

## 1. 開催概要

- ・ 開催日 : 2022年12月19日 (月) 18:00~20:20
- ・ 開催場所 : ZOOM 開催
- ・ 進行役 : 加藤 (本年度座長)
- ・ 議事録作成 : 野原
- ・ 出席者数 : 6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。

- ・11/30 デスクトップエクササイズの内容確認
- ・BCAOアワードの募集開始について
- ・和歌山地域勉強会と関西地域勉強会コラボについて
- ・IT-TFについて

現在、システム監査人協会（SAAJ）との協業を検討。来年2月IT-BCP訓練等の共同開催ができないかBCAO本部から直接SAAJへコンタクト中。

⇒IT-TFから本部へ協業として訓練で何がしたいのか問い合わせるネタの資料を作成中で、今月中に問い合わせる予定。

IT-TF内部でも意見交換が活発でない。皆さんから忌憚のないご意見を募集

- ・上級管理者資格について
- ・その他勉強会の状況について

### (2) 最近のトピックスについて討議

- ① LogmiBiz もう「バックアップさえあれば大丈夫」ではない 弁護士が解説する、サイバーインシデント対応の4つの「疑問」

[https://logmi.jp/business/articles/327612?fbclid=IwAR3vgqkkNoSztvSOMjGqJc\\_vIvL5\\_2i4-9fp5aNfn-uzxHGoQPYPYMoqXs68E](https://logmi.jp/business/articles/327612?fbclid=IwAR3vgqkkNoSztvSOMjGqJc_vIvL5_2i4-9fp5aNfn-uzxHGoQPYPYMoqXs68E)

- ・オフラインバックアップの重要性
- ・日本では当人が支払う場合は違法性はないが、海外では身代金を払うこと自体が違法  
コンサルタントが、払うように指示すると犯罪ほう助になる。
- ・データ復旧のために業者が身代金を払うと組織犯罪処罰法により日本国内でも処罰対象になる。
- ・身代金を払っても、2回目の攻撃もありうる。(ダークウェブにお得意様リストとして掲示)
- ・欧州でUBERは身代金を払ってデータ復旧したが、個人情報の漏洩のおそれを当局に報告しなかったため、2カ国から制裁金を科せられた。

- ・株主への説明も必要

対応が不十分であるがために身代金を払ったということは善管注意義務違反で株主代表訴訟の対象になる場合もある。

- ・ランサムウェア被害において個人データが含まれていないデータはない。2020年の改正個人情報保護法により、本人への通知が必要など以前より法的対応が厳しくなっている。

- ・漏洩のおそれがあるかどうかを判断しなければならないため、PCの初期化は、被害を拡大する可能性がある。個人情報漏洩のおそれがあるか判別するための、エビデンスが残らない。＝外部へのアナウンスが必要。

- ・迅速の復旧と原因の究明は別物。こと（インシデント）が進行中のリカバリは地震等、他のリスクとは 違うところ。

- ・証拠保全ができておらず、初期化することは法令違反につながる可能性がある。

- ・ITBOの意見としては予備のPCを送って、元のPCは、電源を切って交換したほうが1番確実ではないか。

- ・感染した先の問い合わせ先を中小企業等へアナウンスするようなガイドのあつてよいのでは。

- ・ガイドラインだけではなくIT-BCPとして、手順を明確に定義すべきである。

- ・こういったノウハウをBCAOから発信していけばよいのでは。

② 読売 サイバー攻撃を受けた大阪の病院、災害用BCPは作成していたが…「訓練とは全く違った」

<https://www.yomiuri.co.jp/national/20221211-OYT1T50104/?fbclid=IwAR2yTdxBD1CHoUCI3aSt3IcS6gTHUsq-bxM6uM3ij-KLKbxbU5bd5-AbvIw>

電子カルテシステムなどのようにデータを紙に出力する事で業務継続が可能な業務の場合はデータの書き換えができないよう書き込みを一度しかできない、DVD-RやBR-R等を使用してデータダンプを保存してはどうか。

### 3. 次回

1月20日（金）18時－20時、ZOOM 開催

### 4. 出席者（敬称略 50音順）

大久保、大塚、加藤、近藤、野原、水落

以上