サイバーセキュリティセミナー

埼玉県警察本部生活安全部
サイバー局サイバー対策課

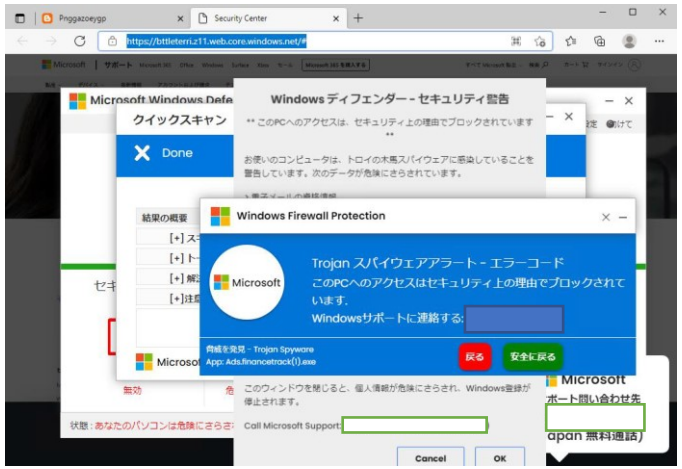
ロマンス詐欺

出会い系サイトやマッチングアプリ、
ＳＮＳ等で出会い、恋愛感情
を抱いた相手から、海外サイトでの
投資などを持ち掛けられる
ロマンス投資詐欺。
はじめは投資とは違う話をして交流
を深め、安心させようとします。
写真や身分証も、偽造されていたり
他人のものを示して騙そうとします。

アジェンダ

サポート詐欺

　ウイルスに感染したと勘違いさせて、パソコン修理費として金銭（サポート料金）をだまし取る詐欺。



ランサムウェア

　データを暗号化して、身代金を要求するウイルス。
　暗号化するだけでなく、データを窃取し、公開すると脅す「二重脅迫」も発生。

メールの危険性

フィッシング詐欺やコンピュータウイルスの感染など、様々なリスクにつながるメール。
何にきを

USBメモリの危険性

ＵＳＢメモリによる情報漏洩の危険性、サイバー犯罪の手口など様々なリスクに直結している。

サポート詐欺とは・・・

インターネット閲覧中、突然「ウイルスに感染した」等と偽の警告画面を表示させ、問題を解決するために遠隔操作ソフトのダウンロードやサポート契約の名目で料金をだまし取ろうとする詐欺の手口です。

しなければなりません すぐにエンジニアが案内してくれます 電話による削除プロセス, だから私たちのエンジニア ウィンドウズ 疑わしい活動のために禁止されています。あなたは私達に連絡しなければなりません すぐにエンジニアが案内してくれます 電話による削除プロセス 5分以内にお電話ください, um コンピュータの完全な誤動作を避けるため.

ティブ化する

スキャナー

分析

WindowsDefender-セキュリティ警告

App: Ads.fiancetrack(2).dll

検出された脅威：トロイの木馬スパイウェア

不審なアクティビティが原因でWindowsがブロックされました.

テクニカルサポートに連絡する: 050-

わかった

絶対に電話しない

アボート

わかった

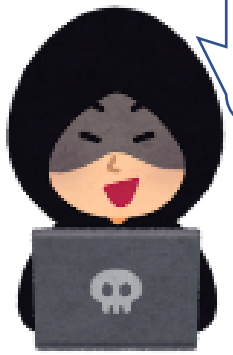
ウイルスなどを阻止します. プレミ

Get suppo

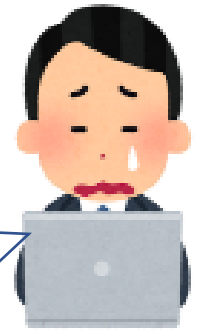
CONTACT US

サポート詐欺とは・・・

表示された電話番号に電話すると・・・



パソコンが感染してマス。今からリモートで修理してあげマス。
コンビニでウェブマネーカードで買って支払ってくだサイ。



職場のパソコンでウイルス感染したなんて、上司や同僚にはとても言えない。自分のお金で解決できるなら、それで済まそう。

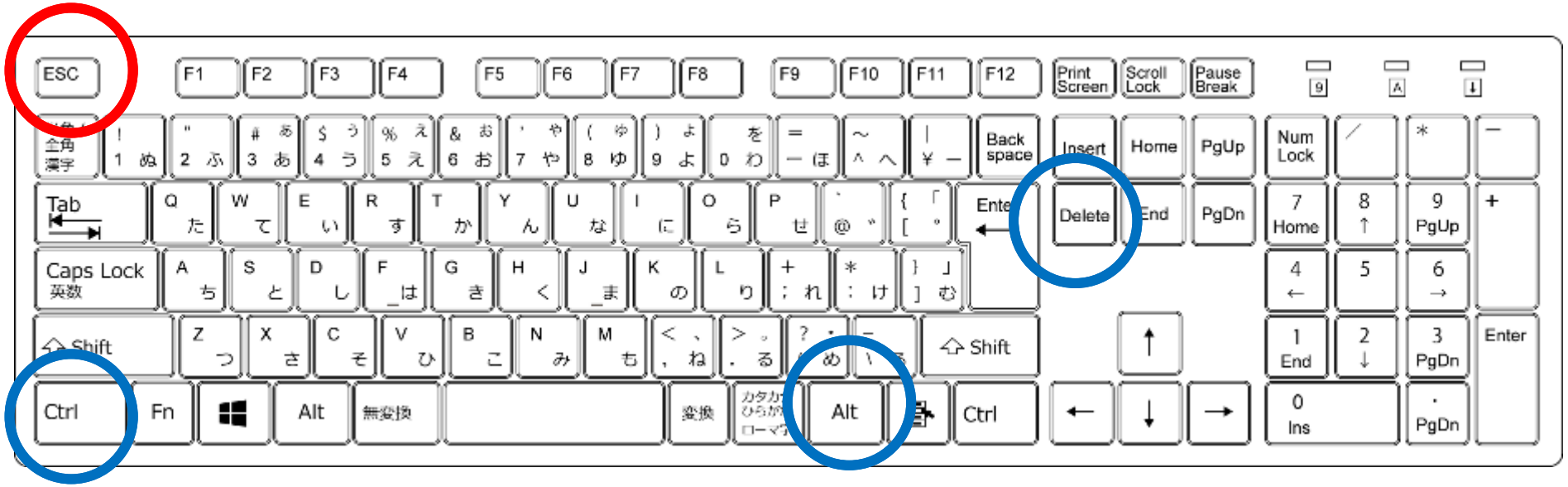
感染しているなんて真っ赤な嘘です！

サポート詐欺サイトの消し方

全画面表示されてしまったら**ESCキー**を押す、又は長押しで通常のサイズに戻せることがあります。

通常の画面に戻ったら、詐欺サイトを消してください。

それでもダメな場合は、**Ctrlキー、Altキー、Delキー**を押してタスクマネージャーを起動してブラウザを消すか、再起動。



企業を狙う「ランサムウェア」

　ランサムウェアとは身代金を意味する「Ransom」と「Software」を組み合わせた造語
　ファイルを暗号化し利用不可能な状態にしたうえで、そのファイルを元に戻すことと引き換えに金銭・暗号資産（身代金）を要求するマルウェア。
　データを暗号化する前にデータを盗み出し、データを戻すことを名目に金銭を要求し、さらにデータを公開することを名目に金銭を要求し、脅迫する。（二重恐喝）

事例に学ぶ　セキュリティ対策

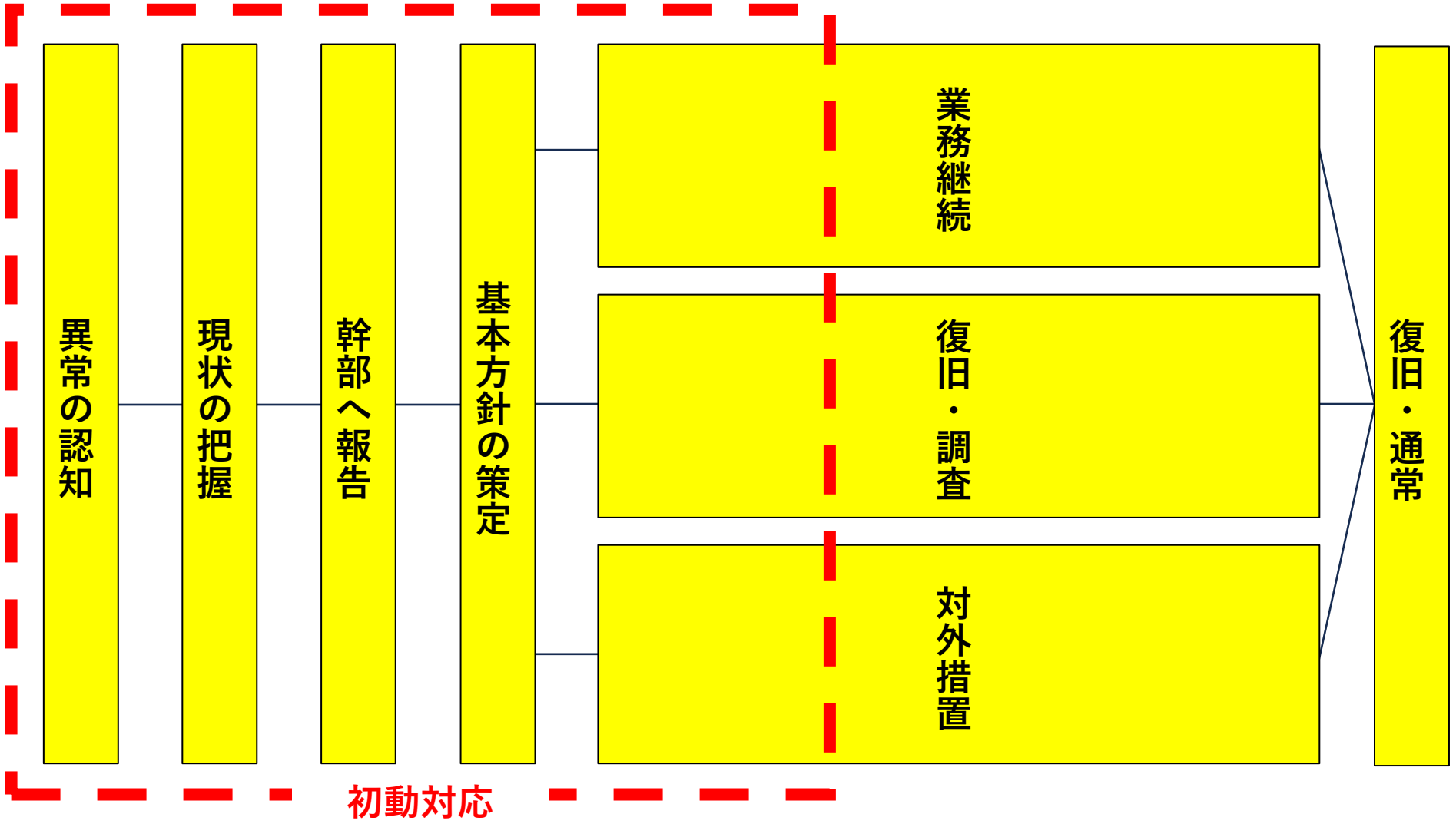
A病院	B病院	C診療所
復旧費用	復旧費用	復旧費用
約5,000万円	約7,000万円	数千万円
内訳	内訳	内訳
データ復旧 新システム購入2,500万円 外注業者費用 人件費　　500万円 コールセンター 弁護士費用　　2,000万円	調査費用　　数百万円 データ復旧　5,000万円 人件費　　2,000万円	フォレンジック費用 システム再構築 データ復元費用 フルスキャン、再設定 残業代等
サイバー保険	サイバー保険	サイバー保険
個人情報漏洩対策費 2,000万円	補償上限　1,000万円	加入無し

出典　日医総研リサーチレポート No.136

犯罪者は常に弱点をサーチ
企業規模、業種関係なく攻撃

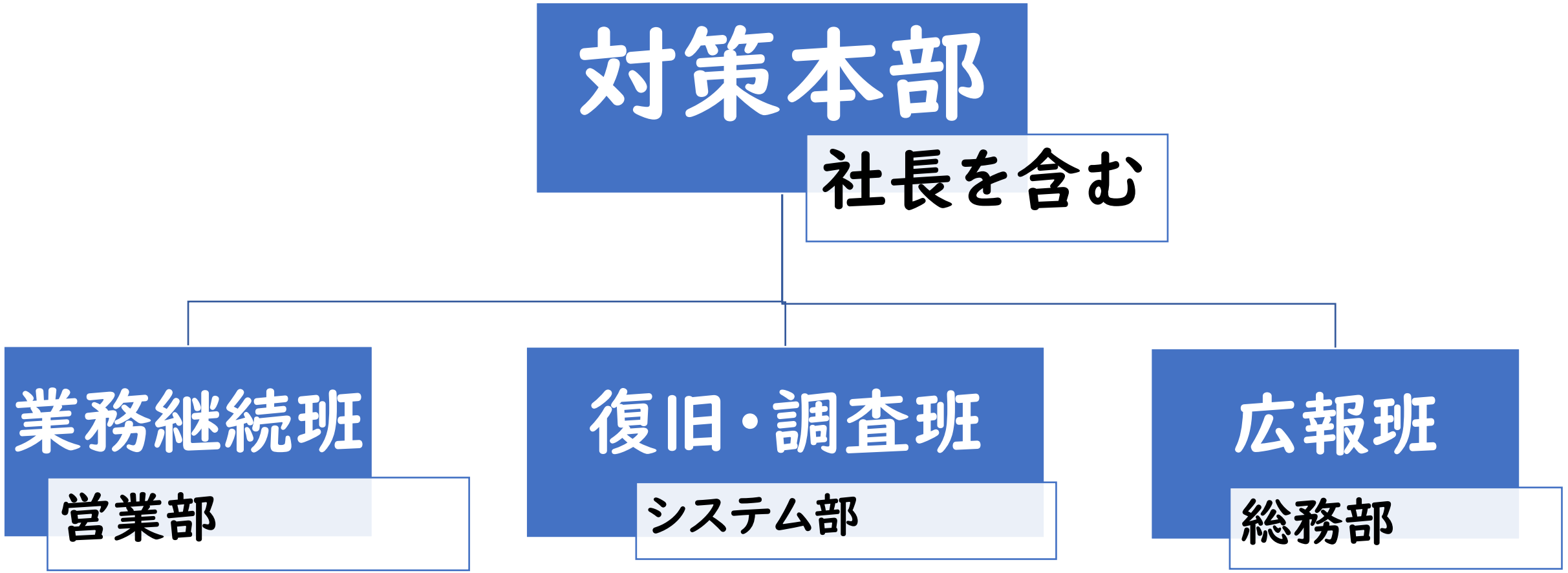
狙われている企業はどこか？という話題になりやすいですが、犯人は常にセキュリティに弱点がないか調査して攻撃をしているため、全ての企業にサイバーリスクは潜んでいると言えます。自分の企業は大丈夫と思い込むことは大変危険です！

サイバー犯罪被害を受けた際の流れ



報告・基本方針の策定

あらかじめ体制を決めていくことが大切



サイバー攻撃を受けた場合には・・・

被害の最小化

業務継続

復旧

感染端末の対処

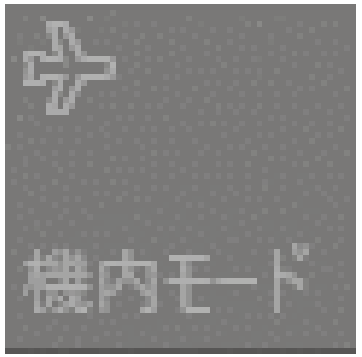
ウイルスに感染した
パソコン・・・
どのように対処
すれば良いか？

感染端末の対処

○ ウイルス感染したPCを発見した時の措置

1．LANケーブルを抜く

2．機内モードにする



3．システムの担当部署に速報する

4．シャットダウン・再起動はしない！！

フィッシング（Phishing）

偽の電子メールの例

フィッシング（Phishing）

フィッシングメールの例

●●銀行
To: 自分
9月10日　詳細を表示

【重要】カスタ・ーセンターからのご案内

平素は、●●銀行をご愛顧賜り誠にありがとうございます。
当社からの重要なご案内をお送りいたしますので、
下記内容をご確認いただきますよう、何卒お願い申し上げます。
ただいま、お客様からの変更処理に基づいて会員登録情報が変更されました。
万が一、本メールの内容に覚えがない場合には以下までお問合せください。

https://www.******-bank.card.co.jp/e-navi/members/information/customer/index69872

*このメールはお客様の会員登録の情報が変更されたことをお知らせする重要なご連絡です。

フィッシング詐欺被害に遭わないために

メールのリンクにご注意を!!

- メール本文に記載されたURLは
安易に開かない。

検索結果にご用心!!

- 検索からも偽サイトに！！
公式アプリの入手、ブックマークを！

ＵＳＢの危険性

・ＵＳＢメモリの４つの心掛け

・なくさない！

・パスワードをちゃんとかける！

・安易に差さない！

・**なくさない！**

ＵＳＢの危険性

ＵＳＢメモリ紛失事案

関西地方の某市において、全市民46万人分の個人情報が入ったＵＳＢメモリを紛失。

データ移管作業を行う委託先の従業員がＵＳＢメモリにデータを保存してカバンに入れて持ち出した。

作業完了後、ＵＳＢメモリを持ち出したまま飲食店で飲酒し、帰宅後にカバンの紛失に気付いたもの。

会見では、紛失に至った経緯とともに、「英数字13文字のパスワードでロックしている。」と説明。

同市は委託先事業者に対して、3000万円の損害賠償請求した。

ＵＳＢの危険性

ＢａｄＵＳＢ攻撃

コンピュータウイルスを保存したＵＳＢメモリを

・郵送で送りつける

・職場のデスクにそっと置く

などにより、会社のパソコンに対して職員が差し込み、
会社のネットワークにウイルス感染させる攻撃。

2022年１月、米連邦捜査局（ＦＢＩ）が
重要インフラ事業者などに対して注意喚起をしたことで
話題となった。

ＵＳＢ以外の記録媒体も注意

ＨＤＤ（ハードディスク）による情報漏洩

ハードディスクによる情報漏洩

2019年12月、神奈川県庁が不要となったＨＤＤ（３ＴＢ）18個を**初期化した上で、処分業者に引き渡した。**

処分業者の職員が、**同ＨＤＤをインターネットオークションサイトに出品**。落札者がＨＤＤを**データ復元ソフトで復元**したところ、神奈川県庁の公文書が多数確認され流出が発覚した。

ＳＮＳによる情報漏洩

顧客情報を含む写真をＳＮＳに投稿し、流出。

投稿先を誤り、個人情報を含むデータが流出

インシデントの原因
となってしまった人

報告を受けた管理職

対応を迫られる
セキュリティ担当者

ひとりにしない！

ご清聴ありがとうございました

X（旧Twitter）

埼玉県警察本部サイバー対策課
＠ｓｐｐ_ｃｙｂｅｒ

キミに響け！サイバーセキュリティ!!