サイバーセキュリティ研究所ダイジェスト！

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
サイバーセキュリティネクサス ネクサス長
井上 大介

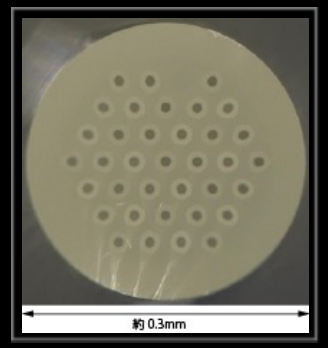
NICT National Institute of Information and Communications Technology

CYBERSECURITY Research Institute

国立研究開発法人 情報通信研究機構とは？

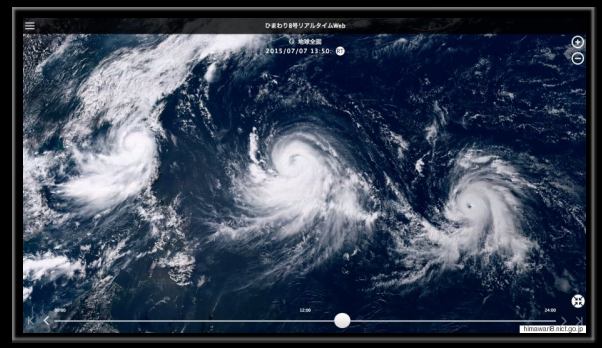
● 情報通信分野を専門とする日本で唯一の公的研究機関

日本標準時の生成・配信
（うるう秒挿入）

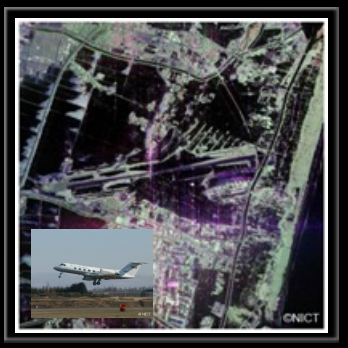


光通信システム
（ペタbps級 マルチコアファイバ）

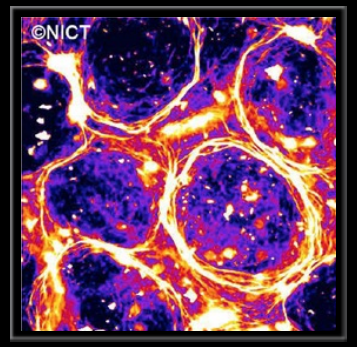
宇宙通信システム
（超高速インターネット衛星きずな）



サイエンスクラウド
（ひまわり8号リアルタイムWeb）



電磁波センシング
（Pi-SAR2による3.11直後の仙台空港）

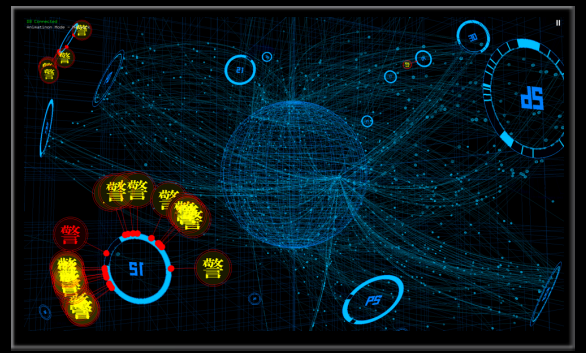


バイオ・ナノICT
（生体分子の自己組織化）

脳情報通信融合
（ブレイン・マシーン・インターフェイス）

多言語音声翻訳
（多言語音声翻訳アプリVoiceTra）

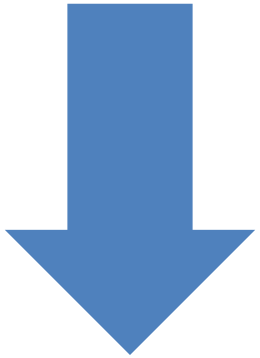
超臨場感コミュニケーション
（初音ミクさんの電子ホログラフィ）



サイバーセキュリティ
（対サイバー攻撃アラートシステムDAEDALUS）

NICT 中長期計画（5ヵ年計画）

●第5期中長期計画：2021年4月～2026年3月



●第6期中長期計画：2026年4月～2031年3月

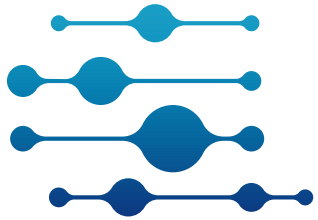
NEXT!!

NICT サイバーセキュリティ研究所 2026

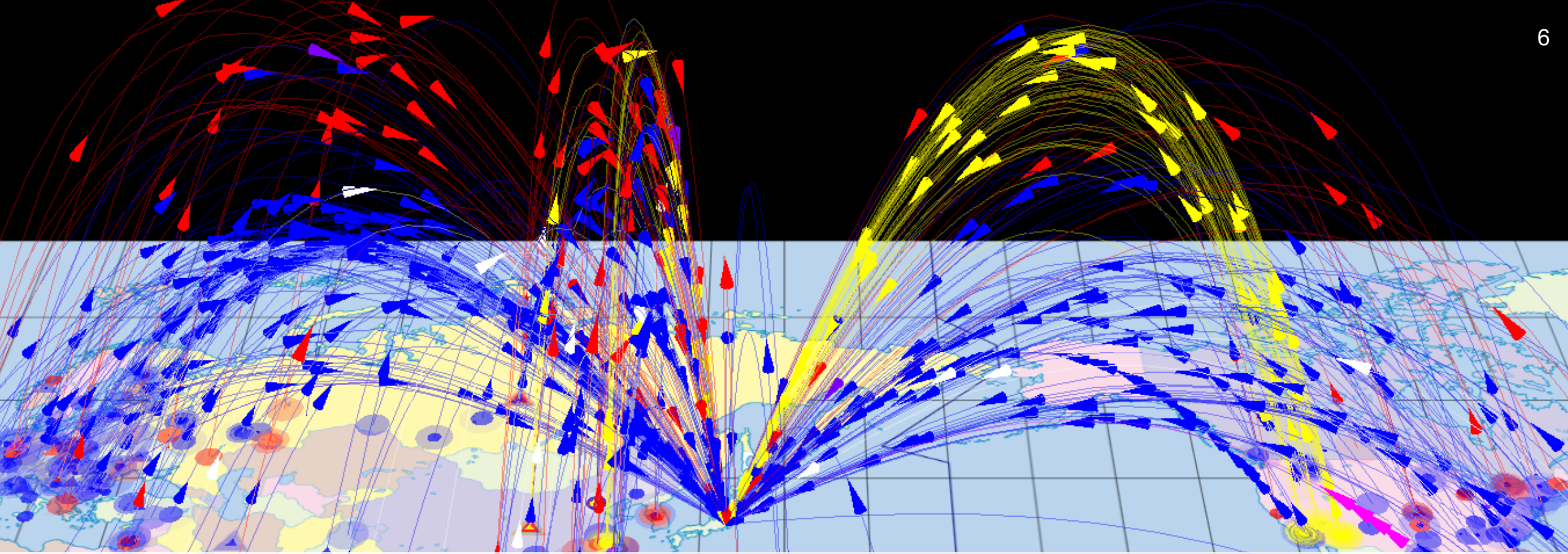
CYBERSECURITY Research Institute
サイバーセキュリティ研究所
(CSRI)

2011	2011	2017	2019	2021	2025 NEW
CYBERSECURITY Laboratory	SECURITY FUNDAMENTALS Laboratory	National Cyber Training Center	NATIONAL CYBER OBSERVATION CENTER	CYNEX CYBERSECURITY NEXUS	CREATE Center for Research on AI Security and Technology Evolution
サイバーセキュリティ研究室 (CSL)	セキュリティ基盤研究室 (SFL)	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)
攻撃観測 分析・対策研究	暗号研究	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



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

NICTER観測レポート2025

https://csl.nict.go.jp/nicter-report.html

NICTERダークネット観測統計（過去10年）

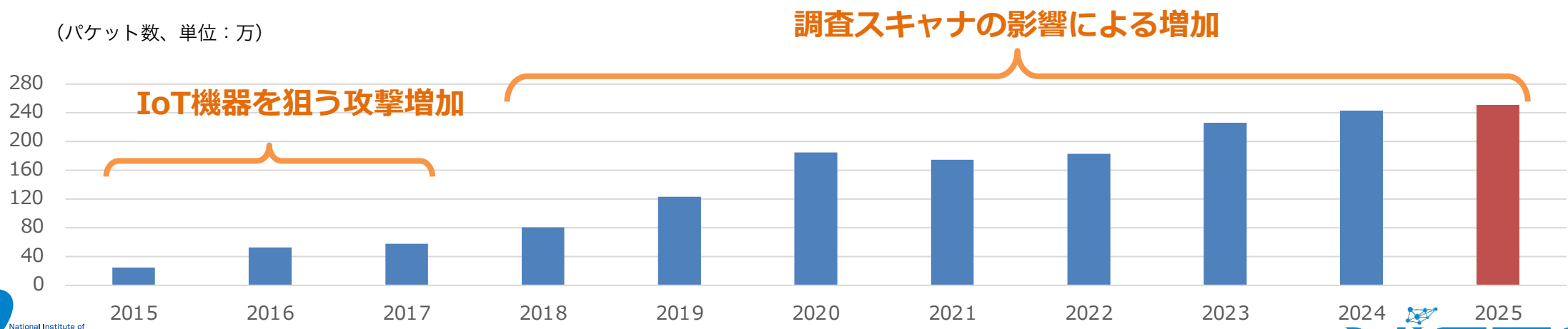
年	年間総観測パケット数	ダークネットIPアドレス数	1 IPアドレス当たりの年間総観測パケット数
2016	約1,440億	274,872	527,888
2017	約1,559億	253,086	578,750
2018	約2,169億	273,292	806,877
2019	約3,756億	309,769	1,231,331
2020	約5,705億	307,985	1,849,817
2021	約5,180億	289,946	1,747,685
2022	約5,226億	288,042	1,833,012
2023	約6,197億	289,686	2,260,132
2024	約6,862億	284,445	2,427,977
2025	**約7,010億**	**284,305**	**2,504,680**

1アドレスあたり

13秒に1回

攻撃関連通信受信

（パケット数、単位：万）



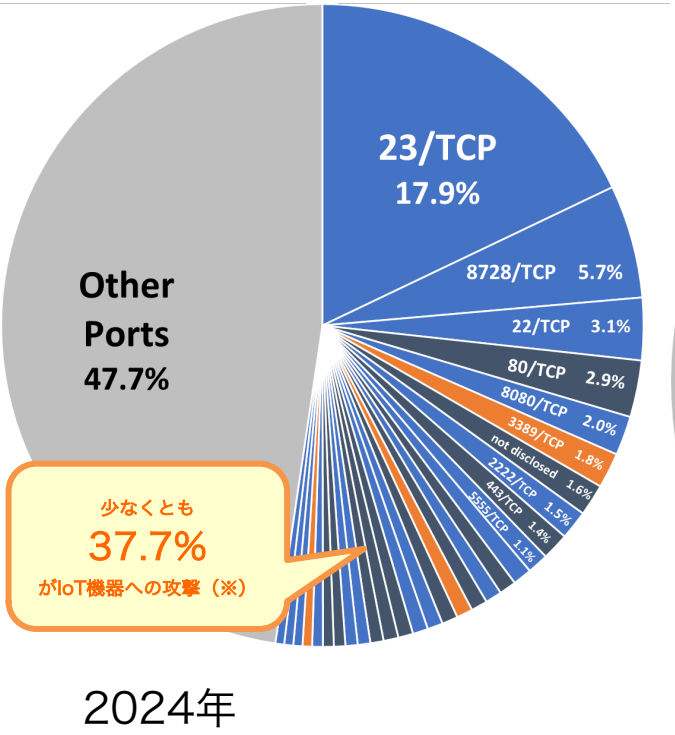
1 IPアドレス当たりの年間総観測パケット数

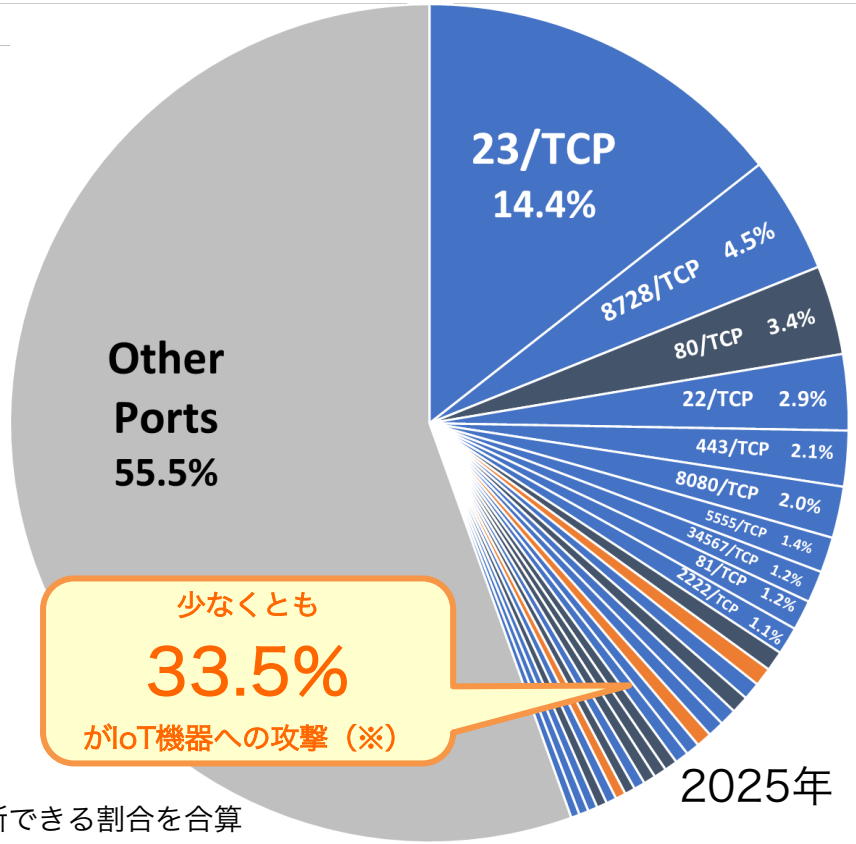
National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

宛先ポート番号別パケット数分布（2025年）

- **2025年の特徴**
  - ✓ 23/TCP（telnet）、8728/TCP（MikroTik）宛てが継続
  - ✓ IoT機器固有のサービスのポート番号宛てが増加傾向
  - ✓ Windows 宛てが更に減少傾向で、上位10位に入らず
  - ✓ 多数のポート（Other Ports）宛てにスキャンするIoTマルウェア





※上位30ポートのうち、IoT機器への攻撃と判断できる割合を合算

ポート番号	主な攻撃対象
23/TCP	Telnet （ルータ，Webカメラ等）
8728/TCP	MikroTik RouterOS API
80/TCP	HTTP（Web管理画面）
22/TCP	SSH（サーバ，ルータ等）
443/TCP	HTTPS (Web管理画面等)
8080/TCP	HTTP（ホームルータ、DVR等）
5555/TCP	ADB（Android Debug Bridge）
34567/TCP	Xiongmai API
81/TCP	HTTP（Web管理画面）
2222/TCP	SSH（サーバ，ルータ等）

宛先ポート番号別パケット数分布
（調査目的のスキャンパケットを除く）

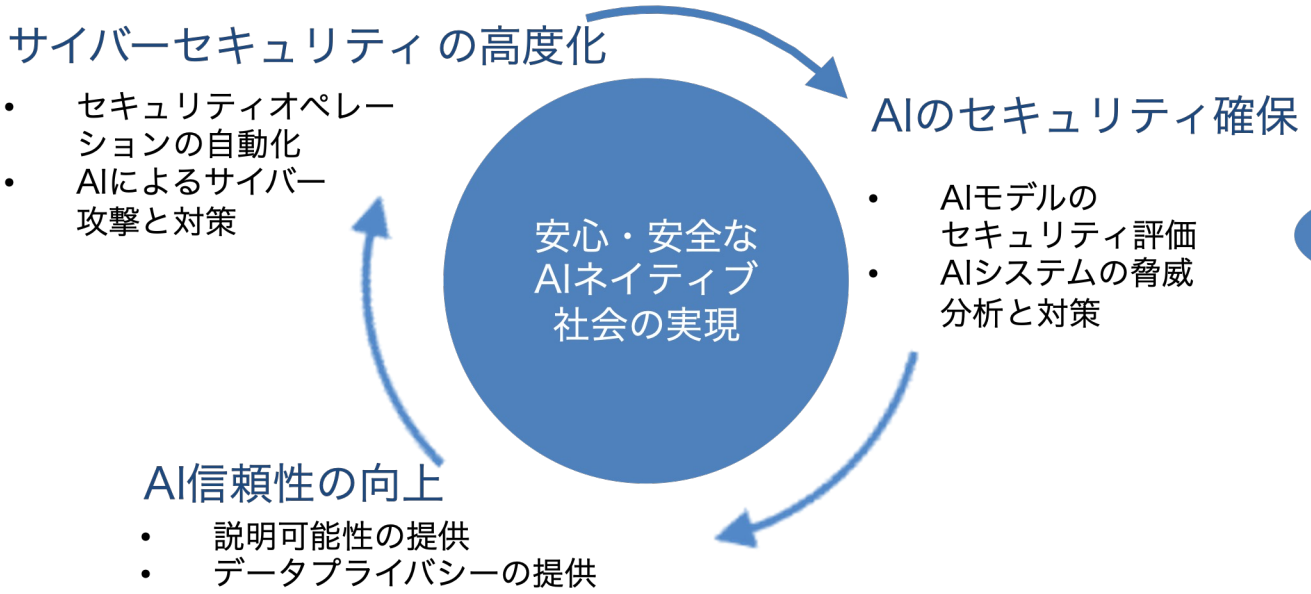
AIセキュリティ研究センター

CREATE
Center for Research on AI Security and Technology Evolution

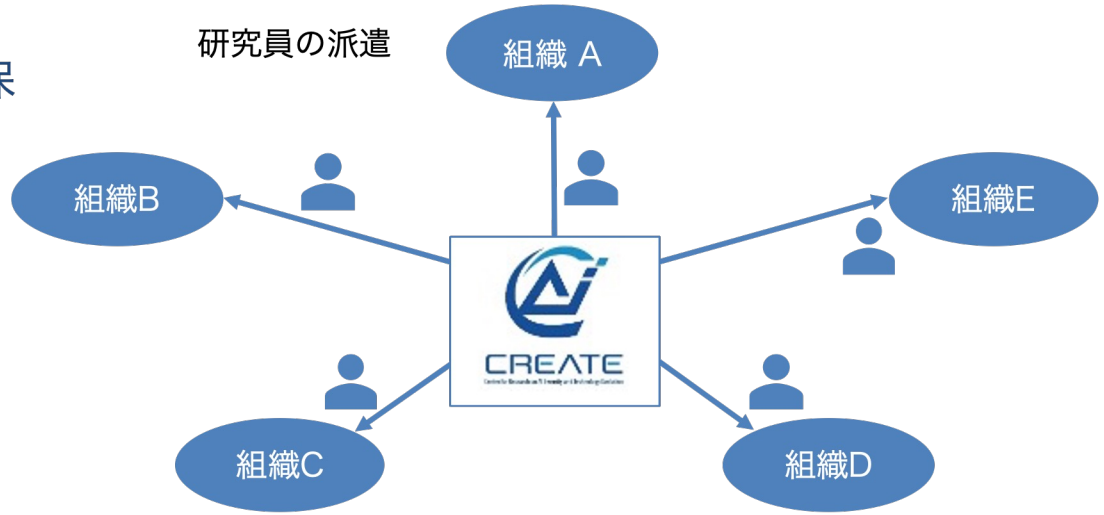
CREATE：AIセキュリティ研究センター

- AI for Security：AIによるセキュリティの高度化
- Security for AI：AI自身のセキュリティ確保

1 AIセキュリティの研究開発



2 強靭なグローバル連携研究の推進



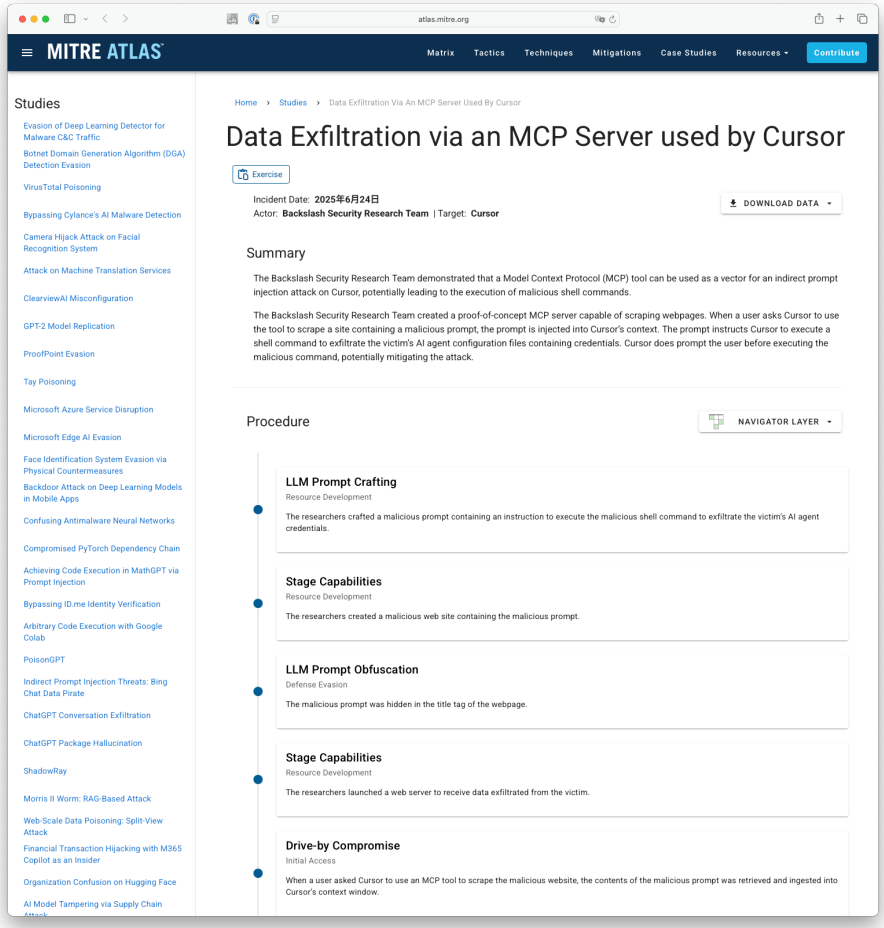
3 日米の連携コミュニティの形成・AIセキュリティ動向分析

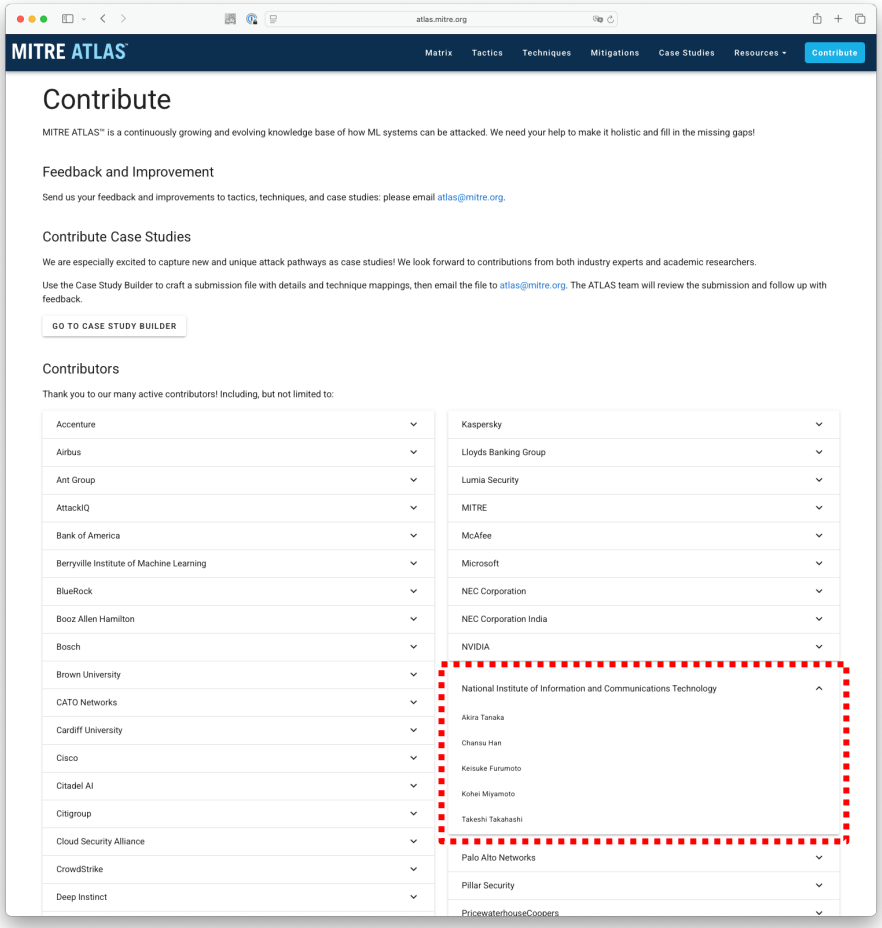
NICT National Institute of Information and Communications Technology

CREATE Center for Research on AI Security and Technology Evolution

LLMセキュリティ評価

- MITRE ATLASのCase Studiesにプロンプトインジェクション攻撃を追加





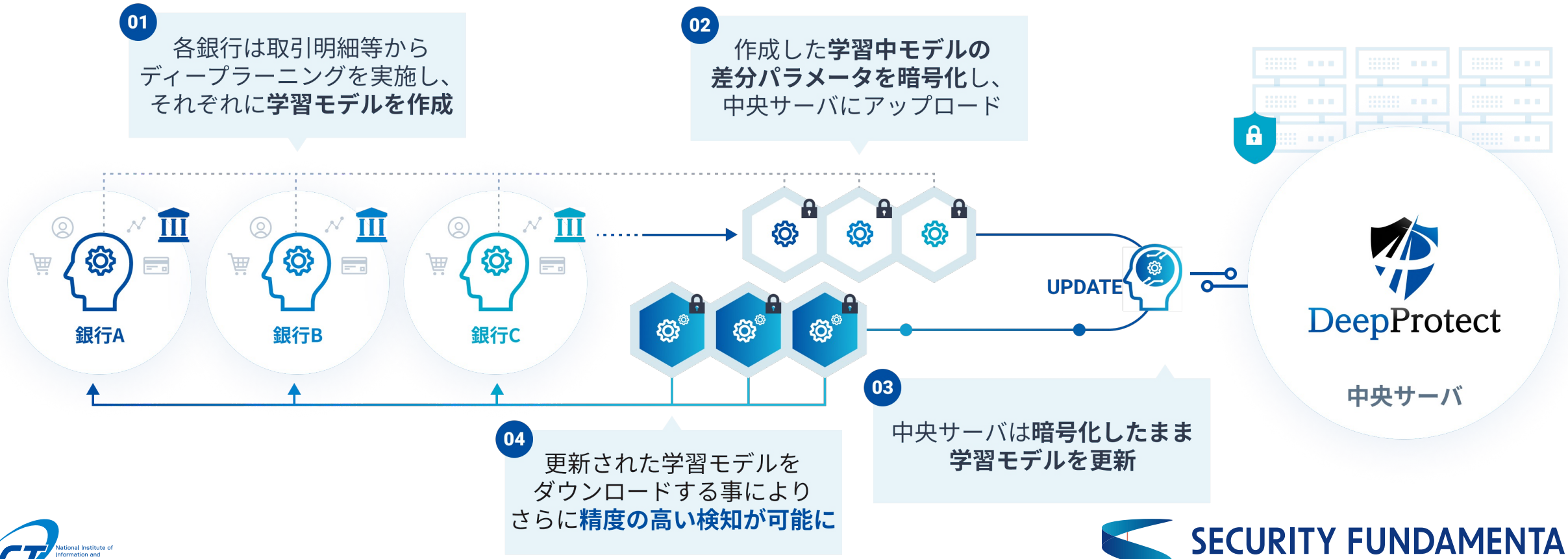
https://atlas.mitre.org/studies/AML.CS0045

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

プライバシー保護連合学習システム DeepProtect

- 外部にデータ開示することなく、複数組織で連携して深層学習を行う
  プライバシー保護連合学習システム
  - ✓ 銀行データを用いた不正口座検知の実証実験



量子コンピュータによる現代暗号の危機

- **大規模量子コンピュータが実現すると**
  現在使われている公開鍵暗号の安全性が急低下

	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	

但し、現時点の量子コンピュータが直ちに脅威になるものではなく、当面、公開鍵暗号の安全性に問題はない

CRYPTREC

- **Cryptography Research and Evaluation Committees**
  - ✓ 電子政府推奨暗号の安全性を評価・監視し暗号技術の適切な実装法・運用法を調査・検討
  - ✓ **2025年3月 CRYPTREC 耐量子計算機暗号ガイドライン発行（改訂版）**
  - ✓ **FIPS 203（ML-KEM）安全性・実装性能評価を実施中**

デジタル庁 Digital Agency　総務省 MIC Ministry of Internal Affairs and Communications　経済産業省 Ministry of Economy, Trade and Industry

暗号技術検討会
事務局：デジタル庁、総務省、経済産業省

NICT 国立研究開発法人 情報通信研究機構 National Institute of Information and Communications Technology

IPA 独立行政法人 情報処理推進機構

暗号技術評価委員会
事務局：NICT, IPA
暗号技術の安全性評価を中心とした
技術的な検討課題を担当

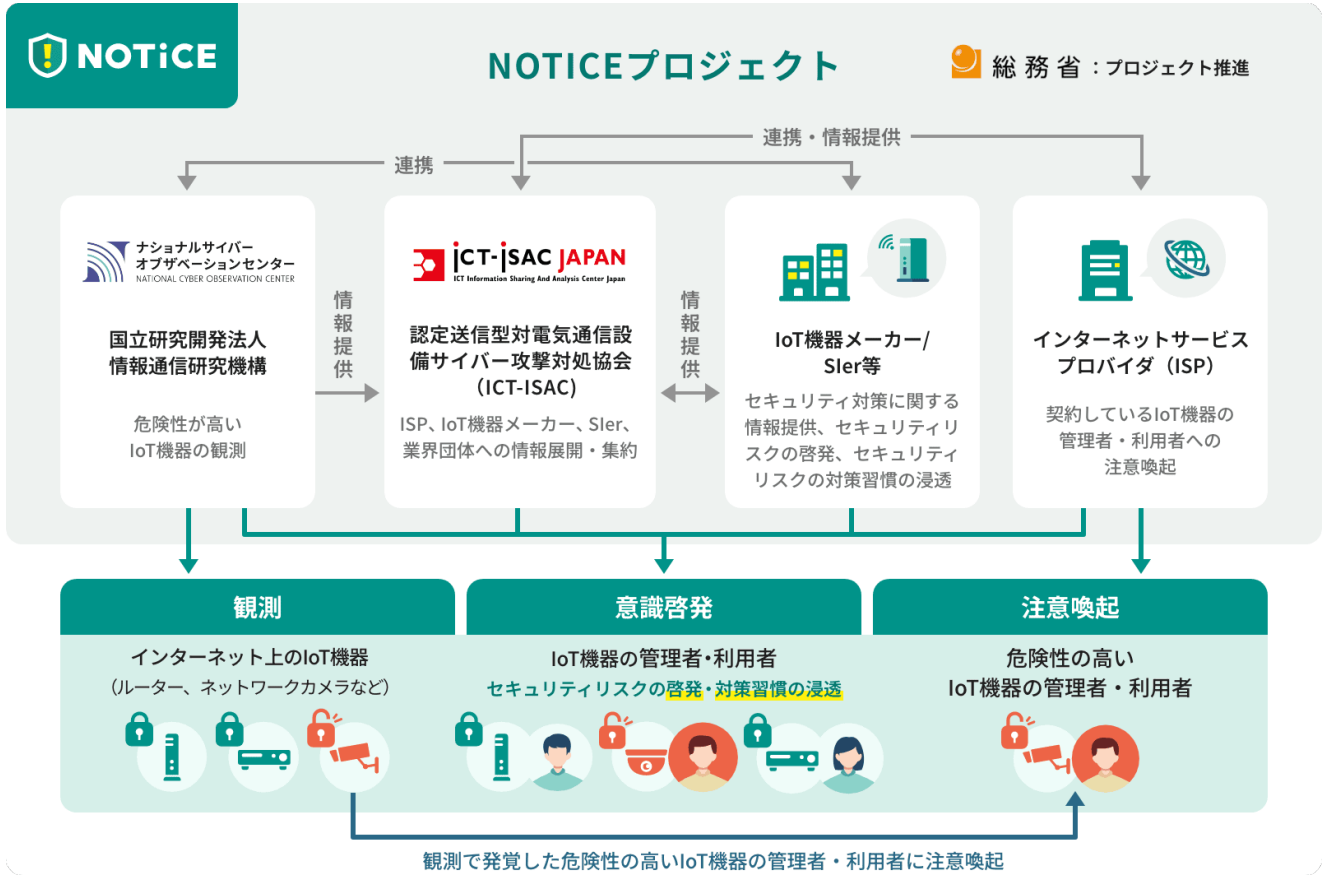
暗号技術活用委員会
事務局：IPA, NICT
セキュリティ対策の推進、暗号技術の利用促進及び
産業化を中心とした暗号利用に関する検討課題を担当

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12月時点）

IoT機器観測総数

月 1.17 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 13,796 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 2,536 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 328 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

月 15,077 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 110 組織

※2025年11月現在

ISP	IoT機器メーカー	SIer	団体
96社	10社	2社	2団体

https://notice.go.jp/

NATIONAL CYBER OBSERVATION CENTER

ナショナルサイバートレーニングセンター

National
Cyber
Training
Center

ナショナルサイバートレーニングセンター

実践的サイバー防御演習
「CYDER」（サイダー）

国の機関、地方公共団体、重要社会基盤事業者等を対象とする実践的なサイバー防御演習

万博向けサイバー防御講習
「CIDLE」（シードル）

2025大阪・関西万博の安全な開催に向けた、関連組織の情報システム担当者等を対象としたサイバー防御演習

実践サイバー演習
「RPCI」（リプシィ）

情報処理安全確保支援士向け特定講習。CYDERのノウハウを活かした、リアリティの高い実践的なインシデントハンドリング演習

「SecHack365」
（セックハック サンロクゴ）

セキュリティイノベーター育成を目的として、NICTが若年層のICT人材を対象に、セキュリティの技術研究・開発を本格的に指導する新規プログラム

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

➡ 2025年度：集合演習 + プレCYDER = 受講者数8,200名超

概要（2025年度）

【受講対象】 国の機関、指定法人、独立行政法人（無料）
地方公共団体の職員（プレCYDERとAコースは無料）
重要社会基盤事業者、民間企業等（有料）
【開催形式】 集合演習（**全都道府県で100回程度**）
オンライン演習

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
A	集合演習	初級	システムに携わり始めたばかりの方 (事案発生時の対応の流れ)	全組織共通
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
B-2				地方公共団体以外
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
プレCYDER	オンライン演習	-	インシデント発生時の対応の学習を これから始める、又は始めたばかりの方	全組織共通

CYDER受講者数の推移（累積数）

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）

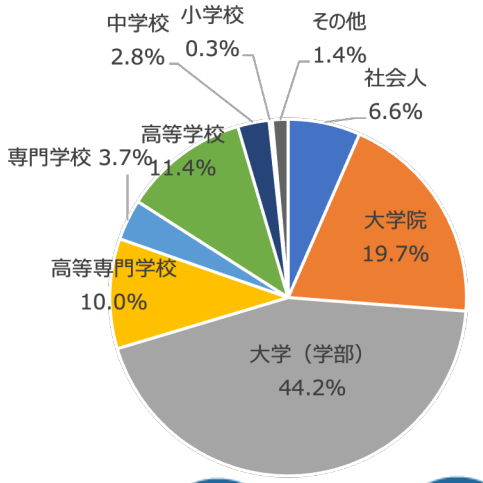
✓ 長期ハッカソンによるモノ作りの機会を通し、1年をかけて技術力や継続力、アイデア発想力、倫理面などの指導を行い、作品作りに取り組む未来のセキュリティイノベーター育成プログラム

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（2017～2024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。

SecHack365 年間プログラム

2025年

第1回イベント	6月14日(土)		キックオフ
第2回イベント	8月1日(金) ～3日(日)	東京	活動状況の把握と助言
第3回イベント	9月26日(金)～28日(日)	東京	作品発表＆レビュー
第4回イベント	11月14日(金)～16日(日)	大阪	作品発表 最終発表への練習と助言
第5回イベント	2026年 1月31日(土)・2月1日(日)		最終発表
第6回イベント	2026年 2月27日(金)・28日(土)	東京	発表練習・成果発表

年間を通して継続開発

成果発表会 2026年 2月 28日 (土) 東京

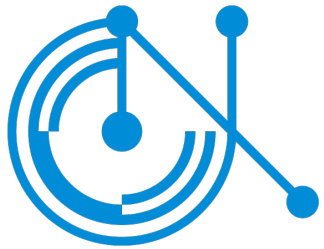
= オンライン開催 = 実地開催

https://sechack365.nict.go.jp

SecHack365 修了生・受講生の活動状況 2025

形式	名前	修了	内容
発表・論文		2024	電子情報通信学会インターネットアーキテクチャ学生研究奨励賞受賞
発表・論文		2023	BlackHatAsia2025発表　sisakulint - CI-Friendly static linter with SAST, semantic analysis for GitHub Actions
発表・論文		2022	CSS2025 SEV-SNPのVMPLによるP4プログラムの軽量な隔離実行
発表・論文		2025	CSS2025 部分的漏洩耐性を持つ合意アルゴリズム
発表・論文		2025	CSS2025 Invisible Consent: LLMエージェントによるブラウザ操作はプライバシーを担保しない
発表・論文		2025	CSS2025 Rustで生成されたマルウェアに対するFLIRTの検証
発表・論文		2024	CSS2025 ファジングにおける希少到達領域の特性に関する実証的研究
発表・ポスター		2025	CSS2025 SDR・スマートフォンを用いた偽基地局検知・位置推定システム
表彰		2018	CSS2025 優秀論文賞　E2EEメッセージングのための透明性と頑健性を備えたコンテンツモデレーション
表彰		2020	CSS2025学生論文賞　敵対的映像攻撃が自律飛行ドローンの位置推定・制御に及ぼす影響評価 (システムトラック)
表彰		2025	CSS2025 優秀論文賞 RowHammerを用いたRISC-V Keystone TEEに対する特権昇格手法の検討
表彰		2022	2025年度（令和7年度）情報処理学会 山下記念研究賞「クライアントの行動に基づくビザンチン耐性のある連合学習の監視メカニズム」
表彰		2020	ACM ASIACCS 2025 Best Paper Award | 25-29 August, Hanoi
採択		2019	GMOインターネットグループ デベロッパーエキスパート クラウドセキュリティ認定
採択		2022	JST 大学発新産業創出基金事業スタートアップ・エコシステム共創プログラム PARKS スタートアップ創出プログラム 学生 PJ（Step1）採択

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産学官連携拠点

- 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]

サイバーセキュリティ研究室

研究開発成果展開

人材育成ノウハウ展開

ナショナルサイバートレーニングセンター

サイバーセキュリティ情報の大規模収集

定常的分析と国内解析者コミュニティ形成

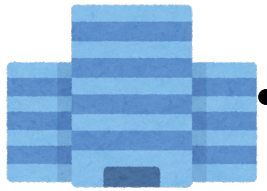
説明可能な国産脅威情報の生成・提供

高度SOC人材育成（Online自主学習＆OJT）

国産セキュリティ技術の検証環境構築

人材育成基盤のオープン化による事業促進

CYNEX ALLIANCE



民間企業・政府機関

共同解析, 育成人材投入,
人材育成基盤利用,
製品プロトタイプ導入, etc.

共同解析, 育成人材投入,
人材育成基盤利用, etc.

教育機関

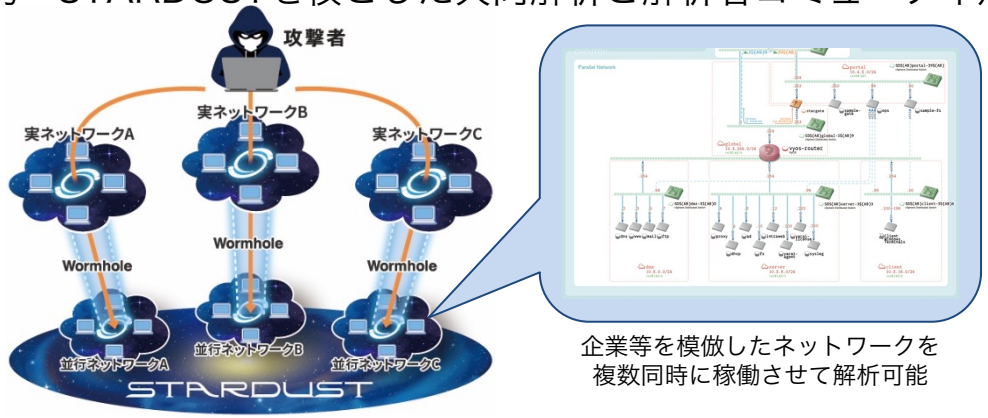
108組織参画中
(2026/1/1)

4つの “Co-Nexus” によるプロジェクト推進

Co-Nexus A (Accumulation & Analysis)

参画組織数：45

- 目的：STARDUSTを核とした共同解析と解析者コミュニティ形成



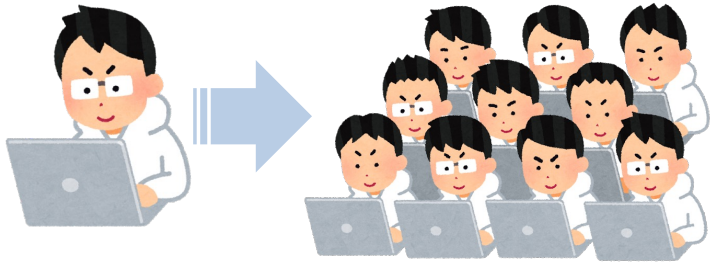
企業等を模倣したネットワークを
複数同時に稼働させて解析可能

サイバー攻撃誘引基盤STARDUST

Co-Nexus S (Security Operation & Sharing)

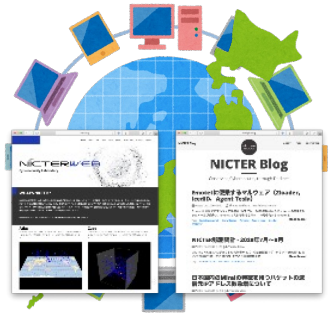
参画組織数：17

- 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



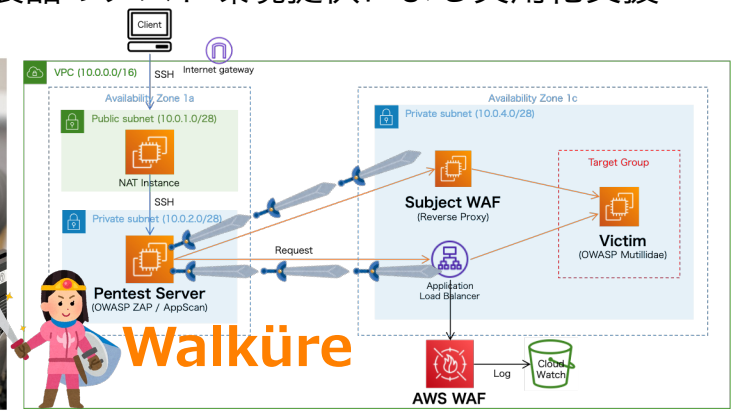
国産脅威情報発信/提供

Co-Nexus E (Evaluation)

参画組織数：7

- 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

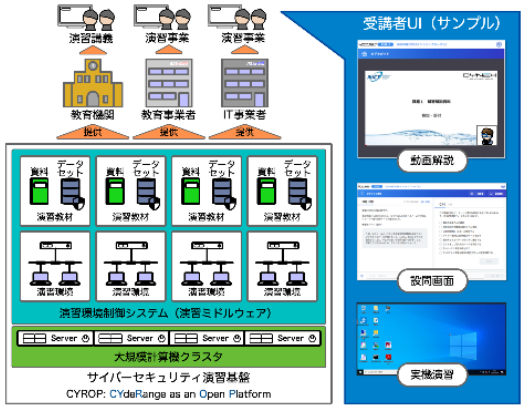


WAF製品検証環境

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

参画組織数：86

- 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

サイバーセキュリティのエコシステム確立に向けて

- 官：国産セキュリティ製品を使う
- 産：国産セキュリティ製品を創る
- 学：イノベーターを輩出する