サイバー攻撃から事業を守るために やらなければならないこと

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
Zホールディングス株式会社ユーザー目線を踏まえた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
北海道警察 サイバーテクニカルアドバイザー
沖縄県警察 サイバー事案対策アドバイザー
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8月21日時点]

読んでほしい事故調査報告書

政策研究大学院大学
情報セキュリティインシデント報告書の公表について
　https://www.grips.ac.jp/jp/news/20230822-0365/

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（動画）
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

実は・・・

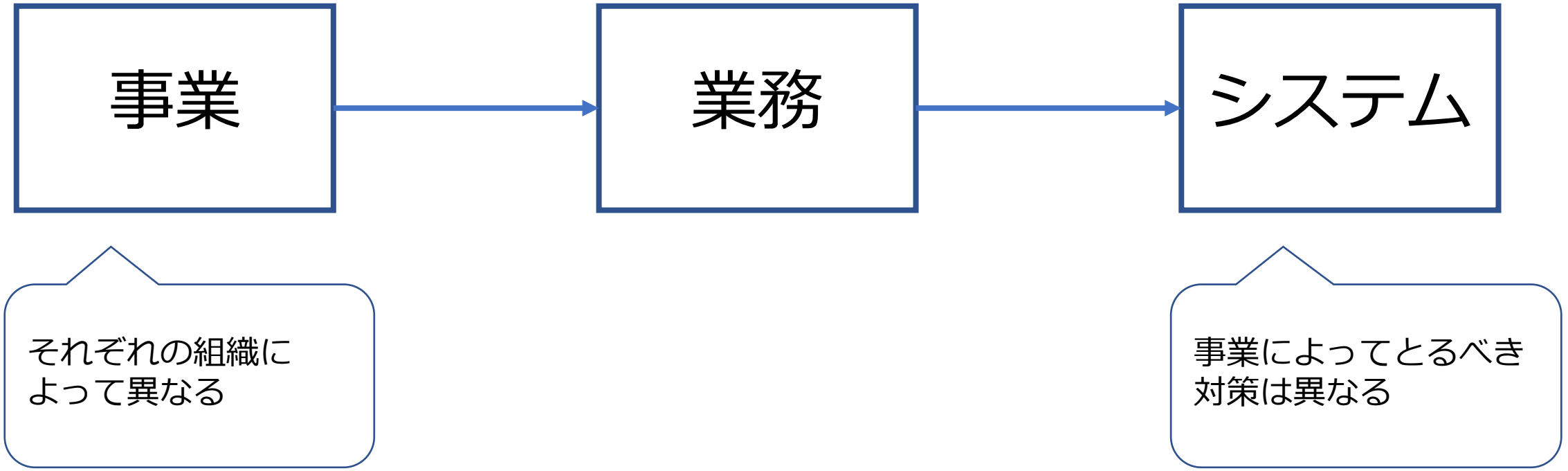
これらの事件には共通点があります
○○○○がないこと
つまり、□□□□□

考えてもらいたいこと

大事なことはそれぞれの組織における「事業の継続」

事業の継続に求められる要件はそれぞれ異なる
異なる組織、業務、システムにおける対策に何が求められるか？

事業継続とサイバーセキュリティ



見えてきた課題

組織的課題

組織構造、業界特性、法律の要件等
ヒト、モノ、カネなど

技術的課題

資産管理、構成管理、パスワード管理、
アカウント管理、脆弱性管理、などなど

見えてきた課題

組織的課題

でも、実際はこちらの問題に起因していることが多い。しかし、手を付けられないので技術的課題に傾倒＆依存する。

技術的課題

セミナーや講演ではこちらが取り上げられることが多い

組織的課題

予算

人員

平時にはどちらも大きく構造をいじることが難しい

もし経営者が○○○○経営者なら？
経営者の目線でみると予算は？

予算獲得に関する目線

もし、忙しい経営者の意識に
訴えるなら？

☆好きな書籍
DeNAのサイバーセキュリティ　Mobageを守った男の戦いの記録
https://www.amazon.co.jp/dp/B01M15IUUG/
もしも社長がセキュリティ対策を聞いてきたら
https://www.amazon.co.jp/dp/4822215911

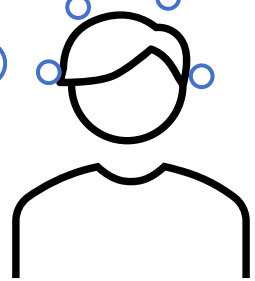
人員獲得に関する悩み

適任者を採用できるのか？

組織内で処遇を
調整できるのか？

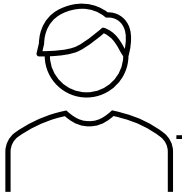
適任者がいるのか？

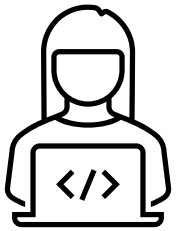
いっそ、外部委託した方
がいいのでは？



多くの組織では手を付けにくい問題

委託先管理に関する理解





ベンダはITとセキュリティのことはわかっているはずだ

提案時にセキュリティのこともアピールしていたからやってるはずだ

他のシステムのことも考えて作業してくれるはずだ

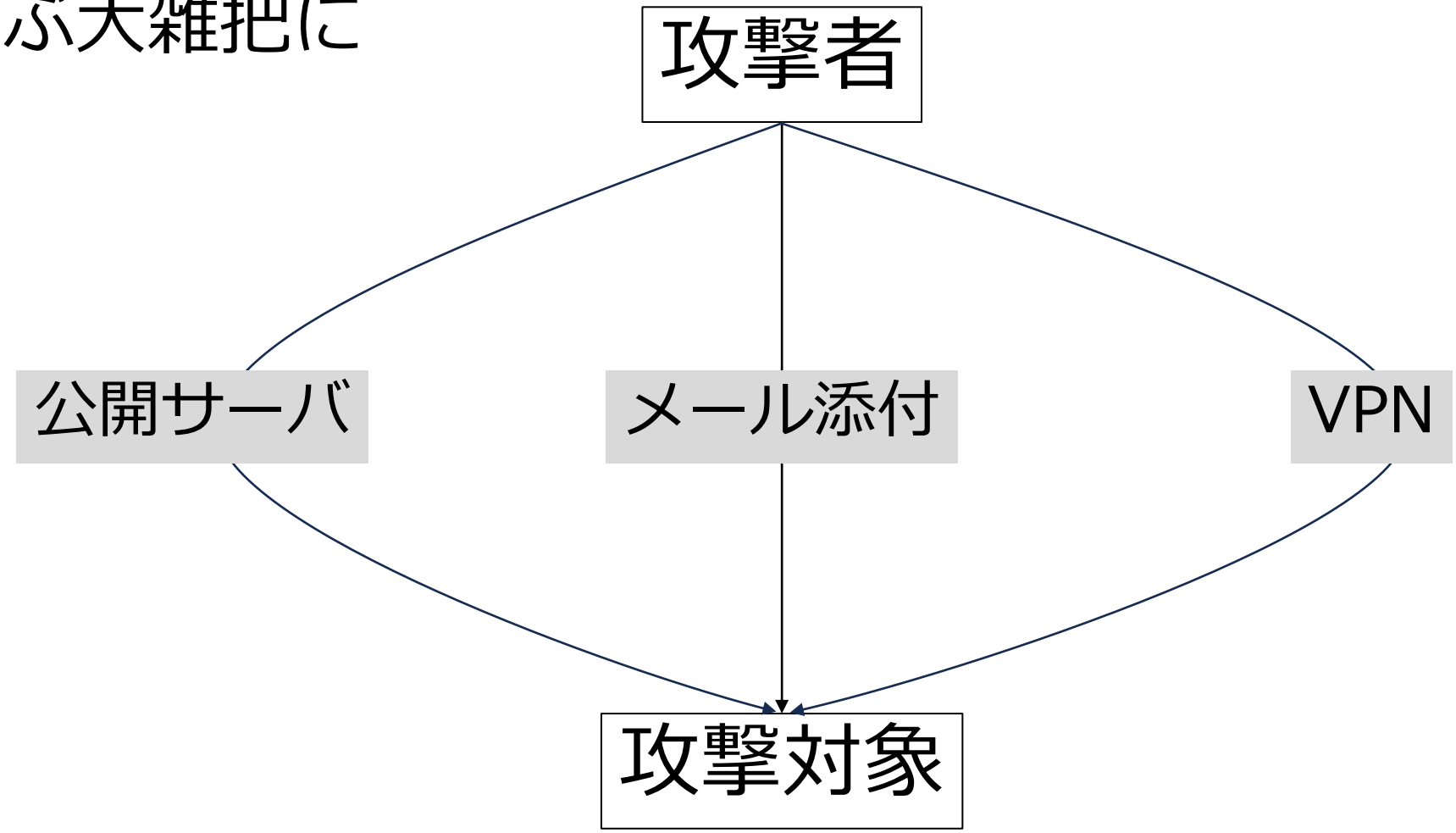
昔はセキュリティのことも”いいかんじに”やってくれていたはずだ

組織の課題と技術の課題

組織的課題に手を付けずに
技術的課題だけに手を出しますか？

攻撃の経路

※だいぶ大雑把に



技術的課題に対するアプローチ

やるべきことをやる
既存の仕組みを活用する

[技術]やるべきこととは？

組織内部の定例会
委託先ベンダとの定例会
内部の監査、ベンダの監査

一つ一つは大した内容ではないが、問題が起きる組織ほど放置されている

[技術]既存の仕組みとは？

アカウント管理、棚卸、パスワード設定
ウイルス対策ソフトの活用
ログの出力設定と保存期間の見直し
Firewall機能の活用
メンテナンス用ポート、管理者画面のアクセス制御
Active Directory機能、資産管理ツールの活用

これからどうするか？

意識してほしいこと

システム担当者を

組織全体で守る意識が重要

経営層

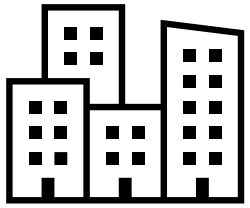
IT部門 | 事業部門 | 管理部門

ユーザ

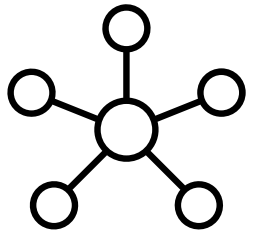
誰かに丸投げしていては
守ることはできない

委託事業者 | 顧客

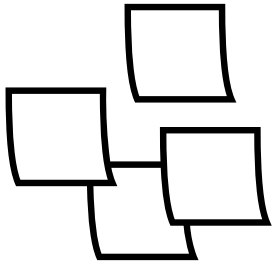
どこに目配りをするべきか



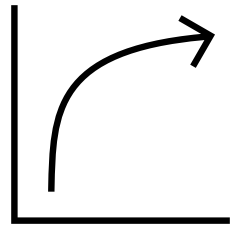
止まると困る業務(システム)



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

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

政策研究大学院大学
情報セキュリティインシデント報告書の公表について
　https://www.grips.ac.jp/jp/news/20230822-0365/

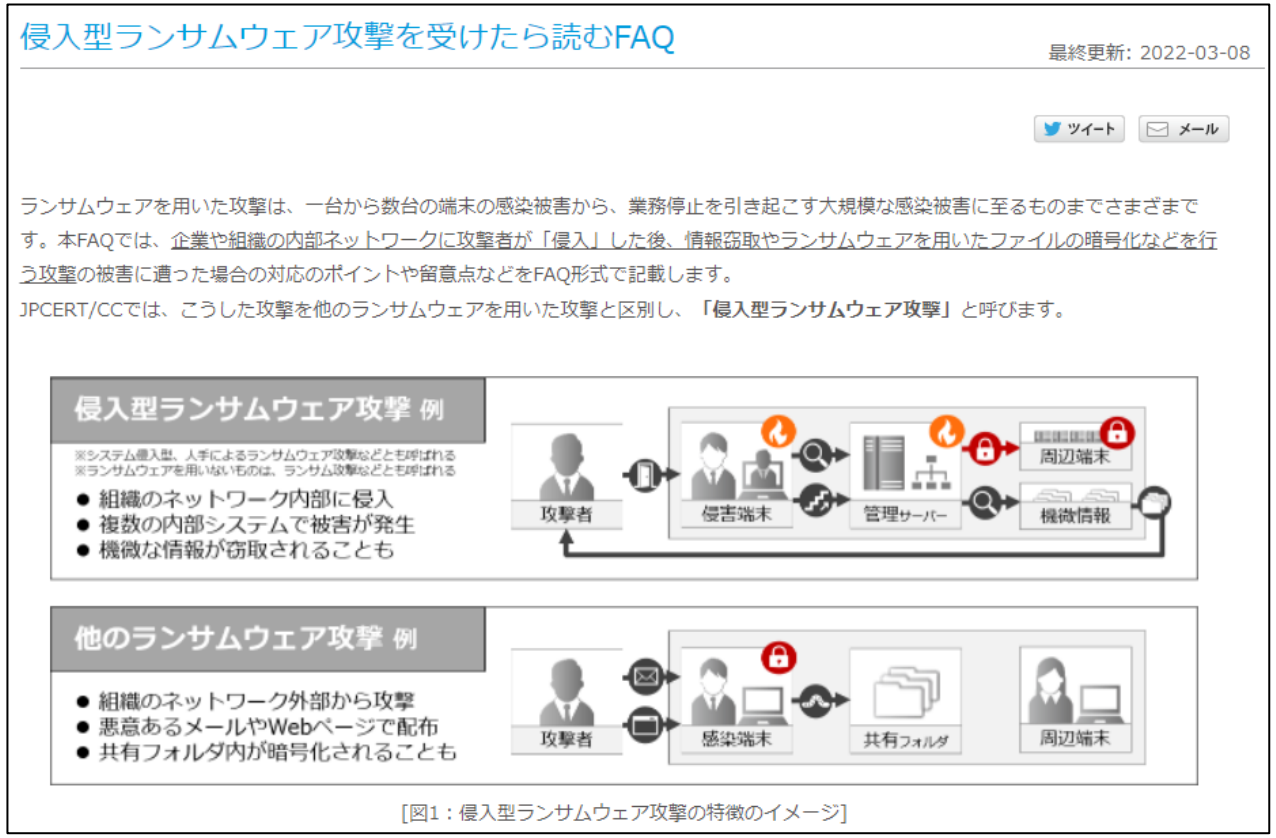
徳島県つるぎ町立半田病院
コンピュータウイルス感染事案有識者会議調査報告書について
　https://www.handa-hospital.jp/topics/2022/0616/index.html

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]

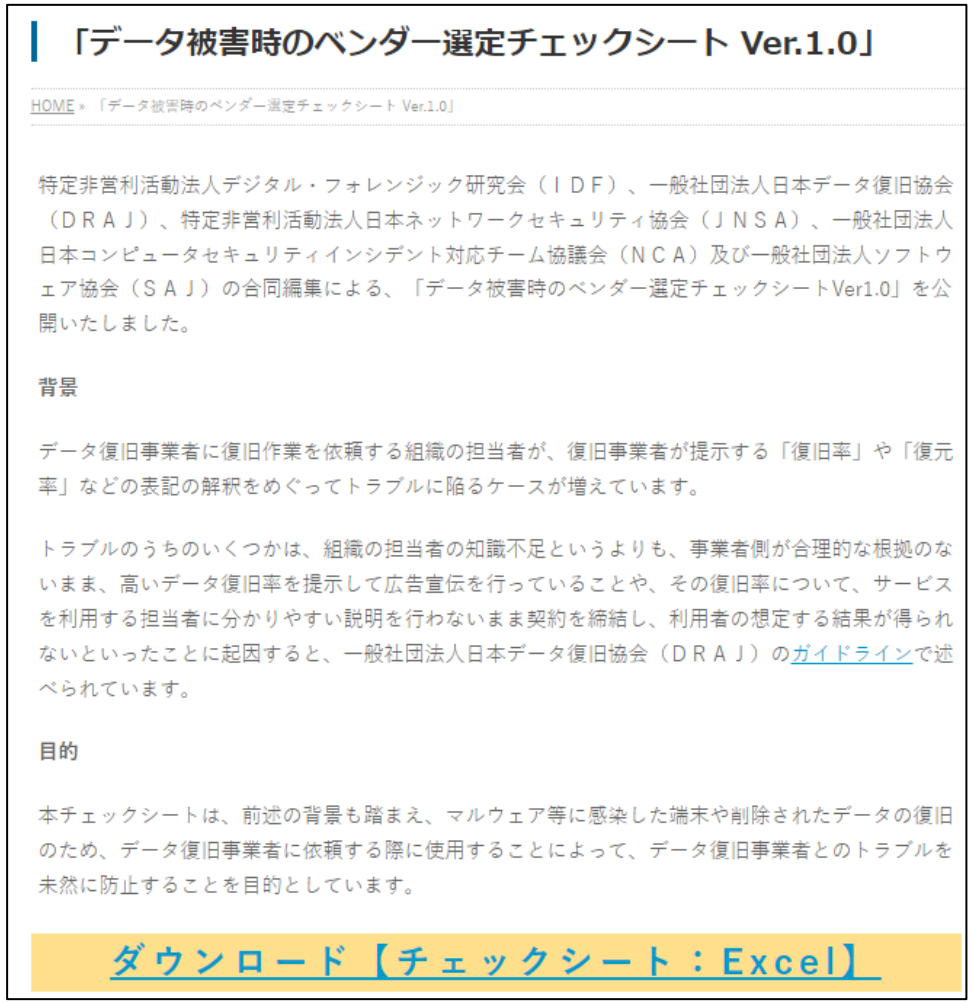
https://www.jpcert.or.jp/magazine/security/ransom-faq.html

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。

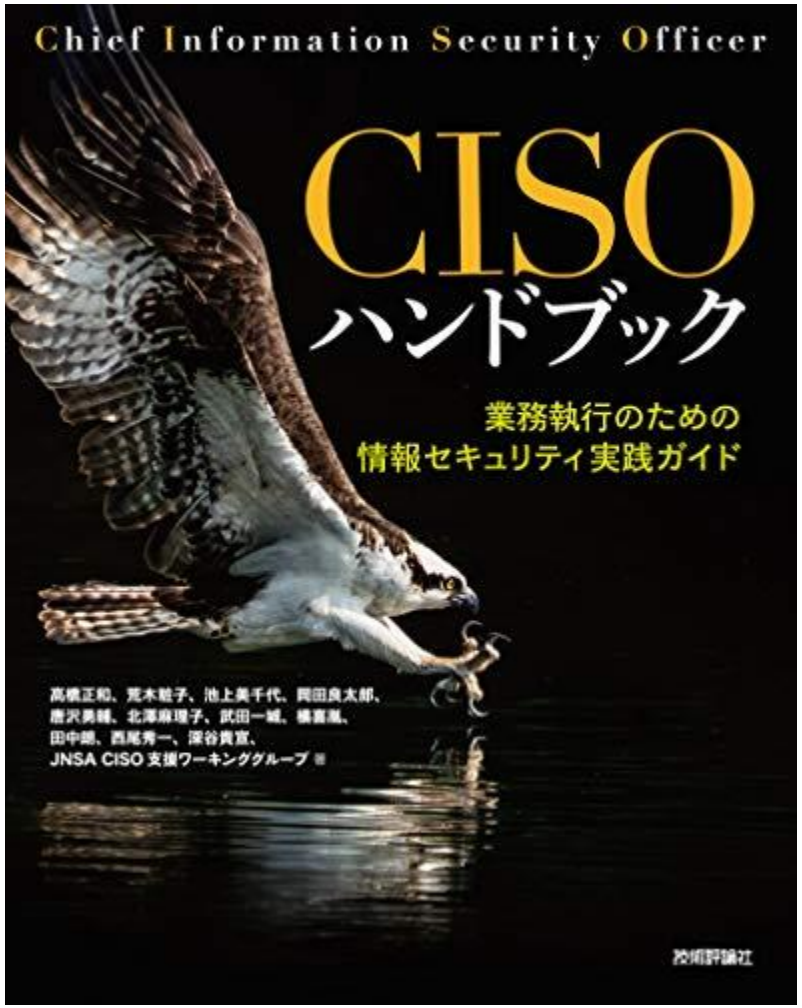
ダウンロード【チェックシート：Excel】

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 イルー覧画像等)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



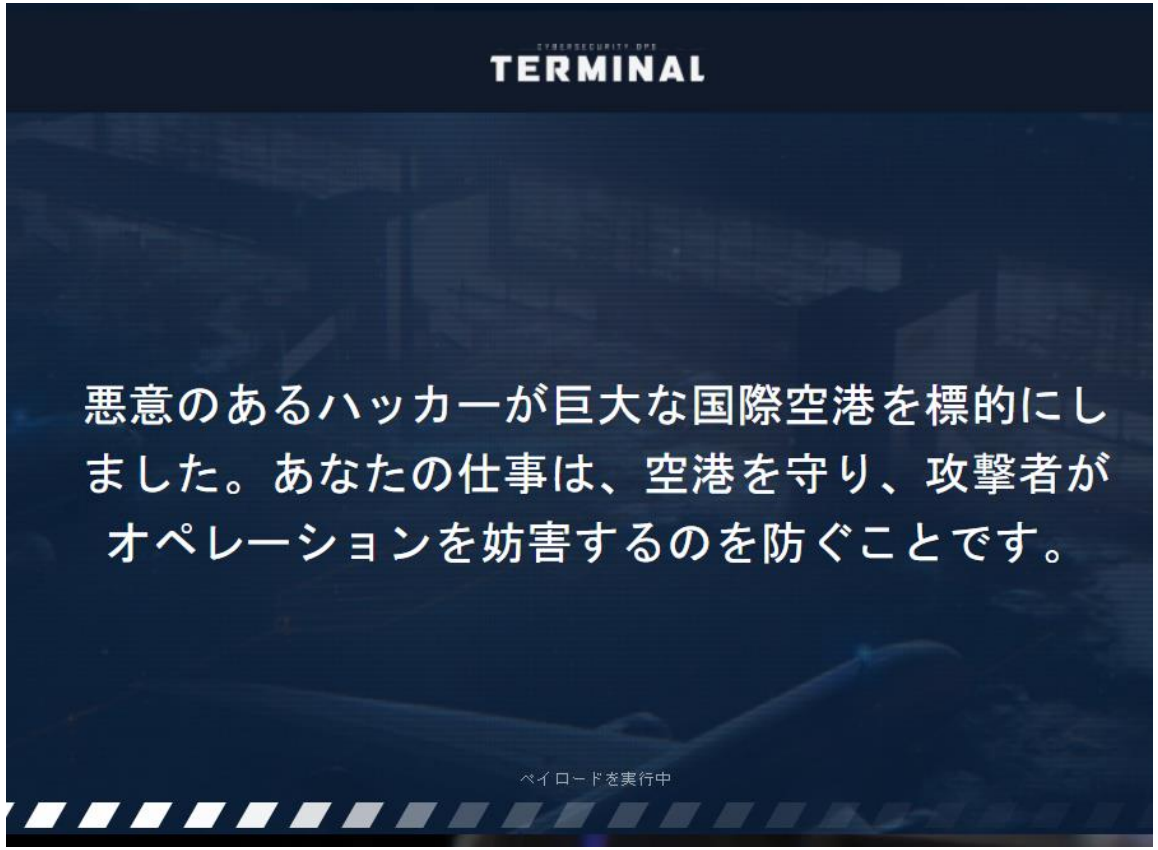
CISOハンドブック

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/

Hardening Project

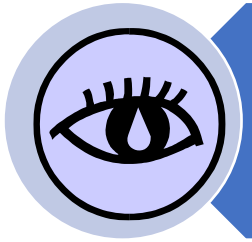
実践的な堅牢化技術の価値を最大化すること

ビジネスの視点

Focus on prevention techniques and process

守る技術の顕彰

Engineering awards and talent discovery



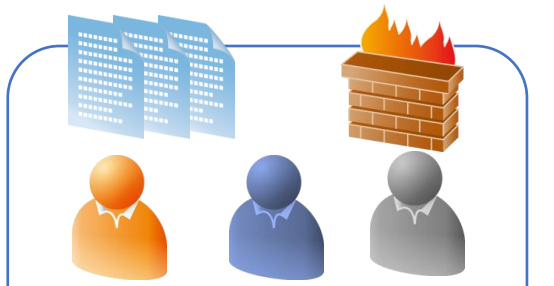
利用者視点の認識向上

Perspective for stakeholder communication

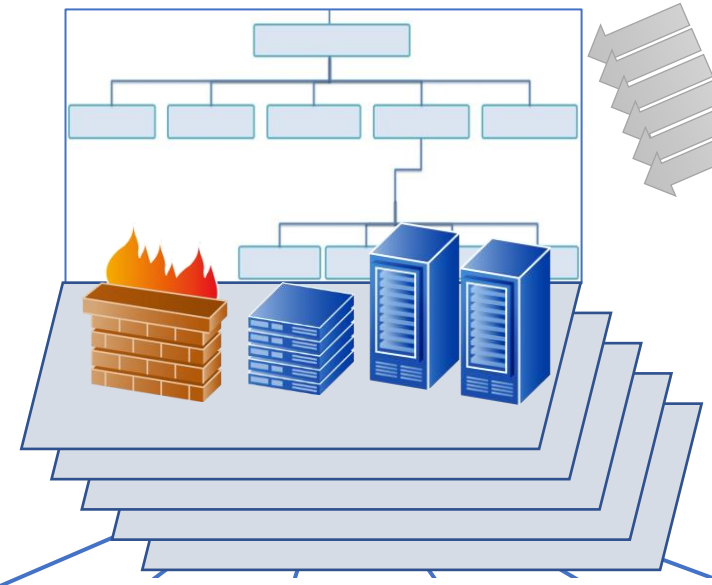
1. 2012年 4月 Hardening Zero（東京）
2. 2012年10月 Hardening One（東京）
3. 2013年 7月 Hardening One Remix（東京）
4. 2014年 6月 Hardening 10 APAC（沖縄）
5. 2014年11月 Hardening 10 Evolutions（沖縄）
6. 2015年 6月 Hardening 10 MarketPlace（沖縄）
7. 2015年11月 Hardening 10 ValueChain（沖縄）
8. 2016年 6月 Hardening 100 Value x Value(沖縄)
9. 2016年11月 Hardening 100 Weakest Link(沖縄)
10. 2017年 6月 Hardening 1010 Cash Flow(沖縄)
11. 2017年11月 Hardening 2017 Fes(淡路島)
12. 2018年 7月 Hardening II Collective(宮古島)
13. 2018年11月 Hardening II SecurEach(宮古島)
14. 2019年 7月 Hardening II SU(札幌)
15. 2020年 1月 Hardening 2020 BO(沖縄)
16. 2020年 9月 Hardening 2020 Deep Digital Dependence(オンライン)
17. 2020年11月 Hardening 2020 H3DX(オンライン)
18. 2021年 8月 Hardening Drivers Conference 2021(オンライン)
19. 2021年11月 Hardening 2021 Active Fault(オンライン)
20. 2022年 9月 Hardening Designers Conference 2022(オンライン)
21. 2022年11月 Hardening Decade 2022(沖縄＆オンライン)
22. 2023年 5月 Hardening Designers Conference 2023(オンライン)
23. 2023年10月 Hardening 2023 Generatives(北海道＆オンライン)

8時間の耐久競技にインターネットの縮図を実現
限られたリソースを最大限に生かし、ビジネス価値の最大化を競う

競技空間で提供される様々なサービスや製品を調達し、自チームに足りない能力を補完

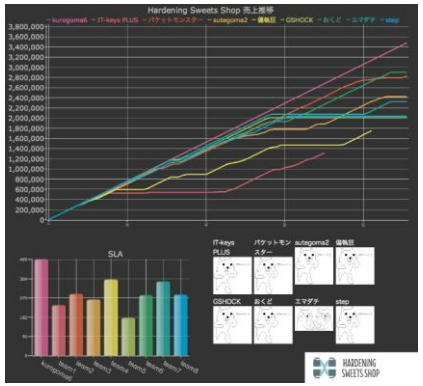


第三者の製品とサービス

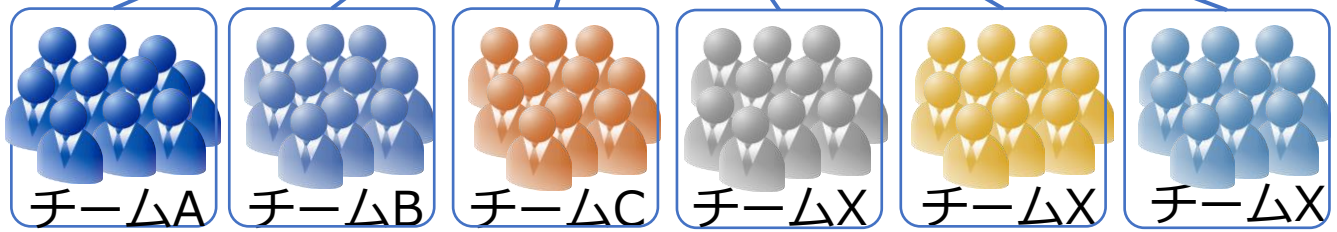


シナリオ遂行・評価
kuromame6

Eコマースサイトの”売上”と”稼働状況”をリアルタイム・スコアボードに



参加者（6人～10人のチームで編成）



チームA　チームB　チームC　チームX　チームX　チームX

参加者は与えられたショッピングサイトの売上を最大化するべく、チームワークを生かして行動する。
「攻撃検知」「被害の極小化」「攻撃対処」「システム復旧」「社内調整」「顧客対応」「商品調達」など様々な技能を競う。

HARDENING宣言

- 私たちの挑戦は、現場で**本当に起きている脅威**と向き合うことである。
- それは、強固な計画よりも**柔軟な変化**を必要とする。
- それは、役割分担よりも**連携と協働**を必要とする。
- それは、隠蔽しようとする誘惑、単純化しようとする誘惑、そして転嫁しようとする**誘惑に抵抗**することである。
- それは、現状よりも**目的**を、知識よりも**経験**を、コンテンツよりも**コンテキスト**を、そしてアイテムよりも**ストーリーを重視**することである。
- これによってはじめて、異なる視点、異なる意欲、異なる役割、異なる手段をもつ**仲間を獲得**し、困難に立ち向かうことができる。
- 私たちの挑戦は、この志と企てを共有し、**前進する**ことである

Hardening Project：万国津梁館にて、HARDENING宣言を発表しました。
https://wasforum.jp/2020/01/hardening-manifesto/