

# サイバー攻撃の動向概論

東洋大学情報連携学部 准教授  
満永 拓邦

# プロフィール

- 名前：満永 拓邦(みつなが たくほう)
- 所属：東洋大学情報連携学部 准教授  
(独)情報処理推進機構 産業サイバーセキュリティセンター 専門委員
- 業務：
  - ・セキュリティに関する情報収集・分析・研究活動
  - ・大学での講義やセミナー等での講演活動
  - ・外部の組織や企業の経営層やシステム管理部門との連携
  - ・セキュリティに関連する書籍やレポートの執筆



Briefing Speaker  
Black Hat Europe 2018  
“Real-Time Detection of Attacks Leveraging  
Domain Administrator Privilege”



「サイバー攻撃からビジネスを守る」  
NTT主版, 監修/共著



「CSIRT」  
NTT主版, 共著

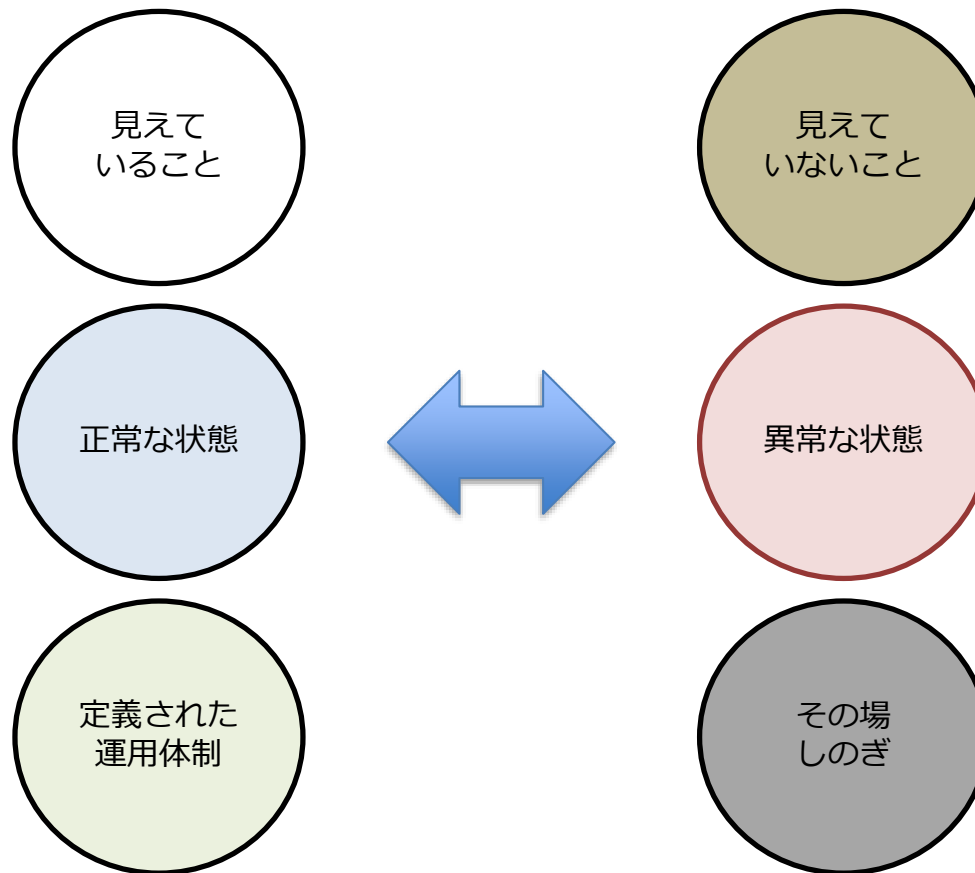
# 期待される研修成果

- この講義は、講義、実機ハンズオン、グループディスカッションを通じて以下の内容を習得することを目指しています
  1. サイバー攻撃の動向
  2. 攻撃手法とその対策（検知、痕跡調査、事前の備え）
- 特にセキュリティ対策が不十分である場合、その状態に気づき、派遣先に改善を提案できるスキルを養成することを目的としています

日常的な運用に加えて、運用改善を提案できる人材に！

# 定常的な運用監視

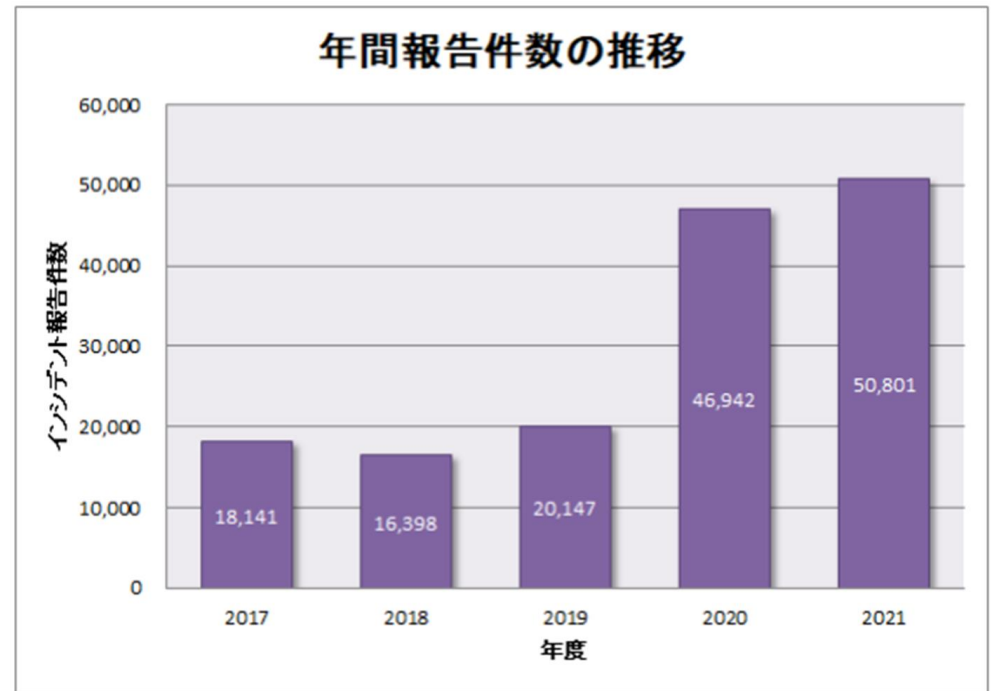
- 「異常」とは「正常ではない」ことを言う
- 具体的な対策に先立って、まず正常な状態が把握・可視化されて、安定的に運用されていることが重要となります



# **サイバーセキュリティを取り巻く現状**

# JPCERT/CCにおける インシデント状況

- JPCERT/CCへの報告  
(Incident Report)
  - 2021年インシデント件数  
**50,801件**



[図 3 : 年間報告件数の推移 (年度比較)]

# インシデント数増加の背景



## ITの社会インフラ化

- ・ 企業活動のIT化
- ・ 電子商取引の発展
- ・ 制御系システムへの利用

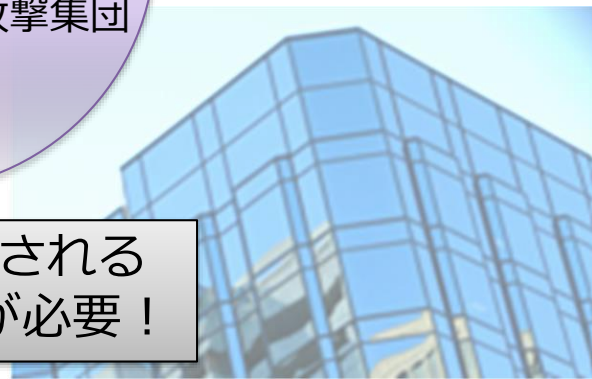


## インターネットの世界的な普及

- ・ ボーダレスの通信
- ・ 物理的な追跡困難性

## 攻撃用インフラの整備

- ・ 攻撃ツールの進歩
- ・ 分業化された攻撃集団



今後、サイバー攻撃の増加が予想されるため、各組織においても対応体制が必要！

# 攻撃者の分類

- 攻撃の目的をもとに攻撃者を分類すると、それぞれの攻撃手法や技術力が異なることが推察できる

	愉快犯/ハクティビスト	金銭目的の攻撃者	標的型攻撃の実行者
攻撃の目的	<ul style="list-style-type: none"> <li>政治的な主張</li> <li>技術力のアピール</li> </ul>	<ul style="list-style-type: none"> <li>金銭の獲得(不正送金)</li> </ul>	<ul style="list-style-type: none"> <li>標的とする組織内の重要情報窃取やシステム破壊</li> </ul>
主な攻撃手法	<ul style="list-style-type: none"> <li>Web サイトに対するDoS</li> <li>政治的な主張を目的とするWeb サイトの改ざん</li> <li>SNS アカウント乗っ取り</li> </ul>	<ul style="list-style-type: none"> <li>マルウェアが添付されたメールの送付</li> <li>Web サイト改ざんによるマルウェアの配布</li> </ul>	<ul style="list-style-type: none"> <li>マルウェアが添付されたメールの送付</li> <li>Web サイト改ざんによるマルウェアの配布 (ただし攻撃対象のみに限定)</li> </ul>
技術力	<div>低</div>		<div>高</div>



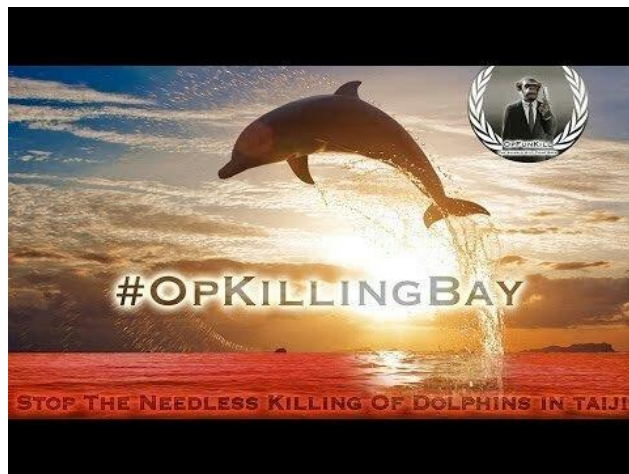
## **攻撃者の分類に基づく攻撃の特徴**

**- 愉快犯/ハクティビストによる攻撃 -**

# ハクティビストによる攻撃例

## #OpKillingBay

- イルカ漁や捕鯨に対する抗議を目的とする活動
- Tweet Storm と呼ばれる Twitter を使用したメッセージの発信が主な活動であるが、アノニマス系の攻撃者により、サイバー攻撃に発展することもある
- 主な対象
  - 捕鯨に関連する自治体
  - 水族館や水族館関連組織
  - 国内の民間企業（捕鯨とは関係なく、注目を浴びる攻撃対象を選定している）



# ハクティビストによる攻撃例

- 2015年10月から国内サイトがDDoS攻撃の対象となり一部のサイトでは、一週間程度サイトが停止する事態となった。
  - イルカ漁、捕鯨とは関係しないサイトであったものの攻撃対象に



画像引用 : <http://japanese.engadget.com/2015/10/28/ascii-jp-anonymous-ddos-1/>

## **攻撃者の分類に基づく攻撃の特徴**

**- 金銭の獲得を目的とした攻撃 -**

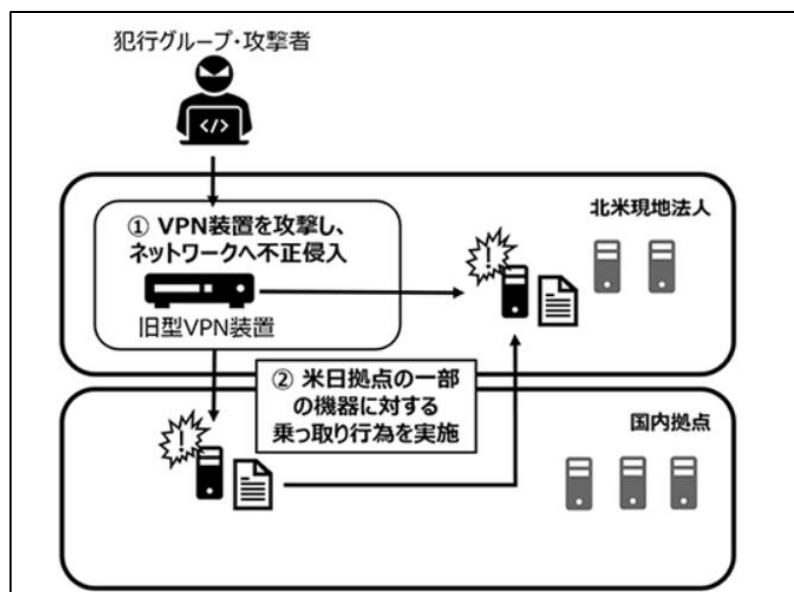
# 攻撃者の分類(再掲)

- 攻撃の目的をもとに攻撃者を分類すると、それぞれの攻撃手法や技術力が異なることが推察できる

	愉快犯/ハクティビスト	金銭目的の攻撃者	標的型攻撃の実行者
攻撃の目的	<ul style="list-style-type: none"><li>政治的な主張</li><li>技術力のアピール</li></ul>	<ul style="list-style-type: none"><li>金銭の獲得(不正送金)</li></ul>	<ul style="list-style-type: none"><li>標的とする組織内の重要情報窃取やシステム破壊</li></ul>
主な攻撃手法	<ul style="list-style-type: none"><li>Web サイトに対するDoS</li><li>政治的な主張を目的とするWeb サイトの改ざん</li><li>SNS アカウント乗っ取り</li></ul>	<ul style="list-style-type: none"><li>マルウェアが添付されたメールの送付</li><li>Web サイト改ざんによるマルウェアの配布</li></ul>	<ul style="list-style-type: none"><li>マルウェアが添付されたメールの送付</li><li>Web サイト改ざんによるマルウェアの配布 (ただし攻撃対象のみに限定)</li></ul>
技術力	低		高

# 国内企業VPN経由のランサムウェア感染

- 2020年10月、北米現地法人に導入していた旧型VPN装置に対するサイバー攻撃により、15,649人の情報が漏洩
- 当時、同法人を含めグループ全体では新たなVPN装置を導入済だったものの、新型コロナウイルス感染急拡大に起因するネットワーク負荷の増大に伴い、通信障害等が発生した際の緊急避難用として旧型VPN装置1台を設置
- ランサムウェアだったため身代金約11億円を要求されたが企業の判断として拒否をした



不正アクセスに関する調査結果のご報告【第4報】

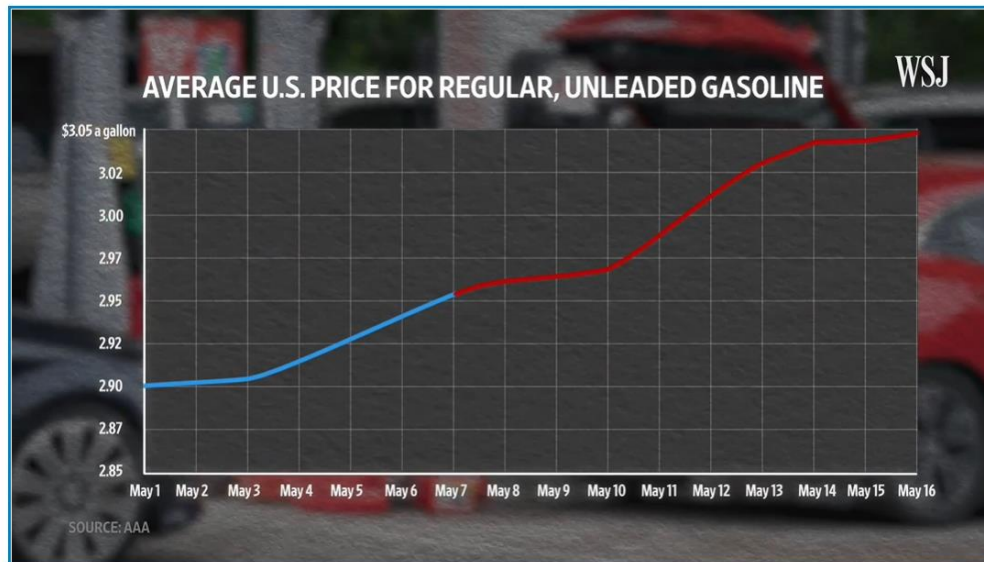
<https://www.capcom.co.jp/ir/news/html/210413.html>

# サイバー攻撃による米国パイプライン停止

- 米国コロニアル・パイプラインはサイバー攻撃を受け、7日から操業を停止し、身代金の支払いののち、12日夜に操業を再開した
- 燃料価格調査会社「ガスバディ」のデータによると、ノースカロライナ州やジョージア州など複数の州でガソリン不足が続き、価格が上昇した
- コロニアル社のブラウント社長は、いつまで操業停止が続くのか不透明だったことから、5月7日に身代金の支払いを承認したと語った

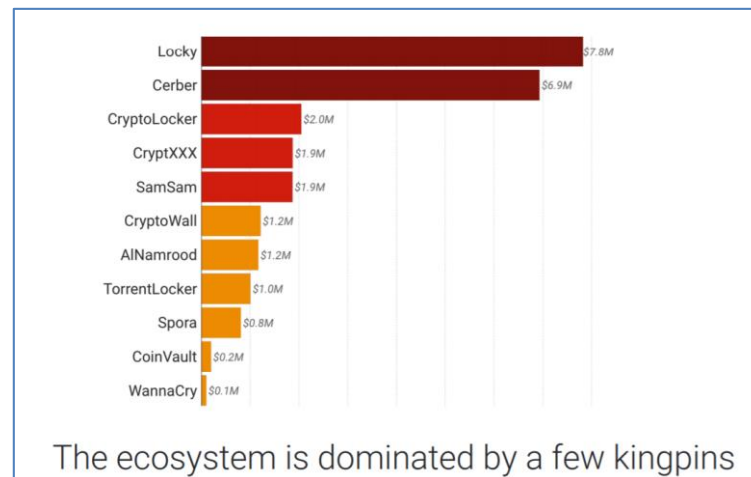
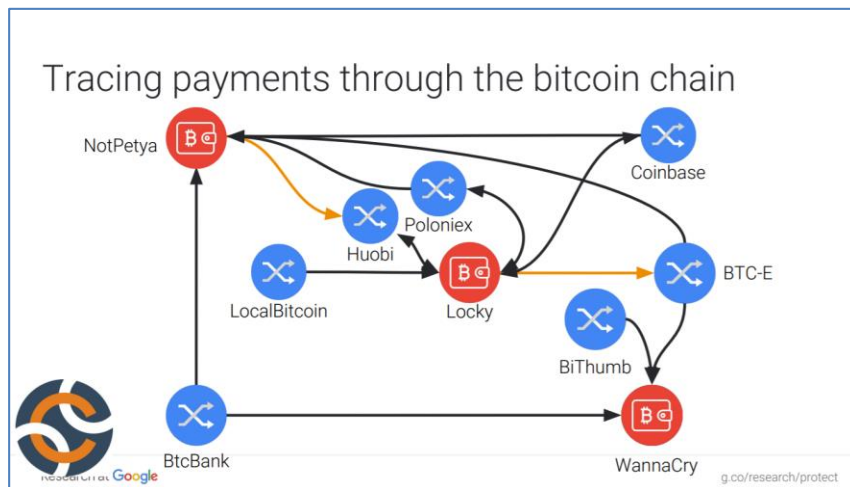
## Colonial Pipeline CEO Tells Why He Paid Hackers a \$4.4

Joseph Blount says he needed to quickly restore service after cyberattack threatened East Coast supp



# ランサムウェアに関する資金移動

- 154,227 個のランサムウェアのデータセットに基づいて、Google、ニューヨーク大学らの研究者がランサムウェアの支払いに利用されたBitcoinを追跡することにより、被害額や資金の流れを調査した
- 調査期間を通じて、総額約 2500 万ドルがBitcoinから現金として換金されており、その約95%がロシアの取引所を通じて現金化されていた



画像引用 : "TRACKING RANSOMWARE END TO END"

<https://www.blackhat.com/docs/us-17/wednesday/us-17-Invernizzi-Tracking-Ransomware-End-To-End.pdf>



# 国内事例：サプライチェーン

- 2022年3月1日に、経済産業省などが昨今の情勢を踏まえて、サプライチェーンに関わるサイバーセキュリティの注意喚起を公開
- 自動車部品メーカーがランサムウェア（身代金ウイルス）の被害を受けて、自動車メーカーの工場稼働が停止したとの報道
- 「鎖の丈夫さは、最も弱い輪によって決まる」by トーマス・リード

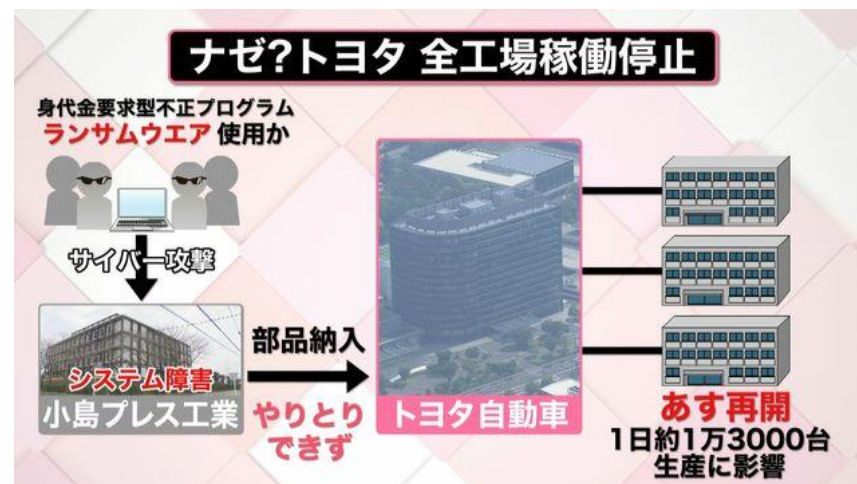
令和4年3月1日  
経済産業省  
金融庁  
総務省  
厚生労働省  
国土交通省  
警察庁  
内閣官房内閣サイバーセキュリティセンター

サイバーセキュリティ対策の強化について（注意喚起）

昨今の情勢を踏まえるとサイバー攻撃事案のリスクは高まっていると考えられます。本日、国内の自動車部品メーカーから被害にあった旨の発表がなされたところです。

政府機関や重要インフラ事業者をはじめとする各企業・団体等においては、組織幹部のリーダーシップの下、サイバー攻撃の脅威に対する認識を深めるとともに、以下に掲げる対策を講じることにより、対策の強化に努めていただきますようお願いいたします。

また、中小企業、取引先等、サプライチェーン全体を俯瞰し、発生するリスクを自身でコントロールできるよう、適切なセキュリティ対策を実施するようお願いいたします。



# 国内事例：医療機関におけるランサムウェア感染

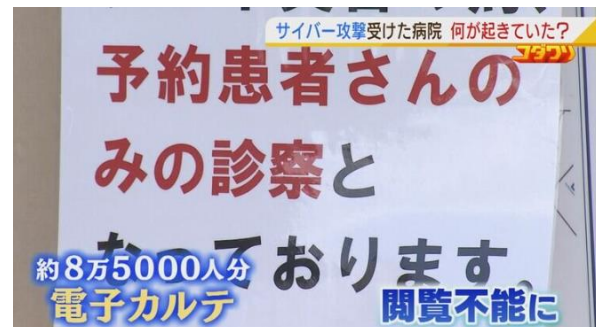
- 2022年6月、徳島県にある半田病院はランサムウェア（身代金ウイルス）に感染し電子カルテをはじめとする院内システムが利用できなくなった
- インシデント対応および得られた教訓を報告書として公開している
- 報告書から学べることは多く、特に対策には「脆弱性管理の課題」「システム設定の課題」などの項目が参考となる

## 徳島県つるぎ町立半田病院 コンピュータウイルス感染事案有識者会議調査報告書について

令和3年10月31日の未明、つるぎ町立半田病院がサイバー攻撃を受け、電子カルテをはじめとする院内システムがランサムウェアと呼ばれる身代金要求型コンピュータウイルスに感染し、カルテが閲覧できなくなるなどの大きな被害が生じました。令和4年1月4日の通常診療再開までの間、患者さんをはじめ関係者の皆さまには多大なご迷惑とご心配をおかけいたしましたこと、改めて深くお詫び申し上げます。

事件発生後、当院の職員は一人丸となって早期復旧を目指しました。全容解明や情報漏えい有無の特定よりも、まずは病院としての機能を一日も早く取り戻すために、患者さんのデータをいかに復元させるか、端末を利用できる状況にどのように戻すかに焦点を当てインシデント対応を行ってまいりました。幸いにして、調査復旧を請け負った事業者の作業、電子カルテ業者の仮システムの構築、そして、電子カルテより必要に応じて抽出していたデータなどを利用し、令和4年1月4日に通常診療を再開することが出来ました。

<https://www.handa-hospital.jp/topics/2022/0616/index.html>



# (参考)ランサムウェアに対する支払い

- “ランサムウェアの身代金要求に応じたときに生じうる法的責任に関する一考察”, 満永拓邦(東京大学)、北條孝佳(西村あさひ法律事務所), SCIS 2018
- 一定の条件下におけるランサムウェアへの支払いは法的な責任が生じうるため、安易に支払ってはならない
- 米国では財務省が「the sanctions risks associated with ransomware payments(ランサムウェアへの支払いに関する制裁リスク)」についてアドバイザリを公開している

Copyright© 2018 The Institute of Electronics,  
Information and Communication Engineers

SCIS 2018 2018 Symposium on  
Cryptography and Information Security  
Niigata, Japan, Jan. 23 - 26, 2018  
The Institute of Electronics,  
Information and Communication Engineers

## ランサムウェアの身代金要求に応じたときに生じうる法的責任に関する一考察 A Study on Legal Responsibility of Payments for Ransomware

満永 拓邦\*  
Takuho Mitsunaga

北條 孝佳†  
Takayoshi Hojo

あらまし 感染端末内に保存されているファイルを暗号化し使用不能にした後、元に戻すことと引き換えに金銭を要求するランサムウェアの被害が、2016年頃から個人・法人を問わず国内で急増している。機密情報を含む重要なファイルが暗号化された場合には、業務上多大な影響を及ぼす可能性があるため、被害者は実際に金銭を支払ってしまうこともあると報告されている。しかしながら、ランサムウェアを用いた金銭の要求は犯罪であり、犯罪者への金銭の支払いは、利益供与と見做される可能性もある。本稿では、やむを得ず金銭を支払った場合にどのような法的な責任やリスクが発生し得るかということについて検討する。

キーワード マルウェア感染、ランサムウェア、法的責任

# **攻撃者の分類に基づく攻撃の特徴**

**- 標的型攻撃、APTによる攻撃 -**

# 攻撃者の分類(再掲)

- 攻撃の目的をもとに攻撃者を分類すると、それぞれの攻撃手法や技術力が異なることが推察できる

	愉快犯/ハクティビスト	金銭目的の攻撃者	標的型攻撃の実行者
攻撃の目的	<ul style="list-style-type: none"><li>政治的な主張</li><li>技術力のアピール</li></ul>	<ul style="list-style-type: none"><li>金銭の獲得(不正送金)</li></ul>	<ul style="list-style-type: none"><li>標的とする組織内の重要情報窃取やシステム破壊</li></ul>
主な攻撃手法	<ul style="list-style-type: none"><li>Web サイトに対するDoS</li><li>政治的な主張を目的とするWeb サイトの改ざん</li><li>SNS アカウント乗っ取り</li></ul>	<ul style="list-style-type: none"><li>マルウェアが添付されたメールの送付</li><li>Web サイト改ざんによるマルウェアの配布</li></ul>	<ul style="list-style-type: none"><li>マルウェアが添付されたメールの送付</li><li>Web サイト改ざんによるマルウェアの配布 (ただし攻撃対象のみに限定)</li></ul>
技術力	低		高

# 増加する標的型攻撃の脅威

- 国内外を問わず、ここ数年で被害が増加
- 対象
  - 政府系組織・自治体
  - 重要インフラ事業者
  - 研究機関
  - 社会に大きな影響をもつ組織
  - 機密情報を保有する組織

**ニュース 日経コンピュータ**  
韓国で大規模サイバー攻撃か、放送局や銀行のシステムが  
2013/03/20 浅川 直輝=日経  
記事一覧へ>>

**ニュース ITpro**  
中小企業狙いと「水飲み場攻撃」が増加、シマン  
2013/04/23 松本 敏明=ITpro  
記事一覧へ>>

**ニュース ITpro**  
農水省へのサイバー攻撃で124点の行政文書の流出の可能性  
2013/05/25 高橋 信頼=ITpro  
記事一覧へ>>

韓国で2013年3月、放送局や銀行のシステムが一斉にサイバー攻撃を受けた。韓国国防省は、戦況を報告した。韓国国防省は、戦況を報告した。

シマンテックは2013年4月、成した「インターネットポート 第18号」の、世界で発生した標的型攻撃の増加したことを紹介した。

顕著なのが、従業員と製造業へ標的型攻撃すること。中でも小規模企業は2012年に全体の18%から急増している。

「中小企業は攻撃のターゲット。セキュリティ対策の不足が原因。中小企業は大企業と異なり、知的財産を持つ」と、高橋氏は指摘する。

農林水産省は2013年5月24日、同省へのサイバー攻撃で、2012年1月から4月にかけて5台のパソコンから合計124点の行政文書が流出した可能性があることを明らかにした。文書には、省内・省外の個人情報、業務上の情報が含まれていたが、いずれも「秘密文書」に当たらない機密性2以下のものであったとしている。

農水省では2013年1月にサイバー攻撃に関する調査委員会を設置。24日に調査結果を中間報告として公表した。5500台の職員パソコンの中から調査の必要があると判断された103台のパソコンを解析したところ、情報流出の可能性のある通信を行った職員パソコンは39台であることが判明した。「既存のセキュリティ対策を回避する高い隠蔽技術を有し、より巧妙化されたトロイの木馬型ウイルス」（報告書より）が検出されたという。

さらに解析の結果、2012年1月から4月にかけて5台のパソコンから合計124点の行政文書が流出した可能性があることが判明。文書の内容は、業務で関わった人の名刺情報などの個人情報、職員などの個人情報、業務上の情報で、いずれも農林水産省の「情報の格付及び取扱制限に関する規程」に定める「機密性2」以下のものであり、「秘密文書」には当たらないとしている。

(引用)

<http://itpro.nikkeibp.co.jp/article/NEWS/20130320/464581/>

<http://itpro.nikkeibp.co.jp/article/NEWS/20130525/479521/>

<http://itpro.nikkeibp.co.jp/article/NEWS/20130423/472869/>

# 標的型攻撃の特徴

- 米セキュリティ企業 Mandiant 社のレポートによると APT による攻撃の特徴は以下の通り、
  - 組織的かつ体系的な攻撃により、20業種141組織から数百テラバイトの情報を窃取された
  - 侵入を発見するきっかけは、94%が外部からの通知による
  - 組織内に侵入されていた平均の期間は、356日であり、期間が長い場合では1764日であった
  - 組織内ネットワークに一度侵入を許すと、数カ月から数年の期間に渡って、組織内に保管されている技術文書、財務資料、経営計画、契約書など様々なカテゴリーの情報、ならびにEメールアドレスなどの外部の連絡先を窃取した

(参考)

Mandiant Intelligence Center Report  
<http://intelreport.mandiant.com/>





# 外部からの通知

- トレンドマイクロ社「企業の9割が気づかなかったサイバー攻撃その脅威動向と企業がとるべき次の一手」によると、年金機構と同時期に被害を受けた15組織のうち14組織は「外部からの指摘」によって発覚した
- FireEye社「日本企業におけるセキュリティ侵害対策向上のための方策」に関する記者説明会(2015年11月)では、取引先、顧客、捜査当局等の「外部からの指摘」で発覚したのは69%とのこと

図1: 2015年4月～6月に公表/報道された主な情報窃取サイバー攻撃(トレンドマイクロが独自に整理※1)

	発覚/公表日	被害組織	発覚原因	侵入経路	情報流出被害
1	6月1日	年金事業	外部からの指摘	標的型メール	101万件の個人情報
2	6月9日	業界団体	外部からの指摘	標的型メール	2万7千件の個人情報
3	6月10日	商工会議所	外部からの指摘	標的型メール	1万2139件の個人情報
4	6月13日	医療保険事業	外部からの指摘	不明	不明
5	6月16日	地方自治体	外部からの指摘	標的型メール	不明
6	6月16日	海外協力事業	外部からの指摘	標的型メール	不明
7	6月17日	医療保険事業	外部からの指摘	不明	個人情報(規模不明)
8	6月17日	施設管理事業	外部からの指摘	標的型メール	不明
9	6月17日	公共施設	外部からの指摘	標的型メール	不明
10	6月17日	海外協力事業	不明	標的型メール	個人情報(規模不明)
11	6月19日	医療機関	外部からの指摘	標的型メール	最大250件の個人情報
12	6月19日	宿泊施設	外部からの指摘	標的型メール	個人情報(規模不明)
13	6月19日	医療機関	外部からの指摘	標的型メール	不明
14	6月22日	教育機関	外部からの指摘	標的型メール	3308件の個人情報
15	6月25日	官公庁	外部からの指摘	不明	不明

企業の9割が気づかなかったサイバー攻撃その脅威動向と企業がとるべき次の一手

<http://sp.trendmicro.co.jp/jp/trendpark/apt/201511-1/20151124035404.html>



# 外部からの通知

- 外部からの通知が必ずしも適切な窓口に来るとは限らない
- 「あなたの組織がサイバー攻撃の被害を受けています」との連絡に対してどこまで信頼できるか

## 「通知」にかかる日数

- 代表電話番号や一般の問い合わせ窓口からセキュリティ担当部門までの情報伝達が、必ずしもスムーズに行われるわけではない
- そのため、セキュリティ担当部門への報告窓口を設置している組織への通知と、設置していない組織への通知は必要な日数は異なることが多い
- 報告窓口に通知できない場合、セキュリティ担当部門に届くまでに約60日を要した事例もある(設置後は即日通知が可能になった)

→セキュリティに関する外部組織との連絡窓口を設置し、また組織内部で実効的な調整を行える体制が必要(組織内CSIRTの必要性)

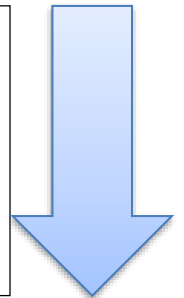


# 「通知」におけるコミュニケーション

- 「御社は標的型攻撃の被害にあっているようだ」と外部組織から連絡を受けた際に、迅速な対応が実施できる体制を構築できているか
- リスク・コミュニケーションという観点からは、「面識がない人から突然連絡を受け、リスク(脅威)を説明されたとしても信頼や理解しづらい」とされる。むしろ疑うのが自然。

→日常的にリスクへの理解や信頼構築を行う必要性がある

1. <b>Credibility</b> (信頼の確立)	価値観の共有を通じた信頼の確立
2. <b>Awareness</b> (気づき・意識)	リスクに気づき、意識する
3. <b>Understanding</b> (理解)	リスクについて理解を深める
4. <b>Solution</b> (解決策)	リスクに対する解決策を理解、検討する
5. <b>Enactment</b> (対処行動)	リスクへの対処行動を起こす



リスク・コミュニケーションにおけるCAUSEモデルの段階  
(参考)KE Rowan: "Why Rules for Risk Communication Are Not Enough"

信頼醸成と  
リスクへの対処

## 組織におけるインシデント対応

# 侵入後の検知と事前対策

- 組織への侵入を防ぐ事には限界がある
  - メール経由以外でも、Webサイト閲覧などにより内部に侵入するケース
  - 未修正の脆弱性を狙う攻撃の発生
  - 従業員のセキュリティ意識の不足、人的エラーの発生
  - セキュリティ対策ソフトによる検知、不審な通信の検知の限界

## 侵入された**後**の対策も重要

- ・ 各機器でログは十分に取れているか？
- ・ 侵入後に検知できる仕組みがあるか？
- ・ 重要な情報資産は切り離されているか？
- ・ インシデント発生時の対応手順は明確か？



# 事前の備え

- ・ インシデント発生に備えて事前に確認すべき事項
  - インシデント対応の経験上、基本的な事項が疎かになっている事例も少なくない

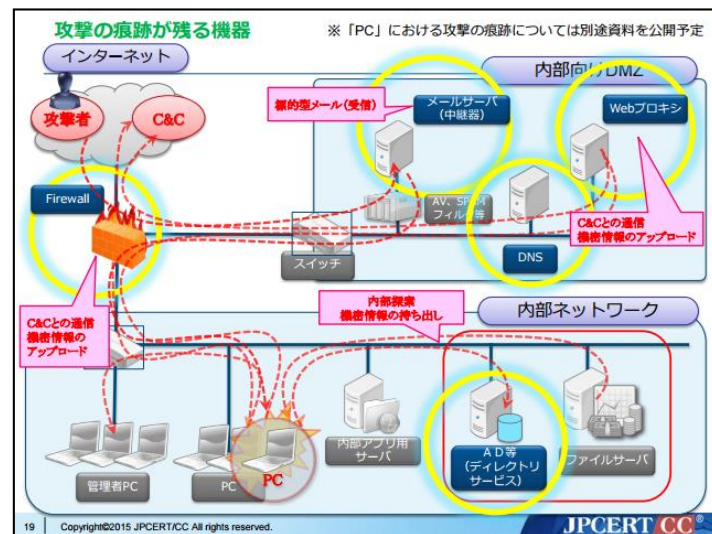
項目	事項
エスカレーション体制	インシデント発生時にどこに連絡するのか。また誰が対応の責任者となるかを事前に定めておく。
情報資産の管理	組織が保有する情報資産（データ）のうち、事業継続に影響を与えるものについて把握し、アクセス権を設定するなど適切な管理を行う。
I T 資産の管理	組織が保有しているパソコンやサーバなどの I T 資産について、管理担当者や設置場所について把握し、適切に管理を行う。
ネットワーク構成管理	パソコンやサーバなどの I T 資産が接続する社内ネットワーク並びに、インターネット接続の構成、各種ネットワーク機器の設定を管理する。
ログの取得	インシデント発生に備えて、サーバやネットワーク機器にてログを取得し、保存する。原因追究と影響範囲の特定には、ログが必要不可欠である。

→パーソルプロセス&テクノロジー社と東洋大学で開発するチェックリストに

# 攻撃検知へのログ活用

- ・「高度サイバー攻撃への対処におけるログの活用と分析方法」

インシデント対応におけるログ採取の重要性は多くの組織で認識されているものの、インシデント発生時に調査に必要なサーバや機器のログが無い、十分な期間のログが無いなどにより全容の解明に到らなかった例も少なくない。こうした状況の改善に向けた一助となるように、攻撃者の活動の痕跡をログとして残すための考え方、それらのログから痕跡を見つけ出す方法などを記載している



# セキュリティに関する対応体制

- インシデント(\*)発生時の対応体制
  - ユーザ部門、システム管理、営業、法務、広報などの関連部署間で情報の共有及び対策の一元化
  - システム責任者、対応フローの明確化(例：誰がサーバを止めれるか?)

インシデント(\*)・・・IT システムの正常な運用または利用を阻害するマルウェア感染、不正アクセス、情報漏えい、DoS 攻撃などの事案や現象の発生をいう

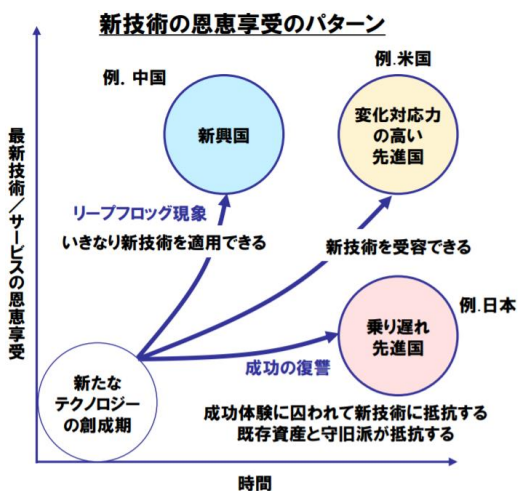


(DX時代を迎えて)  
今、セキュリティを学ぶことのメリット

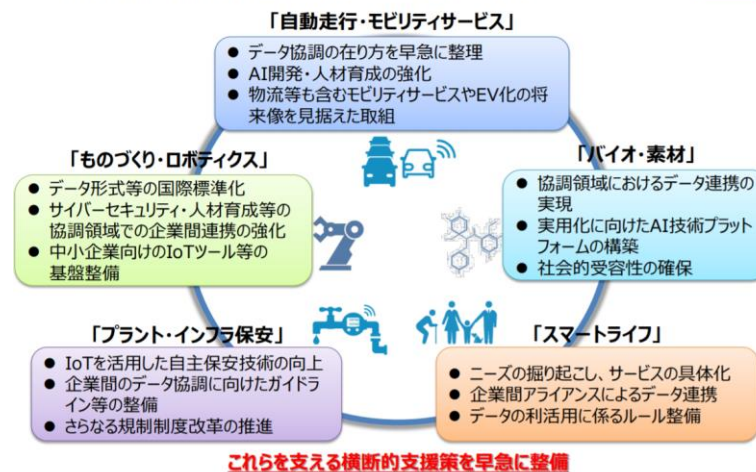


# 次世代に向けた日本の取り組み

- 次世代の技術の実用化に向けて、産官学連携を通じて各組織が努力を注いでいる
  - ドローン(Drone)
  - AI機器(AI Device)
  - 自動走行車・無人ロボット(Automated Car, Robot)
  - 遠隔操作ロボット(RPA)
  - クラウド技術の活用(Cloud)



## 「Connected Industries」5つの重点取組分野



# サイバーフィジカルシステム（CPS）とIoT

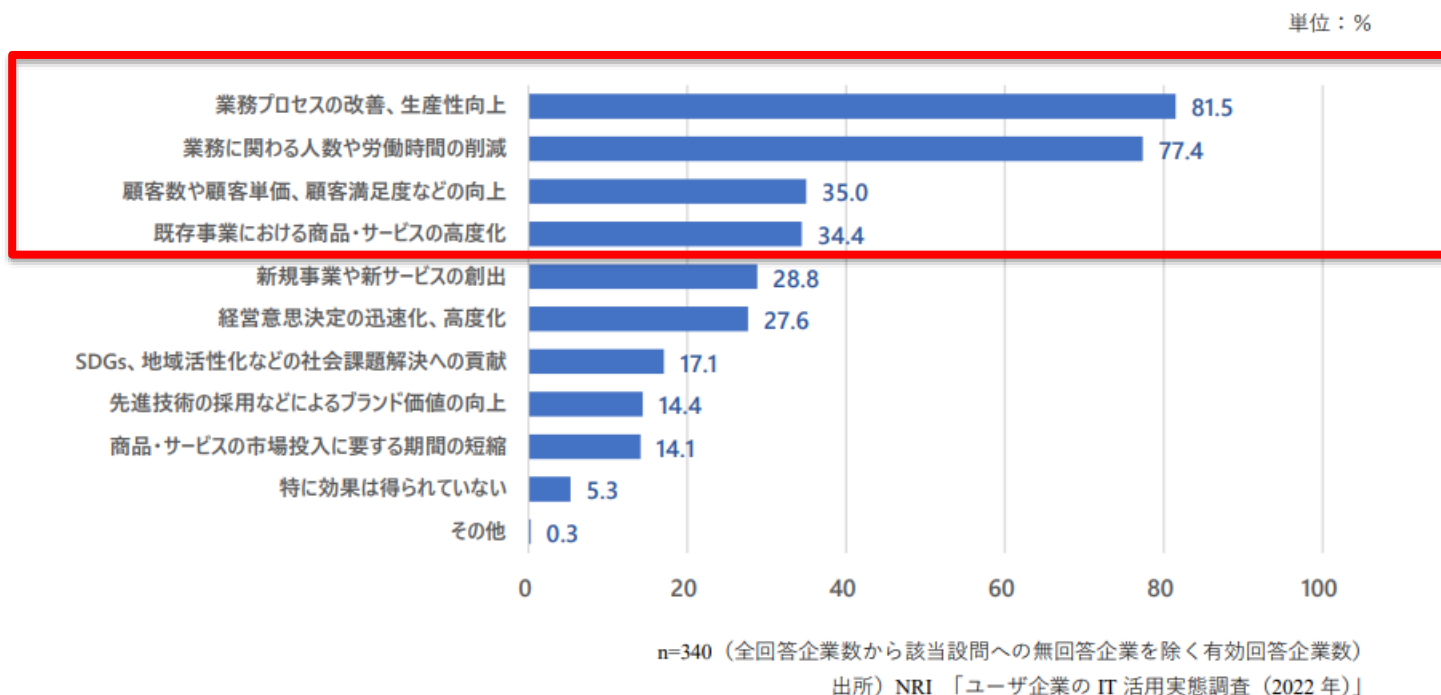
- 実世界（フィジカル空間）にある多様なデータをセンサーネットワーク等で収集し、サイバー空間で大規模データ処理技術等を駆使して分析／知識化を行い、そこで創出した情報／価値によって、産業の活性化や社会問題の解決を図る



# DX時代のデジタル投資

- デジタル推進は事業にポジティブな効果をもたらす
- IT投資が増加した企業 52.9%、減少した企業 6.1%

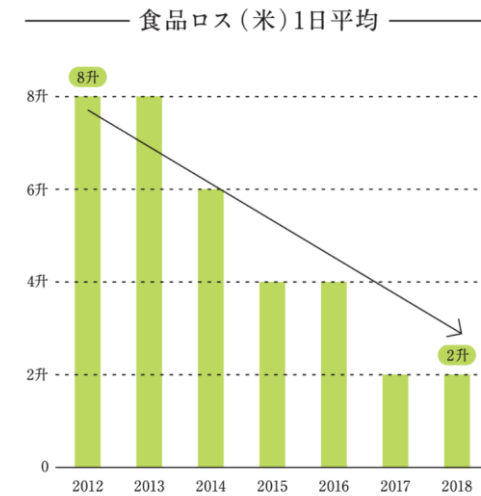
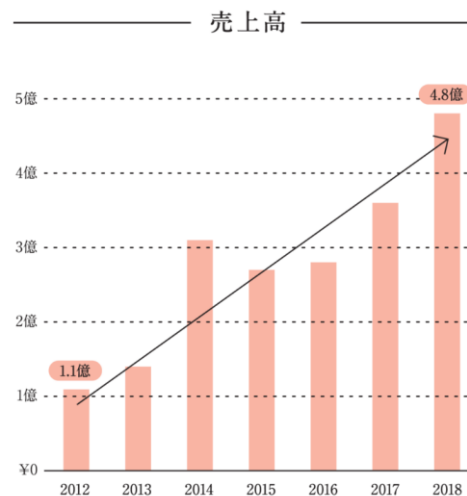
図2：デジタル化の推進による効果（どのような側面で得られているか、複数回答）



引用：野村総研「IT活用実態調査2022」  
企業466社のCIOへのアンケートに基づく

# DX事例：ゑびや

- 社員十数人、アルバイトパートを入れても40名ほどの老舗食堂
- 店舗運営をIT化、クラウドPOSレジを導入
- 来客予測システムやIoTデバイスによる在庫の管理・自動発注を開始
- 従業員一人あたりの売上が400万円弱から数年で約1100万円へ大幅アップを実現



# 生成系AI

- ChatGPTを始めとする生成系AIの普及に伴い、IT分野の生産性向上は急速に増加していくと考えられます
- 今後、IT技術が企業において加速度的に進むことが考えられます

TA

DX時代にセキュリティは重要でしょうか



はい、DX（デジタルトランスフォーメーション）時代においてセキュリティは非常に重要です。DX時代は、企業や組織がデジタル技術を活用して業務プロセスやビジネスモデルを変革し、競争力を高める時代です。しかし、デジタル化が進むことで、情報セキュリティの脅威も増加しています。



デジタル化により、企業や組織は大量のデータを扱うようになります。このデータには、顧客情報や取引記録など、機密性が高い情報が含まれることがあります。セキュリティの不備や漏えいが起これば、重要な情報が悪用されたり、競合他社に漏洩したりする可能性があります。その結果、信頼性やブランドイメージの低下、法的な問題、経済的な損失などのリスクが生じます。

さらに、DX時代ではクラウドコンピューティング、モバイルデバイス、インターネット・オブ・シングス（IoT）、人工知能（AI）などの新たなテクノロジーが広く利用されています。これらのテクノロジーは、ビジネスプロセスの効率化やイノベーションを実現する一方で、セキュリティリスクをもたらす可能性もあります。例えば、クラウドに保存されたデータやモバイルデバイスからのアクセスが不正に行われる、IoTデバイスがハッキングされる、AIシステムに悪意のある操作がなされるなどの脅威が存在します。

したがって、DX時代においてはセキュリティ対策が重要となります。組織は、適切なセキュリティポリシーや規程の策定、セキュリティ意識の向上、セキュリティ技術の導入などを通じて、情報セキュリティを確保する必要があります。セキュリティの考慮がなされていないDXの実施は、企業や組織に重大なリスクをもたらす可能性がありますので、セキュリティは常に重要な要素として考慮されるべきです。

IT技術が企業の生産性向上に不可欠なツール  
となっていく中、安心安全にIT技術を活用するための  
「セキュリティ」の重要性も増していきます

この研修でセキュリティ技術と知識を学び、  
皆さんの今後の活躍に繋がてもらえればと思います

# まとめ

- サイバー攻撃は突然無くなることはなく、今後も様々な攻撃が継続して発生すると考えられる
- 100%の防御手法がないため、被害発生に備えた体制やフローを確立する必要がある(CSIRT)
- 万が一、被害が発生しても所管官庁はじめ周囲とコミュニケーションを図り、協調して対応を進めることが望まれる
- 外部リソースを活用しつつ、**基本的な対策**から始める。まずは、サイバーセキュリティの避難訓練から！