最新の脅威動向と中小企業のお客様にご提案いただきたいセキュリティ対策

トレンドマイクロ株式会社

シニアプロダクトマーケティングマネージャー（SMB）

坂本健太郎

本セッションの内容

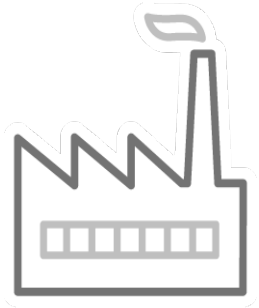
- 最新の脅威動向（２０２２年総括）

- 中小企業のお客様にご提案いただきたいこと

最新の脅威動向（２０２２年総括）

「サイバーリスク＝ビジネスリスク」

事業に甚大な被害が発生した２つの象徴的事件



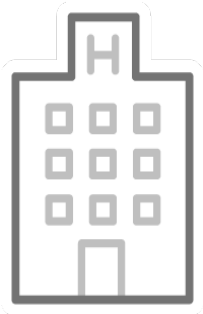
2022年3月：工場ラインの停止(国内自動車メーカー)

取引先部品メーカーのランサムウェア被害の影響により、
自動車メーカーに関連する国内全工場14カ所の28ラインを停止。
翌日再開したが、約1万3000台の生産に影響。

2022年10月：手術や診療の停止(国内医療機関)

大阪の医療センターがランサムウェアに感染、電子カルテシステムを含む基幹システムに障害が発生、緊急以外の手術や外来診療の一時停止など、通常診療ができない状況に。

12月12日に電子カルテシステムが一部再稼働。



「サイバーリスク＝ビジネスリスク」を示す象徴的な被害が日本国内で発生

ビジネスを停止させるランサムウェア攻撃

組織のサイバーリスクが事業への甚大な被害として顕在化

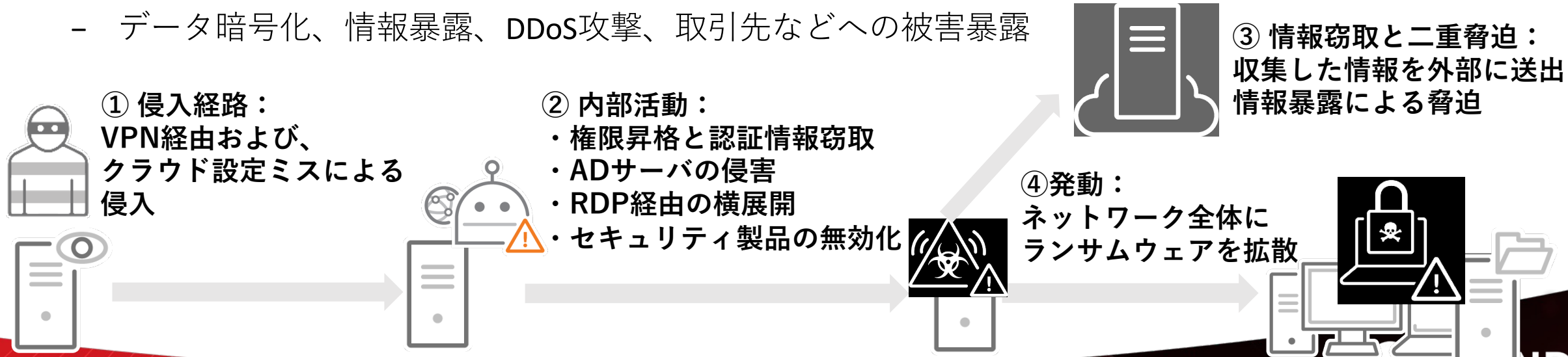
サイバーリスクに繋がるビジネスとセキュリティの不整合

ビジネスを停止させる
ランサムウェア攻撃

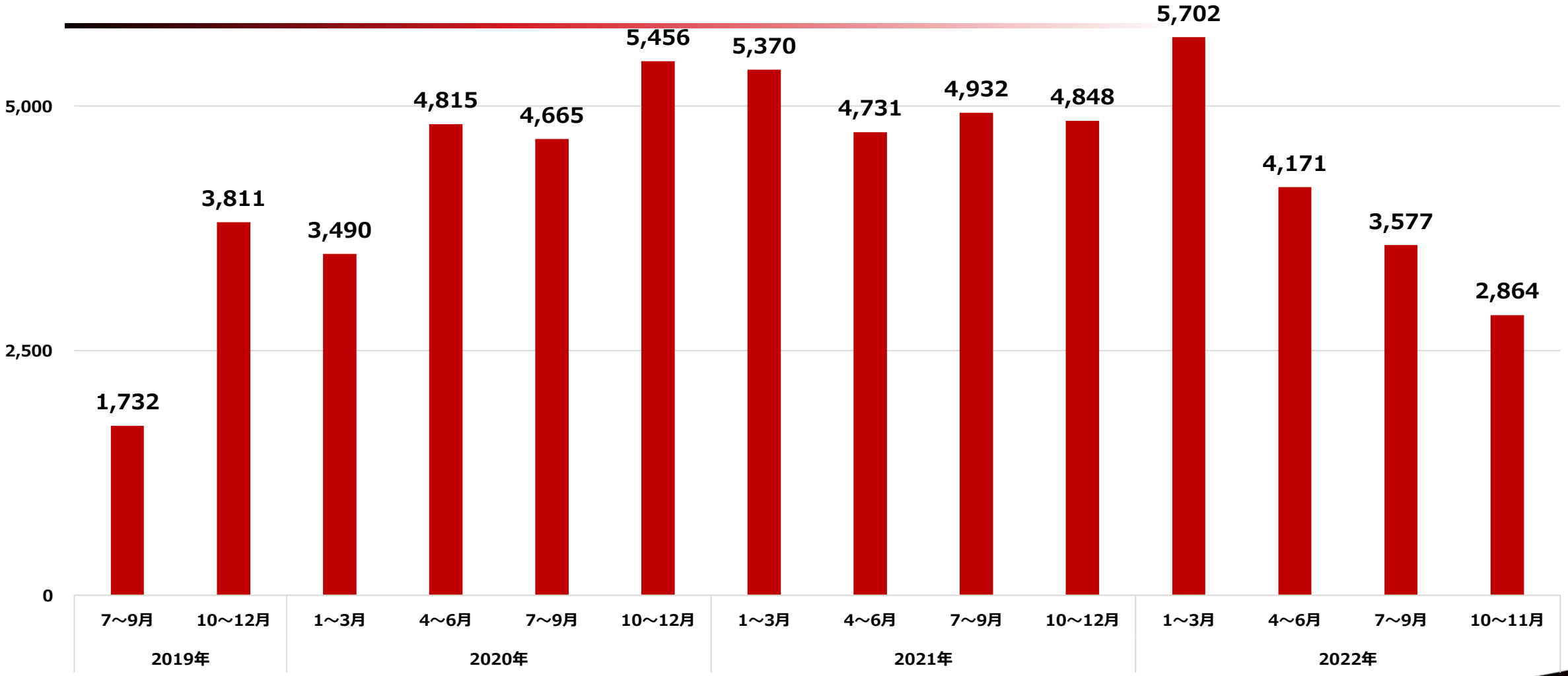
TREND MICRO™

現在のランサムウェア攻撃＝標的型

- **ネットワーク内への侵入と内部活動：**
  - メール経由に加え、**VPN経由**（脆弱性攻撃、認証突破）などの**直接侵入が顕著化**
  - **管理者権限**と認証情報の窃取、**ADサーバ**の侵害と**グループポリシー**の悪用、**ファイル共有やRDP**を利用した横展開、セキュリティ製品の無効化/アンインストール
- **二重（多重）脅迫による身代金要求：**
  - データ暗号化、情報暴露、DDoS攻撃、取引先などへの被害暴露



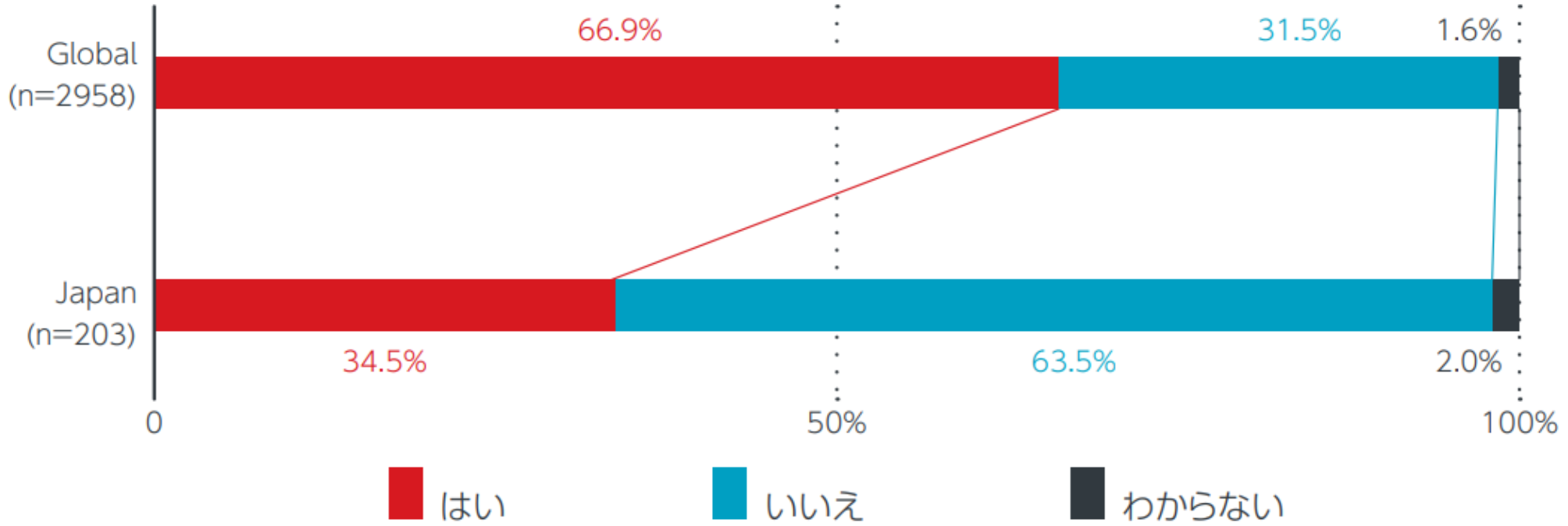
国内ランサムウェア検出台数が2019年以降最多を記録



図：国内でのランサムウェア検出台数推移（トレンドマイクロ調べ）

国内の「3社に1社」にランサムウェア攻撃

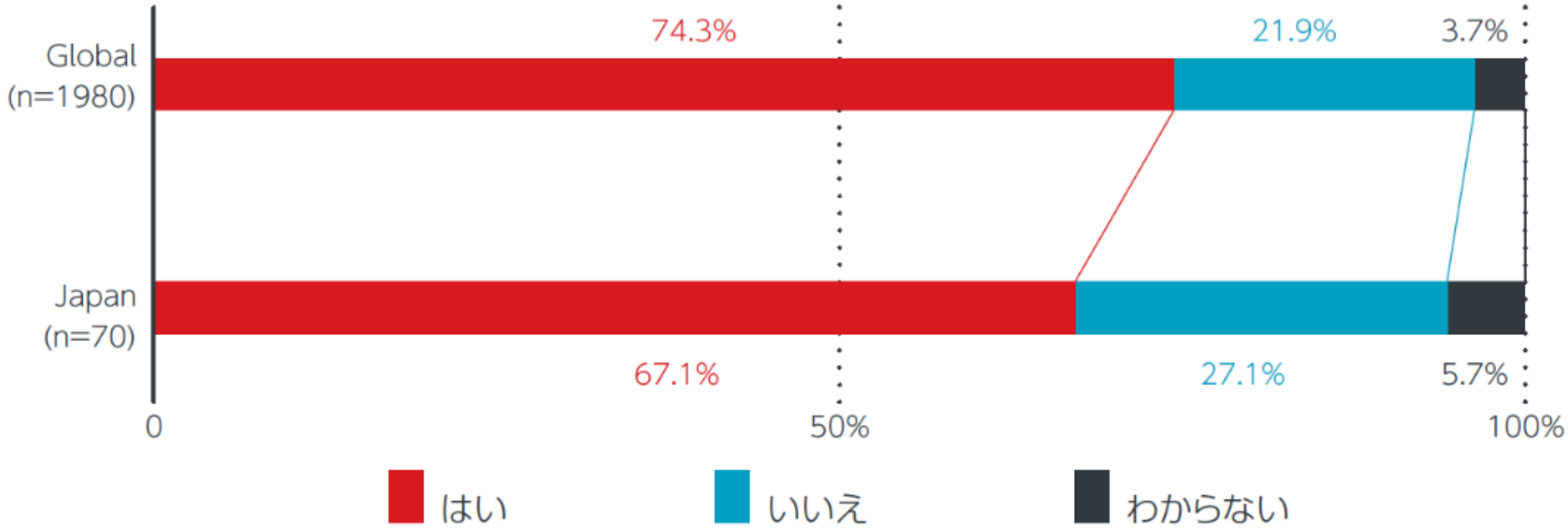
- ランサムウェア攻撃を受けた割合
  あなたの組織は、過去3年間にランサムウェアの攻撃を受けたことがありますか？



【出典】「ランサムウェア攻撃 グローバル実態調査 2022年版」（2022年、トレンドマイクロ）
https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20220907-01.html

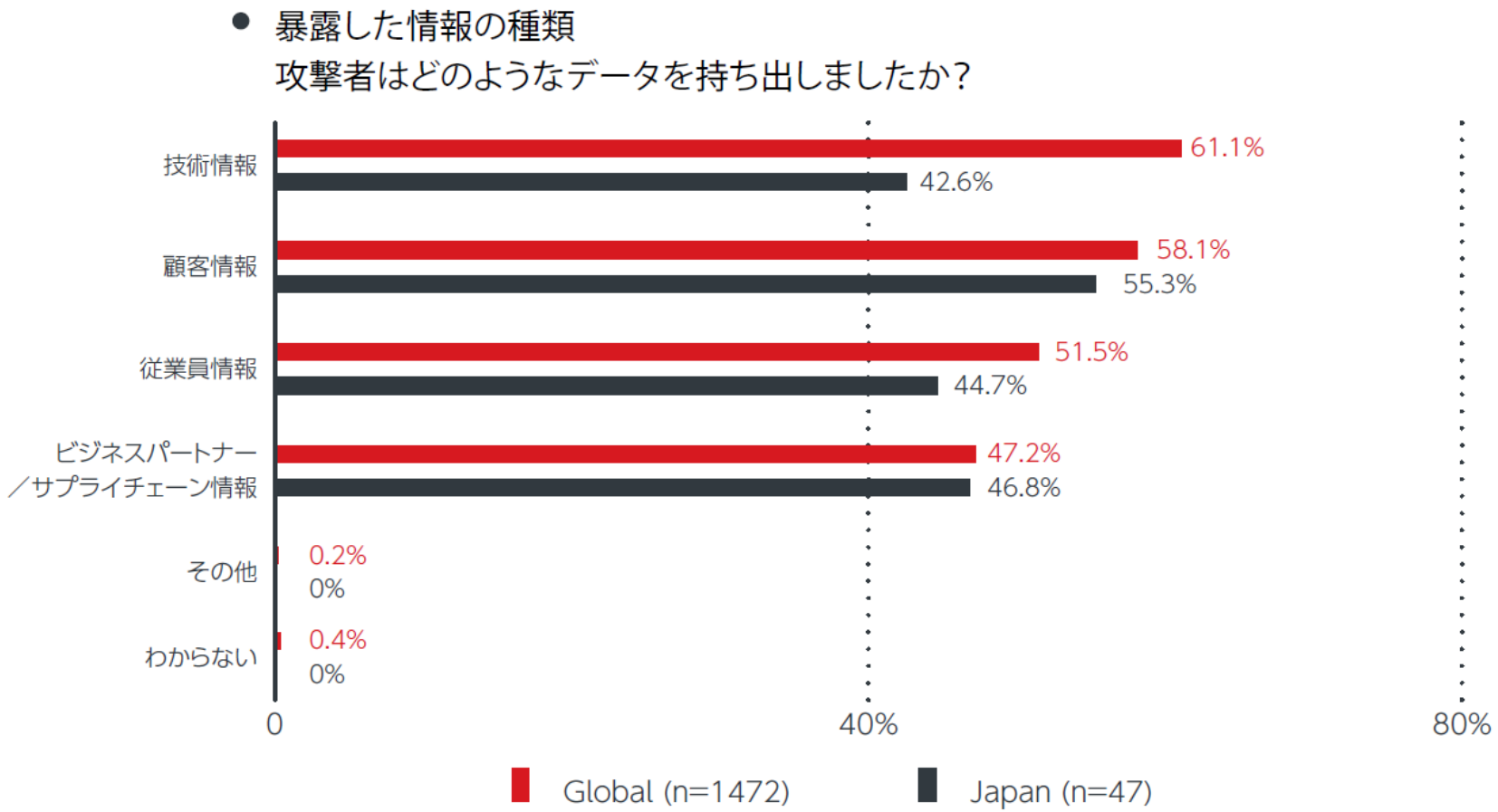
二重脅迫：日本国内は約7割で情報漏洩

- 情報暴露の脅迫（二重脅迫）
  ご勤務先は、ランサムウェア攻撃の際にデータの流出に関して恐喝を受けましたか？



【出典】「ランサムウェア攻撃 グローバル実態調査 2022年版」（2022年、トレンドマイクロ）
https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20220907-01.html

二重脅迫：特に技術情報・顧客情報が漏洩



【出典】「ランサムウェア攻撃 グローバル実態調査 2022年版」（2022年、トレンドマイクロ）
https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20220907-01.html

ランサムウェア攻撃が組織にもたらす甚大な影響

データが暗号化されることで
生産活動や営業活動などを行えなくなる

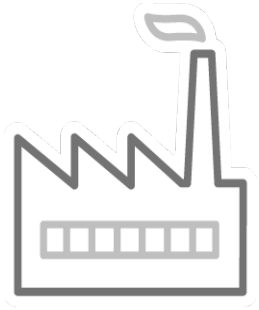
ビジネスの中断や破綻による
「顧客離れ」
「サプライチェーン」からの離脱

顧客やビジネスパートナーからの
「信用失墜」
損害賠償等の「金銭的損失」

組織のサイバーリスクが
事業への甚大な被害として顕在化

TREND MICRO™

事業に甚大な被害が発生した２つの象徴的事件



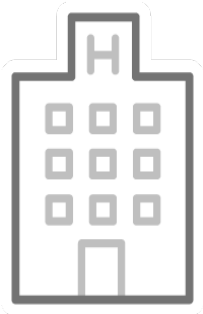
2022年3月：工場ラインの停止(国内自動車メーカー)

取引先部品メーカーのランサムウェア被害の影響により、
自動車メーカーに関連する国内全工場14カ所の28ラインを停止。
翌日再開したが、約1万3000台の生産に影響。

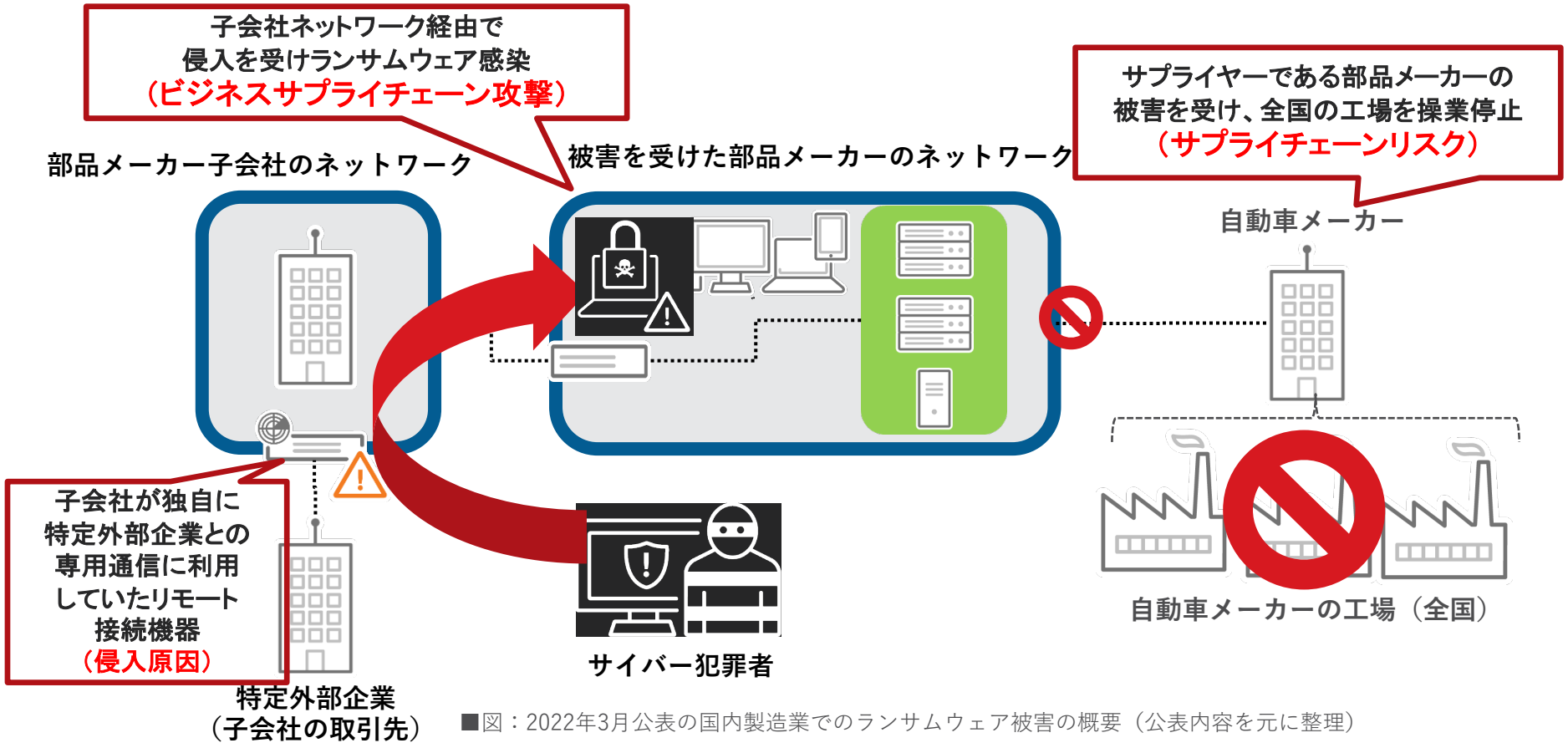
2022年10月：手術や診療の停止(国内医療機関)

大阪の医療センターがランサムウェアに感染、電子カルテシステムを含む基幹システムに障害が発生、緊急以外の手術や外来診療の一時停止など、通常診療ができない状況に。

12月12日に電子カルテシステムが一部再稼働。



「業務上の繋がり」を経由した被害連鎖（国内自動車メーカー事例）



■図：2022年3月公表の国内製造業でのランサムウェア被害の概要（公表内容を元に整理）

サプライチェーンの弱点

◆サプライチェーンリスク：

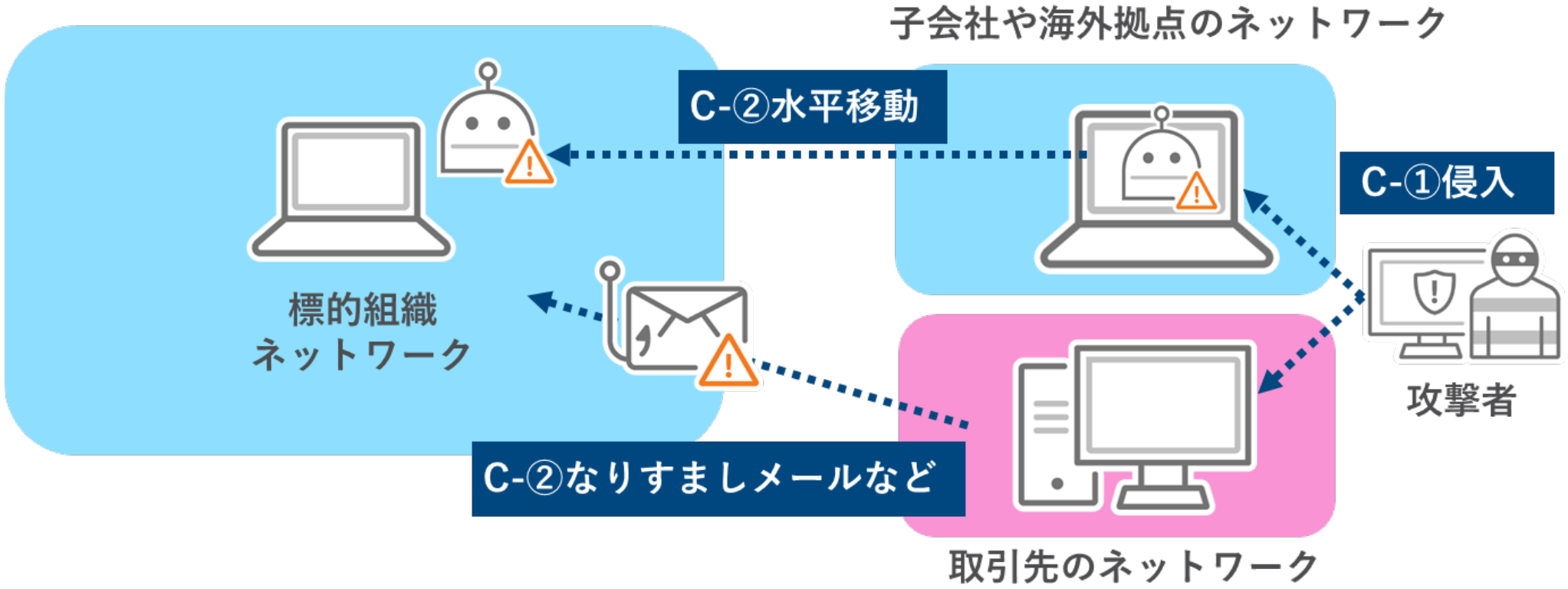
サプライチェーン上の要因によって計画的な供給ができなくなるリスク

◆サプライチェーン攻撃：

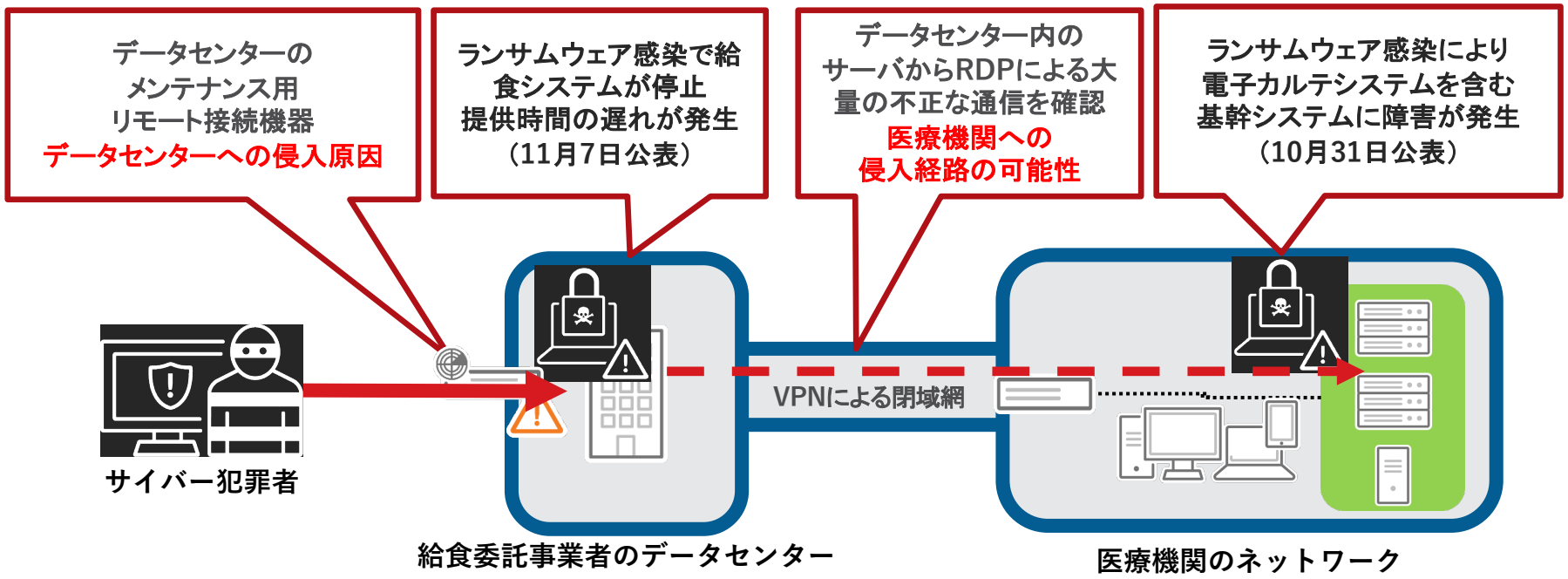
サプライチェーンにおける業務上の繋がりを利用して、
取引先や子会社を標的組織への攻撃の踏み台とするサイバー攻撃手法
サプライチェーンリスクの中の一要因

業務上の繋がりで広まる「ビジネスサプライチェーン攻撃」

既に信用している相手から攻撃が来るため、侵入段階で気づくことが困難
自社が踏み台になる「加害者」リスクも

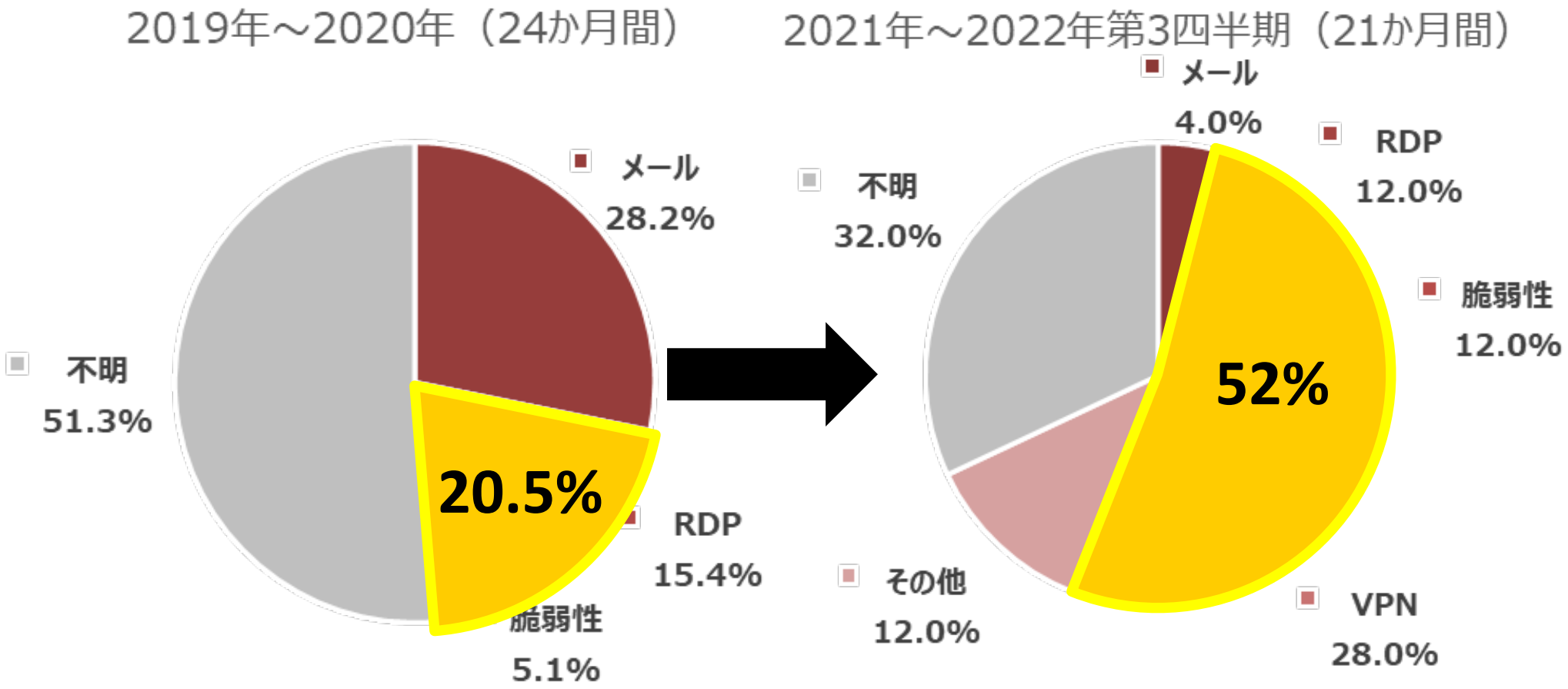


システム上の弱点を悪用した攻撃（国内医療機関の事例）



■図：2022年10月公表の国内医療機関でのランサムウェア被害の概要（公表内容を元に整理）

攻撃者は弱い所を狙う



■図：トレンドマイクロが詳細を調査した国内法人組織のインシデントにおける侵入経路種別

セキュリティ上の弱点＝顕在化したリスク

◆サプライチェーンのリスク：

サプライチェーンを構成する他組織が侵入口となる
既に信用している他組織の侵害を起点に自組織に被害が連鎖

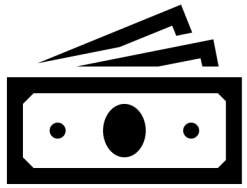
◆システム上のリスク：

VPN、RDPなど、外部からのアクセス経路に
脆弱性や突破可能な認証情報などの弱点が存在し、侵入を許す

サイバーリスクに繋がる
ビジネスとセキュリティの不整合

TREND MICRO™

リスクの主体が「事業基盤」へと変化しビジネスモデルが狙われる時代に



サイバーリスクが
経済的損害に
直結するようになった

直近3年間に起きたサイバー事故/事件

- 電子決済サービスからの不正送金
- ランサムウェアによる工場の操業停止
- 教育事業者が開発したアプリ経由の情報漏洩
- ランサムウェアによる石油パイプライン停止
- 暗号通貨交換所から580億円相当の暗号通貨が流出
- ATMマルウェアによるATMからの不正出金
- SWIFTコードによる金融取引が狙われた不正送金

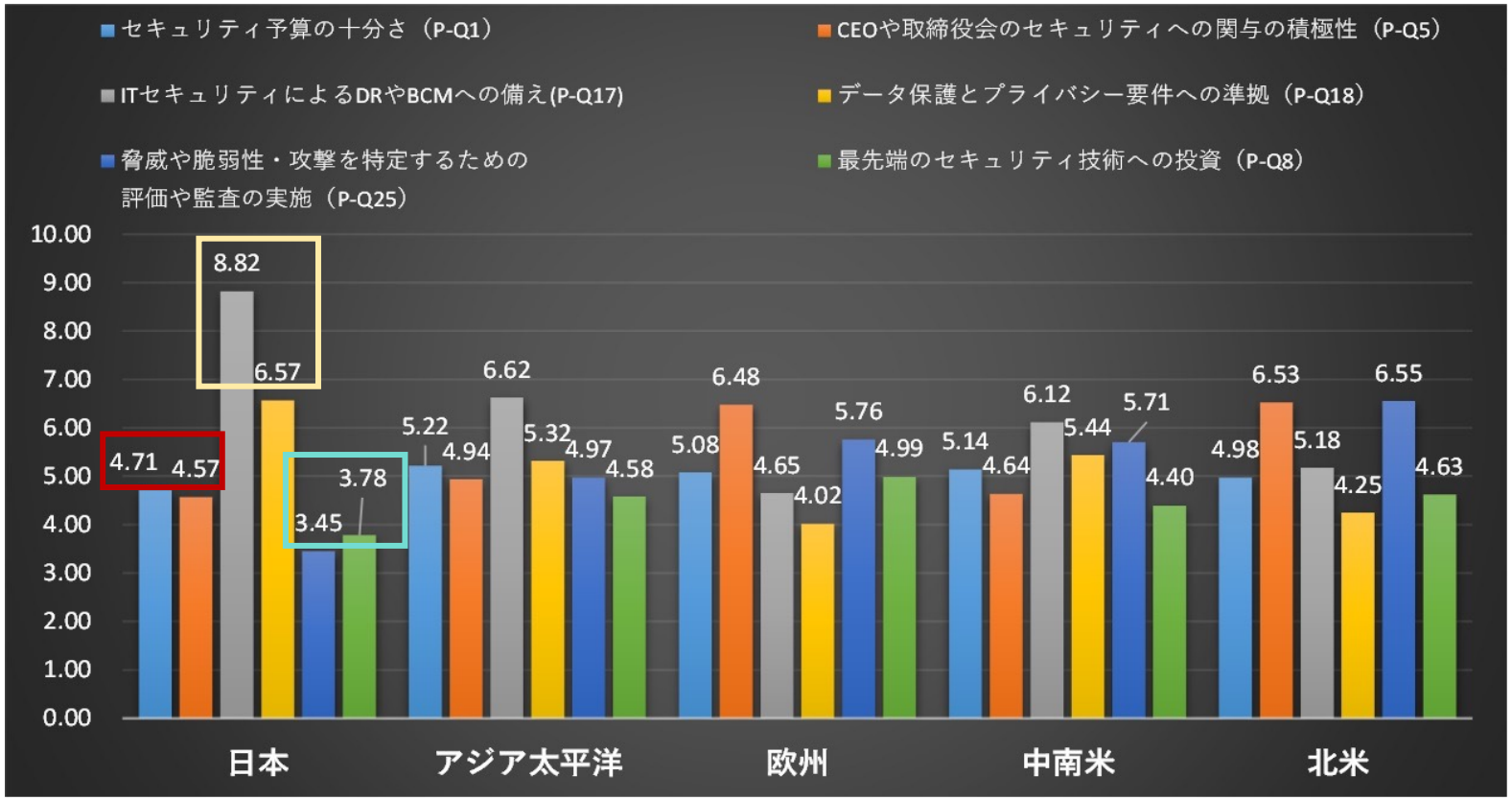
ビジネスとセキュリティの不整合を解消するために
サイバーレジリエンスを向上させることが重要

基本の考え

- **サイバーリスクをビジネスリスクとして認識する**

- **復旧までを見据えたセキュリティの構築**
  →「侵入されなければ被害も発生しない」から脱却し、
  「侵入を前提」、「被害発生を前提」として対策を考える

不整合：経営陣の積極的な関与が足りない



グラフ：セキュリティの体制構築状況に関する主な質問の結果

■出典：トレンドマイクロ　組織のサイバーセキュリティリスク意識調査「Cyber Risk Index」2021年下半期版
https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20220621-01.html

不整合：経営陣の積極的な関与が足りない

- セキュリティ予算
- 経営陣の積極的な関与

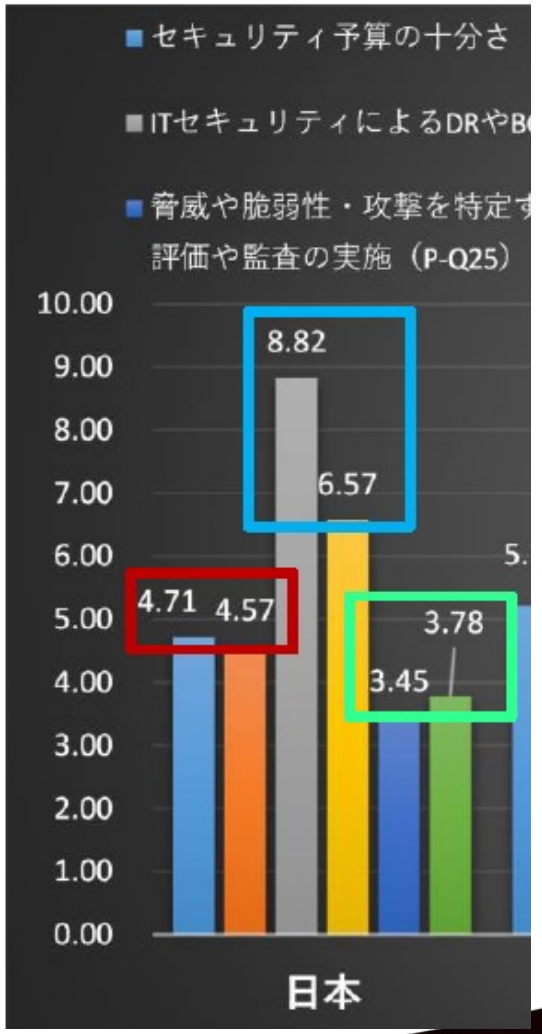
→他のエリアと比較してそれほど多くない/高くない

- ディザスタリカバリなど災害時対策
- プライバシー対策

→他のエリアと比較して突出して高く、かなりよくできている

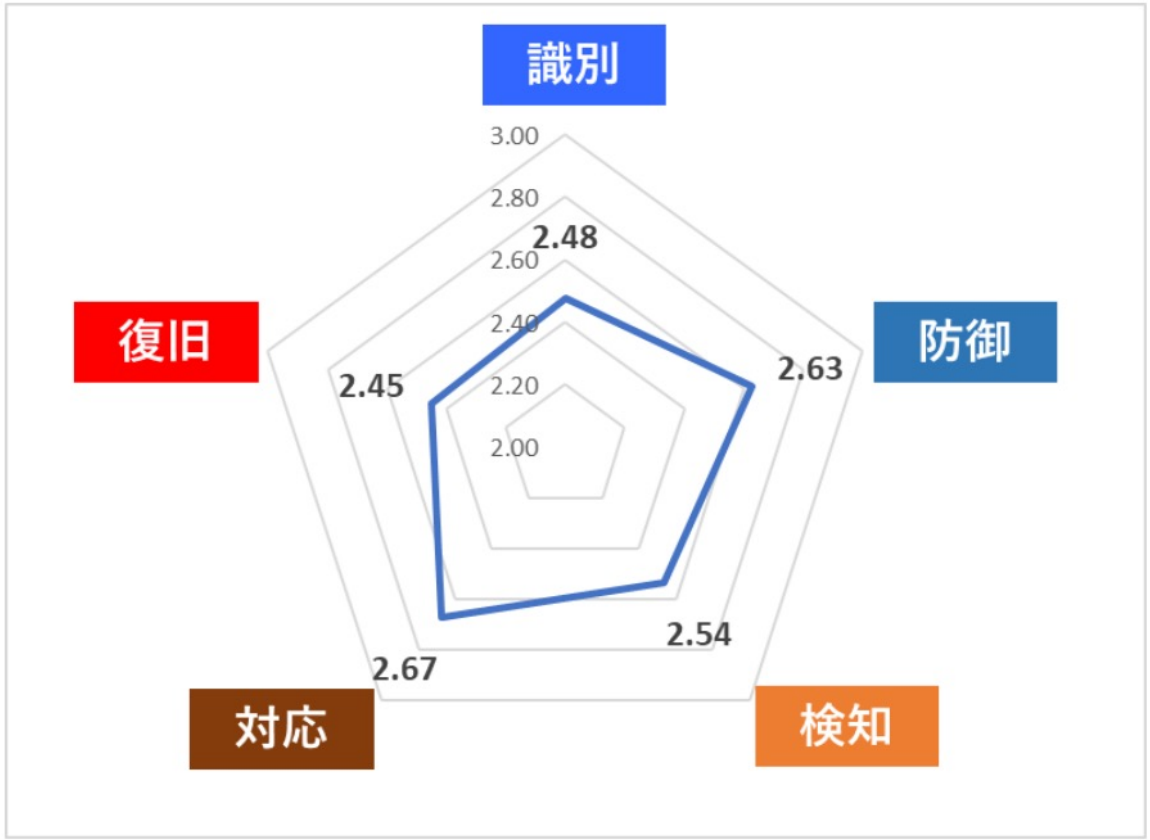
- 脅威、脆弱性、攻撃の特定
- 最先端セキュリティへの投資

→他のエリアより低く、不十分



■出典：トレンドマイクロ　組織のサイバーセキュリティリスク意識調査「Cyber Risk Index」2021年下半期版
https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20220621-01.html

サイバーセキュリティ機能の中では「復旧」が低い



セキュリティ成熟度の機能毎の平均点 (n=253)

■出典：トレンドマイクロ　「法人組織のセキュリティ成熟度調査」（2022年12月に発表）
https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20221207-01.html

セキュリティ担当部門だけでは資産とリスクの特定は難しい

	営業	マーケ	事業開発	製造	開発	広報	法務	財務	人事
情報資産管理	◎	◎	◎	◎	◎	◎	◎	◎	◎
デバイス管理	◎	◎	◎	◎	◎	◎	◎	◎	◎
アプリケーション管理	◎	◎	◎	◎	◎	◎	◎	◎	◎
アクセス権管理	◎	◎	◎	◎	◎	◎	◎	◎	◎
セキュアな企画・設計	○	◎	◎	◎	◎				
セキュアな開発と品質保証（セキュリティ面での）			○	◎	◎				
セキュアな業務オペレーション	◎	◎	◎	◎	○	○	○	◎	◎
サプライチェーンマネジメント	◎	◎	◎	◎	◎	◎	◎	◎	◎
入退室など物理セキュリティ			○						◎
人的セキュリティ			○						◎
事業継続マネジメント			◎	◎	◎				
インシデント対応			○	◎	◎	◎	◎		○

出典：トレンドマイクロ　『プラス・セキュリティ ナレッジトレーニング基礎』　＊テキストより一部抜粋

ビジネスを守るセキュリティはセキュリティ部門だけでは行えない

事業継続上のリスクである以上、
サイバーセキュリティの担当者だけでは不十分

現場にいる関係者を含め、ビジネスに関わる全員が
リスクオーナーの責任を果たす必要がある

→「専門人材以外」がセキュリティの鍵を握る

「専門人材以外」を活用するためのセキュリティ体制構築が必要

セキュリティ体制、特に識別、対応、復旧の段階に
リスクオーナーとして組み込む

セキュリティ意識を高めてもらうための教育

2022年脅威動向総括

2022年脅威動向からの学び

- 「サイバーリスク＝ビジネスリスク」の再認識

ビジネスとセキュリティの整合をとるために

- サイバーレジリエンスの向上

今後のセキュリティの鍵

- 経営陣の積極的な関与と「専門人材以外」の活用

2023年
セキュリティ脅威予測
～ランサムウェアのクラウド対応や窃取情報のマネタイズなど、ビジネスモデルの多様化が進む～

■ プレスリリース（2022年12月26日）
https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20221226-01.html

■ ダウンロードページ
https://resources.trendmicro.com/jp-docdownload-form-m532-web-prediction2023.html

中小企業のお客様にご提案いただきたいこと

当社の考える中小企業の皆様のお困り事

漠然とした不安はあるが、**何をすべきか**わからず対策できていない
・・・という事に、心当たり御座いませんでしょうか？？

インターネットの業務活用が
当たり前に。**社員が自主判断**
で活用していることも

中小企業も高度な攻撃の対象になり
業務停止・データ流出した
ニュース聞き**漠然とした不安**感

自社が**何をすれば**
いいかわからない。
対応できる人財不足

当社の考える中小企業の皆様のお困り事

具体的な対策を検討時に、自社はどこまで対策すればいいかわからなかった
・・・という事に、心当たり御座いませんでしょうか？？

本当に多種多様なセキュリティー対策製品の例（ごく一部です）

自社に最適な製品を選定、運用できる、高度な知見を持つ人人財の確保が困難な事も

ファイアウォール　不正侵入防止　E-mail保護　情報漏洩対策　端末保護

難しいセキュリティー対策は、プロに任せる時代です

TREND MICRO™

日系セキュリティー専業30年による
1台で基本的なセキュリティー対策
が網羅できる**最強の防御機器を・・・**

×

Trend Micro
Partners

皆様に最適な設定で導入
導入後の運用・ご報告まで
手厚いサポートをセットでご提供

最強の防御機器を手厚いサポートとセットで皆様にご提供します

TREND MICRO™

トレンドマイクロの中小企業向け製品

ウイルスバスター ビジネスセキュリティ サービス

手間のかからないエンドポイント
セキュリティサービスで
管理負荷を軽減したい
お客様向け

Worry-Free XDR

エンドポイントセキュリティ運用の
負荷軽減に加え、有事の際に
メール環境も含めた原因の
発見と再発防止を迅速に
行いたいお客様向け

Worry-Free Managed XDR

Worry-Free XDRに加え、
有事の際の調査を含む
マネージドサービスを
受けたいお客様向け

Cloud Edge

ファイアウォールによる一般的
なアクセス制御だけでなく、
不正プログラム対策やURLフィル
タからAI技術や
サンドボックスを使った
高度な脅威検出まで、
幅広いセキュリティを提供

圧倒的なデータ量で迅速な対応を実現

クラウド型セキュリティ基盤：

Trend Micro Smart Protection Network™

世界規模のセンサーネットワーク

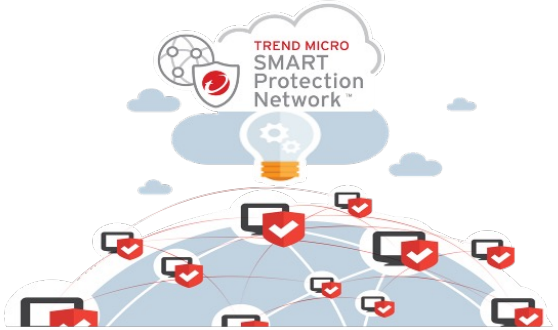
広範囲な地域から膨大な脅威情報を収集

- 2億5,000万以上※1のセンサーを活用
- 年間2兆6,000万件※2以上のクエリ処理
- ファイル、IPアドレス、URL、モバイルアプリ、脆弱性などの情報を収集

世界規模の脅威インテリジェンス

正確な分析と迅速な脅威の検知

- テラバイト単位のデータを分析
- 年間54億件※2以上の新たな脅威を検知
- 高度な分析によるリアルタイム検出とゼロアワー攻撃の検出



先の脅威を見越した防御力

新たな脅威を素早くブロック

- 年間520億件以上※2の脅威をブロック
- 全世界の法人組織、個人ユーザ、ファミリーを脅威から保護

※1 2017年トレンドマイクロ調べ
※2 2020年6月トレンドマイクロ調べ

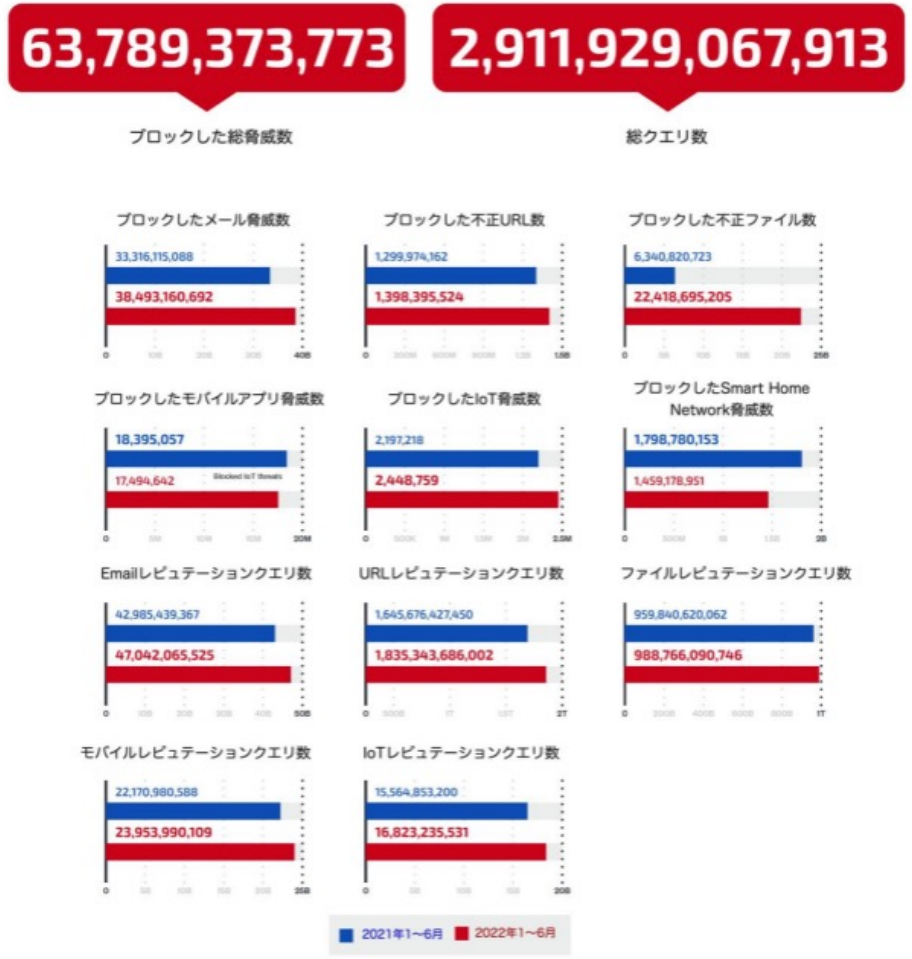


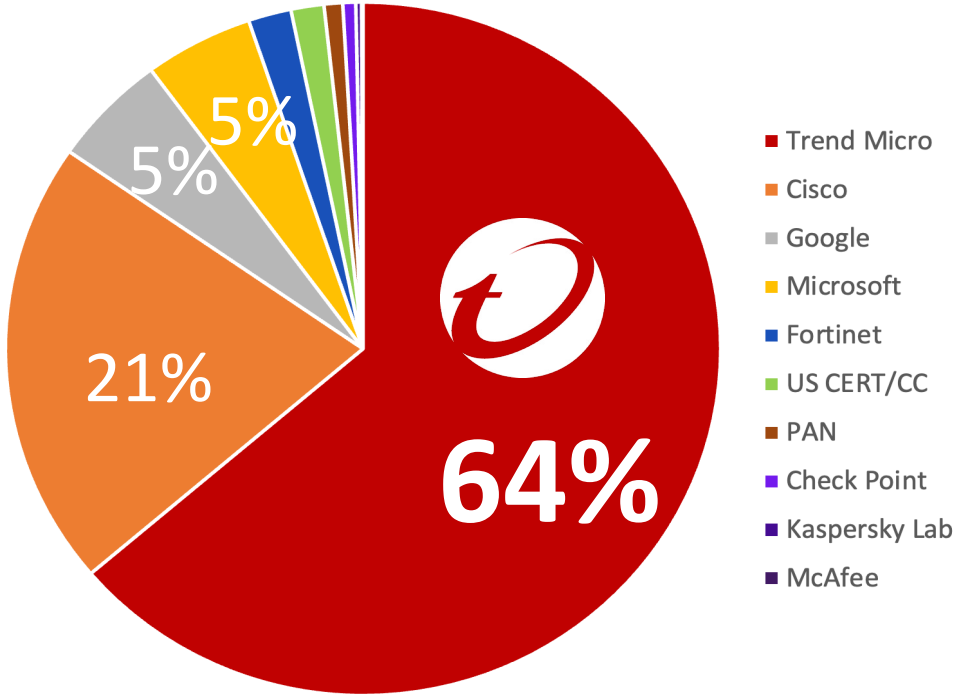
図 24：トレンドマイクロ製品によるメール、ファイル、URL の脅威検出数とクエリ数の推移
2022 年上半期は、2021 年上半期と比較しすべてにおいて増加がみられた

脆弱性公開のマーケットリーダー

Zero Day Initiative(ZDI)

- **10,000人** を超える脆弱性リサーチャを有する世界最大級の脆弱性発見コミュニティ
- 2007年から脆弱性公開市場をリード
- 主な脆弱性調査ベンダ11社※1が2021年に公開した脆弱性のうち、**約64%※2をZDIが発見**
- 脆弱性が一般に公表されるより**平均102日早く**※3Tipping Point™にてゼロデイフィルタを提供

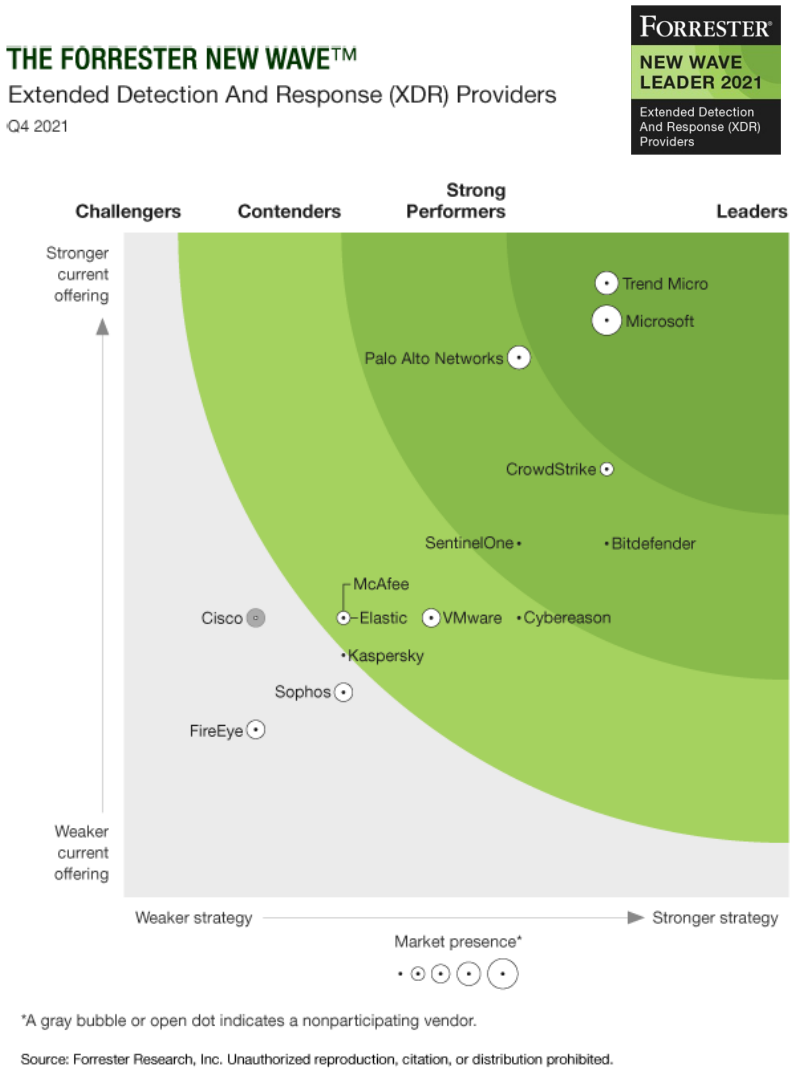
Quantifying the Public Vulnerability Market, Omdia, May 2022



※1 2022年調査の結果、報告された脆弱性が帰属するとされたのは10組織です。
※2 掲載しているパーセンテージは、少数第一位を四捨五入した数字です。
※3: 2021年の平均実績値（トレンドマイクロ調べ）

TREND MICRO | research

Extended Detection and Response(XDR) の「リーダー」に選出



The Forrester New Wave™: Extended Detection and Response (XDR) Providers, Q4 2021にて、「リーダー」に選出されました。

＜FORRESTERの評価＞

- **“強力なクロスレイヤーの検知、調査、対応を提供。**トレンドマイクロの強みは、エンドポイント、クラウドワークロード、メールそしてネットワークを独立また横断的に検知、調査、対応する仕組みを、SIEMやAzure ADとの連携も含めて、従来から提供している点だ”
- “トレンドマイクロは、**堅牢で操作が簡単なセキュリティを必要とする企業に最適”**
- “既存のセキュリティの**横断的なテレメトリー統合を可能にするプラットフォームと、最高のカスタマーサービスを必要とする企業**は、トレンドマイクロの利用で**ベネフィット**を得られるだろう"

出典： The Forrester New Wave™: Extended Detection And Response (XDR) Providers, Q4 2021

中小企業のお客様にご提案いただきたいこと

1

中小企業の皆様においても業務でのインターネット活用が広がっている
が同時にセキュリティー被害も拡大している
（自社が踏み台となり、取引先に影響がでることも・・・）

2

ランサムウェア等の感染してしまうと業務停止・取引停止のリスクがある
経営への大きなインパクト

3

高度な専門知識を有するセキュリティー対策を
まとめておまかせできるサービスの導入がおすすめ

THANK YOU!