産業サイバーセキュリティ研究会 WG1 ビル SWG（第 15 回）
議事要旨

会議： 産業サイバーセキュリティ研究会 WG1 ビル SWG（第 15 回）
日時： 2023 年 1 月 31 日 15:00-17:00
場所： オンライン開催（Teams 会議）
構成員（敬称略）：
（座長）江崎 浩 東京大学大学院 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（欠席）
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
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（欠席）
ICSCoE 2 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（欠席）

（事務局）

経済産業省（商務情報政策局サイバーセキュリティ課、製造産業局産業機械課）
株式会社三菱総合研究所

議題：

1．　開会
2．　各構成員より挨拶・１年間の振り返り
3．　インシデントレスポンスの検討状況について
4．　委託事業調査の中間報告
5．　森ビルにおけるビルセキュリティの取組について
6．　自由討議
7．　閉会

議事：

２．　各構成員より挨拶・１年間の振り返り

- 電気事業法の改正や個人情報保護法により、サイバーセキュリティ対策を求められるようになった。空調編の対応など、OT のサイバーセキュリティに地道に取り組んでいる。
- 顧客から建設設備のサイバーセキュリティに係る要望が増えている。全体的に意識が高まってきていると思う。
- SOC を備えたビルの計画を行っている。建設の観点からはサイバーセキュリティの意識がある程度進んできたが、運用の観点からはまだ実感がなく、サイバー攻撃の事例等の共有が必要ではないか。
- ビルオーナーからのサイバーセキュリティに係る問い合わせが増えている。
- 利用者のサイバーセキュリティに係る意識が高まってきていると感じる。脆弱性情報があると、システムへの影響や対応方法についての問い合わせを多く受けるようになっている。ユーザーの関心が高まっており、早いレスポンスも期待されているため、対応体制の強化を図っている。
- スマートビルや DX の問い合わせが増えており、付随して外部設備との接続とセキュリティに係る問い合わせが増えている。
- 不動産会社からクラウドシステムを導入する際のチェック項目が提示されるようになったが、対応に苦慮している。欧州では法制度化され、対応が大変になっている。
- 中小ビルでは、まだサイバーセキュリティの意識が高まっていない感覚である。
- スマートシティ、スマートビル、ビル OS が何をするのか、議論が活発になっている。CO2 削減も盛んになっており、セキュリティと合わせたビジネスが生まれそうである。

- 工場 SWG でサイバー・フィジカル・セキュリティ対策ガイドラインを策定・公開した。ビルと工場は両輪になると考えている。
- 建築設備設計基準に追加される設備では、エネルギー管理関係が多い。これらの設備はネットワークと関連するので注目している。令和 5 年版にはサイバーセキュリティ対策の記述を提案しており、本 SWG での議論をインプットしたい。
- ロボット導入や自動化のニーズが高まっており、クラウド連携が必要になっている。ヒヤリハットが発生しており、基本的な対策が重要だと実感している。
- IPA のデジタルアーキテクチャ・デザインセンター（DADC）ではデータ交換、認証技術なども含めて議論がされており、活動が盛んになっていると感じる。JEITA ではスマートホームの議論が行われている。建物とサイバーセキュリティの議論が多くなっているように感じる。
- ビル以外では、ランサムウェアが情報系のサーバーに感染して、制御系を止めざるを得ない事例が出ている。今後、クラウド連携がいろいろな分野で進化しつつあり、その辺りも注目が必要と思っている。
- 電気事業法対応の問い合わせが増えており、プロダクトのセキュリティ対策を本格化に取り組んでいる。顧客からの工場セキュリティに係る問い合わせも増えていると感じる。
- 共通編のガイドラインに倣って独自の OT セキュリティガイドラインを作成し、適合状況の点検を年 1 回実施している。電気設備のサイバーセキュリティ対策の対応をどうするか、検討中である。電気事業法の保安規定にどう盛り込むか、独自の OT のセキュリティガイドラインをどう変更するか、検討している。ビルにおいて一番リスクが高いのは、公開サーバーのある物件であり、悪い動きをした時に即座に検知できるようなシステム構築を進めている。
- 大規模ビルでは情報系の通信を利用する業者が増えており、ビル単体でも 30 数社になる。そのため、セキュリティの統制が取れない。業者による対応レベルの違いをどうするか、構築段階で頭を悩ませている。

3．インシデントレスポンスの検討状況について

（事務局より説明）

4．　委託事業調査の中間報告

（事務局より説明）

5．　森ビルにおけるビルセキュリティの取組について

（構成員より説明）

6．　自由討議

（1）体制について

- システムを止める場合に、本当に止めてよいのか、誰の責任で止めるのか。アクションを起こす場合の権限の明確化を整理しておくと良い。
- ビルのサブシステムで起こったインシデントで、ハンドリングを誰が行うかで時間がかかってしまったことがあった。ガイドラインでは、どのような関係者が統制を取るのが良いのか、触れてほしい。ビルオーナーか管理者かベンダか、ビルによって決めればよいと思う。
- ビルや企業の規模、対象設備により同一の施策は難しい。セキュリティ施策だけでなくインシデントレスポンスについてもレベル感が必要ではないか。

（2）ログ及びシステムバックアップの取得・活用について

- ログを取っておくことも重要である。ログをどう取って、分析・検索するのか、ログを取らなければできないことを示さないと、現場で実際に対応してもらえないのではないか。
- バックアップについては、取り方がポイントである。コントローラはリセットすれば戻ってしまうことが多いので、設定値のバックアップが重要である。
- バックアップは、基本的にはベンダに対応してもらうしかない。そのため、どこを対象にしてどこを対象外にするかを決めておく必要がある。頻度は、定期的にやることが重要である。これらは保守契約等で決めておくと良い。
- バックアップに対して、①誰が実施するか、②対象はどれか、③頻度はどのくらい実施するか、の 3 点について検討することを明記されると良い。

（3）ビル全体のシステム関係情報の整理について

- 「準備段階」で、ビルのシステム的に観た全体図を整理することを記載して欲しい。IT と同様に、OS やミドルウェアやバージョンも記載する必要がある。
- システムの全体像について、ネットワークの全体像（セグメンテーションなど）もあるとよい。少なくとも、誰に聞けば分かるかだけでも整理しておくと良い。
- システムの全体像は、現状では外部の委託がない。ガイドラインの中でも、準義務ぐらいに書くと、全体像を描くという作法が根付くのではないか。
- あるビルで全体像を描いたことがある。その時はネットワークから調べて作成した。いろいろな設備ベンダが入るため、全体像を作るのは、全体をまとめているゼネコンが良いのではないか。
- システムの全体像については、ニーズがあれば各事業者が対応するようになるのではないか。OA や FA 業界の事例を記載してはどうか。

（4）インシデント発生後の対応

- インシデントの起きた状況を社内の他のビルの部門と連携して、注意喚起を最初にやるべきではないか。自社だけでなく、協会等で共有できるとなお良い。

- ビルは可用性が重視されるので、根本的な対処ができなくても監視を強化して運用継続する、手動で運用することもありうる。
- 「c.封じ込め段階」の中で、「影響を受けたシステムは、切り離した後、詳細調査用データを取得完了するまではマシンの電源を切らずに置いておく」ことも、明記したほうが良い。電源を落とすと消えてしまう侵入痕跡もある。

（５）その他

- 「フォレンジック」と書くと重い作業に思われる可能性がある。目的を明確化してログを取る例を示すぐらいでも良いのではないか。
- インシデントなのか故障なのかの切り分けは困難であるが、BA システムがランサムウェアに感染したら何が起きるか等も記載してはどうか。
- 参考まで、故障をふくめて FTA を整理することが必要ではないか。
- ログは、なにを取るかを整理しないと「ログ貧乏」となるため、何を見つけたいからどのログを取るのかを整理する必要があると思う。

（以上）