YouTuberと学ぶ！

【DX入門】インターネットのリスクとセキュリティ

ITすきま教室　渡辺さき

自己紹介

株式会社すきまデザイン 代表取締役
ITすきま教室 編集長

渡辺さき

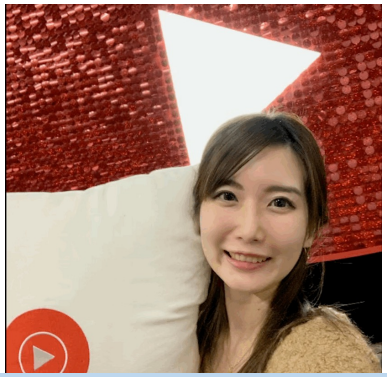
2015年
- 東京都立大・理学部化学科卒業

2015年～
- 株式会社リクルート入社 / WEBマーケティング職

2019年～
- 在職中にYouTube発信を開始

2021年
- 1週間で基礎が身につくITパスポート出版

2021年～
- 独立・ITすきま教室編集長、情報学講師



チャンネル登録7.8万人!
ITすきま教室

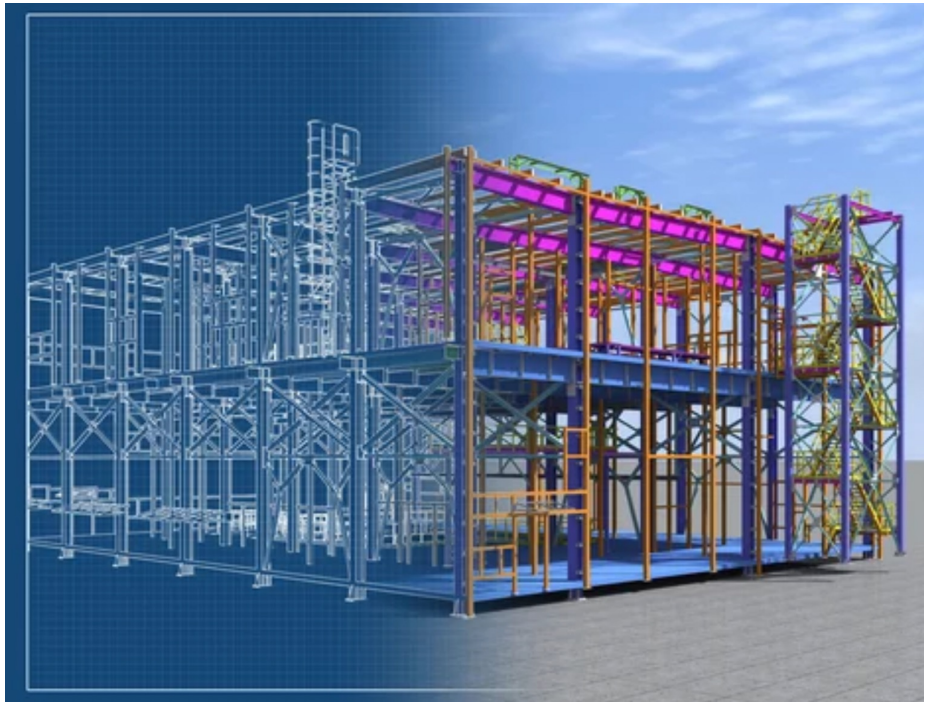
本日のゴール

- DXトレンドから、情報セキュリティの事例を学び、明日からの業務に活かす◎

建築・土木業界で進行するDX

- 建設業界：2024年問題に向けて、BIM導入・推進が進む。（国土交通省）
- 不動産の維持管理の業務でも、DX推進の流れが目前に。

▼BIM(Building Information Modeling)



▼日本建築積算協会

不動産ID

- データ駆動型社会に向けた情報の整備・連携・オープン化の一貫。
- 住所の表記ゆれや同一住所・地番に複数の建物がある場合でも、一義的に不動産を特定できるようにする。

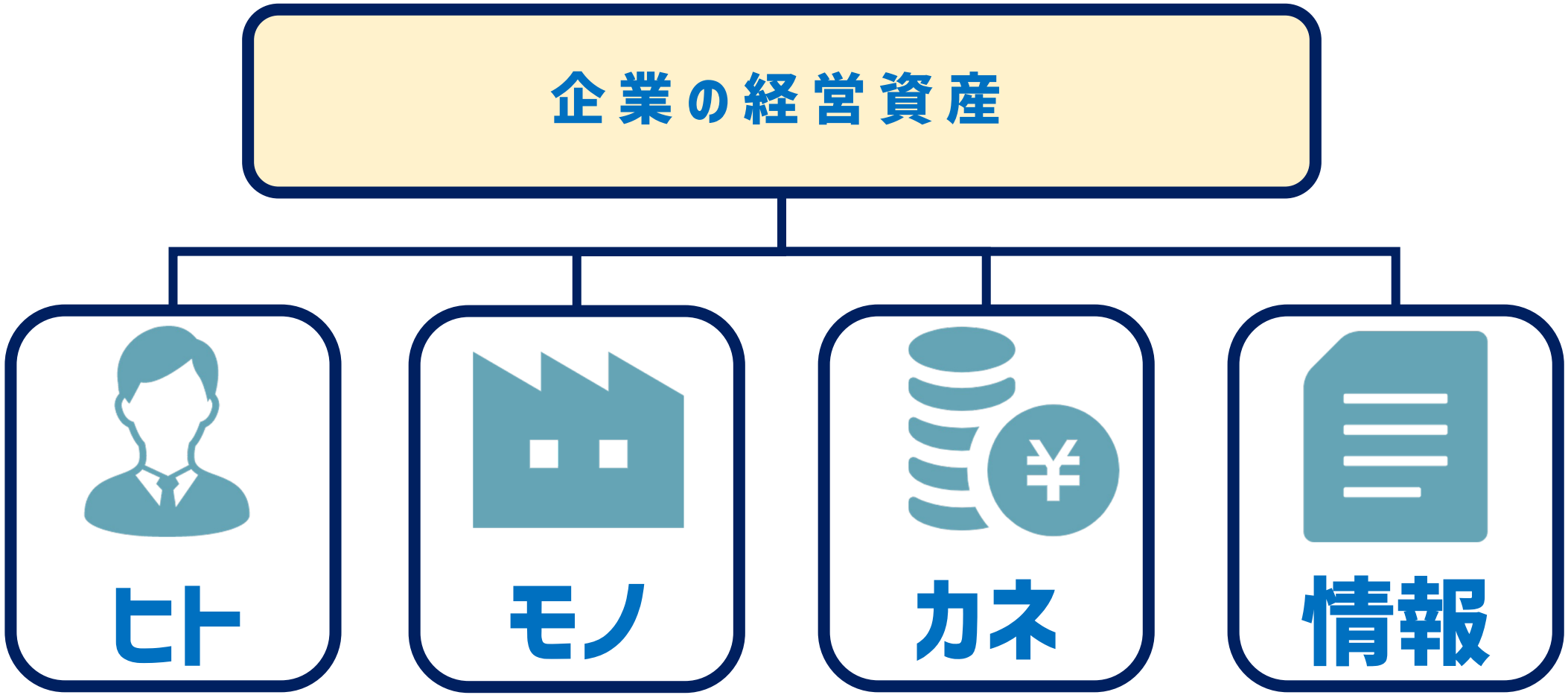
（表）不動産 ID の基本ルール

	IDを付す単位		使用する不動産番号の対象	No.	IDのルール
土地	筆ごと		土地	①	不動産番号(13桁)-0000(４桁)
建物（戸建て）	建物全体		建物	②	不動産番号(13桁)-0000(４桁)
非区分建物	〔商業用〕フロアごと		建物	③	不動産番号(13桁)-階層コード(2桁)・階数(2桁)
	〔居住用〕部屋ごと			④	不動産番号(13桁)-部屋番号(４桁)
	建物全体			⑤	不動産番号(13桁)-0000(４桁)
区分所有建物	〔商業用〕	専有部分ごと	専有部分	⑥	不動産番号(13桁)-0000(４桁)
		フロアごと		⑦	不動産番号(13桁)-階層コード(2桁)・階数(2桁)
	〔居住用〕	部屋ごと	専有部分(=1部屋の場合)	⑧	不動産番号(13桁)-0000(４桁) ※一般的な分譲マンションの各部屋はこの類型に該当
			専有部分(=複数部屋の場合)	⑨	不動産番号(13桁)-部屋番号(４桁)
	建物全体		建物が建つ土地	⑩	不動産番号(13桁)-建物を表す符号(４桁)

不動産取引時の必要情報が不動産IDに集約できるため、契約までの期間短縮やコスト削減が可能に。

「情報」セキュリティ とは

- 経営資産である ヒト・モノ・カネ・情報。このうち、**情報**の部分が **I**nformation **T**echnology.



情報資産とは

- パソコンで管理されているデータだけでなく、ビジネスのあらゆる情報が資産となる。

ビジネスのアイデア，営業秘密

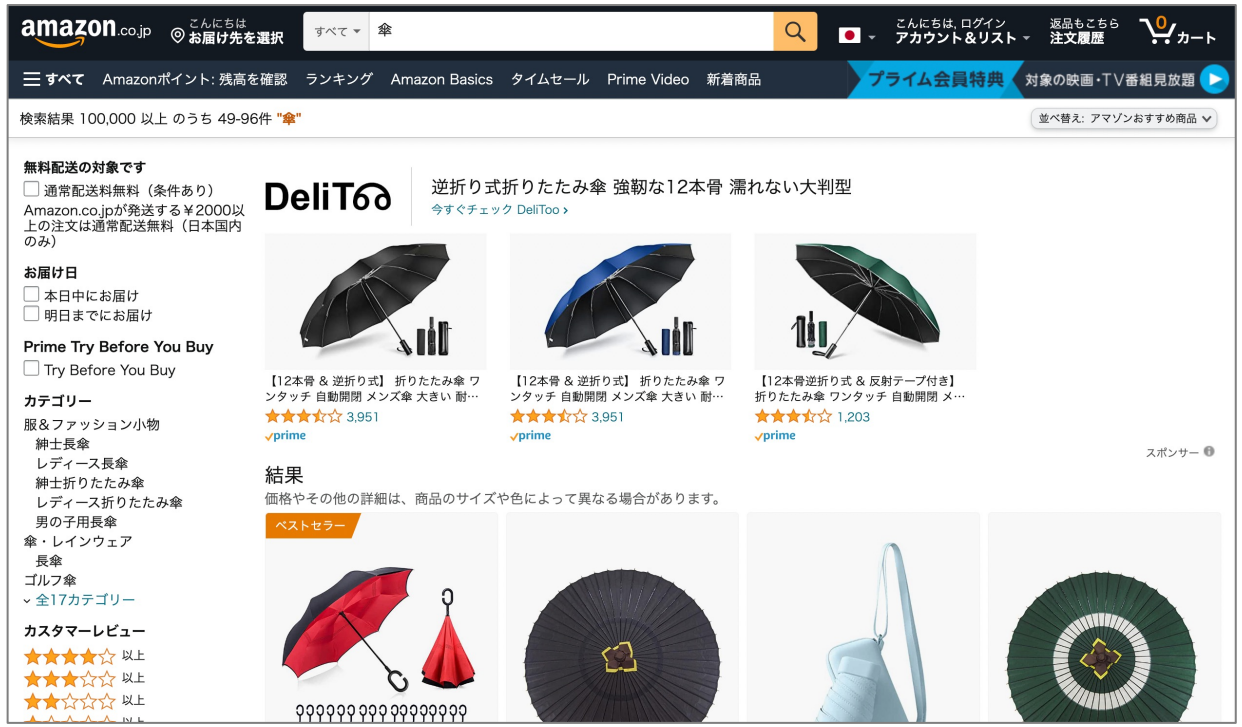
顧客情報

従業員情報

会計・法的文書

情報資産へのリスク

- 盗聴・改ざん・拒否 の具体的被害。



【盗聴・不正アクセス】

通信から情報をぬきとる

【改ざん】

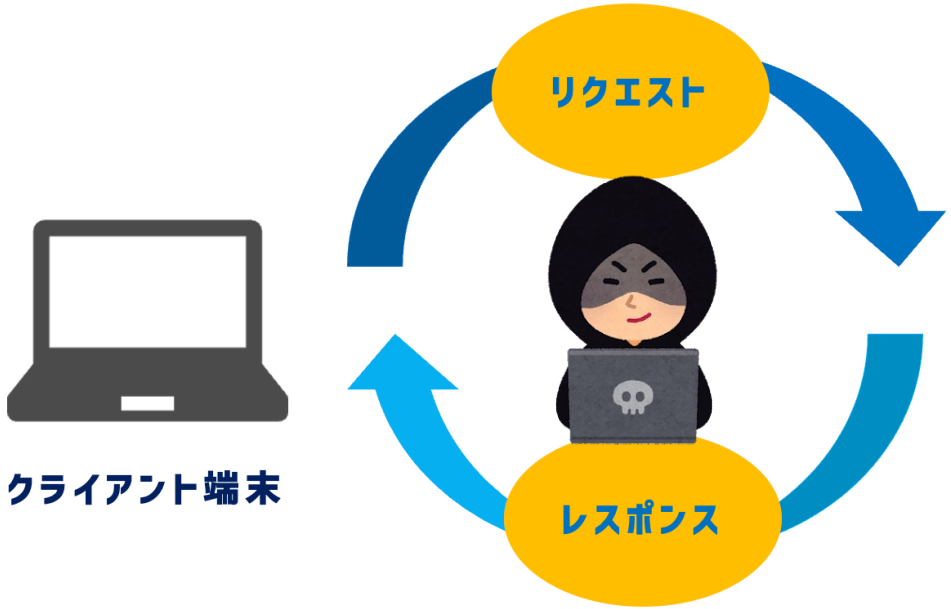
WEBサイトなど、本来とは異なる状態とする

【破壊・拒否】

正常なユーザーをアクセスさせない

情報資産へのリスク

- 盗聴・改ざん・拒否 の具体的被害。



【盗聴・不正アクセス】

通信から情報をぬきとる

【改ざん】

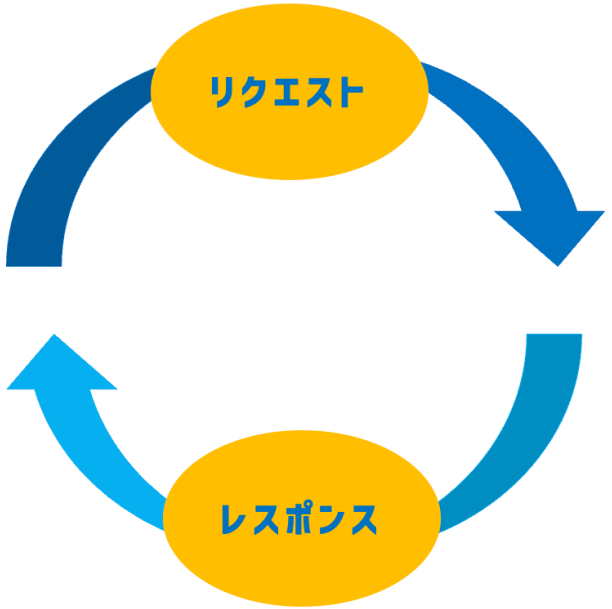
WEBサイトなど、本来とは異なる状態とする

【破壊・拒否】

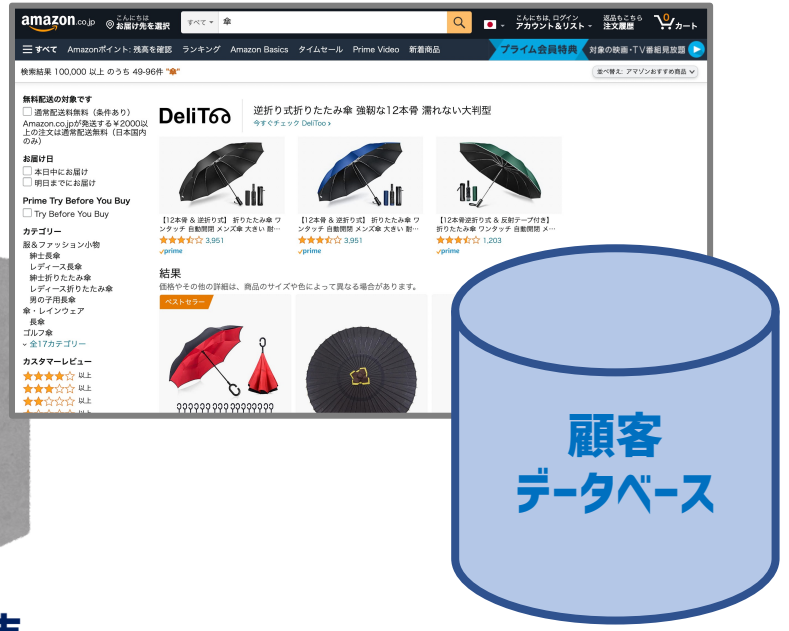
正常なユーザーをアクセスさせない

情報資産へのリスク

- 盗聴・改ざん・拒否 の具体的被害。



サーバー端末



【盗聴・不正アクセス】

通信から情報をぬきとる

【改ざん】

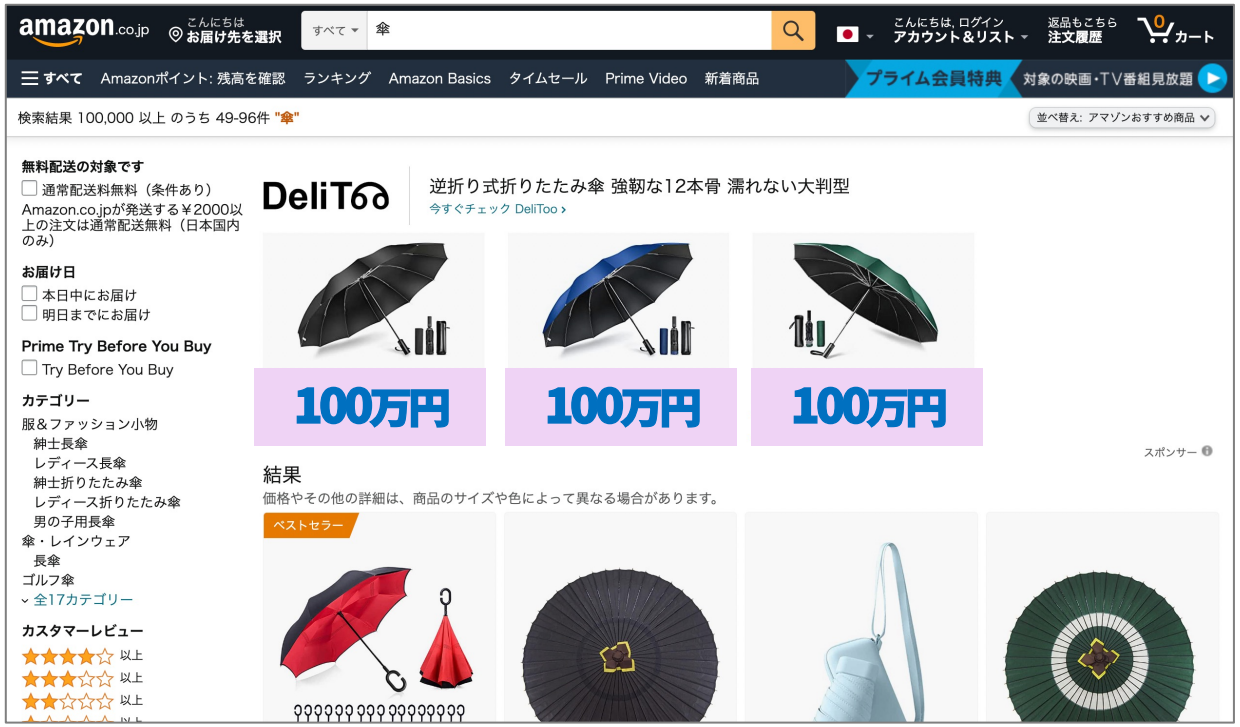
WEBサイトなど、本来とは異なる状態とする

【破壊・拒否】

正常なユーザーをアクセスさせない

情報資産へのリスク

- 盗聴・改ざん・拒否 の具体的被害。



金額を
書き変えてやる！

【盗聴・不正アクセス】

通信から情報をぬきとる

【改ざん】

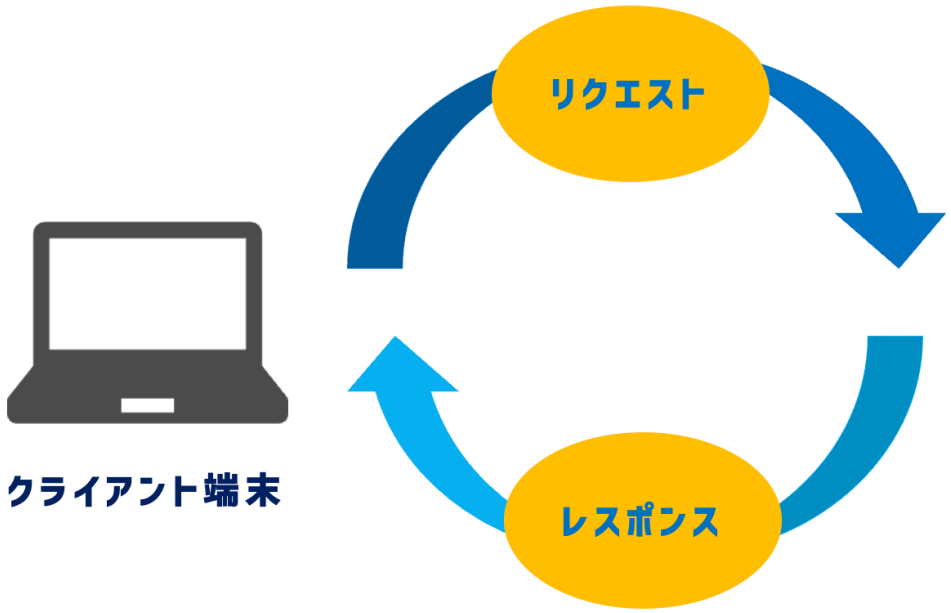
WEBサイトなど、本来とは
異なる状態とする

【破壊・拒否】

正常なユーザーをアクセスさせない

情報資産へのリスク

- 盗聴・改ざん・拒否 の具体的被害。



【盗聴・不正アクセス】

通信から情報をぬきとる

【改ざん】

WEBサイトなど、本来とは異なる状態とする

【破壊・拒否】

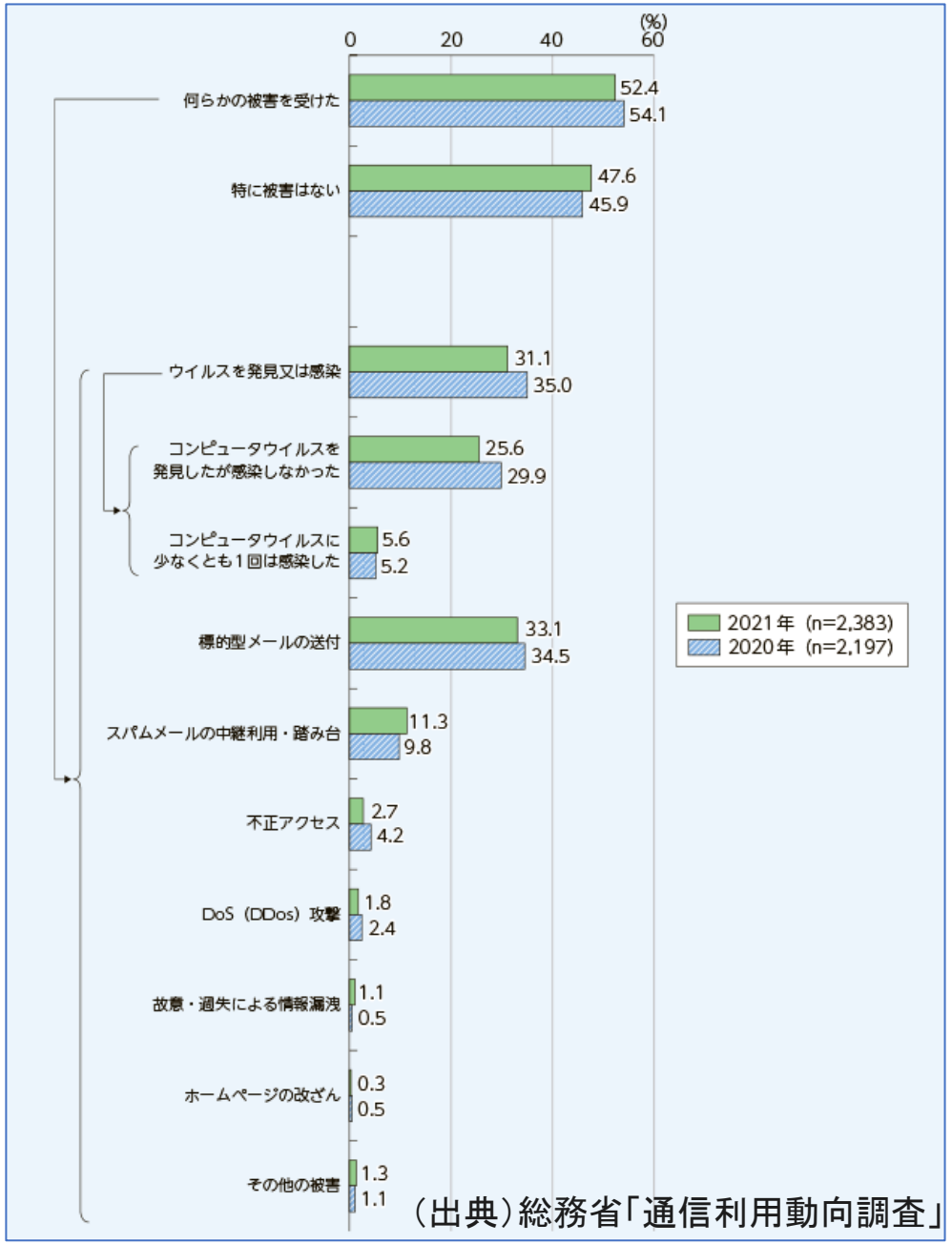
正常なユーザーをアクセスさせない

本当に、自分の身にも起きるのか…？

いやいや、そんなの映画の中だけの話でしょ～

セキュリティ侵害の被害

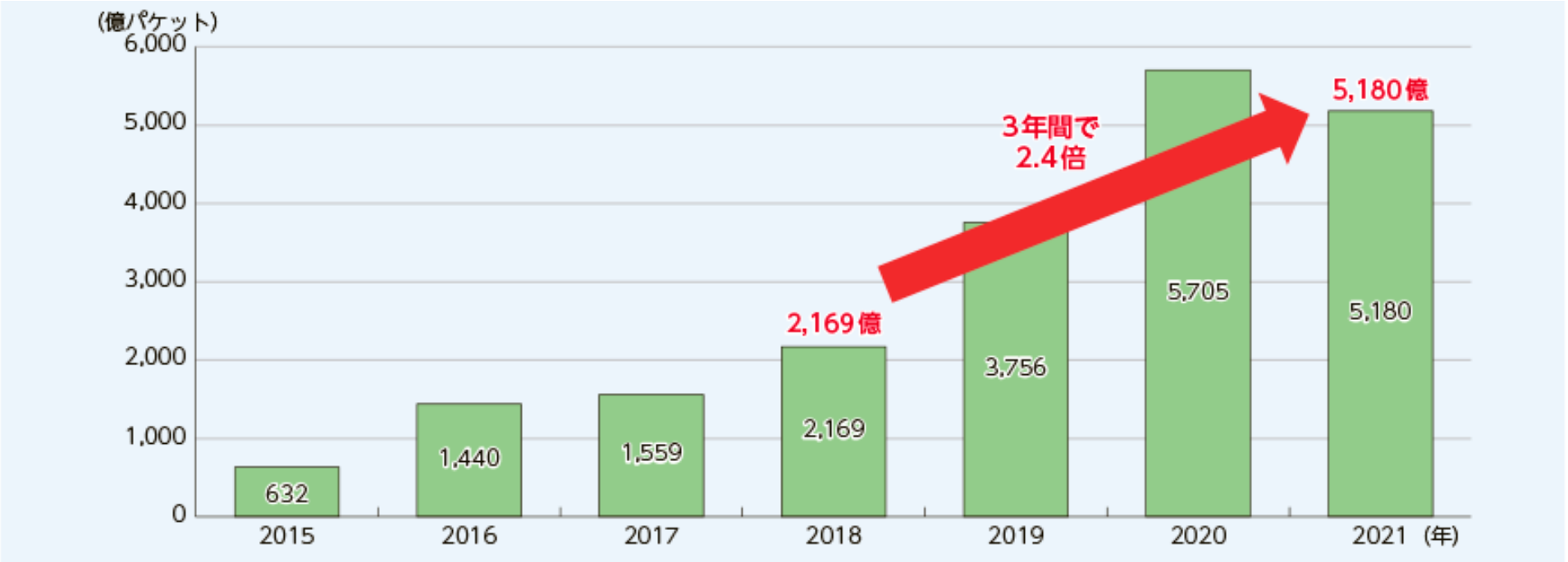
- 企業における
  情報通信ネットワーク利用の際のセキュリティ侵害。
- 例年、半数以上が被害を受けている。



（出典）総務省「通信利用動向調査」

サイバー攻撃自体も、増加傾向にある

- サイバー攻撃関連の通信数は、コロナにより在宅・オンライン化が進んだ時期に急速に増加している。（令和４年版・総務省サイバーセキュリティレポートより）



NICTERにおけるサイバー攻撃関連の通信数の推移 | 総務省・制作白書掲載番号（3-7-2-1）
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/html/nf307000.html

情報資産・脅威の種類

- 人為的脅威は、システムで一定レベルのコントロール。

◆人的脅威

人による誤操作や、
紛失・不正利用・怠慢など、
「人」が原因となる脅威。

◆物理的脅威

地震・洪水・火災・停電などの天災、故障や悪意ある人物による破壊行為など
システムを動かす機器が物理的に動作できなくなる脅威。

◆技術的脅威

ネットワーク上の脆弱性（弱点）をついた不正アクセスや、
コンピューターウイルスなど
悪意ある第三者による攻撃など
技術的な手段による脅威。

何が起きても技術で守れる体制

- 人為的な脅威は「気をつけよう」だけで対策を怠らない。

- 万が一、脅威にさらされても
更に技術的な対策に寄って、防げることが理想的。

【例】
→端末が盗まれても、ID/PASS管理
→生体認証を導入する
→端末のローカルで情報保持しない
（VPNや仮想デスクトップなど）

尼崎市民“46万人”個人情報USB紛失…酒に酔い路上で3時間近く寝入る

2022/6/23(木) 16:03 配信 70

日テレNEWS

兵庫県尼崎市は、全市民46万人分の住民基本台帳の情報が入っているUSBメモリーを紛失したと発表しました。

Yahoo!JAPAN ニュースより

情報資産・脅威の種類

- 人為的脅威は、システムで一定レベルのコントロール。

◆人的脅威

人による誤操作や、
紛失・不正利用・怠慢など、
「人」が原因となる脅威。

→技術的対策

◆物理的脅威

地震・洪水・火災・停電などの天災、故障や悪意ある人物による破壊行為など
システムを動かす機器が物理的に動作できなくなる脅威。

→ファシリティマネジメント

◆技術的脅威

ネットワーク上の脆弱性（弱点）をついた不正アクセスや、
コンピューターウイルスなど
悪意ある第三者による攻撃など
技術的な手段による脅威。

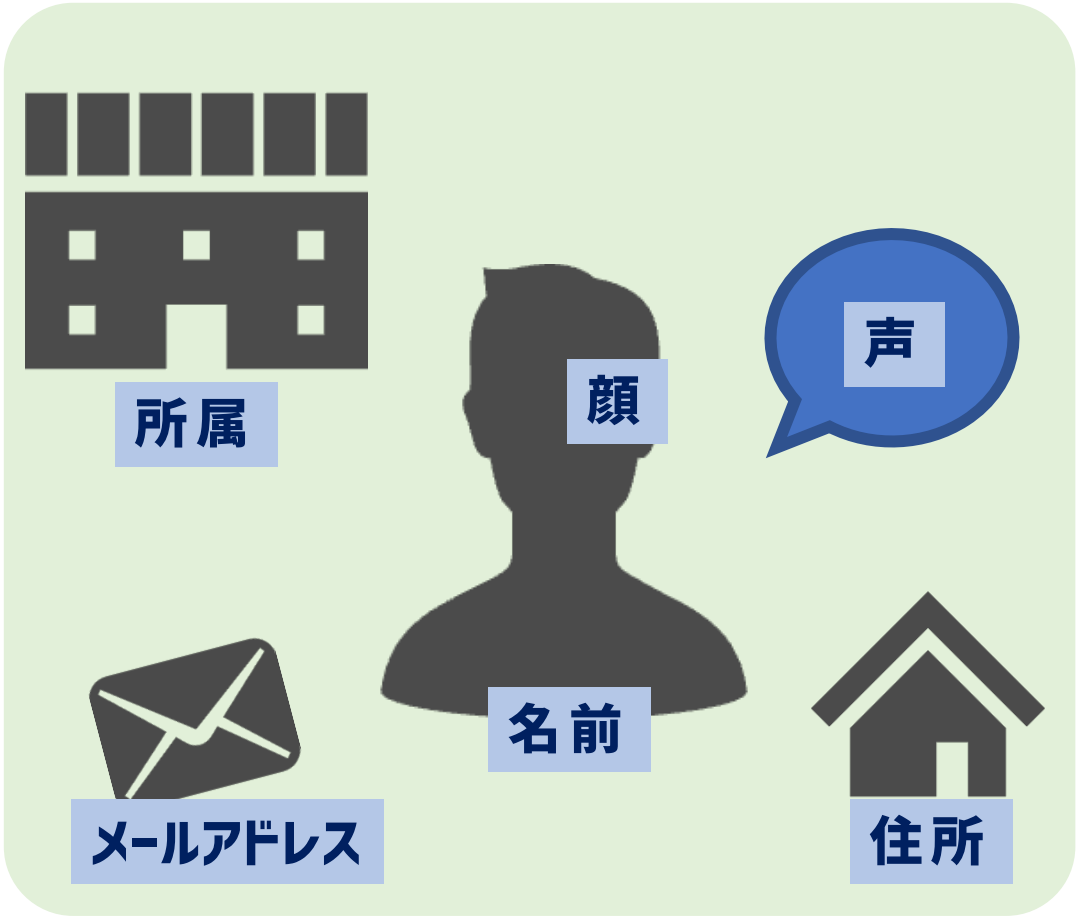
→技術的対策

技術的脅威の事例①

- 無料占いをよそおった、個人情報取得。詐欺被害等に悪用される。

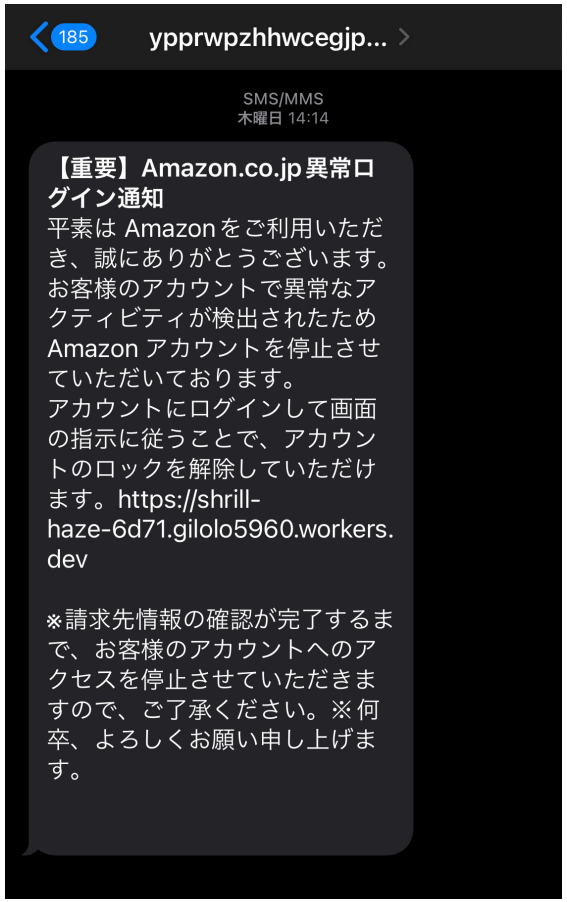
情報提供している気にさせない手法

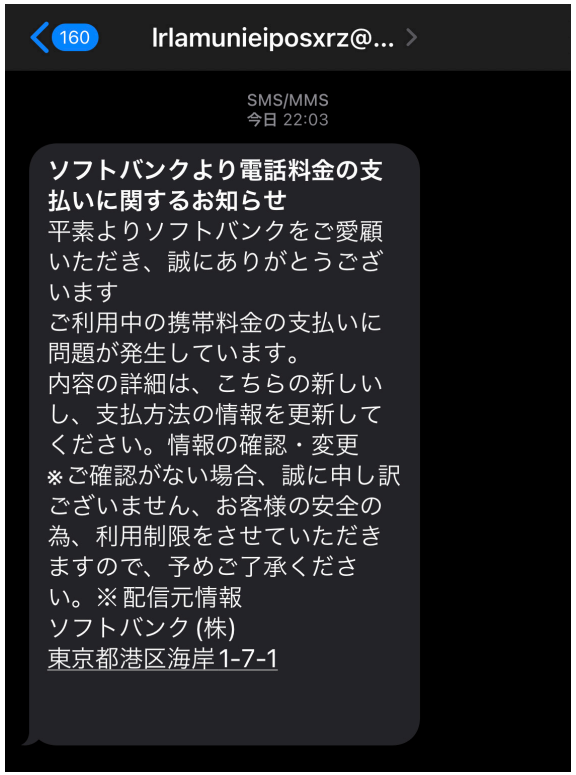
- 個人情報を疑いなく提供させる仕組み。



技術的脅威の事例②

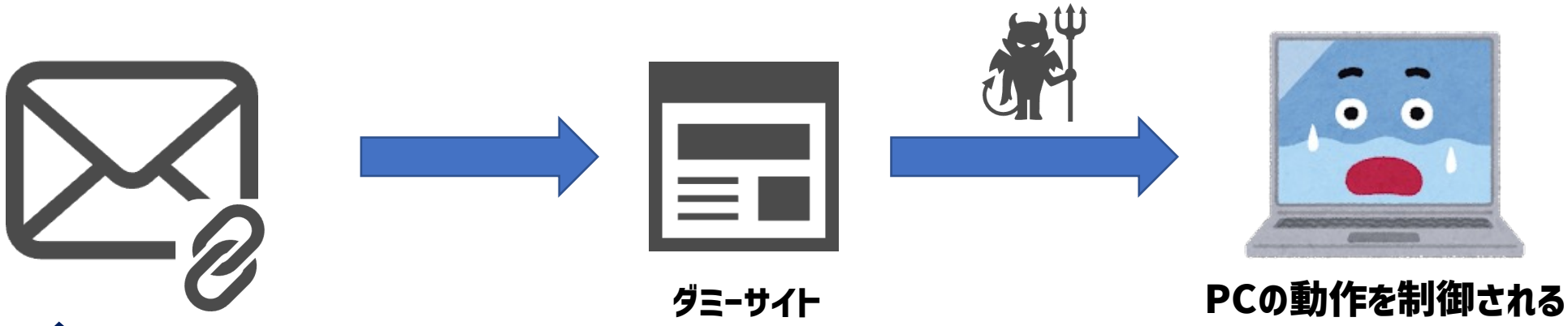
- なりすましメール。企業や行政（国税局や水道局）をよそおった事例。





リンクを開くと、何が起こる？

- ダミーサイトが開かれ、悪意あるスクリプトが起動。PCの動作制御につながる。



被害の経路は様々…

メール添付ファイル　　SNS　DM　など

技術的脅威の事例③

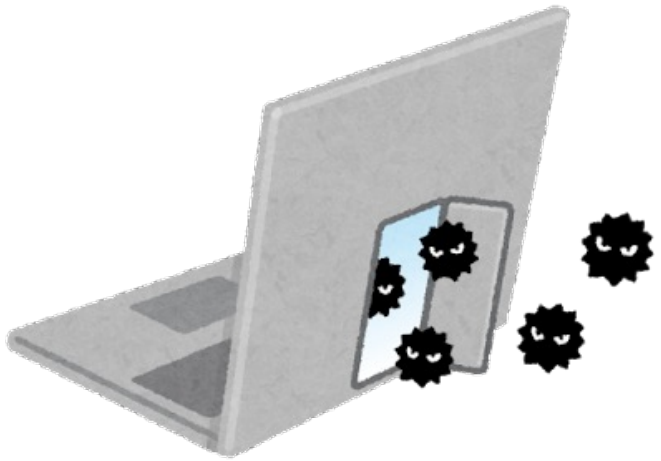
- 一見悪意のない、フリーのウイルス対策ソフトをダウンロード。
  身代金の請求や、情報の改ざん・盗聴など、様々なトラブルを引き起こす。

ネットサーフィンで見つけた、無料の
ウイルス対策ソフトを発見！

トロイの木馬
一見悪意のない ソフトウェアに見せかけて
コンピューターに侵入する

不正アクセスの温床に

- 感染源をすぐに認識させないよう、**バックドア**を作る。 盗聴や改ざんを容易にする。



バックドア
感染したコンピューターに攻撃者が自由に
アクセスできるバックドアをつくるケース

◆PC端末内の情報が盗聴される。

◆Wi-Fiを経由して、他の端末にも
同様のウイルスを仕込む。

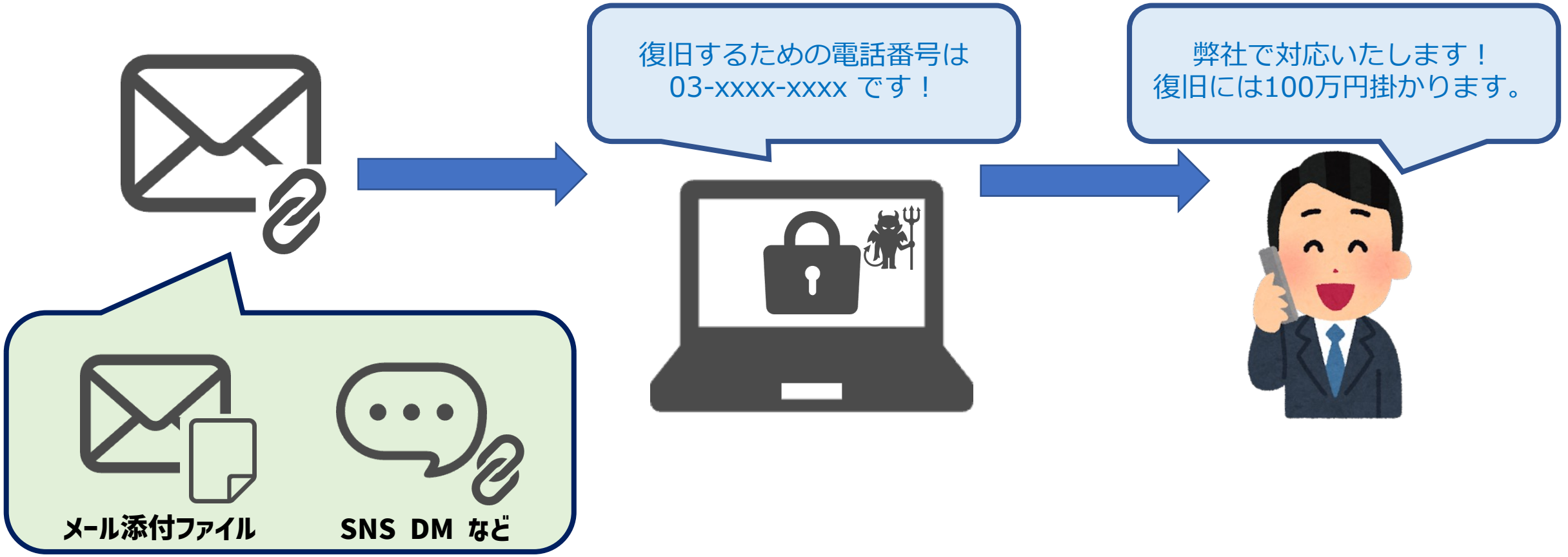
◆端末を操作し、メール経由で
別の被害者を生み出すリスクがある。

バックドアのリスクがあるアプリ

- **【海外】キーボードカスタムアプリ**
- スマホのキーボードビジュアルをカスタムデザインするためのアプリ。
- 無料で利用できるが、一部ではキーボードのトラッキングにより
  情報盗聴リスクがあると言われている。　※表向きには、キーワードマーケティングが目的

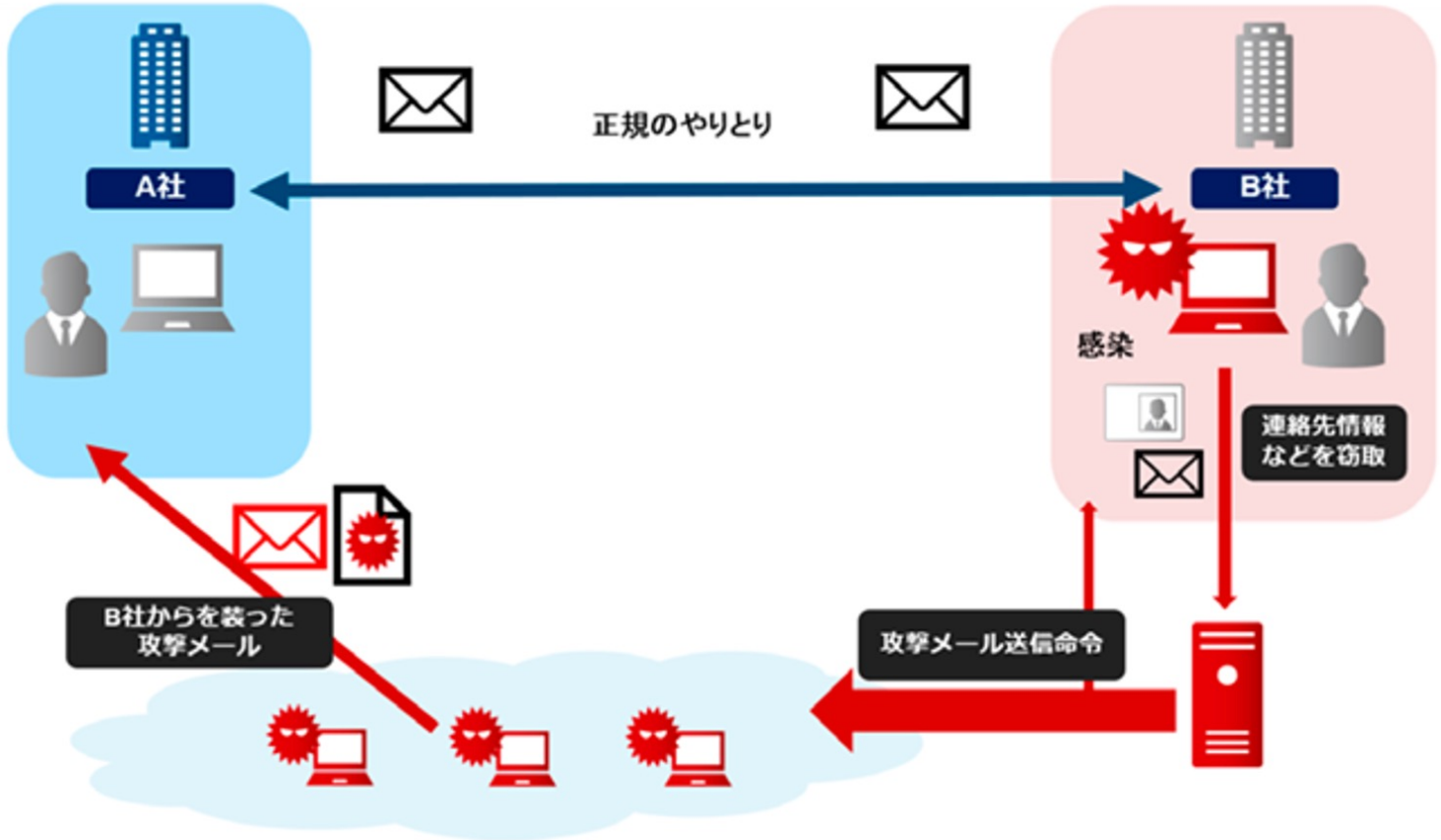
技術的脅威の事例④

- **ランサムウェア**（Ransom：身代金）
- メールの添付ファイルや、不審なリンクを開くことで感染。



技術的脅威の事例⑤

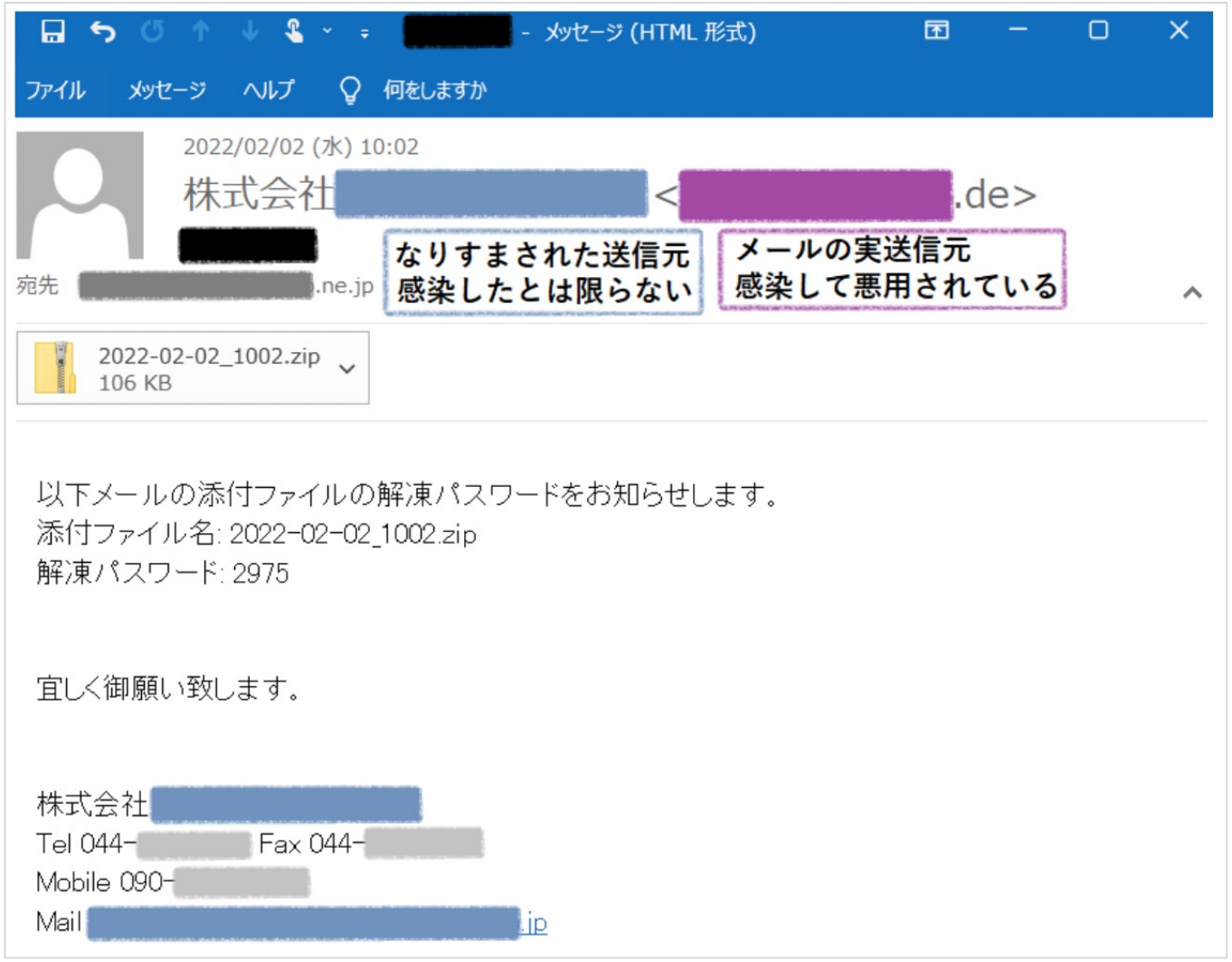
- **EMOTET被害**：メールの添付ファイルなどを通じて感染するマルウェア。
- メールアドレスやブラウザに保存されたパスワード情報などの窃取、EMOTETの感染拡大を起こす“なりすましメール“を他の組織や個人に送信し、被害を拡大する。



（出典）一般社団法人JPCERTコーディネーションセンター（2019）

EMOTETによる悪意あるサーバーからのメール配信

- 従業員が被害にあった場合、
  取引先の被害リスクが高まるため、
  企業間の信用問題に繋がる。



JPCERT/CC https://www.jpcert.or.jp/at/2022/at220006.html

脅威の種類は多岐にわたる

- このほか、IPA（経済産業省管轄・情報処理推進機構）が発表した最新版の情報脅威

▶情報セキュリティ10大脅威 2022

昨年順位	個人	順位	組織	昨年順位
2位	フィッシングによる個人情報等の詐取	1位	ランサムウェアによる被害	1位
3位	ネット上の誹謗・中傷・デマ	2位	標的型攻撃による機密情報の窃取	2位
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	3位	サプライチェーンの弱点を悪用した攻撃	4位
5位	クレジットカード情報の不正利用	4位	テレワーク等のニューノーマルな働き方を狙った攻撃	3位
1位	スマホ決済の不正利用	5位	内部不正による情報漏えい	6位
8位	偽警告によるインターネット詐欺	6位	脆弱性対策情報の公開に伴う悪用増加	10位
9位	不正アプリによるスマートフォン利用者への被害	7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
7位	インターネット上のサービスからの個人情報の窃取	8位	ビジネスメール詐欺による金銭被害	5位
6位	インターネットバンキングの不正利用	9位	予期せぬIT基盤の障害に伴う業務停止	7位
10位	インターネット上のサービスへの不正ログイン	10位	不注意による情報漏えい等の被害	9位

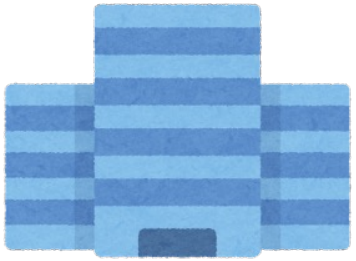
https://www.ipa.go.jp/about/press/20220127.html

NEW：初めてランクインした脅威

ハッカーの目的

- グローバル規模でインシデント解決の実績のある企業の技術知見が必要。

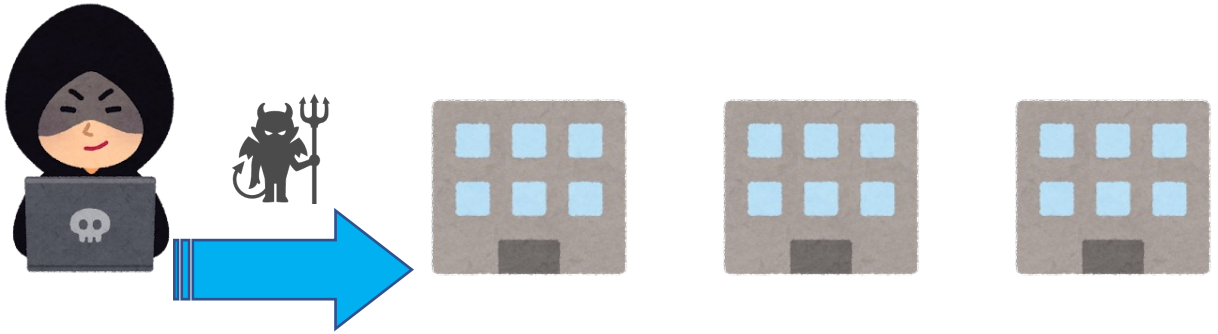
◆ハッカーはお金目的でやっている。
できれば大手を狙いたいが、大手を狙うのは技術的に厳しい。
大手と取引のあるサプライチェーンが狙われやすい
→中小企業はセキュリティ対策が不十分なケースが多い



大手企業

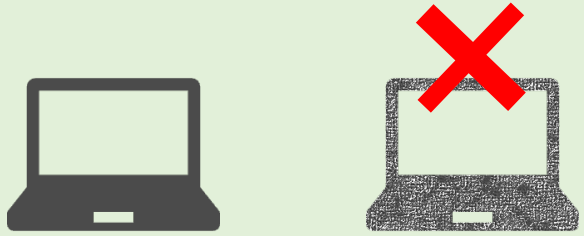
◆数ヶ月復旧までに時間がかかり、営業停止
その間の資金繰りが停止する　→　倒産リスク

◆世界中で起きている攻撃
データ破壊、サイバー攻撃、不正攻撃



情報セキュリティが保たれる状態

- 情報セキュリティマネジメントシステム：Information Security Management System(ISMS)
- 国際規格ISOで 情報が守られる状態を定義

機密性		情報を閲覧・使用できるのは 許可された人に限定する状態
完全性		情報が改ざんされていない、 消去や破壊もされない状態
可用性		必用なとき情報が利用できる状態。 バックアップ等で、障害や故障に備える。

情報セキュリティが保たれる状態

- 機密性・完全性・可用性を完全に満たそうとすると、誰も・何もできない情報となる。

適切に情報資産を保てるよう、事前準備が大切◎

無料のインターネットセキュリティ診断

- NTT東日本にてお客様へ訪問し、インターネットセキュリティ診断を無料で実施

NTT東日本

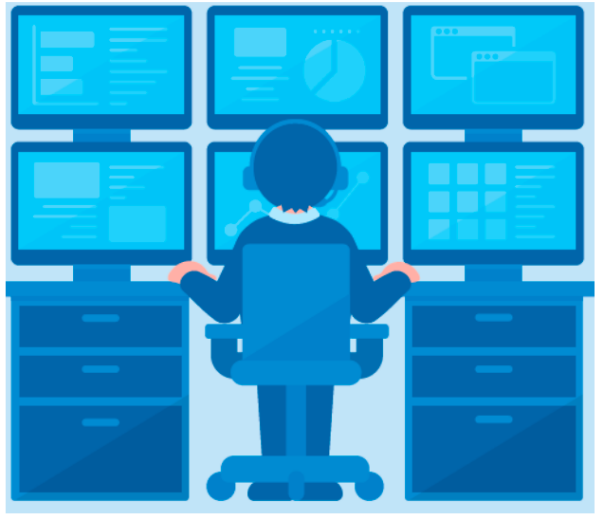
地域の企業の経営者・システム担当者様へ

診断内容のご紹介

無料受付中！

診断所要時間：概ね30分～1時間程度

・専門の担当者が診断いたします！
・診断結果は即日ご説明！



無料のインターネットセキュリティ診断

- PC端末のウィルス感染状況やお客様のネットワークへの不正アクセスがないかを診断

診断メニュー例

感染状況診断

PC端末のウイルス感染状況を診断します
感染が確認された場合、駆除まで実施します

不正アクセス診断

お客様NW環境に、実際にどれだけ不審な通信アクセスがあったかを診断します

その他

診断と併せて、ご利用環境におけるリスク要素についてもご案内いたします