産業サイバーセキュリティ研究会　WG1　ビル SWG（第９回）　議事要旨

日時　：　令和元年 5 月 29 日（水）　15 時 00 分～17 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
独立行政法人情報処理推進機構　産業サイバーセキュリティセンター(ICSCoE)

（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（欠席）、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

議題　：

１．ICSCoE 有志によるガイドライン解説書の紹介について
２．パブリックコメント結果と公開案について
３．今後の SWG における検討事項について
４．自由討議

要旨　：

１．自由討議

（１）パブリックコメント意見への対応について

- パブリックコメント案について専門の人間にも確認してもらったが、全体としては実態を反映しているということで、違和感はない。将来にわたって適切な管理を目指しているところも良いと思う。
- コントローラなど、現実的にウィルスチェックができないものも存在する。ウィルスチェックだけでなく、クリーンな環境で製造されたもの、という言い方で機器が汚染されていないことを担保するという表記も必要ではないか。
- 担保するというのは書けないだろう。
- 新規に入れるものについて、OS でウィルスチェックは掛けられないということか。既存の物にアップデートを全部掛けろというのは、制御系では壊れる可能性もあるので難しいが、入れる段階の物についてはある程度はチェックを掛けないといけないのではないか。
- 実際の製品で改造を加えた OS を使うことはあるので、市販のウィルスチェックはできないのは事実である。工場での製造時に製造 PC でチェックをすることはできると思うが、納入後にそのコントローラに対して現場でチェックを掛けるのは難しい。
- 製造者は製造時、出荷時にホワイトなものをチェックして出しましょう、現場受入側もそれを確認して施工しましょう、組みあがったら竣工時にも白であることをチェックしましょう、という意図である。白であることを確認して欲しいというポリシーで使っている。
- まず、ガイドラインは、マストではなく、ポリシー的な部分をそれぞれの立場でできる範囲で読み替えて判断して対応して欲しいという前提がある。その上でクリーンであることを求めているのであり、逆にクリーンな製造の仕方まで規定するのは書き過ぎになる。
- 製造プロセスの V 字型のモデルがあって、企画、設計と最終的にパーツまで落とし込んで、各レベルで OK なのかを見て、最後に組み上げて最終テストをするとき、最終パーツで OK か確認できればいいのであり、V 字で上に戻った後に、同じことを下まで戻ってやれとはならない。

- 最近は全部自分のところで開発しているのではなく、いろんなオープンソースソフトウェアや買ってきた部品・ソフトウェアをいろいろと組み合わせて作られている。その時に必ずしもソースの検証がされていなかったりする点は懸念される。サプライチェーンの中での品質保証というところも含めて見て行くべきだろう。
- 今後の検討事項について、書いているところはカバーしていただいた。今後も走るので、新しい検討項目が出てきたら、そこで入れて行く。そして、続けなければいけないというのがコンセンサスだと思う。
- ガイドライン公開版に向けてここまで長いご審議をいただいたということで、ここまでこぎつけられたということで御礼申し上げる。

（２）SWG の今後の検討事項／ゾーニング管理について

- 今回のガイドラインで場所に紐づけた対策と言っているが、場所というのはフィジカルのゾーニングの世界の話で、ゾーニングに対するアクセス制御が前提で、場所のセキュリティが決まる。つまり一番ベーシックなビルにとってのセキュリティは、物理的ゾーニングとそれに対するアクセス制御である。
- 重要インフラ施設やデータセンターのような厳格なゾーニングの管理は、いろいろなテナントやいろいろな人がいるビル一般では難しい。関係者でどうコンセンサスをとって管理をするか、ステークホルダーとしての意識がどう共有できるかが大事で、そういったところで ISAC の活動の中で情報共有して、意識も整っていくというのは期待したい。

（３）SWG の今後の検討事項／インシデントレスポンスについて

- インシデントレスポンスの話があったが、マルチステークホルダーで個別の環境が違いすぎるので、インシデントレスポンスが何かは示しにくい。最低限、コミュニケーションが取れる体制がすごく重要だということだと思う。ガイドラインでは、何かあった時、担当者と連絡が付くような連絡網の体制構築が視野に入っていることを書いた方が良い。
- インシデントレスポンスに関しては今回欠けていたと感じている。すごく難しいのだが、次の課題として重要だと思う。
- 今のガイドラインの内容を NIST フレームワークと比較してマッピングしたが、復旧とか対応のところがすっと抜けているので、そこは最優先の課題であると指摘させてもらった。
- 多くの場合は組織におけるやり方や体制の話だが、マルチステークホルダーではどう記述するかは知恵がいると思う。
- 組織には CSIRT があり、情報漏洩や業務障害などのエスカレーションやインシデント時の対応も決められている。しかし、ビルでインシデントがあったとき、他のビルや製造メーカに、どの時点でどう情報共有をしたらいいのか。他のビルに被害が拡大しないように、どう対応をとったらいいのか。それと、ビルのインシデントはどこが最初の発見の起点になるのか。そういうところのベストプラクティスやモデルがあると、全体の CSIRT の体制づくりでも参考になると思う。
- ビルでインシデントが発生していることに誰が気づくのか。インシデントなのか、故障なのかも分からない。故障かと思ってベンダを呼んで、ベンダが部品を持ち帰って検査して、2 か月後にウイルスだと分かる

のが現実である。エスカレーションも重要だが、社内でどこにエスカレーションするのか、部署がない、人がいないというのが現状で、まず人材を育てましょう、こういう組織で見て行きましょうというところから考えていくべき。実際にどのようにガイドラインに書けるかも分からないので、いろいろな事例を参考にまとめて行った方がいいと思う。

- インシデントについては、東京オリンピックに向けて事例収集しているところなので、それはかなりの事例になると思う。
- ビルの場合はサイバーセキュリティに特化したインシデント対応は難しいのではないか。セーフティなどもある。故障・安全対応は既にやっていることから、その中にサイバーセキュリティのインシデント対応もある、ということになるのではないか。
- アメリカとフレームワークの議論をしていると、インシデント対応はまさに足りないところだと感じる。ただし、1 つのモデルだけの整理ではマルチステークホルダーだと難しいところもある。仮に業界単位で何かが起きた時、サイバー攻撃で起きたのか、システム故障で起きたのか分からないまま、始めの 1 日、2 日は耐えなければならなかったりする。その辺はプラクティスを通じて組んでいけたらいいと思う。
- 運用段階の連絡体制については、比較的この業界は持っていると思う。ビルオーナー、ビル管理会社、建設会社、設計事務所もビル運用時は何かあったらきちんと情報を回せる体制はある。ただし、それは雨漏りや設備が壊れたとか、人がケガしたとかのための連絡体制であり、サイバーアタックに対応できる人材はいないので、人材をどうするというところまでは書ききれていない。

（4） SWG の今後の検討事項／ISAC について

- コストが高いか安いかの議論は、情報システム一般でも同じ歴史があった。そこではインデックスを貼ることが既にできる状態だったので、メトリクスの議論ができ、非機能要求の可視化をすることが出来たが、ビルではまだインデックスがないので、その議論が出来ない。今回のガイドラインがインデックスの役割を果たすことになるので、データを集めていってメトリクスまで持っていけるようになれば、工数もある程度見えるようになるかもしれない。そのためにはデータを集める体制を組む必要があり、ISAC とかでデータを収集蓄積し、解析できるチームを作れれば、コスト評価ができるようにもなっていくと思う。
- ISAC について、本当に情報共有、データ蓄積が出来るのかという疑いが社内にはまだある。労力やマンパワーにみあう効果があるのか不明であり、あまり過剰に考えない方が良い。
- ビルの大手オーナー各社の意見を伺ったが、総論では情報共有の場が必要となるが、体制の話になると各社各様となる。スモールスタートで、各社の負担のない形で開始し、実効性が出てくれば、それを広げる形でやっていければと思う。
- 銀行も、テレコムも ISAC を作っているが、オペレータが中心である。ベンダから情報をもらうのではなく、オーナーがエキスパートを呼びつけてやる形がいい。銀行も、3 社とか 4 社でスタートした。ビルもオーナーサイドのコア数社からスタートすると良い。
- 情報共有はある程度信用するところからは始まる。そして、せーのドンで動く。そうでないと動けない。意外と成果が認められて拡大しているものも多い。
- ISAC をやることは反対でないし、情報共有するならそこに出ている個人限りで、会社に持ち帰るの

もダメというところから始めるということだと思う。まずはなるべく経費の掛からない形で進められればと思う。ビルオーナーで持ち回りの開催とし、Web 上で情報共有するなど、工夫できると良い。

- ISAC についてのコンセンサスとしては、直ちにちゃんとしたものを作るということではなくて、少数で、顔の見える個人の繋がりでスタートすることだと思う。うまくいっているところはそうなっている。

（５）SWG の今後の検討事項／普及啓発について

- 今後について是非考えていきたいものとして、教育・啓発、アセスコンサルティングがある。既存のビルでどの辺に弱点がある、ということが見えてきているので、そこに絞って見ていき、現在のビルはどうなっているのか、自分のビルはどうなっているのか、そういうコンサルがローコストで出来ると良い。既知の課題は結構転がっているので、それをオーナーに伝えていくことが必要で、その辺をこの SWG で見ていけると良い。
- 不動産関係のセミナーで話したが、オーナーに話ができる良い機会だった。啓発という意味での正確な情報をオーナーサイドに伝えるチャンスであり、関係する業界でチャネルをしっかり押さえていくことが大事である。
- 業界として役員クラスに集まってもらって、そこでサイバーセキュリティについて講演していただいた。具体的な話を聞けば、それに対する理解や問題意識は高まるというところはあると思う。それを受けて各社で機会をとらえてやってもらえると良いと思う。

（６）SWG の今後の検討事項／IoT など今後のテーマについて

- IoT デバイスの適用が広がっていくのでそこも網羅していきたい。また、ガイドラインを適用しようとすると高額な提案になりがちだが、一般のオーナーの資金力には限界があるので、その点は課題認識を持っていきたい。
- ヨーロッパでは、IoT はコンシューマ向けか、制御系なのか、制御系としてもクリティカルエリアなのか、そうでないのか、それぞれ守る価値が違うはずだが、同じルールを入れたがる人たちもいて、トラストマークも乱打している状態で、かなり議論が割れている。
- このような状況の中で一律で何かやるのは危ない。まず、この分野で確認をしておきたい機器が何かを議論してほしい。例えばエレベーターについて、ここまでは共通で見ていてもらえると、あとは自社で確認すればいいということが分かれば、認証の仕組みのようなものは支援に入れる。サブシステムとしても、エレベーター、エネマネ、災害の警報機など、これを取り扱おうということであれば、是非取り扱って欲しい。どういう射程において、どこからやってきたいという議論をいただければ、そこは手伝いをしていきたい。空調のところなどアメリカで厳しい議論になっているので、その辺から議論されるといい。
- 今回、ひとまずは完成となるが、全てを網羅出来ているわけではなく、例えば Wi-Fi など、次のステップで書き足していくべきこともある。ただし、IoT を導入しているような先進ビルなど少数のレアケースのビルに向けた工夫にも限界があるので、今回のガイドラインをベースに、うちのビルはここまでやっている、という目で見ていってもらえばいい。
- 例えば空調の機能は空気を冷やすということだが、その質をどこまで確保するのかはニーズに応じてい

ろいろなレベルがあると思う。メーカとしては、そこを何らか整理をしてもらってレベルを決められれば、対応ができるというところである。

- 5 年前のビルに比較して、今建設中のビルは 3 倍以上のシステムがつながっている。知らないうちに同じラインを共有するような設計になっている場合も、このような情報を集めるだけで精一杯で、かなり危険なことが進行していると実感している。問題のあるシステムに全体が引っ張られることになるが、それを見つけ出して対策するのはかなり大変な作業である。
- SWG メンバーへのアンケートで、ビルのオペレーションや運用マネジメントの認証があるとうれしいという意見があった。一方で、ビルに納入する機器について何か認証されているものがあると安心して使えるという声もあったので、機器、システム、マネジメントのそれぞれのレベルで認証ニーズはあると認識している。ただし、単にコスト増となるのは避けたいので、どういうレベルのものがあると良いかというのは皆さんでご議論いただきたい。
- これからはデマンドレスポンスなど、サービス、システム、データを直接つなぎ、連携するというのが出てくる。その際には信頼できるところとつなげたいが、サービサーのセキュリティレベルやデータのセキュリティレベルなど、そういうものの規格なり、認証なりも必要になると思う。

（以上）