産業サイバーセキュリティ研究会　WG1　ビル SWG（第 13 回）　議事要旨

日時　：　令和 4 年 3 月 28 日（月）　13 時 00 分～15 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）（欠席）
鹿島建設株式会社
株式会社九電工（欠席）
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（欠席）
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（欠席）
三菱地所株式会社（欠席）
三菱電機株式会社
横浜市
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

議題：

１．ガイドライン・個別編（空調編）の検討について
２．インシデントレスポンスの検討について
３．ビルシステムセキュリティに関する情報共有について
４．自由討議

要旨：

１．ガイドライン・個別編（空調編）の検討について

・　意見は全部出させていただき、基本的にすべて反映されている。

２．インシデントレスポンスの検討について

・　JDCC の資料のインシデント対応概要の中にフォローアップがあり、これが非常に重要である。インシデントの発生の後の報告や情報公開に関して、ビルシステムの業界では、きちんとした会社としての体制、ルールが、まだまだ出来上がってないのではないか。会社のガバナンスの中に組み込むことが重要である、ということを書き込むとよい。
・　インシデントレスポンスについて、実際にはサイバー攻撃によるインシデントなのか故障によるインシデントなのかの区別つかないということが大きな議論のポイントである。汎用的なインシデント対応フローのようなものを用意し、これをベースに各社で体制等を議論してもらうという方法もあるのではないか。
・　インシデントレスポンスで封じ込めをした後に、どのように報告するのか、自社内の経営層も含めるようなワークフローを書いてよいのではないか。事故発生時だけでなく、普段のオペレーションの中でも、未遂も含めて報告するパスを最初から組み込んでおくと、起きていることが経営層に自然に伝わっていくので、理解も得やすくなる等の良いサイクルが回ってくるのではないか。
・　データセンターのガイドラインは、事故が起こらないようにするということを前提として作られている。一方で、一般のビルの場合はそうではない場合もあり、復旧を早くするためのフローというものを意識してガイドラインを修正してはどうか。
・　どのようにして常時議論、情報共有ができるチームをつくるか、ということが非常に重要である。
・　ガイドラインの中に事例的に書き込めると、緊急性の高い、重要性の高いビルの守るべきポイントを中心に、インシデントレスポンスの対応フローの検討や、データのセパレーション等の封じ込めがやりやすいのではないか。
・　設計の立場、運用の立場からそれぞれ意見交換しながらセキュリティを考えることが今後必要であり、その体制が必要ではないか。ビルオーナーが全体の調整をして、運用側、設計側を含めた体制を組めると良いと思う。そのようなことを今後、ガイドラインや SWG の中で提案していきたい。

３．ビルシステムセキュリティに関する情報共有について

- どのようにして、ビルオーナー、ゼネコン、ベンダー間でコミュニケーションの事例を作っていくかということ、SWG に参加していない各社に向けて、どのように情報発信していくかということが重要ではないか。
- ガイドラインとしてつくられたものを自社のビルの対策に反映していくことが難しい、使う人に伝えていくことが難しい、というご意見も頂いている。これらの情報をいかに使う人にわかるように伝えていくか、ガイドラインの中身の質と共に教育についても枠組みとして考えていく必要がある。
- リスクアセスメントに関連して、優先順位が示されると良いのではないか。優先順位があると、設計の段階でどこをセパレーションしておけば良いのか等の設計方針を示すことができるのではないか。
- 運用に関連して、ログ分析基盤が心臓部分であると感じている。ログを残して検索できるようにしておくことで、すぐにアクションも取れ、事実を把握することができることにつながる。ログ分析基盤が丁寧に作られると、問題の切り分けから、判断からすべてが加速される。
- ビルシステムのログは、適切なものがとられていないのが現状だと思う。どのようなログをどのように取るのか、ベンダーと一緒に検討させて頂けると非常にうれしい。ビルオーナーだけではとてもできない話である。
- 機器の動作ログを取っていくことによって、機器の故障の予兆を発見する等の予防保全にもつながる。

（以上）