シン・サイバーセキュリティ研究所

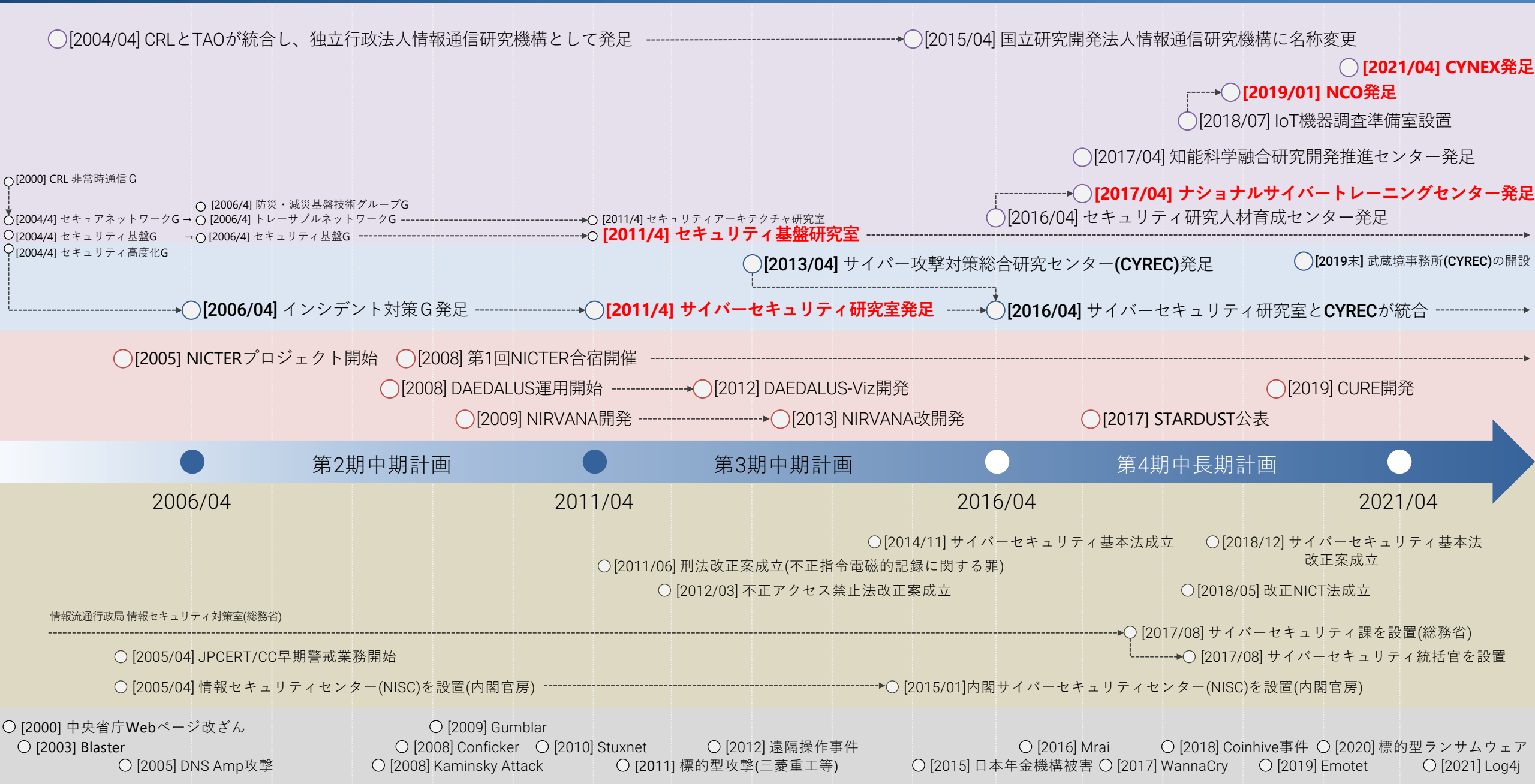
～ つづけていくこと、つないでいくこと ～

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

NICTのサイバーセキュリティ分野のタイムライン (2000年~)

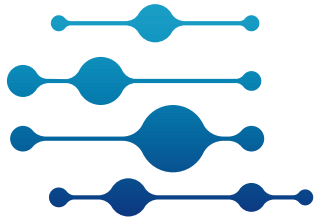


NICT サイバーセキュリティ研究所 2025

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

2011年	2011年	2017年	2019年	2021年	2025年
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/暗号解析/暗号応用研究	サイバー攻撃観測/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促進	産学官連携拠点形成	AIセキュリティ研究/国際連携

サイバーセキュリティ研究室



CYBERSECURITY
Laboratory

2025年

NICTER観測20周年

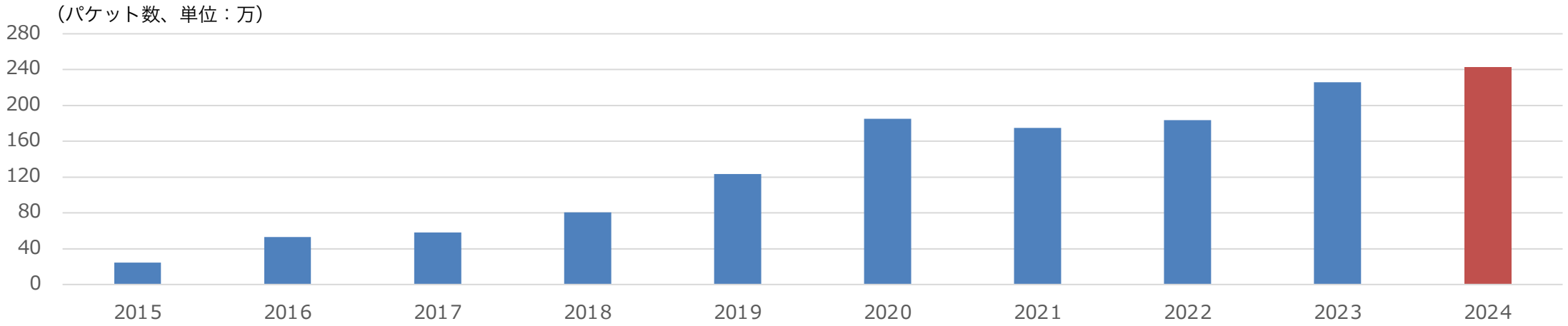
NICTER ダークネット観測統計（過去10年）

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

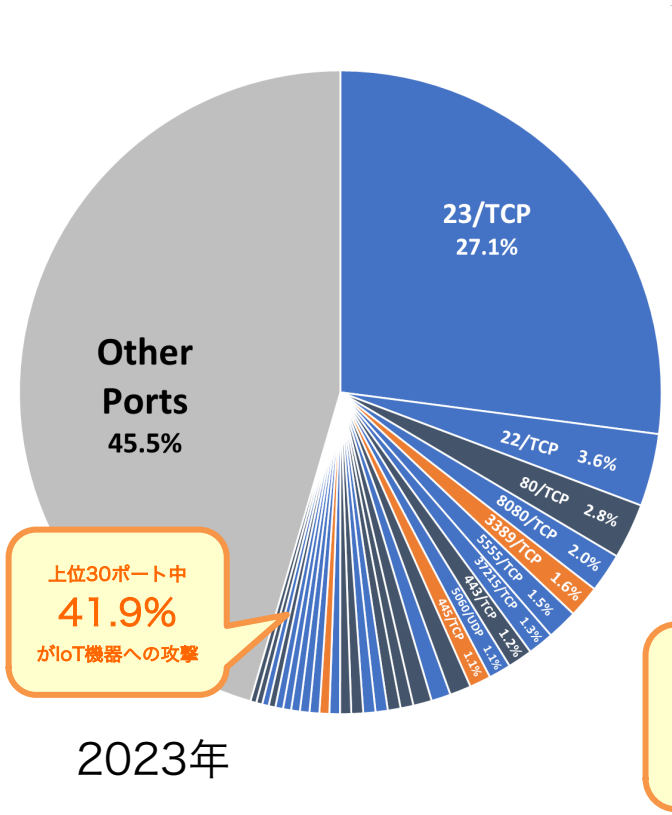


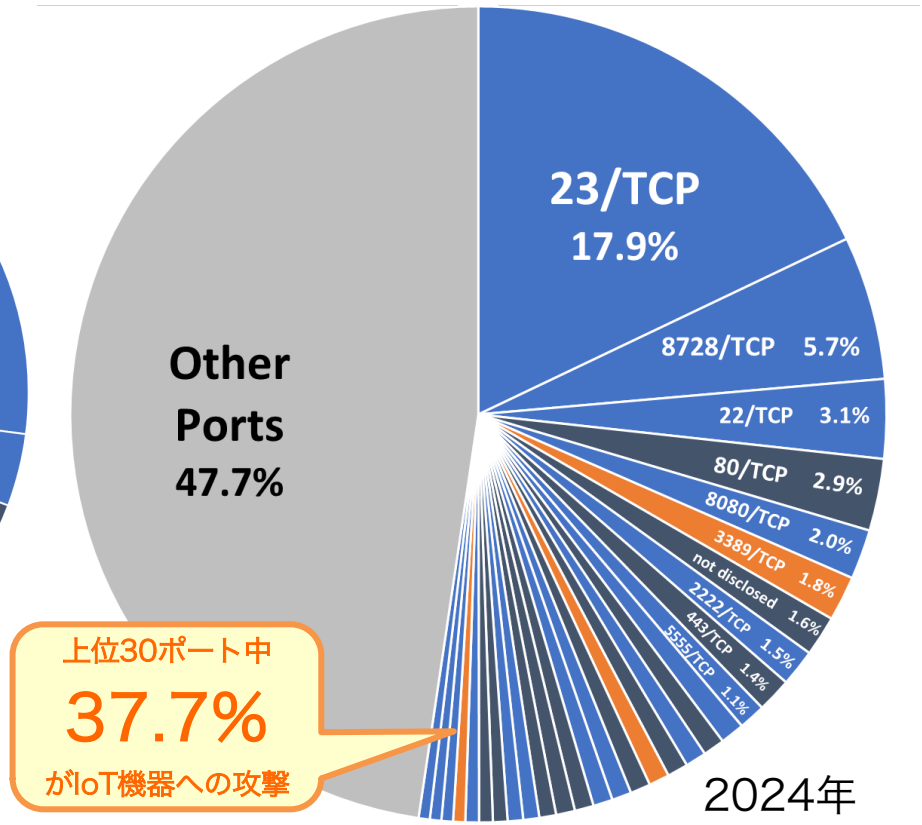
1 IPアドレス当たりの年間総観測パケット数

宛先ポート番号別パケット数分布（2024年）

● 2024年の特徴

- ✓ 上位30ポート中 37.7%がIoT機器への攻撃
- ✓ 23/TCP（Telnet）宛てが減少
- ✓ IoT機器固有のサービスのポート番号宛てが増加





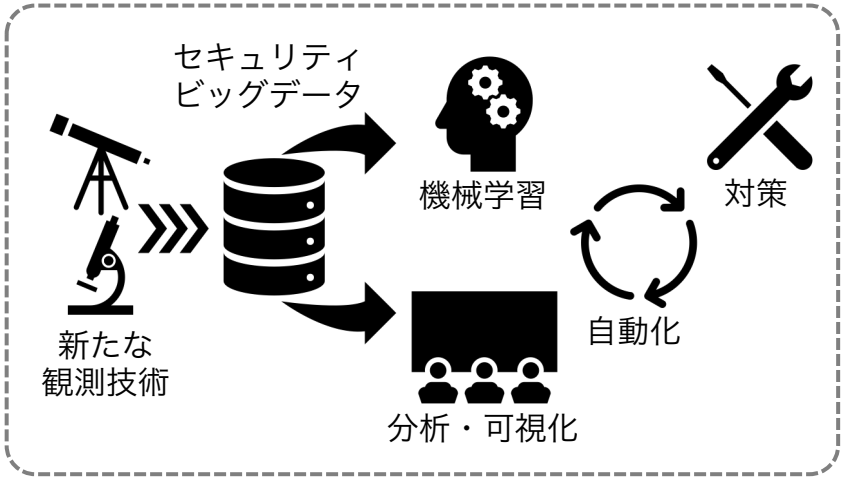
ポート番号	主な攻撃対象
23/TCP	Telnet （ルータ，Webカメラ等）
8728/TCP	MikroTik RouterOS API
22/TCP	SSH（サーバ，ルータ等）
80/TCP	HTTP（Web管理画面）
8080/TCP	HTTP（ホームルータ、DVR等）
3389/TCP	Windows Remote Desktop
not disclosed	目的不明
2222/TCP	SSH（サーバ，ルータ等）
443/TCP	HTTPS (Web管理画面等)
5555/TCP	ADB（Android Debug Bridge）

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）

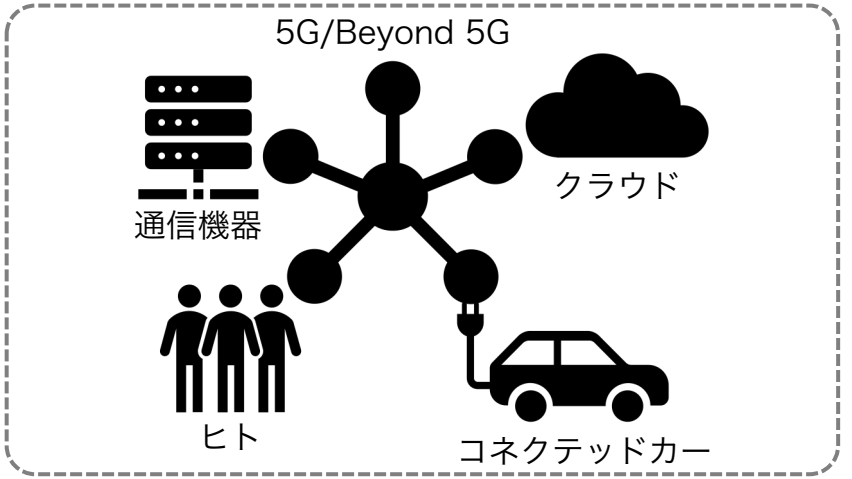
詳しくは…
『NICTER観測レポート2024』で！
https://csl.nict.go.jp/report/NICTER_report_2024.pdf

サイバーセキュリティ研究室の研究課題 (2021-2026)

- **データ駆動型サイバーセキュリティ技術**
  - ✓ 次世代**STARDUST**研究
  - ✓ **CURE**への情報集約と持続的進化
  - ✓ **AI x Cybersecurity**融合研究, etc.



- **エマージングセキュリティ技術**
  - ✓ **5G/B5G**セキュリティ
  - ✓ **ローレイヤ**セキュリティ
  - ✓ **ユーザブル**セキュリティ, etc.



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

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

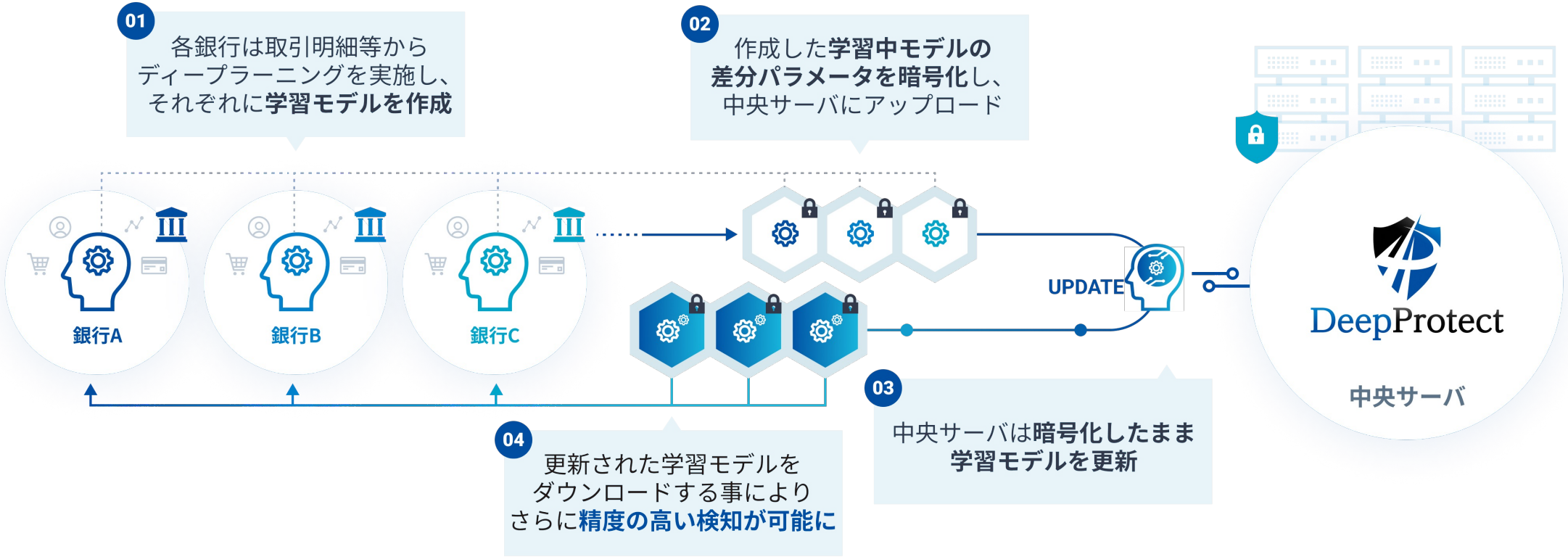
- データのセキュリティ・プライバシーの確保
- 秘密計算等のプライバシー保護解析技術
- 組織横断連携を含むデータ利活用技術
- 安全なテレワーク等に資する研究開発

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

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



基本論文が2023 IEEE Signal Processing Society Best Paper Award 受賞

Le Trieu Phong, Yoshinori Aono, Takuya Hayashi, Lihua Wang, and Shiho Moriai for “Privacy-Preserving Deep Learning via Additively Homomorphic Encryption”, IEEE Transactions on Information Forensics and Security, May 2018.

CRYPTREC

- **Cryptography Research and Evaluation Committees**

  目的：電子政府推奨暗号等の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討することを通じてセキュアなIT社会の実現を目指す。

総務省 MIC Ministry of Internal Affairs and Communications

経済産業省 Ministry of Economy, Trade and Industry

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

IPA Better Life with IT 情報処理推進機構

暗号技術検討会

事務局：デジタル庁、総務省、経済産業省

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

➡ **2025年4月発行予定**

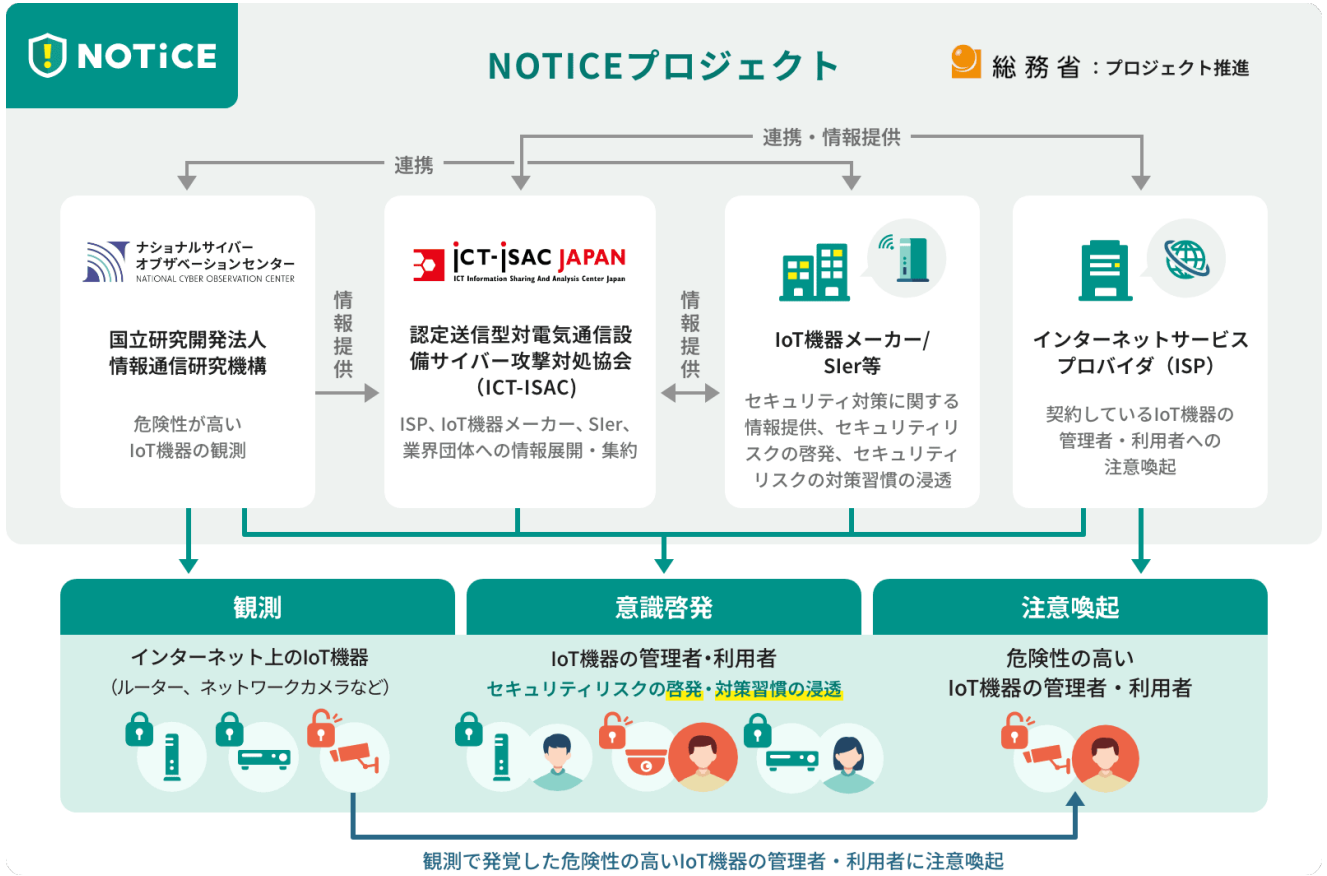
『CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）』（改訂版）

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（2024年12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14,665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4,399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1,929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16,097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94組織

※2025年2月現在

ISP	IoT機器メーカー	SIer	団体
85社	6社	1社	2団体

https://notice.go.jp/

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 FY2024

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一連の対応の流れを体験

➡ 2024年度 集合演習 + プレCYDER = 受講者数8,000名over！

CYDER
Cyber Defense Exercise with Recurrence

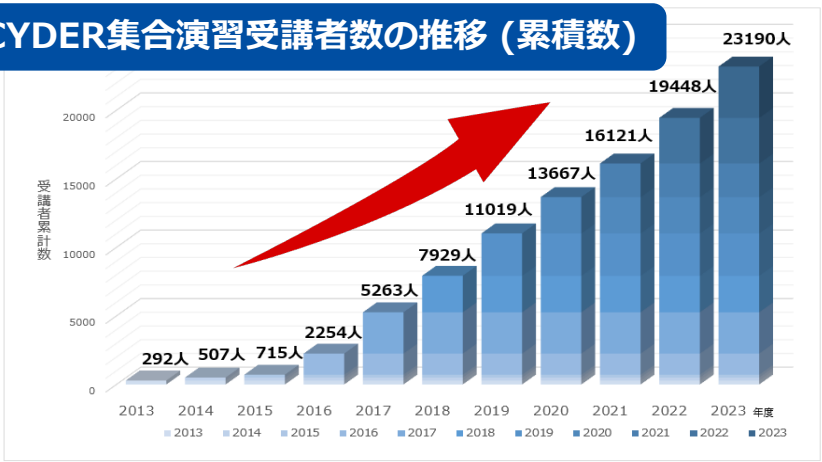
2024年度の実施内容および対象組織

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集合演習受講者数の推移 (累積数)



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

● 若手向け『セキュリティイノベーター』育成プログラム

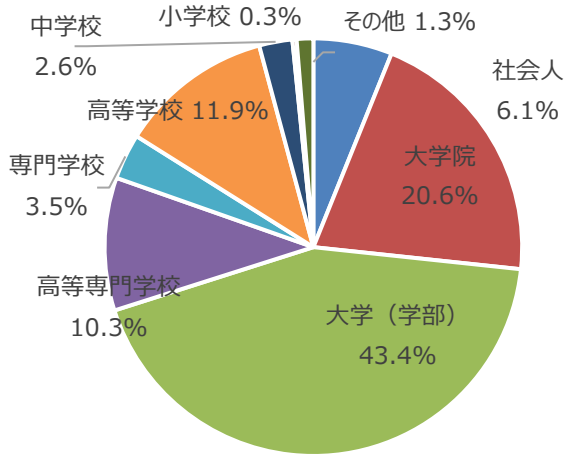
✓ 長期ハッカソンによるモノ作りの機会を通し、1年をかけて技術力や継続力、アイデア発想力、倫理面などの指導を行い、作品作りに取り組む未来のセキュリティイノベーター育成プログラム

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。

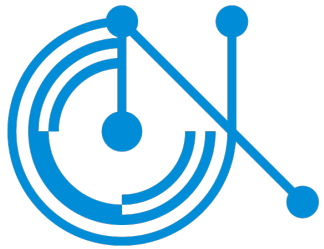
2024年 SecHack365 年間プログラム

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

サイバーセキュリティ産学官連携拠点の形成に向けて

● 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）

● 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

CYNEX：サイバーセキュリティ統合知的・人材育成基盤

- サイバーセキュリティ情報を国内で**収集・蓄積・分析・提供**するとともに、社会全体で
  サイバーセキュリティ人材を育成するための**共通基盤を構築**し、産学官の**結節点**として開放

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

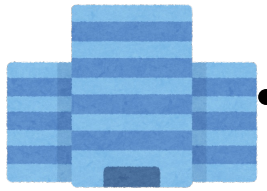
説明可能な国産脅威情報の生成・提供

高度SOC人材育成（Online自主学習＆OJT）

CYNEX ALLIANCE

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



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.

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, etc.

教育機関

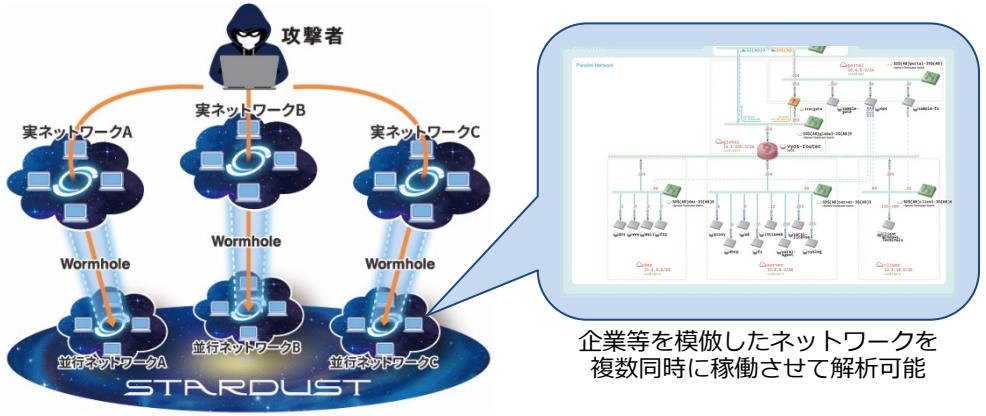
91組織参画中
(2025/2/1)

4つの “Co-Nexus” によるプロジェクト推進

参画組織数：40

Co-Nexus A (Accumulation & Analysis)

- 目的：STARDUSTを核とした共同解析と解析者コミュニティ形成



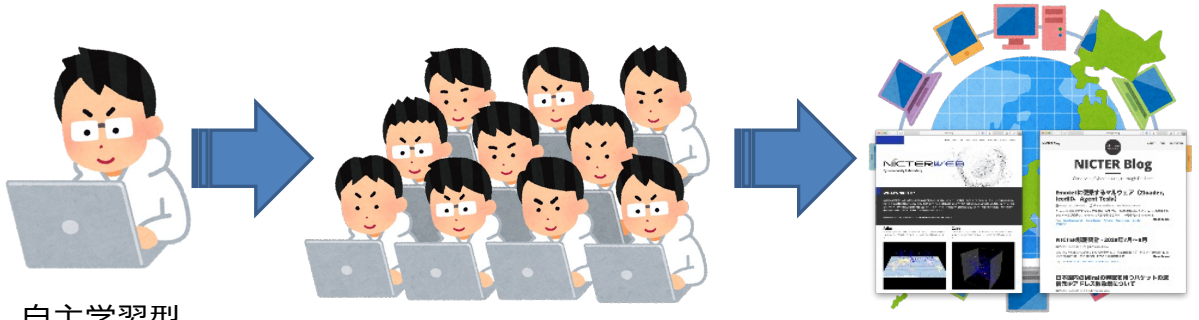
企業等を模倣したネットワークを
複数同時に稼働させて解析可能

サイバー攻撃誘引基盤STARDUST

参画組織数：18

Co-Nexus S (Security Operation & Sharing)

- 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

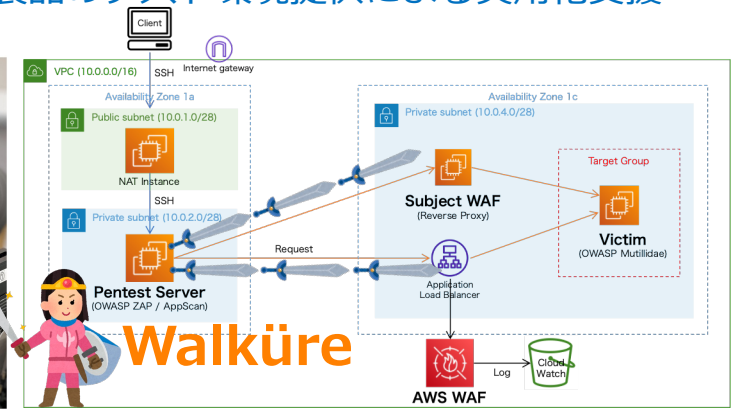
OJTでのSOC業務従事

国産脅威情報発信/提供

参画組織数：8

Co-Nexus E (Evaluation)

- 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



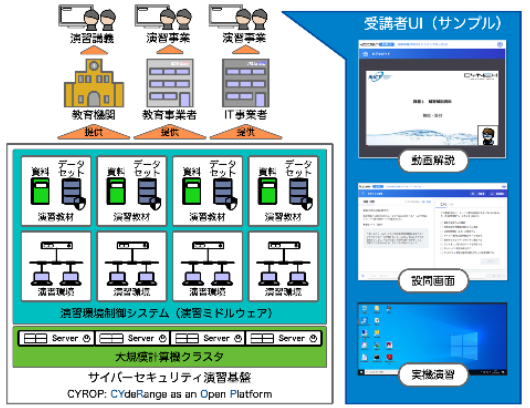
IoT機器検証環境

WAF製品検証環境

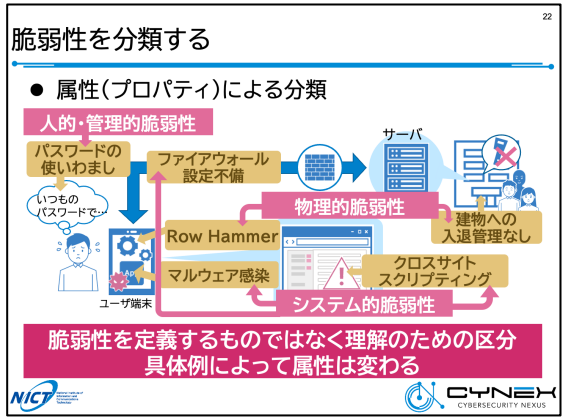
参画組織数：65

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

- 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



CYNEXオリジナル演習教材

AIセキュリティ研究センター

CREATE: Center for Research on AI security and Technology Evolution

USENIX Security 2024

- 2024年8月14〜16日@Philadelphia, US
- 参加者 > 1,000人
- 論文投稿数：2,276
- 採択数：417（採択率18.3%）
- 7パラレルセッション
- 合計セッション：98
- **機械学習（ML）関連セッション：17**
  - ✓ **うちLLM関連セッション：4**（昨年1発表のみ）
  - ✓ 他のセッションの論文も大多数は評価でMLを利用
- ドイツ『CISPA』旋風（採択論文22本）
- 中国系研究者大増（特にML関連研究）
- 韓国系研究者躍進（採択論文16本）
- 日本系研究者低迷（採択論文4本）
  - ✓ NICT+NTT、KDDI総合研究所
  - ✓ NTT Research（米国）、SONY AI（スイス）

https://www.usenix.org/conference/usenixsecurity24

プログラム全体像（1画像1セッション時間）

- **Day 1: Aug 14, 2024**


11:15 am–12:15 pm

1:45 pm–2:45 pm

3:15 pm–4:15 pm

4:30 pm–5:30 pm

- **Day 2: Aug 15, 2024**


9:00 am–10:15 am

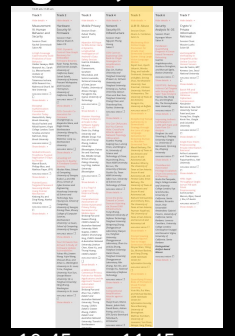
10:45 am–12:00 pm

1:30 pm–2:45 pm

3:15 pm–4:15 pm

4:30 pm–5:30 pm

- **Day 3: Aug 16, 2024**


9:00 am–10:15 am

10:45 am–11:45 pm

1:15 pm–2:15 pm

2:45 pm–3:45 pm

4:00 pm–5:00 pm

NICTにおける AI x Cybersecurity 研究（これまで）

ダークネット分析
- マルウェア活動の早期検知
- 広域スキャナのフィンガープリント

侵入検知
- セキュリティアラートの分析・削減
- 説明可能な侵入検知

Webセキュリティ
- Webのアクセスログ分析
- 説明可能なフィッシングサイト検知

マルウェア分析
- IoTマルウェア分析
- Androidアプリ分析

脅威情報分析
- ダークウェブからの脅威情報抽出
- 脆弱性情報の分析・アノテーション

CREATE：AIセキュリティ研究センター（2025年2月1日発足）

- **NICTの強みを活かした AI x Cybersecurity 研究へ**
  - ✓**AI for Security**
    - 例：セキュリティ・ビッグデータへのAIの適用による分析・オペレーションの自動化
  - ✓**Security for AI**
    - 例：生成AIの開発・利用に関するリスク評価、脅威分析、対策確立

- **日本の AI x Cybersecurity 研究の国際競争力強化**
  - ✓サイバーキュリティ分野は政策と研究開発が密接不可分
  - ✓**海外機関との研究連携や人材交流促進**

まとめ

●つづけていくこと

- ✓ サイバーセキュリティは進化する人間が相手
- ✓ いたちごっこが宿命づけられた研究分野
- ✓ 継続的な実データの観測・分析が最重要

●つないでいくこと

- ✓ 産学官・国内外をつなぐ結節点
- ✓ 次世代へと研究開発をつなぐ人材育成

➡ サイバーセキュリティ研究所 絶賛人材募集中！

https://csri.nict.go.jp