サイバー攻撃から事業を守るために考えるべきこと

株式会社川口設計 代表取締役
川口 洋
kawa@sec-k.co.jp

自己紹介：川口 洋

2002年 大手セキュリティ会社に就職

社内のインフラシステムの維持運用業務ののち、セキュリティ監視センターに配属

2013年～2016年 内閣サイバーセキュリティセンター(NISC)に出向

行政機関のセキュリティインシデントの対応、一般国民向け普及啓発活動などに従事

2018年 株式会社川口設計 設立　代表取締役

株式会社川口設計 代表取締役
SOMPOリスクマネジメント株式会社 サイバーセキュリティテクニカルアドバイザー
GMOインターネットグループ株式会社 顧問
GMOサイバーセキュリティ byイエラエ株式会社 顧問
Zホールディングス株式会社 プライバシーに関する有識者会議 委員
消費者庁 最高情報セキュリティアドバイザー
経済産業省 情報セキュリティ対策専門官
文部科学省 サイバーセキュリティアドバイザー
カジノ管理委員会 最高情報セキュリティアドバイザー
富山県警察 サイバーセキュリティ対策アドバイザー
青森県警察 サイバーセキュリティ対策テクニカルアドバイザー
山口県警察 サイバーテクニカルアドバイザー
千葉県警察 サイバーセキュリティ対策テクニカルアドバイザー
大阪府警察 サイバー攻撃対策アドバイザー
兵庫県警察 サイバーセキュリティ対策アドバイザー
経済産業省 情報セキュリティサービス普及促進に関する検討会 委員
経済産業省 地域SECUNITY形成促進WG アドバイザー
消費者庁 特定商取引法等の契約書面等の電子化に関する検討会 委員
国立研究開発法人情報通信研究機構(NICT) 実践的サイバー防御演習 CYDER 推進委員
Hardening Project 実行委員
Micro Hardening プロデューサー
日本セキュリティオペレーション事業者協議会 技術WGリーダ
GMOインターネット財団 助成選考委員

令和3年 サイバーセキュリティに関する総務大臣奨励賞 受賞

保有資格
- CISSP (Certified Information Systems Security Professional)
- CEH (Certified Ethical Hacker)

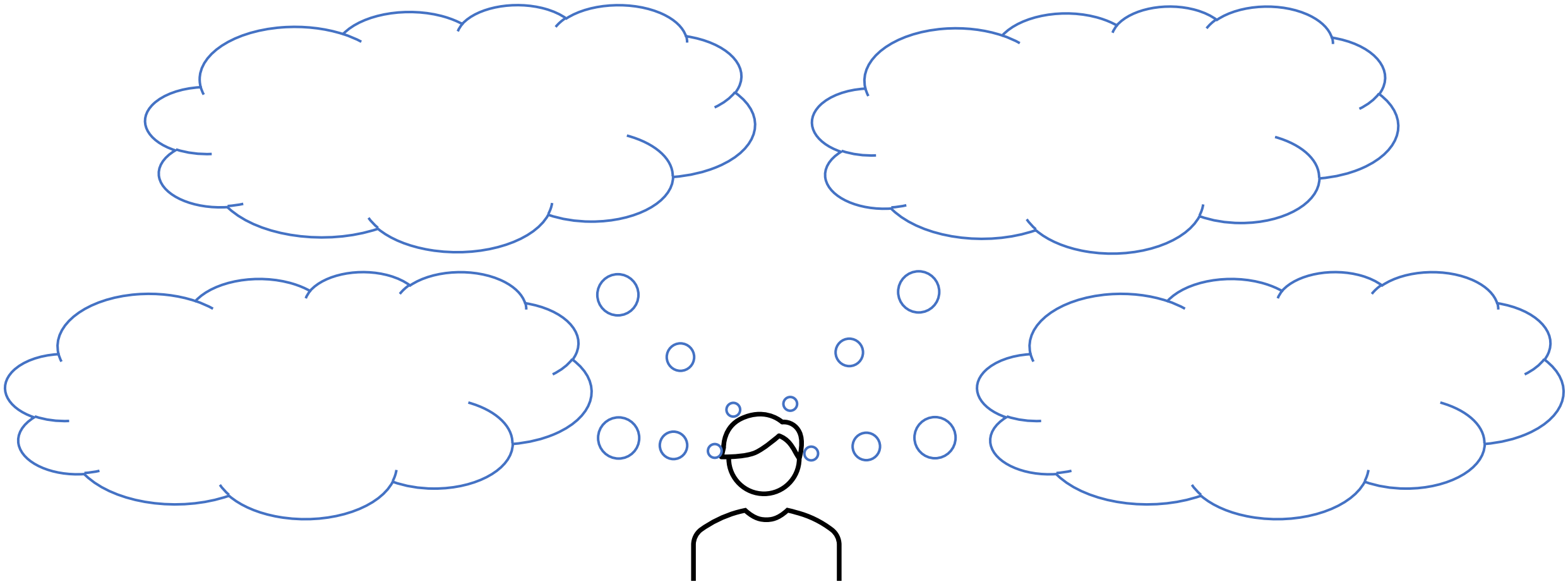
[2023年1月1日時点]

最近のニュース

スーパーマーケットが「セルフレジ」を悪用した万引き被害に頭を悩ませている。バーコードの読み取りや精算を客が自ら行うセルフレジは、人件費削減への期待などから普及が進むが、万引き犯に「人の目」の少なさにつけこまれた格好だ。故意の万引きと悪意のない精算ミスを見分けづらい難点もある。

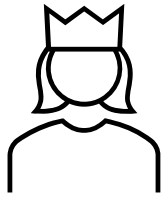
「セルフレジ」で万引き横行「ミスか故意か見極め難しい」
https://www.yomiuri.co.jp/national/20221010-OYT1T50114/

どう考える？

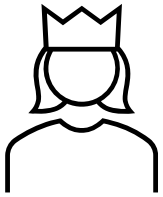


経営者・事業責任者が考えるべき問題

皆様は・・・？



日々の売上のことで頭がいっぱいなんだからその辺はそこそこの予算でうまくやっといてよ



利益確保、事業の安定性確保、ブランディング等を考えたらしっかりやるべき

我々の生活はサイバー空間に依存している

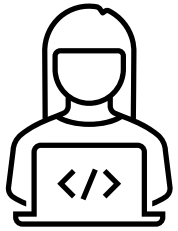
電気
水道
医療
製造
流通
テレビ
ゲーム
などなど

20年前は？

紙が前提の社会
人手でやればよかった
残業もOKだった
インターネット？
セキュリティ？

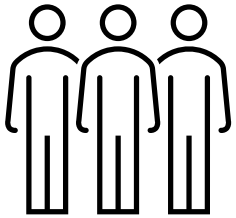
今のご時世、ITなしには仕事は回らない

サイバー攻撃をするのは誰か？



興味本位の個人

お金目当ての犯罪者
(個人 or グループ)



名前を上げたい
ハッキンググループ

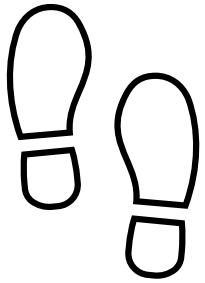
国家が支援するハッキンググループ

これらの攻撃者の間で分業や委託ももちろん存在する

盗まれて困る情報はない？

情報は盗んでから価値をみる

システム停止や業務停止の影響



さらなる攻撃の踏み台に

風評被害や説明責任

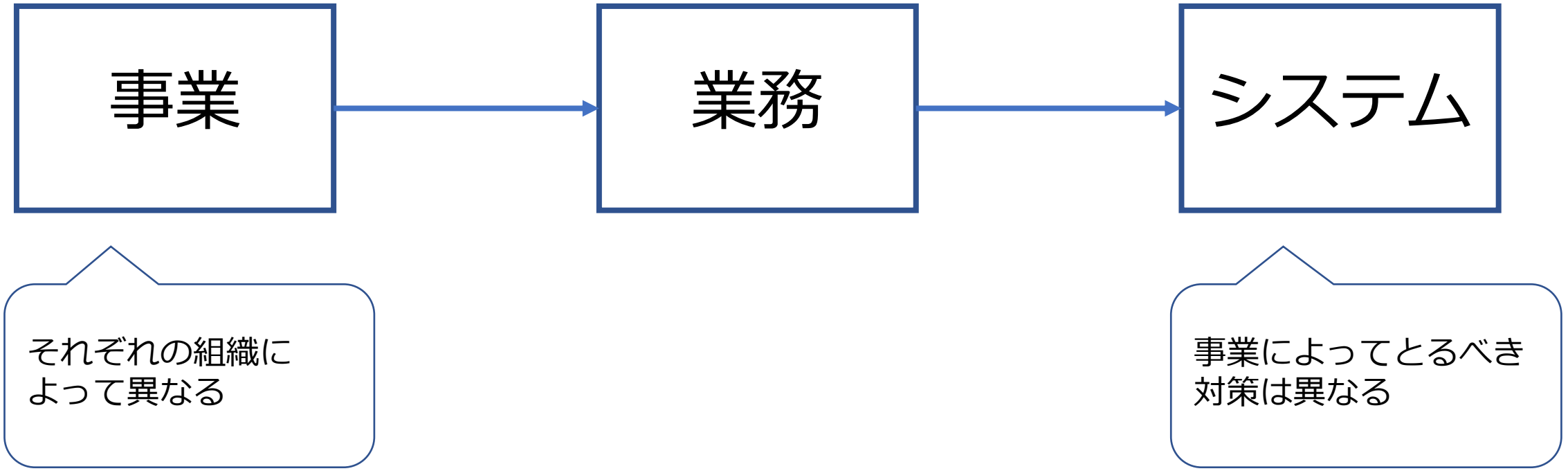
セキュリティはなぜ？

事業継続

情報漏洩対策

説明責任

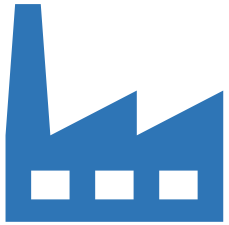
事業継続とサイバーセキュリティ



事業を継続するためのポイント

お金

取引先



業務システムとデータ

サイバー攻撃で発生している問題

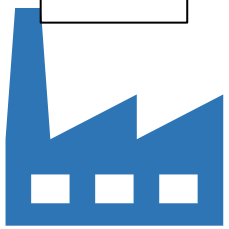
あらゆる組織

偽の送金指示による金銭被害
（ビジネス詐欺メール）

病院

業務システム破壊
→手作業での業務

工場



製造関係データの破壊
→関連企業の工場も停止

①お金を守る

法人口座を守る

＝

不正ログインを防止する

不正ログインに気付く

具体的に何をするか

- 銀行が推奨する対策を実施しているか？
- パスワードを強固なものにしているか？
- 二要素認証を使っているか？
- ワンタイムパスワードを使っているか？
- メール関係のパスワードと別にしているか？
- 使用するパソコンをアップデートしているか？
- 取引履歴を確認しているか？
- 取引時にお知らせがくるようにしているか？
- ログイン履歴を確認しているか？

②取引先を守る

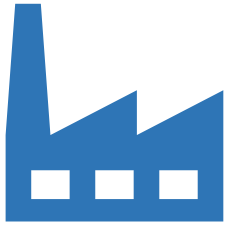
取引先

取引先はどれくらいの数？

情報システムが止まると取引先に迷惑がかかる？

取引先が求めていることは何か？

③業務を守る



業務システムとデータ

もし、情報システムが突然止まったら？

バックアップを取っておく
　→意外に取ってない！！

パスワードをちゃんとつける

アップデートをする

組織全体で守る意識が重要

経営層

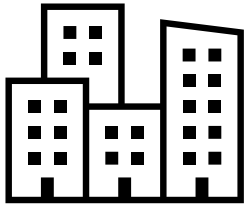
IT部門 | 事業部門 | 管理部門

ユーザ

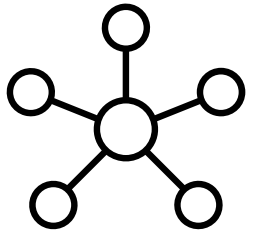
誰かに丸投げしていては
守ることはできない

委託事業者 | 顧客

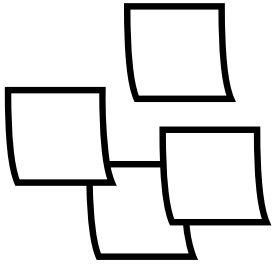
どこに目配りをするべきか



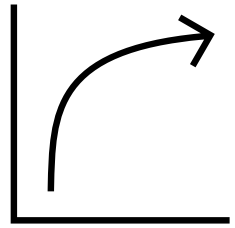
止まると困る業務(システム)



海外子会社、海外事業



個人情報をたくさん持つ事業



うすーく安定的に利益を稼いでいる事業

大事なことは「早く動くこと」

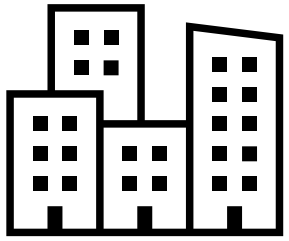
早く

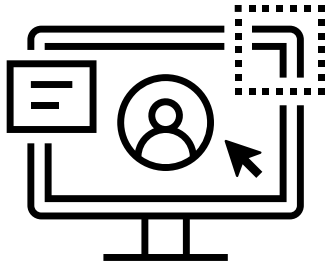
情報を吸い上げる

判断する

指示を出す

早く動くためには

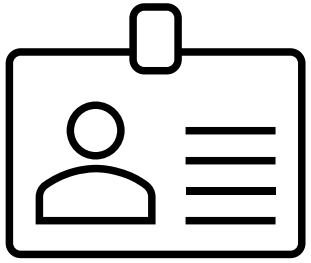




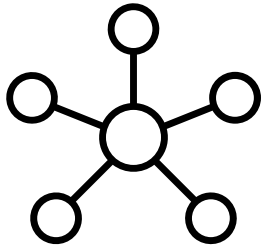
事業とITの両方を把握
平時から情報把握

資産管理をしましょう

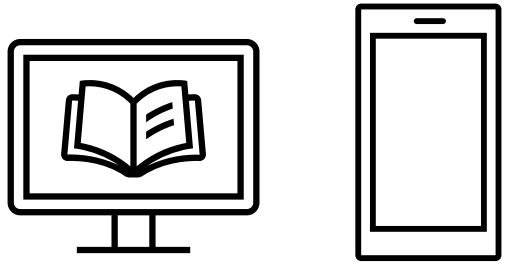
把握できていない資産が被害を受ける
資産管理がまず第一歩



ID



ネットワーク



デバイス

覚えてほしい技術的なこと

IDとパスワードがもれるとおおごとになる

メール　　顧客情報　　銀行口座　　業務システム

困ったときに相談する人

運用委託事業者
各県警本部のサイバー担当
サイバーセキュリティお助け隊
IPA
JPCERT/CC
このセミナーを紹介してくれた人

情報収集、勉強の仕方

- 公式情報を参照する
  - 製品メーカーやサービスベンダ
- セキュリティ関係組織の情報を参照する
  - IPA
  - JPCERT/CC
  - NISC
- セミナーや勉強会に参加する
  - 最近はオンラインのものもあるので、参加しやすくなりました
- 事故調査報告書を読む社内勉強会をする
  - 参加者1人ずつ感想を言ってみる
  - 「うちでこれが起きたらどうする？」
  - 「この原因のところ、うちは大丈夫？」

[参考]重大事故の時にやったほうがいいこと10個

1.作戦司令室をつくる
2.キックオフが重要
3.チームをわける。そしてチーム毎に一人だけチームリーダをつくる
4.定時連絡の仕組みをつくる
5.ホワイトボードを用意
6.食い物と睡眠も復旧対策
7.広報はユーザーファーストに
8.対外リリースも定時化
9.トップは帰ってはいけない
10.終息宣言

引用：重大事故の時にどうするか？　(東京都副都知事 宮坂さん)
https://note.com/mmiya/n/n746eb2e36f81

最後に

備えていないことは対処できない
情報を仕入れて正しく対処する

以下、参考資料

[参考]ぜひ読んでほしいもの

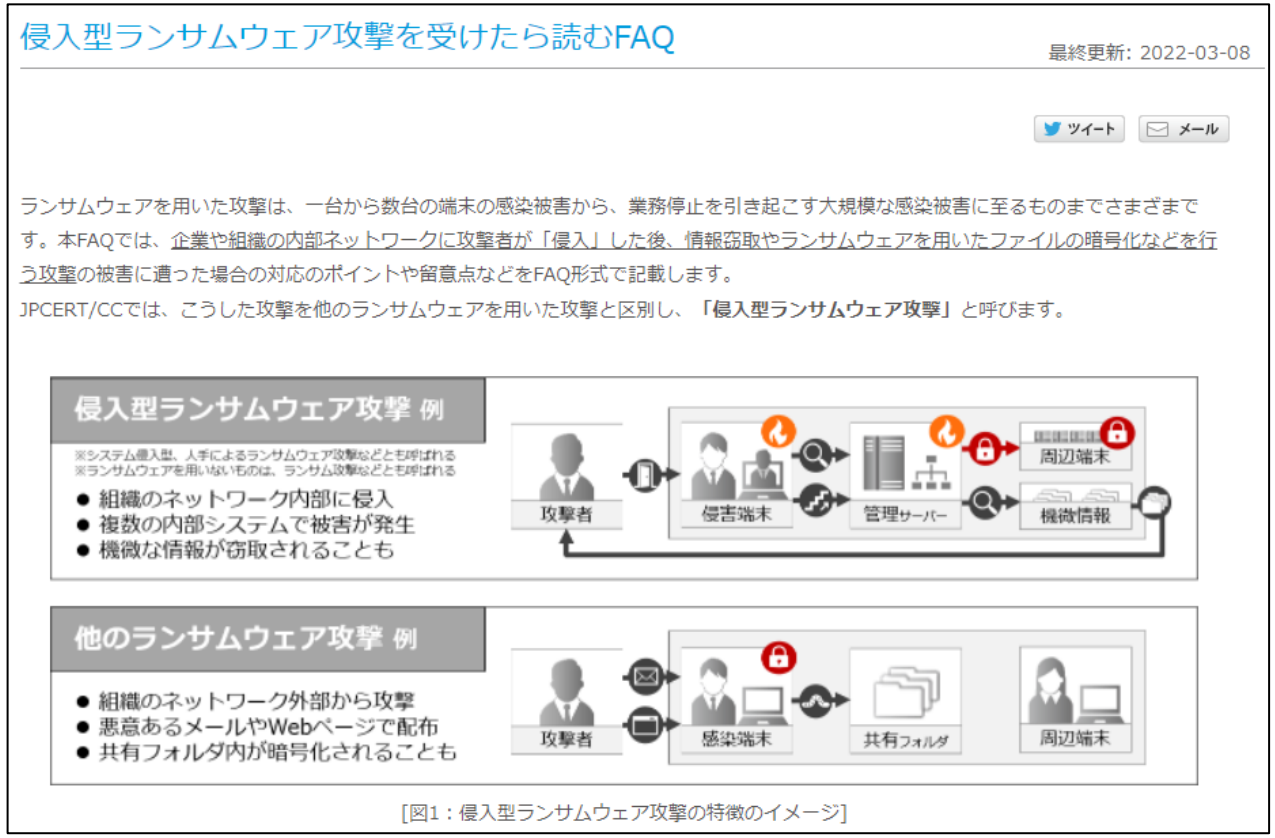
徳島県つるぎ町立半田病院
コンピュータウイルス感染事案有識者会議調査報告書について
　https://www.handa-hospital.jp/topics/2022/0616/index.html

尼崎市
個人情報を含むUSBメモリーの紛失事案について（尼崎市と委託事業者それぞれの報告書）
　https://www.city.amagasaki.hyogo.jp/kurashi/seikatusien/1027475/1030947.html
　https://www.biprogy.com/com/info_security/info202206.html

大阪急性期・総合医療センター
情報セキュリティインシデント調査委員会報告書について
　https://www.gh.opho.jp/important/785.html

トヨタイムズニュース
小島プレス、サイバー被害から1年　苦難乗り越え深めた絆
　https://toyotatimes.jp/newscast/008.html

[参考]侵入型ランサムウェア攻撃を受けたら読むFAQ



[図1：侵入型ランサムウェア攻撃の特徴のイメージ]

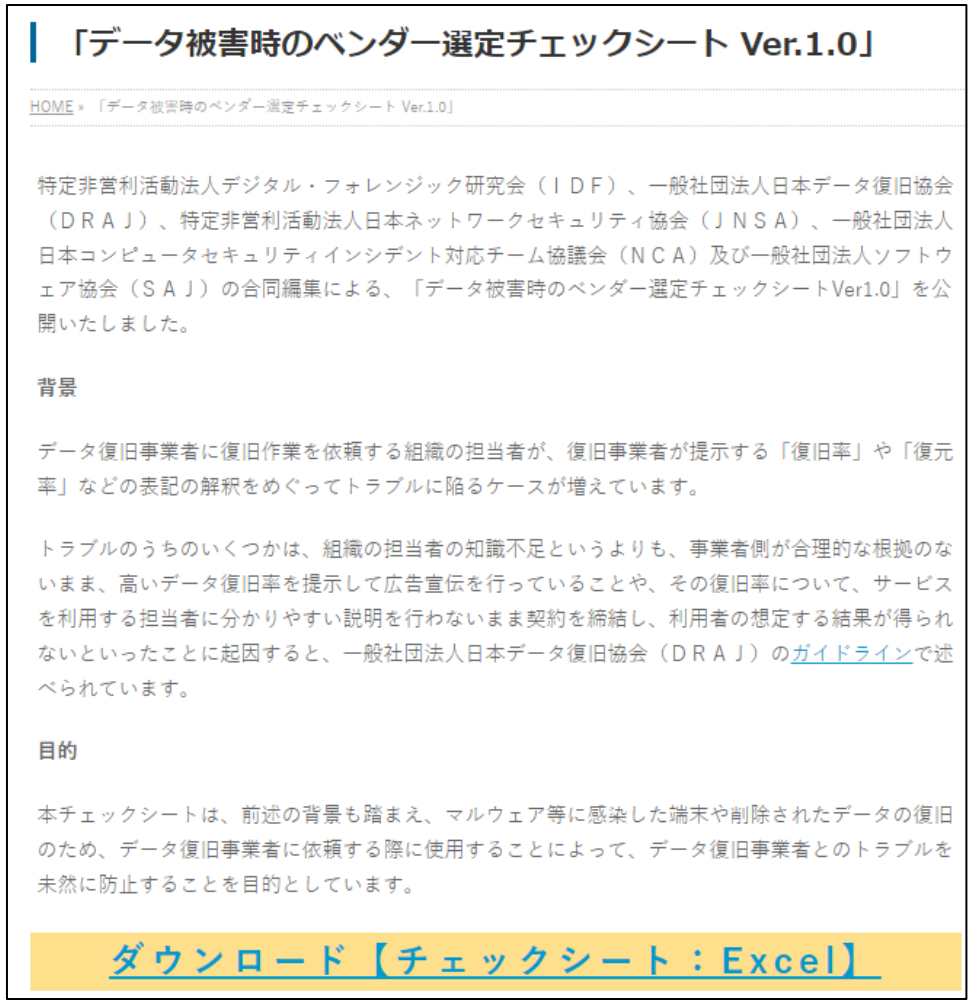
https://www.jpcert.or.jp/magazine/security/ransom-faq.html

1. 被害を受けたら
Q1-1. 被害について相談したいがどうしたらいいか？（被害報告/相談）
Q1-2. 被害を受けたかどうか判断がつかないがどうしたらいいか？（被害の状況把握）
Q1-3. 被害にどのように対応すべきか？（対応方針決定）

2. 被害への対応
Q2-1. 被害を抑えるためにはどうすべきか？（被害を抑える）
Q2-2. 被害の原因をどのように特定し対処するのか？（原因に対処する）
Q2-3. 被害からどのように復旧すべきか？（被害から復旧する）

などなど

[参考]データ被害時のベンダー選定チェックシート



「データ被害時のベンダー選定チェックシート Ver.1.0」

HOME » 「データ被害時のベンダー選定チェックシート Ver.1.0」

特定非営利活動法人デジタル・フォレンジック研究会（ＩＤＦ）、一般社団法人日本データ復旧協会（ＤＲＡＪ）、特定非営利活動法人日本ネットワークセキュリティ協会（ＪＮＳＡ）、一般社団法人日本コンピュータセキュリティインシデント対応チーム協議会（ＮＣＡ）及び一般社団法人ソフトウェア協会（ＳＡＪ）の合同編集による、「データ被害時のベンダー選定チェックシートVer1.0」を公開いたしました。

背景

データ復旧事業者に復旧作業を依頼する組織の担当者が、復旧事業者が提示する「復旧率」や「復元率」などの表記の解釈をめぐってトラブルに陥るケースが増えています。

トラブルのうちのいくつかは、組織の担当者の知識不足というよりも、事業者側が合理的な根拠のないまま、高いデータ復旧率を提示して広告宣伝を行っていることや、その復旧率について、サービスを利用する担当者に分かりやすい説明を行わないまま契約を締結し、利用者の想定する結果が得られないといったことに起因すると、一般社団法人日本データ復旧協会（ＤＲＡＪ）のガイドラインで述べられています。

目的

本チェックシートは、前述の背景も踏まえ、マルウェア等に感染した端末や削除されたデータの復旧のため、データ復旧事業者に依頼する際に使用することによって、データ復旧事業者とのトラブルを未然に防止することを目的としています。

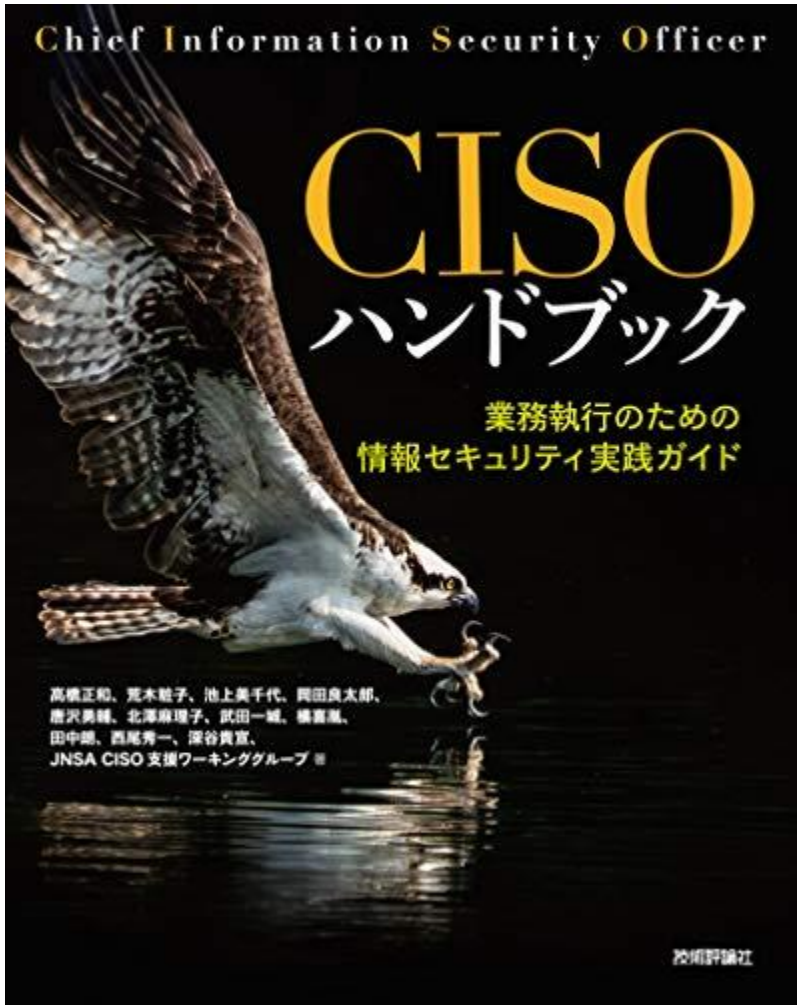
ダウンロード【チェックシート：Excel】

https://digitalforensic.jp/higai-checksheet/

データ復旧を依頼する前に確認すべきこと(ランサムウェア版)

No.	時期	キーワード	質問	回答選択肢	
1	依頼前・事業者選定・問い合わせ	データ復旧	どういう場合にデータが復旧できたといえるかを理解していますか？		データ復旧には、対象 定義するデータ復旧の
2		データ復旧	データ復旧は、依頼組織が復旧を希望するデータが復旧しない場合でも、「データは復旧した」とされることがあることを理解していますか？		
3		復旧率 広告 宣伝	データ復旧率の高さをデータ復旧の事業者選定の基準にしましたか？		データ復旧率の定義は ※一般社団法人 日本
4		問合せ 口頭説明	復旧事業者に問い合わせた際に、復旧事業者から、契約前に「復旧できます」などと口頭だけの説明を受けましたか？		「復旧できます」という事 た」と言われても契約違
5		問合せ 催促	復旧事業者に問い合わせた際に、HDDやSSDをパソコン等から取り外している、または電源を落としているのに、時間の経過とともに、復旧が難しくなると言われましたか？		HDDやSSDをパソコン
6		ランサムウェア 復号鍵	ランサムウェア対策サイトで、暗号化されたファイルの復号鍵を入手する方法を試しましたか？		ランサムウェア対策サイ ランサムウェア対策サイ ransom.html）、ラ
7		事前送付 簡易診断	データ復旧の事前確認として、契約前に復旧事業者に対象機器を送付して確認してもらったり、電話やWebサイトによる簡易診断を実施してもらいましたか？		対象機器を送付しての 合も多々あります。その イル一覧画像等）を要
8		事前送付 説明	事前確認や簡易診断後、実際の解析調査に着手していないにもかかわらず、復旧事業者から、「復旧できます」、「高い確率で復旧見込みあり」といった説明を受けましたか？		
9		事前送付 口頭説明	事前確認や簡易診断後、電話による口頭だけの説明をされましたか？		説明でデータ復旧に成

[参考]CISOのための必読本



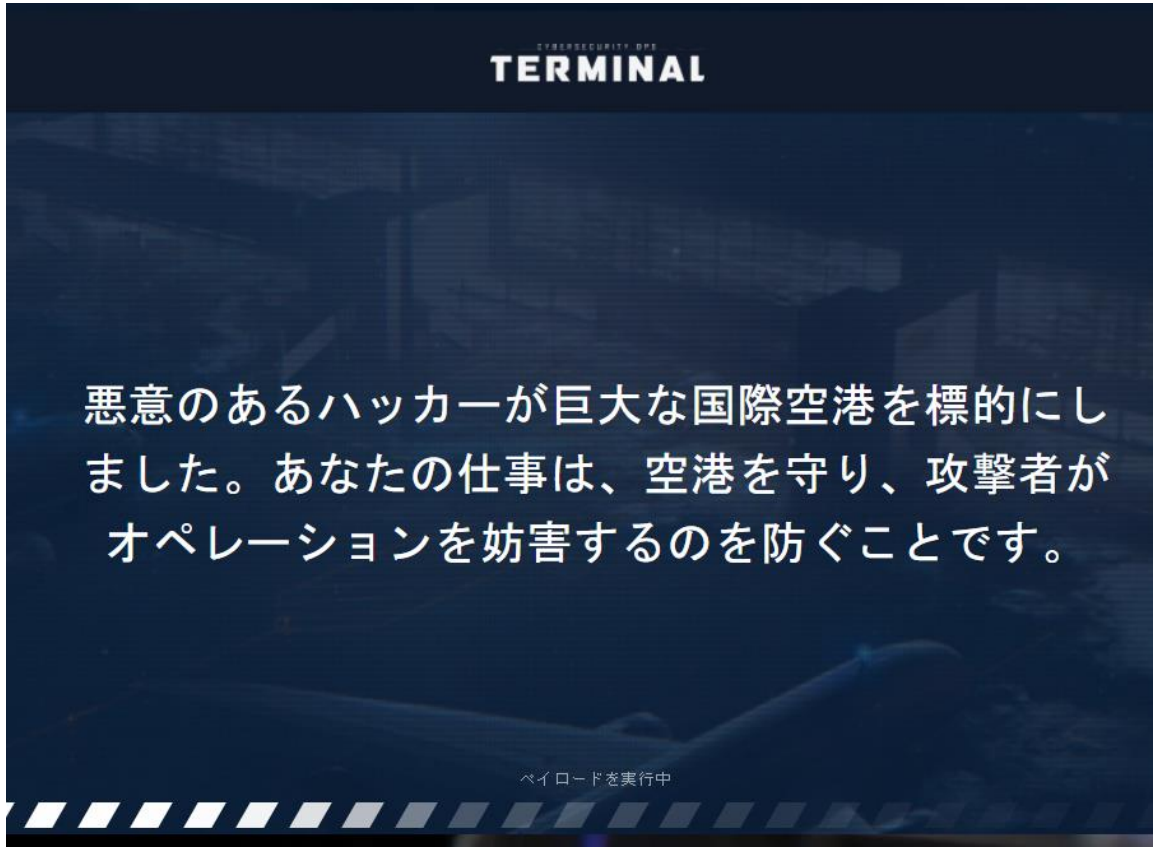
CISOハンドブック

業務執行のための情報セキュリティ実践ガイド

https://www.amazon.co.jp/dp/B08T5VH94X

企業はDX（デジタルトランスフォーメーション）によって変化しなければならない、しかしIT化すればするほど情報セキュリティの問題が発生！　業者に頼めばいいのか……、いや継続的に情報セキュリティの問題は起きてしまうだろう……。そう、企業がIT化を進めDXを促進すると、情報セキュリティが生命線になることは避けられないのが本当のところです。そこで欧米では技術職の視点をもった経営陣の一人としてCISO（Chief Information Security Officer）の役職が誕生しました。情報セキュリティ問題に悩むあらゆる企業の担当者の皆さんのために、本書はCISOがすべき情報セキュリティの問題解決方法を最新の情報をもとにまとめあげました。

[参考]ブラウザでできるインシデント体験ゲーム



IBM社が公開しているサイバー攻撃シミュレーションゲーム

空港のオペレーションを「IT担当」「マネージャ」「経営者」の立場でインシデント対応をする

ブラウザのみで30分程度で体験可能。ぜひ一度体験してみてほしい。

https://www.ibm.com/security/digital-assets/cybersecurity-ops/terminal/#/jp-ja/