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9回 議事録

１． 開催概要

- 開催日 ：2023年1月20日（金）18:00～20:00
- 開催場所 ：ZOOM 開催
- 進行役 ：加藤（本年度座長）
- 議事録作成： 加藤
- 出席者数 ： 5名（出席者名は末尾参照）

２．議事内容

（１）運営会議の報告

- 今月開催の運営会議の内容を研究会メンバーに報告した。
- 専門家レベルアップ教育、月例オープン勉強会、中小企業技術研修会、運営部門・タスクフォースの進捗
- 各会合で、訓練・演習が取り上げられてる。BCAOの主要活動の一つになったと思われる。
- ITサイバータスクフォースについて（別項で説明）
- 2月月例勉強会について（テレワーク系の内容をITタスクフォースにて実施予定）
- その他

（２）ITサイバータスクフォースについて

- 日本システム監査人協会（SAAJ （注：エスエーエージェイと読む））とのコラボの状況説明
- 1月13日に2回目会合を実施。
- SAAJでは「テレワークを題材とした机上訓練」を2月に計画中とのことであった
- ITタスクフォースから想定内容の資料を提出
- SAAJからも実施概要が提出
- SAAJは2月25日（土）午後に実施予定。これにITタスクフォースから可能なら参加する。
- BCAOは月例勉強会の形で別途実施する。ITタスクフォースにて担当。SAAJからも参加を要請。
- 今後、SAAJとの打ち合わせを実施し、月例会の実施内容を作成する。

（３）最近のトピックスについて討議

JNSA 2022セキュリティ十大ニュース、半田病院のランサムウェア感染事件に関連する、普及事業者等の対応に関する記事を検討

① JNSA 2022セキュリティ十大ニュース ～セキュリティニュースの二極化は何を示唆するのか～
https://www.jnsa.org/active/news10/index.html?fbclid=IwAR1hOwHrM_aoTkaDP1-sUTPrp4yJMrmiLaBrOfPpizu5ZqJAm7Duy4OclIE

- 物理的な戦闘行為とサイバー攻撃は、今のところ別扱いのようであるが、今後は注視が必要
- 2022年は重大なネット障害等が多発した。
- USBメモリー紛失事件は、IT関連業務の実施・契約形態等での課題がある。
- 病院関係のランサムウェア被害が続出、等

② 47NEWS 「解除不可能」ロシア・ハッカー犯罪集団のコンピューターウイルスはなぜ解除できたのか？ サ

イバー攻撃を受けた徳島・半田病院、復旧の裏で起きていたこと【前編】
https://nordot.app/977511889856217088?c=39546741839462401&fbclid=IwAR0KC6Cz-WdtsD0l7QHBX6ugJzx01eCZoPsIr_uD_1ivq17bu5GbEIVI98Q

③ 「身代金はもらった」ロシア・ハッカー犯罪集団が明かした交渉の一部始終　サイバー攻撃を受けた徳島・半田病院、復旧の裏で起きていたこと【後編】
https://nordot.app/978208573179396096?c=39546741839462401

④ 日経　サイバー脅迫に「交渉人」 身代金減額、委任リスクも
https://www.nikkei.com/article/DGXZQOUC249070U2A021C2000000/?fbclid=IwAR2BPhv28kSBA1rbbbmvCs7KjczxnFB5XPK5Mf0uWNxnh49GEZizq74oQSA

⑤ ZDNet　ランサムウェア被害のデータ復旧でトラブル、業界団体が共同で確認リストを公開
https://japan.zdnet.com/article/35197633/?fbclid=IwAR1B_RLw4itKHNH878EChZtCiAExUoz7PfbWrkAWcAzpvUQDUO2Vo3Nvrts

- 半田病院はサイバー攻撃の詳細や復旧に至る道筋について、セキュリティー専門家による有識者会議に調査を依頼した。２０２２年６月に報告書がまとめられ、本研究会でも検討した。
- 報告書では、どうやって電子カルテなどのシステムを復旧させたのかを特定できなかった。有識者会議は「復旧事業者から詳細な情報が得られなかった」とし、特定を断念。報告書には「データ復元に必要な手段を入手したと考えるのが妥当」と記述するにとどめた。
- 本記事の内容が完全に正しいかの見極めがいるが、本記事によれば、犯人と復旧事業者間での裏取引などの存在が示唆されている。
- 公費が犯人に支払われていたとすれば、大きな問題となる可能性がある。
- 復旧事業者の他、この種の事件では、他のハッカー、交渉人等の関与者が存在する。
- このような流れの中、デジタルフォレンジック団体等が、復旧事業者とのトラブル防止のチェックリストを発表している。
- ランサムウェア被害が続出する中、複雑な関係者からなる世界が広がっており、注意が必要である。

３．次回
2月14日（火）18時－20時、ZOOM 開催

４．出席者（敬称略 50音順）
大塚、加藤、近藤、野原、水落

以上