NTT DATA
Trusted Global Innovator

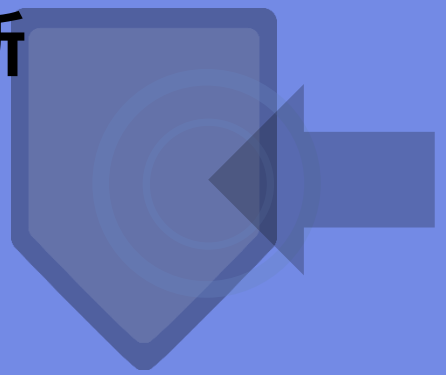
# 中小企業を襲うサイバー攻撃の最新手法と被害の実例

2022年2月14日
株式会社NTTデータ

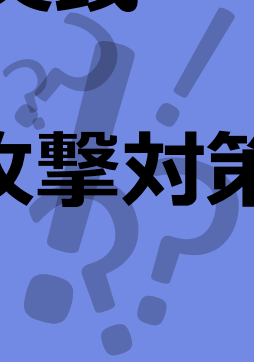
1 中小企業も
サイバー攻撃の
標的に

2 サイバー攻撃の
事例と手口

3 サイバー攻撃対策
の勘所



4 今日から実践
すぐできる
サイバー攻撃対策





NTT DATA

# 皆さん、こんなこと思っていませんか？

**攻撃者は、企業の規模に関係なく、皆さんの企業も標的にしている。**

- 自分の会社なんて、**誰も狙わない**でしょ？
- 盗まれて困る**秘密データなんてない**し
- 万が一攻撃にあっても、

  **誰にも迷惑をかけない**でしょ？

# 重要データは皆さんの組織にも

**ほとんどの企業は、企業活動を営む上で必要となる「重要なデータ」を保持している。**

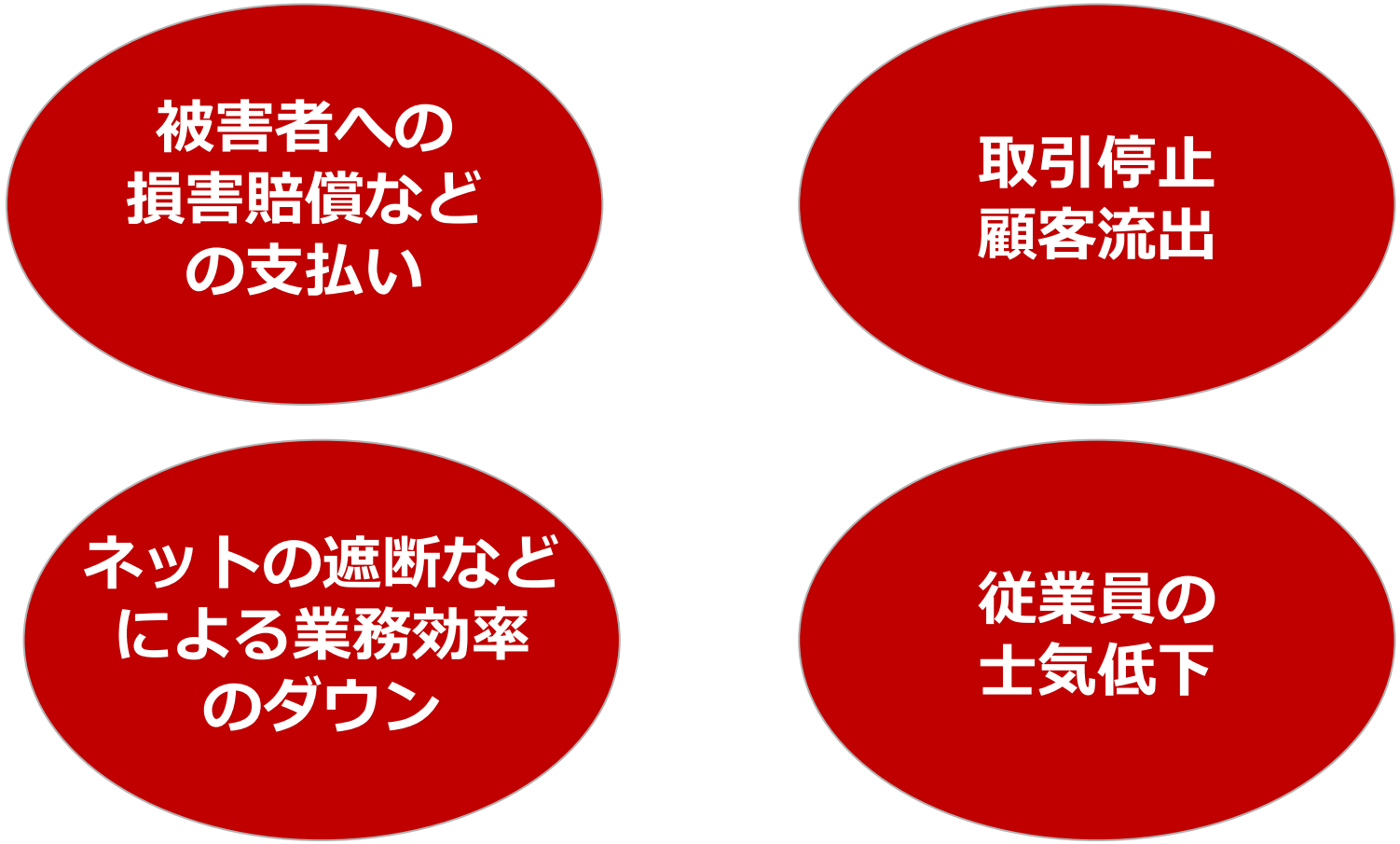
**例えば、こんなデータを保持していませんか？**

- 従業員のマイナンバー、住所、給与明細 
- お客様や取引先の連絡先一覧 
- 新製品の設計図などの開発情報 
- 取引先から"取扱注意"として預かった情報 
- 取引先ごとの仕切り額や取引実績 

<出典：（独）情報処理推進機構「情報セキュリティ5か条」>

# 重要データがサイバー攻撃により漏洩したり、破壊されると？

**サイバー攻撃による被害は甚大。**




＜出典：（独）情報処理推進機構「情報セキュリティ5か条」＞

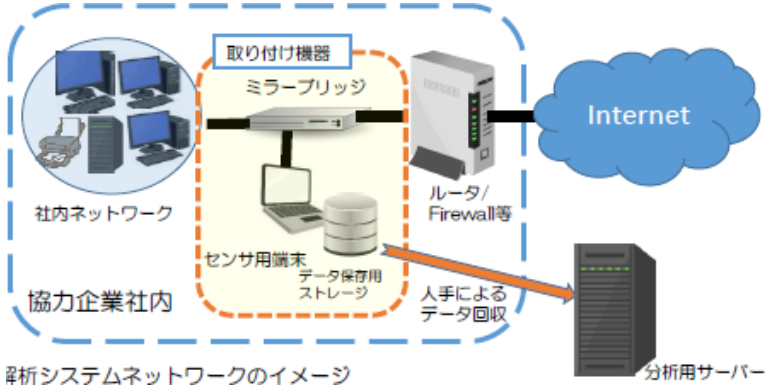
# 中小企業に対するサイバー攻撃の調査・分析結果

## 地域の中小企業も、例外なくサイバー攻撃の脅威にさらされている。

### 中小企業被害実態に関する調査

**■調査内容**

実証期間：平成30年9月～平成31年1月
実証内容：中小企業30社を対象に、ネットワーク上の通信データ等を一定期間収集。



解析システムネットワークのイメージ

**■ 調査結果**

- 調査した**30社全てでサイバー攻撃に繋がりうる不審な通信**が記録されていた。
- 少なくとも5社ではコンピューターウイルスに感染するなどして、**情報が外部に流出したおそれ**があることが分かった。

＜出典：大阪商工会議所「平成30年度中小企業に対するサイバー攻撃実情調査（報告）」共同研究実施者：神戸大学、東京海上日動火災保険（株）(2019年7月）＞

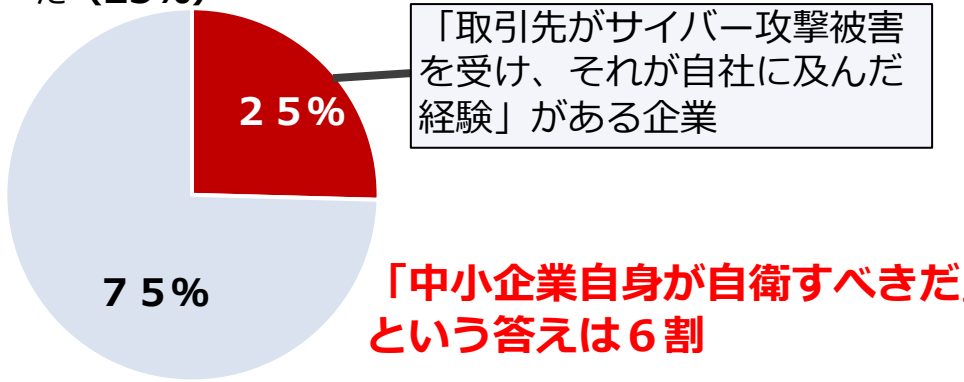
### 取引先経由の被害に関する調査

**■調査内容**

調査期間：平成31年2月～3月
調査内容：全国の従業員100人以上の企業を対象に、郵送、FAX、メール、Web、対面による依頼・回答

**■調査結果**

- 大企業・中堅企業118社に調査したところ、取引先がサイバー攻撃被害を受け、**影響が自社に及んだ経験**がある企業が30社あった（**25%**）




**「中小企業自身が自衛すべきだ」という答えは６割**

＜出典：大阪商工会議所「サプライチェーンにおける取引先のサイバーセキュリティ対策等に関する調査」（2019年5月）＞

# サプライチェーン経由で発生する事故

取引先も含めてセキュリティを確保することが重要。
自社が対策をしていないことで**委託元に迷惑**をかけてしまう可能性もある。

| 公表年 | 委託元業種 | 被害内容 | 原因 |
|---|---|---|---|
| 2013 | 卸売業、小売業 | 会員の個人情報が改ざん。<br>**約２ヶ月間サービス停止**。 | **委託先が管理**するWebサイトが不正アクセスを受けた。 |
| 2014 | 情報通信業 | Webサイト内のファイルが改ざん。オンラインバンキングで不正送金を行うマルウェアが設置され、当該**マルウェアが委託元製品の顧客に数千件ダウンロードされた**。<br>サービスの再開にあたってWebサイトの委託先を別企業に変更した。 | ダウンロードサービスを委託している**委託先のWebサイト**が不正アクセスを受けた。 |
| 2015 | 卸売業、小売業 | ECサイトの会員の個人情報が漏洩。<br>事故の発表後、委託元企業の**株価が３日間下落し、年初来安値を更新**。 | **再々委託先が管理**するサーバが不正アクセスを受けた。 |
| 2016 | その他サービス業 | 顧客の個人情報が漏洩。事故の影響もあり、<br>**販売数が前年比1割減**となった。 | **委託先の端末**がマルウェアに感染し、攻撃者が個人情報のあるサーバに侵入した。 |
| 2017 | 国家公務、地方公務 | 救急医療機関等の情報を掲載しているWebサイトの内容が改ざん。<br>再発防止策実施までの間、**Webサイトの公開を停止**した。 | **委託先が類推可能なIDとパスワードを利用**していた。 |

# 中小企業の被害事例

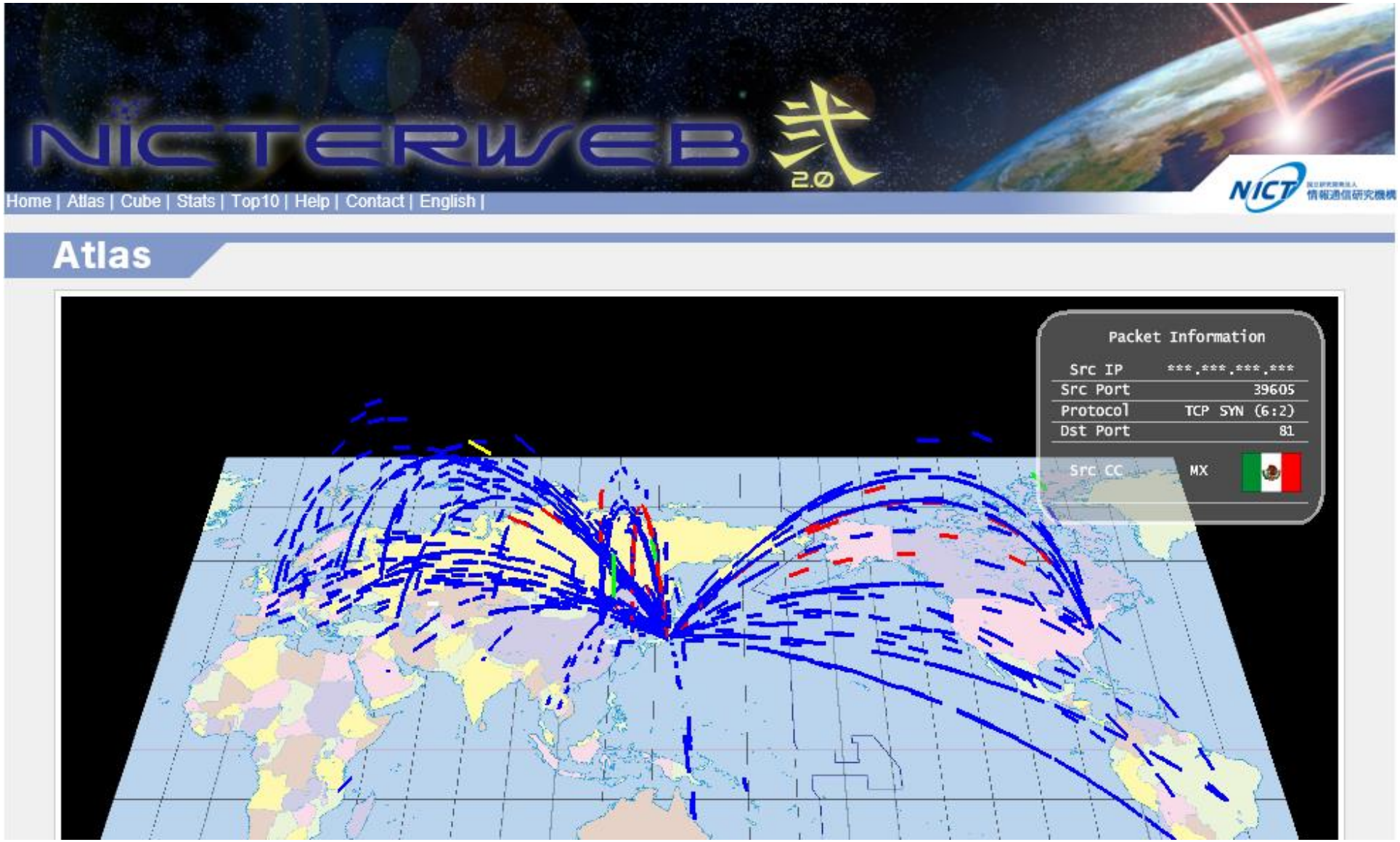
重要インフラや大企業だけでなく、中小企業においてもサイバー攻撃の被害は発生。

| | 事例 | 業種 | 所在地 | 従業員規模 |
|---|---|---|---|---|
| ウィルス感染 | 従業員が**メールに添付されていたファイルを不用意に開き**、基幹システムの設定が書き換わる障害が発生した。システムベンダの協力を得て障害の調査を行い、復旧するまでの**1週間ほど、基幹システムの一部が使用できなくなった**。 | 製造業 | 静岡県 | ５１～１００名 |
| | 役員のパソコンが**ウイルスに感染**し、保存されていた過去の電子メールが、これまでの送受信先などに大量に送信され、自社および取引先の**重要な情報が漏洩**してしまった。取引先からはクレームが上がり、謝罪をしたものの**信頼を失墜**することとなった。 | 製造業 | 栃木県 | ５１～１００名 |
| | ウイルス対策ソフトの契約更新を失念し、数日間サポートが切れた。そのわずかの間に、インターネットに繋がっていたPCが**「トロイの木馬」に感染**した。<br>急ぎアプリケーションを停止し、自社でリカバリーしたが、**復旧までに約2か月**を要し、その間、仕事にも支障をきたした。 | 卸売業 | 福岡県 | ２１～５０名 |
| ランサムウェア | ある日届いた経営者宛の**メールに添付されているファイルを開いて**しまった結果、「ファイルをロックしたので、解除して欲しければ連絡をするように」と電話番号を含む**警告画面がパソコンのスクリーン上に表示され消えなくなった**。<br>社内の重要データは共有サーバで管理されており、**バックアップ等を行っていた**ため会社としての被害はなかったが、個人の写真などのデータは参照できなくなっていた。 | 製造業 | 神奈川県 | ６～２０名 |

<出典：IPA 2016年度中小企業における情報セキュリティ対策の実態調査>

デモ

# 日本にどのくらい攻撃が来ているの？




<出典：http://www.nicter.jp/#>

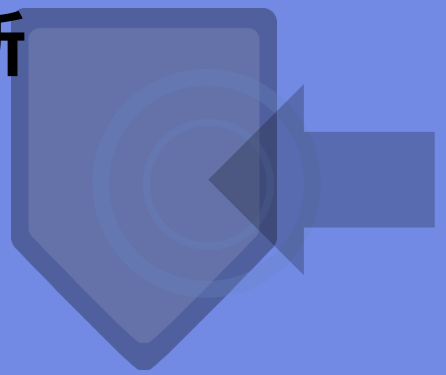


NTT DATA

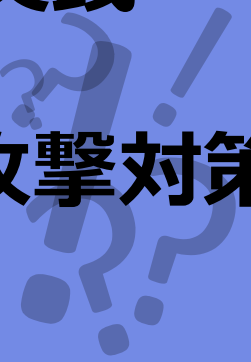
1 中小企業も
サイバー攻撃の
標的に

2 サイバー攻撃の
事例と手口

3 サイバー攻撃対策
の勘所



4 今日から実践
すぐできる
サイバー攻撃対策





NTT DATA

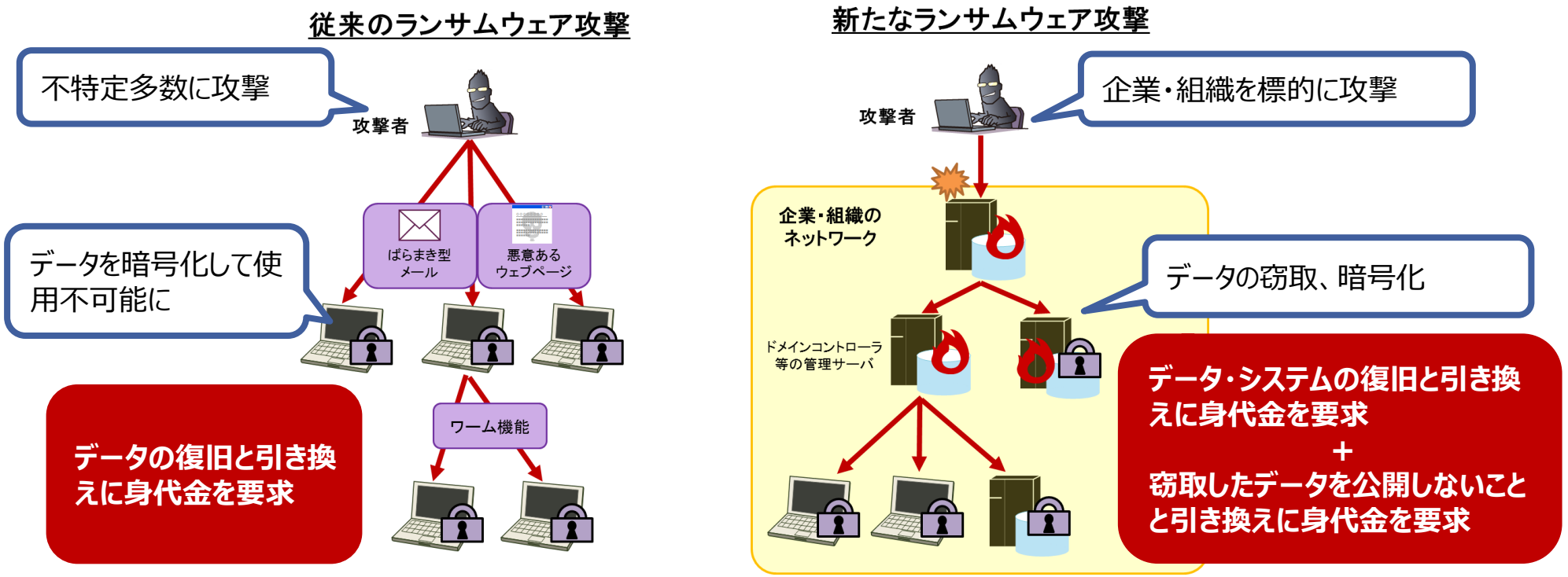
# 情報セキュリティ10大脅威 2022

| 昨年順位 | 個人の脅威 | 順位 | 組織の脅威 | 昨年順位 |
|---|---|---|---|---|
| 2位 | フィッシングによる個人情報等の詐取 | 1位 | ランサムウェアによる被害 | 1位 |
| 3位 | ネット上の誹謗・中傷・デマ | 2位 | 標的型攻撃による機密情報の窃取 | 3位 |
| 4位 | メールやSMS等を使った脅迫・詐欺の手口による金銭要求 | 3位 | サプライチェーンの弱点を悪用した攻撃 | 4位 |
| 5位 | クレジットカード情報の不正利用 | 4位 | テレワーク等のニューノーマルな働き方を狙った攻撃 | 3位 |
| 1位 | スマホ決済の不正利用 | 5位 | 内部不正による情報漏えい | 6位 |
| 8位 | 偽警告によるインターネット詐欺 | 6位 | 脆弱性対策情報の公開に伴う悪用増加 | 10位 |
| 9位 | 不正アプリによるスマートフォン利用者への被害 | 7位 | 修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃） | NEW |
| 7位 | インターネット上のサービスからの個人情報の窃取 | 8位 | ビジネスメール詐欺による金銭被害 | 5位 |
| 6位 | インターネットバンキングの不正利用 | 9位 | 予期せぬIT基盤の障害に伴う業務停止 | 7位 |
| 10位 | インターネット上のサービスへの不正ログイン | 10位 | 不注意による情報漏えい等の被害 | 9位 |

<出典：（独）情報処理推進機構 https://www.ipa.go.jp/security/vuln/10threats2022.html>

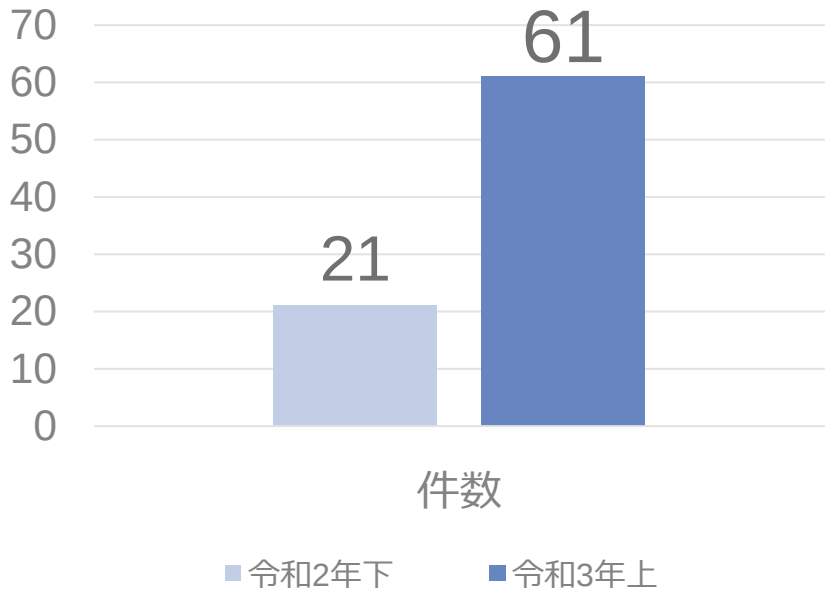
# ランサムウェアとその手口の変化（二重の脅迫）

- **ランサムウェアとは**
  - 「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語。感染したパソコンのデータを暗号化するなど使用不可能にし、その解除と引き換えに金銭を要求する。
- **新たな（侵入型）ランサムウェア攻撃（二重の脅迫）とは**
  - ターゲットとなる企業・組織内のネットワークへ侵入し、パソコン等の端末やサーバ上の**データを窃取した後に一斉に暗号化**してシステムを使用不可能にし、脅迫をするサイバー攻撃。
  - システムの**復旧に対する金銭要求**に加えて、窃取した**データを公開しない見返りの金銭要求**も行うので、**二重の脅迫**と恐れられる。

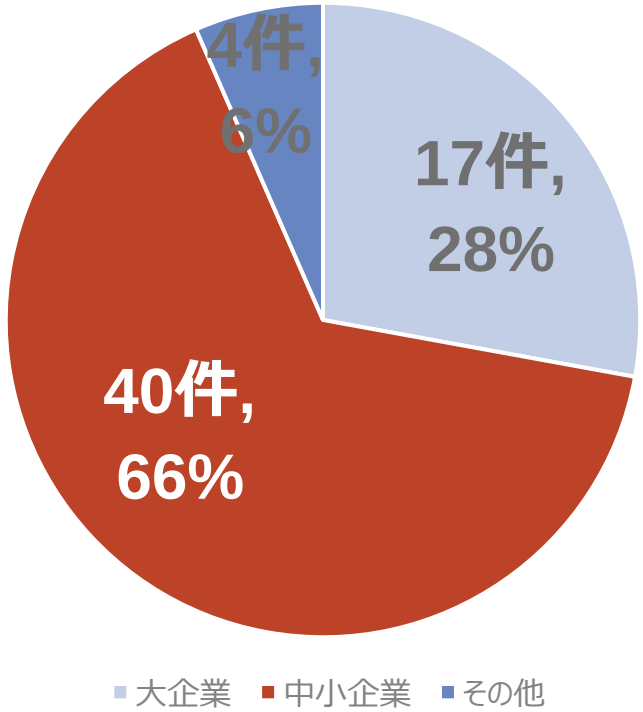


# 中小企業のランサムウェア被害の増加

- 企業・団体等におけるランサムウェア被害として、令和3年上半期に都道府県警察から警察庁に報告のあった件数は61件であり、前年上半期(21件)から大幅に増加。
- 被害件数(61件)の内訳は、大企業17件に対して、**中小企業は40件**。
- 侵入手段には**VPNやリモートデスクトップといったテレワーク用の設備が狙われている**ことも併せて明らかに




企業・団体等におけるランサムウェア被害の報告件数の推移




ランサムウェア被害の被害企業・団体等の規模別報告件数

<出典：警察庁「令和３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（2021年9月9日）」>
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_kami_cyber_jousei.pdf

# 事例：ランサムウェアに支払ってしまった事業者

- 北海道・小樽にある鮮魚店では、ランサムウェアに感染してしまった結果、売り上げなどを含む**重要なデータ15年分が暗号化**され、身代金としてビットコイン**30万円相当を要求**された
- この事業主は、会計士と相談したうえで**ビットコインを支払い**、暗号化を解除するための手段をサイバー犯罪者から提供を受けた
- ただし、**復元できたのは重要データ全体の8割**ほどであったため、全体復旧はできなかった

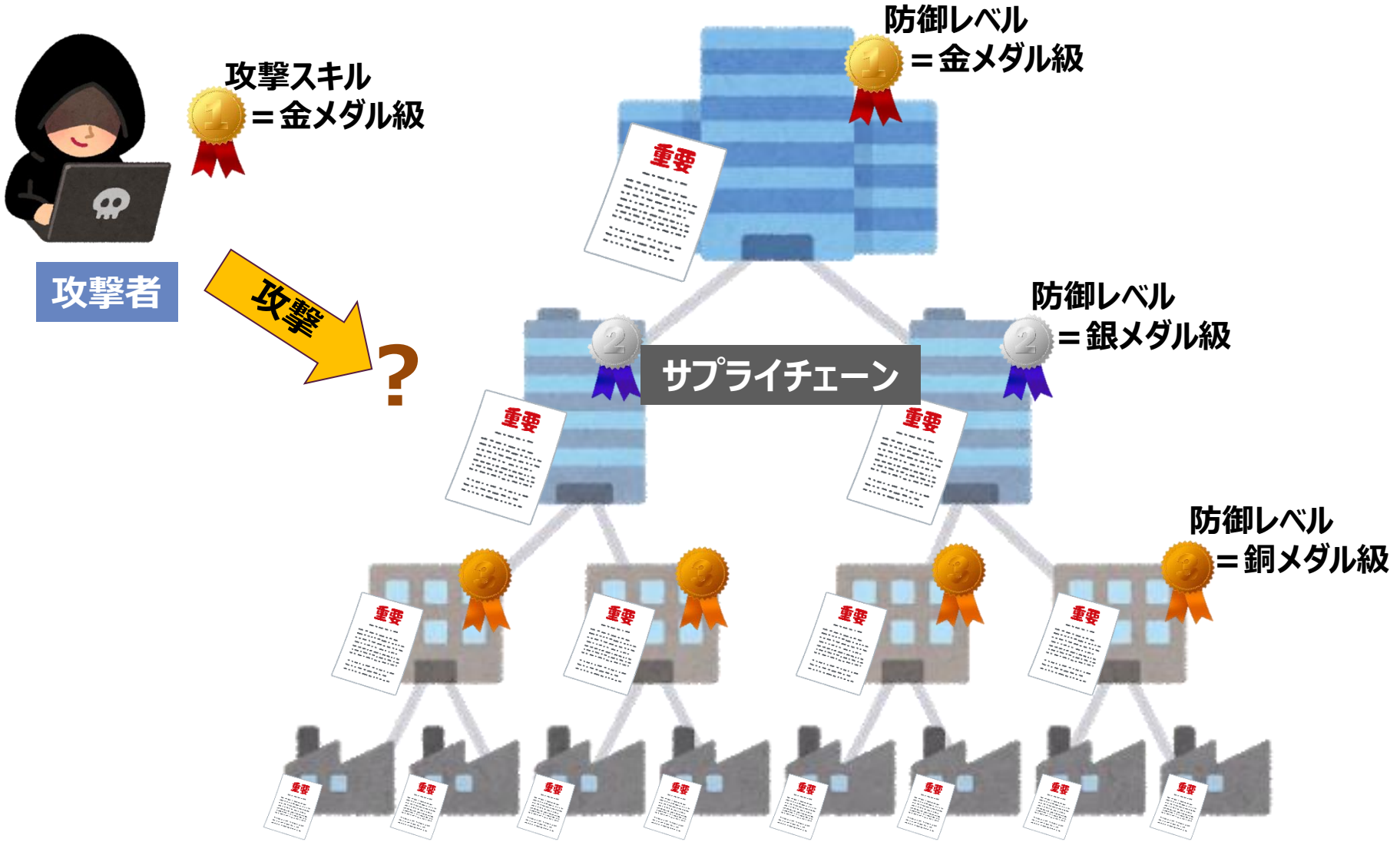
# 情報セキュリティ10大脅威 2022

| 昨年順位 | 個人の脅威 | 順位 | 組織の脅威 | 昨年順位 |
|---|---|---|---|---|
| 2位 | フィッシングによる個人情報等の詐取 | 1位 | ランサムウェアによる被害 | 1位 |
| 3位 | ネット上の誹謗・中傷・デマ | 2位 | 標的型攻撃による機密情報の窃取 | 3位 |
| 4位 | メールやSMS等を使った脅迫・詐欺の手口による金銭要求 | 3位 | サプライチェーンの弱点を悪用した攻撃 | 4位 |
| 5位 | クレジットカード情報の不正利用 | 4位 | テレワーク等のニューノーマルな働き方を狙った攻撃 | 3位 |
| 1 位 | スマホ決済の不正利用 | 5位 | 内部不正による情報漏えい | 6位 |
| 8位 | 偽警告によるインターネット詐欺 | 6位 | 脆弱性対策情報の公開に伴う悪用増加 | 10位 |
| 9位 | 不正アプリによるスマートフォン利用者への被害 | 7位 | 修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃） | NEW |
| 7位 | インターネット上のサービスからの個人情報の窃取 | 8位 | ビジネスメール詐欺による金銭被害 | 5位 |
| 6位 | インターネットバンキングの不正利用 | 9位 | 予期せぬIT基盤の障害に伴う業務停止 | 7位 |
| 10位 | インターネット上のサービスへの不正ログイン | 10位 | 不注意による情報漏えい等の被害 | 9位 |

<出典：（独）情報処理推進機構 https://www.ipa.go.jp/security/vuln/10threats2022.html>

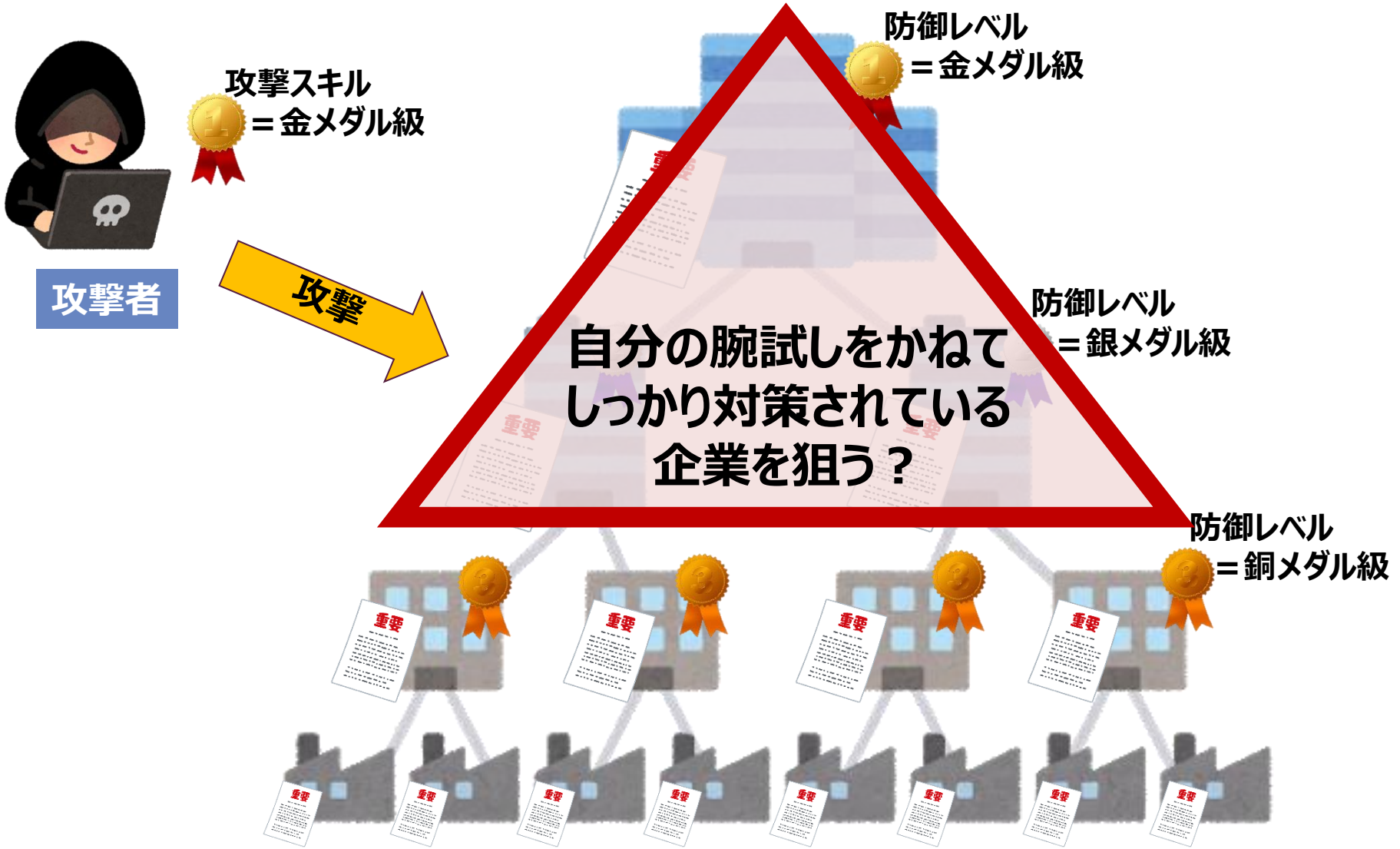
# 攻撃者はサプライチェーンのどこを狙うか

企業の対策レベルはバラバラだが、「金（カネ）」になる重要情報は至る所に存在する。



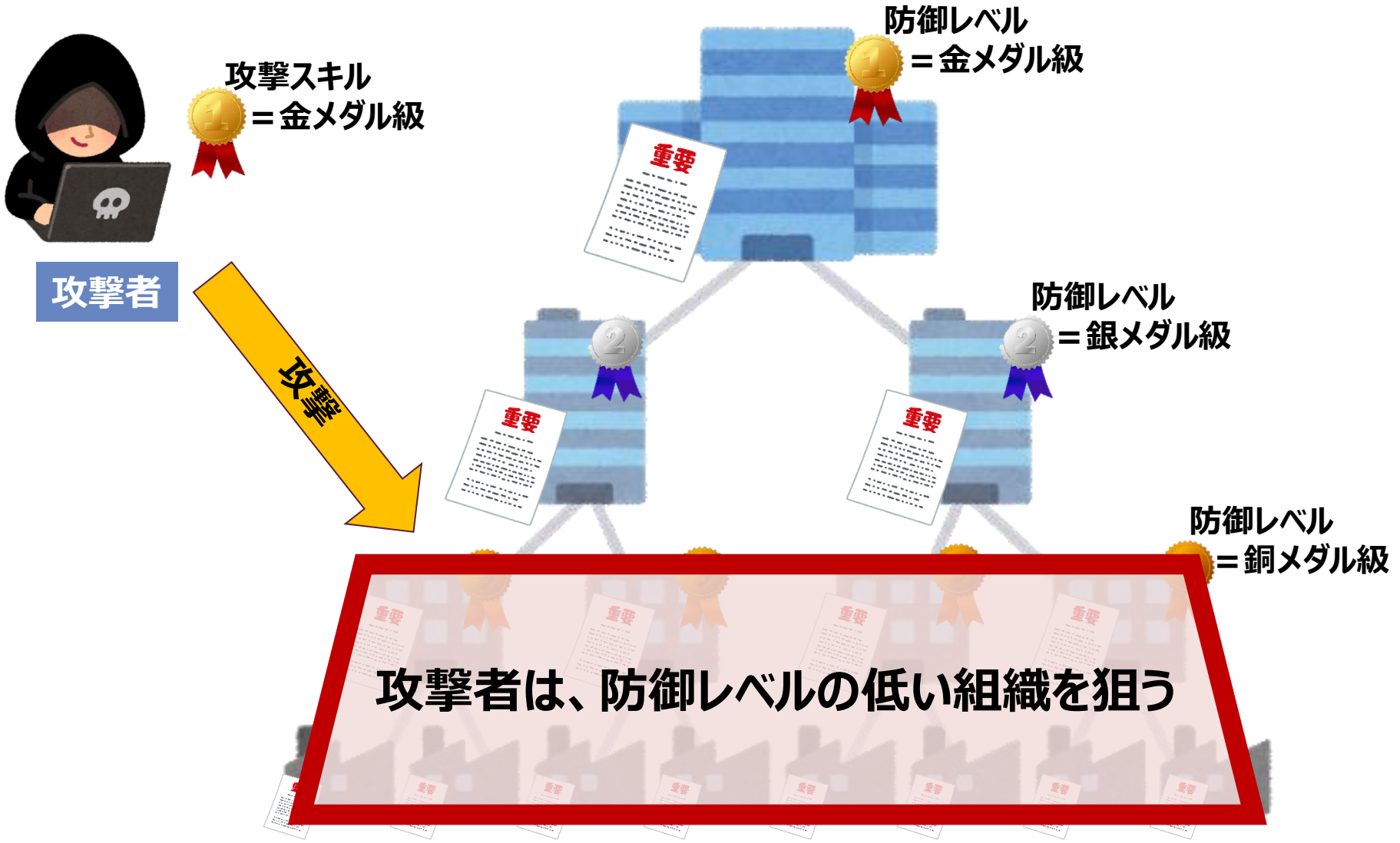
# 攻撃者はサプライチェーンのどこを狙うか

企業の対策レベルはバラバラだが、「金（カネ）」になる重要情報は至る所に存在する。



# 攻撃者はサプライチェーンのどこを狙うか

企業の対策レベルはバラバラだが、「金（カネ）」になる重要情報は至る所に存在する。

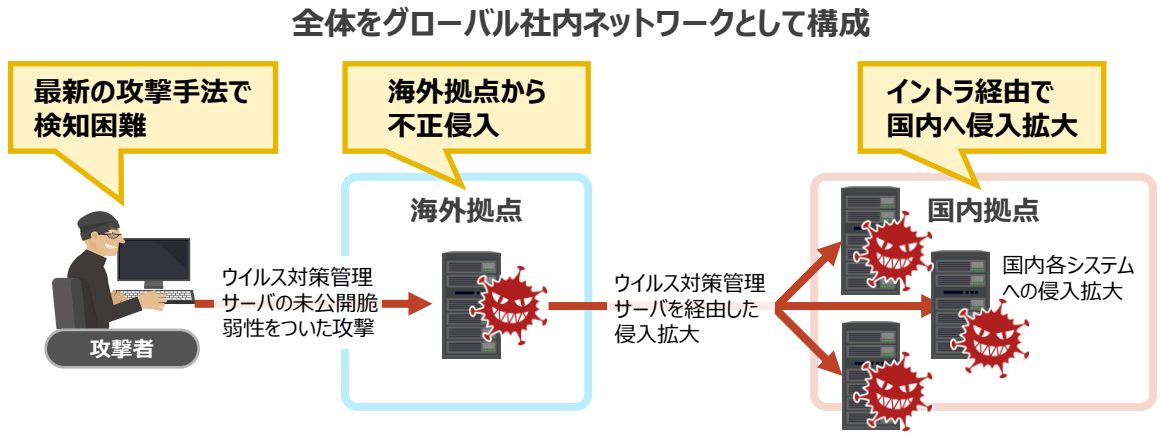


# 狙われるサプライチェーン：海外拠点／国内G会社経由の攻撃

**海外拠点や国内G会社（ 提携先、取引先等を含む）においては、国内本社と同等レベルのセキュリティ対策が十分に取れないケースが多く、攻撃の起点となるケースが増加。**

- **海外拠点**や**国内G会社（提携先、取引先等を含む）**においては様々な原因により、**国内本社と同等レベルのセキュリティ対策が十分に取れない**ケースが多い。
  - 品質管理が不十分なソフトウェア利用、脆弱性放置、私用機器の接続　等
- このような**セキュリティ対策の不十分な拠点において不正侵入を許してしまい、そこを足掛かりに、本社システムの奥深くまで到達されるケースが増加。**

**A社事案における攻撃ルート**




**B社、他数社の事案の概要**

- 国内拠点から侵入され、防衛機密が狙われる。
- 攻撃者は社内の複数システムを渡り歩き、27,445件のファイルが不正アクセスを受ける。
- 検知が遅れていれば、さらなる広範なシステムへの侵入を許していた可能性。

＜経済産業省公表資料を元に編集＞

# 標的型攻撃　不審なメールの特徴

**添付ファイルを開いたり、本文URLをクリックするだけでマルウェアに感染する標的型攻撃メール、ばらまき型攻撃メールについて職場に注意喚起ください。**

## 標的型攻撃メールの例

マルウェアを特定の個人・組織等へ送り込み、機密情報を窃取する

| | |
|---|---|
| 差出人 | XYZ@mail.goo.ne.jp |
| 宛先 | AAA@nttdata.com |
| 件名 | Fw:(打合わせ)人事会議結果 |
| 📎 | 202xxxxx_来期人事情報.doc |

関係各位　お世話になっております
標記について、別添の
よろしくお願いいたし

----○○　人事部
TEL:XX-XXXX-XX


- 受信者がつい開いてしまうような件名のメールを送ってくる。
- 添付ファイル(.doc)を開くとマルウェアに感染する。

＜例＞

- 件名に「Re」が付き、やり取り中を思わせるもの
- 製品やサービスに対する照会 or クレーム
- ゴシップ的な内容、災害情報

## ばらまき型攻撃メールの例

マルウェアを不特定多数の個人・組織等へ送り込む

| | |
|---|---|
| 差出人 | 佐々木　明日香<redirect@xxx.yyyy> |
| 宛先 | BBB@nttdata.com, CCC@nttdata.com,... |
| 件名 | ご請求につきまして |

お世話になっております。

提題の通り、2月分の請求書を
送付させていただきます。
よろしくお願い致します。

請求書は下からダウンロードください
hxxp://vvv.invoice.download.vrs

佐々木


本文のリンクをクリックすると不正なプログラムがダウンロードされ、マルウェア感染する。

# Question

- マルウェア（コンピューターウィルス）の製造に、どの程度時間が必要だと思いますか？

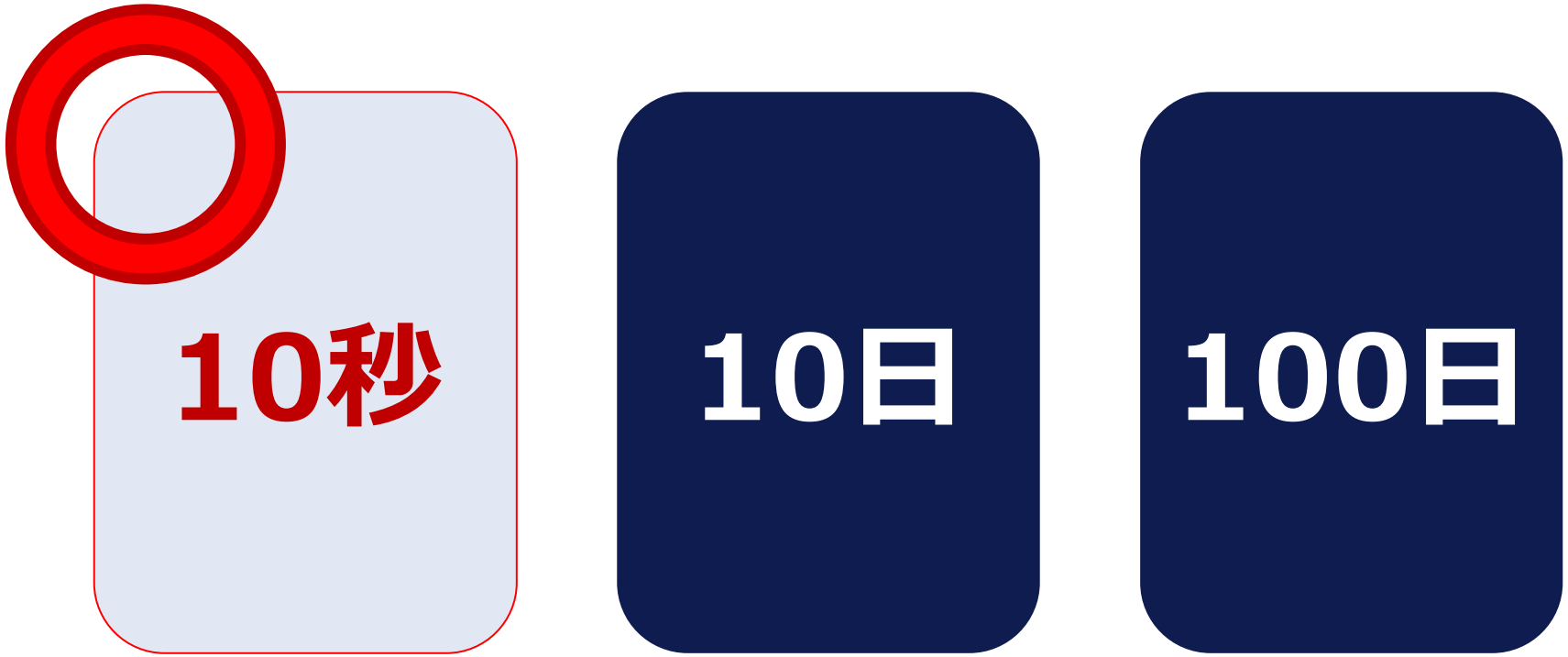
10秒

10日

100日

# Answer

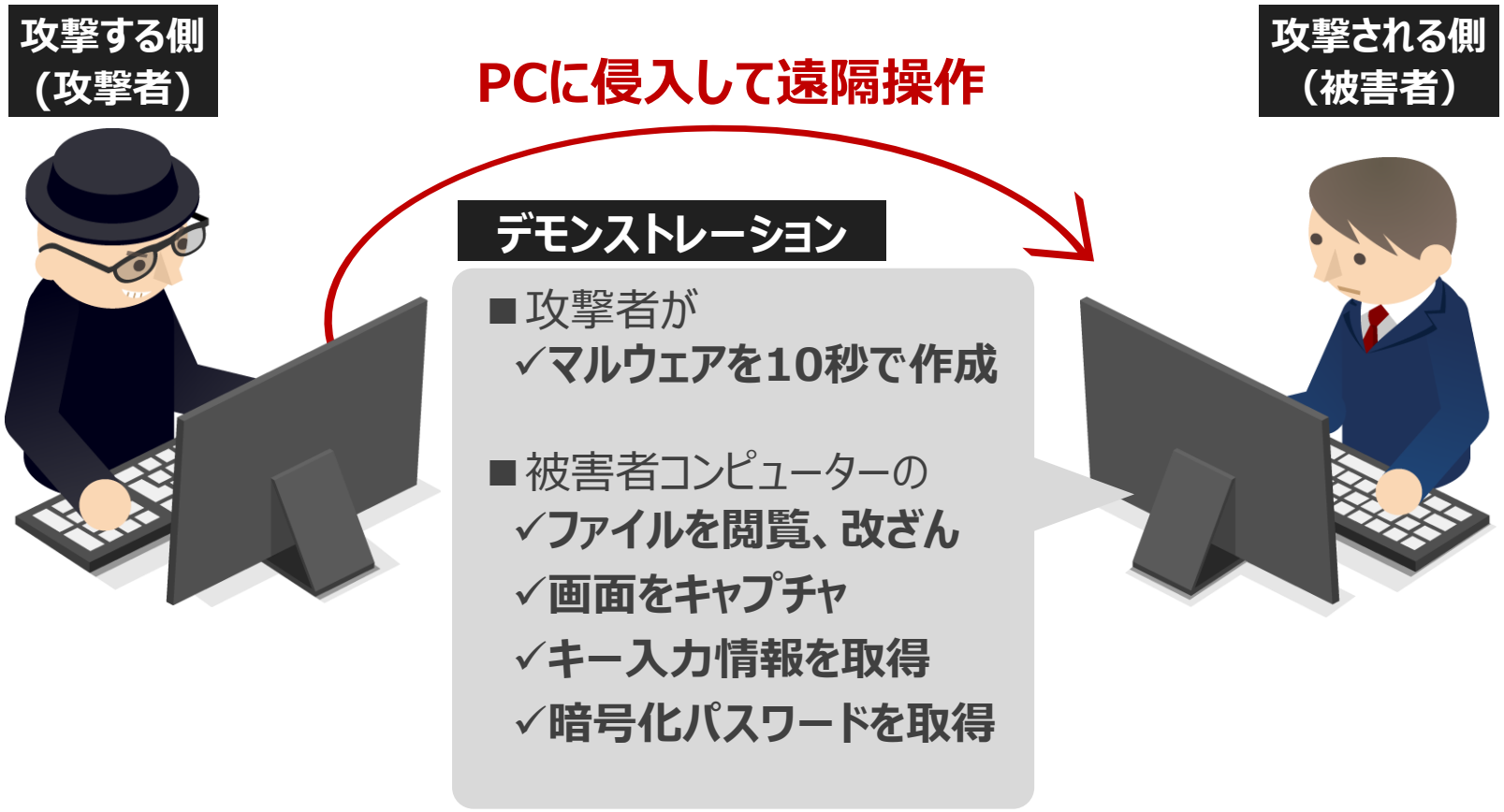
- マルウェア（コンピューターウィルス）の製造に、どの程度時間が必要だと思いますか？



デモ

# 遠隔操作ウィルスのデモンストレーション

**あなたのコンピューターは、こんな風に遠隔操作されている！**



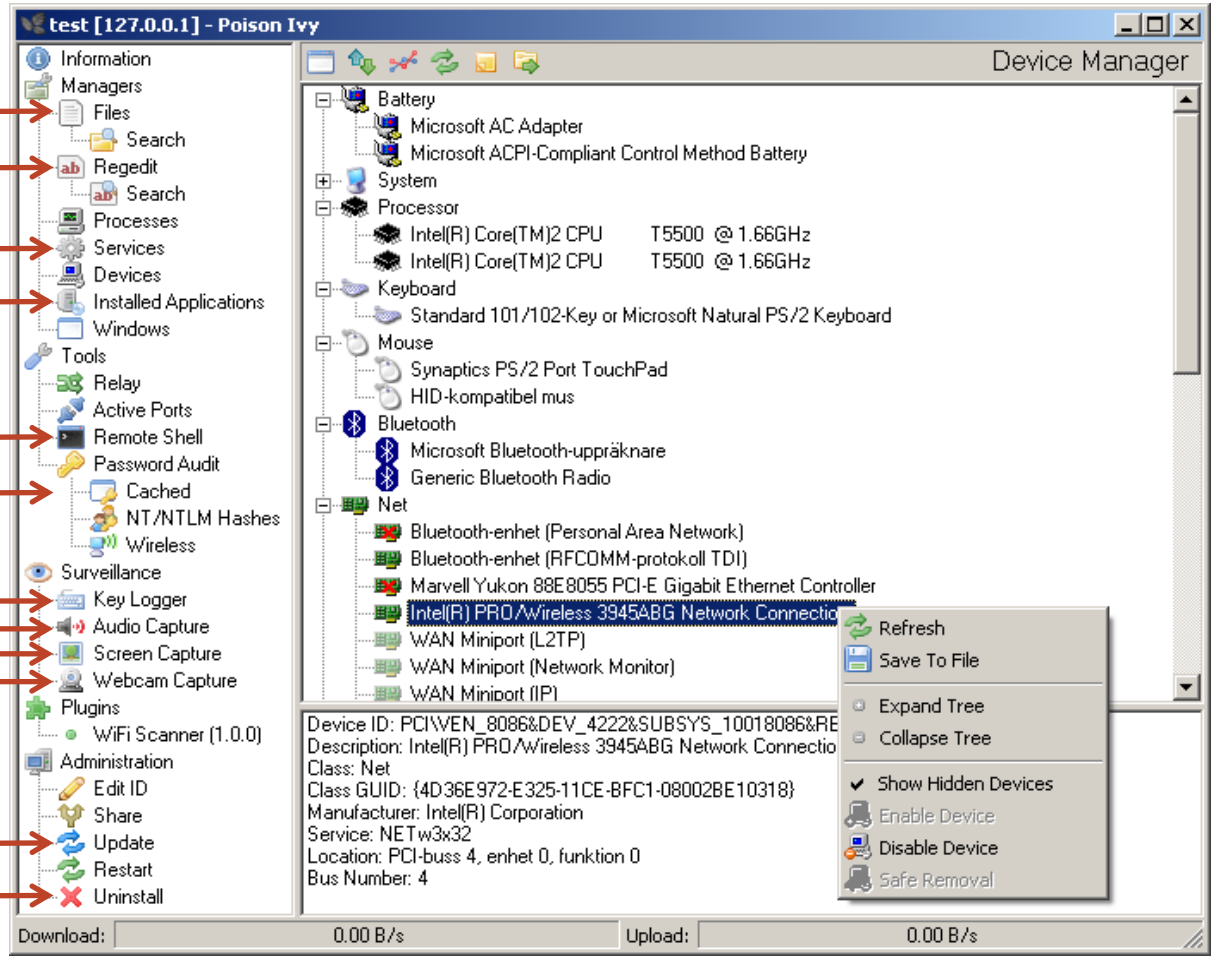



NTT DATA

# 攻撃者が使用するツールは、攻撃メニューが充実

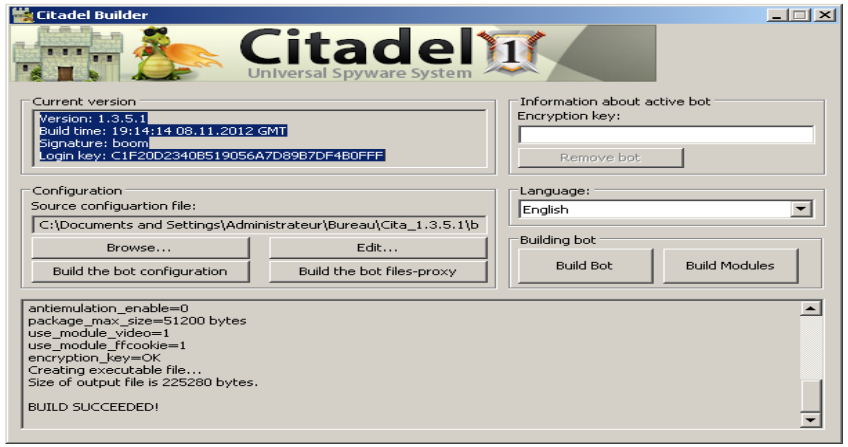
**攻撃メニューが充実した攻撃ツール**

- ファイルの閲覧・改ざん・削除
- レジストリの閲覧・改ざん・削除
- サービスの停止・起動
- パッチなどのアンインストール
- 任意のコマンド実行
- パスワードの取得
- キーロガー
- 音声取得
- 画面取得
- カメラ画像取得
- マルウェアのアップデート
- マルウェアのアンインストール



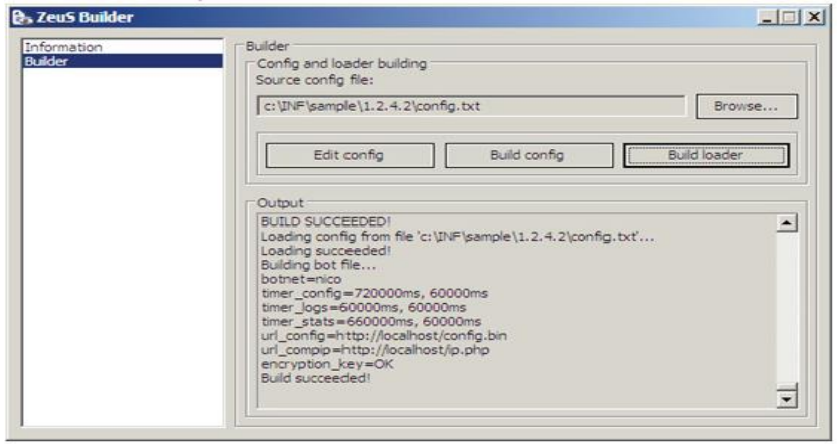
# 多数の使い勝手の良いウィルス製造ツールが存在

## Citadel

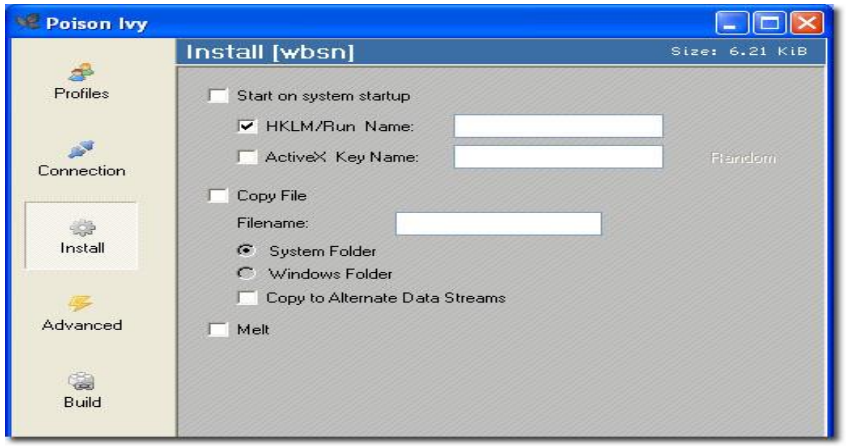



## Spy Eye


## Zeus




## Poison Ivy






NTT DATA

# 情報セキュリティ10大脅威 2022

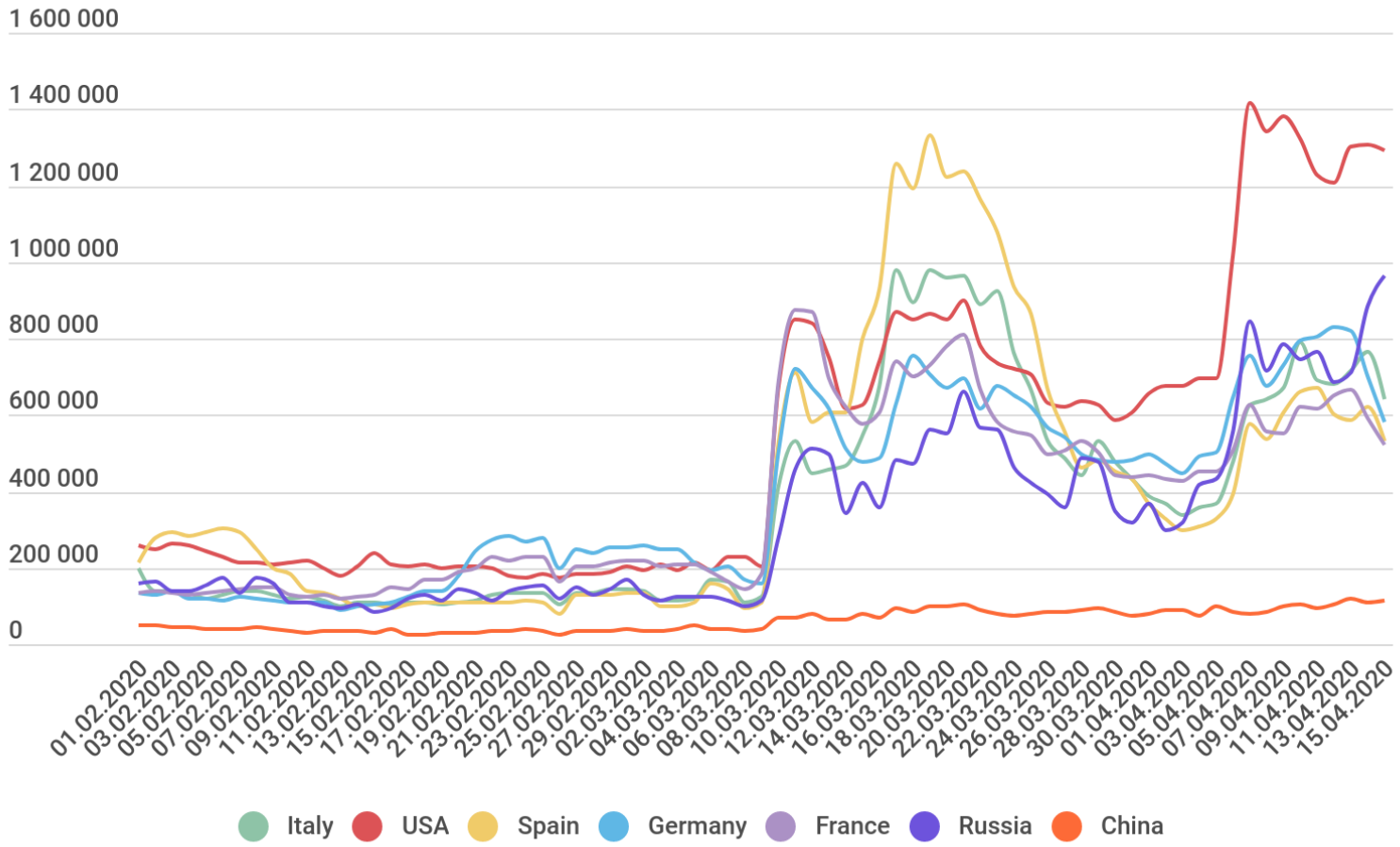
| 昨年順位 | 個人の脅威 | 順位 | 組織の脅威 | 昨年順位 |
|---|---|---|---|---|
| 2位 | フィッシングによる個人情報等の詐取 | 1位 | ランサムウェアによる被害 | 1位 |
| 3位 | ネット上の誹謗・中傷・デマ | 2位 | 標的型攻撃による機密情報の窃取 | 3位 |
| 4位 | メールやSMS等を使った脅迫・詐欺の手口による金銭要求 | 3位 | サプライチェーンの弱点を悪用した攻撃 | 4位 |
| 5位 | クレジットカード情報の不正利用 | 4位 | テレワーク等のニューノーマルな働き方を狙った攻撃 | 3位 |
| 1 位 | スマホ決済の不正利用 | 5位 | 内部不正による情報漏えい | 6位 |
| 8位 | 偽警告によるインターネット詐欺 | 6位 | 脆弱性対策情報の公開に伴う悪用増加 | 10位 |
| 9位 | 不正アプリによるスマートフォン利用者への被害 | 7位 | 修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃） | NEW |
| 7位 | インターネット上のサービスからの個人情報の窃取 | 8位 | ビジネスメール詐欺による金銭被害 | 5位 |
| 6位 | インターネットバンキングの不正利用 | 9位 | 予期せぬIT基盤の障害に伴う業務停止 | 7位 |
| 10位 | インターネット上のサービスへの不正ログイン | 10位 | 不注意による情報漏えい等の被害 | 9位 |

<出典：（独）情報処理推進機構 https://www.ipa.go.jp/security/vuln/10threats2022.html>

# 新型コロナウイルスによるサイバー攻撃の急増

Microsoftのリモートデスクトッププロトコル(RDP)を狙った攻撃が、2020年3月上旬以来急増

**在宅勤務の従業員がアクセスしている会社のリソースを狙って、総当たり方式でパスワードを破ろうとする攻撃が激化**




Growth in the number of attacks by the Bruteforce.Generic.RDP family, February–April 2019

kaspersky

<出典：https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2020/04/29113731/rdp-stats-all.png>



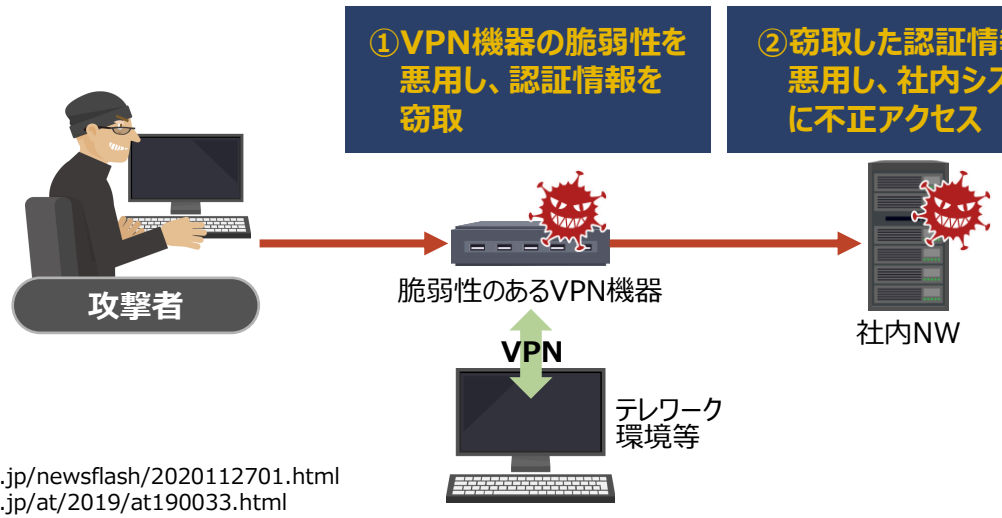
NTT DATA

# 狙われるテレワーク環境：VPN機器の認証情報流出

**テレワーク利用増加に伴い、VPNの利用も増加。VPN機器の脆弱性を悪用され、なりすましログインされたり、マルウェアを送り込まれるインシデントが全世界で急増。**

- **VPN機器の脆弱性**が相次いで報告され、脆弱性を**悪用するコードが公開**されるなど深刻な状況が発生。**攻撃者が直接社内ネットワークへ侵入**し、攻撃を展開。
- **どちらのケースも既に悪用されている可能性**があるため、**機器のアップデートや多要素認証の導入といった事前対策**に加え、事後的措置として**侵害有無の確認や、パスワード変更等の対応**が必要。

## VPN機器に対する不正アクセス




https://www.jpcert.or.jp/newsflash/2020112701.html
https://www.jpcert.or.jp/at/2019/at190033.html

## Pulse Secure製VPN機器の脆弱性

| | |
|---|---|
| 2019年4月 | 脆弱性情報公開 |
| 2019年8月 | 脆弱性の悪用を狙ったとみられるスキャンを確認 |
| 2019年9月 | 脆弱性を悪用したとみられる攻撃を確認 |
| 2020年8月 | **国内外900社（国内は38社）の認証情報が公開** |

## Fortinet製FortiOSの脆弱性

| | |
|---|---|
| 2019年5月 | 脆弱性情報公開 |
| 2019年8月頃 | 脆弱性の詳細情報公開、悪用やスキャン開始 |
| 2020年11月 | **脆弱性の影響を受ける約5万台の機器情報が公開**<br>IPアドレス、ユーザーアカウント名、平文パスワード等 |

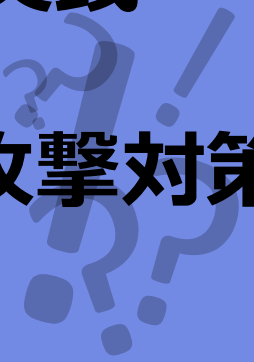
<経済産業省公表資料を元に編集>

1 中小企業も
サイバー攻撃の
標的に

2 サイバー攻撃の
事例と手口

3 サイバー攻撃対策
の勘所

4 今日から実践
すぐできる
サイバー攻撃対策



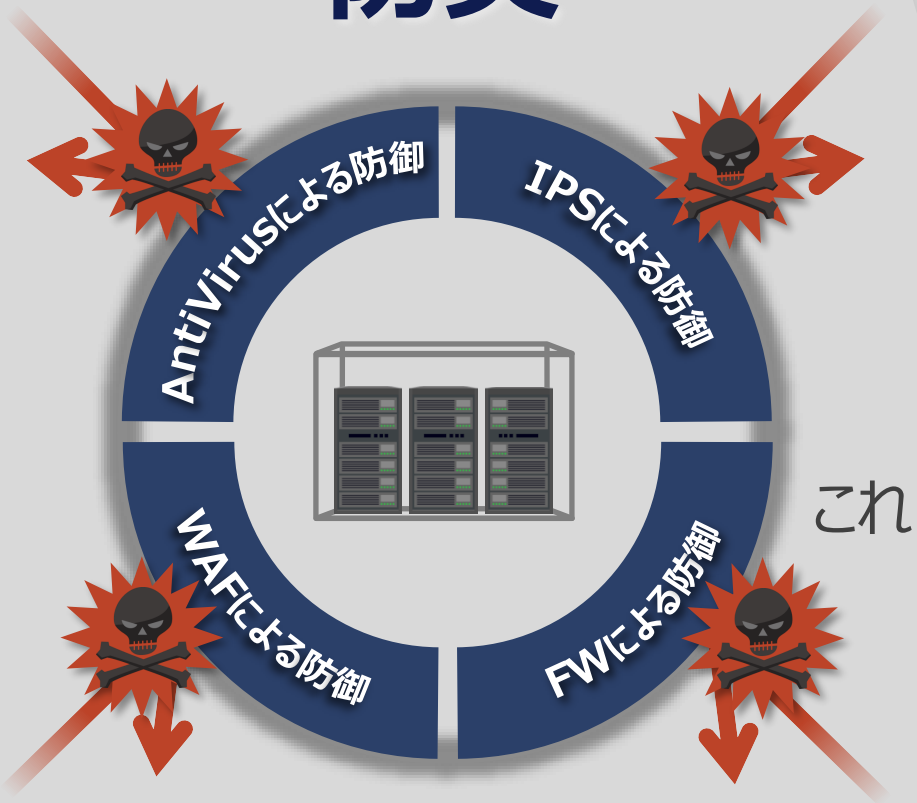


NTT DATA

# サイバー攻撃は攻撃者が圧倒的に有利な状況

# セキュリティ対策に求められる変化

## 防災




対策

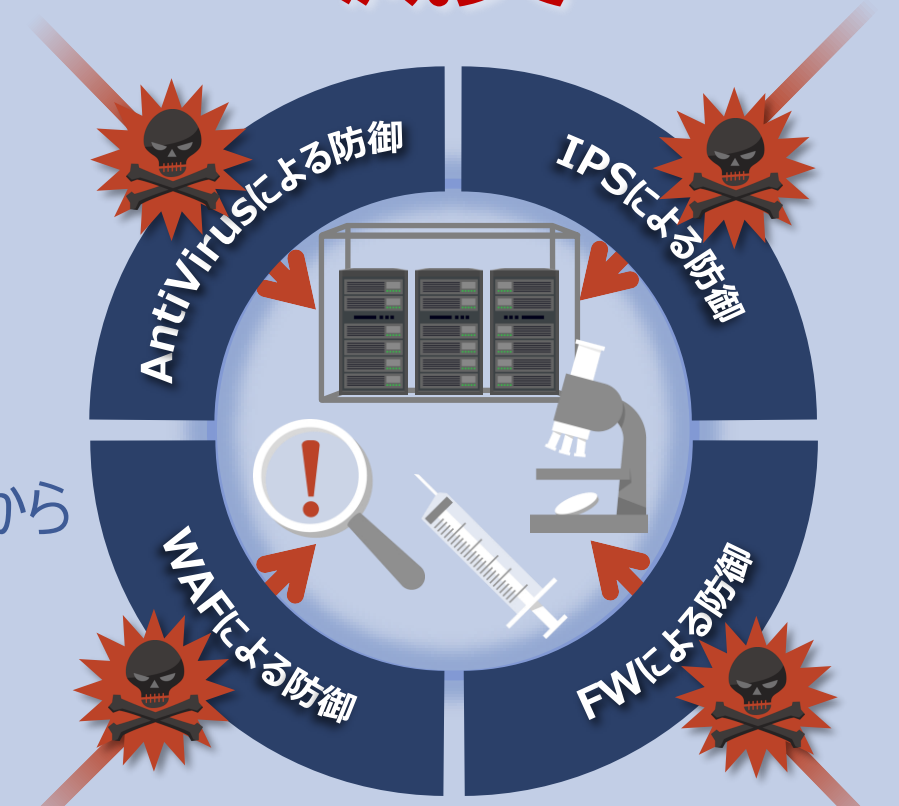
予算配分

| IDS | WAF | FW | 防御 | 検知 | 対応復旧 |
|---|---|---|---|---|---|

これまで

これから

## 減災




| 防御 | 検知 | 対応・復旧 |
|---|---|---|
| 1 | 1 | 1 |



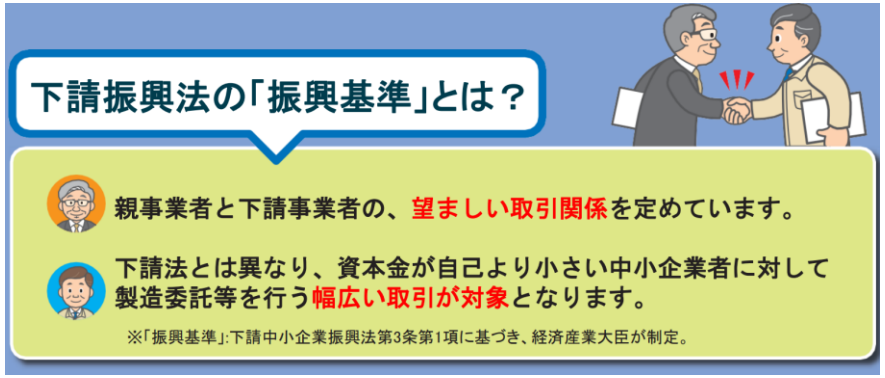
NTT DATA

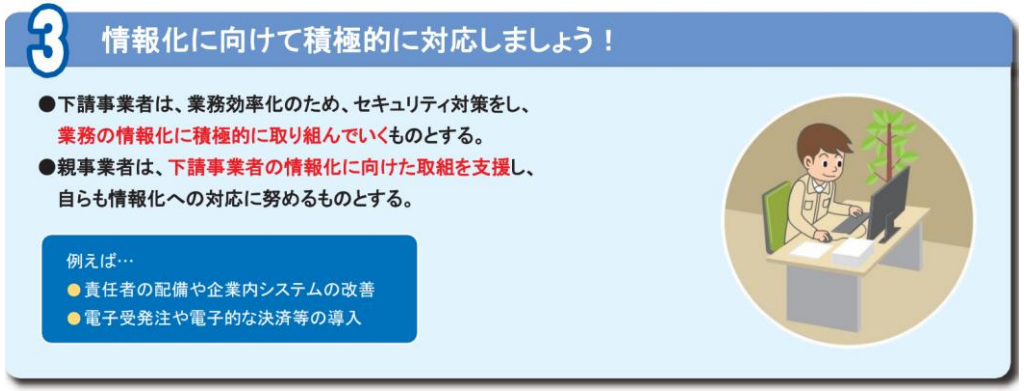
## セキュリティ対策はどこまで進んでいる？

| 現状 | 危険度 | |
|---|---|---|
| 体系的なセキュリティ対策は実施していない。 | 危険 | 既に侵入され、情報が漏洩したり、攻撃者の踏み台となり、他企業を攻撃している可能性があります。 |
| 「**防御的なセキュリティ対策**」は実施済だが、感染の有無を検知する仕組みはない。 | 要注意 | すべてのサイバー攻撃を防ぐことはできません。感染の有無を定期的に確認しましょう。 |
| 侵入されることを前提に、防御だけではなく、「**早期検知・対応・復旧の対策**」を実施している。 | 油断禁物 | サイバー攻撃者の技術は日々進歩します。油断せずに、対策を定期的に見直しましょう。 |

# サプライチェーンで連携してサイバーセキュリティ対応を実施

**下請中小企業振興法の「振興基準」において、下請事業者の要請に応じた、親事業者による下請事業者へのセキュリティ対策の助言・支援が推奨されている。**




**【下請中小企業振興法　振興基準（令和３年７月）】**

第３ 下請事業者の施設又は設備の導入、技術の向上及び事業の共同化に関する事項

**５） 情報化への積極的対応**

⑴ 下請事業者は、管理能力の向上、事務量軽減、事務の迅速化等の業務工程の見直しによる効率性の向上のため、**必要なセキュリティ対策と併せて**、次の事項に積極的に対応していくものとする。

① 情報化に係る責任者の配備及び企業内システムの改善（業務のデジタル化推進を含む）
② 中小企業共通ＥＤＩ（電子データ交換）などによる電子受発注
③ 電子的な決済等（インターネットバンキング、電子記録債権、全銀ＥＤＩシステムなどの活用）

⑵ 親事業者は、前号の下請事業者による取組の支援のため、**下請事業者の要請に応じ、**管理能力の向上についての指導、標準的なコンピュータやソフトウェア、データベースの提供、オペレータの研修、**セキュリティ対策の助言・支援**及び国・地方自治体による情報化支援策の情報提供等の協力を行うものとする。また、サプライチェーン全体の業務工程の見直しによる効率性向上を図る観点から、次号の配慮を行いつつ、電子受発注及び電子的な決済等の導入を積極的に働きかけていくとともに、自らも共通化された電子受発注又は電子的な決済等に係るシステムへの接続に努めるものとする。

https://www.chusho.meti.go.jp/keiei/torihiki/shinkoukijyun/zenbun.pdf

# ランサムウェア攻撃を受けたら読むFAQ

## コンテンツ概要

### (1) コンテンツ内容

- 攻撃を受けた場合の対応のポイントや留意点、よくある質問をFAQ形式を掲載（html形式）
- 攻撃を受けた後の対応に特化したコンテンツ

### (2) コンテンツ想定読者

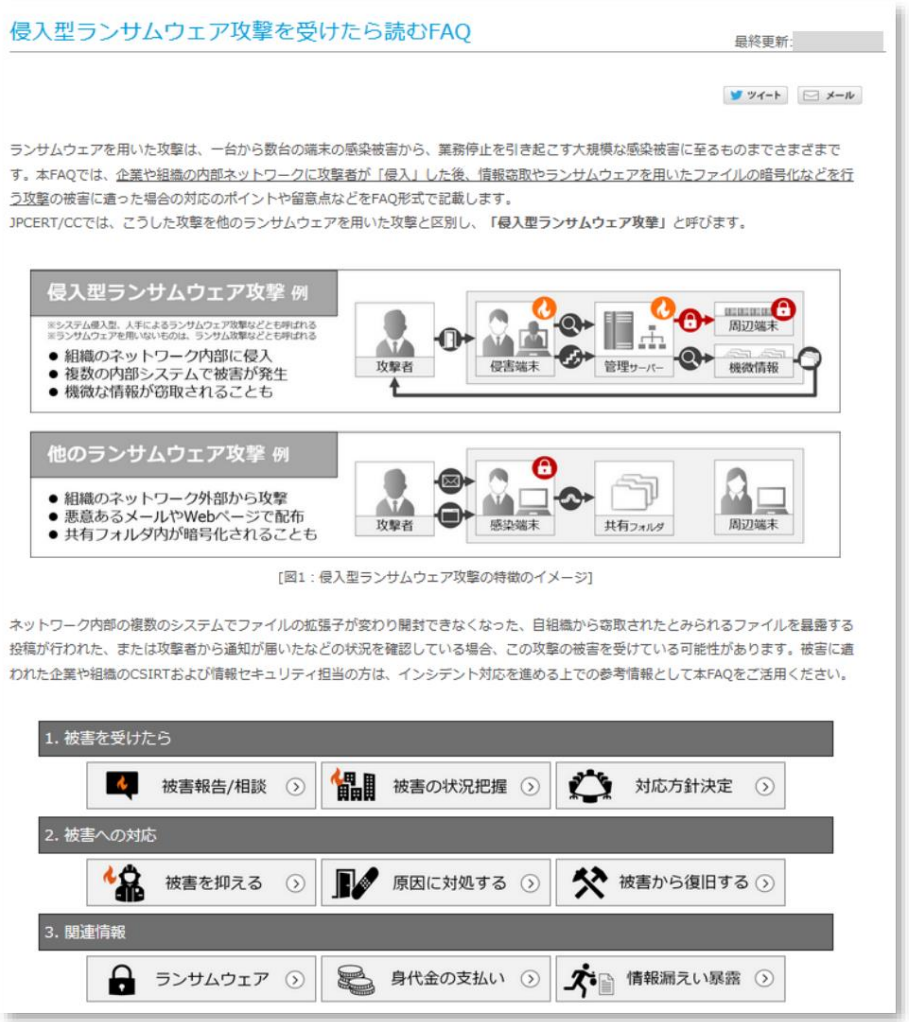
- 被害組織のCSIRT／情報セキュリティ担当
- 被害組織を支援するセキュリティベンダー会社
- 被害組織の支援や捜査にあたる都道府県警　　など

### (3) コンテンツ構成

1. 被害を受けたら：被害報告/相談、状況把握、対応方針決定
2. 被害への対応　：被害最小化、原因対処、被害復旧
3. 関連情報　　：ランサムウェア、身代金支払い、情報漏えい調査

### (4) コンテンツの期待効果

- 攻撃の全体像や侵害原因を速やかに特定
- 不必要なNW停止などを最小限に留めて対応
- 専門機関等へ速やかに報告・連絡

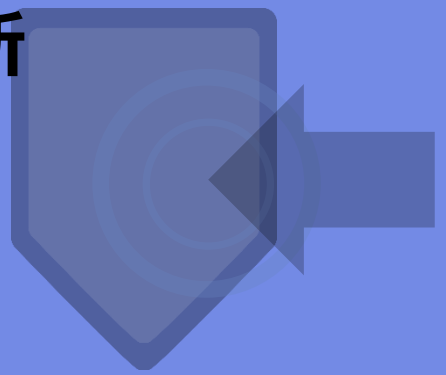



<出典：JPCERT/CC　https://www.jpcert.or.jp/magazine/security/ransom-faq.html>

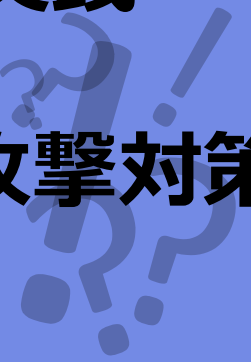
1 中小企業も
サイバー攻撃の
標的に

2 サイバー攻撃の
事例と手口

3 サイバー攻撃対策
の勘所



4 今日から実践
すぐできる
サイバー攻撃対策





NTT DATA

# 今日から実施するセキュリティ対策 ①

**メールにだまされないために**

1. 不用意に添付ファイルを開かない
2. 不用意にURLをクリックしない
3. 少しでも怪しいと思ったときは、添付ファイルを開いたり
   URLをクリックする前に、類似の攻撃メールが流行していないか調べる（IPA、JPCERT/CCなどのサイト確認）

# 今日から実施するセキュリティ対策 ②

**ウィルス感染を防ぐために**

1. セキュリティパッチは、公表後**1週間以内**にあてる
2. Windows、ブラウザ（IE、Chrome、Firefox）、MS-Office、Adobe、Javaのパッチは最優先
3. ホームルーター等、ネット接続する**家電のファームウェア**のアップデートも忘れずに
4. 初期設定されているパスワードは変更

# 今日から実施するセキュリティ対策 ③

**USB等を安全に利用するために**

1. 拾ったUSBメモリ（CD/DVD/SDメモリ等の媒体）や中古品は使用しない
2. USBメモリの貸し借りはしない
3. USBケーブルを含めて、パソコンやスマホに物理的に差し込むものは要注意

# 今日から実施するセキュリティ対策④

**暗号化されても困らないように**

1. **大切なデータは、外付けのハードディスク（or SSD）ドライブに保存し、インターネット接続中はPCから取り外しておく**

# 今日から実施するセキュリティ対策 ⑤

**Wi-Fiを安全に利用するために**

1. できる限り、無料Wi-Fiは利用しない
   Wi-Fiルーターを持ち歩く
2. 暗号化されていないWi-Fi や
   弱い暗号化(WEP)のWi-Fiは利用しない
3. ブラウザのみを使用し「https://」のサイトにだけアクセスする（現実的には困難）
4. VPN通信を利用

# 今日から実施するセキュリティ対策⑥

## アンチウィルスソフトの使用法

1. パターンファイル（シグネチャ）は毎日更新
2. リアルタイムスキャン（リアルタイム保護）を有効に
3. 昔に感染して潜伏中のウィルスを見つけ出すために、
   フルスキャン（完全スキャン）も必ず有効に
4. フルスキャンの頻度は1日1回
   PCが重たくなっても止めない！

# 今日から実施するセキュリティ対策⑦

**他人に迷惑をかけないように**

1. セキュリティ対策をしていない貴方の端末が、他人に迷惑をかけるということを忘れずに

# 今日から実施するセキュリティ対策⑧

**不正ログイン被害に遭わないために**

1. 簡単なパスワードは駄目。最低でも8文字(できれば10文字）以上で、英大文字・英小文字・数字・記号から3種類以上を混ぜて
2. パソコン内にパスワードをメモしたファイルを保存しない
   自宅であれば紙に書いて保管の方が安全
3. Webサイト毎にパスワードを変える

# 今日から実施するセキュリティ対策⑨

**不正送金の被害に遭わないために**

1. 自分の端末がウィルス感染しないように対策を
2. セキュリティ対策がしっかりした銀行を選ぶ
3. ATMの利用限度額・限度回数は低めに設定
4. 最低でもワンタイムパスワードを利用
5. できれば、トランザクション認証、二経路認証を利用

## まとめ

### サイバー攻撃に遭うと

- 大切なデータが盗まれる
- 大切なデータが破壊される
- 口座からお金が盗まれる
- 貴方の端末が加害者に

### マルウェアなどのサイバー攻撃を完全に防ぐことは可能か

- コンピュータを使用している以上、残念ながら不可能です
- **継続的なセキュリティ対策**を

NTT DATA

Trusted Global Innovator

本資料に記載されている会社名、商品名、又はサービス名は、各社の登録商標又は商標です。