情報システム・バックアップオフィス研究会（ITBO 研） 2022 年度 第 13 回 議事録

1．開催概要

- 開催日 :2022 年 5 月 20 日（火）18:00～20:00
- 開催方法 :ZOOM 開催
- 進行役 :加藤座長
- 議事録作成: 野原
- 出席者数： 5 人 （敬称略 順不動） 加藤、水落、大塚、相原、野原

2．議事内容

（1） 本部運営会議の概要説明

（2） BCP 維持運用研究会（2022/5/4 開催）（加藤座長）

・昨日（5/19）の維持管理研究会の状況報告　OT セキュリティとは

・OT や工場ネットワークセキュリティ、サイバーフィジカル等 いろいろな言い方がある。

・PC セキュリティとOT等、情報セキュリティを一言で言っても管轄が違う。一般の PC セキュリティは、情報システム部門で OT は工場の開発部門等、セキュリティ担当者が異なる。

・OT に関しては BCAO の中でも専門家がいないため、正しい整理を BCAO として行うことが可能なのかわからない。

・イラン核施設を攻撃したマルウェア「Stuxnet」については国レベルの攻撃で、国の軍隊が一般企業に対して、そこまで行うリスクの可能性はかなり低い。そのレベルの話を、一般の中小企業に対して求めるのはどうかと思う。

・OT に対して、ゼロトラストは要求できない。そもそも昔のシステムはパッチも出ていないし、機器をネットワークに接続できるものも少ない。

・35 年前、PCは OS のバージョンアップしたらですねプログラムが絶対に動かくなくなるに決まっている。何も触らず、壊れるまで使用できればよい。

・OT が問題になり始めたのは、最近で、デバイスとして今までメーカ独自のOSや通信プロトコルが、Windows Embedded などのオープン化された汎用コンピュータが入り始めたことと、TCP／IPが通信プロトコルになったことで Internet へすぐ出ていけることが問題。

・汎用コンピュータになるとアップデートできるのでは。うまくやると、アップデートできるのでは。

・昔のコンピュータは化石の様なシステムで動作しているが、今は汎用的な PC なので、侵入されることが問題。

・30 年前の PC を入れ替えようとすると、汎用的な PC を導入せざるをえない。きれいなところにそのような汎用 PC が入り Internet に接続されると、汚染される。

・今後 BCAO で OT を行う場合は協力を求められることがある。普通の OA 系の話題でも参加者がついていけないのに OT の話題だとついていけないのでは。BCAO としては、整理することはよいが、他の団体が取り組んでいることを理解して、やっているのであればよいが、理解していない。理解してどこまで行うのかというのを検討してほしい。

・今までのサイバーセキュリティリスクから重要インフラを守るという取り組みが終わったので、一般の工場まで広げようとしているのは何か意図があるのではと思ってしまう。

・経産省や IPA が行うのはわかるが、なぜ BCAO が OT の話をしなければならないかわからない。

・ウクライナ侵攻の前、ウクライナの重要インフラに対するサイバー攻撃が増加した話がある。

・今や家電もコンピュータで動いている。ゴルゴ13の話。温度センサーをハッキングし、エアコンが火を噴いて、通報ができないよう電話回線を停止して、重要人物を殺害する話がある。リアルな話。

・アメリカのドラマ CSI サイバー等のドラマにもサイバー犯罪の手口が紹介されている。

・センサーに対してい低い温度のデータを送ってヒーターを過熱させるというのは容易にできそう。

・自動車の自動運転について国連で決まった WP29 の規制などはまさに人命を守るための規制。

・セキュリティの話は IoT 全体にかかわる話で、製品の中にプログラムが入るものは、開発の初期段階から、セキュアバイデザインで開発するよう働きかけた。容易に想定できるリスク。
・それぞれの製造設備の口に簡易な FW、(通信可能な IP を限定できる機能があればよい)を一つ一つつけるとか、個々の PC、設備だけでなく、ネットワークの設計を組み合わせたセキュリティの構築が必要。
・IoT と OT の区分けはどう考えればよいか。
・IoT はネットワークにつながるすべてのもの(機器)。OT は IoT に含まれる。
・IoT はオフィスと工場とそれ以外も含まれるということ？
確かに場所という意味ではオフィス、工場、営業所、倉庫といった区分けはあるが、場所という区分けではなく、その場所にある、ネットワーク接続する機械(WIndowsPC,Lniux,Andriod)という見方で、考えたほうが、セキュリティを考える人にとっては整理できるのではと思う。
・一般の人には OS の話をしてもイメージがつかないため、オフィスとか工場といったロケーションで話してしまうが、その場所には、様々な機械があるのでわかりにくい。
・人間が生活する空間に何らかの制御装置があって、外部の何らかの悪意を持ったものがアクセスできてしますと、人命にかかわる。
・車の自動運転はまさにそう。そこで規制がかかってきている。規制は本当に車だけでいいのか。電気の取り扱いをするときに電気主任技術者のような資格があるように、IT の世界もそのような方向に行く、そのような資格が必要ではないかと思う。
・情報処理安全確保支援士が、そのような資格か。
・そこまでの資格ではないが。
・今、家庭で一番危ないのは、ペット監視用のカメラが危ない。
・コピー機でもそのようなことを考慮しているのか。
・コピー機も外部からのセキュリティ対策をしっかりするようにより考慮されている。設計、営業含めて考えているが、皆様のご意見を反映させていくようにしたい。今後ネットワークのセキュリティを考えた、製品設計をしなければならない
・コピー機もゼロトラストも求められるのか？
・最近はお客さんに提供する製品の中にプログラムが入っているものはそれなりにセキュリティを求められてきている。PSIRT の設置を行っている企業も増えてきている。
・コピー機の印刷自体は少なくなってきており、すべてデータになっているため、セキュリティの確保は必須だが、どこにデータを送るかはお客自身が設定することになっている。製品の使い方はお客さん次第。
・PSIRT の組織として担当役員は決まっているのか。
・役員は、決まっていない。そういう組織つくりを企画したが、CSIRT は取りまとめるといったものの、結局、製品についてはわからないということで現在は品証へ主管が移りつつある。体制の再構築を行っているところ。
・製品のプログラムについては、製品品質の一つとして捉えるということは重要。
・ソフトウェア会社ではなくメーカなので品証の組織内にプログラムについて詳しい人は少ないので支援を行っているが、本来自分の仕事ではない。
・セキュアバイデザインについての安全を保障する法律等はないのか。
・車の自動運転の規制として国連の WP29に沿った国土交通省の法令はある。一般の製品についてはない。
WP29　https://unece.org/reference-documents-0
国土交通省　(道路運送車両の保安基準等及び保安基準)
https://www.mlit.go.jp/report/press/jidosha10_hh_000242.html
・一般の製品については、個人情報保護に関しては定められている。EU では、監視カメラを公道に向けてはならないといった規則がある。
・ISO9001 は、品質マネジメントシステムなのでセキュリティ基準は定められていない。

・セキュリティ製品についてはISO15408の規格があるが、どの機能を認証するのか製品全体ではなく、機能を限定してセキュリティの認証をえるものとなる。
・ウクライナの戦争でドローンが活用しているが、プロトコルはTCP/IPではないかと思われる。ほとんどの製品について今後、セキュリティの対応が必要になるのではないか。民生品であるDJIのドローンも多く使用されているが、使用開始時に比べ、最近、爆弾投下の際の命中率の低下が、話題になっている。一部の噂では、中国が意図的に GPS 等の処理にデータ制御（ハッキング）を行っているのではないかとの話がある。
・軍需用の UAV は通信が暗号化されているため、セキュリティは強固だが、民生品はセキュリティの問題が発生する。
・ISO15408は、IPA に記載がある。
https://www.ipa.go.jp/security/fy14/evaluation/event/20021206/docs/2IPA.pdf
・他の国にも相互認証となっているので、日本で取得すれば、相互認証している国で取り直しは不要。
・ISO15408 の枠組みをセキュリティ製品だけでなく IoT 製品に規格を広げるとよいのでは。
・今は、NIST の SP800-53/171 が、使用されている。（この番号でしたが、製品セキュリティというよりは、業務環境における情報セキュリティ管理策全般の話でした。SRI）
NIST SP 800-53 組織と情報システムのためのセキュリティおよびプライバシー管理策
NIST SP 800-171 非連邦政府組織およびシステムにおける管理対象非機密情報 CUI の保護

（3）JPCERT／CCの情報共有のあり方について（加藤座長）

https://blogs.jpcert.or.jp/ja/2022/04/sharing_and_disclosure.html?fbclid=IwAR1mft0BlqdsSL3c0TuajxaueBRgzGnq4sADUAgkBZbJXWCgjvcKtc_z6NI
・情報漏洩時の対応　被害組織のお詫び？
・半田病院の事例について詳細に解説されており珍しい。
・コンテクスト情報は企業の心証をよくするために重要では。コンテクスト情報のひな形は、今までなかったわけではない。
・今後、発表される内容を見て活用したい。

（4）Freee が実施した、障害対応訓練について、事例紹介

・PSIRT が実施した、障害回復訓練
https://www.itmedia.co.jp/news/articles/2203/17/news038.html

（5）相談事項（加藤座長）

・幹事の推薦について
相談した結果、新年度は新幹事として水落さんを本部に推薦する。
・次回、6 月 24 日（金）18:00

以上