情報通信研究機構（NICT）における サイバーセキュリティの取り組み

Contents:

(1) NICTが保有するサイバー攻撃観測・分析能力
(2) NICTのサイバーセキュリティ人材育成プログラム
(3) 日本のサイバー攻撃対処能力の向上に必要なもの

国立研究開発法人 情報通信研究機構
サイバーセキュリティ研究所 研究所長
井上 大介

NICT National Institute of Information and Communications Technology

CYBERSECURITY Research Institute

我が国のサイバー攻撃対処能力の向上を目指して

● 課題：サイバーセキュリティ自給率の低迷

✓ サイバーセキュリティ戦略本部 研究開発戦略専門調査会（2019年5月17日）

● 原因：データ負けのスパイラル

✓ データが集まらない → 研究開発/人材育成できない → 国産技術を作れない
→ 国産技術が普及しない → データが集まらない → …

● 今、日本に必要なこと

✓ 実データを**大規模に収集・蓄積**する仕組み
✓ 実データを**定常的・組織的に分析**する仕組み
✓ 実データで**国産製品を運用・検証**する仕組み
✓ 実データから**脅威情報を生成・共有**する仕組み
✓ 実データによる**人材育成をオープン化**する仕組み

これらの仕組みの実現を目指す
産学官の結節点を構築

NICT National Institute of Information and Communications Technology

CYBERSECURITY Research Institute

NICT サイバーセキュリティ研究所

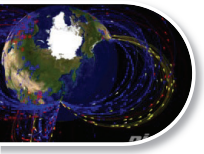
CYBERSECURITY Research Institute
サイバーセキュリティ研究所
(CSRI)

SECURITY FUNDAMENTALS Laboratory	CYBERSECURITY Laboratory	National Cyber Training Center	NATIONAL CYBER OBSERVATION CENTER	CYNEX CYBERSECURITY NEXUS	NEW NOW Printing
セキュリティ基盤研究室 (SFL)	サイバーセキュリティ研究室 (CSL)	ナショナルサイバートレーニングセンター (NCT)	ナショナルサイバーオブザベーションセンター (NCO)	サイバーセキュリティネクサス (CYNEX)	AIセキュリティ研究センター (CREATE)
暗号研究	攻撃観測 分析・対策研究	セキュリティ人材育成	IoT機器セキュリティ対策	産学官連携拠点形成	AIセキュリティ研究

サイバーセキュリティ研究室

CYBERSECURITY
Laboratory

サイバーセキュリティ研究室 研究マップ



インシデント分析センタ（ニクター）

NICTER

対サイバー攻撃アラートシステム（ダイダロス）

DAEDALUS

サイバー攻撃統合分析プラットフォーム（ニルヴァーナ・カイ）

NIRVANA改

脆弱性管理プラットフォーム（ニルヴァーナ・カイ・ニ）

NIRVANA改弐

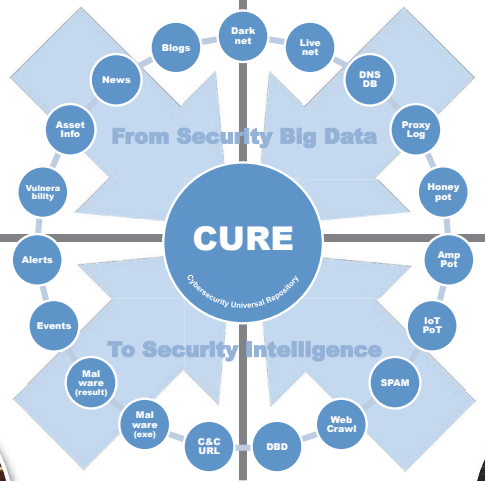
受 Passive

Global (無差別型攻撃対策)

(標的型攻撃対策) Local

全

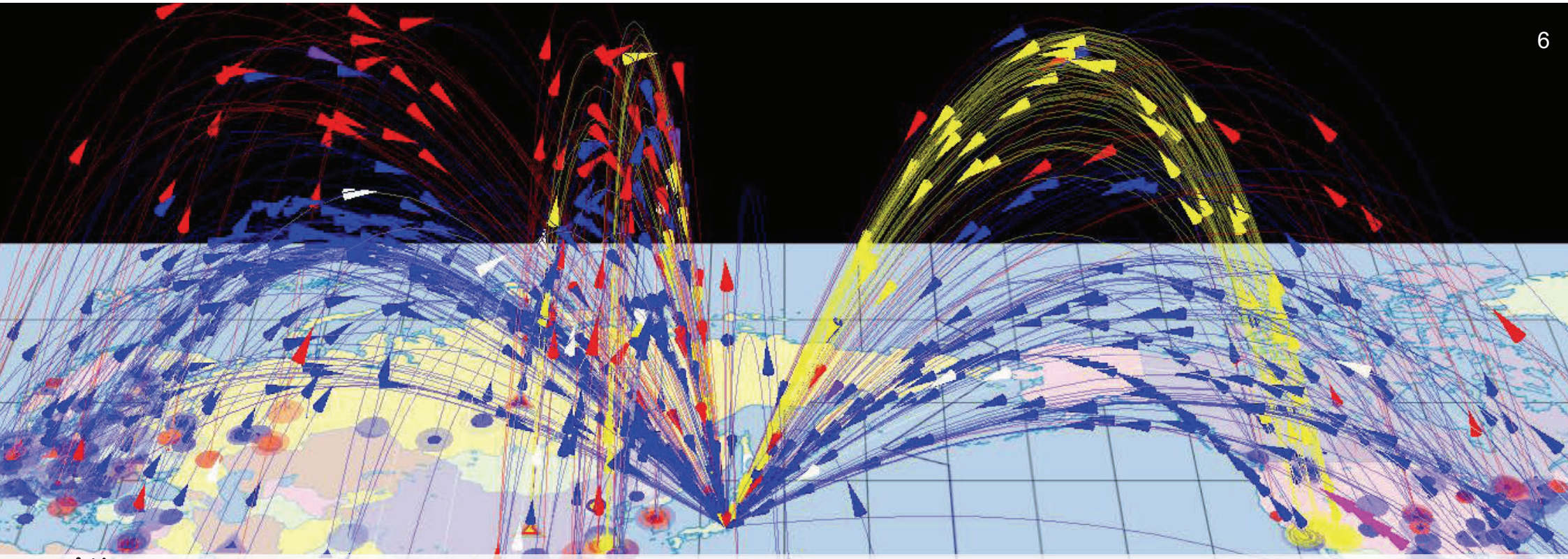
局



サイバーセキュリティ
ユニバーサル・リポジトリ

CURE

能 Active



NICTER

- サイバー攻撃リアルタイム大規模観測・分析システム（2005年観測開始）
- 国内外で30万の未使用IPアドレス“**ダークネット**”を観測
- 無差別型サイバー攻撃の大局的な傾向把握に有効

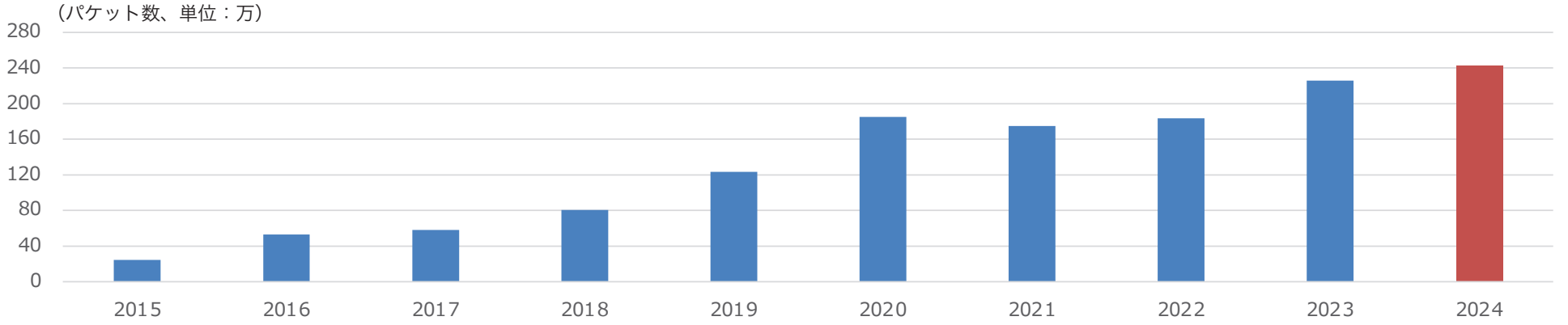
➡ **2024年：13秒に1回の攻撃観測**

➡ **感染後のIoT機器や未知の指令サーバ等のIPアドレスを検知可能**

NICTER ダークネット観測統計（過去10年）

年	年間総観測パケット数	ダークネットIPアドレス数	1 IPアドレス当たりの年間総観測パケット数
2015	約631.6億	270,973	245,540
2016	約1,440億	274,872	527,888
2017	約1,559億	253,086	578,750
2018	約2,169億	273,292	806,877
2019	約3,756億	309,769	1,231,331
2020	約5,705億	307,985	1,849,817
2021	約5,180億	289,946	1,747,685
2022	約5,226億	288,042	1,833,012
2023	約6,197億	289,686	2,260,132
2024	**約6,862億**	**284,445**	**2,427,977**

1アドレスあたり
13秒に1回
攻撃関連通信受信



1 IPアドレス当たりの年間総観測パケット数

STARDUST

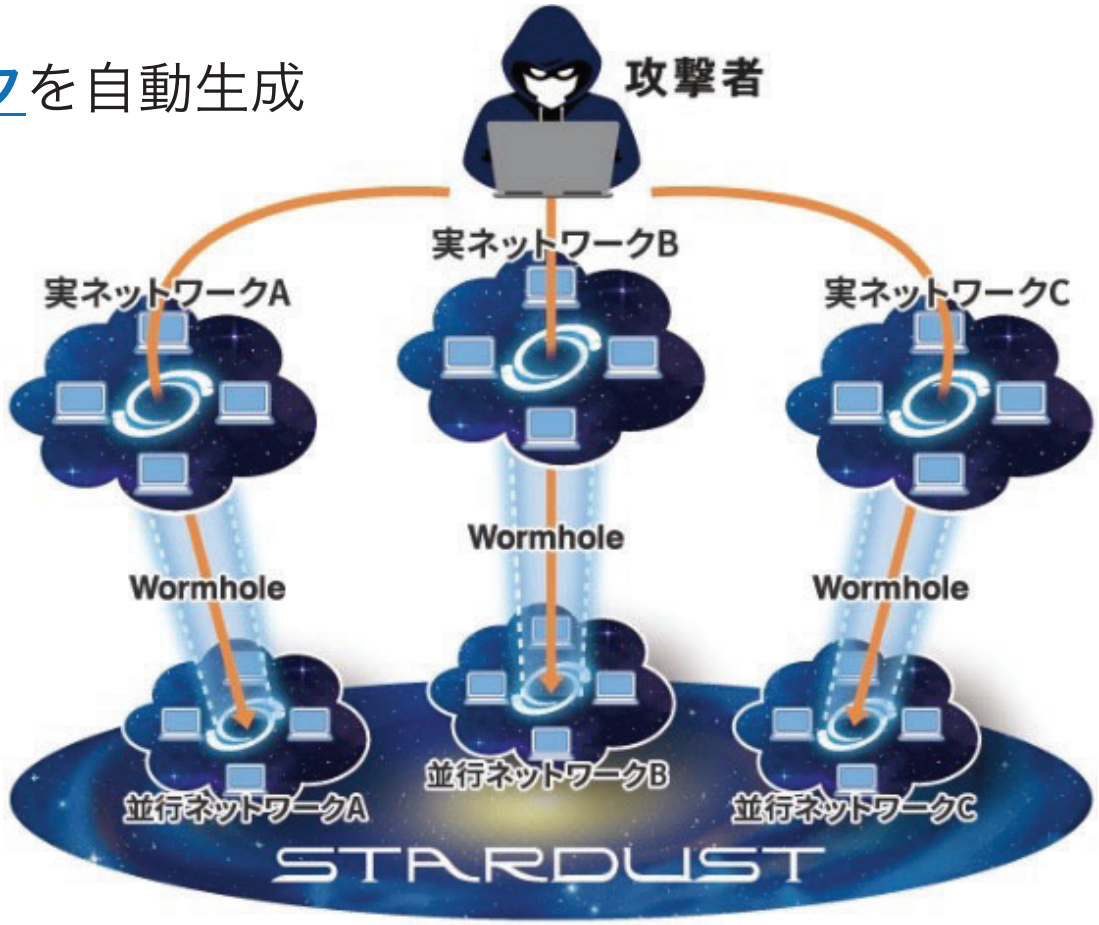
- 標的型攻撃等の人間の攻撃者を誘い込む**サイバー攻撃誘引基盤**

- 組織を精巧に模擬した**並行ネットワーク**を自動生成
  - ✓ 解析者が柔軟に使える実験・演習環境

➡ **2015年から毎年300件超の攻撃者誘引を実施**

➡ **攻撃者のアトリビューションや未知の指令サーバ等を検知可能**

- **STARDUSTの応用例**
  - ✓ 能動的な**ランサムウェア誘引環境**
  - ✓ サイバー攻撃を実施可能な**大規模演習環境**



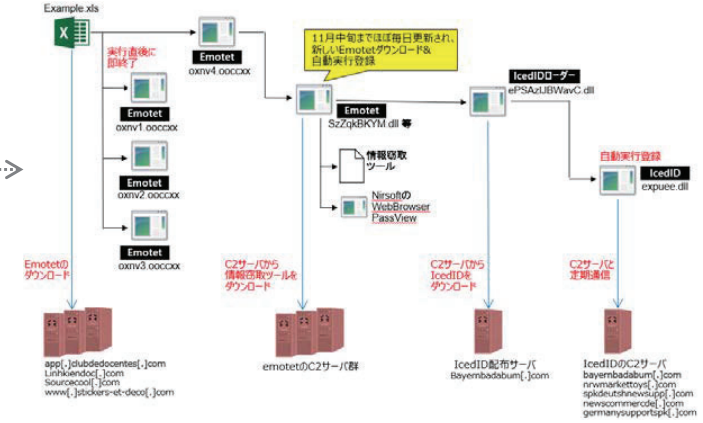
STARDUST 観測・分析事例

● 攻撃活動観測 概要レポート（一部抜粋）

Case	実施期間		検体名称	進行度	実施結果
	開始	終了		1 2 3 4 5 6 7 8	
220810_CL12_001	2022/9/20	2022/9/20	Remcos		実行後、transfer.sh への接続を行っていたが、その他の動きが無かったため観測を終了
220828_CL12_002	2022/8/28	2022/8/29	OilRig	1	検体を実行するも、通信が発生せず、観測を終了
220819_CL12_003	2022/8/19	2022/8/19	Lazarus (Job Offer)		Coinbase のデコイを用いた Lazarus の転職希望者を狙う。接続先との通信が成立せず観測を終了。
220829_CL12_004	2022/8/29	2022/8/30	Lokibot	1	検体に解析環境検知機能があり、通信が発生せずにプロセスが即終了
220902_CL12_005	2022/9/2	2022/9/6	Lazarus (Dangerouspassword)		lnk ファイル実行後、子プロセスから C2 サーバへの通信が発生したものの、以降は不審な通信や挙動が発生しなかったため、観測を終了
220905_CL12_006	2022/9/5	2022/9/6	Lokibot	1	検体に解析環境検知機能があり、通信が発生せずにプロセスが即終了
220907_CL12_007	2022/9/7	2022/9/9	Nanocore		1 次検体で nanocore、2 次検体で Formbook に感染し、C2 サーバへの通信などを確認されたが、その後の継続的な攻撃が見られず観測を終了
220907_CL12_008	2022/9/7	2022/9/7	Formbook		SUTARDUST 環境ではプロセスインジェクションに失敗して終了
220914_CL12_009	2022/9/14	2022/9/14	Kimsuky	1	接続先に名前解決できず終了
220916_CL12_010	2022/9/16	2022/9/16	Kimsuky		C2 サーバーからエラーメッセージ(404)が返ってきて通信終了、以降不審な挙動も無し
220926_CL12_011	2022/9/26	2022/10/28	AgentTesla		途中から動きが見られなくなった。ディスク容量が足りなくなったため、攻撃が見られなくなった可能性も
220928_CL12_012	2022/9/28	2022/9/30	Konni		C2 サーバへ端末情報を送付。その後、不審な挙動無し
221004_CL12_013	2022/10/4	2022/10/4	Kimsuky		2022/10/4 14:45 の時点で通信先が 404()
221012_CL12_014	2022/10/12	2022/10/12	Kimsuky	1	接続先に名前解決できず
221024_CL12_015	2022/10/24	2022/11/1	Royalroad sharppanda		観測初日のみ別の C2 サーバーと通信を行い、情報収集結果を送付
221104_CL12_016	2022/11/4	2022/11/9	Emotet		C2 サーバーとの定期通信のみを観測
221104_CL12_017	2022/11/4	2022/12/2	Emotet		情報窃取と外部メールサーバーへのメール配信試行(FW でブロック済),二次検体のダウンロードを観測
230117_CL12_018	2023/1/17	2023/2/17	Emotet		Emotet の検体更新と情報窃取は定期的に観測できたが、メール配信は観測できなかった。また、ダウンロードされた Emotet も前回キャンペーンとの差異は見られなかった。その後、不審な通信や挙動が発生しなかったため、観測を終了した。

STARDUSTで観測した攻撃の進行度
（1：検体実行不可 ～ 8：継続的に攻撃発生）

● 攻撃活動観測 詳細レポート（一部抜粋）



● NanoCore RATの攻撃者の挙動一覧

分類	行動
メール	Outlook を開く
	受信トレイを確認する
	送信済みアイテムを確認する
	下書きを確認する
	ユーザのアカウント情報を確認する
	特定のメールを検索する
	メールの送信を試みる
ブラウザ	Chrome や Internet Explorer を開く
	Google アカウントへのログイン状況を確認する
	言語設定を英語に変更する
	ブックマークを確認する
	ブックマークされたページを開く
	特定のページを開く（PayPal，Alibaba，xvideos など）
	閲覧履歴を確認する
	特定のツールをダウンロードする
	よくアクセスするページや最近閉じたタブを確認する
権限昇格	管理者権限を要求する

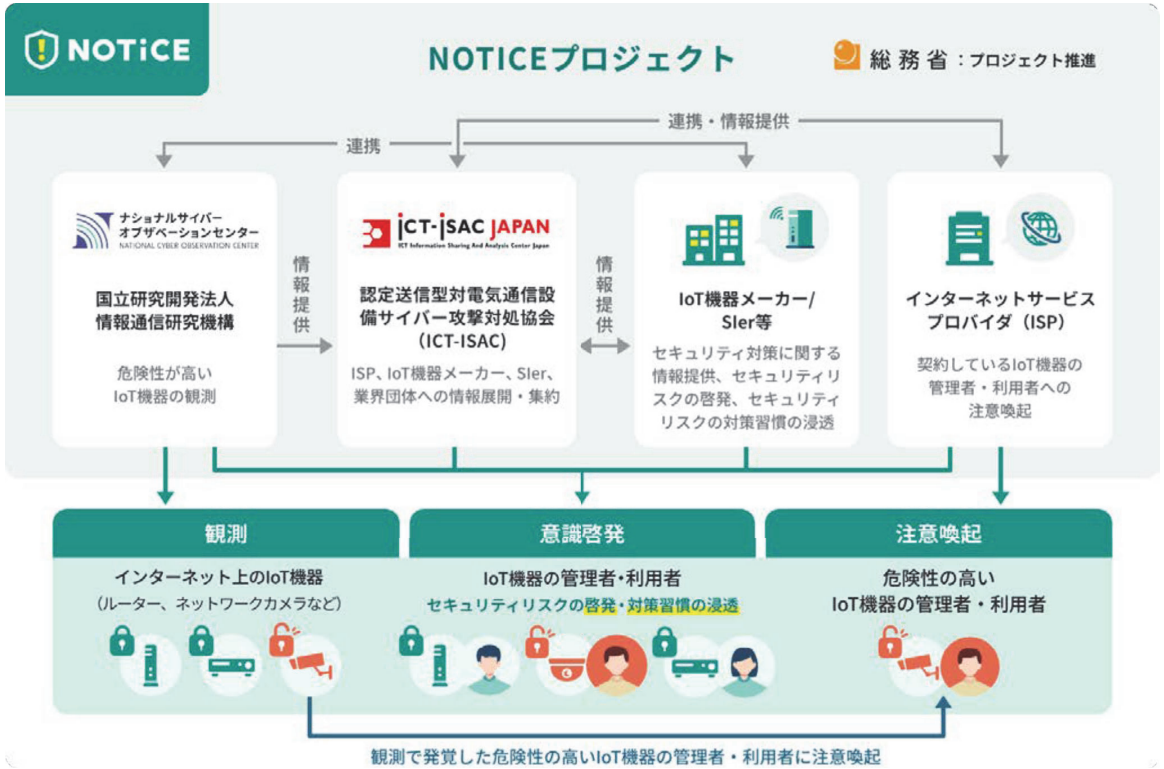
分類	行動
ファイルアクセス	デスクトップ上のファイルやフォルダを開く
	最近表示した場所を開く
	ファイルを圧縮する
	ネットワークドライブを確認する
	ファイルを C2 サーバにアップロードする
	他のマルウェアを実行する
	NanoCore クライアントを更新する
	NanoCore クライアントをアンインストールする
	スタートメニューからアプリやファイルを検索する
アカウント情報	ブラウザに登録されたパスワードを窃取する
	メーラーに登録されたアカウント情報を窃取する
ネットワーク接続	タスクバーのネットワークアイコンから通信状況を確認する
	コントロールパネルのネットワークと共有センターを確認する
コマンド	ipconfig，net view コマンドを実行する
	systeminfo コマンドを実行する
その他	NjRAT チャット機能で話しかけてくる
	操作できないようにするために画面をロックする

ナショナルサイバーオブザベーションセンター

NATIONAL CYBER
OBSERVATION CENTER

NOTICEプロジェクト

- NOTICE: National Operation Towards IoT Clean Environment
  - ✓ 総務省、NICT、ISPが連携し、IoT機器のセキュリティ対策向上を推進することにより、サイバー攻撃の発生や、その被害を未然に防ぐためのプロジェクト



https://notice.go.jp/

NICT National Institute of Information and Communications Technology

NATIONAL CYBER OBSERVATION CENTER

IoT機器観測状況（2025年2月時点）

IoT機器観測総数

月1.25億件

参加インターネットサービスプロバイダ（ISP）のIPアドレスに対して観測している総数

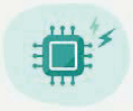
容易に推測可能なID・パスワードであるIoT機器

月14,022件

容易に推測可能なIDやパスワードを使用しているため、攻撃者によって管理権限を乗っ取られたり、サイバー攻撃に加担させられる危険性がある機器

ファームウェアに高リスク脆弱性を有するIoT機器

月4,247件



第三者に不正利用される危険性があるファームウェア脆弱性を有するIoT機器

マルウェア感染IoT機器検知数

最大1,042件/日

Miraiに既に感染していると推定されるIoT機器。サイバー攻撃に加担させられている可能性がある。

※IPアドレスが変動している場合は、重複して計上している場合があります
※当月1日あたりの最大値を掲載しています

リフレクション攻撃の踏み台にされうるIoT機器数

月16,140件

リフレクション攻撃の踏み台にされうる可能性のあるIoT機器だと検知した数

NOTICEの取り組みに参加していただいている会社・団体は以下です。

延べ96組織

※2025年3月現在

ISP	IoT機器メーカー	SIer	団体
85社	7社	2社	2団体

https://notice.go.jp/

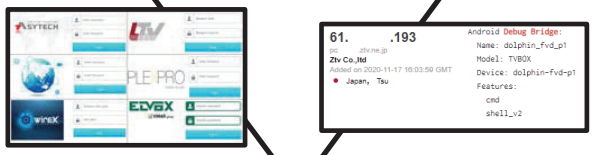
NICTER + NOTICE + 実機ハニーポットの連携

1. 大規模観測で未知の機器発見

受動的観測　　能動的観測

NICTER　　NOTiCE

機器のバナー情報

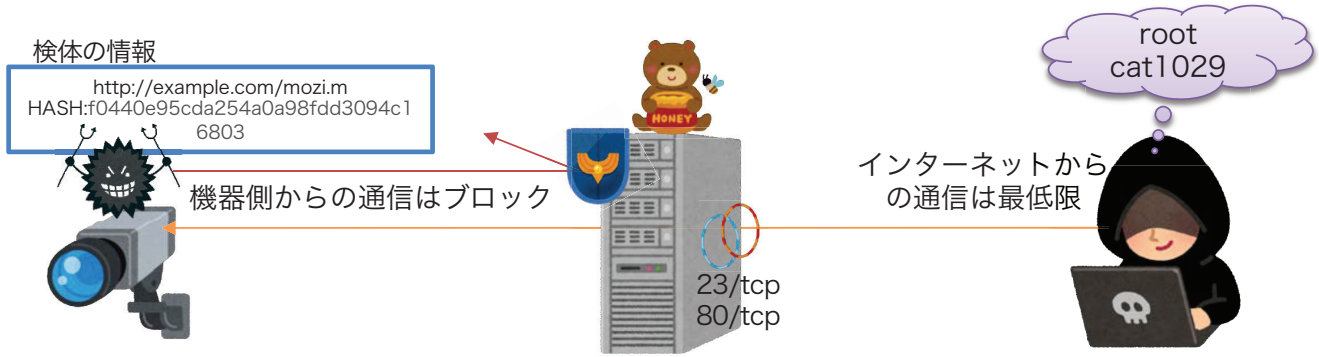


発見した機器から、脆弱性が多い物、販売台数が多そうな物、影響が大きい物を選定して購入

2. 機器の初期調査

- ✓ ポートスキャン
- ✓ 設定項目の調査
  ※ ユーザIDが変更可能か等
- ✓ ファームウェアの調査
  ※ 必要に応じてファームウェア解析等を実施

3. 実機をハニーポット化して調査



マルウェア検体、侵入経路、攻撃ペイロード、隠しユーザ情報、指令サーバ情報、等を収集

4. 情報共有・発信

- ✓ JPCERT/CC、IPAへの報告/連携
- ✓ 機器ベンダーへの報告/連携
- ✓ 機器設置組織、県警等への報告/連携
- ✓ BLOG/Twitter等での情報発信

➡ 未知の機器、脆弱性情報、マルウェア検体、指令サーバ等を検知可能

ナショナルサイバートレーニングセンター

National
Cyber
Training
Center

実践的サイバー防御演習 CYDER (Cyber Defense Exercise with Recurrence)

- **インシデント対応をロールプレイ形式で実体験できるサイバー演習**
  - ✓ 組織のネットワークを再現したリアルな環境でインシデント対応の一連の流れを体験

➡ 2024年度：集合演習 + プレCYDER = 受講者数8,000名超

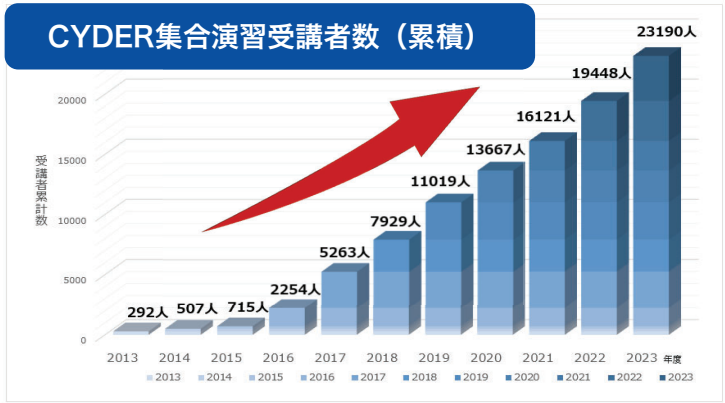
2024年度の実施内容および対象組織

2024年度コース概要

- ✓毎年 **約 3,000人が受講**（集合（実地）演習）
- ✓集合演習は1日間（Cコースは2日間）
- ✓集合演習のほかオンライン演習（個人学習）を実施
- ✓組織当たり1名でも複数名でも参加可能
- ✓重要社会基盤事業者、民間企業等は、受講料が必要

A/Bコース	（集合）	… 77,000円（税込）
Cコース	（集合）	… 121,000円（税込）
プレCYDER	（オンライン）	… 11,000円（税込）

CYDER集合演習受講者数（累積）



コース名	演習方法	レベル	受講想定者（習得内容）	受講想定組織	開催地	開催回数	実施時期
A	集合演習	初級	システムに携わり始めた方 (事案発生時の対応の流れ)	全組織共通	47都道府県	64回	7月～翌年1月
B-1		中級	システム管理者・運用者 (主体的な事案対応・ｾｷｭﾘﾃｨ管理)	地方公共団体	全国11地域	18回	10月～翌年1月
B-2				地方公共団体以外	東京・大阪・名古屋	13回	翌年1月
C		準上級	セキュリティ専門担当者 (高度なセキュリティ技術)	全組織共通	東京・大阪	5回	11月～翌年1月
プレCYDER	ｵﾝﾗｲﾝ演習	超入門	自治体等のCSIRT初任者 かつ集合演習受講困難者	全組織共通	（受講者職場等）	―	前半：5月～7月 後半：10月～翌年1月
オンライン実践		初級・中級	集合演習受講困難者	選定した地方公共団体		4回	11月～12月

セックハックサンロクゴ

SecHack365

● 若手セキュリティイノベーター育成プログラム（毎年約40名、累計300名超）

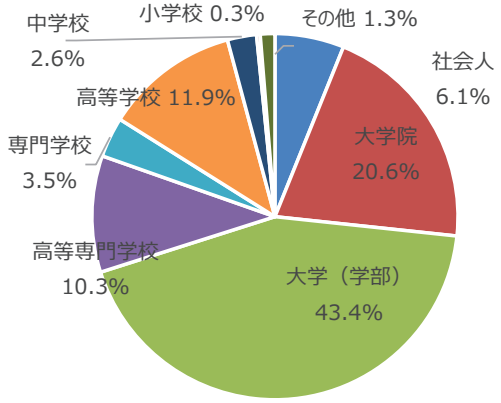
✓ 長期ハッカソンによるモノ作りの機会を通し、1年をかけて技術力や継続力、アイデア発想力、倫理面などの指導を行い、作品作りに取り組む未来のセキュリティイノベーター育成プログラム

対象者

日本国内に居住する
25歳以下の若手ICT人材
(学生、社会人、無職等※)

※令和3年度より25歳以下の無職・無収入者へも補助

受講生属性（2017～2023年度）



特長

複数回の集合イベント

アイデアソン・ハッカソンのイベントを年間複数回、オンラインとオフラインで開催することで、継続的に開発を進めます。

学生向け支援

学生は集合の際の必要経費を全額補助※。学業との両立についての相談や進路相談も可能です。
※旅費等実費相当分

NICT ならでは

サイバーセキュリティの研究開発のノウハウや、実際の貴重な攻撃データ等を活用できる“NONSTOP”が利用可能。

多様な講義とオンラインの活用

倫理・法律をはじめオンラインコンテンツも活用。遠隔でもチャットやタスク管理ツールを使いコミュニケーションを図ります。

最先端技術の体験

先端企業の見学による社会体験で発想力を強化。ゲスト講演者からプレゼンテーションスキルや知識を習得。

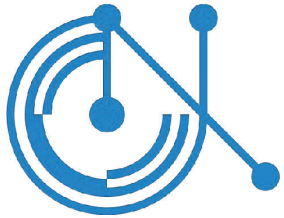
2024年 SecHack365 年間プログラム

第1回イベント	6月15日(土)		キックオフ
第2回イベント	7月19日(金)～21日(日)	東京	活動状況報告・テーマ指導
第3回イベント	9月27日(金)～29日(日)	広島	作品・全体発表・社会実装指導
第4回イベント	11月15日(金)～17日(日)	大阪	作品発表・最終発表の準備
第5回イベント	2025年 2月1日(土)・2日(日)		最終発表・審査
第6回イベント	2025年 3月8日(土)・9日(日)	東京	発表練習・成果発表

成果発表会 2025年3月9日(日) 東京

https://sechack365.nict.go.jp

サイバーセキュリティネクサス



CYNEX
CYBERSECURITY NEXUS

CYNEX：サイバーセキュリティ統合知的・人材育成基盤

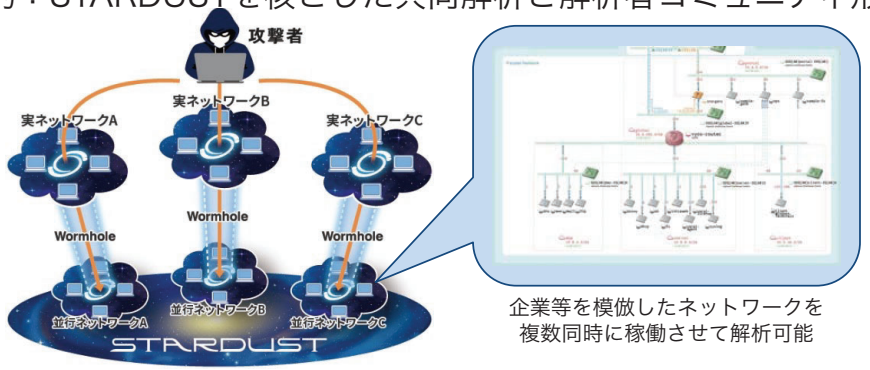
- 日本の**サイバー攻撃対処能力**と**セキュリティ自給率**向上のための産学官の**結節点**

CYNEX CYBERSECURITY NEXUS サイバーセキュリティ産学官連携拠点

Co-Nexus A (Accumulation & Analysis)

参画組織数：40

- 目的：STARDUSTを核とした共同解析と解析者コミュニティ形成



企業等を模倣したネットワークを
複数同時に稼働させて解析可能

サイバー攻撃誘引基盤STARDUST

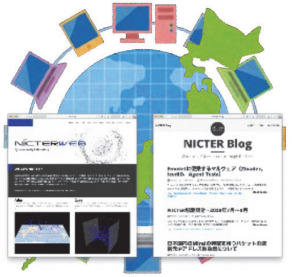
Co-Nexus S (Security Operation & Sharing)

参画組織数：18

- 目的：高度な解析者の育成とCYNEX独自の脅威情報の生成・発信

自主学習型
オンラインSOC研修

OJTでのSOC業務従事



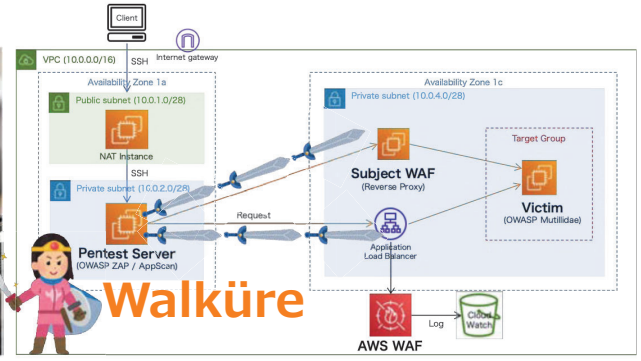
国産脅威情報発信/提供

Co-Nexus E (Evaluation)

参画組織数：8

- 目的：国産セキュリティ製品のテスト環境提供による実用化支援

IoT機器検証環境

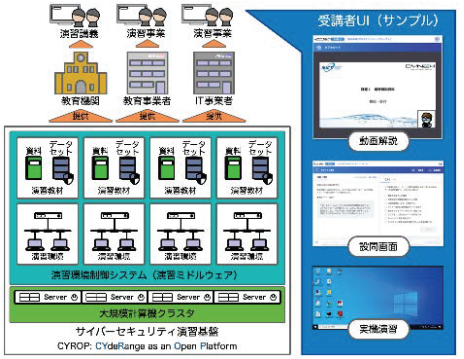


WAF製品検証環境

Co-Nexus C (CYROP: Cyber Range Open Platform)

参画組織数：65

- 目的：演習基盤開放による国内セキュリティ人材育成事業の活性化



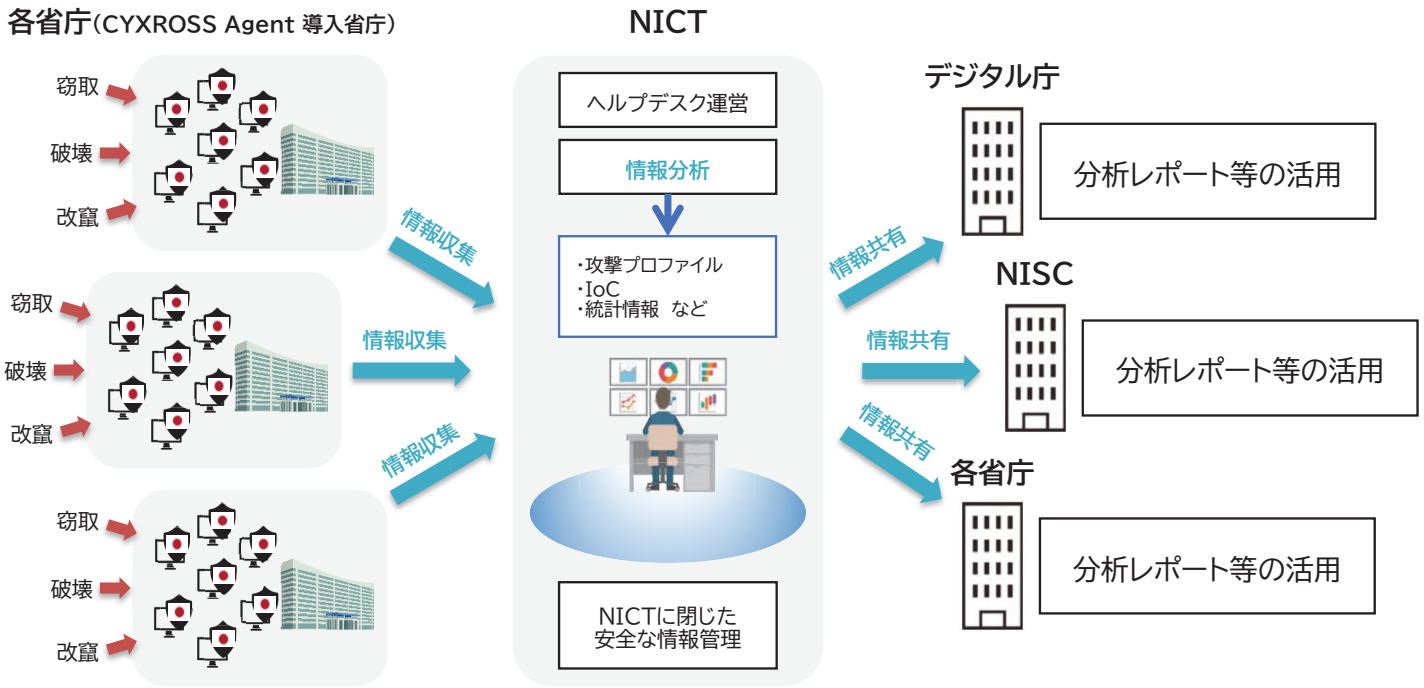
サイバーセキュリティ演習基盤CYROP

教育機関での演習教材利用事例

- **安全性や透明性の検証が可能なNICT開発のセンサー**を政府端末に導入し、得られたマルウェア情報等をNICTにおいて集約・分析する実証事業を実施

➡ **NICT開発センサー『CYXROSS Agent』を政府端末に導入開始**

➡ **政府内でマルウェアや指令サーバ等の情報収集可能（関係省庁の協力が重要）**



セキュリティ基盤研究室

セキュリティ基盤研究室
Security Fundamentals Laboratory

NICT National Institute of Information and Communications Technology

SECURITY FUNDAMENTALS Laboratory

セキュリティ基盤研究室の研究課題 (2021-2026)

安全なデータ利活用技術

- データのセキュリティ・プライバシーの確保
- 秘密計算等のプライバシー保護解析技術
- 組織横断連携を含むデータ利活用技術
- 安全なテレワーク等に資する研究開発

量子コンピュータ時代に向けた暗号技術の安全性評価

- 耐量子計算機暗号
- CRYPTREC：電子政府システム等において使用される暗号技術の安全性評価
- 国民生活を支える様々なシステムの安全な運用に貢献

量子コンピュータ時代に向けた暗号研究

- 大規模量子コンピュータが実現すると公開鍵暗号の安全性が急低下
- **耐量子計算機暗号**（PQC）の研究開発と**移行検討が世界的な急務**
  - ➡ **2025年4月 CRYPTREC 耐量子計算機暗号ガイドライン発行（改訂版）**
  - ➡ ガイドライン発行などの技術面についてはNICTも関わるCRYPTRECで実施。
    そのうえで、**暗号技術の取扱い方針は「政府」としての方針決定が不可欠。**
    例えば、RSA1024の移行の際は、「NISC」作成の移行方針が重要な役割を果たした。

	暗号技術 Cryptosystem	現在のコンピュータでの強度 [bits] Classical security	量子コンピュータでの強度 [bits] Quantum security	解読に使われる量子アルゴリズム Quantum algorithm
公開鍵暗号 Public-key crypto	RSA 2048	112	0	ショアのアルゴリズム Shor's algorithm
	RSA 3072	128		
	DSA 2048	112		
	DSA 3072	128		
	ECC 256	128		
	ECC 521	256		
共通鍵暗号 Symmetric-key crypto	AES 128	128	64	グローバーのアルゴリズム Grover's algorithm
	AES 256	256	128	

日本のサイバー攻撃対処能力の向上に必要なもの

- **サイバー攻撃の一次情報を自ら収集・分析できる能力**
  - ✓一次情報を持つ国同士でサイバー空間の国際連携は進んでいく
  - ➡ NICTER, NOTICE, STARDUST, CYXROSS

- **確度の高いアトリビューションを実施できる観測能力**
  - ✓能動的サイバー防衛の大前提として高精度な攻撃者特定が必要
  - ➡ STARDUST, CYXROSS

- **攻撃者の視座をもった高度対処人材の育成・確保**
  - ✓被害発生前の防御を実施可能な高度人材の育成/確保
  - ➡ CYDER, SecHack365, CYNEX Co-Nexus S, Co-Nexus C

ヒアリング資料

2025年３月21日
日本商工会議所

1．中小企業のデジタル化の現状

○急激な人口減少・少子高齢化の進展に伴い、**中小企業の人手不足は深刻化**。女性や高齢者の活躍、新規採用等で賄うことが困難であり、**デジタル化による生産性の向上は必須**の状況。

○業務効率化や事業変革など、中小企業においても**デジタル化の取り組みが進展してきている一方**、デジタル化**未着手の企業も**2023年時点で**約３割強**存在する。

中小企業のデジタル化の現状

出典：中小企業庁（2024）『中小企業白書』

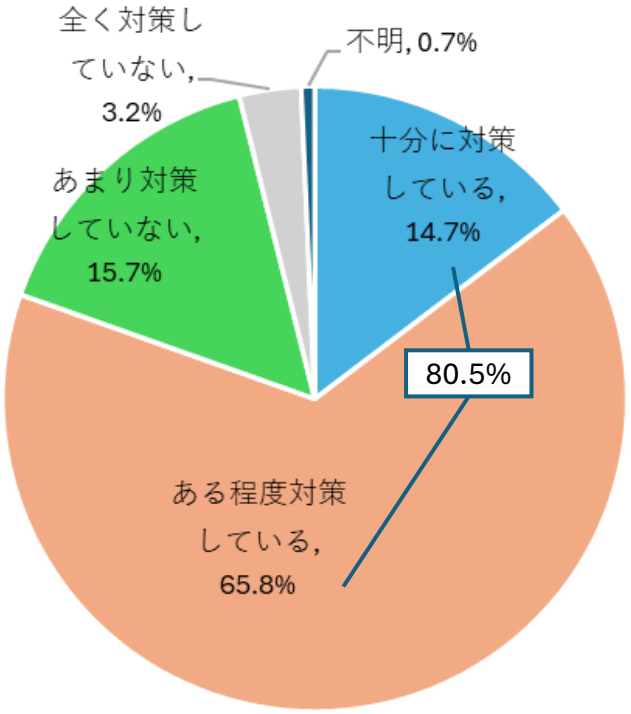
段階４：ﾃﾞｼﾞﾀﾙ化によるﾋﾞｼﾞﾈｽﾓﾃﾞﾙ変革や競争力強化に取り組んでいる状態
段階３：ﾃﾞｼﾞﾀﾙ化による業務効率化やﾃﾞｰﾀ分析に取り組んでいる状態
段階２：デジタルツールを利用した業務環境に移行
段階１：紙や口頭による業務が中心

2．中小企業のサイバーセキュリティ対策の現状①

○サイバーセキュリティ対策について、**「十分に対策している」**（14.7%）**または「ある程度対策している」**（65.8%）**企業は約8割**であり、「自社は対策している」と考える企業が多い。

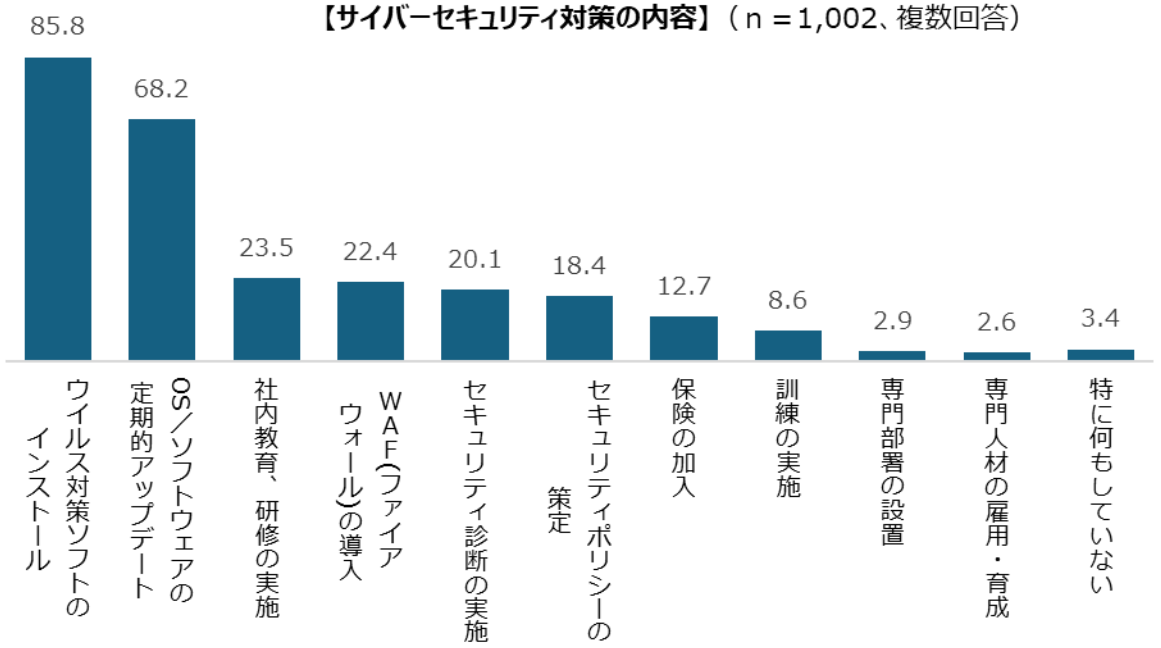
○一方、実際に行われているサイバーセキュリティ対策は、**「ウイルス対策ソフト」が85.8%**、**「ソフトウェアの定期的なアップデート」が68.2%**と、基本的な対策に留まり、「社内教育」「セキュリティ診断」「訓練」などの**専門的対策は（いずれも25%以下と）進んでいない**。

【サイバーセキュリティ対策の状況】（n=1,002）



※2025年1月東京商工会議所「中小企業のデジタルシフト・DX実態調査」
（東京23区内の会員中小企業1,218社が回答）

【サイバーセキュリティ対策の内容】（n＝1,002、複数回答）

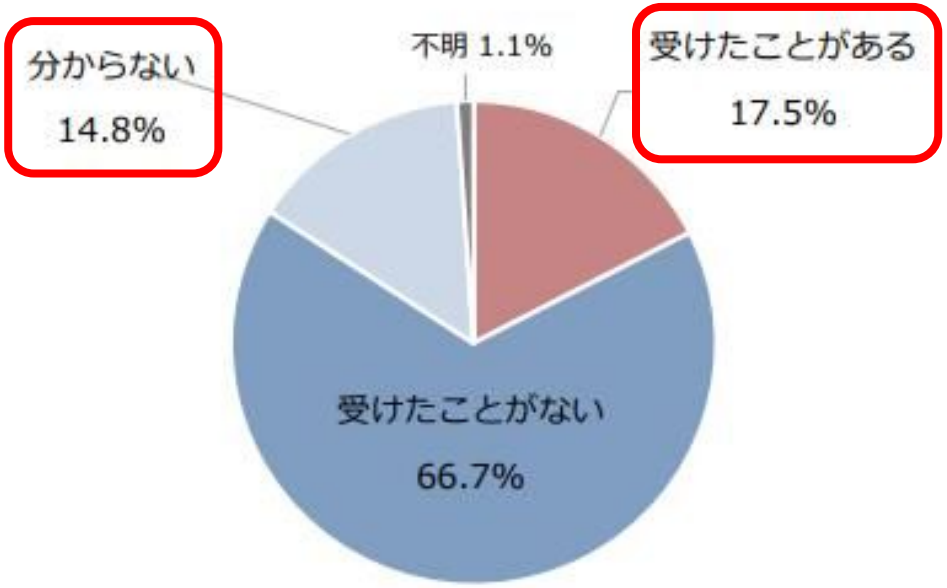


2．中小企業のサイバーセキュリティ対策の現状②

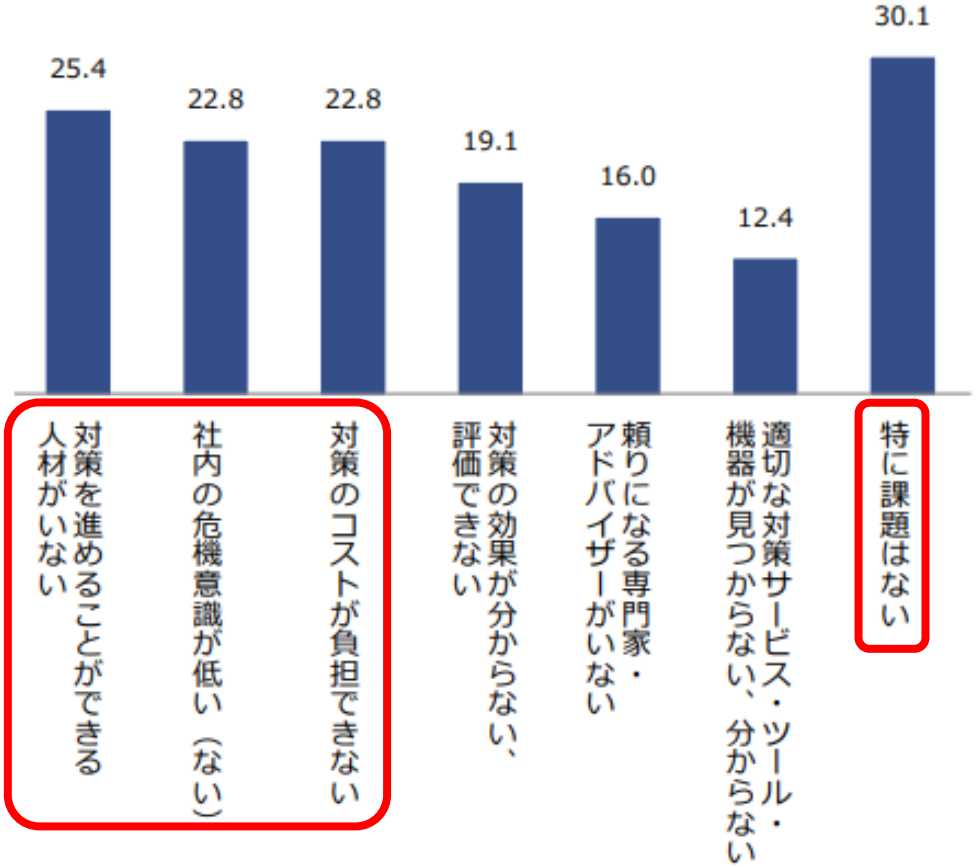
○**サイバー攻撃を「受けたことがある」企業は17.5%**。他方で**「分からない」とする企業も約15%**おり、サイバー攻撃に対する**検知や対処体制に課題**を抱える可能性が残る

○**サイバーセキュリティ対策の課題**は**人材や危機意識、コストに関する課題が上位**に挙がる一方、「特に課題はない」とする企業も30.1%ある

【自社に対するサイバー攻撃の経験】 (n=1,002)



【サイバーセキュリティ対策に関する課題】 (n=1,002、複数回答)



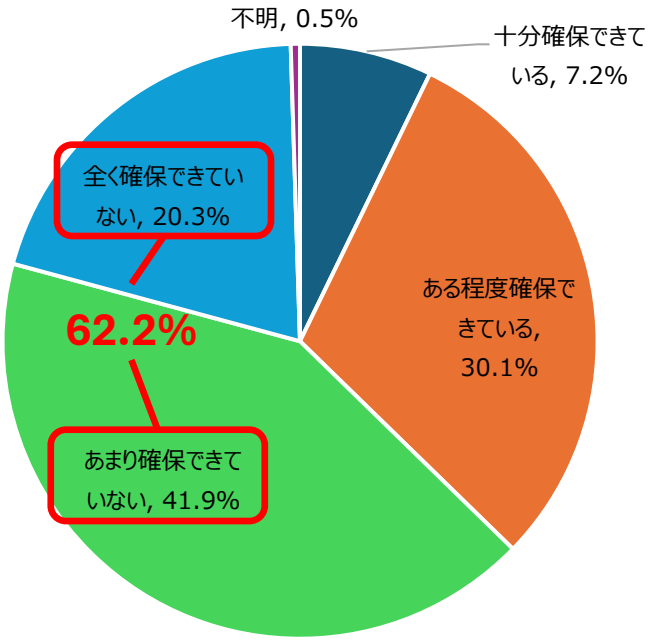
※2025年1月東京商工会議所「中小企業のデジタルシフト・DX実態調査」
（東京23区内の会員中小企業1,218社が回答）

3．サイバーセキュリティ人材の育成・確保

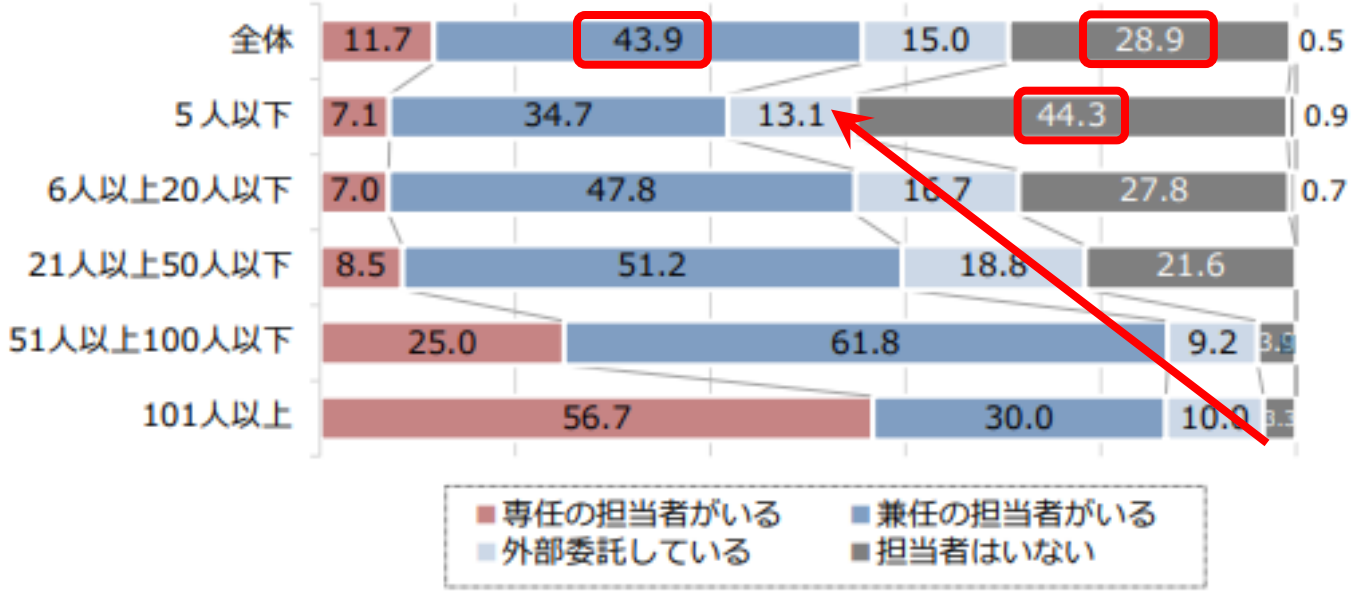
○中小企業において、**デジタル人材を「十分確保できている」企業はわずか7.2%**で、「あまり確保できていない」「全く確保できていない」企業は62.2%とデジタル人材そのものの確保でさえ苦慮しており、**「セキュリティ人材」となると一層深刻**。

○また、「情報システム担当者の設置」は、43.9%の企業が兼任の担当者であり、「担当者がいない」企業も28.9%で、5人以下の企業は44.3%と**規模が小さい企業ほど深刻**。**中小企業は人材も予算も不足しており、兼務でセキュリティを担う「プラス・セキュリティ」人材の育成は重要**。

【デジタル人材の確保状況】（n=1,002）



【従業員規模×情報システム担当者の設置状況】 (n=1,002)



※2025年1月東京商工会議所「中小企業のデジタルシフト・DX実態調査」
（東京23区内の会員中小企業1,218社が回答）

4．サプライチェーンで狙われる中小企業

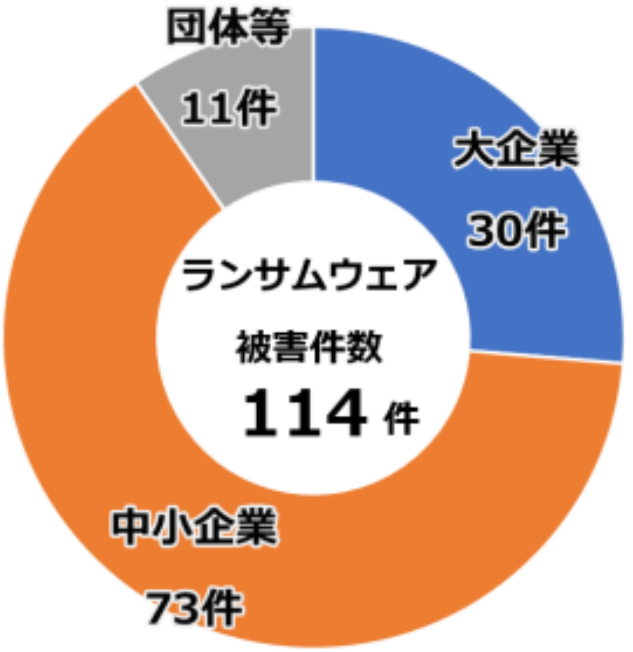
○社会基盤を支えるサプライチェーンのサイバーセキュリティ対策は極めて重要。近年、**サプライチェーンの弱点を悪用した攻撃の高まりが増えている**。狙われるのは、最終的なターゲットとなりうる大手企業と取引があり、予算・人材不足などの都合でセキュリティ対策が不十分になりがちな中小企業。

○実際にランサムウェア（身代金要求型ウイルス）の**被害は、6割超が中小企業**となっている。

情報セキュリティ10大脅威の推移（(独)情報処理推進機構[IPA]）

	2021	2022	2023	2024	2025
1位	ランサムウェアによる被害	ランサムウェアによる被害	ランサムウェアによる被害	ランサムウェアによる被害	ランサムウェアによる被害
2位	標的型攻撃による機密情報の窃取	標的型攻撃による機密情報の窃取	**サプライチェーンの弱点を悪用した攻撃の高まり**	**サプライチェーンの弱点を悪用した攻撃の高まり**	**サプライチェーンの弱点を悪用した攻撃の高まり**
3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	**サプライチェーンの弱点を悪用した攻撃の高まり**	標的型攻撃による機密情報の窃取	内部不正による情報漏えい	システムの脆弱性を突いた攻撃
4位	**サプライチェーンの弱点を悪用した攻撃の高まり**	テレワーク等のニューノーマルな働き方を狙った攻撃	内部不正による情報漏えい	標的型攻撃による機密情報の窃取	内部不正による情報漏えい
5位	ビジネスメール詐欺による金銭被害	内部不正による情報漏えい	テレワーク等のニューノーマルな働き方を狙った攻撃	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	標的型攻撃による機密情報の窃取

ランサムウェアによる被害件数



警察庁「令和6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」

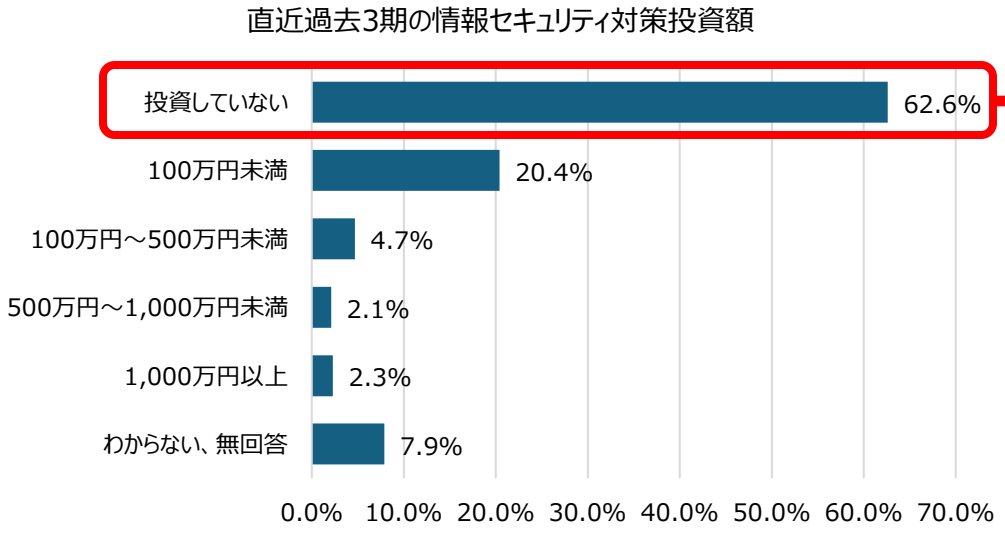
（参考）中小企業のサイバーセキュリティ対策でよく寄せられる声①

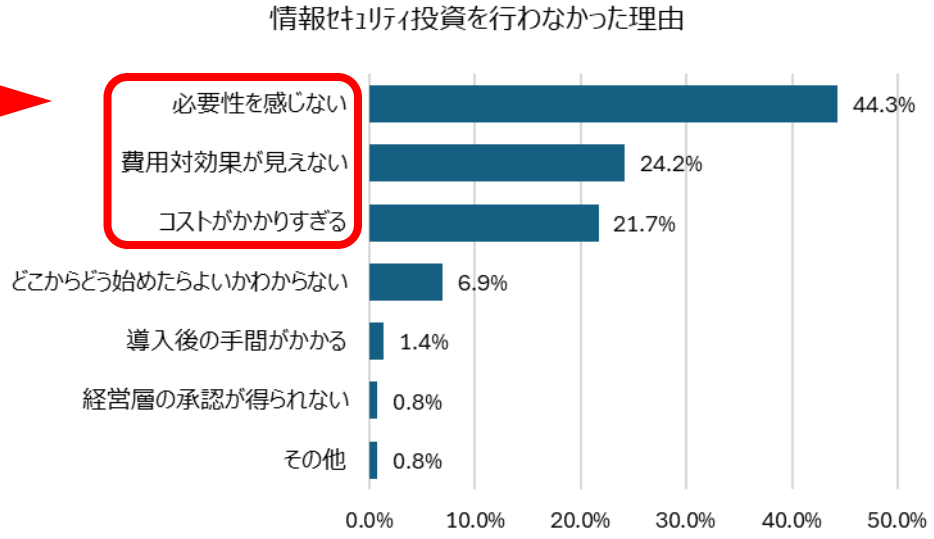
（中小企業のセキュリティ意識に関する声）

○**中小企業はセキュリティを「自分ごと」として理解してもらえない。継続して粘り強く何度でも、**打ち上げ花火ではなく線香花火のように取り組む必要がある。**インシデントの事例が大企業だったり、欧米の事例を語っても中小企業には響かない。**

○サイバーセキュリティ対策は**効果が見えず売上にも貢献しないので、経営者は金銭を負担したくない。**

○**中小企業のセキュリティ対策は「ウイルス対策ソフト」を導入しているのみという企業も多い。**サイバーセキュリティ対策の底上げには政府の支援も重要。





独立行政法人情報処理推進機構（IPA）「2024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報告書」速報版
（2025年2月、全国の中小企業4191社を対象にウェブアンケート）

（参考）中小企業のサイバーセキュリティ対策でよく寄せられる声②

（基準やメリットに対する声）

○中小企業は規模や業種がさまざま。サイバーセキュリティ対策は**どの程度の規模の企業にどんな対策を求めるのか。**ターゲットごとの対策が必要

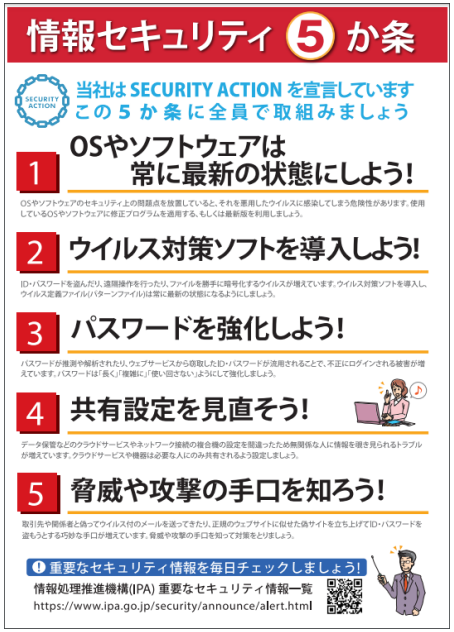
○**どこまで対策をすればよいかわからない中小企業も多い。**現状は**対策の程度や深さの理解がなく評価軸がない。**Security Action一つ星や情報セキュリティ5か条などがあるが普及していない

○株式上場していない中小企業に「セキュリティ対策をすれば信頼度が向上する」と言っても響かない。**身近にメリットをPRできるインセンティブが中小企業にとっては重要**

「SECURITY ACTION」～中小企業自らが、情報セキュリティ対策に取組むことを自己宣言する制度

①★一つ星取得要件
- 「情報セキュリティ５か条」に取り組むことを宣言。

②★★二つ星取得要件
- 「情報セキュリティ自社診断」を実施。
- 「セキュリティポリシー」を策定して外部に公開。



○中小企業や支援機関等が自ら情報セキュリティ対策に取り組むことを自己宣言する制度。2017年に情報処理推進機構（IPA）が創設。

○全国30万者を超える中小企業や支援機関等が宣言。商工会議所も418ヵ所が宣言。セキュリティ対策に関心をもって取組む姿勢を内外に「見える化」している。

（参考）中小企業のサイバーセキュリティ対策でよく寄せられる声③

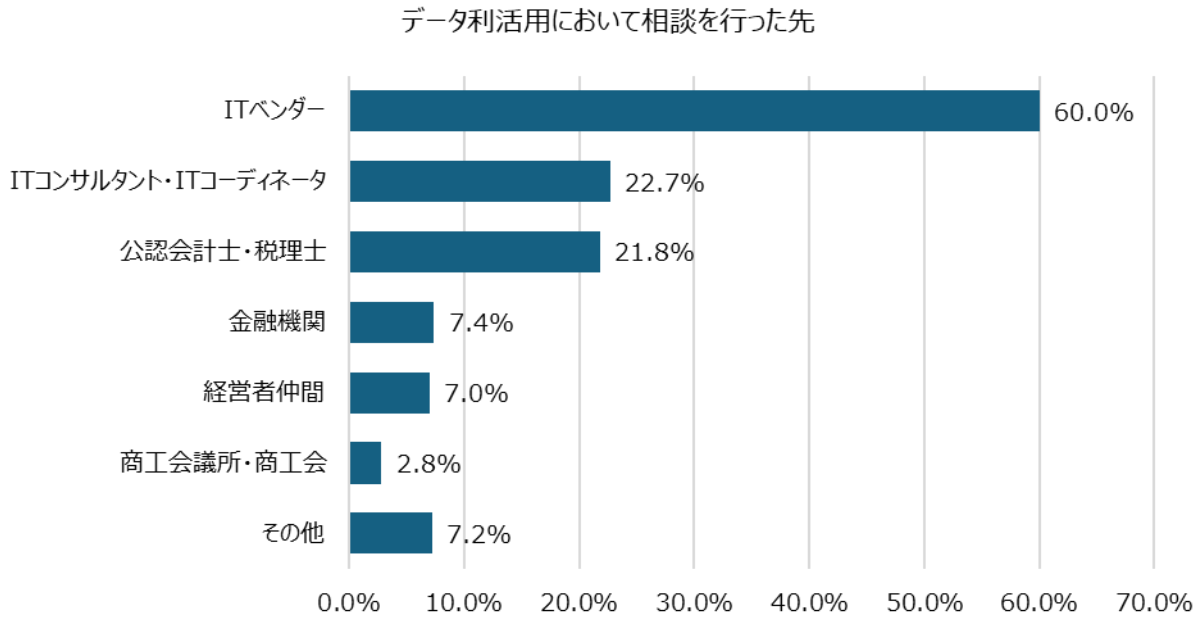
（相談先や専門家とのコンタクトに対する声）

○**中小企業の相談先は「ITベンダー」が圧倒的に多い。ITベンダーは**自社製品のプロフェッショナルであり、**必ずしもセキュリティの専門家ではなく、**コピー機のメンテナンスに来たときに相談するイメージ。ほとんどわからない人がよくわからない人に説明するようなもので、**過剰スペックの対策を強いられている事例も散見される**。

○**商工会議所の相談窓口**にスポットで配置しているIT専門家はITコーディネーターである場合が多く、**攻めのIT専門家であり、セキュリティ対策がわかる守りの専門家ではない。**

○中小企業の**相談先として、ITベンダー以外には身近な税理士や金融機関が想定される。セキュリティの専門家につなぐ仕組みづくりが必要**。

○サイバーセキュリティ専門家には**専門用語を中小企業にもわかる言葉で噛み砕く能力**が求められている。



「2022年中小企業白書」掲載資料
（株）東京商工リサーチ「中小企業のデジタル化と情報資産の活用に関するアンケート」

要望事項

1. 中小企業の対応強化に向けた政府支援の強化

- 一般的にセキュリティ対策が脆弱である中小企業は攻撃を受けるリスクが高く、被害がサプライチェーン全体に及び甚大化・長期化する可能性もあり一層のセキュリティ対策が重要。**最低限の対策に留まっている中小企業の支援を強化**すべき。
- 中小企業が何をどこまでセキュリティ対策を行うべきか、**具体的な目安と方法を示し、浸透するよう支援**すべき。

2. 中小企業のインシデント発生時の事業継続に向けた官民連携とITベンダーの対応力向上

- 政府から、昨今のサイバーセキュリティに関する動向や中小企業にとって身近な対策事例などを発信し、官民連携のもと、中小企業の**インシデント発生時における「事業継続」に向けた支援**をお願いしたい。
- 中小企業の多くは能力・リソース不足のため、セキュリティを専門としない一般的なITベンダー（システム開発業者等）に対策を委託するケースが多い。**ITベンダーのインシデント対応力（支援力）向上の支援**や、**セキュリティ専門家（情報処理安全確保支援士＝登録セキスペ等）への支援**も必要。

3. サイバーセキュリティ人材の育成・確保

- セキュリティの専門人材・プラスセキュリティ人材の育成・確保を行い、**中小企業の内部人材のセキュリティ対策の底上げ**を図っていただきたい。
- 中小企業の身近な相談先は、税理士や金融機関も想定されることから、こうした関係者を結節点と位置づけ、外部の**セキュリティ専門家（登録セキスペ等）に容易にアクセスできる仕組みづくり**が必要。

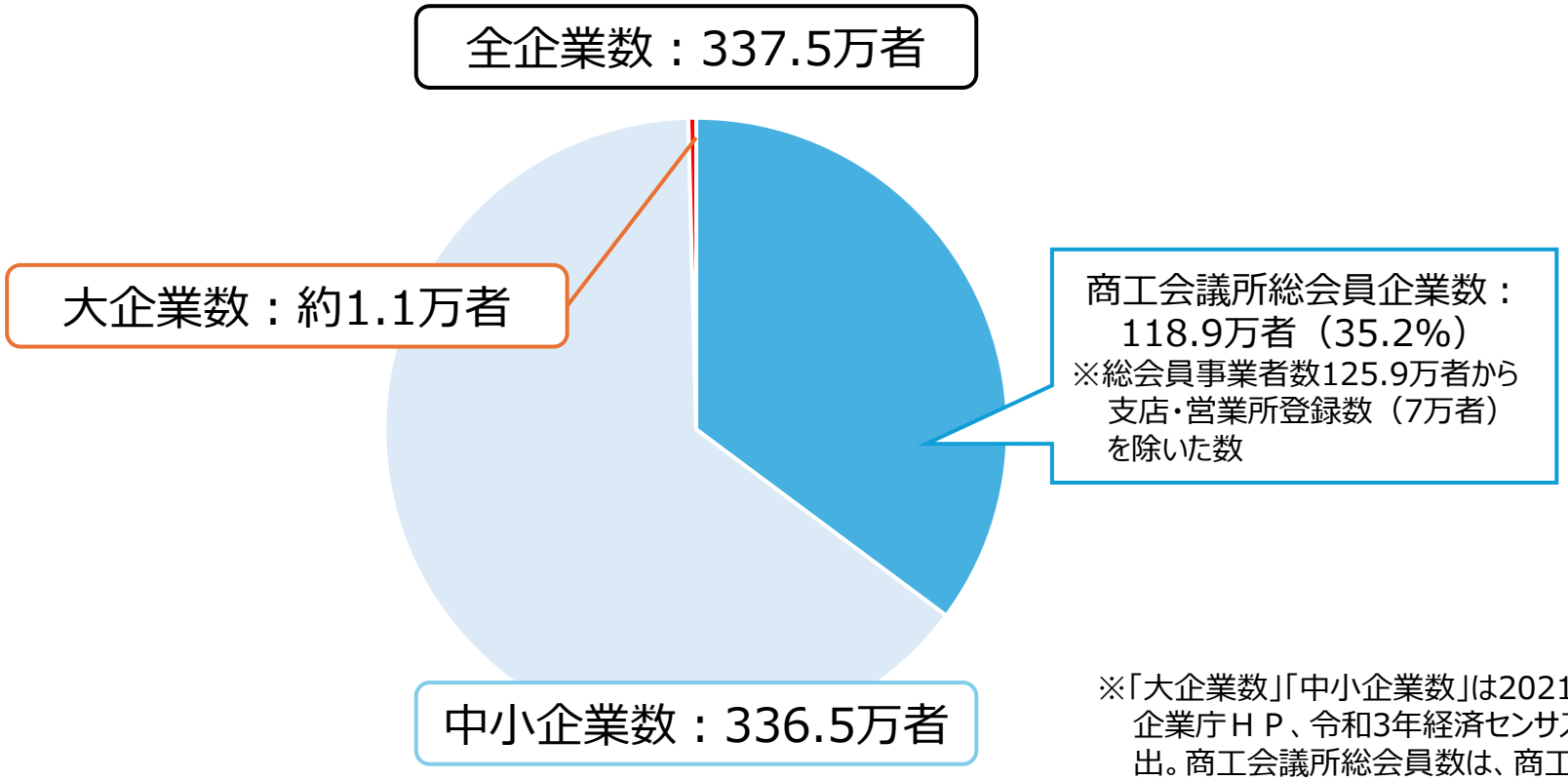
4. 政府からの情報提供の強化

- 中小企業経営者が自分ごとと捉えてもらえるような中小企業の具体的な被害事例を公開するなど、**わかりやすい周知・広報を強化**すべき。
- **中小企業でも取り組めるセキュリティ対策の支援**を行い、支援策の中身を踏まえた周知を行うべき。

（参考）商工会議所とは

○商工会議所は**全国515か所に立地**し、おおむね「市」の単位に１つの商工会議所がある。総会員企業数は「119万者」（総会員数は支店等を足した126万者）で、**全国の中小企業336.5万者**（うち285万者[84.5%]が小規模事業者）**の約1/3強（35.2%）が会員企業**である。

○商工会議所は、「中小企業・小規模事業者の活力強化」、「地域経済の活性化」を主なミッションとして、さまざまな活動を行っている。



※企業数は、個人事業主を含む。支店、営業所数は含まない。

※「大企業数」「中小企業数」は2021年中小企業庁ＨＰ、令和3年経済センサスから算出。商工会議所総会員数は、商工会議所現状調査（2022.3末）から集計。

（参考）日本商工会議所のサイバーセキュリティ対策促進に向けた取り組み

○日本商工会議所は、**中小企業及び各地商工会議所のサイバーセキュリティ対策の促進に向けて活動**を展開。「現状把握・体制整備」「職員の人材育成・リテラシー向上」「ツールの活用による対策強化」「会員企業などへの情報提供」の4つの視点で取り組んでいる。

○中小企業の**サイバーセキュリティ対策は、デジタル化の推進と車の両輪**であり、何度も**繰り返し周知・啓蒙**していくことが重要。

商工会議所が取り組む情報セキュリティ対策

1．現状把握・体制整備

①情報セキュリティ5か条
②情報セキュリティ自社診断
③セキュリティポリシー策定
④関係規定類整備
⑤相談窓口・通報先
例：IPA「情報セキュリティ安心相談窓口」
https://www.ipa.go.jp/security/anshin/

2．職員の人材育成、リテラシー向上

①情報セキュリティ啓発映像コンテンツ
②研修会参加
③資格取得の推進
④会議所向け攻撃メール訓練
ITパスポート試験
ITコーディネータ試験

3．ツール活用による対策強化

①SECURITY ACTION
②情報セキュリティ対策ガイドライン
③データバックアップ
④会議所向け保険

4．会員企業などへの情報提供

①ホームページ
②会報誌
③会員向けセミナー
④部会等の勉強会
⑤事業者向け攻撃メール訓練
⑥事業者向け保険
⑦WEBサイト運営ガイド
⑧サイバーセキュリティお助け隊サービス

（参考）中小企業のサイバー攻撃被害事例

（独）情報処理推進機構「中小企業サイバー攻撃被害事例収集等業務　実施報告書」（2024年3月29日とりまとめ）参照

【メールを通じた被害】

○官公庁からの連絡を装ったウイルス付きメールを開封し感染

○UTMを導入する前に迷惑メールを開いてしまった

○**ウイルスに感染していた私物パソコンを、社内ネットワークに接続**し、**社内システムにウイルスが拡散**。社員教育や不許可端末の検知機能が十分ではなかった。

○ランサムウェア被害により複数台のサーバーが感染。復旧に１週間以上を要した。

○エモテットによる攻撃メール被害に遭遇した。不審なメールが一定の時期に集中して社内に送られて発覚。**協力会社からの情報漏洩が原因**と見られる。

【ホームページ改ざんの被害】

○自社ホームページの管理用IDとパスワードが漏洩し、ホームページが書き換えられ、ホームページをクリックすると別のサイトにリダイレクトされる事象が発生。**漏洩の原因を調べたかったが、見積もりが高額だったため断念**。書き換えられたコードを元に戻し、UTMとエンドポイントセキュリティを導入するなどの対策を講じて問題を解決。**担当者が一人で、管理者が十分に社員教育をしていなかったことが要因の１つ**。定期的なパスワード変更などにより再発防止。

（参考）商工会議所の「サイバーセキュリティお助け隊サービス」

○情報処理推進機構（IPA）は、中小企業のセキュリティ対策としてサイバー攻撃への対処に最低限必要な**①異常の監視**（24 時間見守って攻撃を検知・通知）、**②緊急時の駆け付け**、**③保険**をセットにした『サイバーセキュリティお助け隊サービス』の基準を制定。

○①②③をワンパッケージに、現在、基準を満たした40社58サービスが登録(2024年12月現在)。同サービスを利用する中小企業はロゴマークを使用でき、自社の社会的信用も向上。

サイバーセキュリティ CSお助け隊

商工会議所 サイバーセキュリティお助け隊サービス

○大阪商工会議所をはじめ、新潟・松本・宇都宮・前橋・高崎・佐倉・静岡・北大阪・広島・福山・竹原・三次・徳島・高知・熊本商工会議所（順次拡大中）は『**商工会議所サイバーセキュリティお助け隊サービス**』を提供。対象地域は「全国」(一部の離島には緊急時の駆け付けなど一部提供できないサービスあり)。

全国いずれかの商工会議所・商工会の
会　員　月額 **6,600**円（年79,200円）
非会員　月額 8,250円（年99,000円）
- 初期費用なし(UTM設置をお助け実働隊に依頼する場合のみ16,500円)
- オプション料金・追加料金など一切なしの明朗会計
- １年ごとの契約更改なので安心（初年度のみ直近3月迄の契約)

※大阪商工会議所ホームページより