経済産業省　御中

令和3年度サイバー・フィジカル・セキュリティ対策促進事業（ビルシステムのサイバーセキュリティ高度化に向けた調査）

報告書

三菱総合研究所

デジタル・イノベーション本部

2022年3月31日

目次

図 目次

表 目次

1. はじめに

1.1 調査背景・目的

経済産業省では、「Society5．0」の実現へ向けて様々なデータの「つながり」から新たな付加価値を創出していく「Connected Industries」という概念を提唱し、その実現に向けた取組を推進している。「Society5．0」の実現へ向けた歩みの中で、産業構造、社会環境の変化に伴う形で、サイバー攻撃の脅威も増大し、これまでとは異なる脅威も発生する。このような脅威の増大、新たな脅威の出現に対する準備が必要である。

このような背景の下、経済産業省では、平成30年2月7日に「産業サイバーセキュリティ研究会ワーキンググループ1（WG1）（制度・技術・標準化）」（以下「WG1」という。）を設置し、「Society5．0」、「Connected Industries」における新たなサプライチェーン全体のセキュリティ確保を目的としたサイバー・フィジカル・セキュリティ対策についての議論を進め、『サイバー・フィジカル・セキュリティ対策フレームワーク』（以下、「CPSF」という。）を平成31年4月18日に取りまとめた。

さらに、CPSFの実装に向けては、産業構造や商習慣などの観点から守るべきもの、許容できるリスクが異なるという実態を踏まえ、産業分野ごとに個別の検討が求められる。ビル設備の分野においてもWG1の下に「ビルサブワーキンググループ」（以下、「ビルSWG」という。）を設置し、ビルシステムの分野に特化したサイバーセキュリティ確保のための検討を実施し、その初歩的な対応を整理した『ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第1版』（以下、「ビルガイドライン」という。）を令和元年6月17日に取りまとめた。これを受けて幅広いビル・施設に対してビルガイドラインの利用を働きかけているが、現在のビルガイドラインは初歩的な対応を整理したに過ぎないところから、さらに具体的な対策の例示、より高度な攻撃への対応、個々の設備に特化した対応等を取り込んで行くことが必要である。また、ビル・施設に関連した業界が、これらの取組を自らの継続的な取り組みとして推進していくことのできる体制の整備も求められている。

本事業では、ビルシステムのサイバーセキュリティ対策の更なる高度化、広範化、個別化に向けた調査を実施するとともに、その推進に資する体制構築に向けた調査を実施し、その成果を取りまとめ、ビルシステムにおけるサイバーセキュリティの一層の確保を実現することを目的とする。

1.2 調査実施概要

調査目的を達成するために、以下の項目に関して調査・検討・支援等を行った。

1. ビルガイドラインの高度化のための調査
   （1）ビルの空調設備システムの対応策に関する調査
   （2）共通ガイドラインの拡充に向けた調査
2. ビルシステムのサイバーセキュリティ推進体制の調査
   （1）推進体制の情報提供・共有・相談等の機能の実践的評価
   （2）推進体制のあり方の調査
3. 検討会の運営
   （1）ビルSWGの運営

（2）作業グループの運営

2. ビルガイドラインの高度化のための調査

現在のビルガイドラインは、ビルシステムのサイバーセキュリティ確保に向けて、最低限の共通的な要件を整理したものである。実際のビルシステムにおけるサイバーセキュリティ対策を実効性のあるものにするためには、個別の状況への対策をさらに整理して示していく必要がある。このため、現在のガイドラインには含まれていないインシデント発生時の対応策について調査を実施した。

具体的には以下の各項目を含む調査を実施した。

2.1 ビルの空調設備システムの対応策に関する調査

（1） インシデント、リスク源、その対策要件としてのセキュリティポリシーの再整理

調査作業は昨年度のビル SWG で提出された空調編本編をブラッシュアップすることから実施した。昨年度の本編では、表 4-1 の空調システム向けの対策ポリシー表において、セキュリティインシデントとリスク源はほぼ共通編と対比が可能な記述であったが、セキュリティポリシーについては、若干独特の記述が目立っており、別紙への展開がより困難になる可能性が想定された。そのため、セキュリティインシデントとリスク源の記述を共通編と比較し、同じような位置に設置される機器か、機器のシステム構成上の性質等を考慮し、同様の共通編の箇所からセキュリティポリシーの記述を転記してくる作業を実施した。もちろん空調システムとしての視点からの判断は必要だが、一旦共通編と揃えた記述にすることで、ブレを少なくするようにした。この修正版の本編を第 12 回ビル SWG の資料として提出した。

（2） ライフサイクルフェーズ別の対応策（別紙）の検討

次に別紙の作成作業を実施した。昨年度のビル SWG では空調編本編までは一旦完成して提出されていたが、その時点では別紙は存在していなかった。ビルガイドラインは本編と別紙がワンセットになって初めて実用的な意味を持つので、別紙の作成は必須である。

前述の作業で空調編本編のセキュリティポリシーを再整理したので、そのポリシーに対応づく共通編別紙からライフサイクルフェーズ別の対策を転記する方法を取った。これによりほぼすべてのポリシーに対応したライフサイクルフェーズ別の対策を埋めることができた。ただし、各フェーズの記述の判断をするには、空調システム独自の視点からの判断が必要となるため、これを第 12 回ビル SWG に提出し、さらなる意見を求めることにした。

（3） ビルSWGにおける意見募集と対応の検討

次にビル SWG に提出した空調編本編及び別紙に対して、ビル SWG の構成員からの意見募集を行った。ビル SWG はビルシステムのサイバーセキュリティに知見と造形の深い人たちが集まっているので、一般向けの意見募集に先立ってビル SWG で資料のブラッシュアップを行うことは非常に有効である。

意見募集の結果、全部で 7 社／組織から合計 162 件のコメントが寄せられた。

表 2-1 寄せられた意見の概要

会社／組織	全般及び本編への意見	別紙への意見
空調メーカー	19件	31 件
総合電機メーカー	60 件	15 件
ビルオーナー	8 件	5 件
技術研究団体	1 件	
サブコン	7 件	
空調メーカー	12 件	
サブコン	4 件	

これらの意見に対し、空調編作業部グループを開催して、次の方針にもとづきコメントの判断を1件 1件行い、対応を決定した。

- 空調編(案)に対するコメントのみを対象とする
- 具体的な修正案の提案を対象とし、抽象的・概念的な指摘は内容に応じて検討をする
- セントラル空調ベンダー、個別分散空調ベンダーを含む作業グループで現実的な検討を実施する

(4) ビルガイドライン(個別設備編:空調編)のとりまとめ

空調編作業グループは 3 回開催し、全てのコメントについての処理を行った。この結果としては、大きくは次のような修正を実施し、本編、別紙ともに修正を完了している。修正結果は、第 13 回ビル SWG に資料として提出している。

- 構成上の大きな変更はなし
- リスク源に対してその類似性を踏まえて共通編から持ってきたセキュリティポリシー及び別表の記述を空調システムの観点で再整理
- 空調の 2 つの方式(セントラル空調方式と個別分散空調方式)の違いを意識した記述の整理
- 表現上誤解を生じそうな記述を整理

今度は細部の微修正をしたのち、経済産業省殿において公開に向けたプロセスに進むものと考えている。

2.2 共通ガイドラインの拡充に向けた調査

共通ガイドラインの拡充に向けた調査として実施すべきことは大きく分けて 3 点である。共通編ガイドラインが完成した段階で既に一部のビル SWG 構成員から指摘のあったインシデント発生時の対応、対策の整理が必要という点に関して、今年度、日本データセンター協会よりインシデントレスポンスガイドが先行して発表された。当初よりビル SWG は日本データセンター協会より中心メンバーにも参加してもらい、連携して検討を行ってきた関係から、今回もこのガイドを参考として検討させていただくこととなった。

また、ガイドラインができた当初はビルシステムのサイバーセキュリティに取り組む会社はほとんどおらず、製品やサービス、現場の作業において、サイバーセキュリティ対策についてのノウハウがほぼない状況であった。このためガイドライン自体も詳細な記述にはなっておらず、様々な経験を事例として積み上げて

相互に参照できるようにする方法を取り入れている。1 年間の間に新たに増えた知見について調査を行い、事例として蓄積するための資料に取りまとめる。

また、ビルガイドラインができて以降、このガイドラインを参照してビルシステムのセキュリティ対策に取り組む人たちは増えつつあるが、一方で、まだまだビルシステムのサイバーセキュリティへの関心や意識は十分には広まっていない。これは現実にはビルへの攻撃があまり明らかになっておらず、危機感が薄いという事情があると考えらえるので、ビルシステムや関連する制御系システムへのサイバー攻撃の事例を収集して広く共有していくことが重要である。

2.2.1 インシデントレスポンスに対する要求の整理

（1） インシデントレスポンスに関する説明会の開催

インシデントレスポンスに関する議論を開始するにあたって、ビル SWG の構成員にそもそもインシデントレスポンスとは何なのか、建物やビルではどういう点に留意する必要があるのかなど基礎的な知識を知ってもらい、検討のための頭合わせを行うことが重要である。そのため、日本データセンター協会より参加いただいている構成員に、第 12 回ビル SWG の場において、インシデントレスポンスガイドの説明を実施してもらった。これにより、ビル SWG の各構成員にも、インシデントレスポンスの議論をなぜするのか、どういう議論をするのか、何がゴールなのかを知ってもらう良い機会となった。

（2） インシデントレスポンスに関する検討方針についての検討実施

実際の議論は他のテーマ別の議論と同様に、作業グループで議論をし、その結果を整理してビル SWG に提出し、様々な意見をいただいて修正をしていくというプロセスを経ることになる。このため、インシデントレスポンス作業グループを開催して議論を実施した。

しかし検討のために参照するデータセンターと一般ビルでは要求が大きく異なっており、そのまま参考にしていくことも難しい。このため、まずは日本データセンター協会のインシデントレスポンスガイドの記述構成を参考に、何を順番に検討し、決めていくのが良いのか、その検討方針の整理から実施した。

1） 検討方針

検討の進め方としては、まず初めに対象を設定することとした。対象としては、どんなビルかというのもあるが、読者として誰を対象とするのかというのもある。つまりビルシステムに係る様々なプレーヤーの中で、誰にガイドラインを理解してもらう必要があるかということである。さらに、インシデントの検知方法とワンセットになる話であるが、どのような攻撃を想定するかについても、あらかじめ考えておく必要がある。

この方針の決定にあたっては、インデントレスポンスガイドのドキュメント構成も参考とした。そして同じくインシデントレスポンスガイドでは、インシデント対応ステップを定めているが、対象に対してどのようなインシデントが想定でき、もしそれが起きたらどのような対応をしなければならないのか、ということで、このステップに応じて、対応を検討し、定めていことが良いだろうということになった。

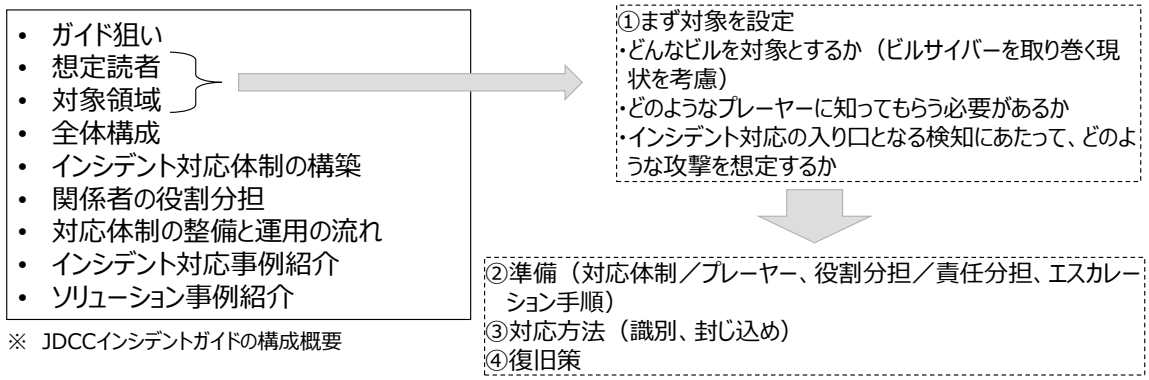

図 2-1 インシデントレスポンスの検討方針

3 回のインシデントレスポンス作業グループを実施して、それぞれの検討テーマに対して次のような議論を行った。

2）対象の設定

a. ビルの種類

- フォローアップは重要で、フォローアップが必要となるようなビルを対象とするべきで、大きめのサーバールームがある、金融機関が入居している、社会インフラとなっているような公共ビル等は対象とするべき
- 重要ビル、ランドマークとなるようなビルが対象で、世の中の大半の中小ビルは対象とするべきではない
- 大手デベロッパについては全ビルを対象とするべきで、所有する中小ビルを CSIRT の対象外とはいえない
- 民間の大手デベロッパはとにかくとして、官公庁舎系や空港等の公共施設系の対応が課題となる
- 新たな利用スタイル（クラウド接続、IoT 利用、ロボット利用など）に対応したビルも対象とするべき
- 産業用施設、一般ビル、病院や公共施設は分けて考えたほうがいい
- IoT やロボットはアタックサーフェスを増加させるので、共通編にも早めの反映を考えるべき

b. 読者

- CSIRT 関係、CSIRT を作るとしたらビルごとではなく、大手デベロッパが所有する物件全体の CSIRT になる
- 大手デベロッパ以外にも独立系の大手ビルはかなりあり、これらは対象外とするか、共同 CSIRT を目指すべきか
- 官公庁舎や公共施設系は異動の問題もある
- 対応フェーズのうちフォローアップは重要で、経営層にもインプットしたい
- インシデントレスポンスは運用段階がメインとなるので、主として運用段階に係る関係者が読者に

なる

- インシデント発生時にはビル事業者だけでは対応が困難で、設備関係、工事に携わるベンダー等の協力を仰ぐことになるので、彼らにも読んでもらいたい

c. 想定攻撃

- 方法：DDoS、マルウェア、不正アクセス、フィッシングなど、これからはロボットや USB が侵入経路となる可能性も想定するべき、メンテナンス端末経由での貰い事故もあり得る、ネットワークは FW とか対策があるが内部に入られると防ぎようがない
- 制御系を止める攻撃：RAM タイプのコントローラは書き換えや特権を取ってのダウンロードもあり得るのと寿命が 10 年 20 年と長いので危険、テナント企業の活動を止める攻撃が一番危惧される、広く使われているコントローラの脆弱性を狙うことで複数ビルを同時に攻撃し社会活動に影響が出ることもあり得る、コントローラを不調にして空調制御がうまくいかない状況を作るとコストが掛かりテナントからのクレームが続発する、大きなビルだとコントローラのリセットに1，2ヶ月要することもあり得る
- 情報流出：入退館の情報は個人情報にあたり特定の人にとっては特に気になる情報、カメラ映像の漏洩も考えられる
- 情報消去：ログを消してフォレンジックを妨害する可能性もある、ログサーバなど別のところで記録しているケースは少ないので機器自体のログを消されてしまえば手がかりを失う

3）検知の方法

- どの時点でインシデントと捉えるかが大事で、データセンターでは予兆レベルからとらえるためにコストを掛けるが、一般ビルでは動作不要や障害が起きてからがインシデントか
- まず障害の検出が大事となる、それが故障なのか攻撃なのかは次の判定の段階で検討する、このケースは故障でこのケースは攻撃とは事前に整理しきれない
- 攻撃の判定も現実には困難ですぐには分からない、考えにくい時間にエラーが出るとかはあるが、通常運転時間内に普通に動いているように見えて設定が書き換えられている場合も考えられ月次でエネルギーデータが上がって初めておかしいとなる、コントローラを替えてもエラーが出続けるケースでは最終的にノイズが原因だと分かったこともある
- 現象としては故障と変わらない形で現れる、故障解析をしても問題が見つけられないときに初めてサイバーを疑うので早期発見は困難でフォレンジックが重要となる、いろいろなログをチェックして解析することになるが、高度な攻撃だと感染後時間がたってから発現することもあり、その時点の状況だけを見ても判断できない
- OT 向けの DPI(Deep Packet Inspection)も出始めているが、コストも高く、ビルによって流れているパケットも異なるのでどのパケットを見れば良いのかのノウハウも蓄積されておらず誤検知もあり得る
- 故障解析するチームは既にあるので、そこにインシデント対応チームも一緒に走る形が現実的ではないか、トラブル時にはサイバーも同時に疑ってみるところから始める必要がある
- ビルの用途によって許容できるリスクも異なるので、どこまで対応する必要があるかも異なってく

る

- 守りたいレベル、絶対に招きたくない状況のレベルを整理することも入り口として大事、許されるなら従来の故障対応と同じレベルでの対応でも良いとなる
- 主装置と従属設備があり主装置が故障すれば従属設備は自律的に一定期間運転できるようになっているが、主装置が攻撃され変なスケジュールがダウンロードされるようなケースは想定していないので、まずユースケース整理が必要
- トラブルシューティングにはログしか頼りがない、ログとフォレンジックが重要
- 今のビル関係者には故障に際してサイバーを疑う意識が醸成されていない、インシデントレスポンスガイドではその可能性を示すことに意義がある
- ビルは関係者が多いので、関係者をどう組織し、連絡を取り合い、どう動くかを整理することが大事となる

4）議論の整理

議論の結果を整理すると以下のようになる。議論で出たコメントや以下の整理を第 13 回ビル SWG に提出し、さらなる意見をいただいた。

検討テーマ	検討結果
対象となるビル	大手デベロッパ（所有する全ビルが対象） 官公庁舎系や公共施設系の建物 新たな利用スタイル（クラウド接続、IoT利用、ロボット利用など）に対応したビル
対象とする読者層	大手デベロッパのCSIRT関係者 フォローアップについては経営層 ビルの運用関係者、設備関係、工事に携わるベンダ等
想定する攻撃	方法としては一般的によく言われる攻撃手法全般 コントローラを不調にしたり制御系を止める攻撃 情報流出をもたらす攻撃 情報消去を伴う攻撃
検知の方法	既存の故障解析チームにインシデント対応チームを並行して走らせる（故障に関してサイバーの可能性も疑うという意識付けから始める） ログ解析、フォレンジックが主要な判定手法となる 用途に応じた許容できるリスクとの関係整理も重要 関係者間の連携体制のモデル整理、ユースケースに応じた対応やエスカレーション手順の整理も必要

図 2-2 インシデントレスポンスについての初期的な議論の整理

（3） 今後の作業指針の検討

第 13 回ビル SWG 開催後に再度インシデントレスポンス作業グループを開催した。ビル SWG での議論を踏まえて、来年度以降、本格的な議論をどのようにするべきか、ということで検討を実施している。

大きくはビルの場合はサイバーの見極めが難しく故障対応にインシデントレスポンスのフローを上乗せしていくことが大事ということで、そのためにも現場でどういう故障対応が実施されているのか聞き取りが必要であること、またビルの用途によって運用も異なるので、ターゲットとして想定したビルを中心にいろいろなビルについて聞き取りが必要であることなどが整理された。

作業グループのメンバーの主な発言は以下の通りである。

- データセンターと一般ビルでは起こって欲しくないインシデントと判断する閾値が違う。そこはビル事業者に聞かないと出てこない。空港とか病院では電源は落とせないので、A 系、B 系を持っているので、そういう状況についての調査がいると思う。病院、官公庁、空港などの話を聞く必要がある。そういうビルを運営している事業者に聞く。
- 建物種別によって違う。共用部は優先度が低くていいとか、低層階ならエレベータは止まっても良い、入退館管理も警備員が見ることができれば代替できる等もある。
- 病院の場合は施設の人も参加して要求書を作るという段階を踏む。公共施設では、電源も空調もどういうデザインにするかは、お客さんとも話して決めていく。そして施設ごとにデザインが違うので、発見の規準とか手法も違ってくると思う。
- 一般ビルだと、テナントからの何らかのクレームから発見するケースがある。また運用管理センターのオペレータが発見するケースでは、故障のタイムスタンプがプリントアウトされて、通常のパターンないエラーを見ている。
- いままでのフローにないところで、サイバーのフローもそのフローに入れないといけない。
- ビルによって受容できないリスク、許容できない故障があり、それはビルや設備の種類によってもちがっている。許容出来ないリスクがあるときに、どう対応するか、その点にフォーカスするのが良いと思う。全部やらなきゃいけないというところにならないように。
- ビルはテナントが暑いとクレームをいうが、データセンターのサーバは暑いとかのクレームを言わない。そのためデータセンターや病院はシステムデザインとして止まらないにようにしないとけない。そのため施設の作りとして二重系の設計をしている。
- ヒアリング先のアイデアとして BA ベンダーとビル管理事業者、中央監視を請け負っている会社などに話を聞くというのがあってもいい。ただし彼らは文化として隠したがるので、彼らに聞くというよりは、彼らにガイドを書いてもらうくらいの強制力を持たないといけない。
- ビル管理をしている事業者に聞く。駅前の大規模ビルになると、BA 主装置も A 系、B 系をもっていて、そこで実際に A 系がやられたらどうするかは現場に聞かないとわからない。不具合時の故障マニュアルがあるのか、どう書いているのか、おかしいときにリセットしてしまうのか、状態保存して B 系に切り替えるのか等、そこはベンダーでないと、現場の運用でないとわからない。
- 最近のビルオーナーは直接に管理部門を持っていない。普通は子会社のマネジメント会社とかに建物維持管理業務を外注する。そこから更に清掃とか、警備とか、ビル管理とかに、小分けにして出すので、根っこの情報が上には上がってこない。そういう日本の現状を踏まえて話を聞いていかないといけない。

2.2.2 現在のガイドラインへの追加情報の充実化

（1） ビルシステムのサイバーセキュリティを促進する事例や情報の収集と整理

Web 調査や文献調査によりビルシステムのサイバーセキュリティ対策を目的とした製品やサービス、実証実験等の情報を 11 件収集し、整理をした。

（2）レポジトリ案の検討

収集した情報から、ビルシステムのセキュリティ向上に資する製品やサービスから３件を抽出してレポジトリ案を作成した。それぞれ次のようなシステムである。

- ビルのネットワークにつながる機器の資産管理、接続監視を行うシステム
- ビルや工場などで稼働する産業制御システム向けの脆弱性評価ツール
- SCADA 向けの監視システムで不正通信などを検知する

2.2.3 ビルシステム及び関連するシステムへの攻撃事例の収集

（1）ビルシステム及び関連するシステムへの攻撃事例等の収集と整理

Web 調査や文献調査によりビルシステムや関連するシステムへのサイバー攻撃の事例を 7 件収集、整理した。ビルの世界では、制御系への直接的な攻撃はほとんど見られないため、受電、受水などビルに導入される個別のサブシステムと関わりのありそうな制御系システムへの攻撃や、IT 系への攻撃だが結果として制御系を止めざるを得なかった事例など、なるべく幅広く事例を集めるように努めた。

（2）ビルシステム及び関連するシステムへの攻撃事例の詳細

収集した事例のうち、直接的に BAS システムが攻撃を受けたドイツの事例、ビルの個別設備と関わりが深い米国フロリダの浄水システムへの攻撃の事例、IT 系へのランサムウェア攻撃ながら制御システムを広範囲にわたって止めざるを得なくなった米国パイプラインの事例について、より詳しく情報を整理した。

1）KNX 社の BAS システムへの攻撃

タイトル	KNX の BAS 機器ロックの事例
事案の概要	
発生時期	2021 年 10 月（被害を受けたエンジニアリング会社がセキュリティ会社にコンタクトした時期）
被害者組織	ドイツのビルオートメーションエンジニアリング会社（顧客先の BAS）
被害システム	BAS システム（照明スイッチ、人感センサー、シャッター・コントローラーなど数百の BAS 機器）
攻撃方法	BAS デバイスの機能を「アンロード」または基本的に消去し、BCU キーをセットして、独自のパスワードでロックした。
攻撃を受けてしまった原因	ドイツのエンジニアリング会社の BAS システムは、公衆インターネット上に公開されたままの安全でない UDP ポートを経由して侵入された。そこから、KNX アーキテクチャに詳しいと思われる攻撃者たちは、BAS デバイスの機能を「アンロード」または基本的に消去し、BCU キーをセットして、独自のパスワードでロックした。 また、被害者は、ビルの建設段階で一時的に設置された IP ゲートウェイを経由して攻撃者が

	侵入したと考えている。この IP ゲートウェイは、ビルの引き渡し後に撤去されるはずだったが、それは忘れ去られ、撤去されることはなかった。 KNX のような BAS システムを設置・管理する専門家の多くは、IT チームやセキュリティ・チームではない。むしろ、BAS システムは通常、エンジニアやビル管理会社の領域です。IT やセキュリティのチームが BAS の運用に関わることはほとんどなく、それが問題となる。
被害の状況や影響	BAS がサイバー攻撃を受け、照明スイッチ、人感センサー、シャッター・コントローラーなど数百の BAS 機器がコントロールできなくなった。 BAS のシステムにはロギング機能が設定されていないため、攻撃者はデジタルフットプリントそのものを残さない。また、身代金要求のメモやランサムウェアの痕跡も残っていないため、攻撃の最終目的すら不明である。 さらに、機器内の BCU キーを忘れた場合、ETS での保護が無意味になるため、外部で変更・リセットすることはできなかった。したがって、数週間かけて手動で照明などの機器のオンとオフをおこなった。 システムの解除には、ロックされた BCU キーを割り出す必要があった。セキュリティ会社は、45 分後に BCU キーを発掘した。手元にある 4 つの機器（ベンダーは異なるが）すべてで一致したため、すべての機器に通用すると確信した。エンジニアリング会社は BCU キーをプログラミングソフトに打ち込み、数週間かけて手動で照明などの自動制御を行っていた BAS システムを 30 分以内に稼働させることができた。
概要	あるビルディング・オートメーション・エンジニアリング会社が、顧客向けに構築したオフィスビルの BAS がサイバー攻撃を受け、照明スイッチ、人感センサー、シャッター・コントローラーなど数百の BAS 機器と突然通信が取れなくなるという悪夢を体験しました。 ドイツにある同社は、オフィスビルのシステム・ネットワークにある BAS 機器の 4 分の 3 が不思議なことに「スマートさ」を失い、システム独自のデジタル・セキュリティ・キーでロックされ、攻撃者のコントロール下に置かれていることを発見しました。このため、ビルの照明を点灯させるためには、中央のブレーカーを手動でオン・オフしなければなりませんでした。 KNX 技術（ヨーロッパで一般的に使用されているビルディング・オートメーション規格）に基づく BAS システムに対する同様のサイバー攻撃は、感染した BAS システムを復旧・復元した産業制御システム（ICS）セキュリティ企業の Limes Security に報告されています。しかし、スマートビルへのサイバー攻撃の多くは報告されていない可能性があります。Catalyst Partners 社の創設者兼代表である David Olive 氏が共有しているように、サイバーセキュリティおよびインフラセキュリティ局（CISA）と連邦捜査局（FBI）の政府関係者は、個人、企業、さらには都市がサイバー攻撃発生時に公表したがらないことを繰り返し認めており、それはしばしば、攻撃の種類、技術的影響、原因を理解できないこと、顧客の混乱や訴訟の可能性の影響を軽減する能力があまりにも不確かで法的責任の暴露に対する懸念からであるとしています。 ブリュッセルに本社を置く BAS ベンダーKNX は、同社のソフトウェアやネットワーク規格を導入する組織に対して、特定のセキュリティに関する推奨事項を提示している。これには、イ

	ンターネットからシステムへの接続に VPN を使用すること、KNX IP バックボーンネットワークを VLAN で他の IP ネットワークから分離すること、KNX IP ネットワークと他のネットワークの間にファイアウォールを設置することなどが含まれます。 Stuxnet や Industroyer、Trisis など、より包括的に行われた攻撃キャンペーンほど洗練されておらず、被害も大きくありません。それどころか、攻撃者は KNX 技術の詳細と、特定の機能がどのように悪用されるかを理解するだけでよかったのです。今回の攻撃では、ある特定の機能が非常に重要でした。KNX では、いわゆるバス・カップリング・ユニット（BCU）キーを設定することができます。 BCU キーが設定されると、この機能をサポートするプロジェクト内のすべての KNX デバイスは、エンジニアリングプロセス中にパスワード（8 文字または 4 バイトの長さ）を使用してロックされます。一度有効にすると、BCU キーで保護されたデバイスは、パスワードが判明しない限り、その後変更することはできません。様々な実装がありますが、ほとんどのデバイスは、デバイスに物理的にアクセスしても、パスワードのリセットを許可しません。 攻撃者は、KNX の特定の機能を悪用する方法を明らかに理解しており、アクセスした後、まず機器をアンロードし、それらの機器に BCU キーを設定しました。これは、パソコンのハードディスクを消去した後に、ハードディスクにパスワードを設定するのと同じです。コンピュータの電源は入るが、OS やアプリケーションを失っているので、もう何の役にも立たない。そして、そのパスワードがなければ、もうハードディスクに OS やアプリケーションをインストールすることはできず、コンピュータは「使えない」状態のままになってしまう。 エンジニアリング会社は、ビル制御システムへのアクセスと制御を回復する方法を探すため、外部に助けを求め始めた。彼らはまず、産業界のサプライチェーンで最も論理的な関係者に連絡を取りました。デバイスベンダーだ。複数のビルディングオートメーションベンダーに連絡を取り、アクセスを回復するためにパスワードをリセットする方法を尋ねました。 しかし、どのベンダーも残念ながらリセットは不可能であり、すべてのデバイスがレンガ化されていると判断しました。提案は、機器を完全に取り壊して交換することだった。この場合、ハードウェア、インストール、検証のコストを考えると、十数万ユーロのコストがかかる。そこで、エンジニアたちは、よりコストのかからない他多くの人は、制御システムのプロトコルが実際にどれほど複雑で強力なものであるかを理解していない。知識のある攻撃者の手にかかれば、この力はもちろん、機器にアクセスしたオペレータにも向けられる可能性がある。このように、現在使われている多くの制御システムは、まだセキュリティが必要でないと考えられていた時代に設計されたため、基本的なセキュリティ機能を備えていません。そのため、敵対者が簡単にアクセスできないような機器にしなければならないのです。
出典 URL1	https://www.darkreading.com/attacks-breaches/lights-out-cyberattacks-shut-down-building-automation-systems
出典 URL2	https://godecrypt.com/news/latest/cyberattacks-shut-down-building-

	automation-systems/
出典 URL3	https://cyberintelmag.com/iot/building-automation-systems-closed-due-to-cyberattacks/
出典 URL4	https://www.hstoday.us/featured/hidden-cybersecurity-challenges-of-smart-buildings/
出典 URL5	https://limessecurity.com/en/knxlock/?_sp=32de7748-f0d0-4ab6-b168-e9379d32b283.1644939635088
出典 URL6	https://smartlight.co.jp/2021/11/10/smart-buildings-are-the-subject-of-cyber-attacks/
出典 URL7	https://www.knx.org/knx-en/for-professionals/newsroom/en/news/Smart-Buildings-are-the-subject-of-cyber-attacks/
出典 URL8	https://connectedmag.com.au/knx-warns-of-cyber-risk-to-smart-buildings/

2）フロリダ州オールズマー市の水道施設への攻撃

タイトル	米フロリダ州　浄水システムに不正侵入
事案の概要	
発生時期	2021 年 2 月 5 日
被害者組織	米国　フロリダ州オールズマー市　水道施設
被害システム	浄水システム（水道施設（浄水場）制御システム（SCADA システム））
攻撃方法	TeamViewer を何者かが遠隔操作で操作し、飲用水に含まれる水酸化ナトリウムの濃度の設定値を変更
攻撃を受けてしまった原因	3 つの要因があった。 第 1：職員間で「TeamViewer」のリモート接続用パスワードが共有されていた。 第 2：職員のコンピュータは、ファイアウォールを通さずにインターネットに直接つながっていた。 第 3：この施設では、2020 年 1 月にサポートの終了した Windows 7 を使っていた。
被害の状況や影響	飲職員がすぐに気づいて設定を元に戻したため実害はなかった。このときの攻撃者の「滞在時間」は 3～5 分間だったとされる。不正操作に気がついたオペレータによって攻撃者による設定変更はすぐに修正された。
概要	フロリダ州タンパ近郊のオールズマーの水道施設の制御システムに外部から不正アクセス。飲用水に投入される水酸化ナトリウムの量を通常は約 100ppm に設定している濃度を 1 万 1100ppm に変更したという。実に 100 倍以上である。不正操作に気がついたオペレータによって攻撃者による設定変更はすぐに修正されたが、重大事故に

	つながる可能性があった。 浄水システムの従業員用コンピュータには、外部からのメンテナンス用にリモートデスクトップアプリの TeamViewer がインストールされていた。 その TeamViewer を何者かが遠隔操作で操作し、浄水システムを設定しようとしているのを監視担当の職員が発見した。 その日は 2 度アクセスがあり、その 2 回目の操作では不正侵入者はマウスをドラッグしプログラムを開いてシステムを操作、水酸化ナトリウムの添加量を 100ppm から 11,100ppm に増やす設定をした。侵入者は 3～5 分間ほど作業していた。職員は侵入者が離脱した後に設定をすぐに元に戻したことでトラブルは防ぐことができた。 逮捕者は出ていない。ハッキングがアメリカ国内からのものなのか、国外のものなのかは分かっていない。 特定の職員はインターネット経由で制御システムにアクセスできるようにしていた。リモートアクセスソフト TeamViewer を使って施設内のパソコンに接続し、そこから制御システムにアクセスしていたようだ。だが職員がすぐに気づいて設定を元に戻したため実害はなかった。このときの攻撃者の「滞在時間」は 3～5 分間だったとされる。 2 月 5 日の午前 8 時、コンピュータ画面を眺めていた水処理施設の職員は、自分のカーソルが勝手に動き出したのに気づいた。しかし、上司がよくリモートアクセスして、施設のシステムを監視しているのを知っていたため、職員は、てっきり上司がカーソルを動かしているものと思い、気にもとめなかった。 ところが午後 1 時半頃、職員はまた誰かがシステムにリモートアクセスしてきたことに気づいた。その何者かは、3～5 分ほど、カーソルをあちこちに動かし、ソフトウェアの機能をいろいろ試しているようだった。そして、水道水の水酸化ナトリウムの含有量を通常の 100 倍以上に押し上げた。 職員は慌てて水酸化ナトリウムを通常レベルに下げ、担当者に一報を入れた。水処理施設は、すべてのリモートアクセスを無効化し、司法当局に通報した。 この水処理施設では、業務効率化のため、複数のパソコンに「TeamViewer」と呼ばれるリモートアクセス用のソフトウェアをインストールしていた。それは、IT システムに問題が発生しても、職員同士でデスクトップ画面を共有し、チームワークで解決しやすくするためである。実際に「TeamViewer」を使って、上司が水処理施設のシステムを遠隔監視することもあった。 調査の結果、施設のサイバーセキュリティ体制に 3 つの大きな穴があったことが発覚した。第 1 に、職員間で「チームビューアー」のリモート接続用パスワードが共有されてい

	た。パスワードが共有されていると、万が一、サイバー攻撃者がパスワードを見つけてしまえば、より多くのシステムに不正アクセスされてしまう。また、同じパスワードをずっと使い続けている場合、退職者に不正アクセスされ、情報漏洩してしまう危険性もある。 第 2 に、職員のコンピュータは、ファイアウォールを通さずにインターネットに直接つながっていた。ファイアウォールは、不正アクセスや情報流出を食い止める防火壁に相当する。 第 3 に、この施設では、2020 年 1 月にサポートの終了した Windows 7 を使っていた。メーカーのサポートが終了すれば、サイバーセキュリティ上の問題が見つかっても、対処されず、脆弱なままになってしまう。 アメリカ連邦政府当局は、サイバー攻撃者が脆弱なパスワードと古い OS などサイバーセキュリティの隙を突いて水処理施設のシステムに侵入したものと見ている。
出典 URL1	水道施設に「毒混入」狙ったサイバー攻撃、お粗末すぎるセキュリティーの恐怖 ｜ 日経クロステック(xTECH)（nikkei.com）
出典 URL2	https://news.mynavi.jp/article/20210216-1733488/
出典 URL3	https://www.bbc.com/japanese/55991571
出典 URL4	https://security.srad.jp/story/21/02/09/1550202/
出典 URL5	https://www.itmedia.co.jp/news/articles/2102/09/news137.html
出典 URL6	https://toyokeizai.net/articles/-/418722
出典 URL7	https://news.livedoor.com/article/detail/19686582/
出典 URL8	https://www.cnn.co.jp/usa/35166249.html
出典 URL9	https://pcsoweb.com/21-015-detectives-investigate-computer-software-intrusion-at-oldsmar%E2%80%99s-water-treatment-plant
出典 URL10	https://www.vice.com/en/article/88ab33/hacker-poison-florida-water-pinellas-county

3）米国コロニアル・パイプラインへのランサムウェア攻撃

タイトル	米最大の石油パイプライン停止　身代金要求型のサイバー攻撃
事案の概要	
発生時期	2021 年 5 月 7 日
被害者組織	米国　コロニアル・パイプライン社
被害システム	具体的な被害システムの名称は不詳。 コロニアル・パイプラインへの攻撃では、ハッカー集団がパイプラインの物理的な状態に直接干

	渉したり、潜在的に危険な物理的な状態をつくり出したりできるシステムにまでアクセスしたかどうかは、まだ明らかになっていない。 ハッカー集団が IT ネットワークへの広範なアクセス権を取得しただけでも、コロニアル・パイプラインが安全対策としてパイプラインの操業を停止する十分な理由になる。確実な運用環境のコントロールと明確な運用の可視性を保証できなくなったら、操業を停止する必要がある。
攻撃方法	ランサムウェアによる身代金要求型サイバー攻撃
攻撃を受けてしまった原因	コロニアル・パイプライン社のレガシーな VPN へのログイン。 認証情報として従業員のユーザー名とパスワードが使用された。この認証情報は以前に侵害された別のウェブサイトで従業員が使用した可能性があり、それを攻撃者が利用した可能性がある。 同社 VPN には MFA（多要素認証）が適用されていたが、アカウントが無効化されていない未使用のレガシーVPN プロファイルがあり、そこには MFA が適用されていなかったためにユーザー名とパスワード認証によるログインができた。
被害の状況や影響	民間企業コロニアル・パイプライン社は、アメリカ東海岸の燃料供給の約半分となる 45%を担っているパイプラインで、1 週間にわたって操業停止に追い込まれた。ハッカーに対して 440 万ドル（約 4 億 8000 万円）の身代金を支払った。アメリカ最大規模のパイプラインが停止したことにより、ガソリン、ディーゼル、ジェット燃料などの貯蔵庫が大きな影響を受け、一般市民から燃料が必要不可欠な機関までをパニックに陥った。 自らを「非政治的」だと主張する Darkside と名乗る犯行グループが使用した秘密鍵を FBI が入手したことで、Bitcoin で支払われた身代金約 75BTC の約 85%、63.7BTC の回収に成功したと発表。 一部ビジネスシステムの復旧には数カ月かかるとし、今回の攻撃による損害は最終的に数千ドルに上ると推定した。オペレーショナルテクノロジーシステムに到達できるランサムウェアは、単に IT ネットワークを標的とするランサムウェアと比べるとかなり少ないが、オペレーショナルテクノロジーシステムに感染させようとしているランサムウェア集団の数は増えている。
概要	犯罪者グループ DarkSide は、コロニアル・パイプライン社のコンピュータシステムに侵入、わずか 2 時間で 100GB 以上の企業データを盗み、5 月 7 日には同社を操業停止に陥らせた。ランサムウェア攻撃を受けた同社は攻撃を受けたデータへのアクセスが不可能になるだけでなく、さらに、情報の一部をインターネット上で公開するという旨の複数の脅迫による身代金要求を受けて燃料配給のパイプラインの操業を停止、その結果、アメリカ東海岸の一部でガソリンとジェット燃料の配給が脅かされてガソリンのパニック買いが発生し、5 月 12 日までに 1000 以上におよぶガソリンスタンドでガソリンが無くなってしまうというさらに悪化した状況を招いた。コロニアル・パイプライン社は身代金を支払ったが、6 月 7 日に支払われた身代金の約 85%を回収したと米司法省が発表した。 2021 年 4 月 29 日：DarkSide がコロニアル・パイプライン社のコンピュータシステムに侵入 2021 年 5 月 7 日：データの暗号化、身代金の要求を受け、コロニアル・パイプライン社はパイプライン操業の一時停止を公表、ブラウント氏は身代金の支払いを承認

	2021 年 5 月 12 日：パイプラインの操業を再開するも、供給網の正常化には数日かかるとの見通しを示す 2021 年 6 月 7 日：FBI が身代金の一部を押収 2021 年 6 月 8 日：ブラウント氏、上院の公聴会で事件について証言 アメリカ最大の石油パイプライン「コロニアル・パイプライン」（米南部テキサス州と北東部ニューヨーク州をつなぐ約 8800 キロメートルに及ぶパイプラインを持つ）がロシアのサイバー犯罪者集団「ダークサイド」からランサムウェアのサイバー攻撃を受けて全ての業務を 5 日間停止。ハッカーに対して 440 万ドル（約 4 億 8000 万円）の身代金を支払う。 米南東部でのガソリン供給に混乱が起きたため、予防的な措置と攻撃を封じ込めるため、5500 マイルすべてのパイプラインが停止させた。同社の発表によれば、サイバー攻撃であることは確実であるとし、パイプラインとコンピューターネットワーク、一部の IT システムを停止させたことを認めた。今回の攻撃でも、他の攻撃でも、オペレータは結局、OT（オペレーショナルテクノロジー）全体の生産を停止することになる。なぜなら、何が攻撃の影響を受けたのか、どのように対応すればよいのかを確信できないからだ。 同社 CEO は 440 万ドル（約 4 億 8000 万円）の身代金を支払ったが、ダークサイドの対応は、コロニアル・パイプラインから奪った身代金を複数のビットコインアドレスに分散し、追跡されにくくしたものの、最後には 1 つに集約した。しかし、米連邦捜査局（FBI）はこの口座の秘密鍵を入手し、230 万ドル（約 2 億 5000 万円）を取り返した。 また、ダークサイドについては、2021 年 5 月中旬に活動停止を表明した。
出典 URL1	https://www.nikkei.com/article/DGXZQOGN084D30Y1A500C2000000/
出典 URL2	https://www.bbc.com/japanese/57181463
出典 URL3	https://www.jiji.com/jc/article?k=2021050900043&g=int
出典 URL4	https://www.cnn.co.jp/business/35170423.html
出典 URL5	https://internet.watch.impress.co.jp/docs/column/dlis/1331673.html
出典 URL6	https://www.sbbit.jp/article/cont1/60376
出典 URL7	https://wired.jp/2021/05/10/colonial-pipeline-ransomware-attack/
出典 URL8	https://www.cloudgate.jp/security-news/colonial-pipeline-ransomware-attack-cause-and-why-it-paid-ransom.html
出典	https://www.bbc.com/japanese/57068072

URL9	
出典 URL10	https://japanese.engadget.com/doj-recover-bitcoin-ransom-from-colonial-pipeline-attack-073045787.html
出典 URL11	https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown

3. ビルシステムのサイバーセキュリティ推進体制の調査

ビルにはビルオーナー、建設会社、設計事務所、各種設備ベンダー、運営会社等、多くの立場の異なるプレーヤーが関わっている。このようなマルチステークホルダーの世界においてサイバーセキュリティ対策を推進し、ガイドラインを維持・高度化していくためには、特定のステークホルダーによらず、マルチステークホルダーからなる相応の推進体制を整備していくことが必要である。このため、ビル分野のISAC(Information Sharing and Analysis Center:情報共有分析センター)組織を念頭に、必要な機能、メンバー体制、設立プロセス等について調査を行った。

3.1 推進体制の情報提供・共有・相談等の機能の実践的評価

(1) ビルシステムや構成機器に関する脆弱性等の情報共有及び相談機会の提供

昨年実施した配信と同様に ICSCoE 第 2 期修了生ビルチームのメンバーの協力を得て、ビルシステムに使われるような機器を中心に脆弱性情報とそれを分かりやすく噛み砕いた解説、有効な対策等をまとめてもらい、メール配信という形でビル SWG 構成員を中心に配布を希望する人へより拡大的な配信を実施した。

昨年と違って今年は月次でレポート作成し、その分内容を深く、わかりやすいものとしている。同時に配信に対する質問の受け付けられる体制は維持した。

(2) 上記活動についての意見交換会を通じた評価

ビルシステムの脆弱性情報の配信に合わせて、ビル SWG のメンバーを小グループに分けて情報共有のための会合を開き、その時に配信内容や配信方法、配信コンテンツの使い方などについてのディスカッションを行った。その結果得られた主な意見は次のようなものである。

表 3-1 ビルチームによる配信の利活用に関する情報共有

業種	コメント
ビルオーナー	● ビルセキュリティとしては制御系の話題が中心かと思っていたが、サイネージとか IT 系の議論が含まれており、その辺はどうなのか。 ● PSIRT を持つベンダーと脆弱性についての議論を行ったり、脆弱性の値踏みをお願いすることはあるが、機器によってはブラックボックスになっていて触れないものもある。 ● 今年度の配信はさらに理解が進みやすく、わかりやすくなっている。 ● 使い道としては、記事をもとに本当に自社の管理ビルで使われているのかの確認になるが、なかなか調べ切れないので、もらった情報からある程度のふるい分けをして確認するような工夫が必要となっている。
ゼネコン／サブコン／設計	● レポートもオープンに出しても良いなら、その旨を書いて送ってもらえると、興味のありそうな人にも展開できてよい。 ● わかりやすいレポートで参考になっている。一方で、営業とか前線の人たちに

	どう展開するかは課題となっている。 ● 我々ではわからない世界なので、専門家が解説をしてくれるのはありがたい。ただし立ち位置的に展開は難しく、ベンダーが受け取って、オーナーに伝えるなどのアクションができると良いと思う。 ● こういう脆弱性情報がデータベース化されて、ホワイトな機器を確認できるといいと思う。 ● 非常にわかりやすくなったと思う。ビル管理や設備管理はこのような情報の専門家ではないので、わかりやすさは大事である。さらにファーストアクションとして何をすべきなのかもあるとより役立つと思う。 ● もらった情報の解釈に困っている。セキュリティリスクについて脆弱性などを分かるようなサービスがあるとありがたい。そういうのがあると、顧客にサービスごと提案を持っていくことができる。
ベンダー	● レポートについては業界団体等からさらに展開できると良いのではないか。 ● 中身は非常によく書かれており、対策もきちんと書かれていて、よくできていると思う。続けてもらえると普及に役立つと考える。 ● 誰向けなのかが難しいと思う。ネットワークにつながざるを得ない部分を抱えた人は見るかもしれないが、既存のビルの人はあまり見ないのではないか。 ● グループ会社で脆弱性配信があるが、それをディスパッチするのが大変である。受信した情報の仕分けが難しい。 ● 放置したらどういう影響があり得るかも知ることができると、現実感が出てよいのではと思う。」 ● 配信情報は興味深く見ている。自社の PSIRT でも同じような脆弱性情報を全社にブロードキャストする活動をしており、内容的に違和感はない。一方、沸騰ワードの取組は面白いと思う。 ● 社内でセキュリティ情報を一括配信している部門も配信先として加えてもらったので、展開が進めやすい。 ● 普段はあまり十分に見られていない。社内教育の事例などで展開できればと思う。

3.2 推進体制のあり方の調査

（1） ガイドラインの活用等の情報共有による相互信頼の醸成

昨年度と同様にビル SWG 構成員を小人数のグループに分けて、小グループ検討会として、情報共有・推進体制についてのディスカッションを実施した。まず、この 1 年間のガイドラインの利用状況やサイバーセキュリティへの取組について情報共有と意見交換を行った。また今後の推進体制の在り方の検討をにらんで、短期的に取り上げてもらいたいテーマや中長期の推進体制の在り方についての意見をいただいた。なおこの小グループ検討会は、前述の ICSCoE ビルチームとの配信に関する意見交換会も

兼ねて実施している。

小グループ検討会で集まった参加者の主な発言は次の通りである。

表 3-2 ガイドラインの活用やサイバーセキュリティへの取組についての情報共有

業種	コメント
ビルオーナー	● ガイドラインをもとにセルフチェックシートを作り、既存のビルに一通り適用してみた。できているところ、課題のところがわかってきたが、解決のためにはベンダーとも協力していくことが必要。ただし、ベンダーによって考え方や対応のばらつきがある。 ● ガイドラインは従来の制御システム部分の確認で使っている。ロボットや IoT などの新しい利用スタイルについては、IT の方で考えている。ただし IT と OT の接合点をどこで考えるのかなどまだ調整が必要であり、社内で議論している。 ● ビル単体というより、スマートシティとか DX とかの大きな枠組みで議論をしている。ただし DX の使い道の話の段階で、個々のセキュリティ確保の話はあまりない。 ● 自社独自のガイドラインを作っている。当初は防御のみの視点だったが、METI のガイドラインの他、米国やドイツのガイドラインなども取り入れて、検知や対処復旧などの観点からも実現可能なものをピックアップして、ブラッシュアップをしている。 ● METI のガイドラインの影響はそれなりにある。読み込む中で、情報セキュリティでは認識、防御、検知、復旧も大事という認識が深まり、自社ガイドラインのブラッシュアップを行った。METI のガイドラインも言っているシーンは同じだが、言い方が異なる。現場としては最低限やることは明示するようにしている。 ● ビルは重要インフラではないが、何かがあってからでは遅いという意識で、テナントに安心安全を提供することが重要と考えている。 ● ネットの入り口がどうなっているかなどのヒアリングを実施し、いくつかの既存ビルで使ってみたが、それ以上には活用しきれていない。ビルごとの担当者のレベルも異なり、ヒアリングに行くのも委託先なので、現場のレベルアップがまず課題である。
ゼネコン／サブコン／設計	● 大手デベロッパの大型物件では、ガイドラインの参照を言われるケースが少しある。ただし、設計に 3 年、建設に 2～3 年掛かる世界なので、実際のビルで実現するにはまだ時間がかかる。 ● 照会があるのは、ほとんどがビル SWG に参加している会社からで、それ以外への広がりがまだない。 ● 見積もりを求められる際に仕様として、機器のパスワードを初期設定から変更して入れることや、LAN のポートを物理的に塞ぐことなどが書かれるケースもあり、少しずつ浸透してきている気がする。

	● 最先端のクラウド型 BA のようなプロジェクトでは今までの成果を取り入れて対策を進めたりしているが、せいぜい年間数件のレベルである。一方で大部分の一般のプロジェクトではまだセキュリティが気にされることはない。 ● 施主からガイドラインを参照するよう求められるケースが少し出てきた。既存ビルのチェックもしたが、できているところ、できていないところを選別し、ここは人的に守るから大丈夫という判断のところは顧客と調整したりした。 ● 数は少ないがクラウドとビル設備が連携するようなケースについて確認を求められることがあり、ガイドラインを活用して検討したりしている。いままでは指標がなかったが、ガイドラインは METI の名前で作られたということで、顧客にも納得してもらえる部分がある。 ● 別表を使った確認をした。設計フェーズの項目を使用して対応の可否をベンダーに埋めてもらったり、構成の提案をもらって、それを顧客に判断してもらうよう方法を取った。ガイドラインの記述は解釈に幅を持たせた記述なので、自社としての解釈を加えたりして調整している。経験を積むことで、建物設備として必要な機能は何かが少しずつ見えてきた。一方他社がどういう基準を持っているかは気になるところで、可能な範囲で共有できると良い。
ベンダー	● 大手デベロッパを中心にガイドラインへの対応状況を施主から求められるケースはある程度は存在する。ただし現場が追い付いておらず、受け答えがスムーズに行っていない。 ● Log4j 以降、脆弱性情報を顧客にどう公開していくのかも議論になってきている。 ● 海外のグローバル IT 企業にはセンシティブなところも多い。独自のチェックシートが送られてきて、主に技術的な内容で暗号化機器の話やビット長などもチェックされる。 ● 顧客のセキュリティ要求にカスタマイズ対応でやることはあるがコストが掛かるので、特定顧客に限られる。 ● ビル分野のベンダーだけでなく、ユーザーも集めた検討会を始めようとしており、ブレーンストーミングから開始している。 ● ビルのセキュリティアセスメントサービスをグループ企業向けにやっている。ガイドラインの他に 62443-2-1 を使って、独自の点検シートを作り、インタビュー形式で確認をしていった。ただし現地の担当者がセキュリティに知識がなく、コミュニケーションが課題となった。またビルによって状況も異なるので、それらを横並びでどう相対的に評価するかという点も難しかった。判断のレベルは顧客側と調整しながら決めている。 ● 通常の業務の中でどう利用するか検討し、まずは社内の人事教育が大事ということで始めている。 ● 大手デベロッパからはガイドラインをもとにしたチェックリストが展開されて聞かれることも増えている。また自社製品そのもののセキュリティ強化のため、PSIRT なども置いて活動している。

	● PSIRT 体制やインシデント対応体制を構築している。脆弱性を作らないこと、脆弱性をいち早く検知すること、事象が発生してしまった場合のインシデント対応の3つが大事であり、それぞれに取り組んでいる。最近では社内での脆弱性発見も増加しており、経験を積んで進化させるようにしている。 ● METI ガイドラインも見ているが、各団体や IPA のガイドラインなども見て、製品の特性に応じて対応している。 ● SWG に参加している会社からの問い合わせはあるが、それ以外にあまり広がっていないように感じる。

（2）短期的な検討テーマ及び中長期の施策の検討

小グループ検討会では今後の推進体制の在り方の検討をにらんで、短期的に取り上げてもらいたいテーマや中長期の推進体制の在り方についての意見をいただいた。

表 3-3 今後の推進のあり方についての意見交換

業種	コメント
ビルオーナー	● 今の国の規制やガイドラインは、仕様規定になっているが、現場で業務に使うには性能規定に変えていってほしい。一方で現在のガイドラインは細かすぎるところもあり、大枠を知る意味では NIST CSF などが役に立つ。 ● 情報共有のメンバーとして、通信系やネットワーク会社などもいたほうがいい。制御系に特化するのか、そうでないのかなどの整理も必要と思う。今後は画像系や個人情報対応なども考える必要がある。 ● ビル ISAC については関係者の準備がまだできていないという理解である。新しい利用スタイルへの対応の議論を並行しつつ、関係者間の調整が必要で、すぐに立ち上げる必要もないと思う。
ゼネコン／サブコン／設計	● 例えば四半期ごととか、時期を決めて定期的に集まれると良いと思う。 ● セキュリティは社外秘も多い世界なので、ざっくばらんに情報交換できる組織があると助かる部分はある。他社の状況も聞きたいし、マルチステークホルダーな構造でそれぞれの役割があるなかで、定期的な会合ができると良いと思う。 ● IT ではゼロトラストの考えが出ているが、OT でも無視できないようになるのではと思っており、今後は従来のセキュリティ対策とどうアジャストしていくかが課題だと思う。 ● 設備ごとのガイドライン整備を進めていってもらいたい。それらが一揃い揃うと施主との話にも活用しやすくなると思う。
ベンダー	● ガイドラインのメンテナンスについては、スケジュールを定めて、それに合わせて皆で集まるのが良いと思う。 ● CSSC でビルの検討会を始めようとしている。その参加者なども呼べると良いのではないか。 ● 仮に組織を作っても、セキュリティへの積極性がないとなかなか参加してもら

	えない。情報共有といっても念のため情報を聞いておきたい程度の人も多い。 ● 病院などは、厚労省のガイドラインでは境界線防御の考え方がメインとなっている。ビルも同様だが、境界線で防ぐのか、中をどこまで見るのか、サジ加減は難しい。 ● ビルのサブシステムごとにガイドラインができるのであれば利用させてもらいたい。 ● 既存ビルを一通り回っての感想だが、新しいビルを作るときに、ガイドラインをバイデザインで入れるという話にまではなっていない。ガイドライン自体の普及も進める必要がある。 ● 月一での実施とか、もう少し定期的な運営だと助かる。 ● 議論のロードマップがあるといい。議論の全容がわかり難い。 ● アウトプットイメージとスケジュール感が明確だと、適材なリソースを当てはめて議論に参加できると思う。 ● ガイドラインも 3 年目となり少し古さを感じる。年 1 回くらいのペースで小出しでもいいのでバージョンアップが見えると良いと思う。

4. 検討会の運営

上記2. ビルガイドラインの高度化のための調査　及び3. ビルシステムのサイバーセキュリティ推進体制の調査　の実施及び取りまとめにあたっては、専門的な見地からの検討、分析、助言を得ることを目的に、ビルシステムの関係者及びビルシステムのサイバーセキュリティに関する有識者からなる検討会として、ビルSWG及びその作業グループを活用することを想定する。このため、検討会の運営を行うとともに、必要な検討材料を提供し、意見を集約し、調査実施に反映させることを行った。

4.1 ビルSWGの運営

ビル SWG は合計 2 回開催した。初回に空調編の作業について説明をするとともに意見募集を行い、インシデントレスポンスの議論についての頭出しを行った。その後、作業グループを活用して具体的な作業を実施し、その作業結果を 2 回目に説明し、空調編に関しては公開に向けた作業に進むことへの了承を得た。またインシデントレスポンスについては今後議論を本格化させる必要があるので、そのための意見やアドバイスを頂戴した。

4.1.1 第 12 回ビル SWG の運営

(1) 開催概要

日時　2022 年 3 月 4 日 9:00～11:00
場所　Teams 会議(Web 会議)
議題

1. 開会(2 分)
2. 各構成員より挨拶・1 年間の取組について報告(20 分)
3. ガイドライン活用事例紹介(三菱総研)(10 分)
4. ガイドライン・個別編(空調編)の検討について(10 分)
5. インシデントレスポンスの検討について(15 分)
6. 自由討議(60 分)
7. 閉会(3 分)

配布資料:

資料1　議事次第・配付資料一覧
資料2　構成員等名簿
資料3　ビルセキュリティ・アセスメントの事例紹介(三菱総研)
資料4　ガイドライン・空調編の検討について
資料4-1　ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン(個別編:空調システム)(案)
資料4-2　ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン(個別編別紙:空調システム)(案)

資料5　（投影のみ）建物設備システムインシデント対応ガイド説明会資料（JDCC）
資料6　今後の予定について

（2）議事要旨

産業サイバーセキュリティ研究会 WG1 ビル SWG（第 12 回）
議事概要

会議：　産業サイバーセキュリティ研究会 WG1 ビル SWG（第 12 回）
日時：　2022 年 3 月 4 日 9:00-11:00
場所：　オンライン開催（Teams 会議）
構成員（敬称略）：
（座長）江崎　浩　東京大学大学院　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
NTT グループ（株式会社 NTT ファシリティーズ）
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
一般社団法人日本ビルヂング協会連合会
一般社団法人ビルディング・オートメーション協会
株式会社日立製作所
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
ICSCoE 2 期ビルチーム有志
（オブザーバー）

国土交通省（総合政策局情報政策課サイバーセキュリティ対策室）
内閣サイバーセキュリティセンター（東京 2020G）
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
（事務局）
経済産業省（商務情報政策局サイバーセキュリティ課、製造産業局産業機械課）
株式会社三菱総合研究所

議題：
1．各構成員より挨拶・1 年間の取組について報告
2．ガイドライン活用事例紹介（三菱総研）
3．ガイドライン・個別編（空調編）の検討について
4．インシデントレスポンスの検討について
5．自由討議

議事：
1．各構成員より挨拶・1 年間の取組について報告

- 顧客とのやり取りにセキュリティチェックシートがあるが、この 1 年間で増えたという感覚はない。ただし DX が推進されるなかで、自社提供システムと顧客システムの接続が増えてきている。
- 顧客との間でセキュリティ対策の話はかなり定常的に出てくる。
- 顧客からビルの設備ネットワークのセキュリティについての問合せが数件あり、ビル SWG で検討したチェックリストを使って話を進めている。
- ビルのネットワークの接続状況について、チェックリストをもとにした確認作業を数ビルで実施した。
- ガイドラインの活用は増えてきているとは思うが、現場の技術者の知識や理解度はまだ上がっていない。建設業界は慢性的に技術者不足が続いており、ビルシステムの試験に十分な時間が取れない。
- 設備面のチェックリストを作成し、数件のビルについてチェックを実施した。今後さらに対象ビルを広げていく予定である。
- ビルシステムに不正端末が接続されたことを検知する仕組みを一部のビルに導入した。これ

までは机上や実証実験レベルだったものが、実装できるレベルになってきた。

- ビルにとどまらない公共空間の利活用やスマートシティ関連、ロボット利活用のときのビルの設定など、少し複合しているところについて、流れを作ってほしいという声が聞こえている。
- 最近は現場では、サイバー空間とフィジカル空間を融合したセキュリティについて言うことが多くなった。
- 見積もりの要件仕様にはまだサイバーセキュリティの要件は載ってきていない。新築でそういう取組への浸透は薄い。
- ロボットやセンサーをネットワークにしたときのセキュリティはこれからの課題になると思う。可用性の観点からビルの複雑化に伴う障害の増加も課題になっていくと思う。
- 最近はアクセス制限や物理的にネットワークを切り離すことで守るという意識から、認証されたメンバーに囲われた中で安全なコミュニケーションやデータ共有をするという形に変わってきている。
- 社内向けのビル制御システムに関する指針をブラッシュアップした。また、物件全てを対象に、チェックリストに基づく点検を実施した。ファイアウォールの設定を厳格に運用する取組や、それでも入られることを前提として検知する仕組みの導入を始めている。
- ビル建設の現場において工事や設計の段階のセキュリティ対策をガイドラインに基づいてチェックしているが、まだ何か壁を感じている。
- 最近は実際のプロジェクトにおいて顧客からガイドラインに従ってやっていきたいとか、設計書に反映して欲しいというリクエストを受けることが増えてきた。社内でチェックリストを作り、プライオリティをつけて着実に反映していくよう進めている。
- 取組の状況には温度差があるということで、かなりアクティブに行っているところ、あるいはまだマーケットの方が反応しておらず受身のところもある状況だと分かった。

2．ガイドライン活用事例紹介（三菱総研）

（三菱総研より説明）

3．ガイドライン・個別編（空調編）の検討について

（事務局より説明）

4．インシデントレスポンスの検討について

（JDCC・竹中工務店より説明）

5．自由討議

（１）トリアージについて

- インシデントレスポンスではトリアージが必要だが、実際にやるにはかなりの知識が必要で、BA システムや IT の知識、その経験も必要になる。
- BA 運用の現場はトリアージの知識はない。システムやネットワークセキュリティの会社は BA に詳しくないので、一緒になって高めていく必要がある。
- インシデントレスポンスにおける保全だが、粒度の問題として切り分けができると良い。末端のシステムはクリーンインストールして、最低限のコンフィグさえあれば原状復帰できるという考えもあるので、局所最適化されたパッケージングが進んでくると、現場の負担感は軽くなると思う。
- 機能安全の観点から設計で安全側に倒すようなアルゴリズムが予め入れてあれば、インシデント対応に反映させられると思う。
- ビルのコントローラもリブートすれば元に戻るのだが、個数が多いので、遠隔実施を考えないといけない。細かいパラメータの再調整の部分まで入れる仕組みを作れば、ビルの予防策として使えると思う。

（２）コミュニケーションと認証について

- BIM とか CAD などを共通のプラットフォームに載せて情報共有すると良いが、現場はまだエクセルとかで、そこに大きな乖離がある。本当は BIM を共有できると美しいが、その途中段階でも、今ある共有基盤に認証の枠組みを用いてデータ共有を実現するすると、物事が進むようになると思う。多くのステークホルダーがいるビルでは、大手デベロッパが認証基準を示して、プロジェクトごとに関係者のアカウント管理をして、その中で業者同士のデータの引き継ぎが行えるようになると大きく前進する。
- インシデント対応の中でコミュニケーションの話しも大事である。

（３）現場意識の乖離について

- ビルの現状との乖離は大きい。トリアージをするにはインシデントに気付く必要があるが、そのためのツールがビルのシステムに入っていない。BA 全体として IP を使っていても、全てが１つのネットワークにつながっているわけではなく、別々に細かなネットワークが多数存在している。IT の世界ではあたり前のものが、BA や OT の世界では乖離している。こうしたいという理想形があるが、そうできないという事情が広くあるのが現場の肌感覚であり、業界をあげて意識を変えていかないと難しい。
- 関係者に問題意識を持ってもらうことは、非常に重要な仕事になると思う。経営サイドの必須条件として意識を持っていただくことも重要である。現場の意識の乖離については、ガイド

ラインとは別に議論をしないといけない。

（４）ロボットや他システムとの連携について

- 最近、ビル業界で挙がっているユースケースとしてロボットがエレベータと連携するというのがある。悪いことをやろうとすると、ロボットがセキュリティラインを越えて人に替わって情報を窃取することが考えられる。システム・オブ・システムで考えてリスクを見定める方向になっていけばと思う。
- ビルでいろいろなロボットを試験的に使ってみたり、実証をしたいという話しはある。ロボットでエレベータを呼びたいという話しになり、どのようにつなぐのかというと、インターネット経由でつなぐという話しが無邪気に出てくる。
- 自動運転車がビルの駐車場に入ってくるようになると、ビル側と通信をしないと駐車場に入れないという話しが出てくる。今後 DX が進むと、ビルと外部との通信は必須なものになるので、少なくともビル内でしっかりと外部との通信ルールを決めておかないと危ないことになる。
- 一時期はビルに安価なモニタリングセンサーが大量に付けられた時期があった。現在、BA にもいろいろな新しいものがつながってきているが、一般ビルほどそういうものを安易に導入する傾向がある。ビル SWG では、一般ビルに向けたリスク喚起のような提言も必要になるかと思う。

（５）エレベータのセキュリティについて

- エレベータ業界でもインターネット経由でロボットとつなぎたいという話しが持ち上がっているが、ロボットを作っている相手メーカーの素性がわからない状況で繋ぐ必要があるケースが出てくることを懸念している。その点を踏まえて、エレベータのセキュリティをどう担保するかという議論が始まろうとしている。
- 海外では、エレベータが Amazon のインターネットサービスとつながったり、オープンネットワークとつながるケースが増えてきている。ISO でもエレベータをどのようにセキュリティから守るかの基準策定が現在進行中である。
- 昇降機個別でオープンネットワークからの操作を一定レベルで止めたり、ディフェンスするシステムを組んでいかないと防御はかなり難しいと思う。この辺のセキュリティ対策はこれから大きな課題になる。
- 今までクローズドだったことを安全の理由にしていたエレベータが変わりつつあるということだと思う。その際に認証の基盤をしっかりと埋め込みなさいという話しで、ゼロトラストを含めた認証の話しが進むと健全な方向に向かうと思う。
- 認証後の振る舞いも考えないといけない。悪意をもってロボットがエレベータを操作すると、ビ

ルの交通量を遮断することも論理的には可能になるので、運用面も含めて議論をしないといけない。

- 一歩一歩最終ゴールを見据えて上手に業界に展開していただいて、今回空調でやったようなことをエレベータでもぜひ進めていくということだと思う。
- こういった機会にエレベータのチェックリストが加速できればいい。

（６）一般ビルでのインシデント対応について

- データセンター協会でインシデントレスポンスのガイドをまとめるにあたって、細かい議論や深い議論があって今のものになっていると思うが、一般のビルだとさらにシュリンクさせないといけない。
- どの段階で何をもってインシデントと認識するのかという判断の課題がある。インシデントの予兆を捉えるために、通信のモニタリングや機器認証の議論は出たが、一般ビルに適用するのは厳しすぎる。その線引きについて、一般ビルによってもレベルがあると思うので、そういう議論が必要である。
- ビルの大きさによっても、インシデント対応をフルパッケージで内製化できるところと、そうではないところが存在しているのが悩ましい。大手はフルパワーでできるが、そうではないところをどうするのかという議論もやる必要がある。
- 何かがおかしいという状況が起きて、機器をメーカーに送って確認してもらったら、故障じゃなくてどうもサイバーだったと後になってわかるケースが多いという話があり、検知が大きな課題になるという気がした。そういう点を含めて、どういうものをインシデントとして、特にサイバーとして捉えるのかというところから、ビルではどうなのだろうという議論が必要だと思う。
- フルパワーでできないようなケースについても、中小ビルなどをクラウドで束ねて監視制御しているという話もあり、小さいビルなどはそういうところが束ねて面倒を見てあげることで、インシデントを捉えられるのではないかという議論にもできる気がした。
- 非常に細かいフルパッケージにすると取組意欲が湧きにくいので、ミニマムに出来るようにというのも考えている。
- ビルのサイバーセキュリティも大分進んで来ている一方で、大多数はユーザーもベンダーもそこまでは来ていないという認識が共有できたと思う。その対応をどうするかを考えて、ガイドラインの書きぶり、主張もシャープにしないといけない。

（７）FA との関連について

- 規模の話や DX の話しに関し、外との広がりのレベルとかも考慮して、マトリックスになると良いかと思う。FA の中で物理セキュリティもテーマになるので、このガイドラインともシームレスに

なるとありがたい。

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

（3）ロジ業務の実施

会議運営のためのロジ業務（日程調整、Web会議環境確保、会議運営に必要な備品等準備、資料準備、Web 会議室設営、出欠、会議運営、議事録作成、有識者委員に対する謝金支払い等）を実施した。

4.1.2 第 13 回ビル SWG の運営

（1） 開催概要

日時　2022 年 3 月 28 日 13:00～15:00
場所　Teams 会議（Web 会議）
議題

1. 開会（2 分）
2. ガイドライン・個別編（空調編）の検討について（10 分）
3. インシデントレスポンスの検討について（10 分）
4. ビルシステムセキュリティに関する情報共有について（10 分）
5. 自由討議（85 分）
6. 閉会（3 分）

配布資料：

資料1　議事次第・配付資料一覧
資料2　構成員等名簿
資料3　ガイドライン・個別編（空調編）の検討について
資料3-1　ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（個別編：空調システム）（案）
資料3-2　ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（個別編別紙：空調システム）（案）
資料3-3　いただいたコメントへの対応について
資料4　インシデンレスポンスの検討について
資料5　ビルシステムセキュリティに関する情報共有について

（2）議事要旨

産業サイバーセキュリティ研究会 WG1 ビル SWG（第 13 回）
議事概要

会議： 産業サイバーセキュリティ研究会 WG1 ビル SWG（第 13 回）
日時： 2022 年 3 月 28 日 13:00-14:10
場所： オンライン開催（Teams 会議）
構成員（敬称略）：
（座長）江崎 浩 東京大学大学院 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
NTT グループ（株式会社 NTT ファシリティーズ）
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
一般社団法人日本ビルヂング協会連合会
一般社団法人ビルディング・オートメーション協会
株式会社日立製作所
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
ICSCoE 2 期ビルチーム有志
（オブザーバー）
国土交通省（総合政策局情報政策課サイバーセキュリティ対策室）
内閣サイバーセキュリティセンター（東京 2020G）

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

（事務局）

経済産業省（商務情報政策局サイバーセキュリティ課、製造産業局産業機械課）
株式会社三菱総合研究所

議題：

1．ガイドライン・個別編（空調編）の検討について
2．インシデントレスポンスの検討について
3．ビルシステムセキュリティに関する情報共有について
4．自由討議

議事：

1．ガイドライン・個別編（空調編）の検討について

- 意見は全部出させていただき、基本的にすべて反映されている。

2．インシデントレスポンスの検討について

- JDCC の資料のインシデント対応概要の中にフォローアップがあり、これが非常に重要である。インシデントの発生の後の報告や情報公開に関して、ビルシステムの業界では、きちんとした会社としての体制、ルールが、まだまだ出来上がってないのではないか。会社のガバナンスの中に組み込むことが重要である、ということを書き込むとよい。
- インシデントレスポンスについて、実際にはサイバーによるインシデントなのか故障によるインシデントなのかの区別つかないということが大きな議論のポイントである。汎用的なインシデント対応フローのようなものを用意し、これをベースに各社で体制等を議論してもらうという方法もあるのではないか。
- インシデントレスポンスで封じ込めをした後に、どのように報告するのか、自社内の経営層も含めるようなワークフローを書いてよいのではないか。事故発生時だけでなく、普段のオペレーションの中でも、未遂も含めて報告するパスを最初から組み込んでおくと、起きていることが経営層に自然に伝わっていくので、理解も得やすくなる等の良いサイクルが回ってくるのではないか。
- データセンターのガイドラインは、事故が起こらないようにということを前提として作られている。一方で、一般のビルの場合はそうではない場合もあり、復旧を早くするためのフローというも

のを意識してガイドラインを修正してはどうか。

- どのようにして常時議論、情報共有ができるチームをつくるか、ということが非常に重要である。
- ガイドラインの中に事例的に書き込めると、緊急性の高い、重要性の高いビルの守るべきポイントを中心に、インシデントレスポンスの対応フローの検討や、データのセパレーション等の封じ込めがやりやすいのではないか。
- 設計の立場、運用の立場からそれぞれ意見交換しながらセキュリティを考えることが今後必要であり、その体制が必要ではないか。ビルオーナーが全体の調整をして、運用側、設計側を含めた体制を組めると良いと思う。そのようなことを今後、ガイドラインや SWG の中で提案していきたい。

3．ビルシステムセキュリティに関する情報共有について

- どのようにして、ビルオーナー、ゼネコン、ベンダー間でコミュニケーションの事例を作っていくかということ、SWG に参加されていない各社に向けて、どのように情報発信していくかということが重要ではないか。
- ガイドラインとしてつくられたものを自社のビルの対策に反映していくことが難しい、使う人に伝えていくことが難しい、というご意見も頂いている。これらの情報をいかに使う人にわかるように伝えていくか、ガイドラインの中身の質と共に教育についても枠組みとして考えていく必要がある。
- リスクアセスメントに関連して、優先順位が示されると良いのではないか。優先順位があると、設計の段階でどこをセパレーションしておけば良いのか等の設計方針を示すことができるのではないか。
- 運用に関連して、ログ分析基盤が心臓部分であると感じている。ログを残して検索できるようにしておくことで、すぐにアクションも取れ、事実を把握することができることにつながる。ログ分析基盤が丁寧に作られると、問題の切り分けから、判断からすべてが加速される。
- ビルシステムのログは、適切なものがとられていないのが現状だと思う。どのようなログをどのように取るのか、ベンダーと一緒に検討させて頂けると非常にうれしい。ビルオーナーだけではとてもできない話である。
- 機器の動作ログを取っていくことによって、機器の故障の予兆を発見する等の予防保全にもつながる。

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

（3） ロジ業務の実施

会議運営のためのロジ業務（日程調整、Web会議環境確保、会議運営に必要な備品等準備、資料準備、Web 会議室設営、出欠、会議運営、議事録作成、有識者委員に対する謝金支払い等）を実施した。

4.2 作業グループの運営

調査を効果的に実施するために、3 種類の作業グループを合計 13 回運営した。空調編に関する具体的な検討作業は空調編作業グループで実施し、インシデントレスポンスの検討はインシデントレスポンス作業グループで実施した。また、情報共有や推進体制のディスカッションはビル SWG 構成員を小人数で分けた小グループの検討会で実施した。

4.2.1 小グループ検討会（空調編作業グループ）の実施

3 回開催し、全てを通してコメントへの対応の検討と具体的な修正案の検討を行った。基本的にメンバーは固定で、日程的に出席可能な者が出る形で運営した。

メンバーは、イーヒルズ、九電工、きんでん、竹中工務店、CSSC、アズビル、ダイキン工業、BA 協会、経済産業省、事務局である。オブザーバーとして日立ジョンソンとアライドテレシスも登録されている。

（1） 各回開催概要

1） 第1回

日時： 2022 年 3 月 17 日 14:00～17:00
出席： ダイキン工業、アズビル、きんでん、イーヒルズ、事務局

2） 第2回

日時： 2022 年 3 月 18 日 16:00～18:00
出席： ダイキン工業、BA 協会、九電工、アズビル、CSSC、事務局

3） 第3回

日時： 2022 年 3 月 25 日 13:00～18:00
出席： ダイキン工業、BA 協会、きんでん、アズビル、事務局

（2） 主な議題

- 空調編の修正作業（コメント対応）

4.2.2 小グループ検討会(インシデントレスポンス作業グループ)の実施

4回開催し、初めの 3 回は第 13 回ビル SWG に先立って検討方針や入り口の議論を実施した。4 回目は第 13 回ビル SWG を踏まえて、今後の進め方について議論を実施した。

メンバーは、イーヒルズ、九電工、きんでん、竹中工務店、CSSC、経済産業省、事務局である。

(1) 各回開催概要

1) 第1回

日時: 2022 年 3 月 18 日 12:30～13:30
出席: イーヒルズ、竹中工務店、CSSC、事務局

2) 第2回

日時: 2022 年 3 月 22 日 12:00～14:00
出席: 竹中工務店、きんでん、イーヒルズ、CSSC、事務局

3) 第3回

日時: 2022 年 3 月 24 日 9:00～11:00
出席: 九電工、きんでん、竹中工務店、CSSC、イーヒルズ、ICSCoE ビルチーム、事務局

4) 第4回

日時: 2022 年 3 月 29 日 10:00～11:00
出席: 九電工、竹中工務店、CSSC、ICSCoE ビルチーム、事務局

(2) 主な議論

- 検討の進め方
- 対象の設定
- 検知の方法
- 今後の具体的な作業の進め方への意見

4.2.3 小グループ検討会(情報共有・推進体制ディスカッション)の実施

ビル SWG から 2 名ないしは 3 名に出席してもらう形式で開催し、それぞれの取組などについて大人数では言い難いことも議論できるように、小人数でより深く踏み込んだ議論ができることを目指している。他に配信コンテンツを素材とした議論も兼ねるため、ICSCoE ビルチーム、経済産業省、事務局も出席している。全部で 6 回開催した。

（1） 各回開催概要

1）第１回

日時： 2022 年 3 月 17 日 10:00～11:00
出席： 不動産協会、三菱地所、ICSCoE ビルチーム、事務局

2）第２回

日時： 2022 年 3 月 17 日 15:00～16:00
出席： ダイキン工業、アズビル、イーヒルズ、きんでん、ICSCoE ビルチーム、事務局

3）第３回

日時： 2022 年 3 月 23 日 10:00～11:00
出席： 竹中工務店、セコム、CSSC、ICSCoE ビルチーム、事務局

4）第４回

日時： 2022 年 3 月 23 日 14:00～15:00
出席： 三井不動産、日建設計、ICSCoE ビルチーム、経済産業省、事務局

5）第５回

日時： 2022 年 3 月 24 日 13:00～14:00
出席： 鹿島建設、九電工、NTT グループ、ICSCoE ビルチーム、事務局

6）第６回

日時： 2022 年 3 月 24 日 16:00～17:00
出席： 日本生命、BA 協会、日立ビルシステム、三菱電機、ICSCoE ビルチーム、事務局

（2） 主な議論

- 自社のガイドラインを利用した取り組み、サイバーセキュリティへの取組
- 配信コンテンツへの意見、要望、配信の方法等への意見、配信の使い方についてのコメント
- 短期的に取り上げてほしいテーマ、情報共有のあり方、中長期の推進体制への意見

5. 総括

本調査では、ビルシステムのサイバーセキュリティ確保のための個別システム向けガイドライン作成の一環として、空調編ガイドラインを公開案まで仕上げることができた。今後は公開に向けた次のプロセスに乗せられることを期待する。

そして、今回から新たにインシデントレスポンスの議論を開始した。日本データセンター協会のインシデントレスポンスガイドが先行して存在しており、それを参考にしながらの作業となるが、データセンターと一般ビルでは用途も要求レベルも異なるものがあり、まずはその点を深く認識し、一般ビル向けの議論をどのように進めるかを検討するところから始まっている。来年度はさらに議論を活発化させる必要があるが、今までのビル SWG に参加している人たちとは別のビルシステム運用の現場の人たちともコミュニケーションを取り、その実態を探りながら検討することが必要との示唆を得ることができた。

サイバー攻撃もますます高度化し数も増加している状況の中で、弱いところが狙われるというロジックに従えば、いつビルが本格的なターゲットとして狙われるようになるか予断を許さない状況であり、ガイドラインの普及や対象の増強を図るとともに、攻撃事例等の情報は常に探っていく必要がある。また、ビルシステム関係者による自主的な推進体制の整備が求められるところだが、全体的にはまだそこまで準備ができていないという意見もあり、引き続き現実的に実現可能な姿を探っていく必要がある。

情報共有のディスカッションの中では、ガイドラインができて 3 年がたち、そろそろアップデートが必要ではないとの意見も出ていた。インシデントレスポンスを取り込むための改訂のタイミングでこれらの対応も検討する必要があるかもしれない。

サイバーセキュリティは留まることなく不断の活動を継続していかないといけないところがり、ビルの分野も引きつづき、サイバーセキュリティ対策のメニューを増やし、その推進に取り組んでいくことが重要である。

令和3年度サイバー・フィジカル・セキュリティ対策促進事業

（ビルシステムのサイバーセキュリティ高度化に向けた調査） 報告書

2022 年 3 月

株式会社三菱総合研究所
デジタル・イノベーション本部
TEL (03)6858-3637