

産業サイバーセキュリティ研究会 WG1 ビル SWG（第 11 回） 議事要旨

日時：令和 3 年 3 月 22 日（月）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
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
株式会社日立ビルシステム
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
ICSCoE 第 2 期ビルチーム有志

（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 東京 2020 グループ
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（欠席）／中部国際空港施設サービス株式会社

アライドテレシス株式会社

日立ジョンソンコントロール空調株式会社

議題：

1. ガイドライン・個別編（空調編）の検討について
2. 構成員よりの発表（ICSCoE ビル有志・森ビル佐藤様
3. その他報告事項
 - （ア）ガイドライン 2 年間の振り返りと課題の共有
 - （イ）インシデントレスポンスの検討に向けて
 - （ウ）レポジトリの充実化について
4. 自由討議

要旨：

1. 自由討議

（1）ガイドライン・個別編（空調編）の検討について

- 空調編において、読み手が手を付けやすい軽い対策も記載できるのではないかな。例えば、一定時間間隔で正しい温度設定値を再設定し続けると、攻撃があってもすぐに元の状態に戻すことが出来るので、緩やかにディテクションした後に、時間をかけて対応することが出来るというメリットもある。
- 空調システムとして、一定の設定値を入力し続けて設定温度を保つようなことは実現できる。何をもらって異常なのか、インシデントなのかを判断できれば、個別空調であればコントローラで把握して、ローカル側でインシデントへの対応が実施できるかもしれない。これまでも人間のミスオペレーションを想定した気温の上下監視等は実施しているが、将来的には攻撃等の検知にも活用できるかもしれない。
- 正常値に一定の幅を設定して一般ユーザのアクションも受け入れられるようにしつつ学習データを蓄積することで、ビルごとの最適化を行い、攻撃への対応時間を稼ぐということも実現できるのではないかな。

（2）ガイドライン・個別編の空調以外への展開

- 個別編について空調編以外の検討は既に始まっているのか。
- 空調以外の個別編はまだ検討を始めている。ニーズに合わせて検討を進めていきたいので、要望があれば挙げてほしい。

（３）ガイドライン・個別編（空調編）のよりハイレベルな記述について

- 本ガイドラインは普通のビルだけではなく、半導体等の最先端の産業用工場の空調にも使われる可能性があるため、安全性が強く求められるような工場や施設にも活用できるように記載を追加した方が良いのではないか。工場等の空調システム等が安全に高品質に正常に戻るまでに時間がかかることを考えると、システムを止めるという判断も難しいため、手順や管理者を設定しておくことも非常に重要だと考える。ビルガイドラインにそのような応用的な記載もした方が良い。
- 米国のペンタゴンがビルのセキュリティに神経質になっており、ビルシステムを納入するサプライヤー側が混乱したことがあった。こういった海外の先行的な事例をとらえ、今後のユーザのハイレベルな要求に応えられるような検討がなされているのかは気になる。
- ペンタゴンからのセキュリティに関する指摘に対応して、空調機のコントローラに対して同様の話が来ている。しかし、個社としての対応の詳細を空調編の記載と突き合わせるような確認は実施していない。今回の空調編にそこまで踏み込んだ記載をするという方向性に決まったら確認をしたいと思う。
- ビルガイドラインもそういった将来的な対応に資する情報も組み込んで、外に対してセキュリティの対応、検討を実施していることを示せるように可視化出来ると良い。
- DoD は以前、ワシントン周辺の民間ビルを借りていたが、ビルのセキュリティを危惧して、DoD 側で新しいビルを建設し、部署を移設して神経質に管理するようになった。同様に、サプライチェーンとリスクを段階ごとに検討していくような方向性にもなっている。このような検討を参考に、今後起きることのスピードについていくために、現段階の検討から少しレベルを高く、厳しく設定しておくべきではないかと考える。

（４）DPI（Deep Packet Inspection）ツールについて

- DPI ツールを試してみたが、古いバージョンの BACnet も読み取ることができて使い勝手が良いと思ったが、運用データを学習して異常検知に利用する機能については、ビルは季節変動によって温度設定の幅が非常に広いことから、学習期間が短いと使いこなすのが難しいという感想を持った。役に立つ機械ではあるが使い方の検討が大事である。
- 学習期間の重要性は認識している。しばらくはインシデント対応に活用するのではなく、検知してアラートを上げるためのものとして使用していきたい。
- DPI に関して、これまではキャプチャーしたパケットなどを対象に模擬的な実証実験等を実施していたが、これからは実際のビルを対象にしてツールを用いた実証を検討している。
- DPI やファイアウォールを入れたら安心と思う事業者が多いが、実際のビルで試してみて、より詳細な検討を進められると良い。
- 限定的だが、温度監視機器側でも年間を通してパケット監視によるチェックを実施している。ただし、何をもって異常とするのかの基準が明確になっていない。そこが明確になれば末端側でも監視が可能になると考える。

（５）インシデントレスポンスの検討に向けて

- インシデントレスポンスに関して、権限を文書化し、インシデントが発生した際に、マニュアルやルールに沿って、誰がどういったアクションをとるべきかを明確化してほしい。属人的な判断に頼るのではなく、文書に規定されている行動を、決められた担当者が行えるようにしておくことがスムーズなインシデントレスポンスの実現に繋がる。
- インシデントレスポンスについては、JDCC でインシデント対応ガイドブックを作成しており、それが完成次第、ビル SWG にも展開していきたいと思う。ただし、一般的なビルにとってはハードルの高い指標になっている。一方で、一般のビルの中でも厳しく管理する必要があるところにはあるかもしれないので、今後のビルセキュリティガイドラインの検討には、ビルのレベル別や規模別の対応検討が必須になってくると理解している。

（６）レポジトリの充実化について

- 今後ビルガイドラインに関して、まず始められるところとして、事例集のような形で充実させていくことから取り組んでも良いのではないかと。事例集であれば読み手からしても手に取りやすく、厳密なレベル分けもせずに始められる。
- 事例集であれば、全体を通した網羅性が要求されないので取り組みやすい。

（７）ガイドライン・ビル SWG の今後の検討について

- セーフティの観点からもインシデントレスポンスを考えていきたい。空調の例だと、熱源系は一旦止めて 30 分以内に再起動すると爆発するケースもあるので、そういう点も検討していきたい。
- ガイドラインについては、空調や受変電といった個別の議論を突き詰めるより、ビルの規模に応じて作成した方がオーナー側としては理解し易い。現状、普通のオフィスビルで起こり得るインシデントはそれほど重くないと考えているので、実情に応じたガイドラインが良い。
- 一方で昨今のビルはセキュリティだけでなく、CO2 削減や、ビルとして利便性向上も重要で、セキュリティと他の観点とのバランスを取りたくとも、その指針がないので検討を始めることが出来ない。さらにスマートシティへの展開が進む中で、セキュリティに関する落としどころや折り合いの付け方を示してほしい。
- ビルガイドラインとして、現場で使いやすさを求めると記載が詳細になってしまい、全体を把握しようとなると抽象的になって使い勝手が悪くなってしまうのが難しい点である。現場だけではなく全体をマネジメントしている側がチェックできるような体系化や体制を整えていくしかない。実際、ビルや機器の全てがサイバー空間に繋がっていく中で、枠組み全体を考え直さなければいけないということ自体に気付いていない事業者も多いので、議論を行い、定期的に情報共有していくことが大事である。
- ビルセキュリティのマネジメントの全体感が把握でき、サイバーセキュリティをどのように捉えるべきかを明確するべきであるとする。
- 実際にビルのセキュリティを誰がハンドリングしていくかとなった際に、ゼネコンや設計会社であるべきだ

という話がある。そこをうまく支援、盛り立てる仕組みは今後考えていかななくてはならない。

- EU で NIS ディレクティブの改正が行われ、人的管理やマネジメントだけではなく、調達機器のセキュリティ対応も求められるようになった。日本においてもサプライチェーンの影響が大きく出ると考えており、今後はビルでも最先端な事例では同じような要求が出てくることが想定される。工事や設備の統合体となるビル業界として、他業界の動きもにらみながらビルセキュリティガイドラインの検討を推進していくべきである。
- FA（ファクトリーオートメーション）の検討も既に始まっており、ビル業界として参考にできる部分もあると考える。
- FA では建物周りの電源や空調は抜けてしまうため、クリティカルな施設における電源や空調の検討はビル SWG で推進しなければいけない。

（以上）