産業サイバーセキュリティ研究会　WG1　ビル SWG（第６回）　議事要旨

日時　：　平成 30 年 10 月 31 日（水）　13 時 00 分～14 時 30 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、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．昇降機分野におけるサイバーセキュリティへの取組み
２．ガイドラインβ版作成報告と今後について
３．海外のビルシステムのサイバーセキュリティに関する検討状況（中間報告）
４．自由討議

要旨　：

１．自由討議

（１）ガイドラインの今後の修正について

- 今回別紙について修正されたものが提示されたが、別紙についても今後修正意見を出すような機会はあるか。
- 随時、修正意見をいただければ、なるべく取り込んでいきたい。足りないものがあれば指摘してほしい。具体的な対策についての意見は、レポジトリに取り込んで行きたい。
- 今回、ポリシーは大体まとまった。具体的なところは別紙やレポジトリに入ってくるイメージだが、その中にはベストプラクティスだけでなくバッドプラクティスも入ってくると、より一層使いやすくなる。失敗したことは情報を出しにくいが、新規にビルを作ることを考えると、ここで失敗をして改修に相当コストがかかったという事例や、構造的に対応することが難しく放置せざるを得ない状況であったという事例などが、早めに見えておいた方が対応しやすくなる。
- 表にそのような情報を出したくないというのが一般的なので、ISAC のようなクローズドなコミュニティで情報を共有して、アドバイスとして出していくべき情報は出していくという形がベストである。
- ガイドラインβ版では、個々の機器やシステムへのアクセスの部分でどう守るべきかという議論があるが、何がどこに繋がっているのか分からないという問題がビルの複雑さに関連して存在する。エレベータの制御システムが乗っ取られて、ビルに大きな被害をもたらすことは基本的にはないが、そこから侵入されて、ビルの普通のセキュリティが破られることは起こりうる。システム間で関連している部分について、ガイドラインで上手な表現ができるとよい。
- コスト感はオーナーにとっては重要な部分である。例えば”ログを取得する”と記載されていても、どこまで実施するのか、どのようなログを取るのかによってコストの幅が出てしまう。ログの取得という１つの項目をとっても、コストの幅が出てくる状況になっている。そのため、具現化について検討していかなければいけない。システムをどう作るのかという部分は、オーナーだけで考えることは難しいので、ベンダーと一緒にどこまで実施すればよいのかを検討する機会があると良い。
- 海外の DoD のガイドラインでは、クリティカルなインフラストラクチャーについては、どのように記載されているか。そのような部分ではコストよりも、ロバストネスが非常に重要視されるので、クラウドバイデフォ

ルトのところは実施しやすい。そこで経験を積んで、より廉価版を作っていくことが出来る。データセンター事業者の経験をこちらにトランスファーできるとよい。

- データセンターの事業者は危機感が非常に高いので、ないものねだりの部分がある。例えば、相手先認証を実施できるシステムがあればよいが、現実的にはそれがない。そのためのコストや工数は、各社の経験知として、蓄積してこなれていくしかないが、そのような経験知の蓄積を民間の中小ビルから実施していくのは無理である。重要な建物で、お手本になるモデルであれば、それを参考にして、次のプロジェクトを実施していくのがよい。免震ビルや BCP の場合もそのような方法で検討し、普及につなげてきている。
- ないものねだりの部分があるという指摘は重要なポイントである。他の分野でも新しい技術が入ってきたときには、ガイドラインの文面どおりではなく、技術でカバーできるものがたくさんある。技術や研究開発のアイデアをサポートするための各種の仕組みはある。

（２）ガイドラインの活用・展開について

- Europian Commission の DG-CONNECT のメンバーとサイバーセキュリティ対策フレームワークについての議論を行ったときに、ビルガイドラインβ版の話をすると、すごく関心を示された。日本のベンダーは海外で事業展開しているケースが多いので、英語版を作ってシェアし、メッセージを出していくことも必要である。ガイドラインの今後の管理体制や運営体制について検討し、海外でも使っていける形にしておくことが大切である。
- これからガイドラインをどう管理していくか、どう普及させていくかについては、グローバルな市場を考えながら検討すること大事である。
- 今後どのような体制で進めていくかも課題である。インセンティブがないとガイドラインβ版に対応しにくいという問題がある。１つのアイデアとしては、協会とかがきちんと対応しているビルを示すマークのようなものを付与することが考えられる。
- 環境認証と似ている。ビルの環境関係では新築時に取得する CASBEE や LEED、改修時に取得する BELS がある。そのよう分け方で認証制度があると目標感になりやすくてよい。インセンティブがないと投資額が増えることに対して、経営層の理解を得ることが難しい。
- ガイドラインβ版をビルオーナーが集まる会合でシェアしたが、今の記述だとオーナー側ではなかなか読み取れないという声が多く出た。記述されている要求が、今のビルでどういう作業に落ちてくるのか、どれぐらいの負荷であるのか、費用はどれぐらいになるのかということが全くイメージできない。レポジトリのレベルは更にわからない。結局そのイメージが分からないと、何の会話もできないというのが実際のところである。
- 特に中小規模のビルには、かなり難しい内容なので、重要度の高い政府関係のビルから適用し、そこから知見を高めていって、徐々に民間のビルにも適用していくべきである。
- レポジトリについても、ある１つのビルで試してみて、１つ１つの作業について、何をするか、それにはどれぐらいの人工や作業ボリュームが掛かるかの検証を行うことで、他のビルでも、どれができる、どれが

できないという判断を早める１つの方法になる。まだビル業界全体でこのガイドラインβ版を普及していくというレベルには達していない。

- どういう作業工程が必要かイメージできないと、なかなか会話ができない。結局、そういう判断できるのは、過去の経験値から紐解いて判断ができる力のあるベンダーや専門家に限られると思う。
- オーナー側にそのような意識を埋め込むためのドキュメントとして、セキュリティ以外に耐震とかも同じ話ではないか。
- 耐震化については、今でこそだいたいこれぐらいで出来るというものが分かっているが、最初の５年間ぐらいは、どれぐらいの工数が必要で、どれぐらいのコストがかかるかは手探りの状態で、各社が苦労して知見を蓄えていった。その後５年経って、東京都等から、公的な法令が出て、徐々に各社がそれに従うようになっていった。
- サイバーセキュリティの取組で一番難しいのは、攻撃に対して、どのような被害が発生するのか分からないことである。攻撃レベルが高くても、被害額が小さいこともある。実際は対策の効果は多様過ぎるので、産業側での取組、とりわけ中小企業においてどのように取り組むかは大きな悩みである。
- サイバーセキュリティ経営ガイドラインは、策定して３年経って、各社に知られるようになった。一方で中小企業では、それを適用することは難しいため、中小企業向けの簡易版を別途策定して、自分たちでセルフチェックを実施しようという、SECURITY　ACTION　をとってもらっており、既に３万社に達している。ビルでも先ずは１つきちっとしたガイドラインを策定したうえで、それをブレークダウンしたものを今後考えていくことは順序立てとして必要である。
- 今回、ビル業界の人と話をして、オーナー、設計事務所、ゼネコンなどがいて、直接関係するところとは会話をするが、レイヤーが１つ変われば会話はほとんどしていないということが分かった。バッドプラクティスの共有が２つ下のレイヤーで起きていたりすると、責任を取る人が２つ上のレイヤーの人であることもある。意見交換する構造を組むのが難しいという印象を受けたが、だからこそ ISAC のようなものがあった方がレイヤー間を越えて、企業の規模を越えて意見交換しやすくなる。このような補助ツールについても実施していく必要がある。
- 知見を集めていく場を設定することは否定していない。ただし普及について急ぐのではなく、いろいろと使ってみたり、いろいろと議論しながら、それらを積み重ねていけばよい。その手順を踏むことが必要である。
- ビルの規模と対策の工数と費用がシミュレーションできるとありがたい。現時点の典型的な対策について、アセスメント上からの判断や、工数とコストが分かるとよい。
- ぜひ使ってもらいたい。このようなガイドラインによるアセスメントは今まで無かったものなので、試し運転をしてみて、先ずは使ってみることは非常に効果があると考えている。
- オーナーも必要性は承知しているが、インセンティブの話はぜひ検討して欲しい。オーナー側にはそれなりの規模を持った企業体もいるが、今の大規模ビルは再開発で個人の地権者が多いので、大規模ビルであってもたくさんの個人や中小規模の資産管理会社が存在する。そのようなオーナーが必要であると理解することが重要だが、サイバーセキュリティ対策はいつまで続くのかというイニシャルとランニングについての漠然としたコスト不安がある。その部分を見据えて具現化しないと普及展開はな

かなか進まない。

- また、スケジュールに関して、ガイドラインを活用して自社保有物件でアセスメントの取組を始める予定である。その結果をもとに、漠然としたコスト不安を持っている中小規模の再開発のオーナーに対し、説得しようと考えている。再開発物件は管理組合の決議がいるが、年に 1 回の総会で決議する必要があり、簡単に 1 年ずれてしまうこともあるので、そのスピード感を予め認識しておいてほしい。
- 経済産業省ではコラボレーション・プラットフォームという取組をしているが、ビルのガイドラインをテーマに開催することも考えられるので、個人オーナーや管理組合の方々にも参加してもらって、実際のビルのハッキングの事例などの情報をシェアして、ビルの状況を理解してもらう場として活用してもらえるとよい。
- スマートシティやスマートビルといったスマートコンテンツが最近、攻撃目標にされている。スマート化すれば、リスクはどんどん増えていくので、利益をより高く求めようとする攻撃者のターゲットにされやすくなる。
- この業界には、先導的な省エネ事業や、スマートシティのモデルタウン事業など、いろいろな補助金が交付される事業がある。インセンティブが付与される仕組みの条件の一つに、このガイドラインを使って BA を組むことという条件が入れば、有効である。
- 長期的にみてリスクを下げるということは、公共の施設については、ものすごく重要である。
- インセンティブの部分は、もう少し総合的に議論しなければいけない。各社がサイバーセキュリティについては必要性を認識しており、それをどのように上手に展開していくかという部分については理解してもらっているので、いろいろなお知恵をいただきたい。

（3）今後の進め方

- 各社でガイドラインβ版をトライアルで使ってもらって、その結果をフィードバックしてほしい。

（以上）