名古屋港コンテナターミナルを襲ったサイバー攻撃

名古屋港コンテナターミナルの概要

取扱貨物（令和3年港湾統計より）

総取扱貨物量　1億7,779万トン（平成14年から20年連続日本一）
主な輸出貨物　完成自動車、自動車部品（輸出量の約65%）
主な輸入貨物　LNG（液化天然ガス）、鉄鉱石、原油、石炭の原料（輸入量の約53%）
外貿コンテナ取扱個数　約254万TEUで国内3位。（1TEUは20フィートコンテナ1個換算）

➡ ５つのターミナルで1日約7,500本のコンテナを扱っている（輸出が輸入より若干多い）

名古屋港は色々な項目で日本一となっている

項目	名古屋港	2位	3位
総取扱貨物量	1億7,779万トン	千葉港	横浜港
輸出額	12兆4,805億円	横浜港	東京港
輸出額から輸入額を差し引いた貿易差引額	7兆1,913億円	神戸港	横浜港
自動車輸出台数	117万台	三河港	横浜港
臨港地区面積（陸域）	4,298ヘクタール	北九州港	横浜港

名古屋港管理組合のWebサイトより

名古屋港コンテナターミナルの概要

主な輸出貨物

完成自動車
自動車部品
皿、カップ
オートバイ
電化製品

主な輸入貨物

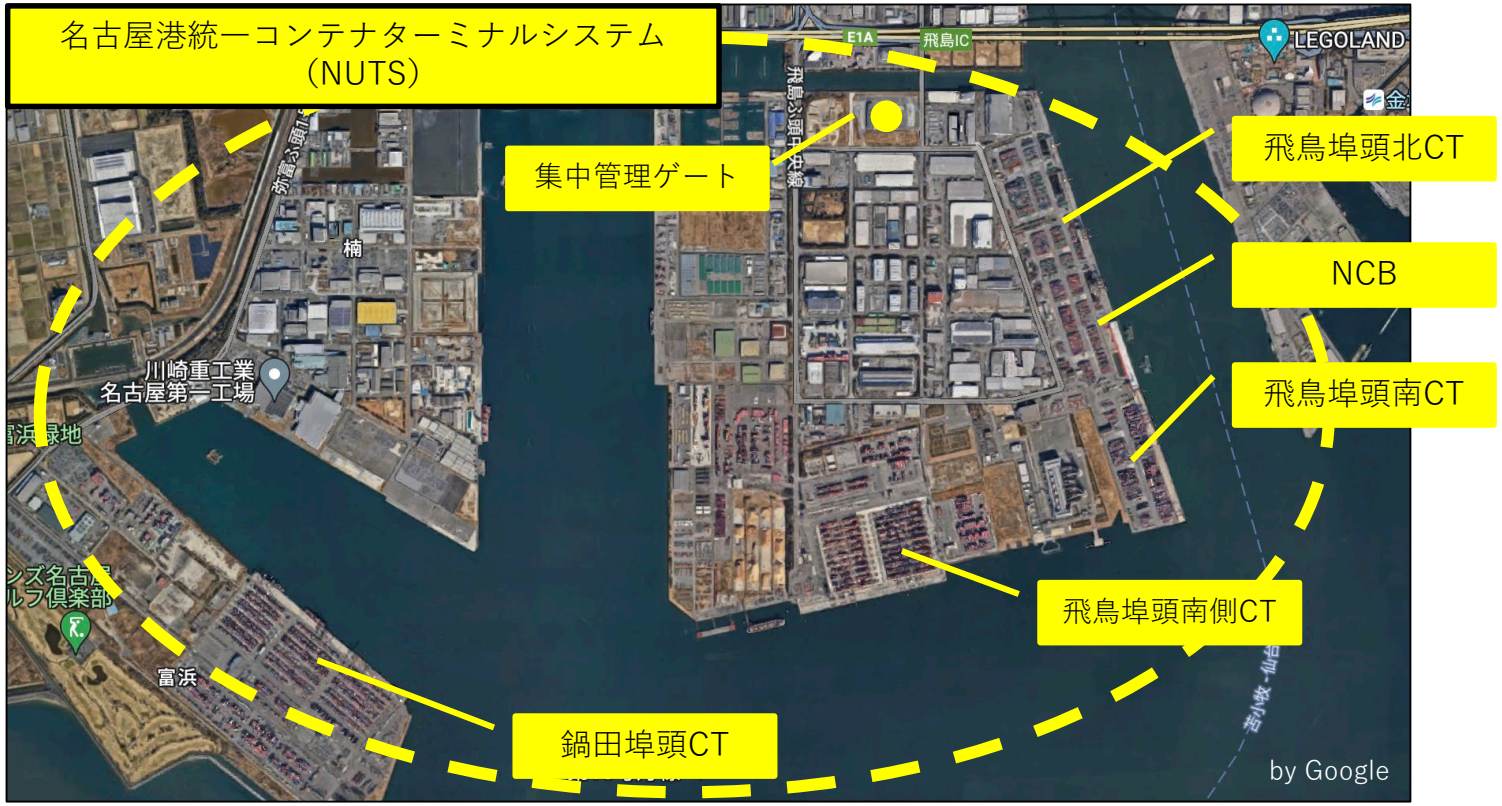
肉類
魚、エビ、カニ
果物
コーヒー豆
衣類
羊毛、綿花
家具
製材
電気機械

名古屋港統一ターミナルシステムのWebサイトより

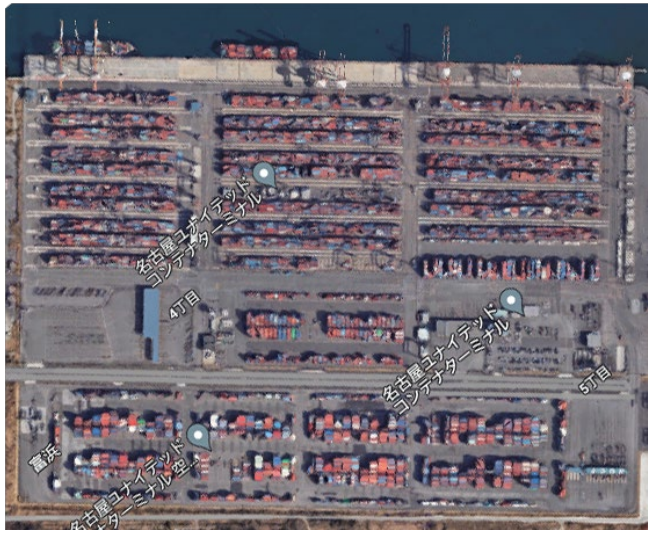
名古屋港統一コンテナターミナルシステム（NUTS）

名古屋港の５つのコンテナターミナルおよび集中管理ゲート（日本で唯一）が統一のコンピュータシステムで運用されている。2007年に現在の姿の基となるシステムがスタートし、機能を拡大しながら今日に至っている。

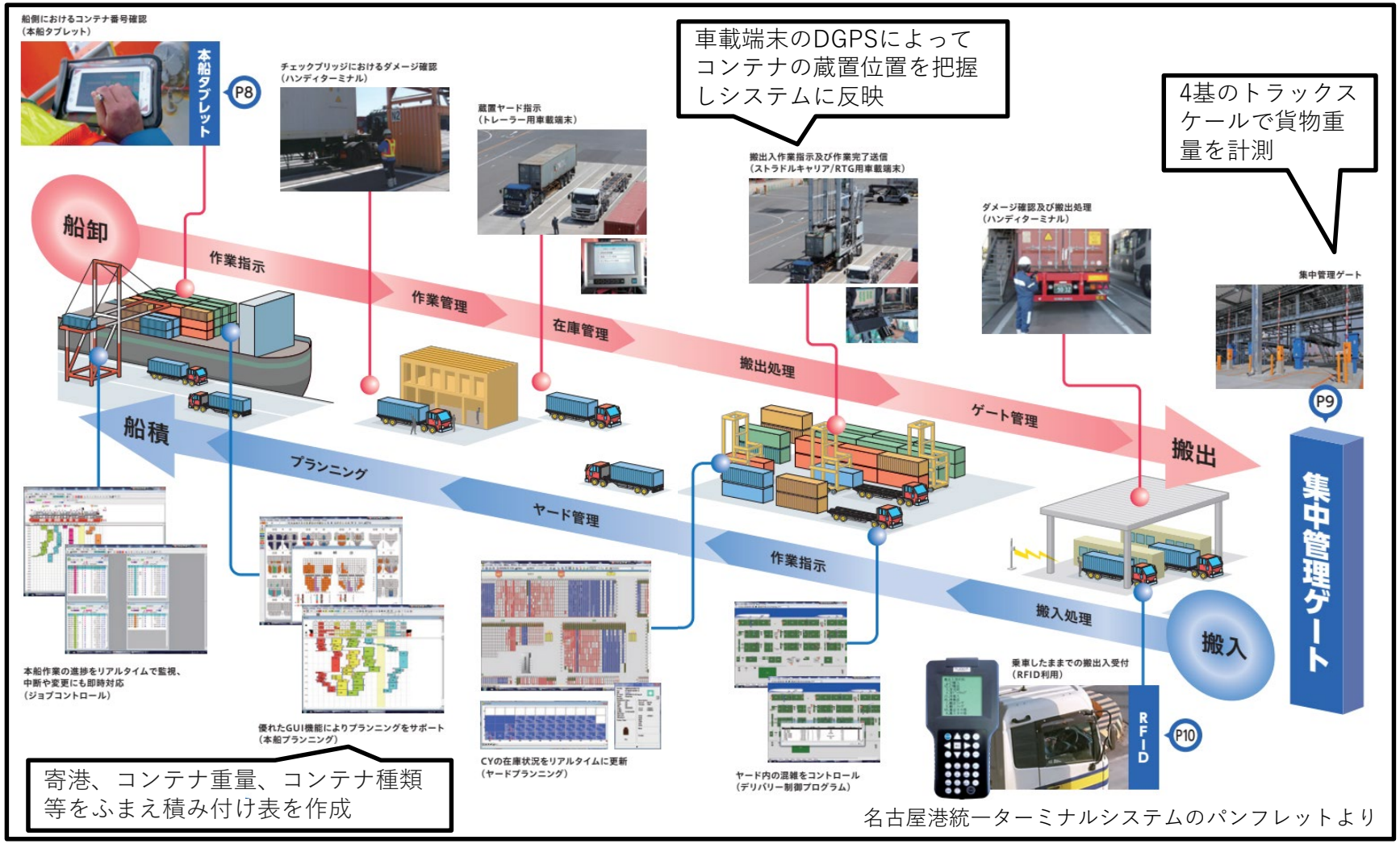
- 複数のコンテナターミナルを統合管理している港は日本では名古屋港と博多港のみ
- 名古屋港は日本で最もIT化が進んでいるコンテナターミナル



名古屋ユナイテッドターミナル（鍋田埠頭ターミナル）



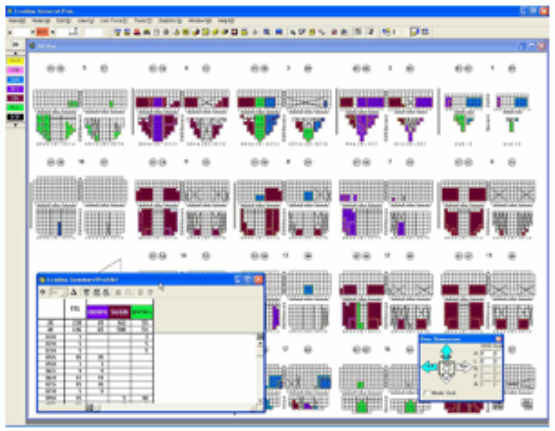
コンテナターミナルにおける全ての作業（コンテナ船積卸作業、プランニング、コンテナ保管管理、コンテナ搬出入管理、 ヤード作業管理、保税管理等）が統合管理され、効率的かつ機能的なオペレーションが実現されている。



名古屋港統一ターミナルシステムのパンフレットより

ヤード（※）管理
※コンテナを集積・保管・受け渡しを行う場所

コンテナ積み付けプランニング作成



➡ ITの支援によって高効率・高利便性を実現

サイバー攻撃の発生

2023年7月4日（火）早朝、名古屋港統一コンテナターミナルシステムがサイバー攻撃によって稼働不可となり、復旧まで3日を要した。

タイムライン（1日目）

国土交通省

【7月4日（火）】

06:30頃	NUTSシステムの作動が停止したことを確認
07:15頃	状況確認後、システム保守会社及びシステム開発会社へ調査を依頼
07:30頃	システム専用のプリンターからランサムウェア の脅迫文書が大量に印刷される
08:15頃	サーバが再起動できないことが判明
09:00頃	愛知県警察本部サイバー攻撃対策隊（以下「愛知県警」）に連絡、状況確認後、ランサムウェアに感染した可能性があるとの見解が示される
10:30頃	港湾での物流を早期に再開させるため、システム復旧を優先するよう判断、復旧作業開始
14:00頃	物理サーバ基盤及び全仮想サーバが暗号化されていることが判明
18:00頃	ランサムウェアに感染の可能性が高まったことから、愛知県警と今後の対応について協議を行う

出典：国土交通省「コンテナターミナルにおける情報セキュリティ対策等検討委員会 取りまとめ」
https://www.mlit.go.jp/kowan/kowan_mn2_000006.html

タイムライン（1日目）

国土交通省

この時の状況と対応

トラックの待ち行列が伸びていった

➡ トラック協会に連絡

朝、一隻が既に着岸しており、昼にも着岸予定あり

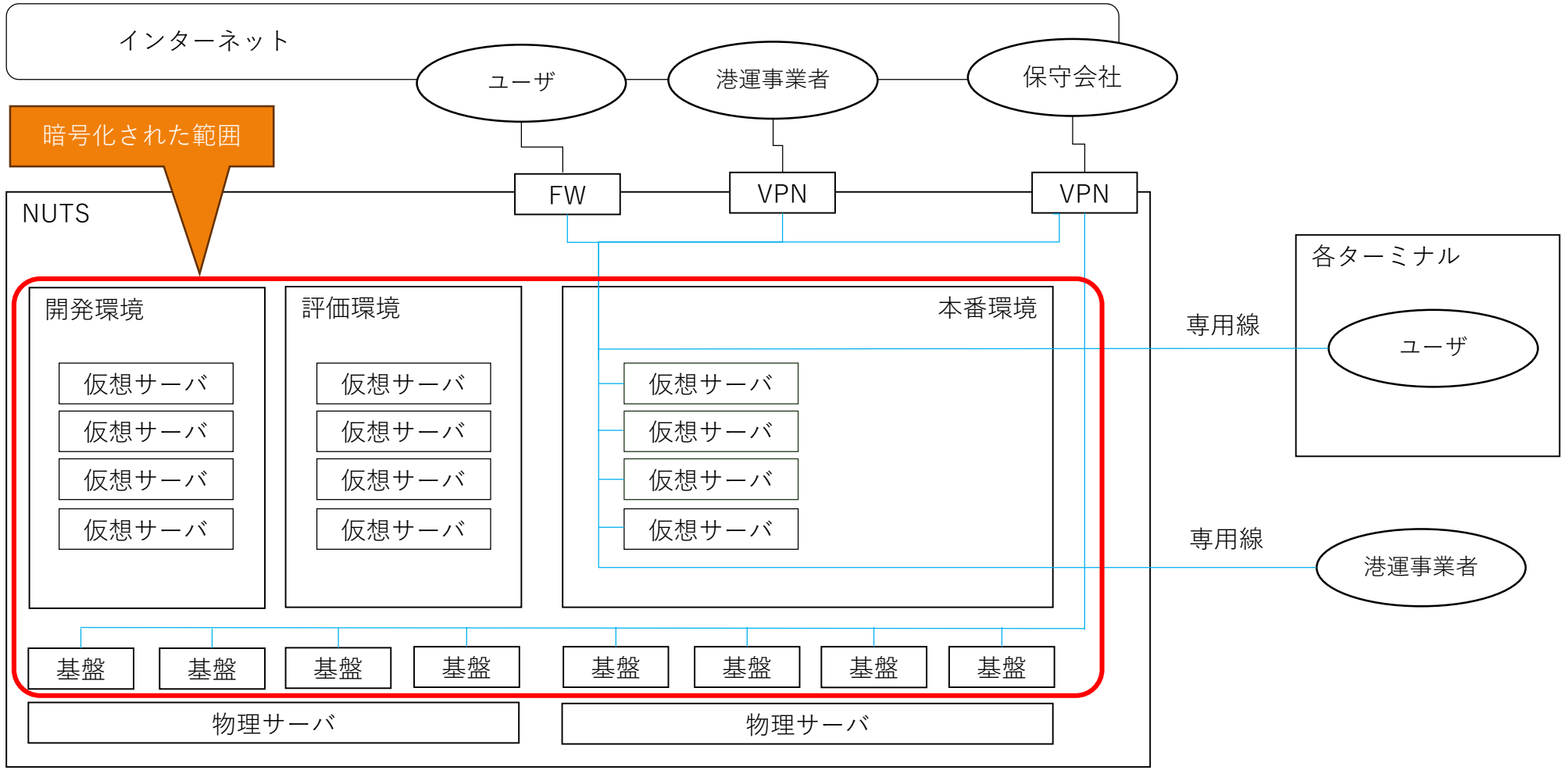
システムが稼働しない（全滅） → 警察に相談し、ランサムウェア攻撃であることを認識

➡ ターミナルのオペレーションを担う機器に問題はなかったが、システムの支援がないと（動かせても）動かせない

➡ システムの復旧を急ぐとともに、復旧までの対処を決定

1. 船卸→搬出はマニュアル作業で継続
2. 既に搬入済みのコンテナはマニュアル作業で船積
3. 新たな搬入は停止

NUTSのシステム・ネットワーク構成



バックアップ

① 本番、評価、開発の3環境あるが、容量の関係上、本番のサーバを1日1回取得し3日分を保存
② 取得したバックアップは同一ネットワーク内だけでなく、<u>複製を別の場所にも保存</u>

タイムライン（2日目・3日目）

国土交通省

【7月5日（水）】

02:00頃　物理サーバ基盤全8台が復旧、仮想サーバ（45台）の復元作業を開始

12:00頃　名古屋港運協会より、今回のシステム障害の原因がランサムウェアへの感染であることが判明したこと等をプレス発表

12:00頃　仮想サーバの復元完了、ウイルスチェックを開始

21:00頃　復元した仮想サーバからウイルスが検知され、ウイルス駆除の必要があると判断

【7月6日（木）】

02:00頃　ウイルスチェック終了、最終的にトロイの木馬120個マルウェア4個その他8件のウイルスを検知、ウイルス駆除を開始

07:15頃　ウイルス駆除終了、バックアップデータから復元が完了したが連携に障害が発生

14:15頃　連携障害が解消、データと実在庫情報の整合性の確認を開始

15:00　飛島ふ頭南側コンテナターミナル(TCB) 作業再開

16:30　鍋田ふ頭コンテナターミナル(NUCT) バンプール(空コンテナ)作業再開

17:00　NUTS WEB 稼働再開

17:20　鍋田ふ頭コンテナターミナル(NUCT) 全ての作業再開

18:15　NCB、飛島ふ頭北、飛島ふ頭南コンテナターミナル作業再開

影響

荷役スケジュールに影響が生じた船舶37隻（マニュアル作業で荷役を行なったため最大24 時間程度の遅延が発生した。）

搬入・搬出に影響があったコンテナ約2万本（推計）

トヨタ自動車の愛知県と岐阜県にある4つの拠点の稼働停止、アパレルメーカーにおける衣類の入荷遅延等

➡ マニュアル作業により船舶との間の荷役が継続されたことで、名古屋港をスキッ プする船舶はなかったとのこと。なお、今回はシステム化以前のマニュアル作業の経験者がいたため、マニュアル対応ができた。

➡ システム障害を想定したBCPは未整備だった

➡ これまでも、システム障害は発生していたが、短時間で復旧していた。
全面的かつ長時間のシステム障害は想定していなかった。

3日で復旧ができた要因

バックアップが生きていた

資産（システム構成やネットワーク構成）の把握や管理ができていた

ターミナルシステムのみが被害

警察との迅速な連携

明確で迅速な意思決定

関係者（港運事業者）の結束

保守ベンダーとの良好な関係

侵入経路

侵入経路として考えられるのは以下の3点

① VPN機器からの侵入

- 港湾事業者用と保守用があるが、保守用には緊急時に即時に対応するためIPアドレスに制限をかけておらず、IDとパスワードさえ合致すればインターネット上で誰からでもアクセス可能な状態にあった
- 脆弱性への対応が不十分であった

② 専用線接続先からの侵入

港運事業者とのデータ授受用。

③ USBメモリ(記憶媒体)からの持ち込み

本船とのデータ授受に使用

➡ 保守用VPN機器経由の可能性が高い

VPN機器のログは仮想サーバに保存していたため暗号化されてしまった。さらに、当該サーバはバックアップ取得対象としていなかったためログの解析ができず、特定には至らなかった。

侵入後の攻撃手口

物理サーバ基盤とその上で稼働していた全仮想サーバが暗号化された
物理サーバ基盤に関して脆弱性への対応が不十分だった

- 攻撃者は（VPN機器経由で）物理サーバ基盤にアクセスしデータを暗号化したと推測
- 物理サーバ基盤の脆弱性を悪用された可能性が高い

システムログやアクセスログはバックアップ取得対象としていなかったため、
暗号化被害によってログの解析ができず、原因の特定には至らなかった。

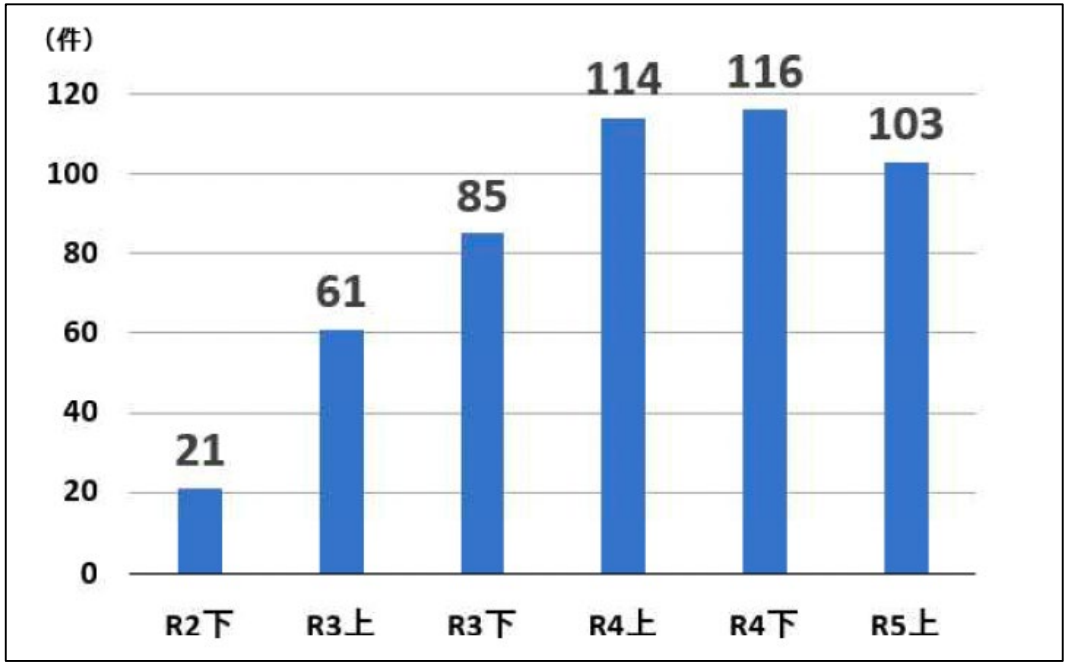
ランサムウェア攻撃について

ランサムウェア攻撃について

NUTSを襲ったサイバー攻撃は「ランサムウェア攻撃」と呼ばれており、コンピュータ上のファイルを暗号化して使用できない状態にした上で、そのデータを復号する対価を要求する攻撃。なお、暗号化のみならずデータを窃取し「対価を支払わなければ当該データを公開する」と対価を要求する二重恐喝（ダブルエクストーション）型も発生している。

ランサムウェア攻撃は、世界中で被害が発生しており。日本の企業・組織における被害も増加している。

＜企業・団体等におけるランサムウェア被害の警察庁への報告件数＞



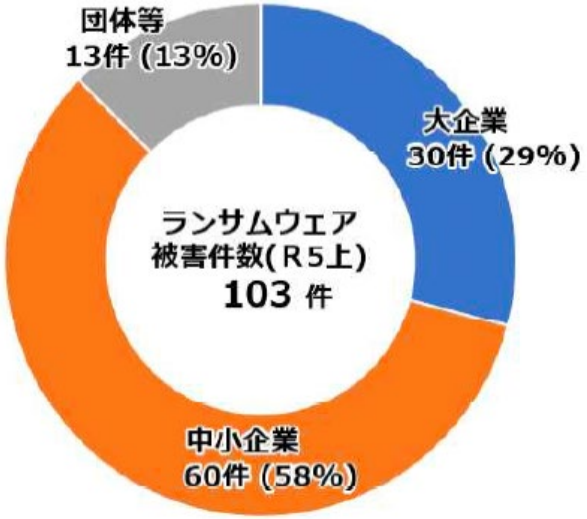
出典：「令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について」（警察庁）

ランサムウェア攻撃の日本での状況

警察庁が令和5年9月に公表した「令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について」によると、令和5年上半期に報告のあったランサムウェア被害は103件であるが、内訳を企業・団体等の規模別に見ると、大企業は30件、中小企業は60件と規模を問わず発生している。

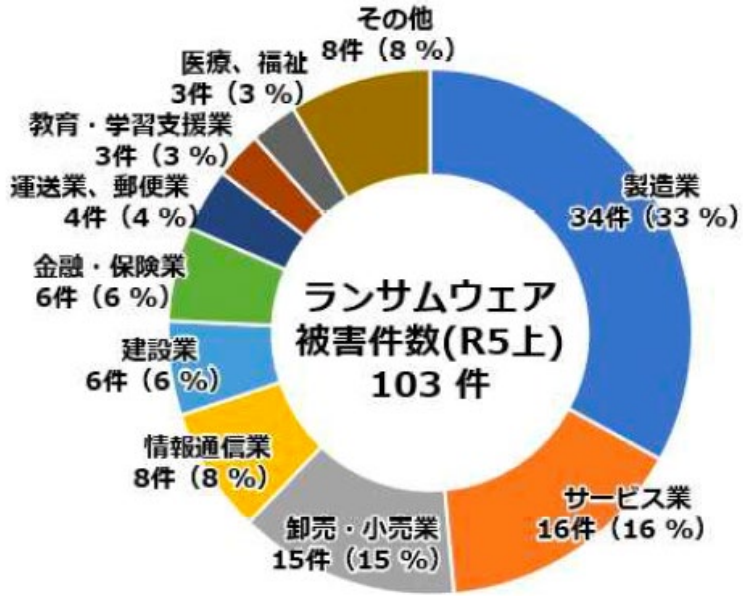
また、業種別に見ると、製造業34件、サービス業16件、卸売・小売業15件と業種を問わず発生している。

＜ランサムウェア被害の企業・団体等の規模別報告件数＞



出典：「令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について」（警察庁）

＜ランサムウェア被害の企業・団体等の業種別報告件数＞



出典：「令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について」（警察庁）

➡ 攻撃者は特定の企業や業種を標的にしている訳ではなく、攻撃可能なところを成り行きで攻撃していると考えらえる。

ランサムウェア攻撃のエコシステム

ランサムウェア攻撃は、近年、Ransomware as a Service（RaaS）と呼ばれる分業モデルによって多くの攻撃者が参加するようになった。RaaSの役割分担は以下の通り。

1. 運営組織
   ランサムウェアの開発・保守や身代金の受け取りを行い、実際の攻撃はアフィリエイトに行わせる。

2. アフィリエイト
   ターゲットとなった企業・組織のネットワークに侵入しランサムウェアを実行する個人もしくは小規模なグループ。この分業システムによって多くの攻撃者が攻撃に参加できるようになった。

3. 不正アクセス仲介人
   インターネット中を探索し侵入可能な機器を見つけ出し、その情報を攻撃者コミュニティーで販売している個人もしくは小規模なグループ。以前から存在していたが、RaaSの登場によって活発化している。

➡ 侵入可能な機器は漏れなく洗い出され、攻撃を受ける時代

ランサムウェア攻撃とは（まとめ）

国土交通省

攻撃者の目的は？

➡ 金銭です。

攻撃者や攻撃者グループはどこにいるの？

➡ 世界中に散らばっています。組織化されている場合でも緩やかなものです。

病院や工場、港湾施設を狙っているの？

➡ いいえ、標的を絞っている訳ではなく、攻撃可能なところを攻撃しています。

小さな会社・組織は弱点があっても見つけられたり、攻撃されたりしないのでは？

➡ 侵入可能な弱点は、探索を専門的に行う攻撃者がいて、遍く見つかります。

➡ 小さな会社・組織は、攻撃も簡単で短時間で済むことが多く、攻撃者は躊躇なく攻撃します。実際、小さな会社・組織においても被害が発生しています。

ランサムウェア攻撃を受けるとどうなるのか？

1. ネットワークの停止、閉塞

   攻撃者による更なる侵害やランサムウェアが拡散する可能性があるため、一旦、ネットワークを停止したり、外部との接続を切断したりすることを余儀なくされる。

2. 多くの端末、サーバが被害に

   侵害可能な端末、サーバは軒並み侵害される。特に管理者権限のID,PWが使い回されていたり、リモートから攻撃可能な脆弱性が放置されたりしていると、瞬く間に多くの機器が侵害されてしまう。

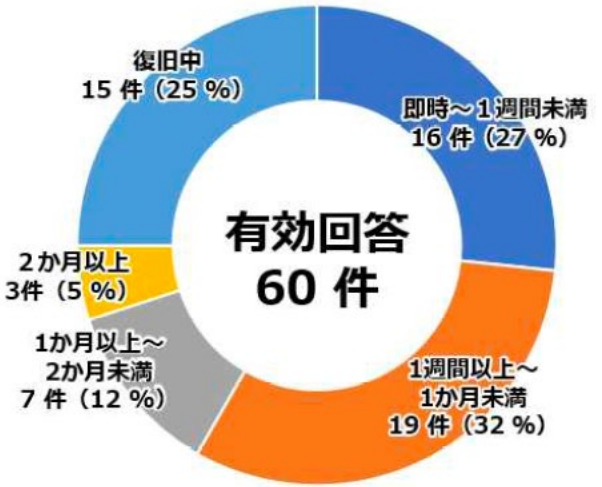
3. 難航する復旧

   バックアップも暗号化されてしまったり、バックアップはあるも最新ではなかったり、バックアップから復旧に失敗したり等、復旧が難航することが少なくない。

➡ 復旧まで数週間から1ヶ月を要することが少なくない

➡ システム障害やネットワーク障害は、1日（長くとも2、3日）で復旧するが、サイバー攻撃の場合は、そうはいかない

＜復旧に要した期間＞



出典：「令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について」（警察庁）

ランサムウェア攻撃への対策

基本的な対策を徹底しサイバー攻撃を防げる健全な状態を保つことが必要

1. ID管理、認証
   - デフォルトの管理者IDは無効化し独自IDとする
   - 複雑なパスワードやログイン試行回数の制限
   - 多要素認証の導入（特にインターネットからの接続は必須）
2. アクセス制御
   - 接続元のIPアドレスを制限（特にインターネットからの接続は必須）
     ➡保守用も例外なし（できない場合は多要素認証を使用）
   - ネットワーク機器の管理画面はインターネットからアクセス不可にする
   - 専用線接続においてもファイヤーウォールを設置し必要な通信のみ許容する
3. パッチの適用
   - インターネットに面している機器は必須
   - ネットワーク内の機器も機器の重要性に応じて定期的にパッチを適用

➡ 基本中の基本であり決して難しいことではない

ランサムウェア攻撃への対策

防御対策に加え、万一、攻撃を受けても壊滅的な状況に陥らない対策も重要であり、その必要性が高まっている。

1. データのバックアップ
   - サイバー攻撃を想定した（破壊されない）バックアップ
   - バックアップからの戻しの手順整備や訓練を定期的に実施

2. ログの取得と保全
   - 早期復旧には何が起きているかを知ることが重要
   - 侵入経路になり得る機器は必須
   - 必要なログが取得できる設定とする（デフォルトだと不十分なことが多い）
   - 攻撃者に消去されない保存方法とする

➡ サイバー攻撃に関する理解がないと必要性を認識できない

BCPについて

自然災害を想定したもの

➡ 施設自体や機器、人員に影響が発生
自社・自組織だけでなく、周辺や地域で広く影響が発生

システム障害を想定したもの

➡ 単一システム（もしくは機器）が停止（ただし、1日程度）
施設自体や機器、人員は影響なし
自社・自組織のみが影響

サイバー攻撃を想定したもの

➡ 複数（もしくは全面的に）システムが停止（しかも、長期間に及ぶ）
施設自体や機器、人員は影響なし
自社・自組織のみが影響

➡ サイバー攻撃を想定したBCPの必要性が高まっている

➡ どれぐらいシステムなしで耐えれるかを明確にすることによって、必要なシステムのレジリエンス（回復力）が決まってくる

ITが止まることで施設全体・業務全体が影響を受ける時代

#	事例	発生時期	被害内容
1	徳島県つるぎ町立半田病院	2021年10月	保守用のリモート接続機器への侵入をきっかけに電子カルテシステムを始め多くのシステムが使用不能となり、予約外患者の受入停止等を余儀なくされた。診療業務の完全再開まで2ヶ月を要した。
2	小島プレス工業	2022年2月	リモート接続機器の脆弱性をきっかけにサーバやPCが停止し、受注・納入が不能となった。同社はトヨタ自動車の主要サプライヤーであり、この影響で3月1日、国内の全工場（14工場28ライン）の停止を余儀なくされた。翌日には仮復旧を果たしたが、本復旧には1ヶ月を要した。
3	大阪急性期・総合医療センター	2022年10月	給食業者のネットワーク経由で侵入され電子カルテシステムを始め多くのシステムが使用不能となり、予約外患者の受入停止等を余儀なくされた。診療業務の完全再開まで2ヶ月を要した。
4	名古屋港コンテナターミナル	2023年7月	保守用のリモート接続機器への侵入をきっかけにコンテナターミナルシステムが3日間、使用不能となった。

- これらの事例の共通点は？
- ランサムウェア攻撃によってITが大きな被害を受けたが、被害を受けていない機械や人も業務ができなくなった
- あらゆる分野でITの利用が広がっており、ITが止まると業務が止まる事業者が続々と生まれている
- 最近でも、総合スーパーや新聞社がランサムウェア攻撃によるITの被害で本業に影響が発生

リモート保守のパラドックス

システム化を進める → 障害の影響が大きくなる → 迅速な保守が必要 → リモート保守導入 → セキュリティ対策が不十分 → サイバー攻撃被害

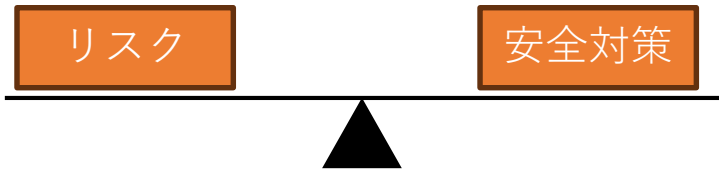
- 保守面の要件が中心で、導入した仕組みのセキュリティリスクや必要な対策への認識は不足しがち
  - 企業・組織側、ベンダー側、いずれも責任がある

日常で、自動車に乗るときこのような格好をしますか？

二輪車でロングツーリングをする時は？

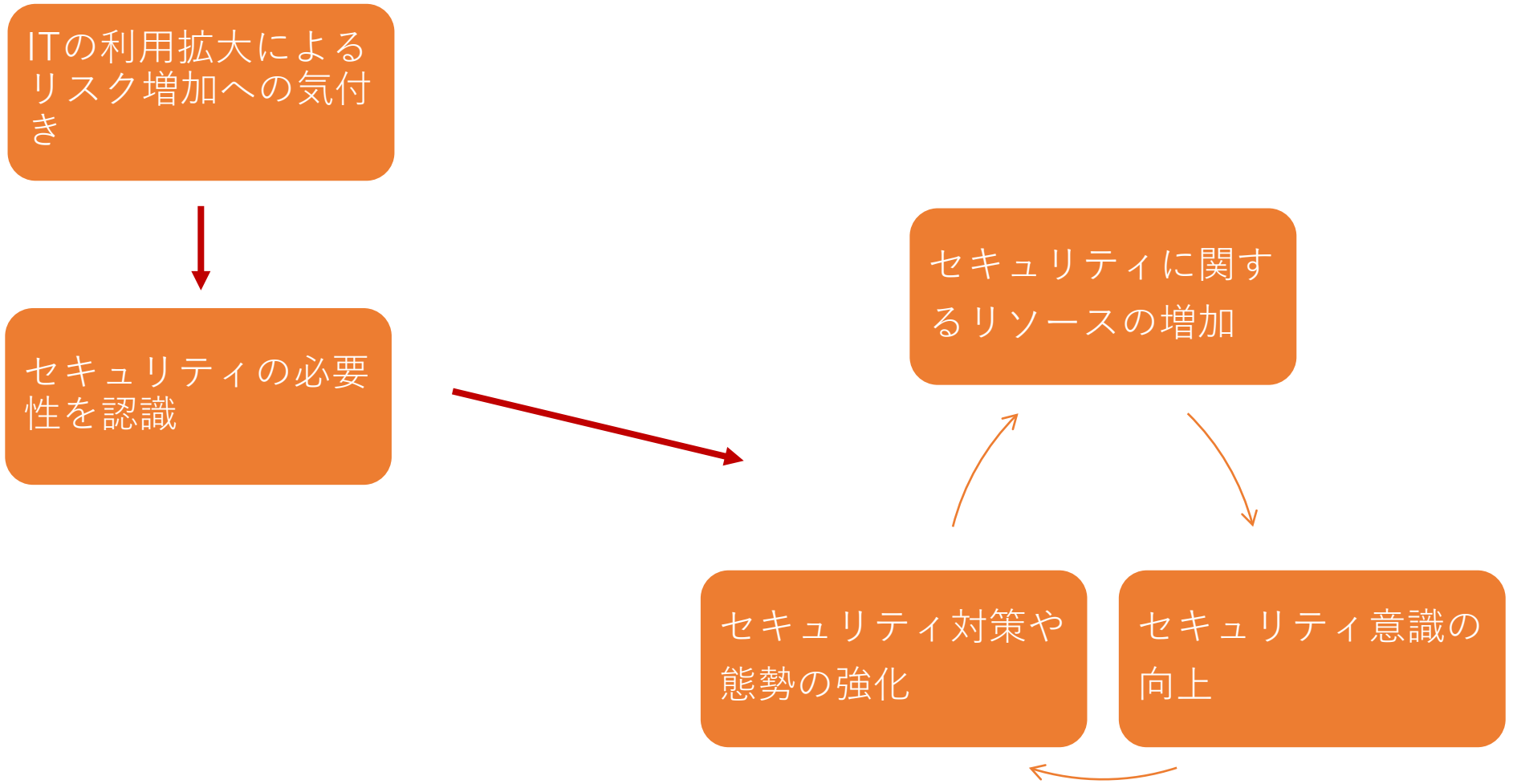
自動車ですが、サーキットでレースをするなら？

実生活において、私たちは、自らの行動に対しリスク評価を行い、適切な安全対策を行っています。



- ITは見えないためか、リスクに気づきにくい
- ITは見えないためか、正常性バイアスが働きやすい

Awarenessの重要性



- 業界・分野でAwarenessを進めていくことも効果的
- 国や業界団体の取り組みや後押しも必要

ご清聴ありがとうございました