

情報システム・バックアップオフィス研究会 (ITBO 研) 2021 年度 第 12 回 議事録

1. 開催概要

- 開催日 : 2022 年 4 月 19 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 : 大塚
- 出席者数 : 7 人 (敬称略 順不動) 加藤、水落、岡、近藤、野原、芦田、大塚

2. 議事内容

(1) みずほ業務改善計画の進捗状況(2022年4月15日発表)のブリーフィング(加藤座長)

https://www.mizuho-fg.co.jp/release/pdf/20220415release_jp_1.pdf

「システム障害の未然防止」「障害対応力向上」に向けた取組みの具体的内容説明

- 例えば ATM コーナーにスピーカー付カメラ設備を設置(22/4 より順次)
- 業務改善計画(2022/1/17 金融庁提出)の進捗を金融庁に報告したもの

(2) BCAO 運営会議報告(2022/4/4 開催)(加藤座長)

- 年会費納入依頼
- 月例オープン勉強会(ITサイバー、コロナ禍への対応、環境変化に対応するBCのテーマで行った)
- 各タスクフォース進捗報告
- 2021年度 BCAO アワード審査開始(応募 14 団体)
- 新年度事業計画案
- 中小企業事業継続研修会(全12講座)順次開催中の報告
- BCAO 事業継続上級管理士資格及び主任・准主任講座等講師指名制度の新設について
- 今年度(2022年)、水落さん(次期副座長)を幹事に推薦したいとの意見があった

(3) IT タスクフォースからフィードバック(大塚)

- (一社)日本サイバーセキュリティ・イノベーション委員会(JCIC) 梶浦代表理事へのコンタクトを行う
- OT(オペレーショナルテクノロジー)サイバーセキュリティの取り組みの調査研究の実施
- BCAO 維持研(2022/5/19 開催)にてOTテーマで研究会を実施(希望者にリンク情報を通知する)
- BCAO 中小企業向け事業継続研修カリキュラム(全12講座)テキスト案について
 - ① 第 10.事前対策(2) 情報バックアップ IT・情報セキュリティ(サイバーテロ) パートの解説
 - ② 内容は 2022/3/15 オープン勉強会発表資料に準拠したもの
 - ③ 目次;情報システム依存度と分類、経営者の認識、情報バックアップ、IT・情報セキュリティ、IT-BCP 様式、維持管理、社員教育と演習の重要性、IT に強いアドバイザーとの連携、補助金の活用、ビジネスチャンスにつなげる
 - ④ 以下、コメント
 - a. 次の新資料が出ているので参考のこと、サイバーセキュリティ経営ガイドライン Ver 2.0 実践のためのプラクティス集(<https://www.ipa.go.jp/security/fy30/reports/ciso/index.html>)
 - b. 情報処理安全確保支援士(RISS)略称登録情報セキュリティスペシャリストとは国家資格、3 年ごとに更新する。結構費用が高い。専門家として中小企業のサイバーセキュリティ構築を行う
 - c. ランサムウェア対策として「オフライン・バックアップ」対策を追加し強調すること
 - d. バックアップ対象領域(5 層)については想定するリスク特性によって自社、外部サービスに分けヌケモレなく対策を検討すること
 - e. 業務重要度を分ける、5 段階の説明が一般の中小企業の事例ではないのでわかりにくい(資料は地方自治体の例示)緊急時システムは最優先で稼働させることは自明である。本業の業務システムの分類例が欲しかった

- f. 情報バックアップ、パートは情報量が多く、もつと時間をかけて説明すべき(2~3時間くらい)
- g. OT(生産系システム)のサイバーセキュリティの重要性を追加すべき。背景として無人化した製造ラインが普及した。製造ラインにリアルタイム指示が必要となるためサイバーリスクによる停止は影響が大。工場の配線を有線から Wifi に替えただけでサイバーリスクが顕在化した事例がある
- h. 経済産業省 第7回「産業サイバーセキュリティ研究会」を開催し、「産業界へのメッセージ」を发出。サプライチェーン重視。
https://www.meti.go.jp/press/2022/04/20220411003/20220411003.html?fbclid=IwAR22X2HfllOk_DBWuffgmHc0vVt1-EaGjSL-oFVgD78zhekokSBbYepA5h4
「産業界へのメッセージ」
- https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/20220411.pdf
- i. オフライン・バックアップの方法とは？ 情報用耐火金庫に入れ管理している事例がある。手間はかかるので、RPO は(オンラインより)長くなる。世代管理は必須

(4)2021年10月31日発生サイバー攻撃による電子カルテ停止を経験して、(加藤座長)

徳島県つるぎ町立半田病院徳島県医師会サイバーセキュリティ研修会資料より

<https://www.tokushima.med.or.jp/> 2022年3月30日

- ・これほど詳しい資料が出ることは珍しい。特にシステム構成も載せている
- ・9時間後災害対策本部立ち上げ、15時間後記者会見実施。結構迅速な対応ができていたと評価する。拠点病院なのでBCP作っていたのでは？
- ・南海トラフ地震への対策で運用する予定であった紙カルテベースの診療でしのぐ。しかし限界
- ・半導体が不足していたため、全く新しくシステムを取りそろえることは半年以上の期間を要する
- ・医事会計システムは稼働していないので診察料は頂いていない
- ・BCPの作成、災害時を想定した模擬訓練、復旧時を想定した組織工程表も考えるべき
- ・サイバー攻撃に備え、セキュリティは万全に！ウイルス対策ソフトを使用し、こまめにアップデート(VPN・PC等)。セキュリティに関しての情報も常に収集(厚生労働省からの通達等)
- ・システム構成図からわかること;VPNが直にインターネットにつながっている。これは外向けのHPサーバがないので電子カルテサーバのリモートメンテ用と考えられる。そうすると常時接続は軽率である。ベンダーの責任もあるか？あるいはしろうとによる設計、ベンダー指示があったか。
- ・VPNの最新のセキュリティパッチがあたっていないとかなりの確率で侵入できてしまう。2段階認証を入れるべき。
- ・電子カルテサーバとクライアントPC、医療機器が同じセグメントに入っているのは問題。ゾーニング設計が考慮されていない。新ネットワークに新ハブ(ゾーニングができるもの)が新設され、部署PC職員用PCが外れたことである程度ゾーニングが考慮されたと判断できる
- ・重要データである電子カルテサーバを守るネットワーク設計ができていなかったとわかる
- ・被害総額、復旧・新システム構築で2億円、被害発生直後の2か月で1億円。計3億円出費

(5)相談事項(加藤座長)

- ・新座長・幹事の若返りについて
相談した結果、新年度は加藤さんが座長、新副座長として水落さん、野原さんをお願いする。
- ・次回、5月20日(金)18:00
- ・BCAO総会、5月30日(月)16:00

以上