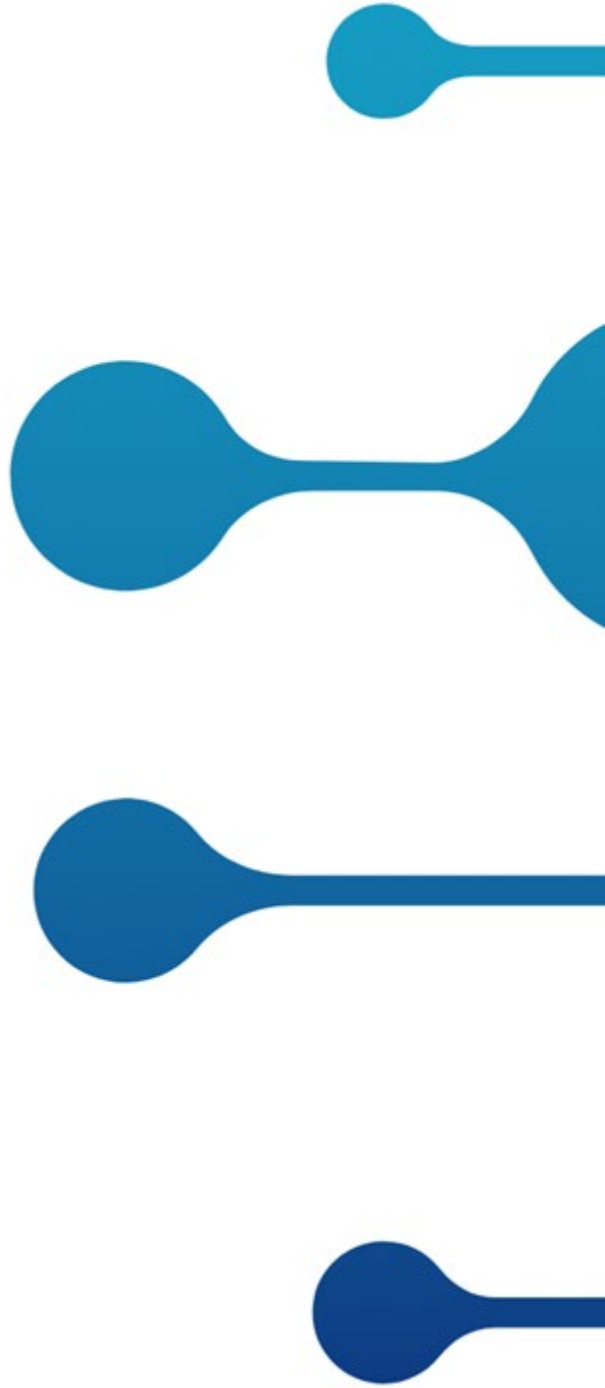
うまくいかなった話をしよう：なぜ、そしてこれから

@NICTサイバーセキュリティシンポジウム2026

笠間 貴弘

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
サイバーセキュリティ研究室



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

Who am I

笠間 貴弘（Takahiro KASAMA）、博士(工学)

サイバーセキュリティ研究所 サイバーセキュリティ研究室　室長

研究分野：サイバーセキュリティ（サイバー攻撃観測、マルウェア解析、IoTセキュリティ、etc.）

経歴：

- 横浜国立大学修了後、2011年にNICT入所。入所後はサイバーセキュリティ分野の研究開発を実施
- サイバーセキュリティ研究室以外では、NOTICEプロジェクトのPMやSecHackトレーナーなども歴任

委員等：

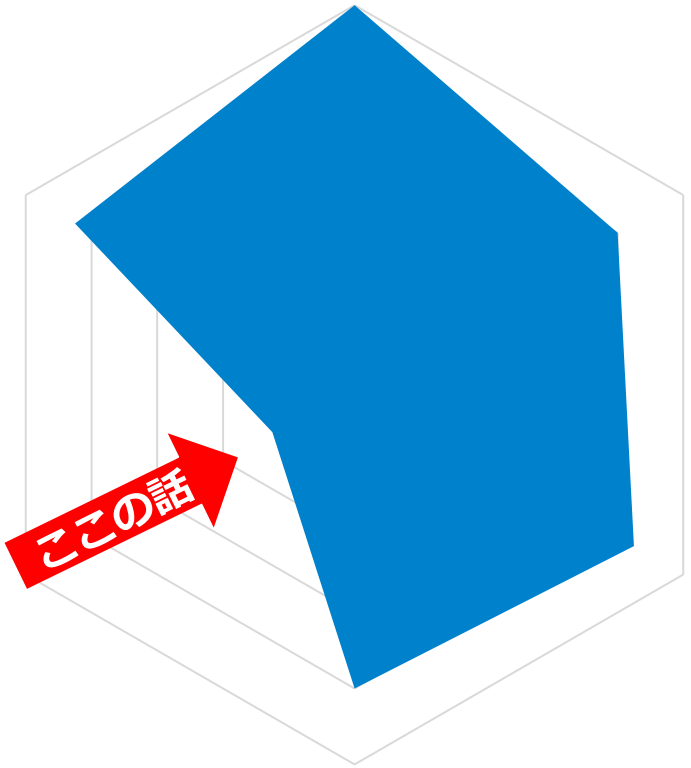
- JC-STAR 通信機器適合基準検討WG 主査/ネットワークカメラ適合基準検討 委員
- 情報処理学会 マルウェア対策研究人材育成ワークショップ(MWS) 委員
- 特許庁「令和7年度特許出願技術動向調査（サイバー攻撃検知技術）」委員、他

受賞等：

- 公益財団法人通信文化協会 第70回 前島密賞
- 電子通信普及財団賞 第40回 テレコム学際研究賞
- ISOC NDSS2019 Distinguished Paper Award, 他受賞多数

免責事項

- 本講演では第5期中長期における研究室の取組についてお話します。
- うまくいった話は全体的に軽く触れる程度です。
  論文や各種外部発表等をご参照ください。
- **うまくいかなった話をしようと思います。**
- 基本はあくまでも私個人の感想であり、
  組織としての統一見解ではありません。



イメージ図

第５期中長期のTimeline

個人

[2019/04] 研究マネージャー → [2022/04] 副室長 → **[2024/04] 室長**

[2019/01] NCOC兼務 → [2024/04] NCOC兼務解除

[2024/04] SecHack365トレーナー退任

サイバーセキュリティ研究室

（R3：CSL本務 53名）研究員16名＋技術員30名 → **（R7：CSL本務 42名）研究員9名＋技術員26名**

[2025/02] CREATE発足

[2021/04] CYNEX発足 → [2023/10] CYNEXアライアンス発足

[2021/04] NIRVANA改 IPv6版開発 → [2023/06] NIRVANA改 横断分析機能開発

[2022/06] CURE Enricher開発 → [2024/06] CURE Watcher開発

2021/04 | 2022/04 | 2023/04 | 2024/04 | 2025/04 | 2026/04

Top Tier 会議（計5本採択）

[2019/02] NDSS採択(Distinguished Paper) [w/ 横国大, TU Delft]

[2022/05] IEEE S&P採択 [w/ 横国大, TU Delft]

[2023/08] USENIX Security採択 [w/ UCL]

[2024/05] ACM CHI採択 [w/ NTT研]

[2024/08] USENIX Security採択 [w/ NTT研]

[2025/04] ACM CHI採択 [w/ 日立]

[2026/05] ACM CHI採択 [w/ NTT研]

NICT外の動き

[2021/07-09] 東京2020オリンピック・パラリンピック開催

[2023/05] 新型コロナウイルス感染症が5類に移行

[2021/09] サイバーセキュリティ戦略 → [2025/12] サイバーセキュリティ戦略

[2025/04-10] 大阪・関西万博開催

[2025/07] 国家サイバー統括室(NCO)発足

[2025/05] サイバー対処能力強化法成立

ChatGPTで生成

うまくいかなった①

業務拡大・新組織設立に伴う

研究者の減少

と採用実績は軟調

CYBERSECURITY Laboratory

一緒に研究開発するメンバーを沢山募集しています！

- **令和9年4月1日採用 パーマネント研究職/研究技術職**
  - ✓ 修士新卒型、ルーキー型（採用時に35歳未満）、女性対象、一般対象公募
- **令和9年4月1日採用 テニュアトラック研究員**
  - ✓ 修士新卒型、ルーキー型（採用時に35歳未満）、女性対象

博士進学支援は、あります!!

- **有期研究員/研究技術員/リサーチアシスタント（随時、次回は令和8年6月採用）**
  - ✓ **研究員８名**、**研究技術員８名**、**RA６名** **を公募中!!**

NICT採用ページ

https://www.nict.go.jp/employment/research_staff.html

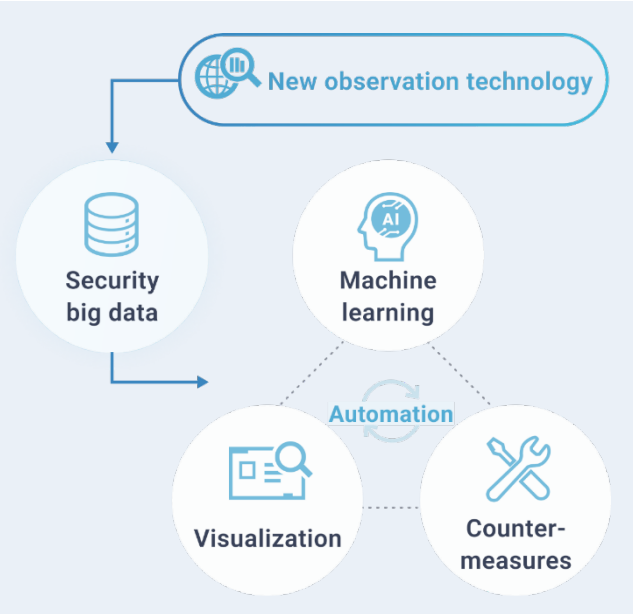
第５中長期における研究開発

CYBERSECURITY
Laboratory

第５期中長期計画（サイバーセキュリティ技術）

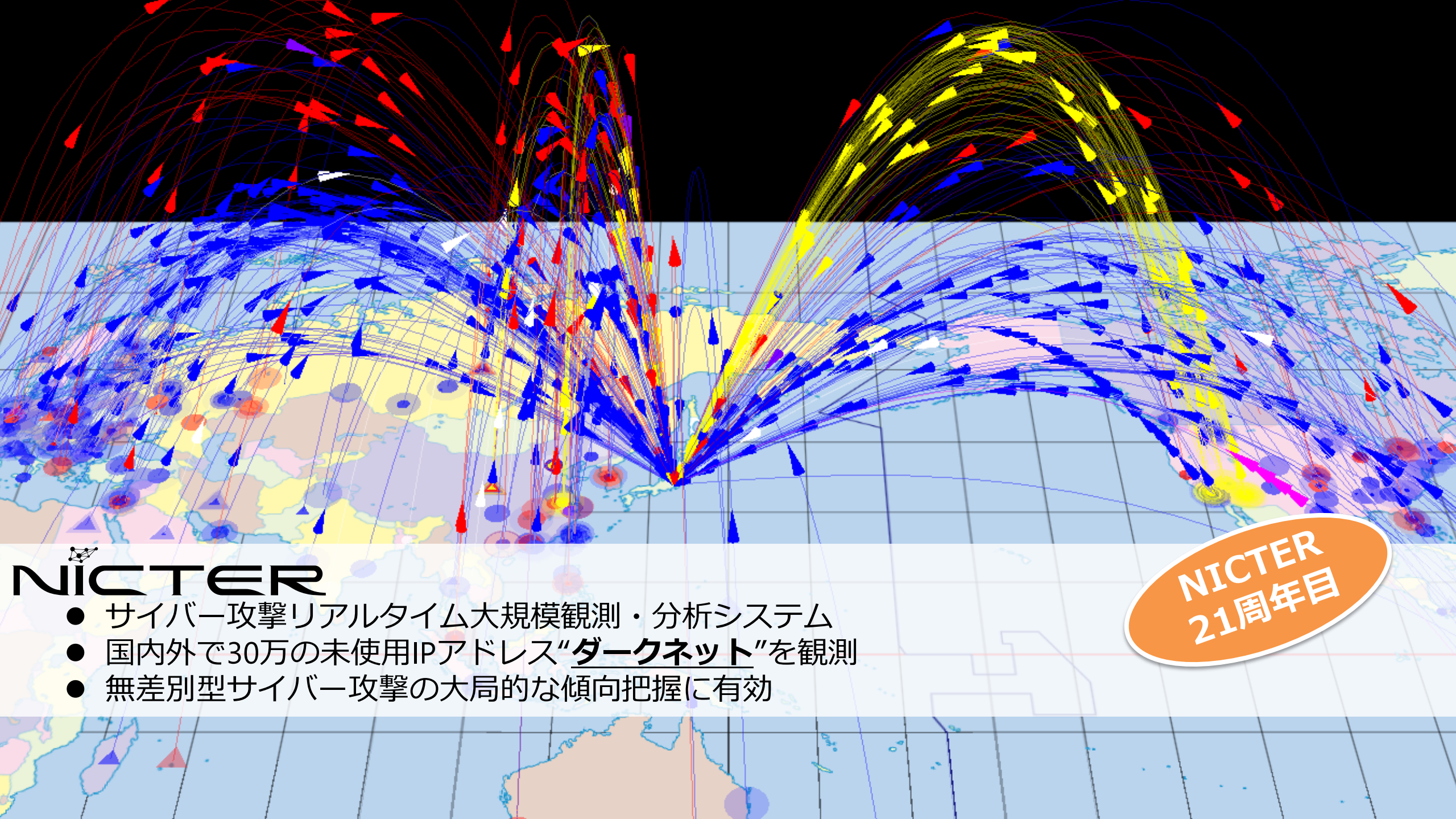
● データ駆動型サイバーセキュリティ技術

- ✓ 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
- ✓ **セキュリティキュレーション**研究
- ✓ **可視化エンジン**開発と**社会展開**, 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.



NICTER

- サイバー攻撃リアルタイム大規模観測・分析システム
- 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
21周年目

NICTER等の社会実装

- **国内26組織・海外10組織との連携の下でNICTER観測を継続**(from 2005)
- **解析チームの体制強化を通じて、積極的な外部情報提供・連携、対処を実施**
  - ✓ **新規脆弱性公表：21件**（CVE-2025-2492, CVE-2024-47001等）
  - ✓ BotConfやBlack Hat Europe、Underground Economy等の**産業系カンファレンスでの発表**
  - ✓ RapperBotの長期追跡＋DNSシンクホール　➡米国担当官との技術情報交換
- **東京2020大会及び大阪・関西万博のセキュリティ監視活動への貢献**
  - ✓ NICTER、DAEDALUS、AmpMon等によるイベントに関連した攻撃観測情報の共有

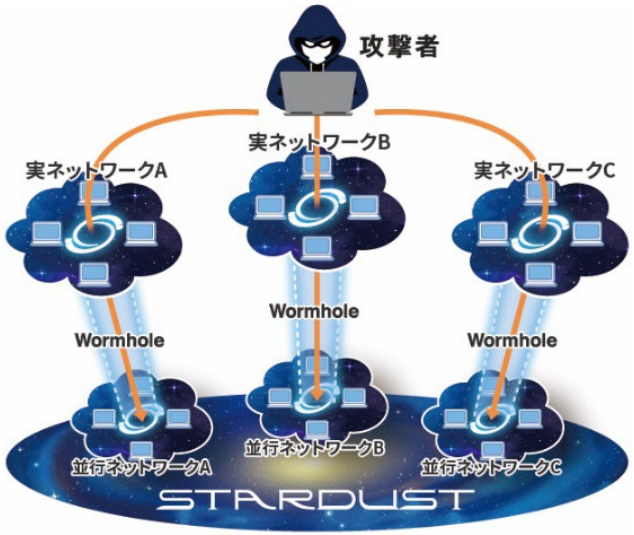
BotConf 2025 での発表

解析チームによる定常的な分析

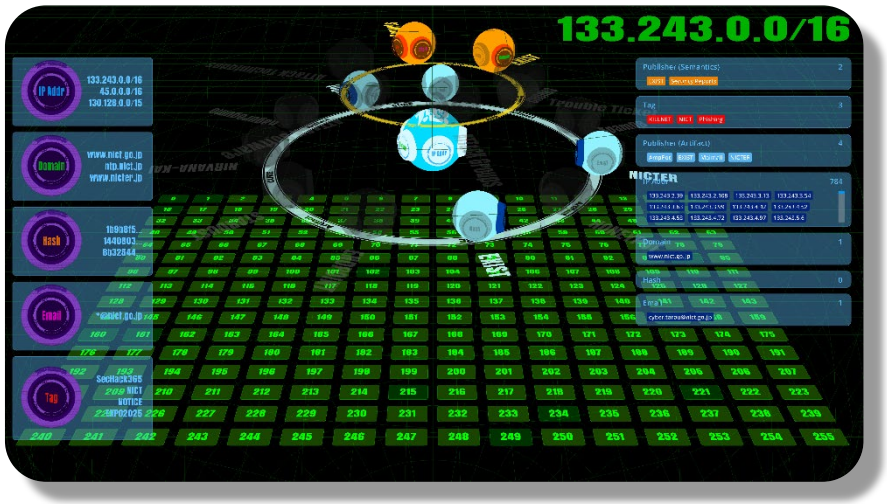

国交省管理の河川監視カメラの感染事例

各種研究開発システムの社会実装

- **STARDUSTの研究開発を継続し**(from 2012)**、CYNEXを通じて国内32組織に提供**
  - ✓ 模擬環境の動的構成変更ツール開発、各種解析補助機能開発、KVM版の開発、等々
- **攻撃観測情報のCUREへの統合を進め、 CYNEXを通じて国内31組織に提供**
  - ✓ 各Publisherのデータ投稿の整備、WebUI/WebAPI開発、カスタム通知機能開発、等々
- **各種可視化エンジンの技術移転と利活用、CYXROSSでの可視化・分析利用**



サイバー攻撃誘引基盤STARDUST

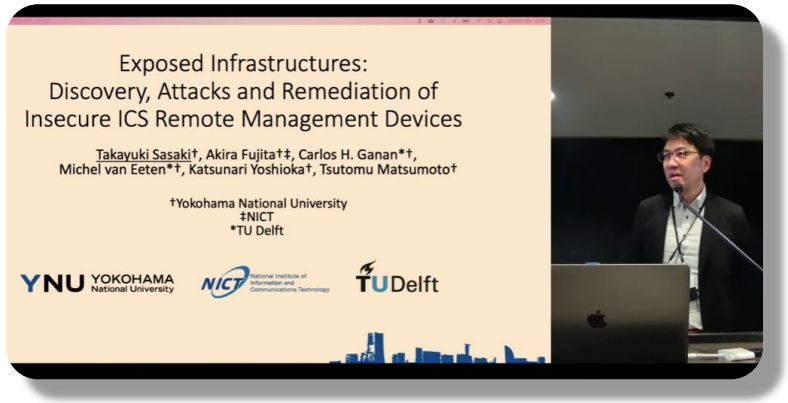


CURE通知機能(Watcher) 可視化

NIRVANA改の民間企業での活用

エマージングセキュリティ技術

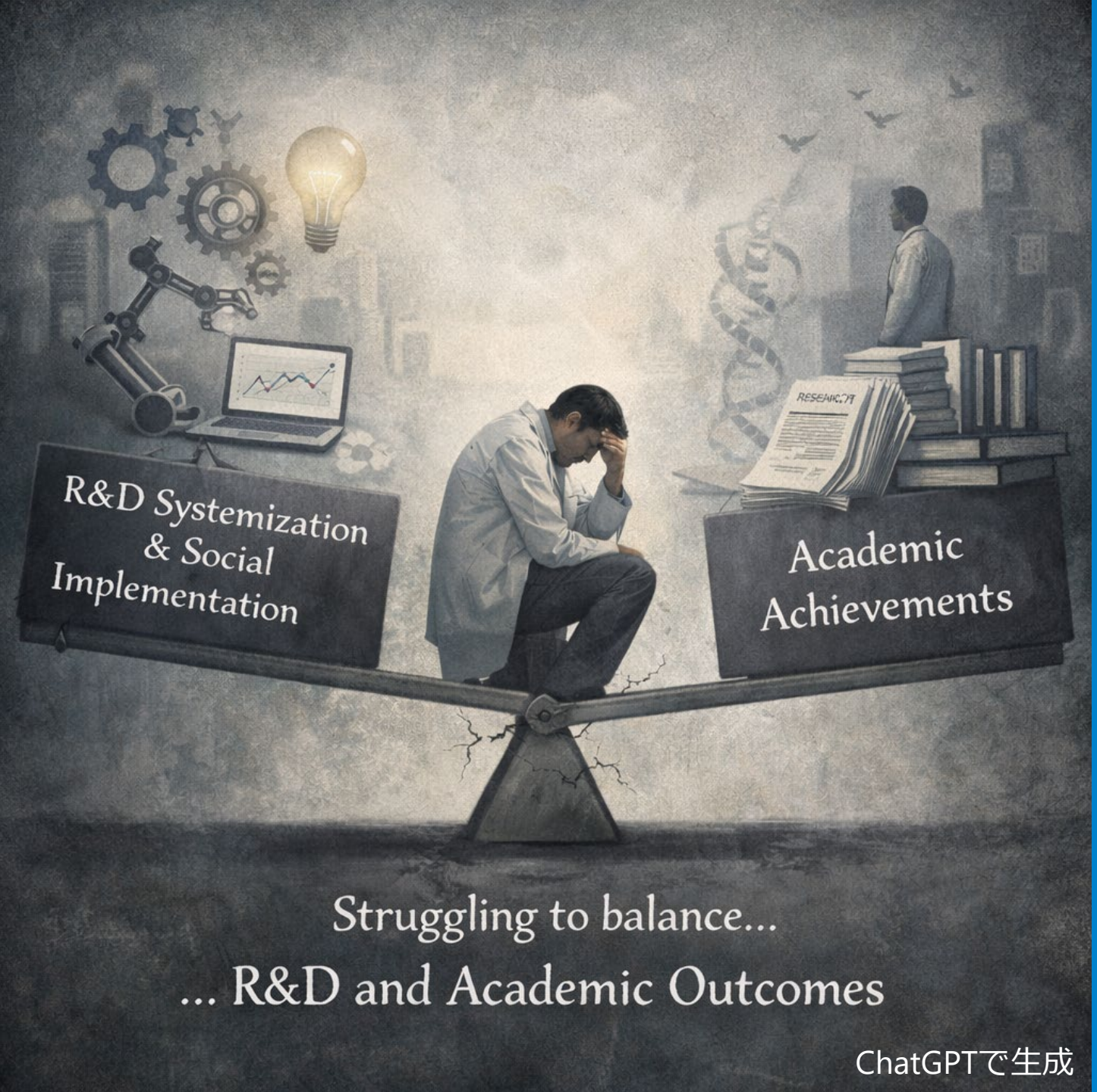
- **5Gセキュリティガイドライン第１版作成とITU-T SG17勧告化(X.1818)完了**
  - ✓ OSSを用いたセキュリティ検証環境の構築、脅威分析とセキュリティ検証、等々
- **サプライチェーンにおけるセキュリティ向上の研究開発**
  - ✓ ハードウェアトロジャン検知、ウェアラブルデバイス、SBOM、コネクテッドカー、等々
- **ユーザブルセキュリティの研究テーマで Tier 1 国際会議へ複数件が採択**
  - ✓ 脆弱なICS管理システムの検知と通知 (**IEEE S&P '22**)
  - ✓ IoTセキュリティ対策実施のインセンティブと課題 (**USENIX Sec. '23**)
  - ✓ ユーザ調査型セキュリティ・プライバシー研究における WEIRD 偏重指摘 (**USENIX Sec. '24**)



YNU、TU Delft (蘭)との共同研究 (IEEE S&P '22)

UCL (英)との共同研究 (USENIX Sec. '23)

NTTとの共同研究 (USENIX Sec. '24)



ChatGPTで生成

うまくいかなった②

システム化・社会実装と

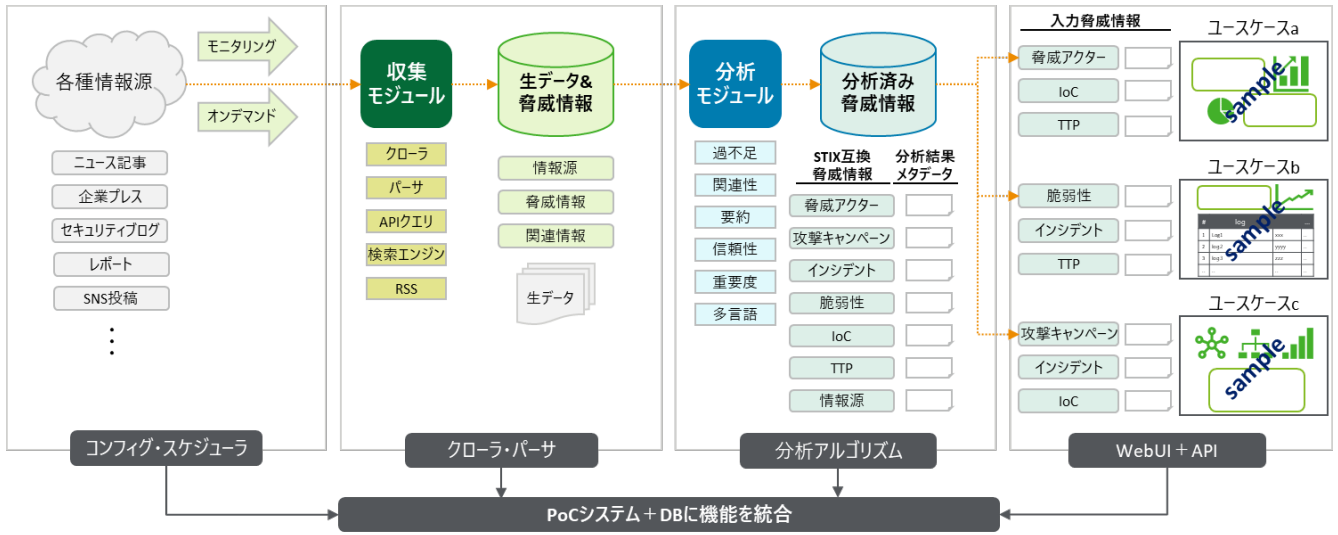
論文成果の両立

の壁は高かった

CYBERSECURITY Laboratory

セキュリティキュレーション技術

- **2022年度からサイバーセキュリティ研究室の新規テーマとして計画に追加**
  - ✓ セキュリティ記事の自動収集、固有表現の辞書整備、文書要約モデルの構築、等々に着手
- **生成AIの登場と日々加速するゲームチェンジ・ラッシュ**
  - ✓ 2022年11月 ChatGPT-3.5 ➡ 2023年 ChatGPT-4 ➡ 2025年 Deep Research ➡・・・
- **生成AIを活用した脅威情報収集・各種分析と多言語対応を中心に軌道修正**



複数言語で発信される脅威情報の自動収集・分析システムの開発

生成AIエンジン・サービスの隆盛

USENIX Security 2025

- 2025年8月13〜15日@Seattle, US
- 参加者 > 1,000人
- 論文投稿数：2,385件
- 採択数：407件（採択率17.1%）
- 5パラレルセッション
- 合計セッション：55
- **機械学習（ML）/LLM関連セッション：11**
  - ✓ ML/LLM関連論文：100件
  - ✓ 他セッションでのML/LLM関連論文：90件

➡ 46.7%がML/LLM関連論文

https://www.usenix.org/conference/usenixsecurity25

プログラム全体像（1画像1セッション時間）

- **Day 1: Aug 13, 2025**


10:00 am–11:30 pm

1:00 pm–2:30 pm

3:00 pm–4:30 pm

- **Day 2: Aug 14, 2025**


9:00 am–10:30 am

11:00 am–12:30 pm

2:00 pm–3:30 pm

4:00 pm–5:30 pm

- **Day 3: Aug 15, 2025**


9:00 am–10:30 am

11:00 am–12:30 pm

2:00 pm–3:30 pm

4:00 pm–5:30 pm

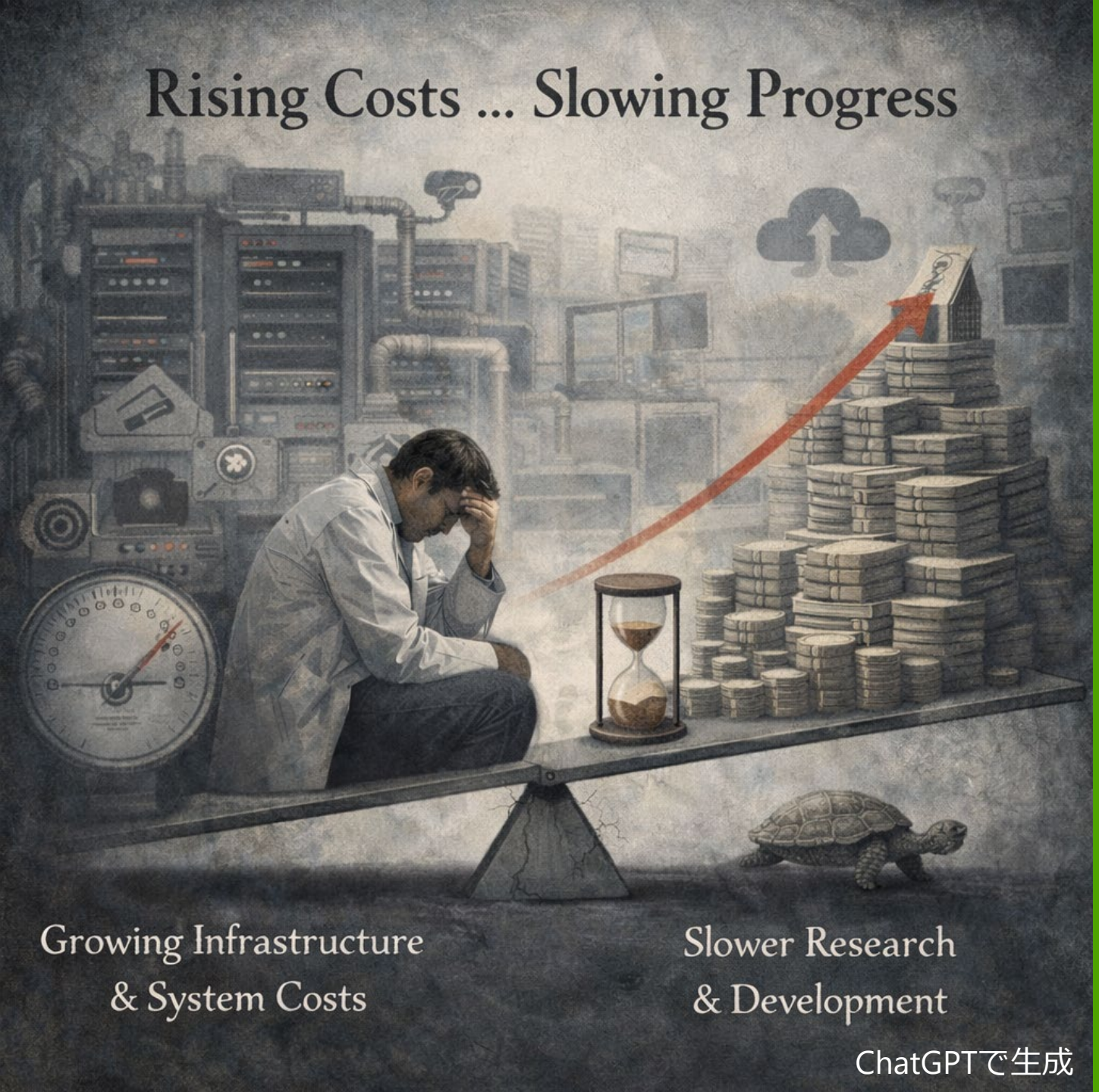
うまくいかなった③

急速に進化する

生成AIの利活用

は周回遅れ

CYBERSECURITY
Laboratory



うまくいかなった④

拡大するインフラ・システムの

維持管理コスト増

によるスピード感の喪失

CYBERSECURITY
Laboratory

ChatGPTで生成

うまくいかなった⑤

継続テーマと新規テーマ

他律性と自律性

答えは見えない

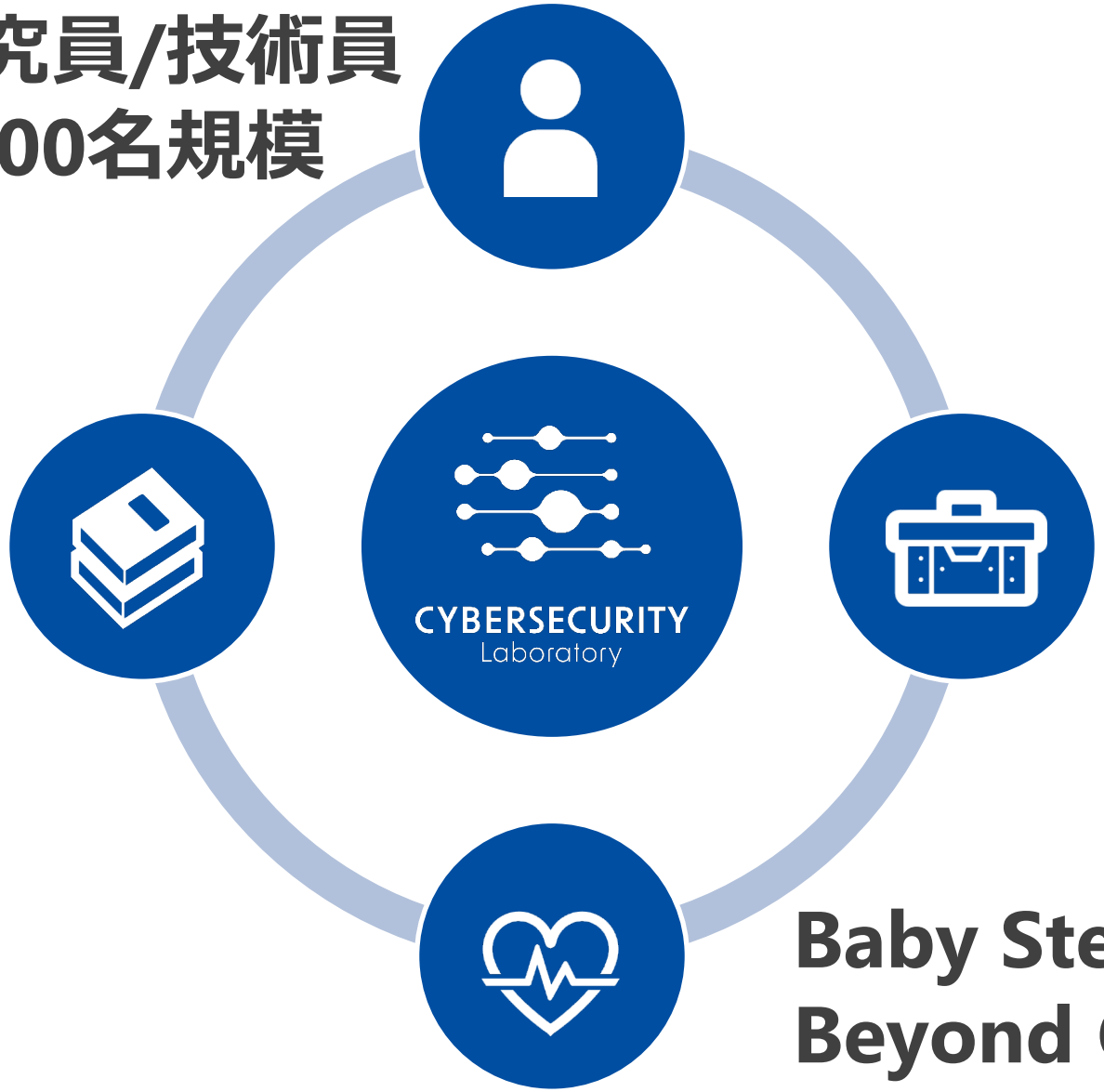
CYBERSECURITY Laboratory

第６期中長期計画に向けて

サイバーセキュリティ研究室の次の５年間

研究員/技術員
100名規模

Tier 1 国際会議
採択常連組織



解析基盤の整備
オープン化

Baby Steps,
Beyond Our Passion

サイバーセキュリティ研究室の
次の５年間にご期待ください。

Baby Steps,
Beyond Our Passion

CSL HP
https://csl.nict.go.jp/en

NICTERWEB
https://www.nicter.jp/en/

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