産業サイバーセキュリティ研究会　WG1　ビル SWG（第７回）　議事要旨

日時　：　平成 31 年 1 月 9 日（水）　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．パブコメ版にむけた修正及び公開範囲の方針等について
２．レポジトリ収集状況の報告
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
４．ガイドラインの管理体制について
５．自由討議

要旨　：

１．自由討議

（１）パブコメに向けた修正について

- ガイドラインβ版の今後のスケジュールについて確認したい。
- 現在、修正作業を行っていて、２月中にガイドライン第１版をパブコメにかけられるようにしたいと考えている。パブコメで出てくる意見の量次第、修正の量次第ではあるが、上手くいけば年度内に公開できる。年度を越えたとしても少しぐらいになる。
- 現在、新築物件に関して、ガイドラインβ版を参考にしたチェックリストによるチェックを工事請負者にしてもらおうとしている。ガイドラインβ版が実際に適用できるかどうかなどフィードバックしたい。
- 新しい調達が始まるので、その際に、このガイドラインを参照してください、と書けるようになるとありがたい。
- 昨年末にガイドラインβ版をもとに、会員向けのアンケート調査を実施している。現在集計作業を行っているが確認したものを大雑把に言うと、「まだまだ分かりにくい」という印象を持っている会員が多い。「今の状態ではどのように使えばよいのかが分からない」、「これからどのように充実されていくのか」という疑問符を持っている会員が多かった。
- ガイドラインを作った後に、その業界のプレイヤーの方々がきちんと理解できるように、ブレークダウンしていく。そのような仕組みができることが一番重要である。
- 当協会の会員には、大手のデベロッパーが多いが、それ以外にもいろいろな業態の会員がいる。専門的な知識のレベル感が異なるので、パブコメは、素人でもある程度分かるような形で実施して欲しい。

（２）レポジトリの収集について

- 現在のガイドラインは網羅性を重視して記載されているが、これをそのまま現場に持っていっても使いづらい。現場で使える解説やチェックリストという形にブレークダウンできると非常によい。
- レポジトリを共有できるとよい。具体的な対応方法を書き込んで共有できれば、実装検討のオーバ

ーヘッドが下がっていくので、ぜひレポジトリの作成に協力してほしい。

- レポジトリを充実させるには、知見を出すことに関するインセンティブのモデルをどのように作ることができるかが大事である。知見を出してもらうことを後押しするようなインセンティブのモデルを設けた方がよい。
- レポジトリはビル SWG メンバーが聞きたい優先順位の高い分野から出していくという形で交通整理ができた方がよい。
- どういうクレジットでレポジトリを出すかが課題である。社名を出す、社名を出さない、このような会社という形で丸めて示す方法もある。
- レポジトリのような読みやすい読み物があると、全体のレベルアップや、理解促進につながる。このレベルまではいかないが、理想はこのレベルであるというイメージのものを、ベストプラクティス集の形で示せるとよい。
- レポジトリについては、番号を付けて、体系図で示してもらいたい。いろいろな分野があり、ツリー構造にもなっているので、体系図で示すことができれば、埋めるべきところが見えてくるようになる。
- 米国では民間に適用するベストプラクティスは、NIST が中心になって行っている National Cybersecurity Center of Excellence の方で策定している。そこで策定された文書には、民間のクレジットがたくさん入っている。それと近い文書を作り、ベストプラクティスを記載するときに、民間のソリューションをベタに書いてしまってもよいのかという問題があるので、そのような民間に適用する文書のあり方について検討する場が必要ではないか。
- National Cybersecurity Center of Excellence は、どちらかと言うと、官民を融合させようとするものであるが、議論がマチュアになっていない。最後は製品安全、セーフティとセキュリティがクロスしてきて、政府の制度にどう乗せるべきかという部分については、まだワンステップ、大きな隔たりがある。
- 一方で、各分野によって動き方に違いが出てくると考えており、WG１で全体のフレームワークが固まると、今後、各分野にこれをどう実装するか、どう適用するかといった話になってくる。ただし、各国とも体制の取り方が違っているので、そのあたりの動向も見ながら、考えていかないといけない。
- レポジトリの中に、セグメンテーションをどうすべきかという観点が最初に記載されていた方がよい。データの重要性のセグメンテーションや、ネットワークのセグメンテーション、物理的なセグメンテーションをどうするかという観点が入ってくる。セグメンテーションが出来れば出来るほど、そこに密結合しているプレイヤーがいるので、そこからより狭い分野のレポジトリの話ができるようになる。それができると、サイバーセキュリティの観点からより安全なものになると考えている。

（３）海外動向との関係

- 認証の話が出ていたが、強制的なものにすると、海外から調達への参入も含めて強い圧力がくる。外部からいろいろと言われないために、強制にするものと、ボランタリーにするものを上手く分けるべきである。一般の公開レベルの話は強制でもよいが、ISAC のような半分閉じた場で検討するような話は、ボランタリーとしての扱いにするなど、ガードが上手くかけられるようにしてもらいたい。

- 非常に重要なポイントである。認証の話は国内でも海外でもよく議論になるが、先ずは検証体制の構築のところから入って、保証できるものをきちんと明確にし、そのうえでの認証であるならば、その価値をマーケットに提供できるのではないかと考えている。
- ビル ISAC のようなものが創設されれば、検証のやり方やその中で一番良い方法は何か、それが確立すれば認証もできるといった議論を実施してほしい。さらに、国外のマーケットを意識した実力を身につけて、提案できるようにしておくことがとても重要になる。

（４）ビル ISAC についての議論

- ビル ISAC の創設については同意する。今後、ビル ISAC の創設を目指していく中で、BIM の話は避けられないので、今後の検討スコープの中に含めていった方がよい。
- ISAC のような半分閉じた場で検討していくことについては賛成である。
- ビル ISAC は、いわゆる ISAC と呼ばれているものよりもスコープをやや広めにして議論ができるとよい。ISAC というクローズドな場では、この部分はオープンにするべきではないという意見も言いやすくなる。
- 情報共有について、現状では事故事例は集まりにくいと聞いている。本社ビル、工場などの所有者側が、自ら公表することはないという気がする。
- 一般論だが、情報共有は信頼関係が一番重要になってくる。情報共有を進めるときには、情報が自社から出たものだと分からないようにするためのマスキングのスキルが重要で、情報の出処が分からないのであれば、安心して情報を出せることが多い。
- 通常は、一般化した形やふわったとした内容までしか情報共有できないのが実態である。１つのソリューションは、ISAC を組むことでお互いに顔見知りになると安心して付き合うことができるので、意外に情報共有が進んでくる。ビル SWG メンバーも既に何回も顔を合わせているので、ISAC のスタートは上手く切れるのではないか。
- 電力業界は、昔から電力各社の監査システムが上手く回っている業界である。横の業界を見ながら、参考にできるものは参考にしていくということだが、不動産業界でできるならば、それがおそらく売りになっていく。
- 普通に考えると事故事例を自ら公表すれば、社会的なブランド力低下やテナントに迷惑をかける事態を公表することになるので、公表は難しい。また対策を表に出せば、攻撃のターゲットになる可能性が増すと考えるのが、一民間企業のオーナーではないかと考える。社会全体の認知が変わっていく流れがないと難しい。
- 経済産業省では、J-CSIP という情報共有体制を構築しているが、重要インフラを中心に各分野の事業者が参加している。そこでは情報を上手くマスキングでき、自社から出た情報であることが分からなければ、他の事業者から情報をもらえて、被害が起きる前に対策を講じることができる。情報共有の範囲は業界内に閉じているので、一般向けに情報が公表される訳でもない。ISAC の利点はそのような情報共有を行うことに加えて、そこに知見を貯めておけば、困ったときに相談してコンサルティン

グを受けることができたり、事業者が共通して困っていることについて、人材育成の共同トレーニングを行い、対応力を上げるなど、他の分野では結構上手くいっているように見える。

- ISAC の現実的な組織イメージが沸かないが、限られた関係者で共有したものでも、人の流動性が上がっている世の中では、関係者に守秘義務を課したとしても情報が漏れ伝わるのが普通であると考えている。
- 今まで情報が漏れたという話は米国でも聞いていない。あれだけ人材の流動性が高くても情報管理の徹底は可能だということだと思う。各社の機微技術に対するアクセス権の設定と似たようなレベルで管理しているのだろう。
- 仮に他の事業者に異動した場合でも、自分が知っている知識は出すが、それが他の事業者に及ばないように工夫するということを分かっている人が、ISAC には参加している。その人たちが上手に仕事を変えてくれると、上手に知見が広がっていく。そういう人が、人の繋がり、リレーションを活かして、新しい情報の獲得を行っている。
- ISAC としての継続性の担保も大事になると感じた。
- ビル業界では、いろいろなステークホルダーがいて、それらの間にも利害関係があるので、ビル ISAC の中に二層構造の形でビルオーナーの会やゼネコンの会などのグループを作って、グループ内で情報共有と他のグループとの共有を分けてできるとよい。
- ビルでは、電力分野や水道分野などのインシデントの影響も受けるので、ビルと繋がっている他の分野の ISAC とも情報交換できると良い。
- レポジトリを蓄えることや、ビル ISAC にコンサルティング機能を備えることはあってもよいと考えるが、ビル ISAC の具体的な組織の運用のイメージが分からない。
- ビル分野も対象が広いが、グループを限定して情報共有を行うと話が早い。いきなり全部についてやるのではなく、先ずこれをやりたいというものを決めて、できる人が集まってグループを組んでいく形にできると、比較的上手く回っていくのではないか。
- 米国の電力 ISAC の場合は、活動の拡張を進めているので、10 ぐらいのタスクフォースが活動している。活動が広がってくると、いろいろと相談したいことが出てくるので、柔軟にタスクフォースを組んでいるという印象を持っている。
- あまり形式張った形で運営するよりは、むしろオフラインでの活動の方が、価値がある場合がある。普段は電子メールで、こういうインシデントがあったという情報を共有している。
- ビルはステークホルダーが非常に多いので、全体の意見調整を図ることがなかなか出来ていない。例えばログの取得について、何のログを、どれだけ取得するのかという議論はされておらず、ビルオーナー、BA 協会、システムベンダー、ネットワークベンダーの方々が共同で研究していかないといけない。ビル ISAC でそのような研究を実施できるのではないかと期待している。
- 課題の解決を関係者に単独で聞きに行くと、なかなか教えてくれないが、ビル ISAC として、聞きに行くことができればよい。
- よく実施されている方法として、勉強会と見学会を組み合わせて実施する方法がある。現場を見たいという人は非常に多い。ビルオーナーが気づいていないこと、ビルオーナーが当然だと思っているが実

際はそうではないということを見学会の参加者が指摘することもある。施設を見学しつつ、そこで話をする機会を作ることは、運用として上手く回るパターンの１つと考えられる。

- 施設のアセスメントでオーナーとサイバーセキュリティについて話をしていても、途中で話がセーフティの観点に変わってしまうことが多い。セーフティは生命に関わるものであり、オーナーの関心が高い。他の ISAC では、セーフティの領域にまで踏み込んだ検討が行われているのか。
- 法令の中のサイバーセキュリティ対策を要求しているのは電力分野になる。
- 一方で、影響があまりにも大きいので、電力分野のネットワークへの繋ぎ込みについては、極めて慎重な姿勢である。打撃が出る範囲、打撃が出るポイントを極力絞り込むという対策を採ってきている。電力分野では、サイバーセキュリティを完全に切っていいものとして認識していない。制御系システムを扱う分野の中では、電力分野は最も危機意識が高い。
- 電力分野は、組織的なガバナンスストラクチャが確立されているが、それが実際に行われていない場合も多いので、法律で上手に強制している。一方でビル分野は、ダイバーシティが大きく一律に遵守するのが難しいので、自主的な取り組みが重要になる。そのためにはインセンティブの話になるので、その仕組みを作っていく必要がある。最初の入口として、米国のように、重要インフラの部分から入るという方法もある。電力分野での取り組みを横展開する形はあり得る方向性である。
- 具体的な姿はこれからの議論にはなるが、ビル ISAC を創設していくという方針については、ビル SWG メンバーの共通のコンセンサスであると理解した。

（５）普及のためのインセンティブについて

- ビルオーナー側の立場として、インセンティブについては、今後、どのように議論されていくイメージか。
- ビル SWG を継続していく場合は、インセンティブが検討の大きなポイントになるが、アメもムチもあるので、単純な話ではない。どのようなアプローチを採れば議論が進みやすいのか、ビル SWG のメンバーの皆様においてもビル ISAC のような形で、意見をまとめてくれる場があると、議論しやすくなると考えている。ただし、それをどういう制度にどう繋ぎ込むかよって話が変わってくるので、あまり乱暴に話すことはできない。
- ビル ISAC のようなグループがコアになって議論して、最後は提言書のような形に持っていくことができると動きやすい。どういう仕組みがあれば、インセンティブが湧くか、そういうものを提言書にまとめてほしい。ビル ISAC を、対策を普及させるためにどのようなインセンティブの手段があるとよいかという提言書をまとめる場として活用することも考えられる。

（以上）