AIで「すりコニッ！」完成版!!

OT現場に「サイバー攻撃」の意識をすりこみたい

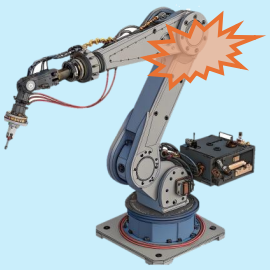
「すりコミッ！」とは…

OT現場の方にサイバー攻撃の意識を**すり**こむ**コミック**

○背景

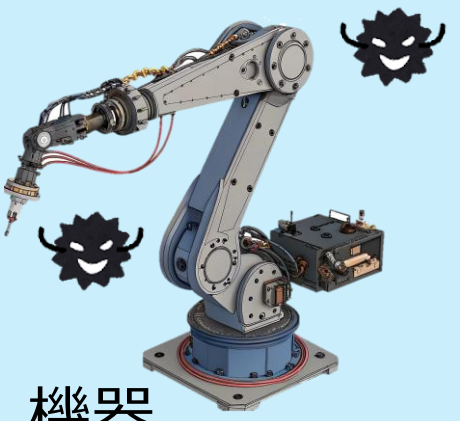
保守員

機器異常発生



機器

▶



機器

単なる機器故障だと
思っていたが…

実際はサイバー攻撃で
機器が感染していた

- 近年、工場やインフラなどの**OT現場**でも**サイバー攻撃**の被害が**増加**
- OT現場でサイバー攻撃が発生した場合、現場担当者の多くは機器故障を疑い、サイバー攻撃とは気づかない可能性がある

○目的

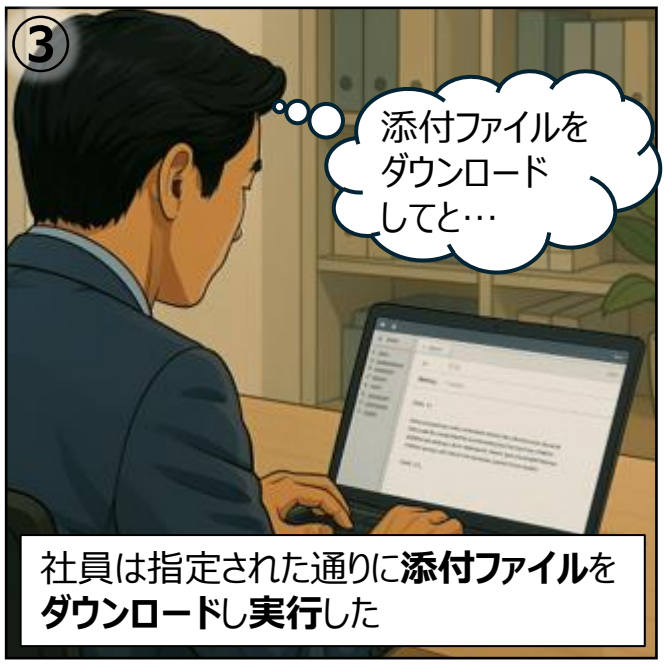
OT現場の方に「サイバー攻撃」を
知ってもらい意識してもらう

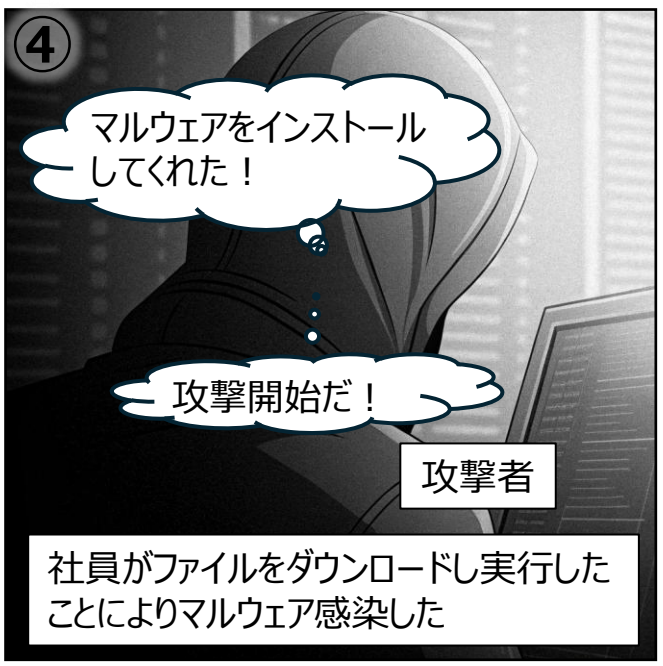
▼

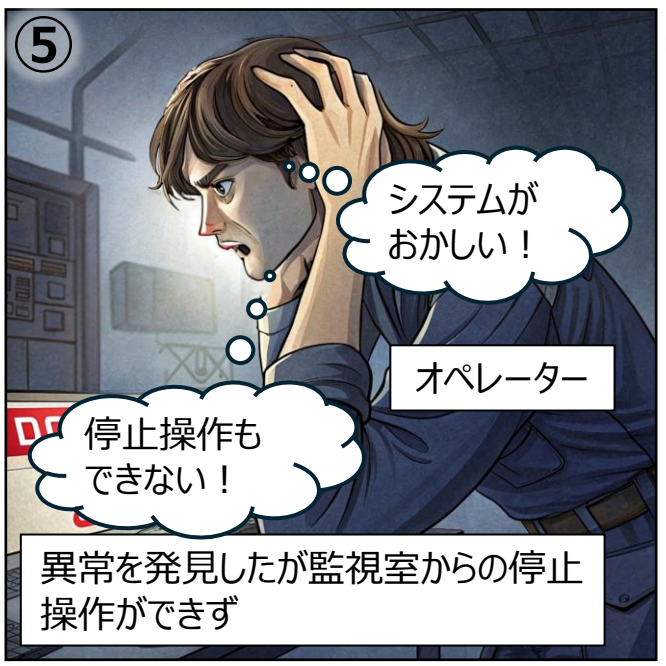
読んでもらいやすい漫画
「すりコミッ！」を作成

※画像はAIで作成しています

1通のメールが引き起こした悪夢







○概要

攻撃者は、従業員に偽のメール（標的型メール）を送りつけ、その添付ファイルを開かせて実行させることで、従業員のPCをマルウェアに感染させた。これにより工場の制御システムが乗っ取られ、設備の操作ができなくなり、溶鉱炉のひとつが甚大な被害を受けた。サイバー攻撃は、情報システムだけでなく現場の機械設備にも深刻な影響を与えることがある。

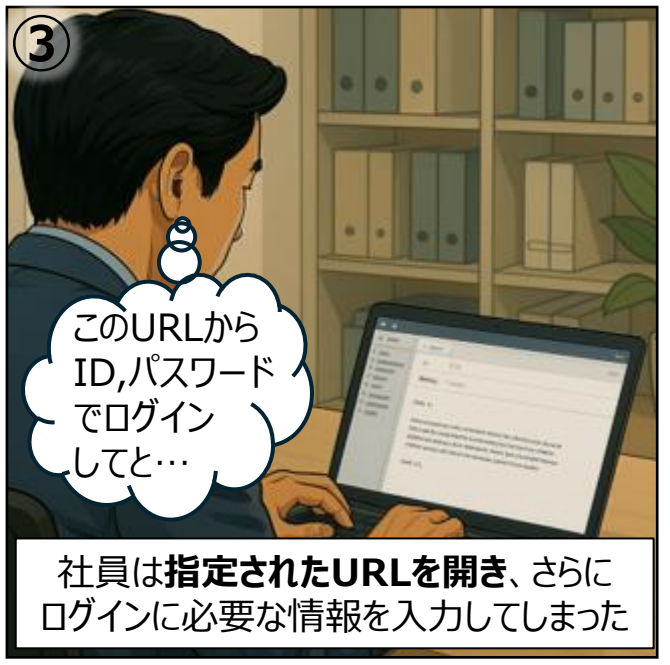
○意識してほしいこと

メールの**添付ファイルから設備が乗っ取られる**こともあるので**安易に開かない**ようにしましょう

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

開くな危険



○概要

天然ガスを供給する施設で、社員が標的型メールのリンクをクリックし、リンク先のサイトにIDやパスワードなどの情報を入力してしまった。これによって攻撃者がログイン情報を入手し、ネットワークに侵入した。侵入された結果、監視画面や制御画面が使えなくなり、プラントは約2日間にわたり操業停止を余儀なくされた。

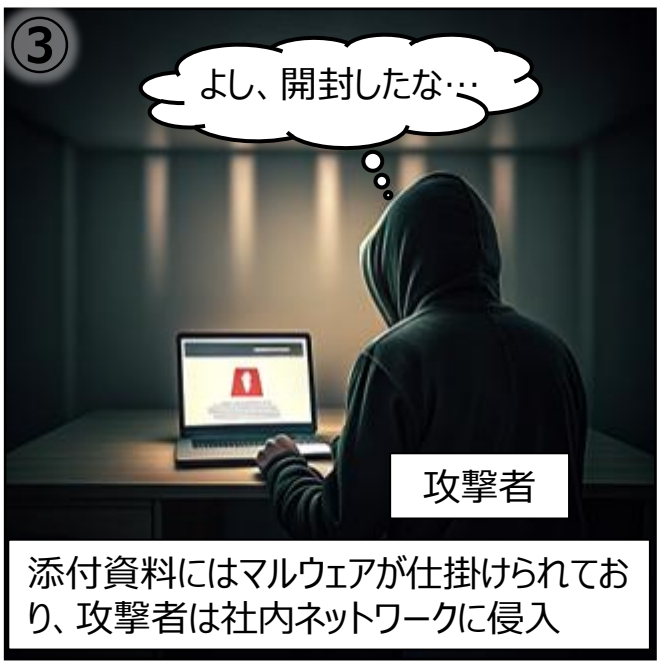
○意識してほしいこと

知っている相手からのメールでも、**リンクを開く前**に一度**立ち止まって確認**をしましょう

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

それ、本当に緊急ですか？



○概要

とある飲料会社で、従業員が受信した緊急を装ったメールを開封したことがきっかけとなり、社内で数百台の機器がマルウェアに感染した。その結果、注文処理などの業務を手動で行うことになり、数日間で数億円の売上損失が発生した。さらに、データのバックアップ設定にも不備があったため、外部専門家の支援を含めても通常業務への復旧に数週間を要した。

○意識してほしいこと

攻撃者は緊急を装うなど**巧妙にメールを開かせようとします**

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

U（うそだろ） S（挿した） B（ばっかりに）

○概要

攻撃者は施設内に侵入してマルウェアに感染したUSBメモリを意図的に落とした。現場管理者は発見したUSBメモリを自社のものと思い込みPCに接続した。USBメモリの接続により、制御ネットワーク内に攻撃者の侵入を許し、遠心分離機が遠隔操作された。これにより、回転数が異常となり、約1,000台が損傷、操業停止に至る事態が発生した。

○意識してほしいこと

USBメモリを挿すだけでマルウェアに感染することがあることを知っておきましょう

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

「知らなかった」では済まされない

○概要

ある航空会社にて、空港の管制システムがウイルスに感染した。感染経路はUSBメモリであった。管制システムに被害が発生し、機体の異常検知処理が停止した。これにより、管制塔は離陸するまでに異常を検知して停止を指示することができず、機体は滑走路を外れ炎上し、多数の死傷者が発生した。

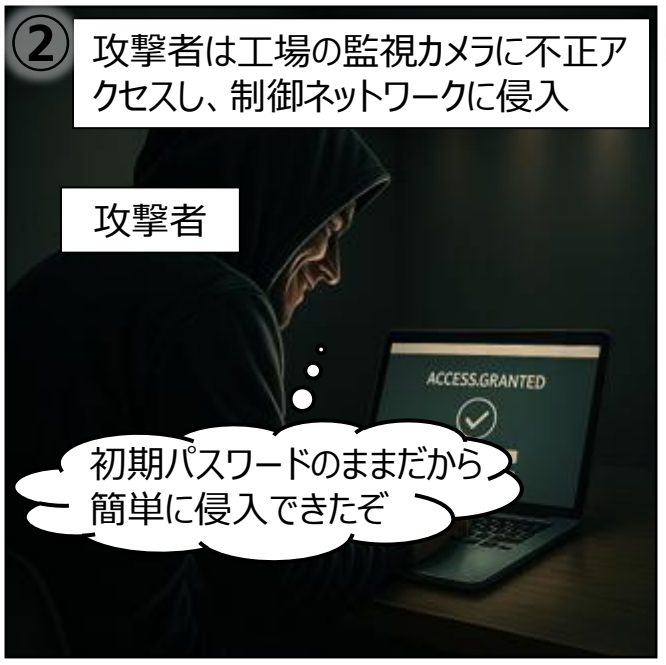
○意識してほしいこと

外部記憶媒体を使用する際は、**許可されたものであるか確認しましょう**

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

パスワードで大炎上



機器設定の不正変更により、工場内で火災が発生

攻撃者により、火災発生時の監視カメラの映像がSNSを通じて外部に公開

復旧作業により事態は沈静化するも、工場は一時的に操業停止に追い込まれた

○概要

攻撃者は、初期パスワードから変更されず使用されていた監視カメラ経由で制御システムを遠隔操作し、機器を異常動作させた。結果として、工場内で火災が発生した。さらに攻撃者は企業への抗議を発信するため、声明文とともに火災発生時の工場内部の監視映像を外部に公開した。死傷者は発生しなかったが、一時的に操業が停止した。

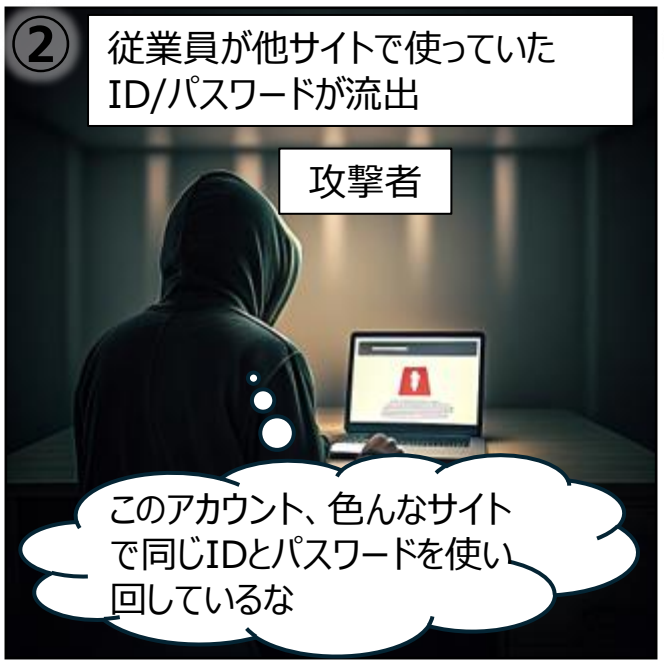
○意識してほしいこと

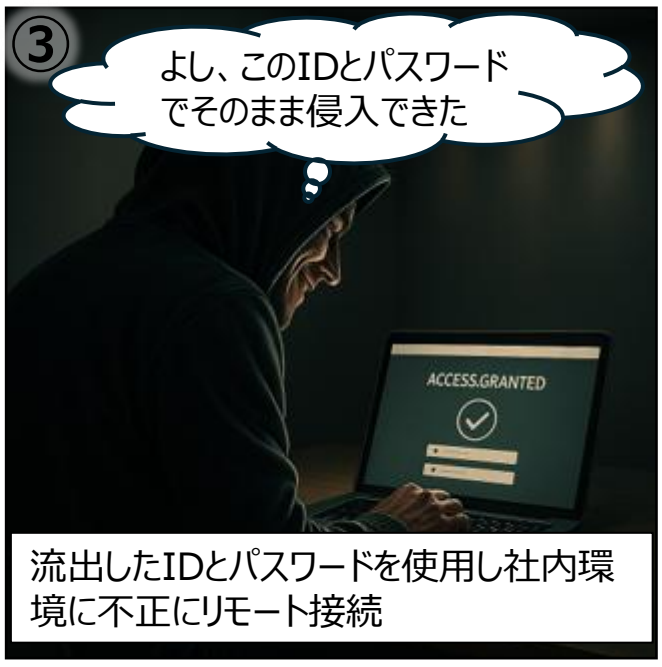
初期パスワードは変更しましょう

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

使い回しの果てに





○概要

石油関連会社のITシステムがランサムウェアにより暗号化される被害を受けた。同社は工場への被害拡大を抑えるため、予防的措置として操業を停止した。これにより石油製品の供給が一時的に滞り、数億円規模の被害が発生した。従業員のIDとパスワードの使い回しが指摘されており、放置されていた社内へのリモート接続用ツールのアカウントの悪用が原因とされている。

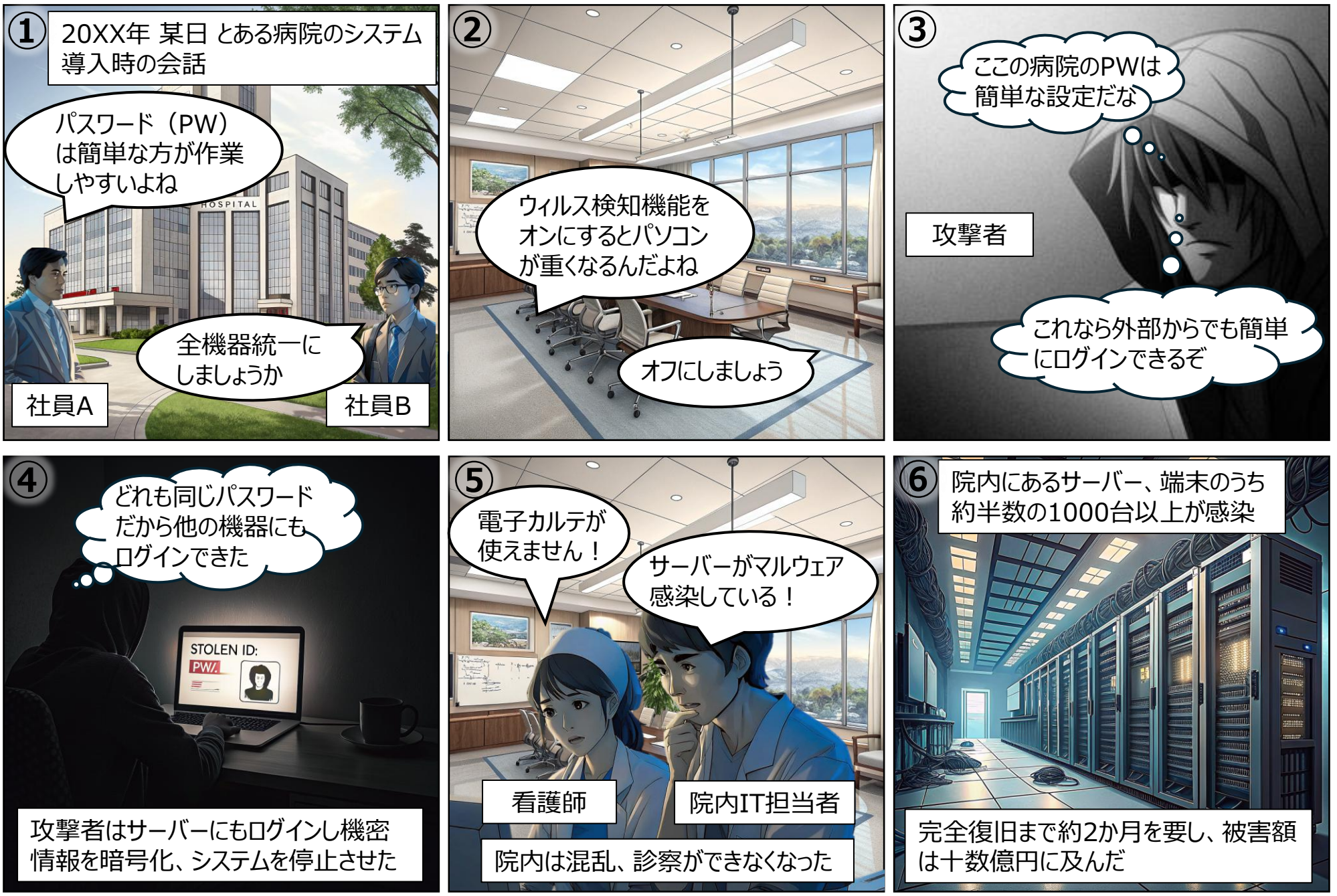
○意識してほしいこと

社内システムの**IDやパスワードを使い回さない**ようにしましょう

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

感染対策していなかった病院



○概要

とある病院で、作業の効率を優先するあまり、簡単なパスワードの使用やウイルス検知機能を無効にした状態で運用されていた。このため、攻撃者は外部から容易にログインでき、患者の個人情報などの機密情報を扱うサーバーを暗号化してシステムを停止させた。結果として、院内にあるサーバーや端末のうち約半数の1000台以上が感染し、完全復旧までに約2か月を要し、被害額は十数億円にのぼった。

○意識してほしいこと

業務の効率性だけでなくセキュリティも意識し、**パスワード**の**適切な設定**と**ウイルス対策の有効化**を徹底しましょう

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

海の玄関に忍び寄る脅威

○概要

港湾で使用されているコンテナターミナルの統合管理システムが保守用のリモート接続機器経由で不正アクセスを許し、ランサムウェアによるサイバー攻撃を受けた結果、システムが停止。これにより港湾業務が約3日間全面的にストップし、多くの企業の物流に深刻な影響が出た。バックアップデータにて復旧されたが、重要インフラにおけるサイバーセキュリティ対策の必要性が改めて注目された。

○意識してほしいこと

リモート接続機器は、利便性がある反面
サイバー攻撃の入り口になると知っておきましょう

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

保守だと信じていたあのログイン

○概要

水道局で、攻撃者が遠隔から制御システムに不正アクセスした。オペレーターは誰かがリモート保守しているのだと思い込み特に対応はしなかった。その後、攻撃者は水に混ぜる薬品（水酸化ナトリウム）の濃度を100倍以上に引き上げようとした。異変に気づいたオペレーターがすぐに設定を元に戻したことで被害は防がれたが、もし攻撃が成功していれば、地域住民の水道水が汚染される危険があった。

○意識してほしいこと

リモート接続させる場合は、**アクセス管理**を徹底しましょう

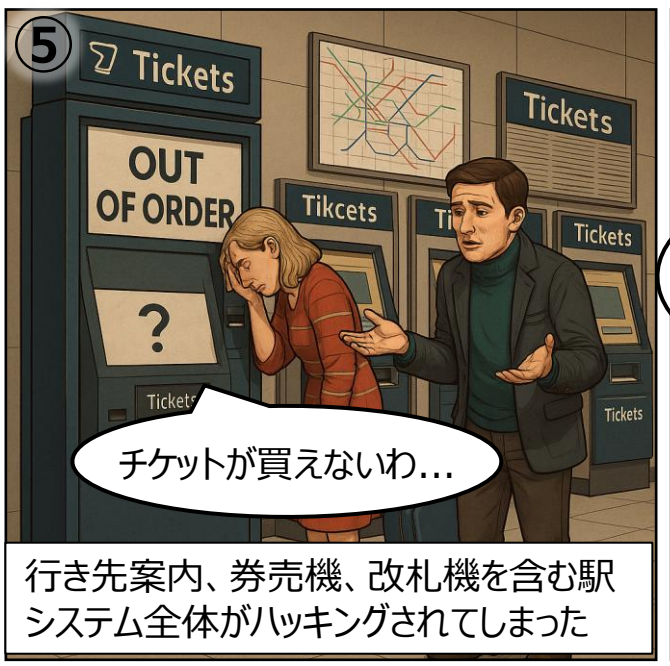
備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

DXで開くのは未来か侵入口か

鉄道会社でもDX化により、保守の省力化が進められている

保守用システムの設定不備から不正ログインに成功し、駅システムまで侵入



行き先案内、券売機、改札機を含む駅システム全体がハッキングされてしまった

駅員は旅客の対応に追われ、駅は大混乱、列車の遅延・運休が発生した

○概要

とある鉄道会社はシステムのDX化により、保守の省力化を進めていた。
保守用システムはDX化に伴いインターネット接続が発生し、設定不備によりインターネット上で閲覧可能になっていた。攻撃者はこれを悪用し、保守用システムに不正アクセスしたのち、駅システム(行き先案内、券売機、改札機など)まで侵入した。改ざんや不正制御によりシステムが機能しなくなり駅は大混乱となった。

○意識してほしいこと

DX化により攻撃の入り口が増える
ことを知っておきましょう

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

列車はどこだ

○概要

とある鉄道会社で、列車が一時的に運休する事態となった。原因は、運行情報を提供する委託先企業がサイバー攻撃を受けたことで列車の現在位置が指令所から確認できなくなり、安全確保のため列車の運行を中止したためである。運行中止により、数万人の乗客に影響がでて、鉄道会社の信頼を失うことに繋がった。

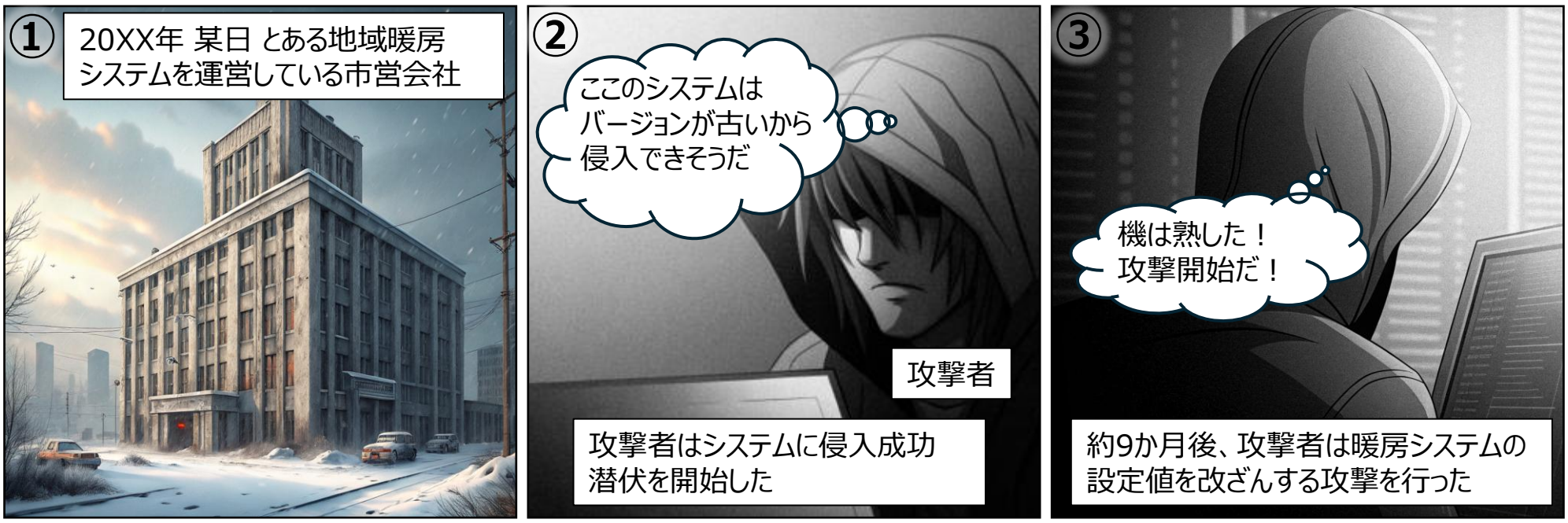
○意識してほしいこと

委託先企業が攻撃されることで自社にも影響があることを知っておきましょう

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

そのとき、暖は奪われた



○概要

建物に暖房と給湯を供給するエネルギー会社において、システムが古いバージョンのまま運用されていた。攻撃者はこのバージョンが古いことを悪用してネットワークに侵入し、その痕跡を気づかれにくくするために長期間(約9か月間)潜伏した。その後、暖房制御の設定値を改ざんし、システムを不安定にさせたことで、600棟以上の建物で約2日間にわたり暖房設備が停止する深刻な影響が出た。

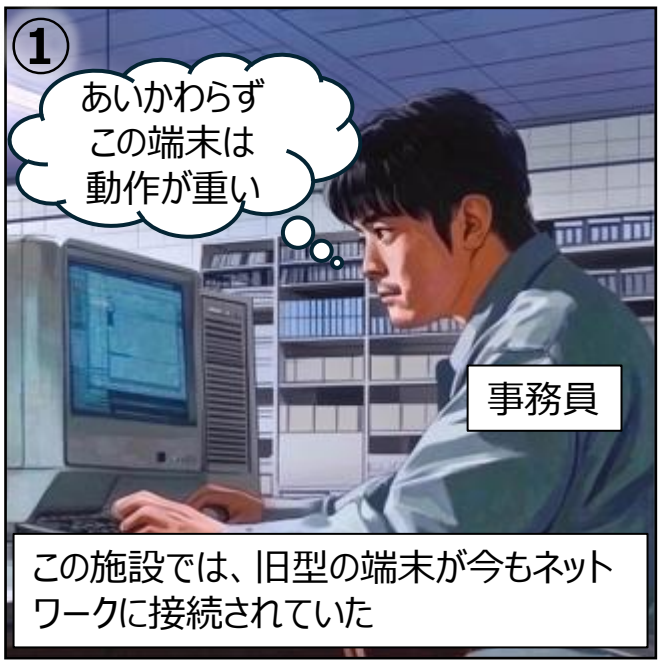
○意識してほしいこと

古いシステムは**攻撃されやすく**、設備が止まる原因にもなるので、適宜**アップデート**を行いましょう

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

化石が牙をむく



○概要

攻撃者は、更新されていない旧型の端末からプラント内のネットワークへ侵入し、制御システムに不正なプログラムを送信した。
異常を検知したため、安全計装システムが作動し、システムが緊急停止した。大きな事故は回避したが、プラントは一時的に操業停止した。

○意識してほしいこと

旧型の端末はサイバー攻撃の入り口になりやすい
ことを知っておきましょう

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

”まだ動く”の代償

○概要

海運企業がランサムウェア攻撃を受けた。OSのサポートが終了しているサーバーが侵入口となり、マルウェアが急速に拡散し、数万台の端末が停止した。港湾拠点ではコンテナの積み下ろしができなくなり、業務が停止した。被害総額は数百億円規模にのぼった。

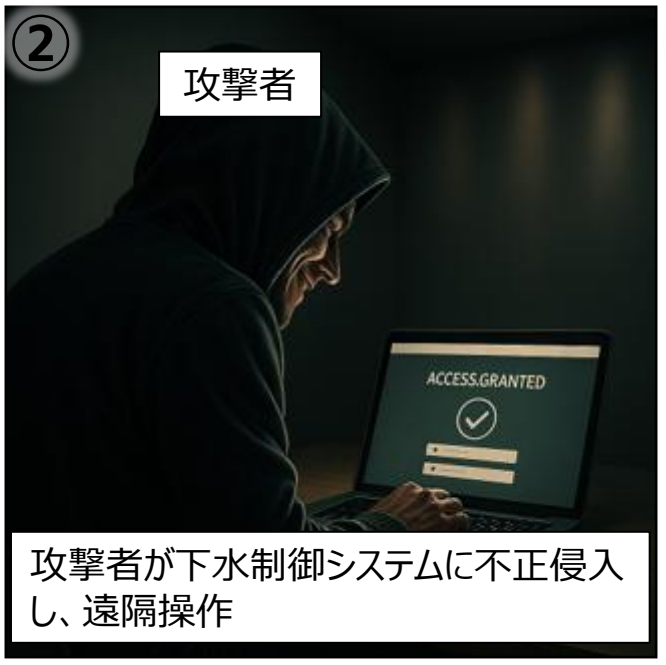
○意識してほしいこと

サポートの終了したOSは、サイバー攻撃の入り口になりやすいことを知っておきましょう

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

さらば、そして侵入



○概要

元関係者による不正アクセスにより水道施設の制御システムが遠隔操作され、大量の未処理下水が公園や川などの公共施設に流出し、悪臭や生物大量死などの被害が発生した。攻撃者は委託業者の元社員で、退職後も在職中のアクセス権限、内部情報および機器を不正利用していたことが判明し、後に逮捕された。水道施設側でも退職者のアクセス権限削除など、適切な管理ができていなかった。

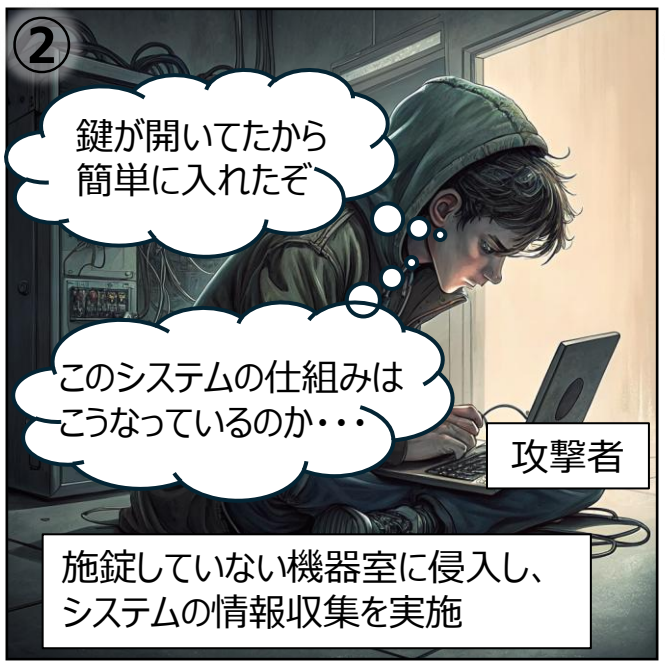
○意識してほしいこと

不要になったアクセス権限（退職者や元委託先）は**即時に削除**しましょう

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

施錠忘れが招いた脱線事故



○概要

攻撃者が鉄道の制御システムをハッキングした。施錠されていない機器室（立ち入り禁止区域）に侵入し、数か月かけて列車の制御システムと列車の行き先を変更する装置を調査。古いテレビのリモコンを改造して赤外線送信機を作り、列車の進路を不正に操作した。その結果、列車が脱線した。

○意識してほしいこと

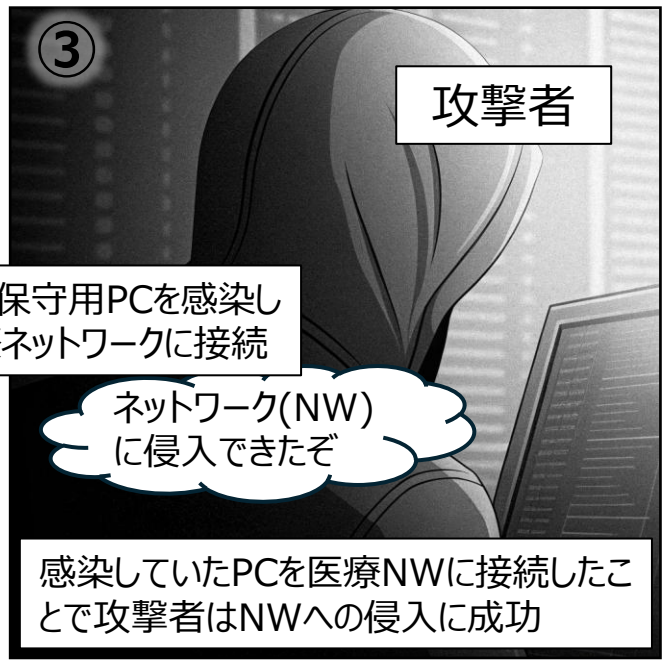
立ち入り禁止区域の**施錠を徹底**しましょう

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

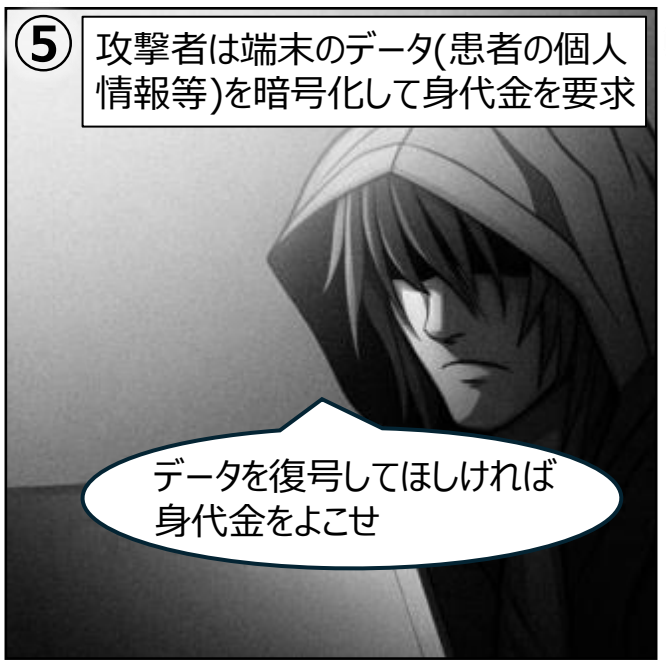
デジタルパンデミック

ウイルス感染していた保守用PCを感染しているとは知らず医療ネットワークに接続



感染していたPCを医療NWに接続したことで攻撃者はNWへの侵入に成功

NWがわかれていなかったため医療機器が次々にウイルス感染



PC類が使えなくなったため患者にも多くの影響が出る結果となった

○概要

院内の保守担当者は、ウイルスに感染していることに気づかずに保守用PCを院内ネットワーク(NW)に接続してしまった。院内のNWは適切に分離されていなかったため、接続後すぐに攻撃者が患者の個人情報を含む機密情報のデータベースへアクセスできる状態となった。攻撃者はこれらのデータを暗号化し、身代金を要求。業務に必要な情報が使えなくなったことで、院内の業務が滞り、多くの患者に影響が及んだ。

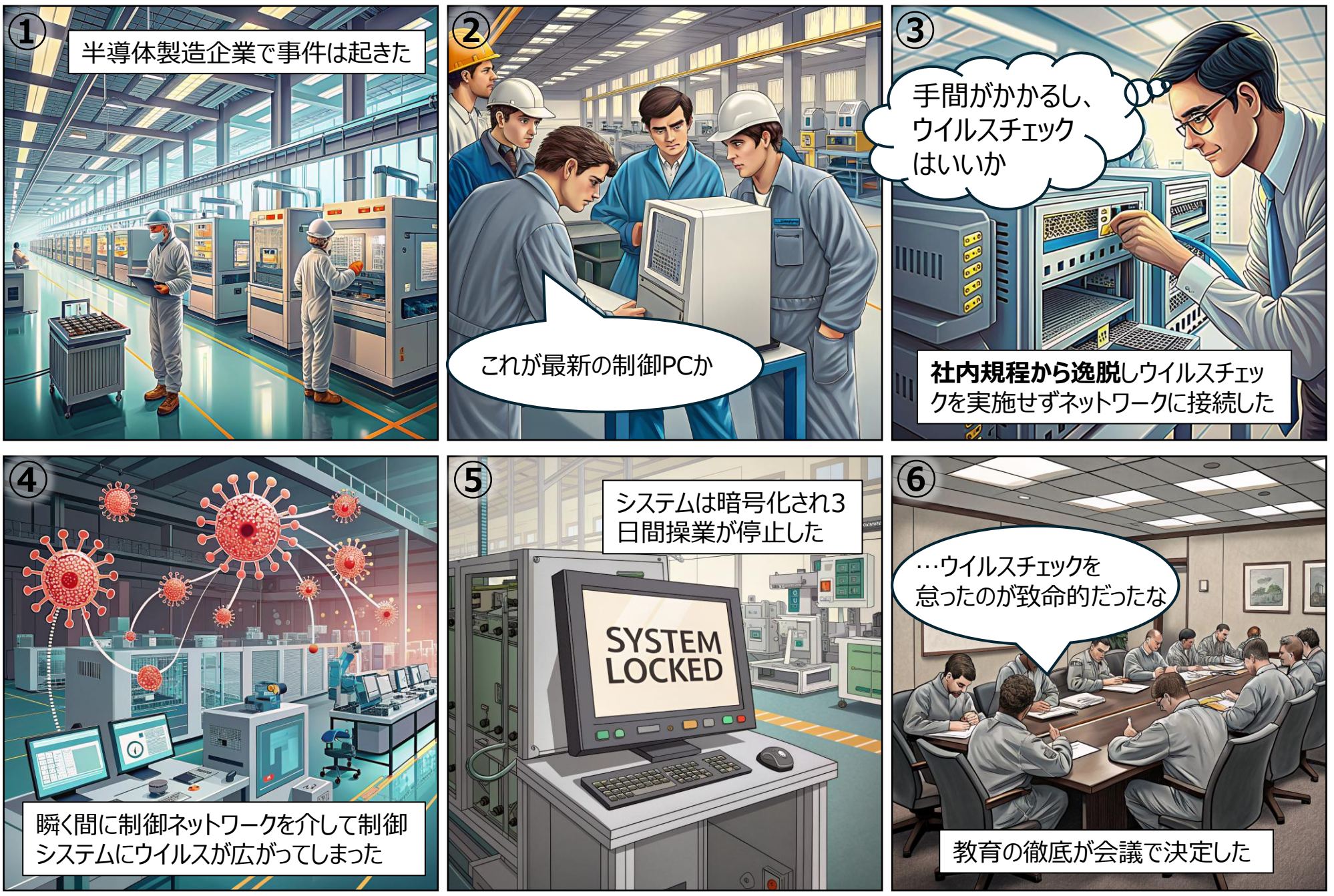
○意識してほしいこと

持ち込んだあらゆる機器は**ウイルスに感染している可能性**があることを知っておきましょう

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

新機材の影にひそむ危機



○概要

半導体製造企業で新たに導入された制御PCが、ウイルスに感染していた。この企業では、新しい機器を導入するときは、ウイルスチェックをすることが社内規程で定められていた。しかし、ウイルスチェックをせずに工場ネットワークへ接続したことで、感染が制御系ネットワーク全体に拡大。複数のコンピュータが制御不能にされ、製造ラインが最大3日間停止する事態に発展した。

○意識してほしいこと

社内規程に従い、機器接続時の確認作業を徹底しましょう

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

怠った報告、止まったライン

リモート接続機器の設定不備を利用して攻撃者は侵入に成功した

オペレーターは違和感を覚えつつも、連絡をしなかった…

工場停止の影響により、グループ全体の生産が停止する事態に陥った

相互作用が働くサプライチェーンでは関連工場全体のリスクが問われる…

○概要

リモート接続機器の設定不備に起因して、あるグループ会社の子会社である、部品生産工場の生産システムがランサムウェアにより暗号化された。オペレーターは身に覚えのないリモート接続を放置してしまったため、被害が拡大し、当工場の製造が一時停止した。さらに、サプライチェーン全体に影響が波及したことによってグループの全工場が数日生産停止に陥る事態となった。

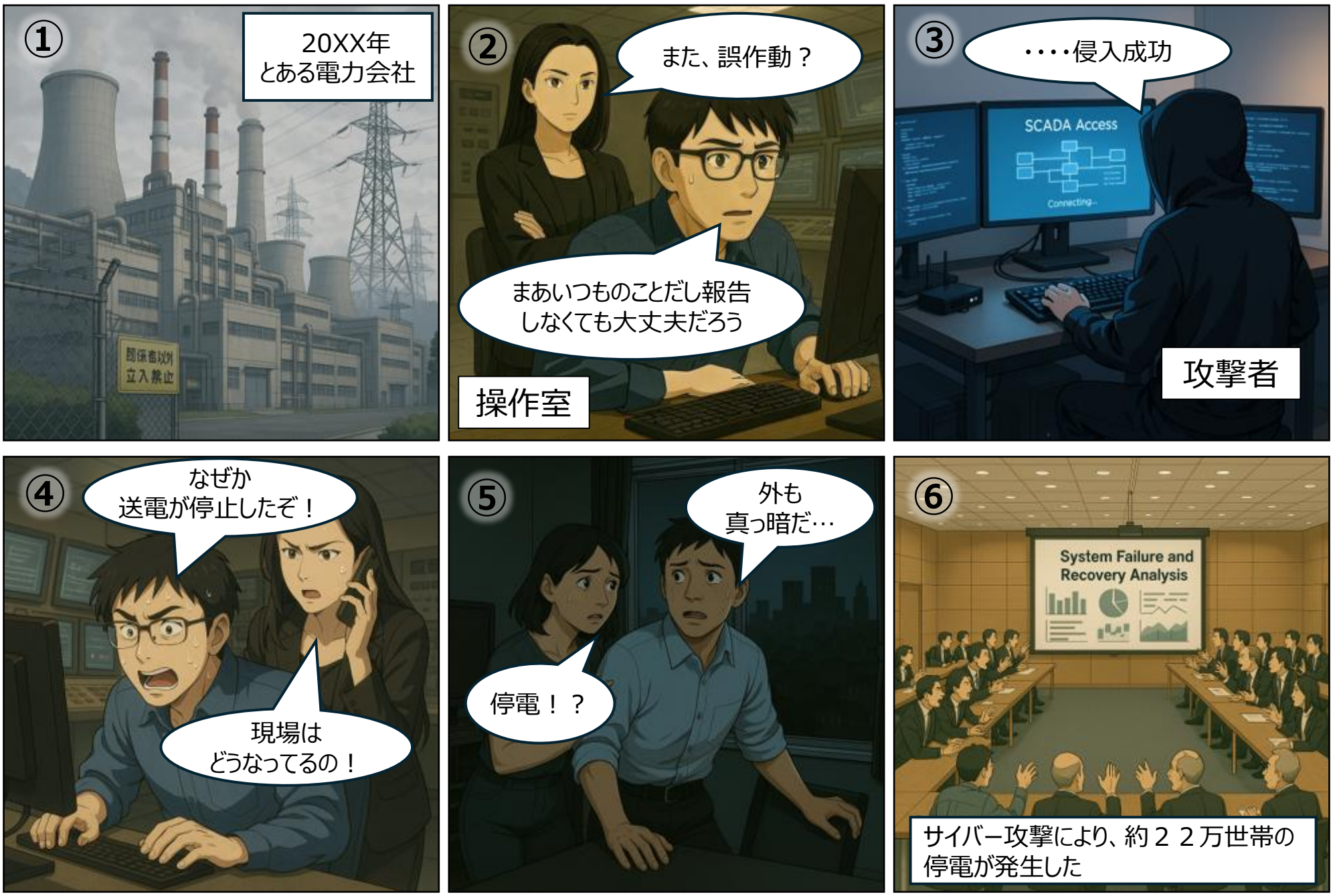
○意識してほしいこと

身に覚えのないリモート接続を見つけたら
すぐに管理者へ連絡しましょう

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

異常です　それが日常　なぜだろう



○概要

電力会社がサイバー攻撃を受け、約22万5,000世帯が数時間にわたって停電した。攻撃者は電力会社のネットワークに不正侵入し、遠隔操作で送電を遮断した。事前にシステムの不具合が現場で確認されていたが、単なる機器の不調とみなされて報告されていなかった。

○意識してほしいこと

作業記録を残し、誤動作などがあれば**すぐに報告・調査**しましょう

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

自己(事故)判断

攻撃者は工場のPCを利用したデータマイニング(お金稼ぎ)を企んでいた

攻撃者が工場のPCを悪用したことで負荷が高くなり、操作ができなくなった

工場内の約100台のPCが被害を受け、生産停止に陥った

○概要

攻撃者は某工場のPCのログイン情報を盗みだした。その情報を悪用して工場内のPCにログインしデータマイニング(お金稼ぎ)を試みた。オペレーターは不審なコマンドを発見し、上司へ相談するか悩んだが相談はしなかった。攻撃者の工場のPCの悪用により負荷が高くなった結果、オペレーターはPCの操作ができなくなった。被害は約100台のPCに拡大し工場は生産停止に陥った。

○意識してほしいこと

対応に迷ったらチームや上司へ**すぐに相談**しましょう

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

水門の向こうに潜む影

担当者はエラーの発生に気づいていたものの、チームへの連絡を怠った

○概要

攻撃者は監視制御システムへ侵入し、遠隔操作で水門を開いて洪水を引き起こした。これにより下流では甚大な被害が発生した。この攻撃による兆候として、操作機器のエラーが発生していたが、保守担当者は設備の老朽化によるものであると断定し、チームへの共有を怠ったために被害が発生した。

○意識してほしいこと

些細なエラーや異変であっても放置せずに
チームへ共有する

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

バックアップはあったけど…

○概要

搾乳牛の名前や体重、乳量を管理している酪農システムがサイバー攻撃によりデータが暗号化されて制御できなくなった。攻撃者は、暗号の解除に約150万円を要求。被害者は支払いを拒否し、バックアップからデータを復旧しようとしたが、1年前のデータしか残っていなかった。システムの停止で牛の適正な管理ができず、一頭の牛がなくなってしまった悲しいお話である。

○意識してほしいこと

適切なバックアップを取得しましょう

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

復旧手段の袋小路

○概要

運賃システムを含む鉄道会社のシステムがランサムウェアによる攻撃を受けた。鉄道会社は、攻撃者からの数万ドルの身代金の支払要求に応じず、バックアップを用いて復旧する手段を選択した。しかし、バックアップデータも暗号化されていたため、システム復旧まで数日間の運行を余儀なくされた。

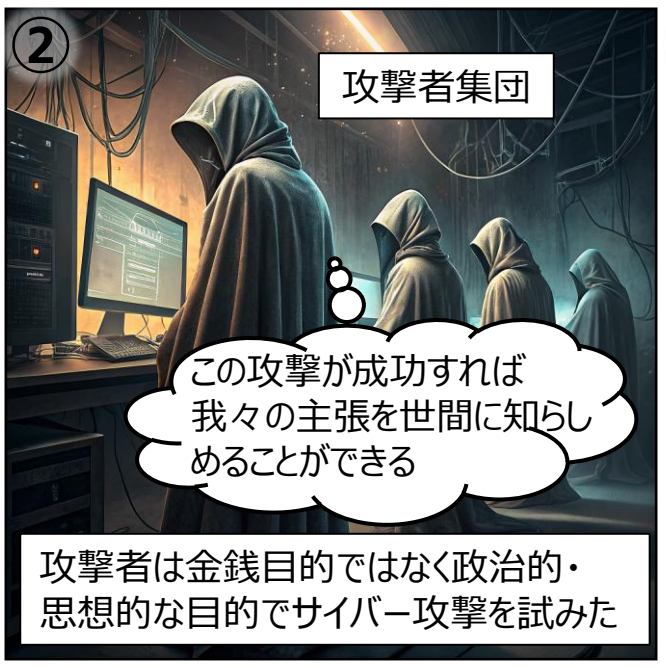
○意識してほしいこと

バックアップデータは**ネットワークから切り離すなど、**
安全な場所に保管しましょう

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

バックアップ　取ってただけじゃ　戻らない



○概要

政治的な思想を持つ攻撃者集団が、ある石油会社に対してサイバー攻撃を行った。攻撃により制御に必要なデータが削除され、システムは停止した。バックアップは日頃から取得していたものの、担当者が復元手順を十分に把握しておらず、復旧に時間を要したことで被害が拡大した。

○意識してほしいこと

バックアップは取得するだけでなく、**復元方法も確認**しておきましょう

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

守れ！空とセキュリティの安全

○概要

ある空港がランサムウェアの被害を受け、システムが暗号化されて航空機の運航が一時停止する事態となった。しかし、バックアップデータによってシステムを復旧し、早期に運航を再開することができた。これは、日ごろからサイバー攻撃に備えた訓練を実施していたことで、インシデント発生時に取るべき行動を組織全体が把握し、迅速に対応できたことが功を奏したものである。

○意識してほしいこと

サイバー攻撃される前提で、備えておくことが大切です

備考

※本漫画は実際のサイバー攻撃を参考にし、画像はAIで作成しています。

本資料に関する注意事項

- 本資料の内容は、独立行政法人情報処理推進機構(IPA)および産業サイバーセキュリティセンター(ICSCoE)の公式見解を示すものではなく、プロジェクトチームの見解に基づいています。

- 記載内容には、技術的あるいは表現上の誤りが含まれている可能性があり、正確性・完全性について保証するものではありません。

- 本資料は、特定の組織、製品、サービス、規格などを推奨・非難する意図を含むものではありません。

- 本資料の利用に起因するいかなる損害についても作成者および監修者は責任を負いません。

- 技術の進展や新たな脅威の出現に伴い、利用できなくなることがあります。

- 画像生成には下記サービスを利用しています。
  - ChatGPT(OpenAI)
  - Recraft

AIで「すりコミッ！」完全版

作成者　OT現場に「サイバー攻撃」の意識をすりこみたい