Change.警察庁も変わりました
～サイバー警察局のお仕事～

2022年７月15日
警察庁サイバー警察局
サイバー企画課　清川敏幸
t.kiyokawa.34.e6@npa.go.jp

自己紹介

- ◆北海道札幌市出身
- ◆民間でプログラマ１０年
- ◆サイバー犯罪捜査１５年
- ◆サイバーセキュリティ対策５年
  （警察職員の指導・教養、中小企業向け広報）
- ◆サイバー防犯対策２年目

本日のアジェンダ

- 警察庁が変わる～28年ぶりの新しい局の誕生
- サイバー警察局のお仕事
- 官民連携事例
- インターネットコミュニティとの連携

警察庁が変わる
28年ぶりの新しい局の誕生

前提知識

警察庁
National Police Agency

警視庁
Metropolitan Police Department

違いを知っていますか？

前提知識

警察庁
National Police Agency

今日はコッチのサイバーのお話

組織改正の内容～旧体制

都道府県警察に対する捜査指導・調整、防犯対策

警察庁の既存部署は捜査権がない

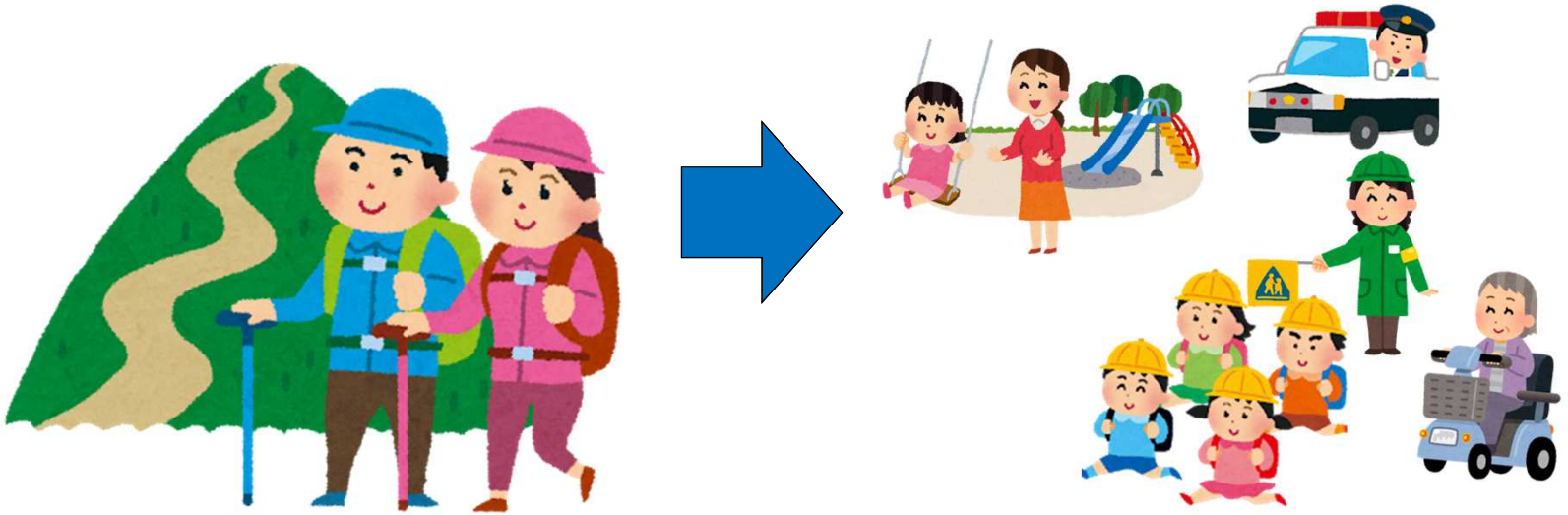
総合調整
人材育成・教養

情報技術の解析

サイバー攻撃対策

組織改正の背景

- コロナ渦を契機とした社会のデジタル化
- サイバー空間の公共空間化
- 悪質なマルウェアを用いた攻撃手法の拡大など、サイバー空間の脅威の拡大



組織改正の背景

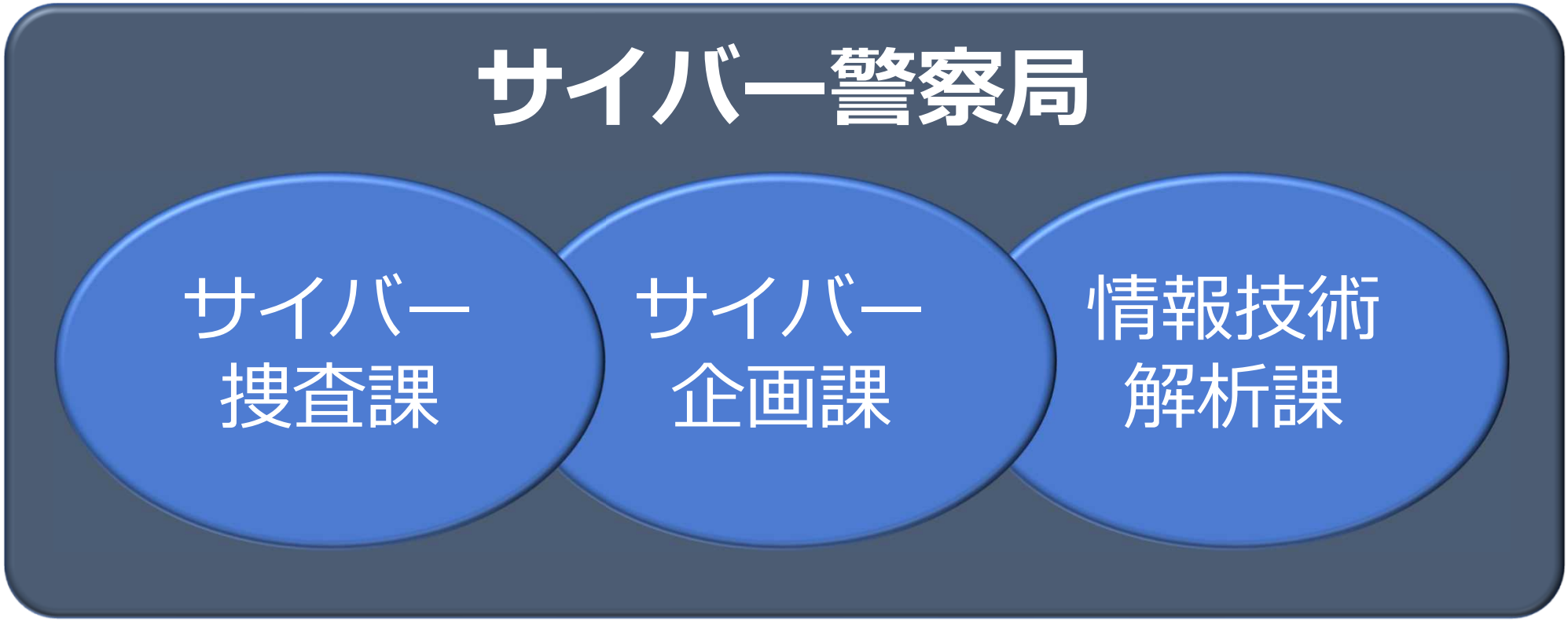
Emotetテイクダウン

2021年１月、ユーロポールは、 オランダ、ドイツ、米国、英国、フランス、リトアニア、カナダ及びウクライナの当局が連携し、Emotetのボットネットを破壊した旨を発表。

【引用元】https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

組織改正の内容～新体制

生活安全、刑事、交通、警備等他部門と緊密に連携し、
サイバー空間・実空間の両者にわたり隙間無く脅威に対処



組織改正の内容～新体制（役割）

- 対策・情報集約・分析
- 捜査（指導・調整）
- 解析
- 人材育成・教養
- 技術的支援

組織改正の内容～新体制

国の捜査機関として【重大サイバー事案】の捜査を推進

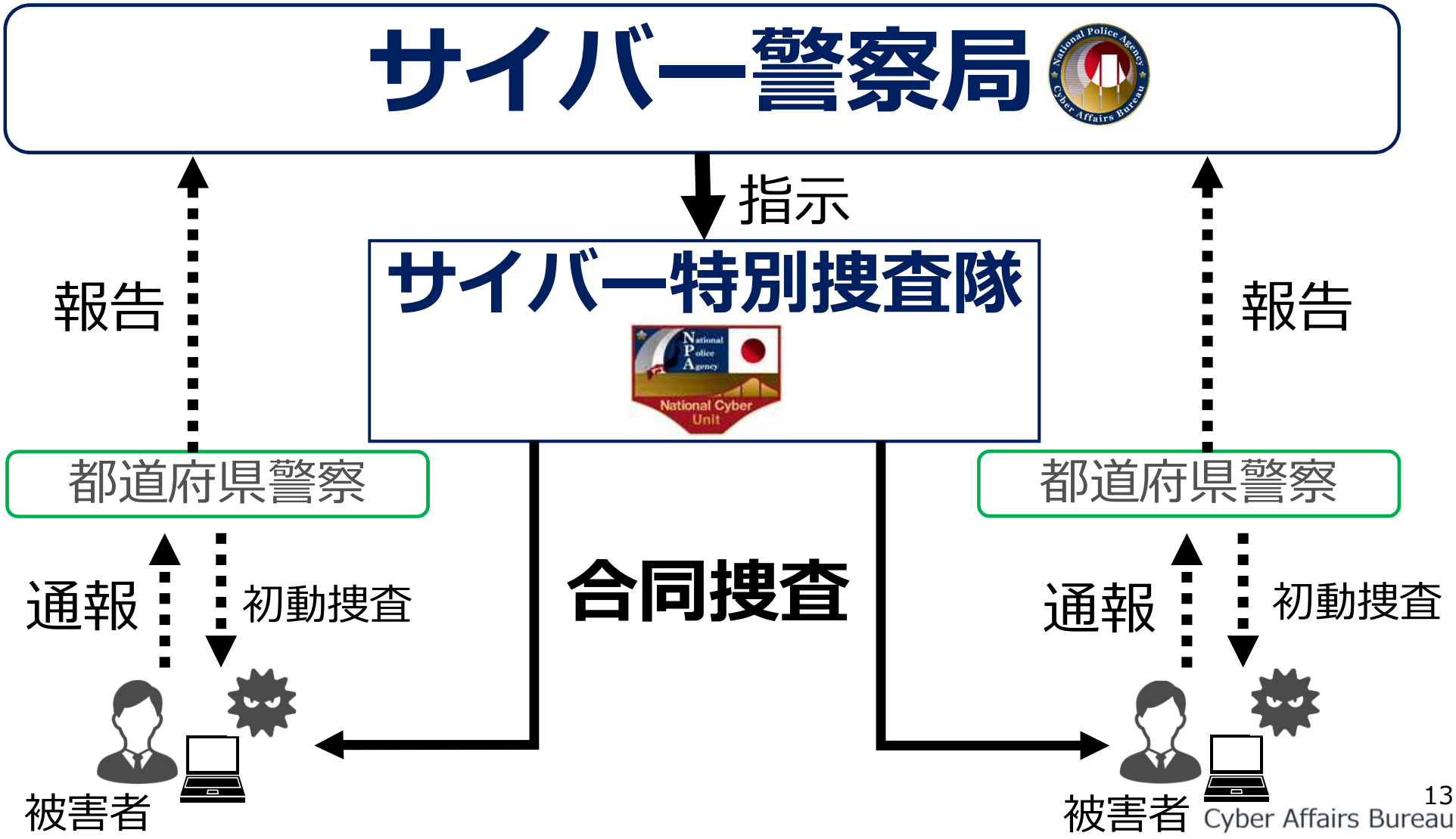
サイバー特別捜査隊

- 重大サイバー事案の捜査
- 国際共同捜査等への積極的な参画

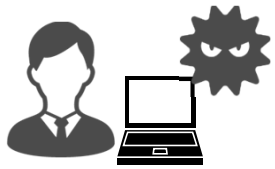
National Police Agency
National Cyber Unit

特別捜査隊には捜査権が付与される

サイバー警察局の役割（事件捜査）

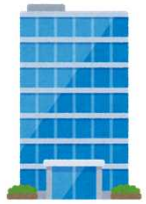


サイバー警察局の役割（情報集約・分析）



被害者（事業者）

都道府県警察



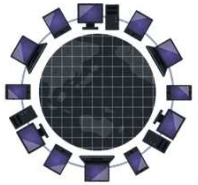
NISC・他省庁

情報

セキュリティベンダ

サイバー警察局

オープンソース



都道府県警察

国民

捜査・広報啓発

これまでの国際捜査（共助）





要請

要請

警察庁
National Police Agency

調整作業

指示

要請


A県警

B県警

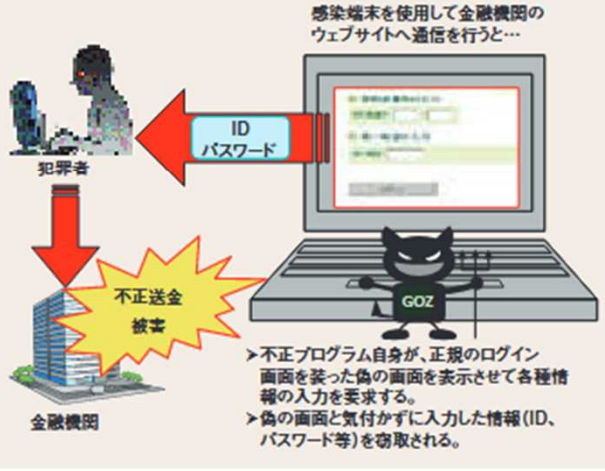
捜査

過去の国際共同オペレーション

コラム 国際的なボットネットのテイクダウン作戦

不正送金事犯に使用されているとみられる不正プログラム「Game Over Zeus」が世界的にまん延した(注2)ことから、26年5月、FBI及びEUROPOL(注3)を中心に、日本を含む協力国の法執行機関が連携して同プログラムに感染した端末の情報を収集し、当該端末[illegible]を通じて当該[illegible]グラムの駆除[illegible]せる「国際的[illegible]ン作戦」を決行

図表3－8 Game Over Zeusの脅威



【引用元】警察庁「平成２７年版警察白書」

広　報　資　料
平成29年3月23日
警　察　庁

インターネットバンキングに係る不正送金の国際的な被害防止対策について

1　概要

インターネットバンキングに係る不正送金事犯に使用されているとみられるウイルスが世界的に蔓延している中、昨年、ドイツ警察が中心となり、関係各国が連携して、コンピュータウイルスを利用したインターネットバンキングに係る不正送金事犯の実行者を検挙する国際的な取組（オペレーションアバランチ）が行われた。

今般、ドイツから、本取組に関し、日本国内のインターネットバンキング利用者のID・パスワード等の情報、コンピュータウイルスの感染端末情報等の提供を受けたことから、関係省庁・団体と連携して、インターネットバンキング利用者、感染端末利用者等に対し、被害拡大防止のための注意喚起を行うもの。

【引用元】警察庁ホームページ

これからの国際捜査（共同捜査）

警察庁 サイバー捜査専門職員をユーロポールに初派遣へ

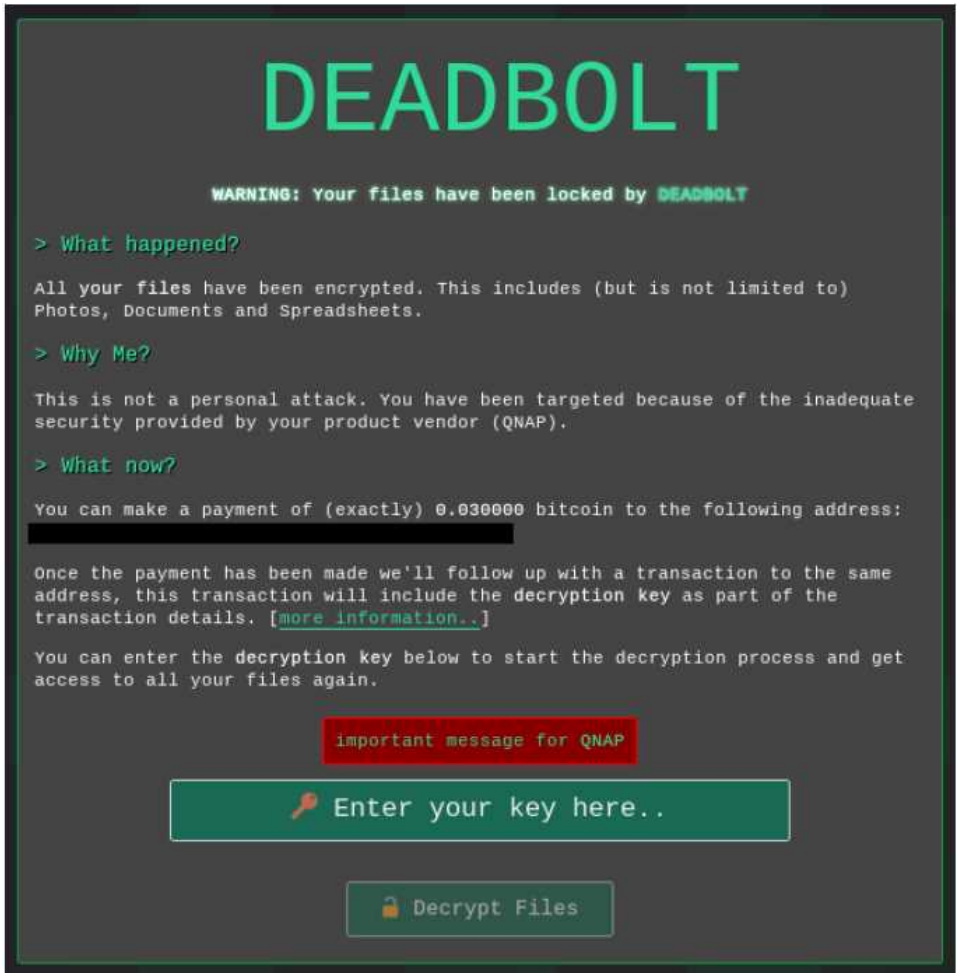
2022年5月24日 5時35分

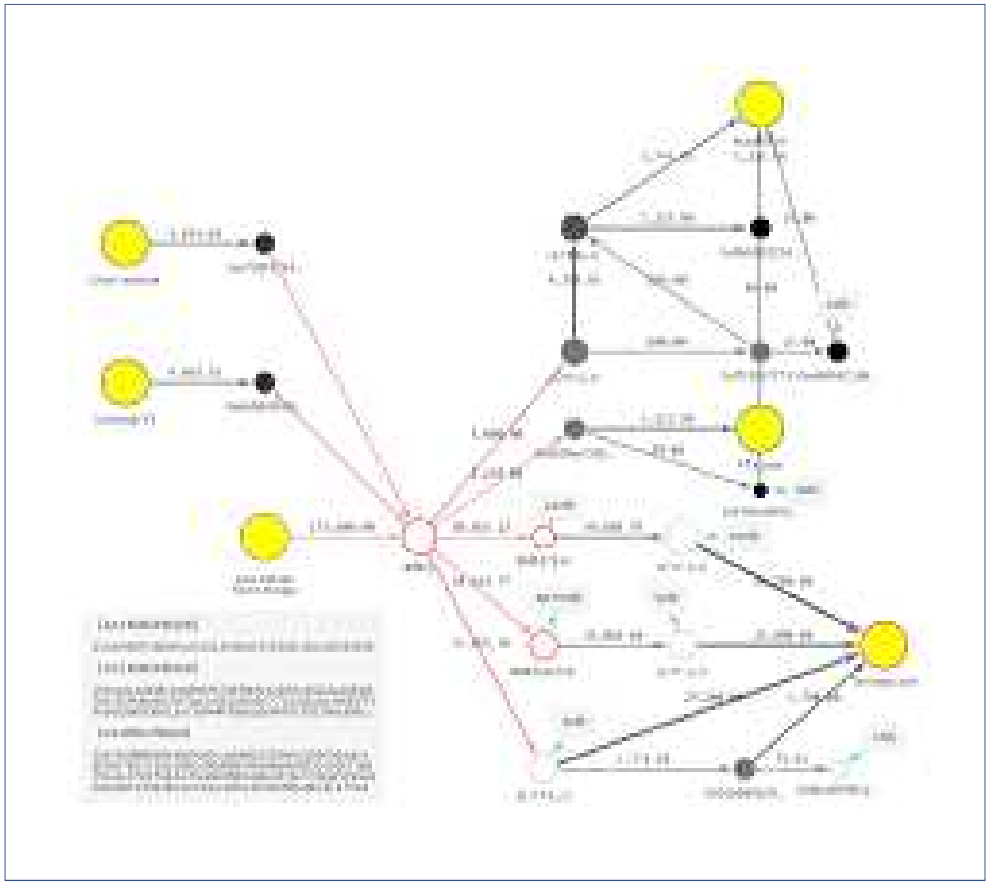
サイバー犯罪が深刻化していることを受けて、警察庁はサイバー捜査を専門とする職員をユーロポール＝ヨーロッパ刑事警察機構に初めて派遣し、世界各国との連携を強化することにしています。

【引用元】ＮＨＫ ＮＥＷＳ ＷＥＢ　２０２２年5月２４日

サイバー警察局のお仕事

情報集約・分析
手口の把握





情報集約・分析

手口の把握

Emotetの解析結果について

2022年6月9日

警察庁

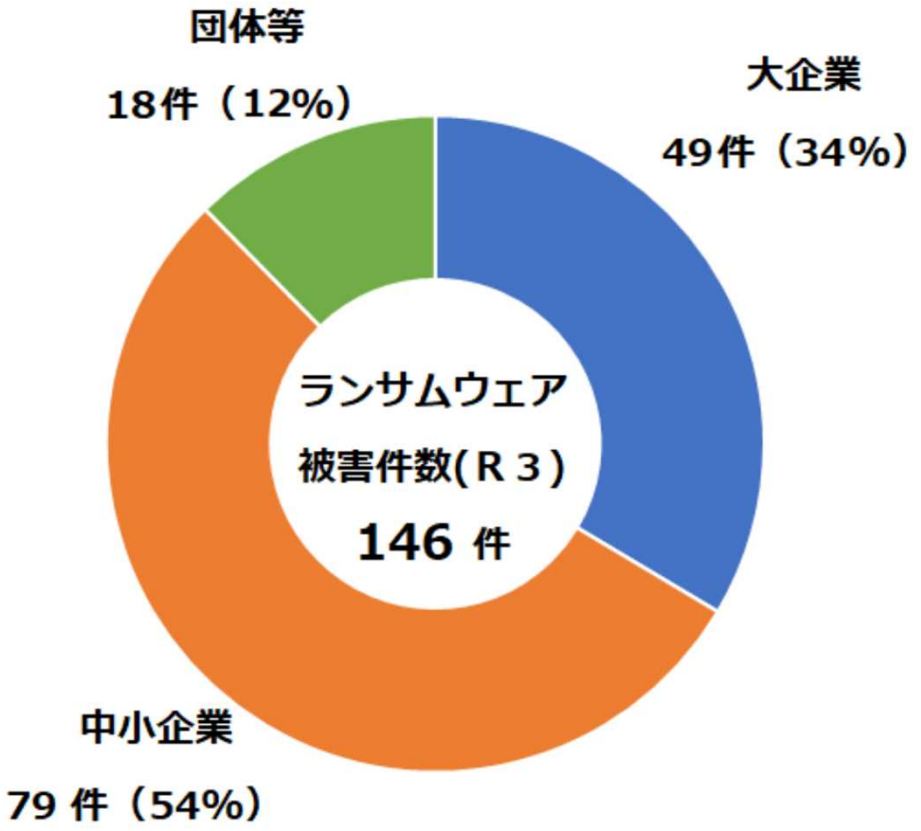
新機能の確認（2022年6月9日）

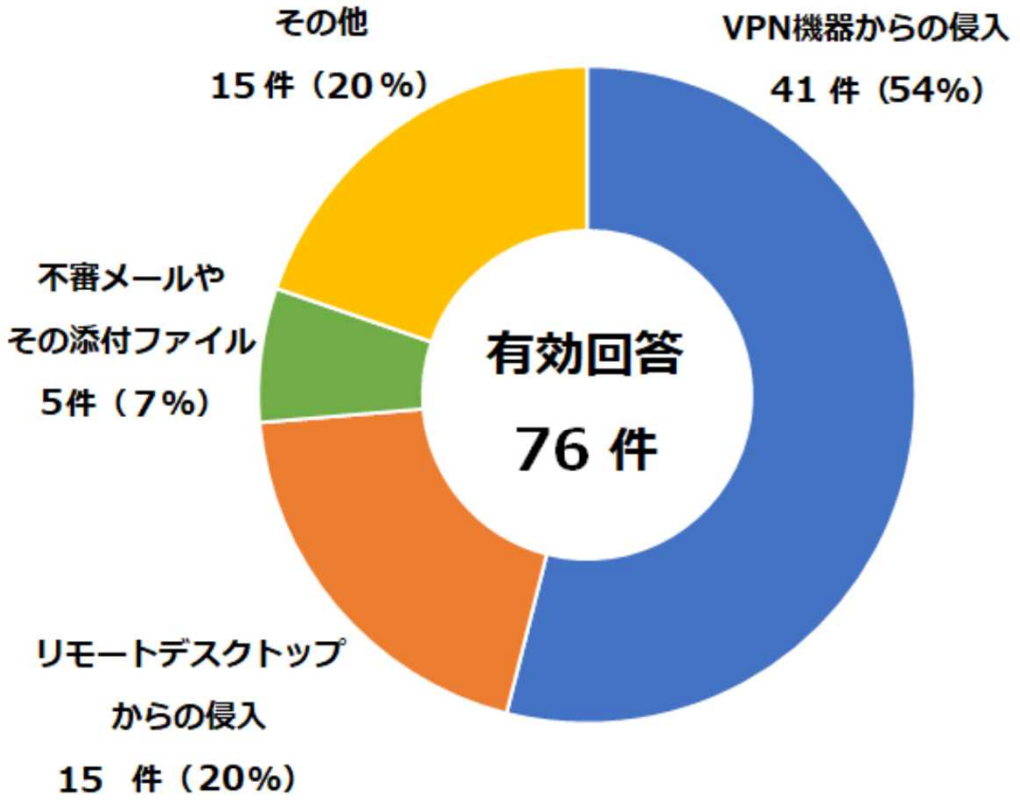
ウェブブラウザ「Google Chrome」に保存されたクレジットカード番号や名義人氏名、カード有効期限を盗み、外部に送信する機能が追加されたことを確認しました。Google Chromeでは個人情報を暗号化して安全に保存していますが、Emotetの新機能は暗号データを元に戻すための鍵も同時に盗み出すため、Emotetに感染すると、お使いのクレジットカード情報が第三者に知られるおそれがあります。

【引用元】警察庁ホームページ

情報集約・分析

ランサム被害状況

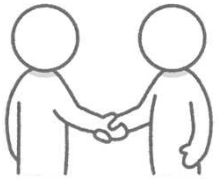




注　図中の割合は小数点第１位以下を四捨五入しているため、総計が必ずしも100にならない。

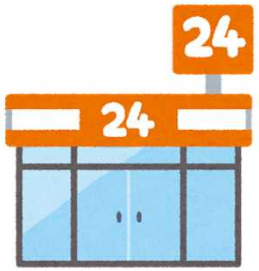
対策（官民連携）

連携（協定等）



人事交流

情報共有



対策（広報啓発）

サイバー犯罪被害に係る企業・団体を対象としたアンケート調査結果及び対策

過去１年以内に受けたことのある被害

ランサムウェア被害が倍増

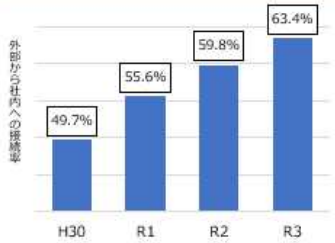
R2			R3		
1位	メール不正中継	12.8%	**1位**	**ランサムウェア**	**22.1%**
2位	ランサムウェア	11.9%	2位	メール不正中継	15.8%
3位	情報流出	6.4%	3位	情報流出	12.6%

※ 被害を受けた団体における割合

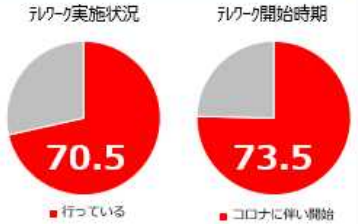
※ ランサムウェアとは、感染すると端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価として金銭を要求する不正プログラム

外部から社内への接続・テレワーク

業務上の外部からの接続が急増



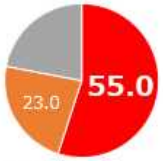
新型コロナ拡大による開始は７割以上



セキュリティ対策

VPNの導入が増加

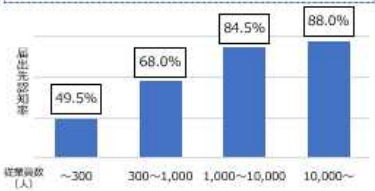
ランサム感染経路は半数以上がVPN



「令和３年上半期サイバー空間脅威情勢」（警察庁）抜粋

被害発生時の届出先の認知状況等

中小企業の認知率が低い



最も多い届出先は「警察」

1位 警察

2位 情報処理推進機構

3位 監督官庁

被害に遭わないために

OSなどの脆弱性対策

OSやアプリケーションソフト、VPN機器などに脆弱性があるとマルウェアに感染したりネットワークに侵入されるおそれがあります。

- OS・ソフトウェアの更新
- ウイルス対策ソフトの更新
- ネットワーク機器ソフトウェアの更新

認証情報の適切な管理

VPN機器やリモート・デスクトップ・サービスなどの認証パスワードが脆弱な場合、ネットワークに侵入されるおそれがあります。

- パスワード長は一定以上に
- 異動で使わなくなったIDは削除
- IDを複数ユーザで共有しない

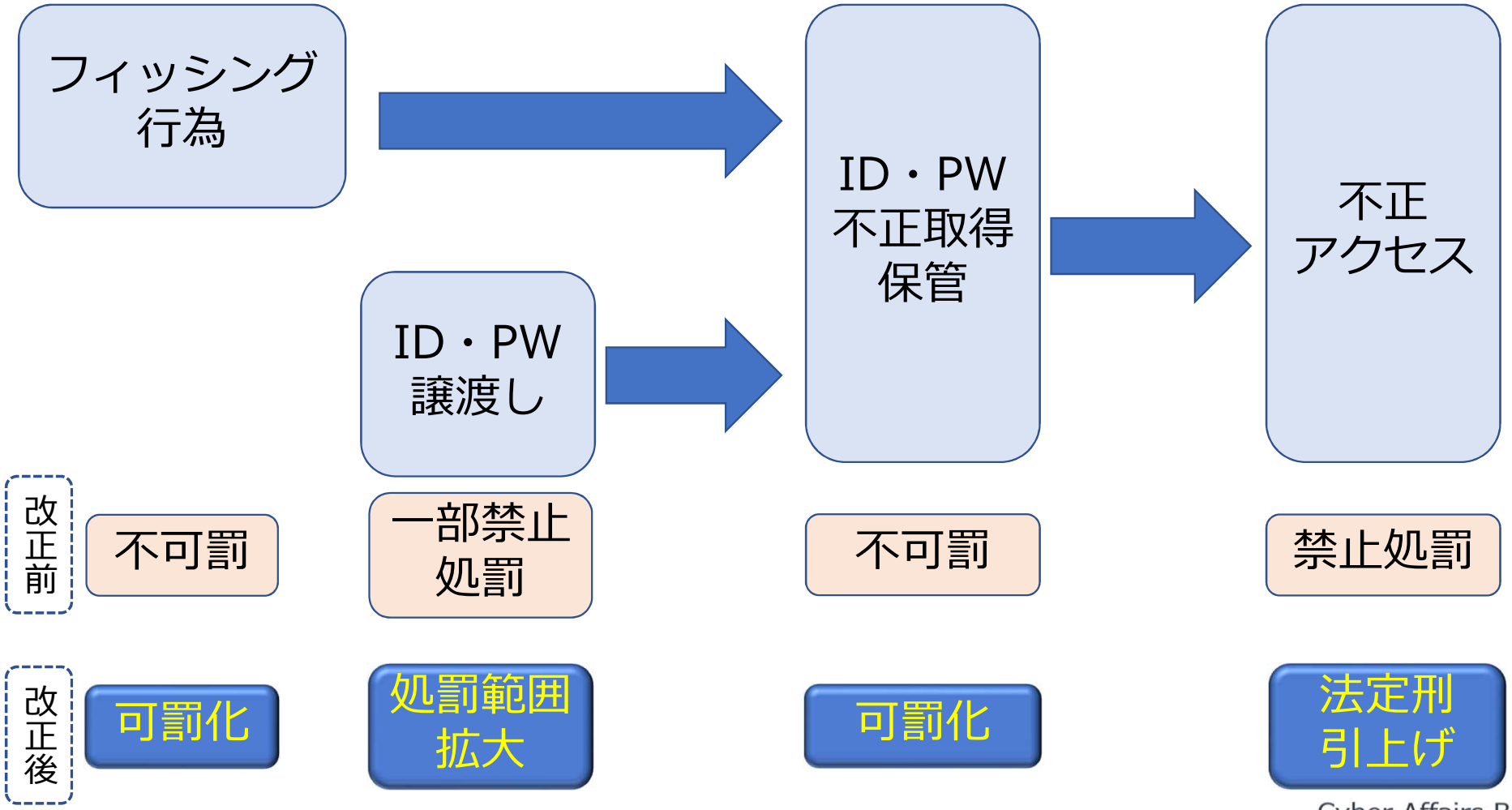
⚠被害に遭ってしまったら
警察へ通報

より詳しい被害防止対策は警察庁「ランサムウェア被害防止対策ページ」→
https://www.npa.go.jp/cyber/ransom/index.html

警察庁 National Police Agency
都道府県警察本部のサイバー犯罪相談窓口はこちら →
https://www.npa.go.jp/cyber/soudan.html

法改正

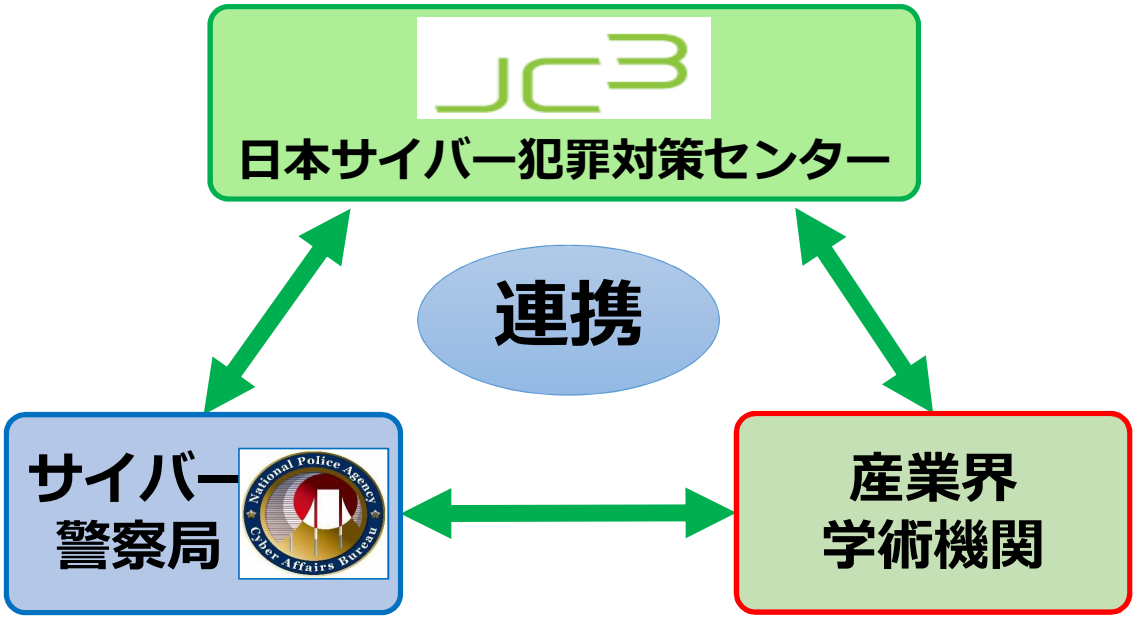
平成24年不正アクセス行為の禁止等に関する法律改正



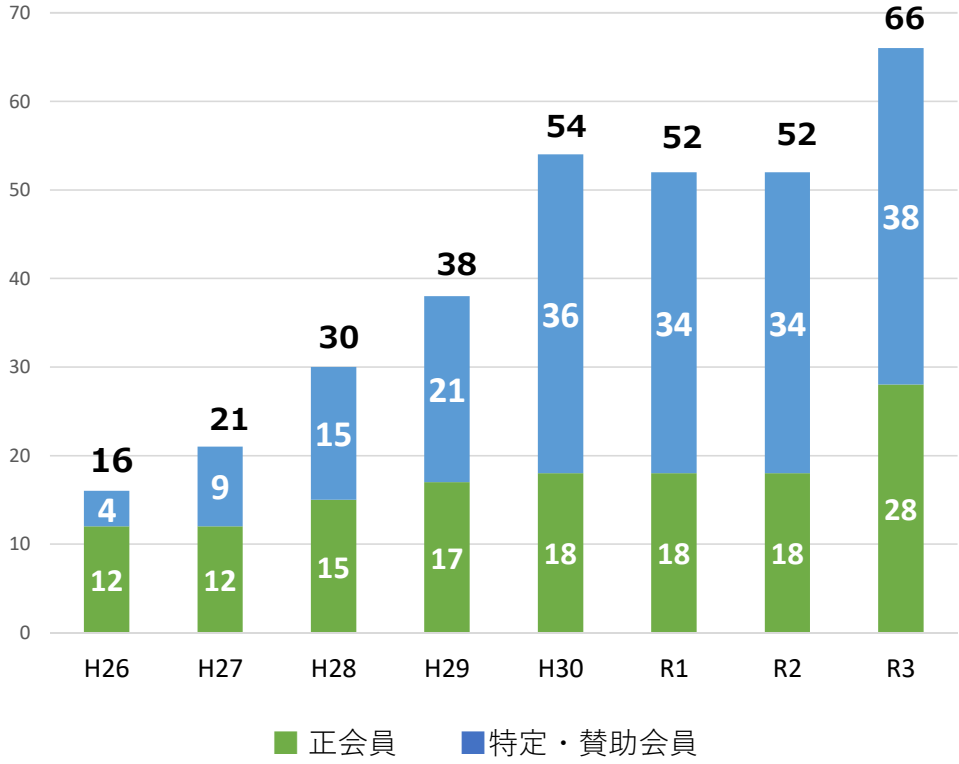
官民連携事例

日本サイバー犯罪対策センター

ＪＣ３を軸とした官民連携



ＪＣ３会員数の推移



サイバー空間の安全・安心のため、**官民連携を一層推進**

不正決済対策

捜査上把握した
手口を分析

捜査

不正決済

業界団体

情報

情報共有
対策を協議

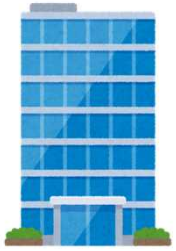
情報

被害状況の分析

被害事業者

システムの改善

情報共有



所管省庁

注意喚起、ガイドライン策定等

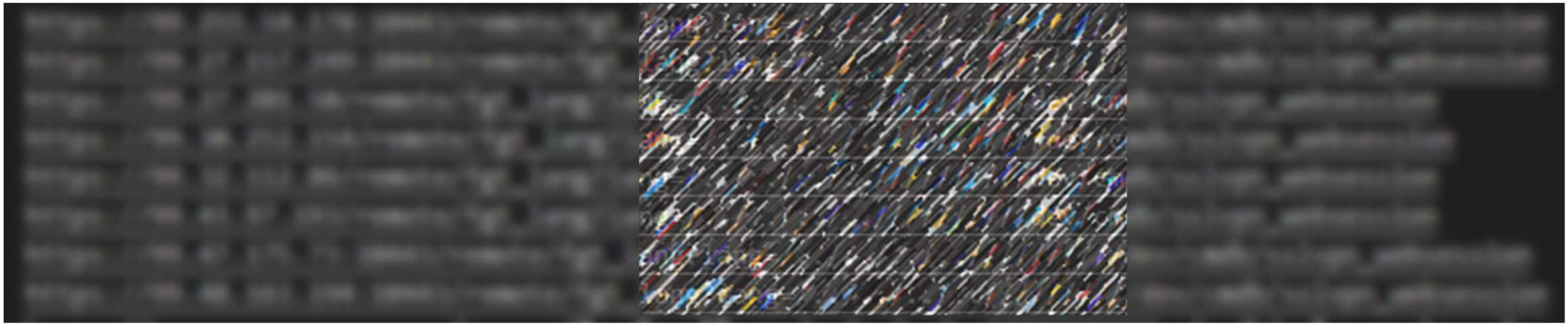
その他事業者

脆弱性対策

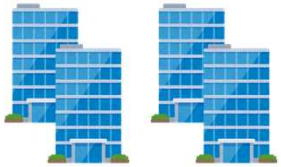
CVE-2018-13379 Detail

Current Description

An Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal") in Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.3 to 5.6.7 and 5.4.6 to 5.4.12 and FortiProxy 2.0.0, 1.2.0 to 1.2.8, 1.1.0 to 1.1.6, 1.0.0 to 1.0.7 under SSL VPN web portal allows an unauthenticated attacker to download system files via special crafted HTTP resource requests.



注意喚起



機器を使用する事業者

ＳＭＳ認証代行対策

MVNO委員会：一般社団法人テレコムサービス協会の委員会

捜査上把握した
手口を分析

本人確認を要請

取締り強化を指示

ＭＶＮＯ委員会

携帯事業者

契約時の本人確認を申し合わせ

都道府県警察

積極的な事件化

ＳＭＳ認証代行対策

2021 年 1 月 29 日
一般社団法人テレコムサービス協会
MVNO 委員会

データ通信契約申込み受付時おける本人確認手続きに関する申合せ書

2021 年 1 月 29 日の一般社団法人テレコムサービス協会 MVNO 委員会において、MVNO 委員会に加盟の MVNO は、データ通信契約申込み受付時における本人確認手続きに関し、下記の通り実施することを申し合わせた。

記

1. 本人確認方法
原則、「携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律（平成十七年法律第三十一号）」と同一の本人確認方法によりデータ通信契約の受付を行うこと

2. 対象役務
ＳＭＳ機能付きデータ通信契約※
※ＳＭＳ機能が付与されていないデータ通信契約を対象役務とすることついて、今後の社会環境の変化及び不正利用の発生状況等を踏まえ、引き続き検討するものとする。

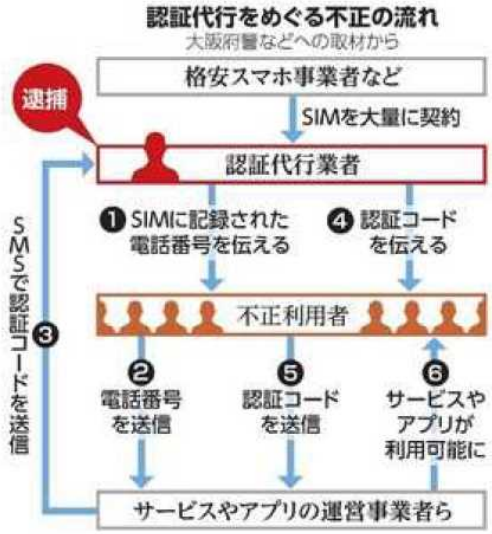
【引用元】一般社団法人テレコムサービス協会ホームページ

2段階認証コード提供容疑　「代行業者」を逮捕　3600回代行か

有料会員記事

河野光汰、華野優気　2021年12月16日 14時30分

シェア　ツイート list　ブックマーク 17　メール　印刷



認証代行をめぐる不正の流れ

偽名で入手したSIMカードを使い、電話番号や 本人確認 のための「2段階認証」用のコードを提供したなどとして、 大阪府警 は 東京都 墨田区 の無職、坂本竜彦容疑者（39）を私 電磁的記録 不正作出・同供用の疑いで逮捕し、16日発表した。府警は、SNSアカウント開設に必要な2段階認証を代行する「認証代行業者」とみている。

サイバー犯罪 対策課によると、坂本容疑者は2019年8月ごろから21年7月ごろにかけ、偽名を使って格安 スマホ 業者など

【引用元】朝日デジタル　２０２１年１２月１６日

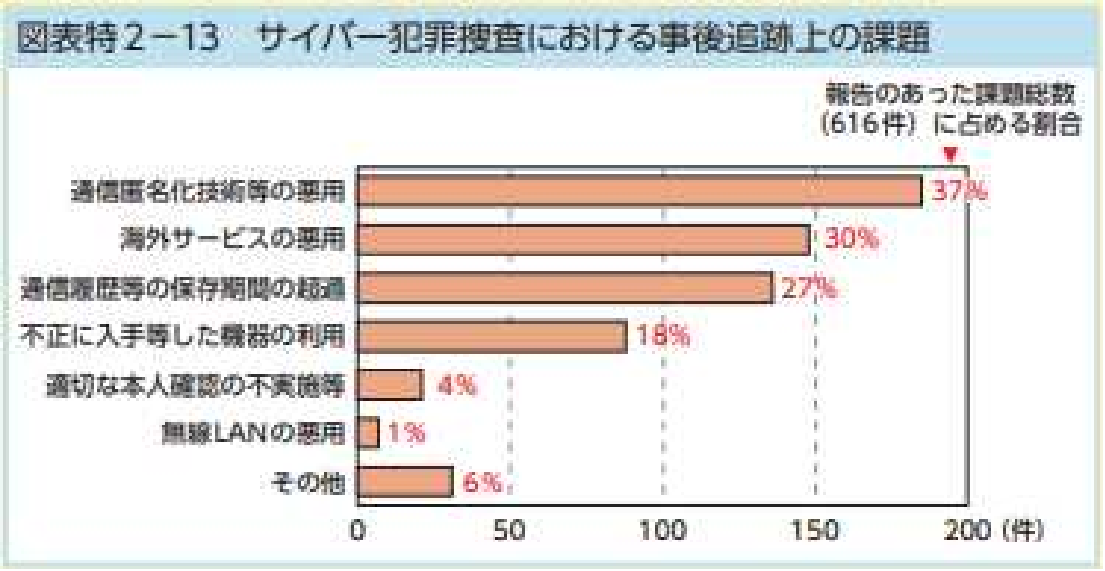
インターネット
コミュニティとの連携

トレーサビリティの確保（警察としてはなるべく広く）

- 契約者の本人確認
  データ通信ＳＩＭ
- 通信履歴の保存
  公衆無線ＬＡＮ
  ＩＰｖ６⇔ＩＰｖ４
  ポート番号
- 適切な保存期間の設定

電気通信事業における
個人情報保護に関するガイドライン

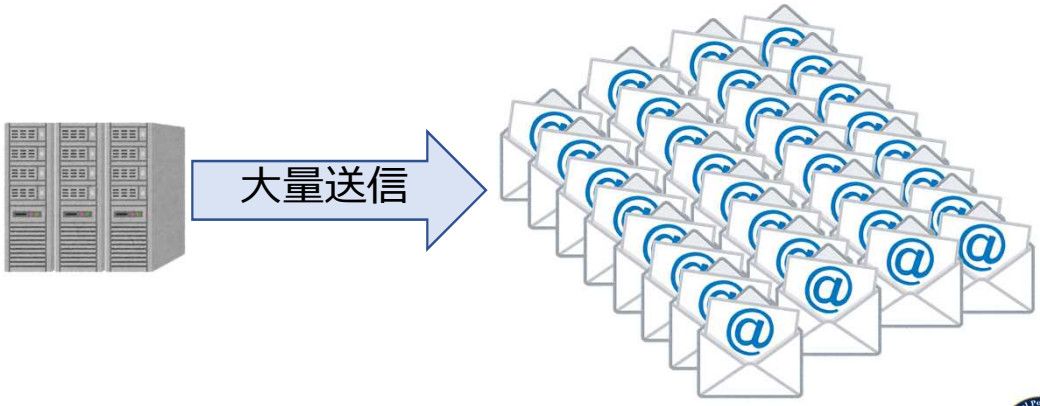
業務の遂行上必要な場合に限り、
記録することができる



【引用元】警察庁「令和３年版警察白書」

不正の排除（国民が被害に遭わないように）

- ✓ 不正サイト対策
  - フィッシングサイト
- ✓ 不正ドメイン対策
  - フィッシング用ドメイン
  - 迷惑メール送信用ドメイン
- ✓ 不正ホスティング対策
  - メールの不正送信・中継
- ✓ 不正ＳＭＳ対策
  - 国外からのＳＭＳ



製品・システムの管理（プロが責任を持って）

- 脆弱性の把握
  開発した製品やシステム、運用（提供）中のシステム
- アップデート実行
- ユーザ管理の徹底
  脆弱性発見時の通知の可能性

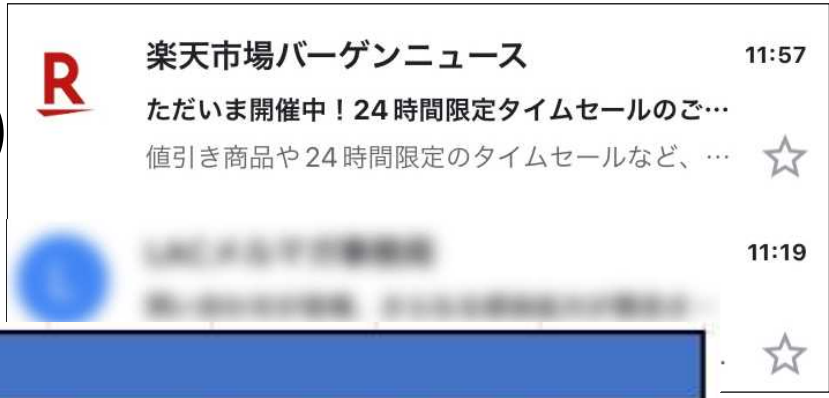
徳島県つるぎ町立半田病院
サイバー攻撃報告書より

報告書によると、サーバーが感染した身代金要求型ウイルス「ランサムウエア」は、病院の外部からシステムに接続する際に使うVPN（仮想専用線）の脆弱性を悪用し、侵入したとみられる。
VPNの提供元は19年に脆弱性について注意喚起したが、システムの提供企業側は病院に説明していなかった。古い電子カルテシステムを安定的に運用するため、ウイルス対策ソフトを稼働させない設定にしていたことも判明した。

【引用元】 ２０２２年６月７日　日本経済新聞Ｗｅｂ版

守るべきものは何か、どう守るのか（を教えてあげて）

- ◆情報資産
  守るべき情報資産の把握
  必要なセキュリティシステム導入
- ◆顧客
  送信ドメイン認証（DMARCなど）
  ブランドアイコン（BIMIなど）



	2021年									
	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月
なりすまし合計	14,216	7,783	10,662	14,462	14,307	16,779	18,784	35,395	29,335	26,469
フィッシング報告数	30,534	21,250	29,566	29,059	25,532	30,560	34,787	53,177	49,953	48,740
なりすましの全体比	46.6%	36.6%	36.1%	49.8%	56.0%	54.9%	54.0%	66.6%	58.7%	54.3%

【引用元】 JANOG49フィッシング対策協議会発表資料

エンドユーザ対策（一緒にやりましょう）

- 注意喚起
  専門家の立場でかわりやすく
  技術者として責任をもって
- セキュリティ意識啓発
  様々な機会を捉えて
  様々な年齢層や対象に

メール（SMS）内のURLは
クリックしない

気軽に個人情報を入力しない！

初期パスワードの使用禁止！！

取引先だとしても添付ファイル
には要注意！

OSや機器のソフトウェア
アップデート

セキュリティソフト（製品）の
導入検討

よろしくお願いします