情報システム・バックアップオフィス
研究会の活動

ーDX化進展の元、情報関係重大インシデント大発生時代の事業継続ー

2022年7月26日(火)

特定非営利活動法人 事業継続推進機構(BCAO)
情報システム・バックアップオフィス研究会

※　本資料の文責は研究会にあり、BCAO全体の見解ではありません。

Copyright © 2022 BCAO

概要－DX化進展の元、情報関係重大インシデント大発生時代の事業継続－

本日は、「－DX化進展の元、情報関係重大インシデント大発生時代の事業継続－」と題し、ITBO研究会の最近の活動内容につき報告します。昨年は「－ウィズ/アフターコロナ、DX推進等における事業継続の検討－」という副題で報告しましたが、

振り返ると、**嵐のような一年**　でした！

研究会での検討テーマも多岐にわたり、

- 基本事項（災害対策本部ポータル、工場セキュリティ、クラウド化、等）
- 各種資料の検討（DX白書、サイバーセキュリティ経営ガイドライン、等）

のベーシックな検討も行いましたが、重大インシデントが多発でした。

- システム障害事例（みずほ銀行、KDDI等）
- ランサムウェア被害事例（半田病院等）
- 情報セキュリティ事故（尼崎市USBメモリ等）
- 国際紛争でのIT攻撃

また、関西地域勉強会との合同開催、維持管理研究会の聴講、従来検討してきた机上訓練成果の岡山地域勉強会での実施等を行いました。

Copyright © 2022 BCAO

1. ITBO研究会の活動のビジョン

現実を見据え

リスクの分析

未来を見通す

情報プラットフォームは社会の基幹インフラ

新動向

- クラウド化
- 暗号資産（仮）
- データ活用
- AI・IoTの進展

問題点

- バックアップ？
- 取引所・運営
- プライバシー
- プロファイリング

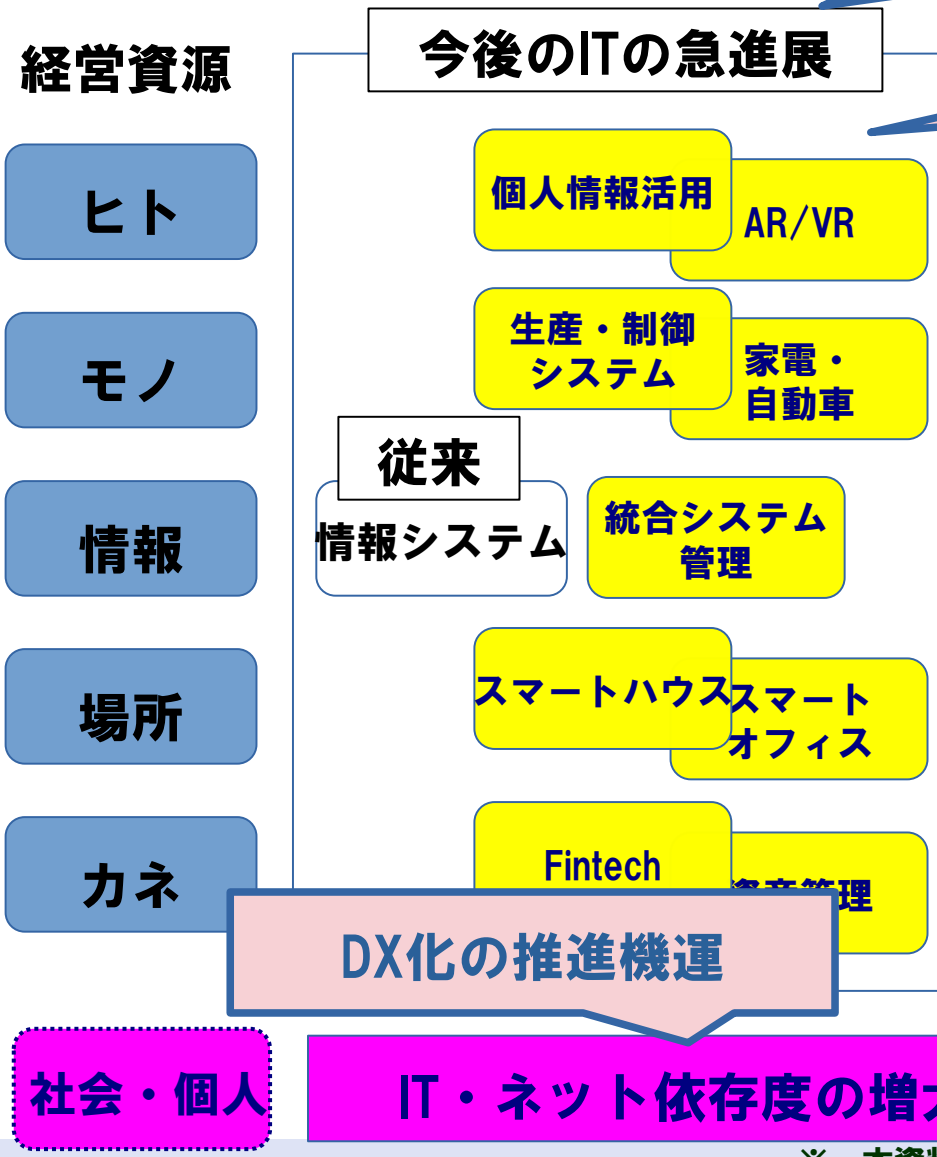
ベースとして
情報セキュリティ

どのように活動すべきか？

※　本資料の文責は研究会にあり、BCAO全体の見解ではありません。
Copyright © 2022 BCAO

2. 現状認識（全般）

COVID-19の発生により、テレワーク等のITの重要性が急上昇・**それを狙った攻撃**



事業継続における情報システムの役割は経営資源全般に拡大

社会インフラの維持
企業・組織活動基盤の確保
個人生活の安全性の確保

分析評価と対策

- ●狭義の情報システム障害から広範囲な社会インフラ全般への影響拡大
- ●情報漏洩等データの被害のみでなく物理的な事故が発生する可能性
- ●AI化などによるフェイク情報の巧妙化

※　本資料の文責は研究会にあり、BCAO全体の見解ではありません。

Copyright © 2022 BCAO

3. 重大インシデント大発生時代の現状認識

対象		インシデント
基本インフラ（ネットワーク）	接続障害	動作不良
プラットフォーム（クラウド）	データセンタ障害	情報セキュリティ事故
情報システム・個人情報	設定不備（AWS等）	マルウェア被害（ランサムウェア）
工場・制御システム	尼崎USBメモリ紛失	サプライチェーン障害（機器・部品）
IoT・自動車	銀行システム	国際紛争での攻撃
重要インフラ（電力網）	半田病院ランサムウェア被害	
	制御システム攻撃	
	ウクライナ	
	太陽フレア	

※　本資料の文責は研究会にあり、BCAO全体の見解ではありません。

Copyright © 2022 BCAO

みずほ銀行情報システム障害

2022年1月25日、4月19日実施

●金融庁に業務改善計画を報告（1/17）

https://www.mizuhobank.co.jp/release/pdf/20220117release_jp.pdf

業務改善計画の提出（1/17）、進捗状況の報告（4/15）等、継続して公開資料検討中。

●システムに関する改善対応策は点検と対応。
→アプリ点検、エラーの波及範囲の対策の確認、安定稼働のためのメンテ作業内容の点検
→システムエラーを人為的に発生させ確認する（今年9月）。
●システム障害発生時対応力強化
→監視システム強化
●SCP（システム・コンティンジェンシー・プラン）の見直し→システム間連携の確認、訓練（実践型訓練、実機を使用した訓練）
●人員の増強
→システム所管部の原因分析力強化
→MINORIシステムに関する専門知識の可視化

検討内容

●予兆管理のポイントはその現象を正確にとらえること、予防実施計画を確実に立てる
●モニタリング要員がいない可能性があるのか、あるいは分析ツールの結果の解析ができない。生データを出すだけでは報告にならないと思われる。
●ＢＩＡ視点の欠如。お客様へのインパクトから逆算する考えが抜けている。現場だけでは難しいので業務部門との連携が必須
●営業統括部門とIT部門の情報共有・伝達の困難、特に、ＩＴ現場レベルではコンポーネントエラーがお客様の何に影響を及ぼすか想像がつかない。
●経営層の思い切った判断が入っていないように見える。改革にはこれが必要。

Copyright © 2022 BCAO

半田病院ランサムウェア被害

2022年4月19日、6月24日実施

●サイバー攻撃による電子カルテ停止を経験して（2022年3月30日徳島県医師会サイバーセキュリティー研修会）

●有識者会議調査報告書（6/16）（https://www.handa-hospital.jp/topics/2022/0616/index.html?fbclid=IwAR2LStik9f0Aw8sobDQdNiXrWExnel5VmKTJCqb8x3yTnJpgSSIMYEdkXKU）

事件の経過

- 2021年10月31日午前0時30分頃　病院内の電子カルテと接続され、電源が入っている全てのプリンターから英文の犯行声明が印刷。印刷は、自動で開始され、プリンターの用紙がなくなるまで継続。
- 当直医師に電子カルテの不具合が報告され、システム担当者が午前3時ごろに駆けつけて対応を開始。ほどなく、ランサムウェアによるサイバー攻撃ですべてのシステムが使えなくなっていることが判明。
- 午前8時過ぎ病院上層部へ連絡。（県内の電子カルテ共有ネットワーク・等）および県警のサイバー犯罪対応部署へ連絡。
- 午前10時災害対策本部を立ち上げ、第1回目の対策会議を開始。
- 午後4時、県内の報道機関に事件について記者会見。

●医療法人久仁会　鳴門山上病院ランサムウェア被害（6/19）との比較
・こちらも半田病院と同様に攻撃を受けたが、オフラインバックアップを適切に作成しており、短時間にシステム復旧し二日後に回復することができた。
・バックアップの原則の重要性

・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。
・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。
・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。
・病院側も情報システム関係に十分な要員を割り当てていないとの報告書中の記載がある。
・ベンダーを含めた対応につき問題点指摘の声があり、検討が必要。

Copyright © 2022 BCAO

ご参考：IPA情報セキュリティ白書2022（7月15日）

●IPAより「情報セキュリティ白書2022」が公開されております。登録、アンケート回答が必要ですが、無料でダウンロードできます。（
https://www.ipa.go.jp/security/publications/hakusyo/2022.html）

・各種情報セキュリティインシデントの詳細な説明があります。半田病院の事例も掲載。
・対策説明の例として以下（p.27）。
ーーーーーーーーーーーーーーー

（g）バックアップからの復旧
「侵入型ランサムウェア攻撃」への対策として重要なことは、データの保護のみならず、「システムの再構築を含めた復旧計画」を事前に策定し、バックアップからの復旧を可能にしておくことである。「1.2.2（2）ランサムウェア攻撃の被害事例」にもあるように、企業・組織のパソコンやサーバ等がバックアップも含めて一斉に暗号化される可能性がある。こうした状況に備え、事業継続に重要なデータやシステムのバックアップデータをオフラインで管理するほか、必要に応じて業務継続やシステムの再構築に必要なリソース等を考慮した復旧計画を策定しておくことが大切である。

Copyright © 2022 BCAO

尼崎USBメモリ紛失事件

2022年6月24日実施

概要

•2022年6月23日、尼崎市は業務委託先企業の関係社員が個人情報を含むUSBメモリを紛失したことを公表（紛失したUSBメモリには同市全市民の住民基本台帳の情報等）。
•BIPROGYがコールセンターにてデータ更新作業実施（BIPROGY社員2人と協力会社社員1人、別の協力会社の委託先社員1人）
•コールセンターでのデータ更新作業完了後、4人で吹田市内の居酒屋にて、3時間にわたり宴会
•解散後、USBメモリを持っていた協力会社の委託先社員が路上で寝込んでしまい、その後目を覚ました後に鞄ごと紛失していることを発見
•BIPROGYでは作業後の速やかな帰社が決まりだったが守られていなかった。また、居酒屋への立ち寄りもBIPROGY社員が提案

議論

（本会合時点では、紛失したUSBメモリーが発見されたという段階）
•昔は、このような媒体を持ち出し紛失する事例が多数あったが、最近には珍しい古典的なものである。
•基本の再確認
＝＝＞持ち出しの必要性、業務に必要最小限か、契約・顧客承認の手続き、等
•発見されたUSBメモリーからデータがコピーされているかどうかは、暗号化等の方法などの情報がないと、簡単にはわからない。発見されたからと言って、即問題解決ではない。

Copyright © 2022 BCAO

工場セキュリティガイドライン検討

2022年6月24日実施

●JNSA西日本支部/今すぐ実践できる工場セキュリティ対策のポイント検討ワーキンググループの成果物　（https://www.jnsa.org/result/west/2022/index.html）

No	脅威の入口	脅威が引き起こす可能性のある事象	懸念されるリスク
1	USBメモリー	USBメモリーから制御システムや製造装置にマルウェアの感染が広がる	工場停止
2	持込パソコン	持込パソコンから制御システムや製造装置にマルウェアの感染が広がる	工場停止
3	スマホ・タブレット	スマホ・タブレットに感染したマルウェアが利用者の意図しない動作をさせる	情報漏洩
4	IoT機器・センサー	IoT機器・センサーが第三者に遠隔操作される	工場停止
5	複合機	複合機が第三者に遠隔操作される	情報漏洩
6	ハンディターミナル	ハンディターミナルに感染したマルウェアがプログラムやデータを改竄する	情報改竄
7	OAネットワーク	OAネットワークからマルウェアの感染が広がる	工場停止
8	インターネット	インターネットからマルウェアの感染が広がる	工場停止
9	Wi-Fi（無線AP）	Wi-Fi通信が傍受されたり、通信が妨害される	情報漏洩
10	保守用ネットワーク	保守用ネットワークからマルウェアの感染が広がる	工場停止
11	クラウドサービス	認証情報が不正に利用される	情報漏洩
12	部品・原材料	組み込んだ部品のセキュリティ不具合が悪用される	品質低下
13	新規購入機器	新規購入した機器から制御システムや製造装置にマルウェアの感染が広がる	工場停止

検討

- 内容範囲は一般的な内容をカバーしているが、２，３箇所、説明が不鮮明な点がある。
- 執筆者が全員IT関係者であり、中小企業の非IT要員が読むものとしては、説明に追加が必要な部分があるのではないか。
- IPAの制御セキュリティのガイドラインもあるが、求めている対応策が高度過ぎるという観点もあり、予定されているJNSAの後続の成果物に期待する。

Copyright © 2022 BCAO

DX白書検討

2021年12月17日実施

●IPA DX白書2021の内容を中心にした講演を実施　（https://www.ipa.go.jp/ikc/publish/dx_hakusho.html）

• DXはいろいろと定義がある（ストルターマン教授等）。一つの見方では下記の違いが重要
✓ ディジタイゼーション （RPA）
✓ デジタライゼーション（ビジネスモデルの変革）
✓ デジタルトランスフォーメーション（社会の変革）
•経営戦略、事業戦略、IT 戦略と一体化したDXが必要
→経営者（コミット）、IT 、事業部門がビジネス変革に向けたコンセプトを共有
•文系思考でコト（ニーズ）を捉え、技術の開発、組合せによる最適化を行う
•課題解決を行う人材の育成が重要

<u>議論</u>

•何になりたいんだ、という利点があり、その段階でデジタルが出てくる。
•社会変革を1企業が起こせるか？
•リスクはチャンスと言う意識が米国では強い
•アジャイルの原則に則ったDX推進

Copyright © 2022 BCAO

他研究会・勉強会への参加・合同開催

●年度中、関西地域勉強会との合同研究会、維持・管理研の講演を聴講、岡山地域合同勉強会にて机上訓練等実施

●関西地域勉強会との合同研究会（2022年2月16日）
•（テーマ）メインテーマ：「with/afterコロナをどう生き抜くか：この1年で進まなかったこと」　①危機管理戦略のアップデート、BCPの議論について　以下、問題意識。
•顧客のニーズ、商品、市場の変化に対するBCPの議論が進んでいない。
•需用減少に対する対策が取れていない。飲食業では補助金で儲かっている事業者もいるが、倒産の危機にある事業者の方が多い。
•また一方で再開時にヒトの確保ができなくなっており、このような問題を我々は抱えているといえる。
•BCPが必要な進化が出来ていない

●維持管理研究会の講演を聴講（2022年5月19日）
•維持管理研究会小田副座長の「OTセキュリティ」に関する講演を有志聴講
•OT（Operational Technology）セキュリティとは？　関連するものとして、OT、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。

●岡山地域勉強会（合同研究会）にて机上訓練・講演を実施（2021年8月）
ITBO研究会にて研究されてきたサイバーインシデントによる事業継続机上訓練・講演を実施

Copyright © 2022 BCAO

まとめ

新型コロナの発生は、働き方改革、DXの進展などへ大きく影響し、情報システムの重要性が更に増していた中のこの1年、情報システム障害、マルウェア、国際紛争での武器化、等の重大インシデントが続発した。

一方で、制御システム、IoT機器、自動走行車、重要インフラ等の事務用情報システム以外での課題が発見・指摘されつつあり、対象範囲・対策が拡がりつつある。

オフィスだけをみても、クラウド化が進み、従来のIT-BCPのノウハウでは対応が難しくなってきているという観点も。

当面、ネット開催になると思われるが、ぜひ、ご加入・ご参加を。

ITBO研究会：メンバー20名強、電機製造、通信、情報システム・サービス、損害保険、建設、コンサルタント、等

Copyright © 2022 BCAO

特定非営利活動法人

事業継続推進機構
情報システム・バックアップオフィス
研究会

A Specified Non-Profit Japanese Corporation

Business Continuity Advancement Organization (BCAO)