産業サイバーセキュリティ研究会　WG1　ビル SWG（第５回）　議事要旨

日時　：　平成 30 年 8 月 10 日（金）　16 時 00 分～18 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
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
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．BA メーカ／サプライヤの立場からビルガイドラインへの意見
２．ビルシステムに関するサイバーセキュリティガイドラインの仮セット版について
３．自由討議

要旨　：

１．自由討議

（１）ガイドラインの構成について

- 脅威から対応策が整理されているが、使う側からみると、セキュリティポリシーから対応策が整理されている方が、逆引きできるので使いやすい。また、セキュリティポリシーから整理すると、網羅性の問題はあまり発生しない。
- ビルに入る方々への啓発という視点も入れられるとよい。ビルの中でいろいろな装置が露出する部分があるので、そういう視点がポイントになると思う。
- リスク要因と脅威とセキュリティポリシーの３つの組を見ていると、バランスの悪い箇所が何箇所かある。
- ポリシーを最初に設定して作るというアセットベースの考え方にすると、網羅性が求められるので議論が分かれるところである。今回は先ずは気になるリスクのところから入って、それに対応したポリシーを設定して、実施しないといけないことに引っ張っていくアプローチを採用している。
- リスクベースアプローチの良い点は、ポイントを絞り込めているところである。今の段階では、松竹梅が必要という議論をしているので、アプローチの仕方で、見え方も、ステークホルダーへのプレッシャーの掛かり方も変わる。これ以上細かくする方がよいのか意見をいただきたい。
- 粒度で言えば、非常に良い粒度で記載されていると思う。公開されるセキュリティポリシーとしては、これ以上ブレークダウンしない方がよい。非公開のブレークダウンの部分が、プロセスに分けられているのも良いと思うし、粒度もこれぐらいがよい。
- セキュリティポリシーの見せ方として、同じものが何箇所も出てくる。実装のチェックを行うときには、アセットベースで見た方が早いので、対外的には、脅威から整理しておいて、裏でアセットベースで引けるように整理しておいた方がよい。
- 北米の場合は、セキュリティポリシーと対策例が一体になってガイドラインが出されている。できれば、切り分けた形にして、セキュリティポリシーと対策例の関係性を示すことにより、対策例は１回しか出てこない形にして、多重感を出さないなどの工夫を考えると良い。
- リスクベースで整理するという方法は、脅しが効く。表には、リスクベースで整理しておくが、プロジェクトマネジメントする側からすると、アセットベースで整理されていた方がよい感じがする。

（２）ステークホルダーについて

- マルチステークホルダーのことが記載されているが、ビルのネットワークを設計し作ってくれるプレーヤーも挙げてもらいたい。ビルのネットワークは重要であるが、そこが破られると一番大変になるので、ネットワークだけでカテゴリーを立てた方がよい。
- ビルオーナーとサブコンだけでなく、コンサルのようなものも入ってくると思う。ステークホルダーとして、もっといろいろなプレーヤーが存在すると思う。
- 今後のビルのガバナンス体制には、コンサルや監査が出てくる可能性があり、人材をどのように確保するかという部分も記載する必要がある。
- リスクに応じて対策を行う、許容するということを決めたうえで、対策ごとにマルチステークホルダーの誰が責任を負うのかを記載した方がよい。マルチステークホルダーになると、誰が最終的に責任を負うのかが不明確になってくる。
- ビルシステムの構成は統合ネットワークにサブシステムが繋がっているイメージだが、統合ネットワーク全体でのトラブルシュートのためには、個々のサブシステムのベンダー以外の全体を見ることのできる専門家が必要になるのではないか。

（３）記載項目について

- インシデントレスポンスや危機対応の部分がまだ結構抜け落ちている。マルチステークホルダーでは、プレーヤーごとの対応が複雑になっていく。典型的なビルをケースに、ステークホルダーとデータとの関係の例を幾つか示しておくと、それを基準にして、現場がアクションを取れる状況になると思う。
- ビルの SIRT 手順を作ることがやりやすい方法である。
- 手順書というより、インシデント発生時の復旧訓練を実施する方法もある。
- 日本ではほとんどの企業で BCP について自然災害対応を考えている。ビルの場合も地震対応については意識をしていると思う。しかし、ビル自体も攻撃対象になって、ハッキングなど結構深刻な事案も発生していることを考えると、BCP の対象にサイバー事案を入れておいてもらうことを考えないといけない。
- 一部の通信系の会社では、自然災害もサイバーインシデントも BCP の対象になっている。インシデントの兆候が起きたときに、すぐには原因が分からないので、初動対応としては同じになる。

（４）記載レベルについて

- ガイドラインの記載のレベルについて、中小規模のビルオーナーはそこまで対応しなくても良いのではという話しもある。松竹梅のようなものを想定してはどうか。
- ガイドラインを使う際には、事業者が単独で使うのではなく、何らかの形でコンサルに相談しながら対

応するのが現実的である。そうすると、これを実施した方がよい、あれも実施した方がよいと、やるべきことが重くなっていくので、松竹梅のところでメリハリをつけて、実施しなくてもよい部分にも気を遣った書き方をしてもらいたい。

- ガイドラインには実施しなければいけないことが記載されているが、実際にビルの場合はどうなるかというところには辿りついていない。ある事例のビルを対象として、対応の具体例があるとよい。
- 現状では対応が無理な内容が入っていると思う。セキュリティパッチやウイルス監視やログ取得などは今の製品群には機能が実装されていない。ガイドラインに書いたものが発注仕様書として出てくることによって製品レベルが上がるという期待と、現実にはできないというジレンマが生じている。
- どこまでオープンにするかという話と近い話である。実施可能なものは先ずオープンにした方がよい。これから期待しているものは、ステークホルダーの中で共有しておいて、作ってくれたらそれをオープンにするかという形が考えられる。
- 対応できないところを認識してもらうことも重要である。対策ドリルのような話になると、そこをどう守るかという議論も必要になる。
- ガイドラインの中で現状対応できていないものについては、そういうことが出来ていると望ましいという書きぶりで対応してもらいたい。モノの調達と委託の調達は異なるので、その部分を書き分けてもよいのではないか。委託の調達の部分には結構気づきもあるので、発注者側にとっては発注仕様書を作るときに良い参考になる。

（５）個別の記載内容／アップデートについて

- ビルのライフサイクルが長いので、継続的なアップデートが必要であるということが書かれるとよい。脆弱性の発見後にすぐの対応は難しくても、どこかのサイクルでアップデートを当てることが入っていると安全性が高まる。
- アップデートについて、どのような文言で記載するのかが欲しいと思う。テンプレートのように記載できると、オーナー側も受注した側もそれをベースに話しを進められる。

（６）個別の記載内容／ログ管理について

- ログの管理は重要である。管理の負荷や流出時のコスト増、攻撃者へのヒントにつながらないように安全にも考慮して、何のログを取るか、何のログを取らないか、どのくらいの粒度で取るか、どのくらいの期間を保存するか、といった観点もあると良い。

（７）個別の記載内容／BACNet/IP について

- BACNet/IP では認証の仕組みがあるにも関わらず普及していないために物理セキュリティが必須になっているのではないか。また日本の使われ方と、米国の使われ方に差が生じているのか。

- BACNet/IP だが、米国の場合はアプライド空調の機器が直接繋がるパターンが一般的である。日本の場合は、BACNet/IP とビル用マルチエアコンとの間にゲートウェイが入っていて、そこでセキュリティを抑えやすくなっている。
- BACNet/IP のバージョンによっては、セキュリティ要件が入ったものがあるが、日本ではまだ普及していない。BACNet/IP 規格は米国の団体で策定していて、それを日本版にアレンジして持ってくるが、その部分で数年のずれが発生している。現実的には、BACNet/IP 規格自体とは別に対応していかないと、空白ができてしまう可能性がある。
- 米国に輸出する機器について、米国から BACNet/IP に関するセキュリティ要件が急に出されたが、すぐには対応できないので困っている。
- 多くの場合、普通は政府対応が早い。米国の場合は産業界もそれで動いている。

（８）セキュリティ設計について

- ビルを企画して、実際に機器の選定や仕様決めていく中で、実務的・現実的には、設計事務所がセキュリティ設計を行うのが妥当ではないかと思う。
- 設計事務所と IT 系の専門会社のようなところと連携しながら対応していく形になるのではないか。
- 理想論で言うと、上流工程を担っている設計事務所が適切なセキュリティ設計を行っていくことが望まれるが、設計事務所にはサイバーセキュリティに対する知見や技術はまだまだ浅い状況にある。
- 専門業者の知恵を借りて対応していくことになるので、その取りまとめやコーディネーター的な立場に設計事務所がいるということはあり得る。
- 従来の延長で考えれば、設計事務所、ゼネコンの設計部、BA のシステムインテグレータ、ベンダーが協力して設計を行っていくというやり方も存在すると思う。
- その他に、システムのセキュリティを監査したり、設計段階でコンサルしたり、プロジェクトマネジメントを行ってくれる専門事業者の登場を望みたい。
- 従来の関係者だけでは足りないということも記載した方が良い。
- 新しいビジネスパートナーが必要である可能性は高いといえる。
- 設計事務所には、特定のメーカや製品の色がつかないという第三者性が求められる。今後、セキュリティに対応した製品レベルで検討していくことになると、設計段階からかなり深い知見を持ったプレーヤーと座組みを作って検討していかないといけなくなる。全体の実行・実務プロセスも今までとは変えないといけない部分も出てくる。
- 設計事務所を中心としてコンサルを活用するという話は、施主側から言うと、これまで実施したことがなく、大きなハードルを越える必要がある。設計事務所の業務の中には監理という業務があり、設計書通りにモノが作られているかどうかをチェックするという仕事だが、今後は監理業務の中に、セキュリティの仕様に則った作り方がされているかチェックする仕事が増える可能性がある。
- そういう仕事を設計事務所に実施してもらうには、原動力が必要で、１つは松竹梅の梅の部分は対応しないといけないという強迫観念が必要で、もう１つは、松まで対応させるのであればご褒美が

必要になる。梅の部分は、Must 感が必要で、ネットワークの仕組みや考え方について、きちんと対応できていることを認定する何かが必要である。このような仕組みを運用・維持できないと、ガイドラインは絵に描いた餅になる。

- 製品の認証については、EDSA 認証や、それよりももっと軽いものができてくると、対応しやすくなる。
- 認証については、人を対象としたものを実施してもよいのではないか。こういう人がいるので、そこに頼めばよいという形にできるのも一つの手である。
- 施主側の立場からいうと、全部チェックするのは無理である。設計事務所に頼むことになるが、設計事務所が出来なくても、ポリシーに則って対策が採られていることをチェックする人が必要になり、その人には開示すればよい。そういう人または機関は免許制でもよいかもしれない。
- 資格を決めるという方法はあり得る。ISAC を創設するという話はどうか。

（９）公開範囲について

- ガイドラインを使って調達の仕様書を作ることになると、ガイドラインの項目を指してそれを満たしていること、という記載になる。ガイドラインが公開されていることが必要であり、ぜひガイドラインの公開について検討してもらいたい。
- ガイドラインが攻撃者に情報を与えることになるとの心配の声もあるが、ドキュメントは広まるものである。公開することのリスクよりは、公開して業界全体のレベルを上げることの方が重要である。
- 調達仕様書のようなものは公開しても全く問題がない。ガイドラインが公開されていると、施主側もこれに対応しなければいけないという意識になる。そして調達仕様書はガイドラインそのものが公開されていないと作れないので、そのための内部公開という建付けになるのではないかと思う。
- 攻撃者の視点としては、細かいことが対策例に書いてあると、それだけは実施することになるので、それさえ避ければ攻撃可能と想像する。そのため、対策は非開示にし、もしも開示するということであれば、４つか５つ対策を並べて、そのうちどれかを行うことを推奨する方法が良いと思う。
- 調達についての意見は重く受け止めないといけない。非公開にすると調達で使えない。一方で、例として見せる方法もあるという意見をいただいた。そのあたりのさじ加減は大事である。
- セキュリティポリシーとそれ以下で切り分けているが、制度要求のような規制の掛け方を行うとセキュリティポリシーになり、仕様要求のような規制の掛け方を行うと対策例のところまで落ちていくことになる。
- 業界団体で解説書を作成するように、多層的な対策を打っていくところは、業法によっても変わってくるが、電事法やガス事業法の世界であれば、セキュリティポリシーに近いような制度要求のような規制を掛けている。一方でその他の分野においては、仕様要求をそのまま省令レベルで要求しており、この部分は各省庁で対応にやや差がある。
- 今回はセキュリティポリシーまでで性能要求のところまでとし、対策例のところは全部非公開にしてしまうのか、事例として公開できるものを４つか５つ掲げておいて、その後ろでアーカイブを作るというやり方を採るのかということになっているが、自治体などが、それを参照事例として調達要件に書き込ん

でいくことになるとインパクトはかなり大きいのも事実である。

- 公開したものは、Must 要件に見えてしまうことがあり、攻撃者に対する情報提供になってしまう可能性もある。前者は Must 要件にならないようにするために、書き方を工夫することになるが、後者のようなことがあり、どこまでいっても解釈の問題があるので、この場でブレークダウンしていく必要があるのか、もしくはビルシステム関係の業界団体でブレークダウンするのか、もしくは本当に ISAC を設立するのかといった管理体制の議論は避けられない。
- 民間で作ったものを国として認証してもらうために、１回形式的に研究会を行うという手もある。国のお墨付きをもらってパブリッシュメントするという方法は有効な方法である。

（１０）今後の進め方について

- 公開、非公開の部分について、調達要件に書きたいのでこういうものは公開してほしい、こういうものは公開してほしくないという意見があれば今後の作業に繋げていくことができると思う。
- 頂いた意見については、作業班で検討し、座長に相談のうえで、β版を決定とさせていただきたい。

（以上）