要である。検知が一番

難しい。構成管理ツールはあるが、ビルオーナーがコストを負担しないと導入できない。

- インシデント対応時のシステム復旧サービスは IT 向けのものはあるが、制御システム向けのサービスはまだない。現場での対応マニュアルも制御システムの内容を反映できておらず、故障した場合と同様に交換(リプレース)で対応することになる。
- 復旧する時に、構成情報の一覧がないと復旧ができないが、バックアップがどこにあるのかもわからないため、コントローラを初期化してもパラメータの設定値が分からない場合もあり、ネットワーク構成図については、ネットワークを設計・構築したベンダーに提出してもらうしかない。

（６）インシデントレスポンスの検討（体制）

- CISO がいないので指揮ができない。リスクシナリオの設定、リスク管理等ができる人材がいないので、インシデント発生時にビルを全て停止するかどうか、コーポレートガバナンスとしての意思決定ができない。
- CISO の育成については、米国の DoD のプログラムが、人材供給源となっており、ICSCoE でも実施している。
- インシデント時、どのような場合にネットワークを切断するのか、誰が何を行うのか等についてルールを決めておくこと、ネットワーク切断後のネットワークの開通等についても復旧手順を決めておく必要がある。CISO、CSIRT はインシデント対応に必要だが、ビル向けに参考になる資料がないので、この場で議論する必要がある。
- CSIRT に関するノウハウの共有はオーナーサイド中心で動いているところがあるが、ベンダーと PSIRT の連携も視野に入れる必要がある。脆弱性の公表については、ベンダーと調整して実施することになる。

（７）空調編の検討

- 文書作成の全体的なスケジュールはどのようになっている。個別編は、空調の他にも作成されるのか？
- 個別編については、作成して欲しい分野についてビルオーナーから要望があるとよい。
- 空調編の検討では、センサー、コントローラが加害者になるケースも考えるとよい。センサー、コントローラが乗っ取られた場合に攻撃に加担することになるリスクを追加するとよいのではないか。
- 攻撃の踏み台にされた場合、新聞記事になる可能性があることにも留意するべきである。
- 個別編では、別紙に相当するものや初心者向けの資料は作成するのか。
- 検討中である。個別編は、共通編との差分を整理するためのものという位置づけであり、詳細は作成しながら考える。個別編は、より専門家向けなので、初心者向け資料は考えていない。
- 共通編に対する別紙として作成しているが、設計・運用の部分については、共通編に合わせて書いた方が良いと考えている。

（以上）