産業サイバーセキュリティ研究会　WG1　ビル SWG（第４回）　議事要旨

日時　：　平成 30 年 7 月 12 日（木）　13 時 00 分～15 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（欠席）
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
日本電信電話株式会社
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．監視カメラシステムにおけるセキュリティ対策で考慮すべき要点
２．ガイドライン素案作成作業について
３．自由討議

要旨　：

１．自由討議

（１）監視カメラにおける課題

・　監視カメラなど、調達では機器のメーカーまでは指定しないので、知らないメーカーが入ってくる。サプライチェーンの点からも要注意である。
・　監視カメラでは、監視以外の用途も増えてきており、人の監視以外の使い方では更にいろいろな影響が出てくるので注意が必要である。
・　インテリジェンスのない機器を繋いでいる場合はさらに要注意で、サプライチェーンのチェックが重要となる。ガイドラインに記載するべき。
・　多機能化されたカメラでは、ユーザが用途を見極めて調達する必要がある。SWG としては用途に見合ったセキュリティ対策になっているかをチェックする。

（２ａ）ガイドラインの作り（体系的な見せ方）

・　各対策リストのナンバリングは、一律に桁を増やすよりも、設計、建設などフェーズでアルファベット表記を変えるなど分けた方が現場では分かりやすいと思う。
・　設置場所から注意点が見られるので、自分の関係するところを見るのには端的にまとまっている。設計者のガイドラインとしては見やすい。
・　作業は網羅的にしているが、最終的にはそれぞれの人に、現場の人にも分かりやすい作りになると良い。
・　まとめ方が場所に拘りすぎていると思う。構築フェーズ、運用フェーズ等の時間軸がいる。リスクの類型化も必要である。p12 のような考え方のガイドラインを最初に示すことが重要である。
・　設計者が使えるということで、それに従って設計出来るという作りだと良い。
・　基本的な方針としては、簡単にできるもの、既存のものに使えるもの、予防まではみんなでやり、検知などの高度なもの、お金の掛かるシステム的な対策は次の段階、というのを入れて行ければ良い。
・　クイックに出来るものが書いてあると、すぐに出来ることが分かる。さらに高度な物をしっかりと作っていく、という作りだと、既存ビル、新築ビルへの対策も分けて分かりやすい。
・　網羅的にまず一回やってみる。セキュリティでは抜けがあっては意味が無い。対策にはランキング、選択肢があるので、何を実行するかは読んだ人が判断すれば良い。実行出来る部分を実行していくことで、セキュリティを高めていける。

- 読んだ人がどう受け取るか、表現の問題もある。バリューとして見えるようにすると、インセンティブは上がると思う。
- アセスメントで有効なので網羅性は残した方が良い。さらに、規模感、新築／既存、課題点などを挙げて、ユースケースを散りばめ、自分と立場があうものを参照すれば良い。
- 物理はどこまで入れ込むべきか。線を物理的に切断されるのはサイバーではない。
- 攻撃者も進化するので、改訂を重ねることで網羅性の担保に近づける。
- 有益な外部参照があれば、それを参照するのでも良いと思う。
- 外部参照は中々見てもらえないのが実態なので、大事な部分はイントロを書いた方が良い。
- 全部読んで項目のブラッシュアップをみんなでしよう。
- モデルだと各システムが閉じて、BACnet の下にぶら下がっているが、最近の提案では BACnet の中をセンサや照明の情報が流れていくようなものも増えてきており、それも意識して欲しい。
- 作業としては優先順位を考えて出口を目指して欲しい。一番大事なのはお金を出すオーナーが満足するものを目指してもらえれば良いと思う。

（２ｂ）ガイドラインの作り（重要ポイント／優先度の表示）

- ガイドライン案にトップダウンの項目がない。どこが重要なポイントか、どのポイントがどのフェーズで必要か、書かれていると分かりやすくなる。
- 網羅されている項目から、特に問題の起こりやすいところをマークしてあると良い。
- ここが危ない、ちゃんと出来ていない、というところが指摘されると良い。
- 新築時にお金を掛けるのは説明しやすいが、既存のビルでは合意形成が難しいので、既存の中での対策の優先順位があると進めやすい。
- 網羅的だとかえって分かり難くなるので、ポイントを絞って優先順位を示すようにする方が良いのではないか。
- これをやっているからここまでは大丈夫、とテナントに言えるガイドラインになる。ただし、優先度のかけ方はテナント毎に異なる点は明記しないといけない。
- ガイドラインでは、半強制的にやって欲しいミニマムマスト、その上、さらにその上のお勧めであるレコメンドまでの何層かを設けてもらうと良い。
- 優先度は、英語だと、Must、Shall、Should、May などの表現になる。
- 建物の区別として、クリティカルな建物か、そうでないかの区別もいるだろう。
- ビルのセキュリティという観点で重要なところ、特に危険なところは書いておいた方がいい。現状、どこにも書かれていない。
- そもそもオーダーを出さないと、それを反映した設計をしてもらえない。最低限のものはあった方が良い。
- この辺は気をつけましょうというのは、注意事項として入れておく。

（２ｃ）ガイドラインの作り（具体例の列挙／ヒントの例示）

- p21 は良くブレークダウンされていて参考になる。具体的な想定事例なども挙げられていると、より参

考になると思う。

- 作業の過程で個別の話しは出てきている。ガイドラインのブレークダウンにより、最後のレベルには入ってくる予定である。
- アクセスポイントを天井に隠す話は、竣工後にテナント工事の中で行われるが、点検口が近くにないとできない。設計時点で気付いておく必要があり、そういう気付きを与えるガイドラインだと良い。
- 具体的な事例があった方が分かりやすい。
- こういう事例が蓄積されるとバリューになる。レポジトリとしてのデータを蓄積していき、特定対象者用のものを切り出して、抽出して作れると良い。
- 可能な限りレポジトリとして持っておきましょうという建て付けにする。

（２ｄ）ガイドラインの作り（発注要件としての整理）

- 調達仕様書にそのまま書けるようなものになると嬉しい。
- 発注仕様書として、設計時、運用時、保守時それぞれに入れ込む要件が出てくる。運用のレベルによって盛り込む内容も違うように例示する。丸写しで使えると良い。
- 調達仕様書にそのまま文言を入れられるように作る。ここが抜けると危ないという点が見えるようにする。

（２ｅ）ガイドラインの作り（個別情報の募集）

- 今の段階ではどのようにガイドで書いていって欲しいかの意見を皆さんからいただきたい。
- 網羅性を要求すると大変になるので、皆さんが抜けていると気付いたところを出していくので良いのではないか。
- 貴重な意見については、整理表への意見も同様にあげていくことで良いか。
- 具体的な物があれば良いと思う。

（３）リスクアセスメント用途での利用

- リスクアセスメントに使える物でもある。全部見るのではなく、自分に関係するサブシステムのところだけを見れば良い。
- ここが出来てないといけない、というポイントを挙げて欲しい。そうするとチェックにも使いやすい。
- リスクアセスメントとしては網羅的にということだと思う。ただし、冗長なところはまとめると良い。

（４）既存ビルの対応

- 既存ビルはほぼ運用でカバーする。システム的にお金は掛けないが、運用の手間は増えると思う。
- 運用でカバー出来ない部分もある。10 年前のビルを今の物に近づけるにはシステムに手を入れる部分も出てくるのではないか。
- 例えば 10 年前のシステムはなるべく触らせないという考え方もある。ネットワークから隔離する。運用で、変なアクセスがされないように管理する。
- アクセスの部分は、L2 スイッチの入替えや GW の対応などはあると思う。少しだけ購入を含むが、アプ

リケーションの入替えに比べれば、ものすごく安く出来る。

- 何らかの要因でリスクが高まって、全部やられるという時には、ネットワークを組み替えるくらいはあると思う。それでもシステムの入替えよりは安く出来る。
- 最終的にはテナントに安心感を売る必要があり、一定レベルはセキュアにするため、既存ビルでは運用でカバーする。ただし状況によってはオーナー投資が増えるので、インセンティブが無ければ浸透しないことになる。
- 安全ということでは、ポートを塞ぐ、ネットワークを繋がないことで、攻撃を防げる。人海戦術で対応する。新築ならば、人ではなく、システムが監視する方がより良いということになる。
- 今でも外とつながっているビルはたくさんある。”ちょっと古いビル”はどうすれば良いか。
- 外とつながる部分については、手を抜くことは出来ない。セキュリティはガチガチにし、お金を掛けるのは仕方が無い。

（５ａ）具体的な注意ポイント（運営課題）

- お客さんのネットワークケアよりも自社のクラウド側の運営課題が抜けがちである、とかがあると思う。

（５ｂ）具体的な注意ポイント（アセットマネジメント）

- IP アドレスのアサイメントを誰も把握していない問題が書かれていない。

（５ｃ）具体的な注意ポイント（物理課題）

- 手の届くところに IP カメラを設置してはいけない。
- 点検口には鍵を掛けるようにするべきである。
- 人が触れるところに機器を置かないようにする。
- 重要な縦シャフトは廊下に面するように、死角にならないようにする。
- 重要なシャフトは鍵も管理者も変えるべきである。
- 歩道のマンホールは 100kg もあって持ち上がらないが、民地内のマンホールは片手で持ち上がる。こういう点もサイバーでは考慮が必要だと思う。
- OA の取り入れ口に人が近づけられないようにする。
- 受水槽に人が近づけられないようにする。
- いろいろと対策しているのに、取り込み口でやられるのは課題である。

（５ｄ）具体的な注意ポイント（認識共有）

- 発注者の設計は要件を言い、施工者の設計は図面に品番を落としていく部分をいう。言葉のレベル、意味が異なるので、関係者間の意識合わせが必要である。
- 言葉の定義が必要ということである。

（５ｅ）具体的な注意ポイント（設計要求）

- ファイアウォールなどはミニマムマストだと思う。
- ネットワークはテナントが自分の責任で引けるようにしており、EPS をテナントが自由に作れるようにしている。床に穴を開けているが、新築時でないと難しい。レコメンドのかなり上の方の話しになるが、書いておけば気がつくことが出来る。
- これを作っておくとやりやすいというのは非常に貴重な情報。進化を取り込める余裕をもった設計が大事である。

（５ｆ）具体的な注意ポイント（通信課題）

- ビルのセキュリティと通信のセキュリティの考え方が一致していない。ビルの物理セキュリティはしっかり考えられていても、通信架線が一番緩いところからビルに上がっていると、重要通信を含めて切られてしまう。通信のセキュリティへの考慮が少ない。
- 無線 LAN も認証とかのセキュリティはしっかりしていても、道路から電波が拾えたりする。遮蔽性が考慮されておらず、物理とサイバーのバランスの考慮も必要である。
- 通信の引き込み口、電源の引き込み口の物理は共に危険である。見えないが重要なところがある。
- ポリシーの中に EPS はあるが、MDF がない。MDF も入れておくと良い。
- データセンターの世界では、引き込み線なども以前から議論をしている。DC での議論の経験も参考になると思う。

（６）具体情報の共有体制

- あまり細かいと報告書には書きにくいが、情報交換のための ISAC 的な仕組みが出来ると良い。
- 当事者でないとビットが立たないので、ビル ISAC 的なものをボランティア的に作り、赤裸々な情報共有が出来ると良い。

（以上）

お問合せ先
商務情報政策局　サイバーセキュリティ課
電話：03-3501-1253