産業サイバーセキュリティ研究会　WG1　ビル SWG（第８回）　議事要旨

日時　：　平成 31 年 2 月 25 日（月）　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（欠席）
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（欠席）
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
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（欠席）、土地・建設産業局不動産業課（欠席）、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
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／中部国際空港施設サービス株式会社

（ゲスト）

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)

議題 ：

１．ビルガイドライン・パブコメ版（案）について
２．ガイドラインの普及策・管理体制の検討について
３．ICSCoE ビル施設管理関連有志の活動紹介
４．自由討議

要旨 ：

１．自由討議

（１）パブコメ版（案）について

- 対応策については、システムに関する防御の観点が強く出ているが、データを中心に見据えた記載が少しあってもよいと思う。データに対してアクセスがあったときにセキュリティリスクのインパクトが大きくなるので、データベースがどこにあって、それをどう守るか、アクセス管理をどうするかといった部分の項目を入れてほしい。
- 具体的にどうしなければいけないかというところがふわっと書かれている。情報管理という観点から体制がどうあるべきかというところが抜けていると思う。
- いただいた意見を踏まえて検討したい。ビルの世界では、扱っているデータが何なのかというところまで落ちてアクセス権の設定が出てくるので、そこまでブレークダウンするのはなかなか難しい。データ中心で捉えていくところはさらに議論が必要だろうと考えているが、データをきちんと管理するという観点について、記述を加えることで対応できるところはあるので、その部分は検討したい。
- データをカテゴライズして、そこにアクセス権の設定が加われば、良い事であるが、コストがかかることも認識している。ビルは物理的なものでもあるので、それと整合性の高いデータの守り方やその切り分けが出てくると、おもしろいベストプラクティスになるのではないか。
- 情報の公開範囲が気になる。建物では図面情報や、設備の位置が記載されているフロア図が含まれることもあるので、一般論として、どこまで公開すべきかについて、海外の事例や、ガイドラインの中で取り挙げているものがあれば教えてほしい。
- 建物の物理的な図面もさることながら、システム構成の図面にも似たような話があって、システム内でどのようなセキュリティツールを使っているかについては、通常非開示である。ただし、これを見られることによって、どういう被害があり得るのかというところをきちんと整理をして説明していかないといけない。

例えばアクセス制限区域のようなところがあって、そこについて情報出す場合には黒塗りで出すと思うが、一般論として何か言うのは難しい。

- 政府のクラウド調達では、ナショナルセキュリティの部分は対象外にして、レベルを 3 段階に分けている。それに沿った形でビルのこの情報は、このレベルの中に入れるという整理をする必要がある。
- 先ほどのデータのカテゴリー分けと極めて近い議論である。どういうデータを扱う箇所なのかというものとセットになるが、かなり個々の具体的なところについては、業界の中での位置づけを先ず整理するということをお願いすることになるのではないか。
- 自治体庁舎は重要インフラになるということでオリパラ関係でも指摘されている。公開しないということになると、審議会にかけないといけないが、一般的な民間企業でも業者に図面を渡すときに注意しているような事例があれば、参考になるだろう。
- ガイドラインの参考文献について、今は国内で出されているガイドラインしか記載されていないが、グローバル展開を考えると、ISO や IEC などの国際標準についても記載しておいた方がよい。
- 参考文献に記載しているガイドラインには、関連する国際標準について記載されているが、それだと 2 段引きになってしまう。グローバルでガイドラインの話をするときに、ガイドラインの参考文献として直接挙げておいた方がよい。
- コントローラーの部分でログを適切に管理可能な機器を導入すると記載されているが、コントローラーレベルの場合はそのようなリソースを持っていないものがある。ここで記載されていることは、ベンダとして要求される可能性があるので、そのような状況を心配している。
- 今までの議論で、重要なビルから対策を導入していくという話だったと認識しているが、重要なビルという価値判断については記載されていない。自社やグループ会社のビルのアセスメントを実施しようとしているが、こういう条件を満たしていれば重要なビルになるので、対策を実施しなければいけないという形に持っていきたいと考えている。
- 重要なビルという判断は、それぞれのビルオーナーが相対的にみて位置づけを決めていくことになると思う。そのような位置づけを行う際に、どういうものからプライオリティを上げていけばよいのかという部分が記載されていた方がよい。
- かなりディテールまで入ってくる世界なので、ビル ISAC が立ち上がって、コンサル機能があると一番よい。
- 業界において調達や運用の基準をどういうものにするかは、自主性を持った形にしたいというのが国としての方針であり、その業界においてのクライテリアを作っていかなければいけない。そのため ISAC のようなものを業界で作り、それでコンセンサスを形成する。業界がクライテリアを変えられる部分も大きなメリットになる。
- ネットワークについて不正接続の有無を定期的に確認すると記載されているが、ネットワーク機器そのものへの不正なログインや身に覚えのない設定変更に関しても、点検することをセキュリティポリシーに入れた方がよいのではないか。ネットワーク機器への不正侵入を踏み台にして設備に攻撃を仕掛けるシナリオも十分考えられる。
- ネットワーク機器への不正接続の有無について、定期的に点検するというよりも、それを検知すること

ができるネットワークスイッチもあるので、このあたりも事業者の首を絞めない程度に入れた方がよい。

- 議論の前提として、ビルの世界は IT 系では当たり前に実施されていることでも、そのまま適用するのが非常に難しいところがある。そのような状況を踏まえ、ベーシックに見えるものしか記載していない。その先については、具体的にどうしたらよいのかといった解説やレポジトリという形で記載したいと考えている。
- セキュリティの専門家から見れば穴だらけに見えるかもしれないが、ビルの業界として出来るところからスタートしないとそもそも無理になる。そこからどうやってステップアップするか、というところに持っていきたい。
- ガイドラインの対象がビルシステムと記載されているが、昨今のビルの中では、IoT 機器など IT ゾーンのものが増えてきている。また、クラウドを使うことでビルの中にサーバを持たないようなシステムがメーカーから提案されている。そういうものが対象になるのかならないのか、分かりにくいところを補足してもらった方がよい。
- ビルの形態はものすごく複雑で、そのような中で一応このような標準的なモデルがあるという形で整理しているので、これを参考にしてもらいたい。ガイドラインの外側に広がる世界について、すべての対応をガイドラインで書き切るのは難しい。こういう場合にどうしているかという悩みをシェアしながら議論できるように ISAC のような形にした方がよい。レポジトリや解説書も充実させ、議論を厚くする取り組みの中で呑み込んでいって、使えるようなものにしていきたい。
- 今のような議論を「はじめに」の部分に入れてもらった方がよいのではないか。ビルオーナーは何が制御システムで何が付加システムなのかが分からないので、ガイドラインで挙げているものが、今の段階で分かっている一部のコアなものに限定されていて、それ以外のいろいろなものについては網羅し切れておらず、今後の議論になるということを最初に説明してもらった方がよい。
- ガイドラインの今後の修正とパブコメ版の確定については、座長に一任ということでよいか。
- パブコメ版というところまで来た。クリティカルな修正があれば、急ぎ頂きたい。それについて修正し、座長に確認してもらったうえで、3 月の頭にパブコメに入りたい。できるだけ早く、バージョン 1 にすることで、東京オリパラの前に実際に現場で使ってもらえる時間をできるだけ長く取りたい。
- 海外の関心も結構高い。G20 を見据えたときに、英語版を持っていると日本からの貢献を強くアピールできる。
- 東京オリパラで終わりではなく、幸いにして、大阪で Expo が開催されるので、それに向けてのステップを踏んでいくという建てつけになったと思うので、引き続き皆様のご協力を御願いしたいと思う。

（2）ガイドラインの普及策や管理体制について

- ガイドラインが公表された後に、どのように普及させていくかという議論はどうなっているか。
- 前回の会合で、ビル SWG メンバーを中心としたビル ISAC を作った方がよいという話をしている。今回のガイドライン公表の先に、このようなケースではどのように対応しているかというものをレポジトリのような形で蓄積していった方がよいと考えている。ガイドラインをリスクアセスメントで使う場合、設計や

構築の段階でガイドラインに記載した内容を認識している人は限られているという現実を考えると、それをコンサルできるような中核のグループがないといけない。そういう観点からビル ISAC を検討するという話はしている。この活動をビル ISAC の方で引き取れるようにすることでポジティブな循環になっていくのではないか。

- ISAC としてはセキュリティインシデントの情報共有だけでなく、プロモーションについて議論していくグループという形でその機能を持てると良い。
- ガイドラインの位置付けを確認したい。ガイドラインを使ってアセスメントを実施し、リスクを把握することまでを求めるのか、その先の対策まで求めるのか。最終的には対策までやり切るのが基本ではあるが、スタートラインにおいては、リスクを把握するところまでであると理解してよいか。
- ガイドラインの位置付けがわからないという点ついては、β版の中でボランタリーかどうかまで記載していないことが一番理由として大きかったため、パブコメ案では、ボランタリーであることも記載した。この後の利用の強制、任意の部分は、これまでの議論でもいろいろなケースがあった。どこからどのような取り組みができるかというところの議論はビル ISAC のような形で進めていくことになるのではないか。その後で制度的なバックアップを付けるかどうかについて、よく議論したうえでまた違った形で議論する必要があると理解している。
- アセスメントを行うことが第一歩として入ると、その事実が組織内で共有されて、それに対するカウンターメジャーをどうするかという観点でコーポレートガバナンスの話になり、次のステップに自然に入ってくる。

（３） ICSCoE の活動紹介について

- 素晴らしいことだと思う。ぜひ頑張ってもらいたい。
- ICSCoE としての活動は、一旦、一区切りになるが、ビル ISAC が立ち上がった場合には、参加させていただきたいと考えている。
- ICSCoE の枠組みの中で、この活動を維持するという話はオーソライズされているのか。
- ICSCoE という組織体としてというよりも、むしろ研修生の中で取り組んでいる活動として捉えてもらった方がよい。
- ICSCoE の中で叶会という OB 会が活動していて、いろいろなグループ活動を行っている。成果物についてフォローしていきたいとすれば、叶会の中で議論して、フィードバックをもらえるようにすることは可能である。
- この活動が将来的にキャリアパスになっていけば、ポジティブスパイラルになる。英語が堪能な人がいれば、グローバル展開のところにも入ってもらえるとうれしい。

（以上）