情報システム・バックアップオフィス研究会（ITBO） 2022 年度 10 月度議事録

1. 開催概要

- 開催日 ：2022 年 10 月 27 日（木）18:00～20:00
- 開催方法 ：ZOOM 開催
- 進行役 ：加藤
- 議事録作成： 大塚
- 出席者数 ： 6 人 （敬称略 順不動） 加藤、野原、水落、岡田、芦田、大塚

2. 議事内容

（1） ITBO 研サイボウズ使用ルール

・資料共有：年度ホルダーを作って月例研究会とトピックのフォルダーを分ける。議事録（案）も放り込む。メール添付の資料はやめて共用ホルダーの URL を添付する
・ディスカッション：掲示板にトピック（カテゴリー）を付加しておく
・会議開催連絡：今まで通りメーリングリストによる通知を継続する
・出欠確認：スケジュールの登録の付加機能を利用

（2） BCAO 運営会議報告（10 月 3 日（月）開催）

・中小企業事業継続研修会続行中
・ITタスクフォース作成テキストのレビュー＆理事会承認。10/31 中小企業オープン勉強会ﾃﾞ 指田座長講演
・SAAJ（システム監査人協会）との合同会議（第一回）を 11/14（月）に予定。意見交換を行う
・事業継続上級管理士の募集・試験の実施予定について
・BCAO HP のリニューアル
・ぼうさい国体実施報告

（3） サイバーセキュリティをめぐる最近の話題

・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）第 1 版
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
・ビル空調システムに対するガイドライン、制御セキュリティの一環
・EUサイバーレジリエンス法（案）2025 年をめどに施行。GDPR に続くものとして日本にも影響あるか注意

（4） ビルシステムのCPセキュリティ対策（第一版）個別編

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_building/pdf/20221024_1.pdf
・2019 年発行のビルシステムのCPセキュリティ対策（第一版）が母体
（https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_building/20190617_report.html）
・経産省の産業サイバーセキュリティ研究会のサブワーキング報告書。中でもビルサブワーキングが先行
・ビルシステムとはビルの資産管理運用を行う制御システム。電力・熱源・空調・照明・防災・エレベータ等。サイバーセキュリティ考慮がなかった
・近年情報ネットワークに接続されてきている。（通常のイーサネット接続）制御IPネットワーク（BACnet）
・この領域は ITBO 研会員である大成の関山氏が専門ではないか？
・ビルシステムは工場制御システムほど複雑ではないので分かりやすいのではないか
・2016 年ウクライナで電力会社へのサイバー攻撃で停電発生の事例ほか照明制御システムハッキングなど 5 例紹介
・シャープのマスクネット販売のシステムが、管理システムと同じサーバに構築されていたため、
マスクの大量受注によるシステムダウンの影響を受けて管理システムが使えなくなってしまった例があった。
・ビルは建設後、50 年近くにわたって非常に長期の運用を行うことが一般的
・ビルの企画から建設、運用、そして最終的な撤去まで、幾つかのフェーズに分かれた非常に長いライフサイクルを有している
・ビルの持ち主としてオーナーがおり、建設に当たってはゼネコン、個別の設備に対応したサブコン、更に設計事業者、個別の設備を納入するベンダがいることが特徴。
・個別編、空調システムで具体的な内容を検討する
・空調システムは、温度湿度を管理。セントラル空調方式（大規模向け）と個別分散空調方式（中小向け）がある

・大規模ビル セントラル空調システム、大規模ビル 個別分散空調システム、中小規模ビル 個別分散空調システムとも一般的な制御システムに類似しているためサイバーセキュリティの考慮点は同じ
・リスクアセスメントから開始してできるところから段階的にすすめる
・空調システムだけやっても全体的な対策がなければ意味がない。しかしビルシスエムのステークホルダーが多く多様であるため困難が予想される。
・データセンタのサーバ室や病院、極寒地のホテル等空調機能を消失することによって深刻な被害を受ける
・上位システムの HMI が攻撃されたことで、空調システムの動作モード、温度設定値等を書き換えられ、本来の動作から逸脱してしまう、など起こりうるケースを想定する
・対策として空調システムを基幹ネットワークから切り離した状態で、空調機能を単独で維持できることが重要
・個別分散空調方式では、サイバー攻撃によってプロトコル変換器が攻撃され、空調システムとして正常動作しない場合を想定し、空調機を単独で操作できるコントローラ等の別の手段を設計時に配慮しておく
・セントラル空調方式では、空調機のみの冗長化や復旧では空調システムを維持できない場合を想定
　上位ネットワークから切り離された状態で各コントローラが自律的に行う制御や手動操作で最低限必要なレベルの空調を動作できる設計及び体制を構築する
・マルウエア（ランサムウエア）感染以前に作業ミス、設計考慮が不足していたための事故が散見される。BIA 視点でリスクの洗い出し検討を行う必要がある
・空調システムに関連する設備のセキュリティインシデント、リスク源、セキュリティポリシー（対策要件）を空調システムに関するビルシステムのリスクと対策ポリシーとして、表にまとめた

（5） 議論・意見交換

・こうやって見ると、工場システムが複雑、ビルシステムが簡単だとは一概に言えない
・Orin（デンソー他が中心となっている工場制御システムの標準化委員会）現在 2.0 版、来年 3.0 版でセキュリティ強化する予定
・かつてスマートメータ（東京電力ほか）にてセキュリティ脆弱性があった。Authentication 機能が不備だったのでなりすまし犯罪が危惧
・工場システムのOSは、ラズパイ、Windows、LINUX（Debian）など汎用性、OSS が主流となっている。特別な OS でなくなっているため一般的なセキュリティ対策が必要
　ゼロデイ攻撃など．．．常に最新バージョンに Update する必要あり。現実は体制も手順も注意も欠如
　OS の Update に伴うアプリの稼働テストなどさまざまな問題をどう解決していくかが検討要
・ビル管理システムにロボット（警備、清掃、配達．．．）が組み込まれるためサイバー攻撃で乗っ取られないようにするための検討が求められる
・以上のリスクアセスメントを設計段階で実施することを含める、かつ PDCA で常に評価し対策していかなければならない。大変なコストになりそう
・現在事例を収集している段階、まだ正解が出ているわけではない

（6） 次回のテーマについての意見交換

・EUサイバーレジリエンス法（草案）2022 年 9 月 15 日
・・https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/eu-cyber-resilience-act.html
・・https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
・・EU のサイバーセキュリティ規制は進んでいる。日本は遅れを取ってきたので注意しなければならない。
・・具体的な規定はまだ不明
・・罰金として 1,500 万ユーロまたはグローバル年間売上高の 2.5%のいずれか高い方が科される可能性があります。
・・ENISA の権限強化、ガイドラインの発行。ただし全部やるのはきつい。
・・案がでてもそのまま施行されるわけではない
・米国輸出製品は SBOM（Software BOM）提示が必須になってきた
・・個人情報移転に関する大統領令で EU 側が同意し EU から米国へ移転の十分性が有効となった
・EUのセキュリティに関する法規制は AI も含めいっぱい出ているので継続調査する

4. その他

- 次回、11 月 24 日（木）18：00 Zoom 開催

以上