サイバー攻撃から事業を守るために今すべきこと

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
株式会社イエラエセキュリティ 顧問
EC-Council セキュリティエンジニア養成講座CEH トレーナー
GMOインターネット株式会社 顧問
Yahoo! JAPAN プライバシーに関するアドバイザリーボード 委員
Zホールディングス株式会社 グローバルなデータガバナンスに関する特別委員会 委員
内閣府本府 情報化参与 最高情報セキュリティアドバイザー
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
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
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

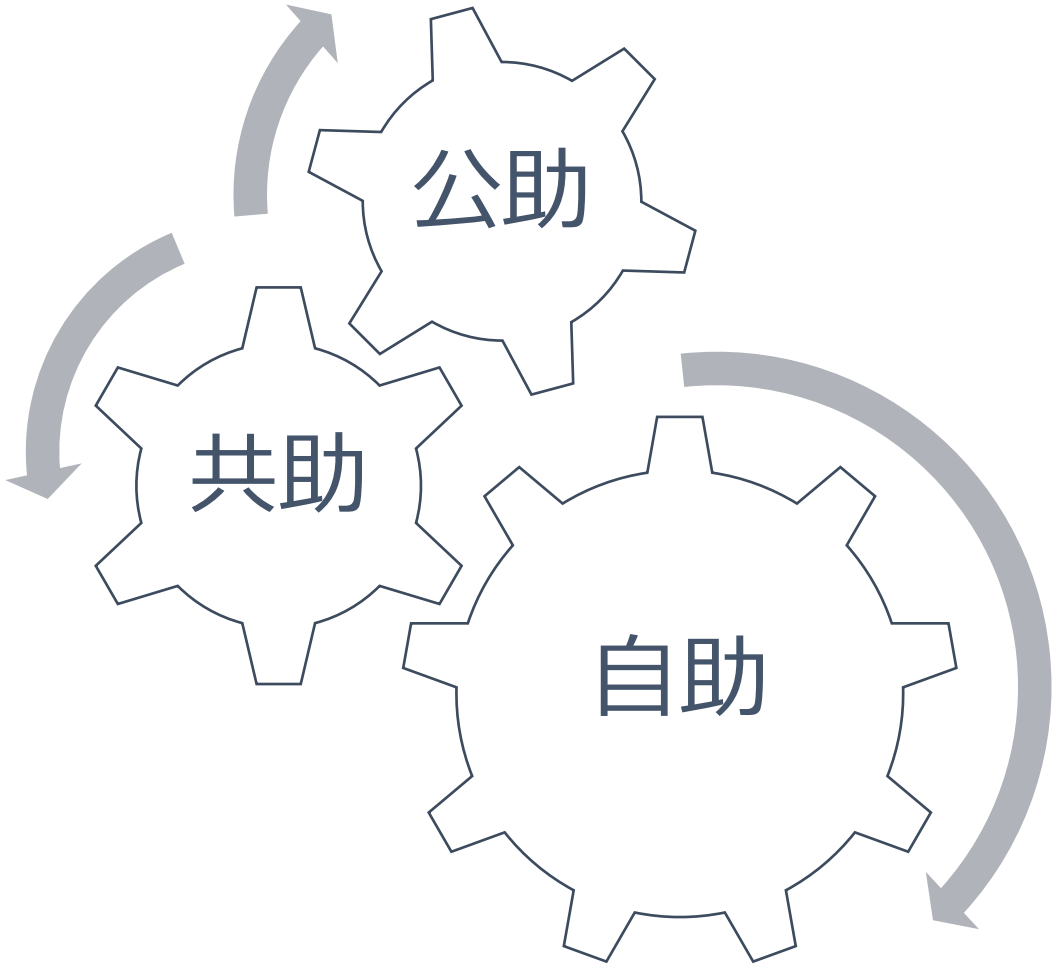
令和3年 サイバーセキュリティに関する総務大臣奨励賞 受賞

[2021年10月1日時点]

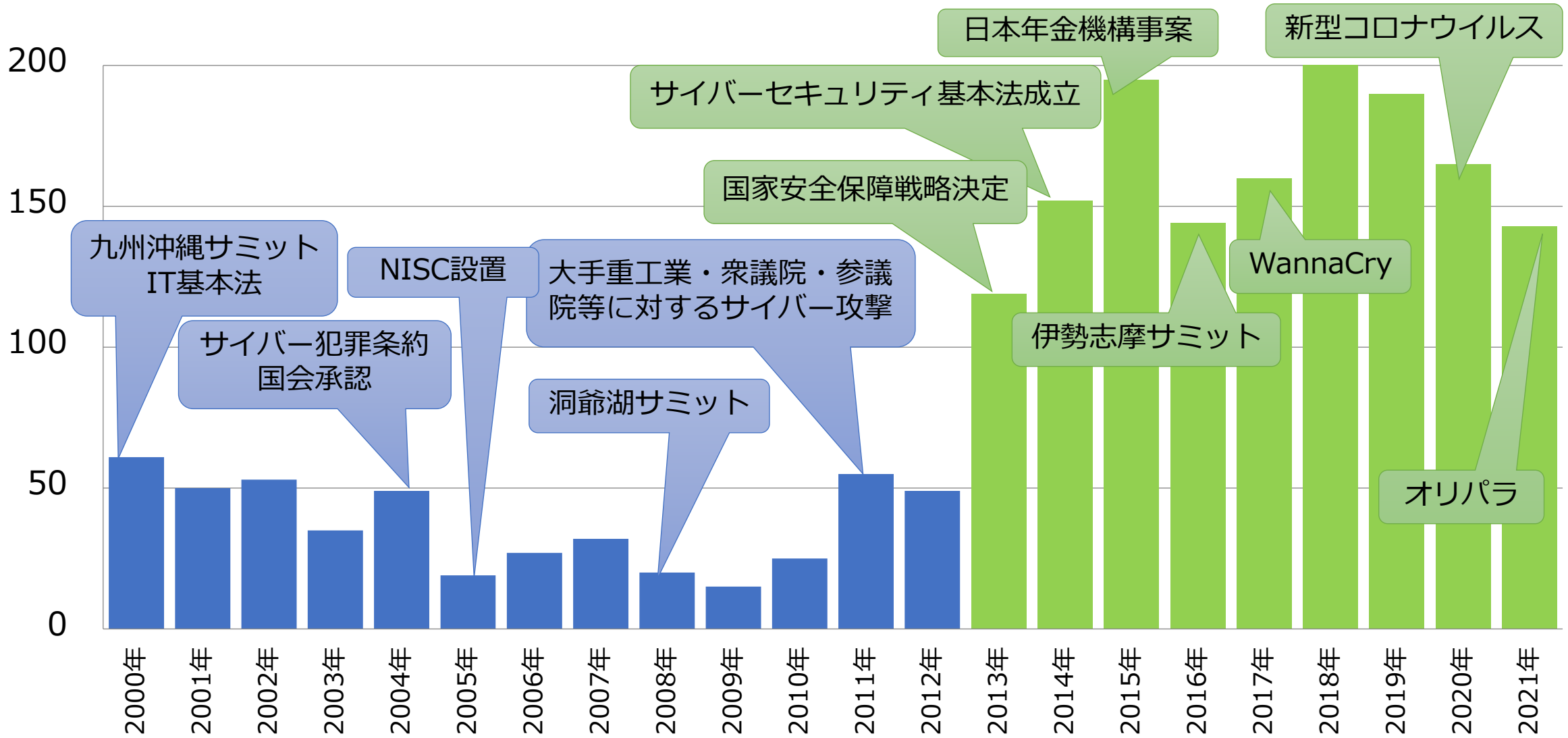
保有資格
- CISSP (Certified Information Systems Security Professional)
- CEH (Certified Ethical Hacker)

川口設計の活動方針

川口設計



サイバーセキュリティの動向



国会会議録から「サイバー」を含むキーワードを検索した数を集計

セキュリティはなぜ？

事業継続

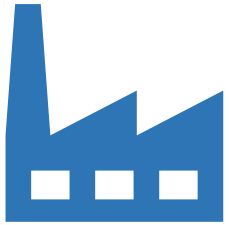
情報漏洩対策

説明責任

事業継続とサイバーセキュリティ

お金

取引先



業務システムとデータ

事業継続とサイバーセキュリティ

お金

銀行口座のお金を守ること

キーワード：不正送金、ビジネス詐欺メール(BEC)

事業継続とサイバーセキュリティ

取引先

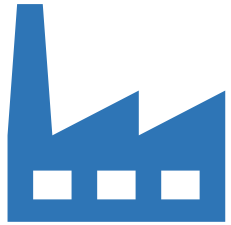
取引を切られないようにすること

キーワード：
NDA関連情報
輸出管理対象技術

事業継続とサイバーセキュリティ

業務を止めない＆復旧できること

キーワード：
アクセス制御
バックアップ



業務システムとデータ

コロナ禍で変化したIT環境

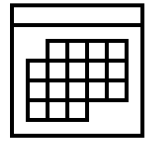
リモートワーク推進

ウェブ会議システムの活用
クラウドサービスの活用

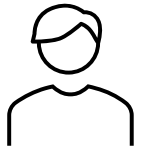
これまでのIT環境

オフィス

パソコン



アプリケーション

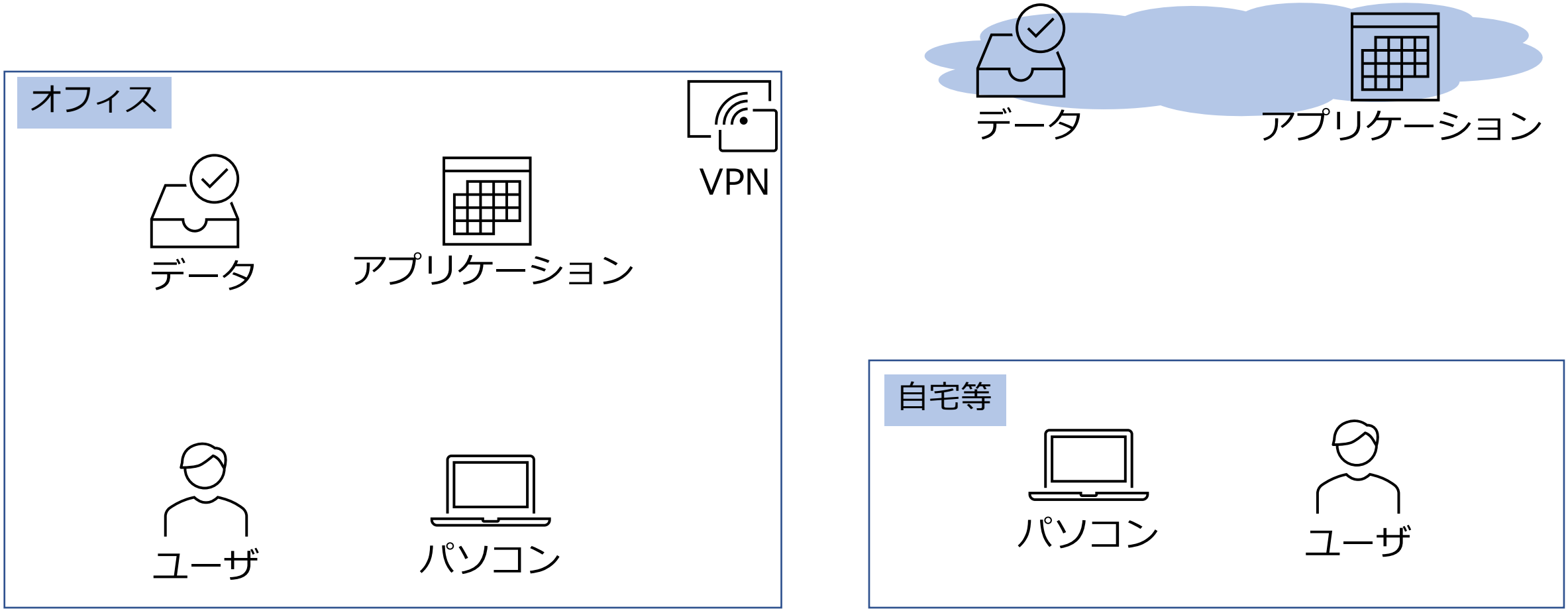


ユーザ

データ

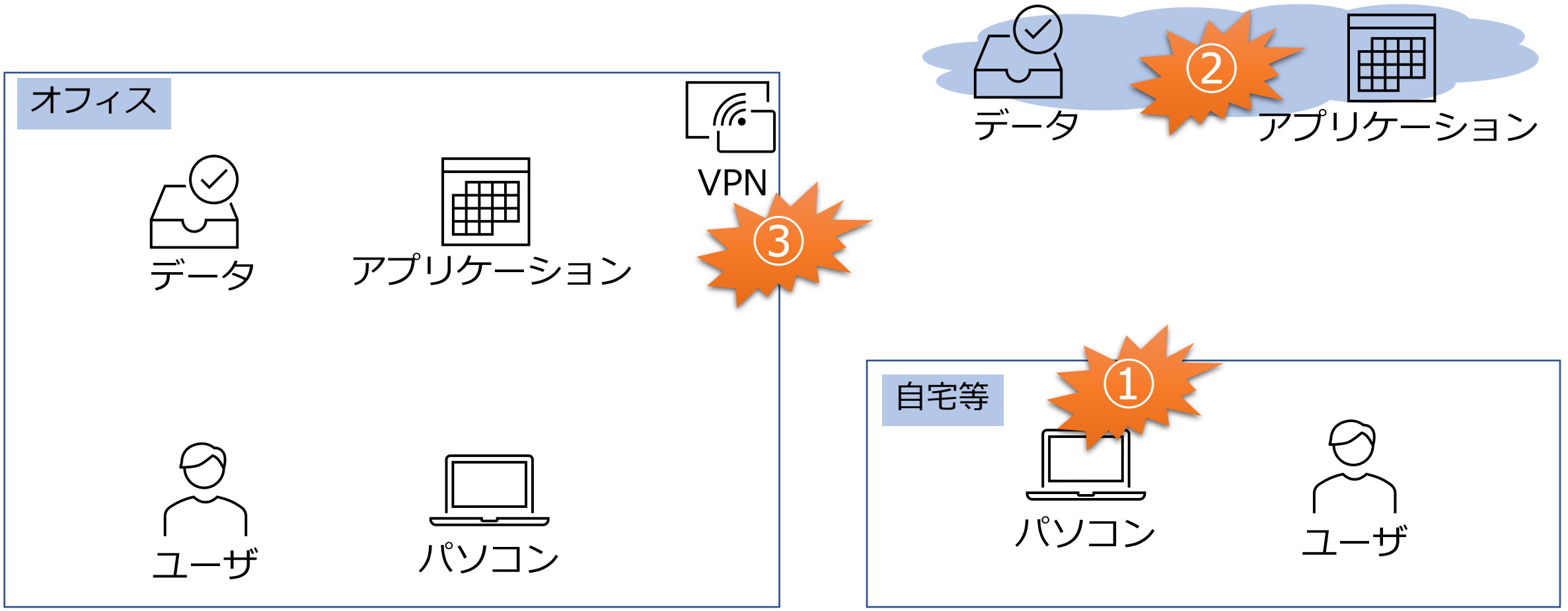
すべての資源がオフィス（＋データセンター）にある
出社することが前提のシステム

現在のIT環境



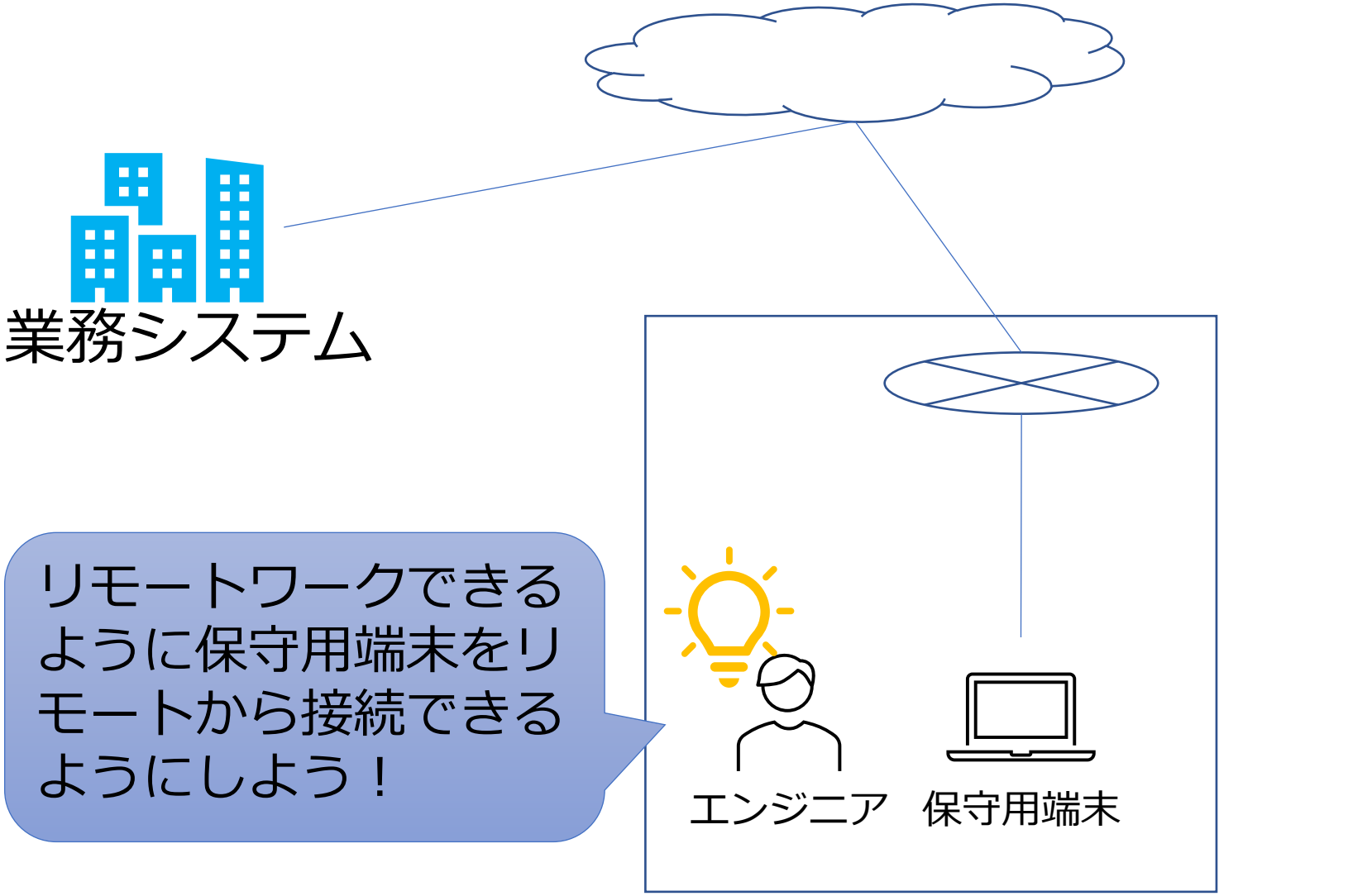
オフィス以外にクラウド側にもデータやアプリケーションがある
自宅等のリモート環境からも仕事をする形態に変わっている

見直してほしいポイント



①リモート接続端末のインシデント

運用委託事業者の作業ミスによる事件



発注側の視点

運用委託事業者がケシカラン
エンジニアの教育がなってない
貴社エンジニアのレベルはどうなってるんだ？

それで済ませる問題だろうか？

受注側の視点

毎年下ばらえる運用委託費

社員

当日のお楽しみ

い

あれこれ求められる書類、書類、書類

この契約、継続する？？

②クラウド環境のインシデント

アクセス権の設定ミス

クラウドサービス（主にSaaS）を使うときのアクセス権の
設定ミスから情報漏えいが発生

コロナ陽性者の個人情報9500人分が流出　クラウドのアクセス権を誤って公開状態に　福岡県が謝罪

2021年01月06日 19時58分 公開　[安田晴香，ITmedia]

印刷　401　Share　B!　37

福岡県は1月6日、県が管理していた新型コロナウイルス感染症の陽性者9500人分の氏名、住所などの個人情報がクラウドサービス上で外部から閲覧できる状態だったと発表した。県は「誠に申し訳ない」と謝罪し、再発防止に努めるとしている。

引用：
https://www.itmedia.co.jp/news/articles/2101/06/news130.html

Trelloの個人情報流出について運営元が公式に説明　セキュリティ設定の定期的な見直しを呼びかけ

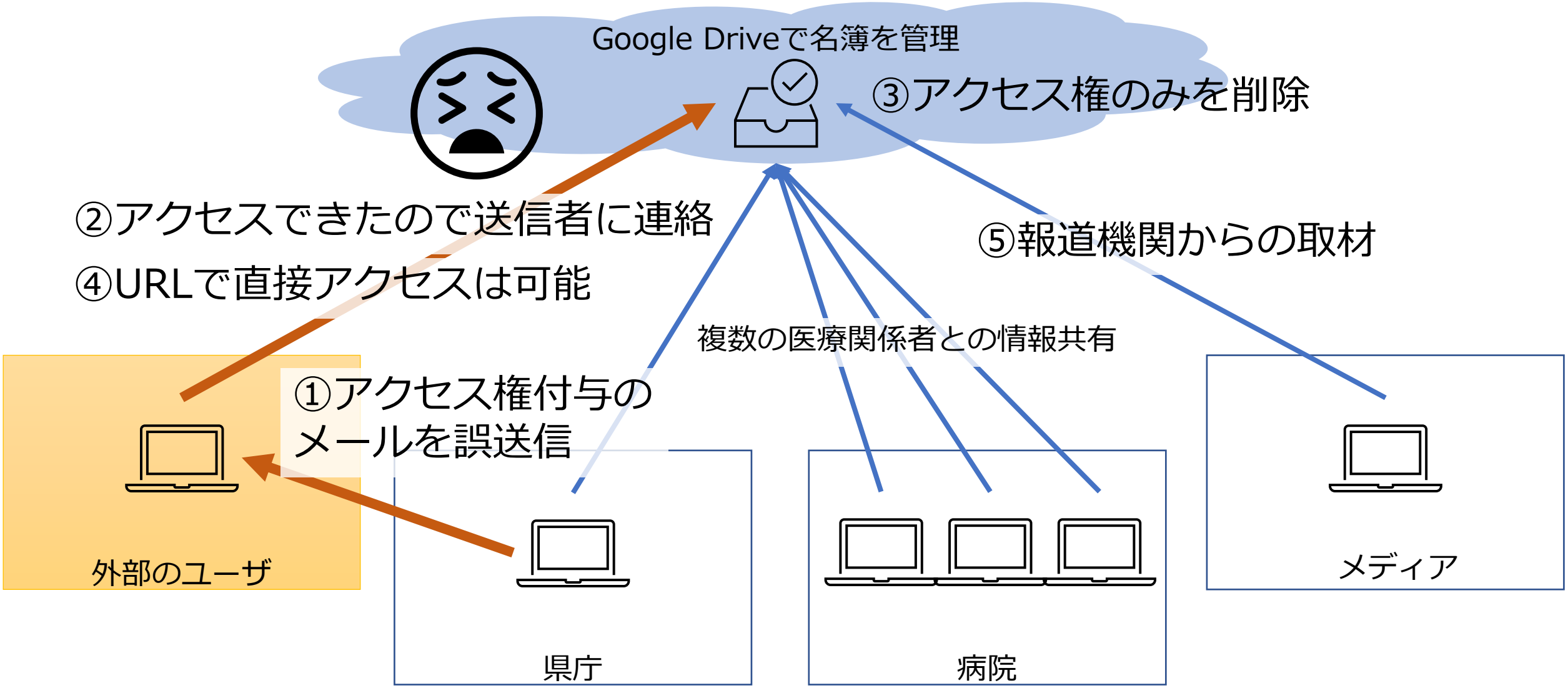
2021年04月09日 19時34分 公開　[ITmedia]

印刷　60　Share　B!　3　0

プロジェクト管理ツール「Trello」で個人情報がネットで公開されていた問題について、運営元のAtlassian（アトラシアン）は4月8日、新たな声明を発表した。同社はユーザーに対し、「Trello」のセキュリティ設定やボードの公開範囲を定期的に見直すことによって、ツールを安全に活用するようブログ上で呼びかけている。

引用：
https://www.itmedia.co.jp/business/articles/2104/09/news126.html

ある自治体で発生した事故



③インターネットに接続するアプライアンス

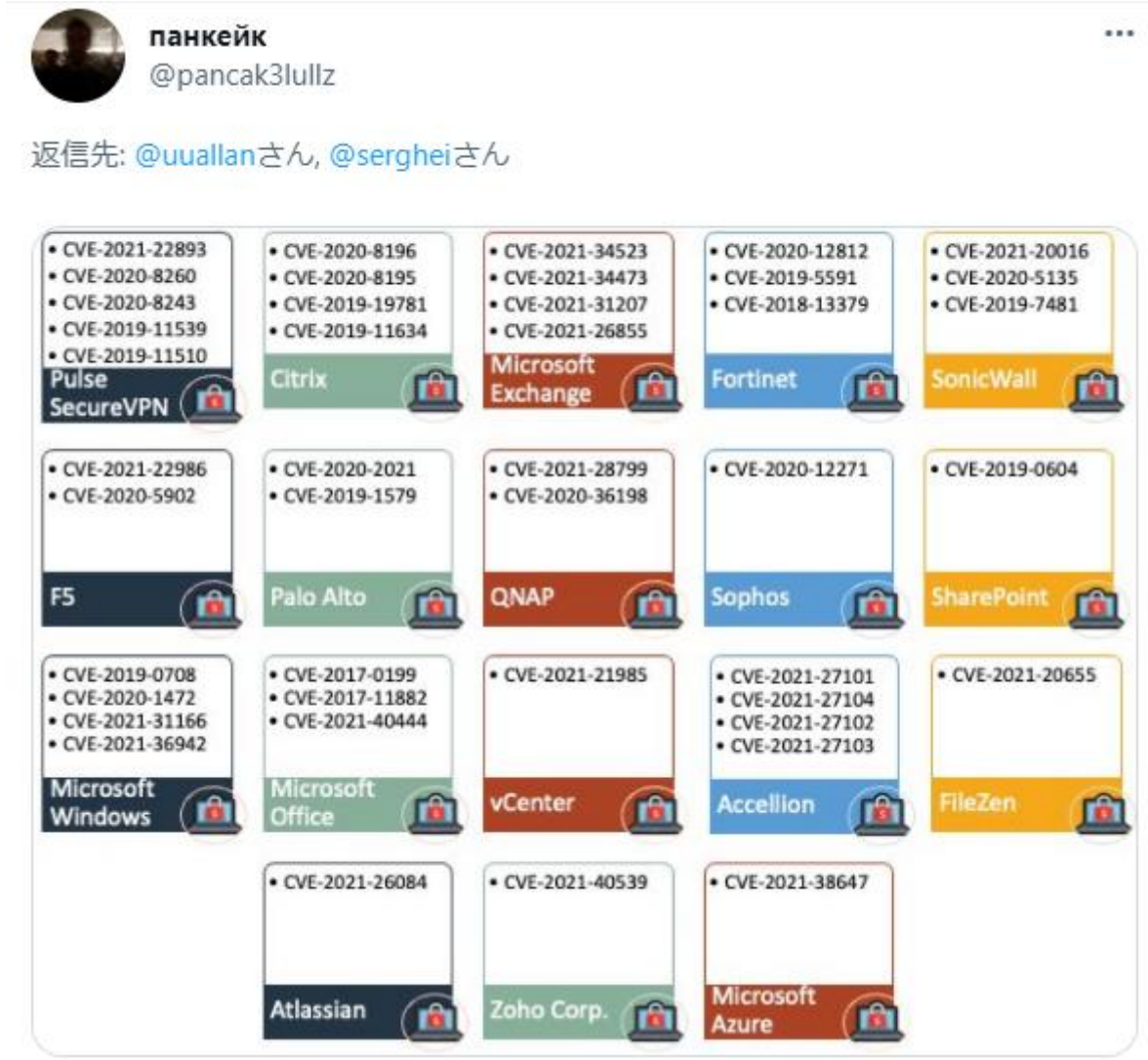
アプライアンスの脆弱性がターゲットに

VPN製品

Pulse Secure
Palo Alto Networks
Fortinet
Citrix

アップデートする運用が組まれていない
システムを止められない
アップデートできない
侵入後、内部に展開できる
アップデートしただけではダメ

ランサムウェア攻撃者が狙う脆弱性



引用：https://twitter.com/pancak3lullz/status/1438897285484720129

VPNの脆弱性

- カプコン
- 三菱電機
- 原子力規制庁
- などなど

ある組織に対する標的型メール訓練

「あなたのメールボックスがロックされています。
至急、ログインして解除設定を行ってください。」

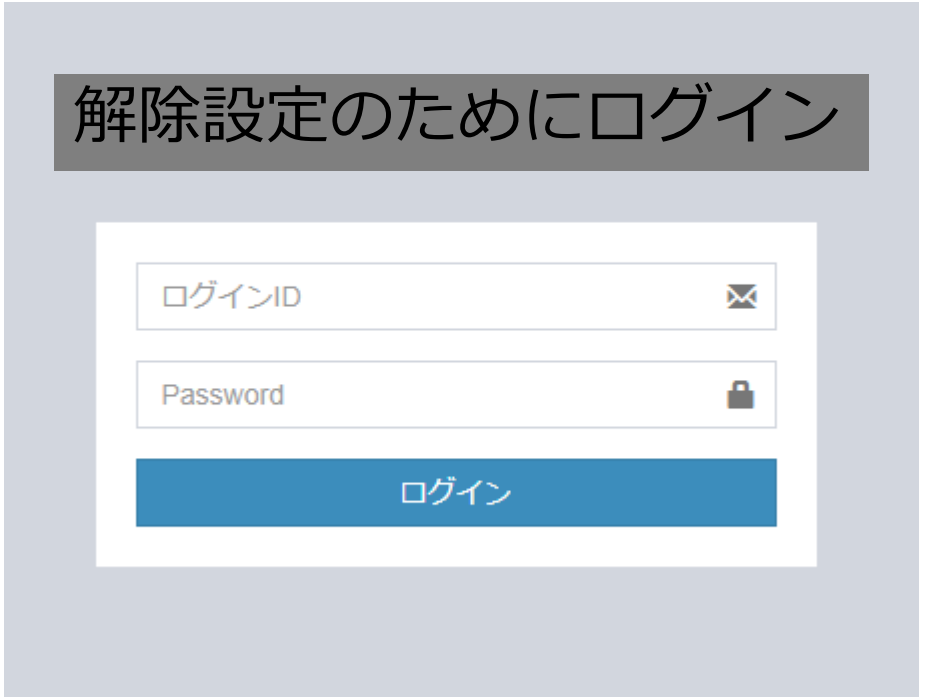
差出人：情報システム部
宛先　：あなたの名前
件名　：【緊急】メールボックス制限

情報システム部門の●●です。

あなたのメールボックスがロックされています。
至急、ログインして解除設定を行ってください。

解除方法はこちら
http://xxxxxxxx/fake.url

担当者：●●



ある組織に対する標的型メール訓練

メールのリンクを開いた人
　　全体の__割

アカウント情報を入力した人
　　リンクを開いた人の__割

ひとたび侵害されると

Active Directoryサーバを狙う

VPNの侵入後

ADサーバ等の重要なサーバが被害に

アッ
内部
「ネ
クラ

当日のお楽しみ

なぜこうなるのか？

原因

当日のお楽しみ を探しているから

まず考えること

事業として何をするのか？

事業としてどんな事故が起きるとマズイのか？

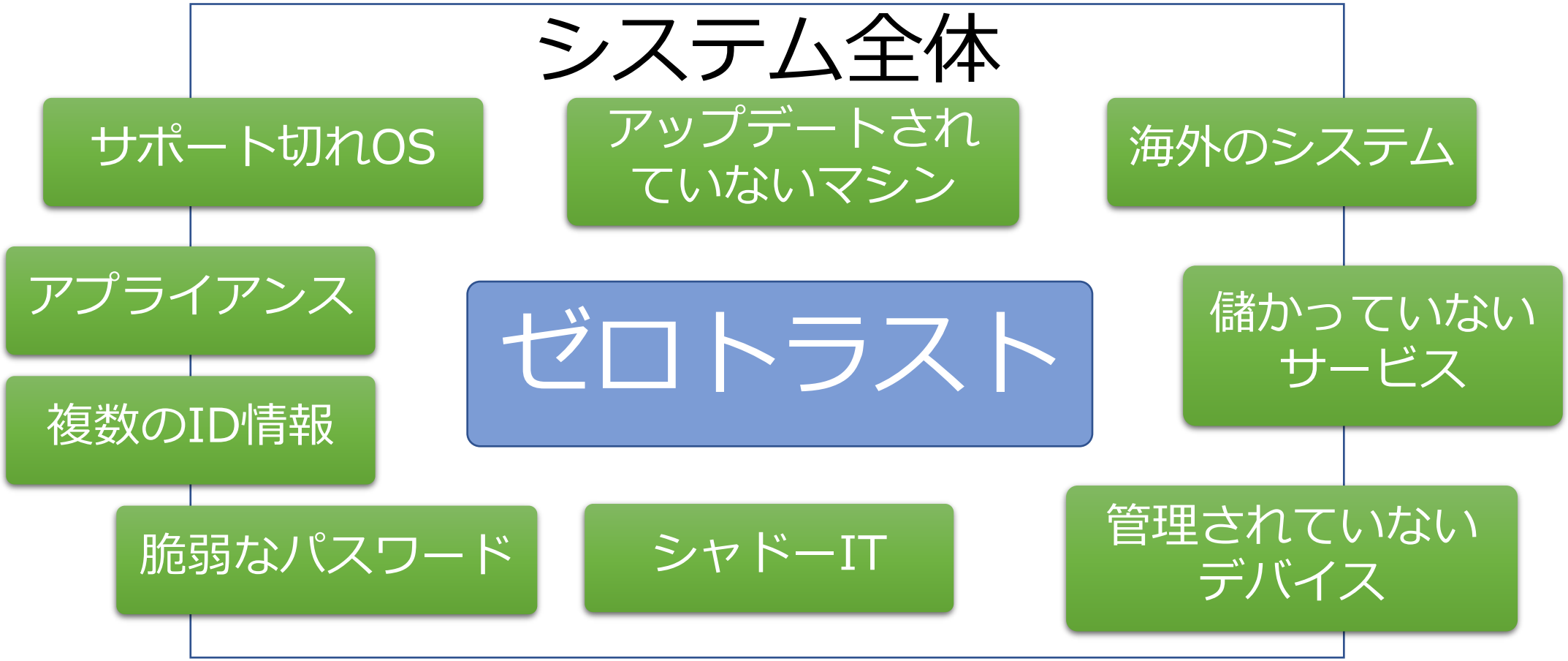
組織全体で守る意識が重要

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

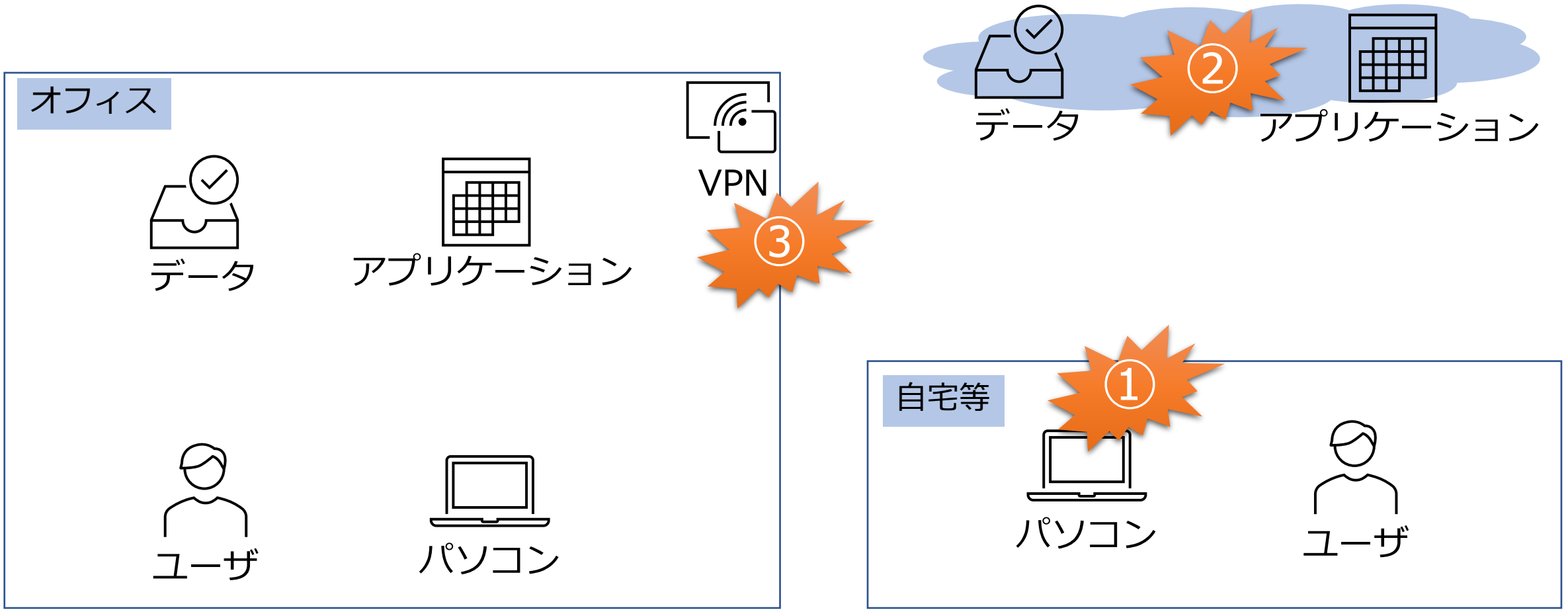
顧客

現実



ゼロトラストを流行りのキーワードに代えても同じ
ケアされていない領域をどのように守っていくか

改めて見直してほしいところ



コロナ禍になって

イベント、セミナーのオンライン化

↓

どこからでも参加できる

情報を手に入れやすい時代になった

セキュリティの情報源

内閣サイバーセキュリティセンター
https://www.nisc.go.jp/

JPCERT/CC
https://www.jpcert.or.jp/

IPA セキュリティセンター
https://www.ipa.go.jp/security/index.html

困ったときに相談する人

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

皆さんに実施してほしいこと

ア

ノ

ノ

当日のお楽しみ

最後に

強固な計画よりも**柔軟な変化**を必要とする。
役割分担よりも**連携と協働**を必要とする。

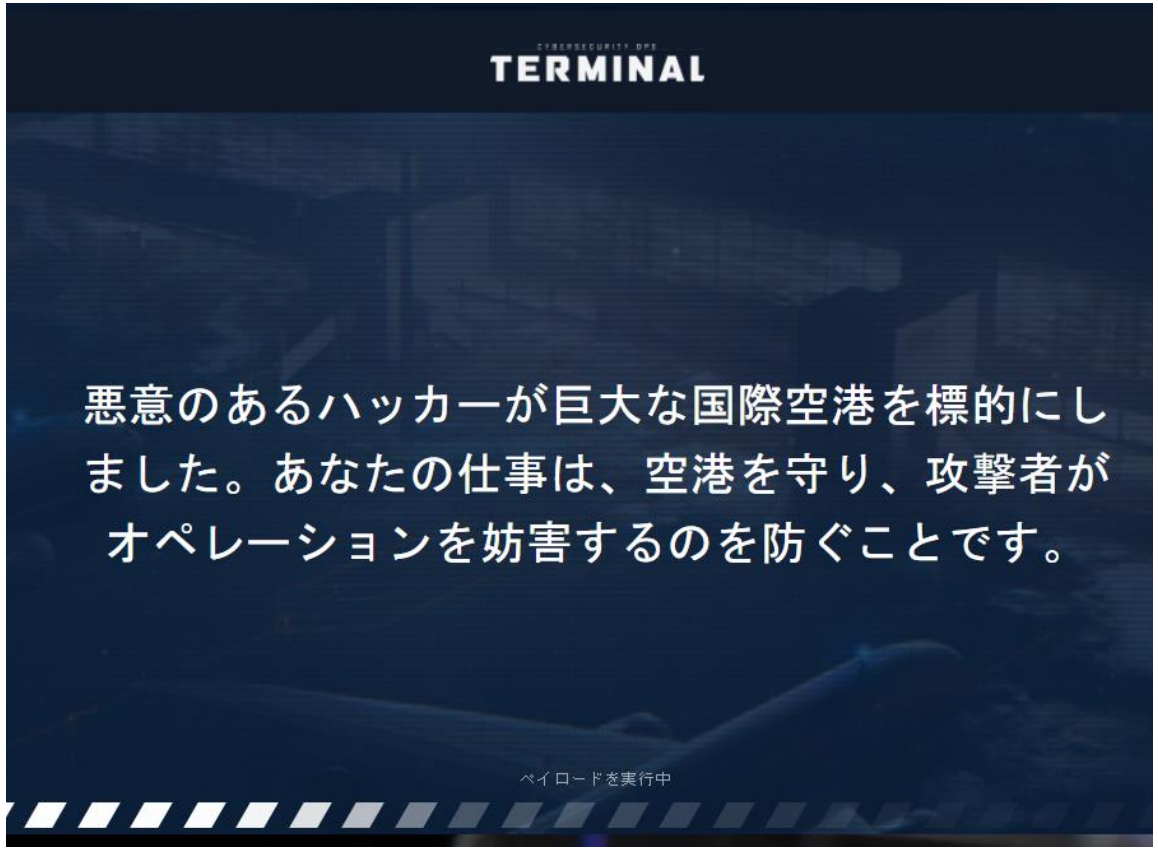
本講演に関するお問い合わせ
株式会社川口設計
代表取締役
川口洋
kawa @ sec-k.co.jp

【参考】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/

ブラウザでできるインシデント体験ゲーム



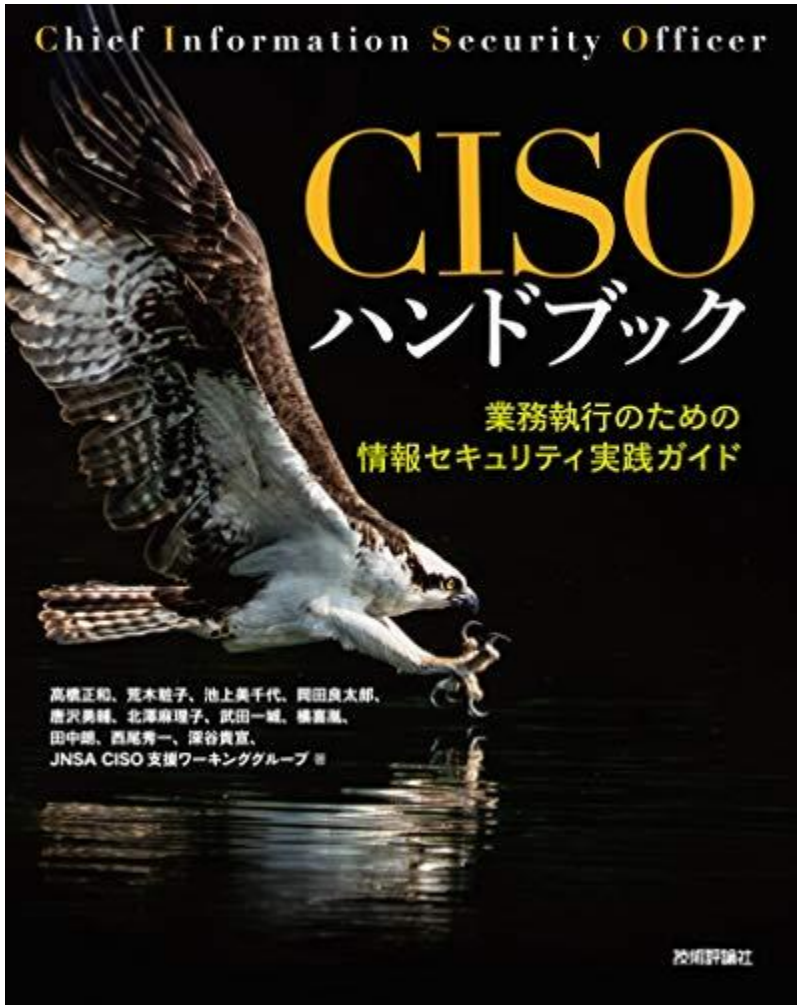
IBM社が公開しているサイバー攻撃シミュレーションゲーム

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/

要チェック



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。

要チェック

元ヤフー社長　現東京都副都知事　宮坂さん
「重大事故の時にどうするか？」
https://note.com/mmiya/n/n746eb2e36f81

リーダーの仕事はいっぱいあるけどなかでも大きな仕事の一つは重大事故の発生の時の陣頭指揮。平時は部下で回せるようにするのがマネジメントだけど、危機の時まで部下にまかせるわけにはいかない。お恥ずかしながらヤフー在職中の22年で何度か重大事故を起こし関係者の人に多大な迷惑をかけてしまった。その度にその陣頭指揮をとった。結果的にヤフーのなかでもっとも深刻な事故対策をやった人の一人じゃなかろうか。そのなかからノウハウ的なものがたまってきたものを部下にメモしておくってあげたものを彼は覚えていてくれたらしい。

彼いわく危機対応の時にすっごく役にたって指針になったといってくれて送ってくれた。ひょっとしたら他の人にも参考になるかとおもって（若干訂正してますが）ここに残しておきます。

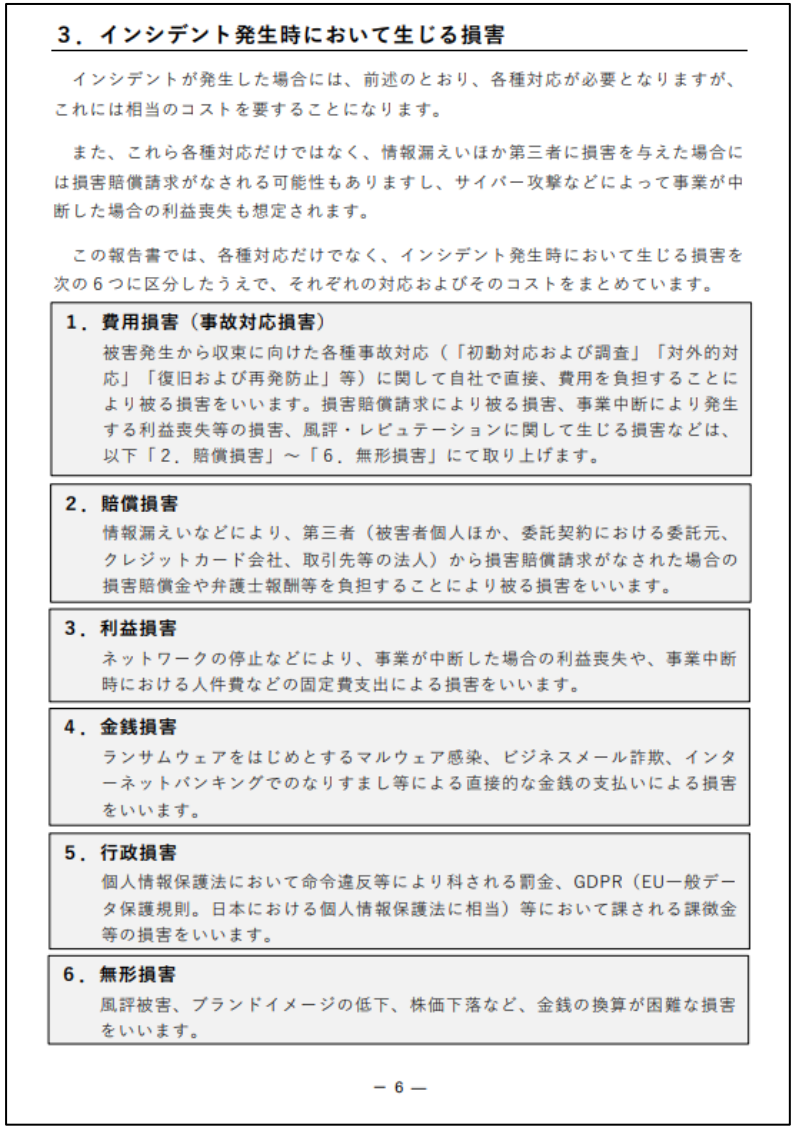
重大事故の時にやったほうがいいこと10個
（続きはWEBで）

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？
https://note.com/mmiya/n/n746eb2e36f81

【参考】インシデント損害額調査レポート



3．インシデント発生時において生じる損害

インシデントが発生した場合には、前述のとおり、各種対応が必要となりますが、これには相当のコストを要することになります。

また、これら各種対応だけではなく、情報漏えいほか第三者に損害を与えた場合には損害賠償請求がなされる可能性もありますし、サイバー攻撃などによって事業が中断した場合の利益喪失も想定されます。

この報告書では、各種対応だけでなく、インシデント発生時において生じる損害を次の６つに区分したうえで、それぞれの対応およびそのコストをまとめています。

１．費用損害（事故対応損害）
被害発生から収束に向けた各種事故対応（「初動対応および調査」「対外的対応」「復旧および再発防止」等）に関して自社で直接、費用を負担することにより被る損害をいいます。損害賠償請求により被る損害、事業中断により発生する利益喪失等の損害、風評・レピュテーションに関して生じる損害などは、以下「２．賠償損害」～「６．無形損害」にて取り上げます。

２．賠償損害
情報漏えいなどにより、第三者（被害者個人ほか、委託契約における委託元、クレジットカード会社、取引先等の法人）から損害賠償請求がなされた場合の損害賠償金や弁護士報酬等を負担することにより被る損害をいいます。

３．利益損害
ネットワークの停止などにより、事業が中断した場合の利益喪失や、事業中断時における人件費などの固定費支出による損害をいいます。

４．金銭損害
ランサムウェアをはじめとするマルウェア感染、ビジネスメール詐欺、インターネットバンキングでのなりすまし等による直接的な金銭の支払いによる損害をいいます。

５．行政損害
個人情報保護法において命令違反等により科される罰金、GDPR（EU一般データ保護規則。日本における個人情報保護法に相当）等において課される課徴金等の損害をいいます。

６．無形損害
風評被害、ブランドイメージの低下、株価下落など、金銭の換算が困難な損害をいいます。

－ 6 －

JNSA(日本ネットワークセキュリティ協会) インシデント被害調査ワーキンググループ
インシデント損害額調査レポート　2021年版
https://www.jnsa.org/result/incidentdamage/2021.html

この報告書は、これらの点を踏まえ、経営者、特に中小企業の経営者の方に向けて、インシデント発生時の具体的な対応、そのアウトソーシング先、対応等によって実際に生じるコスト（損害額・損失額）を各事業者への調査により明らかにして、これをお伝えし、そのうえで事前対策・事後対応の両面を踏まえたセキュリティ対策の強化を図っていただくことを目的として作成しています。