3. 人材・技術に係るエコシステム形成　関係

官民共通の「人材フレームワーク」の策定（概要）

- 諸外国ではサイバーセキュリティ人材について、職種（ロール）ごとにT（タスク）K（知識）S（スキル）を定義した人材フレームワークを整備し、人材育成に活用。
- 我が国の実情に沿った官民共通のサイバーセキュリティ人材フレームワークを、諸外国の事例も参考にしつつ策定し、官民一体となって効率的・効果的に人材確保・育成を推進。

✓ 諸外国のフレームワークにおける職種（ロール）数の比較

- 細分化することできめ細やかな人材定義ができる一方、活用場面が限定的な職種も生じる
- 雇用の流動円滑化やミスマッチを防ぐ観点からも、代表的な人材像の定義によるスキルの可視化が必要

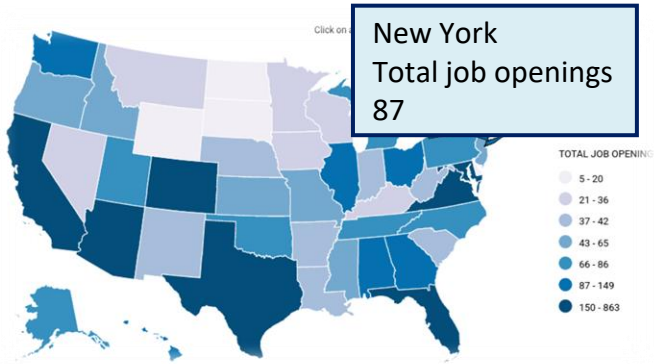
国等	策定年	職種数	LV分
米国	2017年初版、2024年改訂、2025年改訂	41	―
欧州	2022年公開	12	有
カナダ	2023年公開	22	―
豪州	2019年初版、2020年改訂	9	有

✓ フレームワークの活用例（米国）

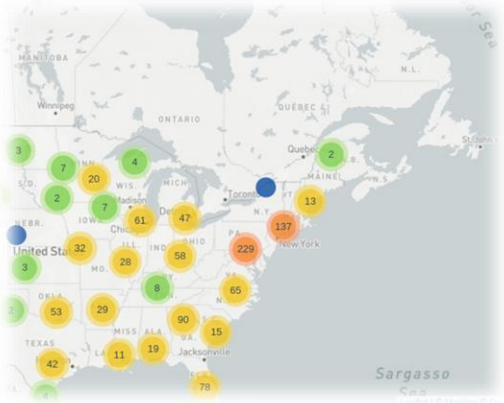
- 米国のCyberseekでは、NICEフレームワークに沿ったサイバーセキュリティ求人情報や教育サービスの検索が可能

（Cyberseek公式サイトにおける表示例）

求人数・採用要件（資格）の可視化



求人数を州単位でマップ表示



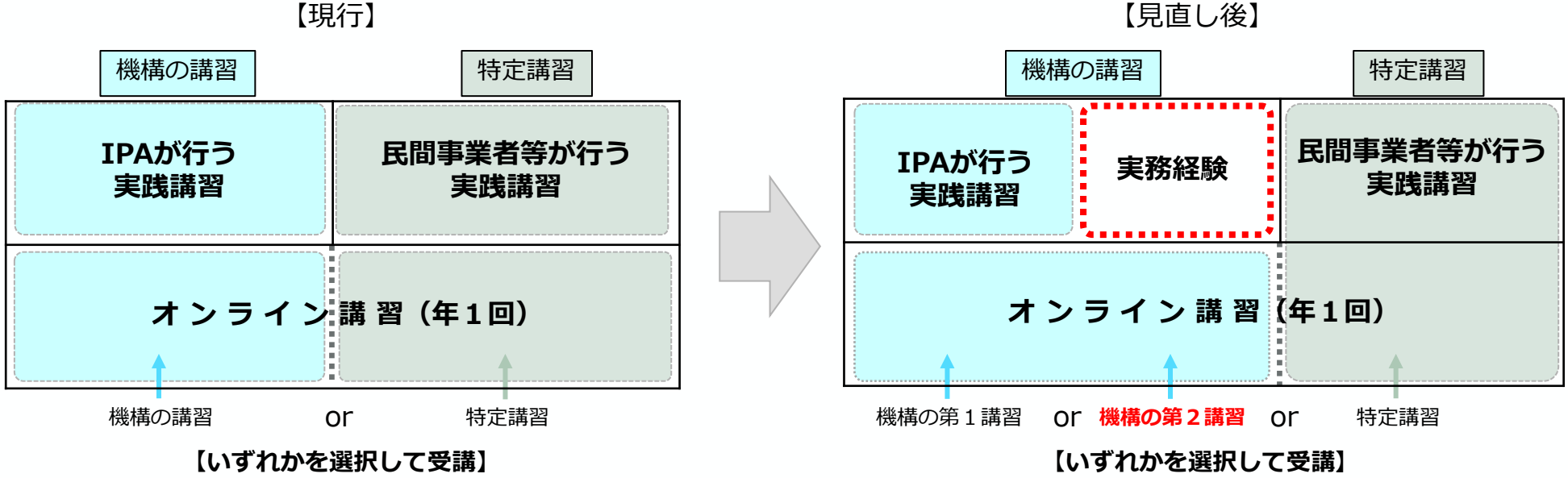
プロバイダー（研修事業者・大学等提供者）ごとにトレーニングセンター等の教育機関を地図上に可視化

（米）cyberseek：https://www.cyberseek.org/

実務経験者に対する講習制度創設の背景

- サイバーセキュリティ分野で必要とされる知識が技術の進歩により変化している中、**情報処理安全確保支援士には、サイバーセキュリティの専門家としてその知識や技能を最新の状態としておくために、講習受講が課せられている。**
- 一方、情報処理安全確保支援士の中には、**実践講習で得られる知識・技能と同等以上の知識・技能を、企業のサイバーセキュリティ対策の支援等の実務を通じて得られるケース**がある。
- また、更新制度が実施されている中で、**実務から遠のいている情報処理安全確保支援士を実務に向かわせるインセンティブを設定**することが、情報処理安全確保支援士の一層の活用促進、ひいては事業者のサイバーセキュリティ対策向上に資する。

このような講習制度や情報処理安全確保支援士の実務の実態を踏まえ、**実務経験から、講習から習得できる知識・技能と同等以上の知識・技能を得ている情報処理安全確保支援士に対して、受講すべき講習をオンライン講習のみとする、新たな講習制度を創設。**



実務経験者に対する講習制度の概要

実務経験者に対する講習制度とは、**下表の実務経験を積んでいる情報処理安全確保支援士に向けた新たな講習制度**であり、具体的には、当該情報処理安全確保支援士が受講する講習をオンライン講習のみとするもの。

実践講習として求める要素

・ITスキル標準レベル４相当（一つまたは複数の専門を獲得したプロフェッショナルとして、専門スキルを駆使し、業務上の課題の発見と解決をリードするレベル、プロフェッショナルとして求められる、経験の知識化とその応用（後進育成）に貢献するレベル）

・情報処理安全確保支援士試験の出題分野の内容を含む

～ 特定講習（※）募集等要領（抜粋）～　　（※民間事業者等が行う実践講習部分を指す）
・・・特定講習は「ITスキル標準レベル４相当」とし・・・登録セキスペの知識・技能の継続的な維持・向上を図り、実践的な活用力を修得 できるものであることが必要なため、特定講習が対象とする科目は、「情報処理安全確保支援士試験」の出題分野の内容を含むこと・・・

実務経験者に対する受講制度の対象となる実務の方向性

○ITスキル標準レベル４に相当する、情報処理安全確保支援士試験の出題科目に該当するもの
○上記以外で、実務経験者に対する講習制度の対象とすることが望ましいもの
から、IPA有識者検討会での議論を踏まえて以下のとおり決定

○ITスキル標準レベル４相当の情報処理安全確保支援士試験の出題科目に該当するもの

対象業務	情報処理安全確保支援士試験出題科目の該当項目
セキュリティ監査／システム監査 セキュリティ統括	1．情報セキュリティマネジメントの推進又は支援に関すること
デジタルシステムストラテジー デジタルシステムアーキテクチャ デジタルプロダクト開発 デジタルプロダクト運用	2．情報システムの企画・設計・開発・運用でのセキュリティ確保の推進又は支援に関すること 3．情報及び情報システムの利用におけるセキュリティ対策の適用の推進又は支援に関すること
脆弱性診断・ペネトレーションテスト セキュリティ監視・運用 セキュリティ調査分析・研究開発	2．情報システムの企画・設計・開発・運用でのセキュリティ確保の推進又は支援に関すること 3．情報及び情報システムの利用におけるセキュリティ対策の適用の推進又は支援に関すること 4．情報セキュリティインシデント管理の推進又は支援に関すること
※いずれも、一定期間（６か月/１年）の従事期間を満たした場合に限る。	

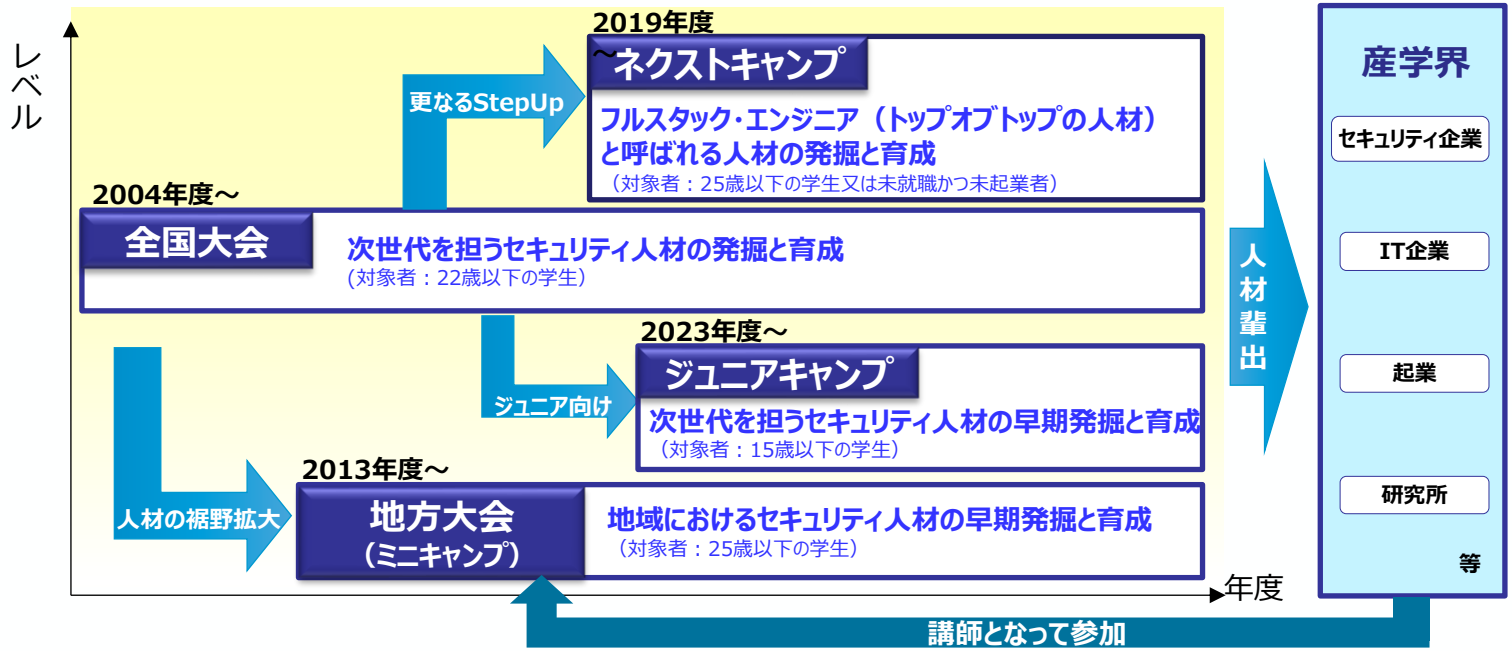
○左表以外で実務経験者に対する講習制度の対象とするもの

対象業務	採用理由
セキュリティ経営 デジタル経営	特定講習 募集等要項(*) 別表１において講習の対象外とされる「経営層」について、ITSS＋（セキュリティ領域）分野に従い、左表の従事期間を満たすことで実践講習と同等の役割があると判断
情報セキュリティ規程の整備 情報資産の洗い出しとリスク分析 クラウドサービスの安全利用 セキュリティインシデント対応 従業員向け情報セキュリティ教育	「中小企業向けサイバーセキュリティ対策支援者リスト」に掲載される者が、左記指導テーマに基づく支援業務として、３回以上の中小企業への支援実績がある場合に限り、実践講習と同等と判断
IPAまたは民間事業者等が行う実践講習の講師	講師として２回以上登壇した場合に限り、実践講習と同等と判断

*出典： 経済産業省「情報処理安全確保支援士特定講習」募集等要領 別表１ https://www.meti.go.jp/policy/it_policy/jinzai/bosyuu250922.pdf

セキュリティ・キャンプ

- **若年層のセキュリティ人材発掘の裾野を拡大し、世界に通用するトップクラスの人材を育成・発掘する**ため、IPAとセキュリティ・キャンプ協議会が開催。計**約1,300名**が修了。
※地方大会（ミニキャンプ）を含めると計約3,100名が修了。
- 今後、裾野の拡大に向けた**新たなキャンプの実施**と、修了生の知見研鑽や活躍状況の共有等を目的とした**コミュニティを整備**していく。



今後の方向性

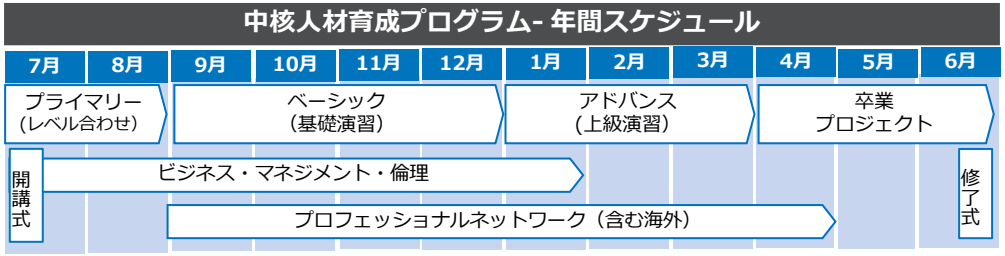
- 単純拡大ではなく、裾野を広げる観点から、特定領域（AI等）の専門性と高度なサイバーセキュリティの知見の双方を兼ね備えた人材の育成を目的とする新たなキャンプを実施。
- 修了生の継続的な知見研鑽・社会還元・活躍状況共有等を目的としたコミュニティを整備。

IPA産業サイバーセキュリティセンター（ICSCoE） ※2017年4月設置

- 社会インフラ・産業基盤における防護力の強化のため、OT(制御技術）とIT（情報技術）の知見を結集させた**世界レベルのサイバーセキュリティ対策の中核拠点**として、IPA内に発足。
- ICSCoEでは世界的にも限られている、制御系セキュリティにも精通する講師を招き、テクノロジー、マネジメント、ビジネス分野を総合的に学ぶ１年の集中トレーニング等を実施。

□　１年を通じた集中トレーニング「中核人材育成プログラム」

□　電力、石油、ガス、化学、自動車、鉄道分野等の企業から1年間派遣
（第1期：76人、第2期：83人、第3期：69人、第4期：46人、第5期：48人、第6期：48人、第7期：65人、第８期：57人、第９期：55人）



- IT系・制御系に精通した専門人材の育成
- 模擬プラントを用いた対策立案
- 実際の制御システムの安全性・信頼性検証等
- 攻撃情報の調査・分析

現場を指揮・指導するリーダーを育成

□　米・英・仏等の海外とも協調したトレーニングを実施

➢ DHSが開催する高度なサイバーセキュリティトレーニングである301演習への参加

➢ 政府機関、産業界等のセキュリティ専門家との意見交換や研究機関の施設見学等を実施

実践的・先進的サイバーセキュリティ人材の育成

○ 情報通信研究機構（NICT）の「ナショナルサイバートレーニングセンター」に大規模な演習環境を整備し、実践的な演習プログラムの提供を通じて、**巧妙化・高度化するサイバー攻撃に対応できるサイバーセキュリティ人材の育成を支援**

CYDER（サイダー）

国機関・地方公共団体・独立行政法人等を対象とした「実践的サイバー防御演習」

全国の会場で**年間計100回**、**計3,000名規模**で実施
2017年度の開始以降、2024年度までに、延べ**25,000名超**が受講

SecHack365（セックハック サンロクゴ）

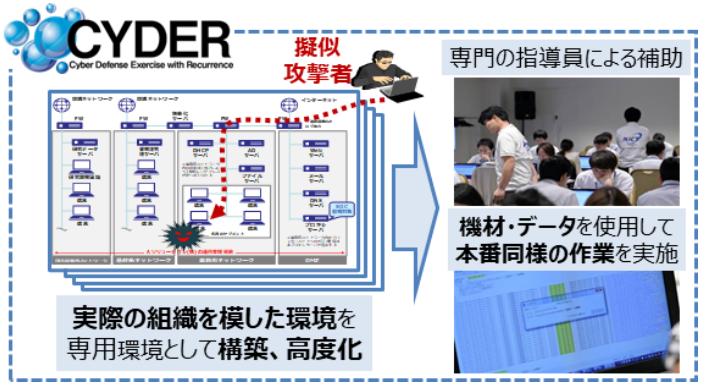
25歳以下の若手人材を対象とした「セキュリティイノベーター育成プログラム」

年間40名程度の受講者を選抜し、**１年間のトレーニング**コースを実施
2017年度の開始以降、2024年度までに、**計300名超が修了**

CYROP（サイロップ）

分野別実践演習の開発・実施基盤「CYROP」

サイバーセキュリティ演習に必要となる基盤（仮想環境、演習教材等）を大学、民間企業等へ開放
2026年１月時点で86組織が参画、利用



実践的サイバー防御演習
CYDER

セキュリティイノベーター育成プログラム
SecHack365

分野別実践演習の開発・実施基盤
CYROP

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

○ 情報通信研究機構（NICT）において、平成29年度から、**国の機関、指定法人、独立行政法人、地方公共団体**及び**重要インフラ事業者等**の情報システム担当者等を対象とした体験型の**実践的サイバー防御演習「CYDER」**（サイダー）を実施

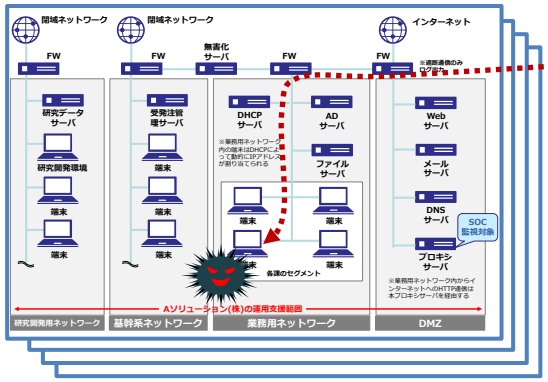
○ 受講者は、**チーム単位で演習に参加。組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴って、**外部のセキュリティ事業者の支援を受けることを前提としてサイバー攻撃によるインシデントの検知から対応、報告、回復までの**一連の対処方法を体験**

○ **全都道府県**において、年間**100回**の計**3,000名規模**で実施(集合コース)。令和６年度は106回の**4,225名**が受講

演習のイメージ

我が国唯一の情報通信に関する公的研究機関である**NICTが有する最新のサイバー攻撃情報を活用**し、実際に起こりうるサイバー攻撃事例を再現した**最新の演習シナリオ**を用意。

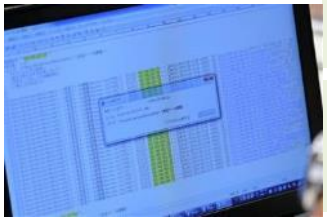
北陸StarBED技術センターの大規模高性能サーバ群を活用



擬似攻撃者

企業・自治体の**社内LANや端末を再現**した環境で演習を実施

受講チームごとに独立した演習環境を**構築**



専門指導員による補助

チーム内での議論を通じた相互理解

本番同様のデータを使用した演習

インシデント（事案）対処能力の向上

令和７年度の実施状況

コース名		実施方法	レベル	受講想定者（習得内容）	受講想定組織	実施地	実施回数	実施期間
CYDER	A	集合形式	初級	システムに携わり始めた者 (事案発生時の対応の流れ)	全組織共通	47都道府県	78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８地域	10回	10月～11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 (初動分析を含む主体的な事案対応)	全組織共通	東京・大阪	５回	11月～翌年１月
プレCYDER		オンライン形式	-	全ての情報システム担当者 (最低限必要となる知識の習得と最新化)	全組織共通	（受講者職場等）	-	1期：５月～８月 2期：９月～11月 3期：11月～翌年１月

分野別実践演習の開発・実施基盤「CYROP」(CYber Range Open Platform)

○ 情報通信研究機構（NICT）の有する**人材育成ノウハウを民間企業・教育機関等に横展開**するため、各組織が**実践的演習を容易に開発・実施可能とする演習基盤「CYROP」**（サイロップ）※を構築。令和５年10月から提供開始

○ 「CYROP」では、サイバーセキュリティ演習の実施に必要となる**演習環境・演習教材を提供**。演習教材をカスタマイズし、自前で講師を用意することで、**分野に応じた演習を容易に実施可能**

※NICT内に設置されたサイバーセキュリティに関する産学官の結節点『**CYNEX（サイネックス）**』の取組の一つとして提供

民間企業の自社向け演習、
大学・高専での講義等で活用

CYDERと同等の演習基盤を
NICT以外の組織においても
活用可能とするサイバーセキュリティ
演習基盤を開発し、
CYROPにおいて提供

分野別実践演習

〇〇向け演習　〇〇向け演習　・・・

講師・追加教材
※演習実施者が自前で用意

演習基盤

演習教材
（資料・データセット）

仮想演習環境

大規模計算機
クラスタ

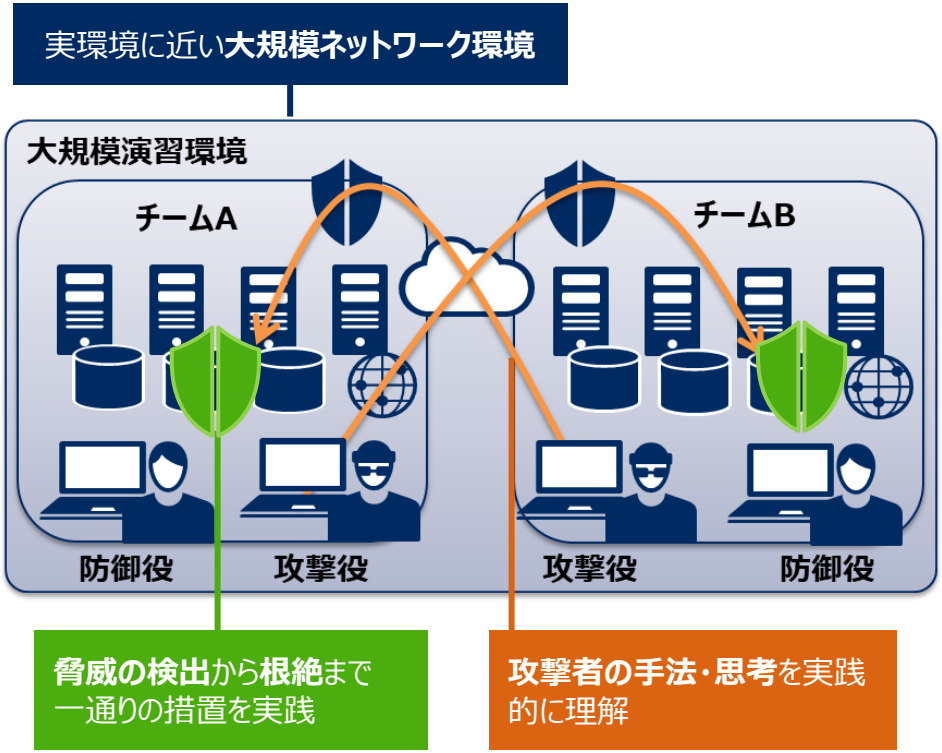
CYDERの教材のほか、
CYROP独自教材も開発

利用者は、既存の教材を編集・
カスタマイズして利用することも可能

高度演習基盤の構築

○ サイバー攻撃による被害を未然に防ぐことができる、高度な対処能力を有する人材を育成するため、情報通信研究機構（NICT）において高度演習基盤を構築し、政府機関・重要インフラ企業等の中核的な対処人材の育成を推進

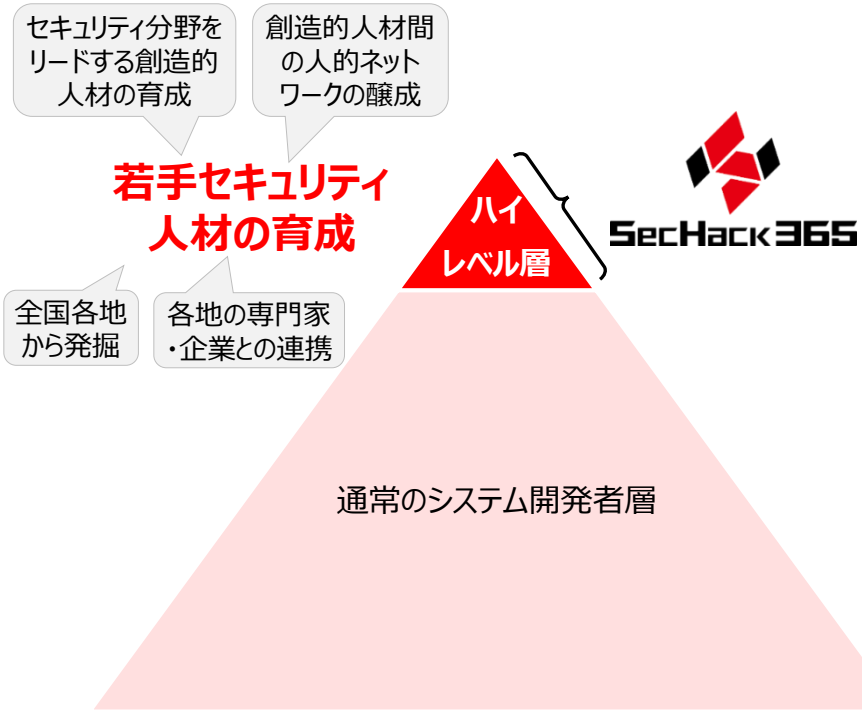
○ 令和７年度補正事業により構築を開始、令和９年度後半からの運用開始を想定。あわせて今後、必要な拡張を継続的に実施



- 現実の攻撃・防御と類似した状況を再現可能な大規模ネットワーク演習基盤を新たに構築
- 潜伏している脅威の探索・検出から根絶まで一連の対処を、攻撃者の視座をもって実践
- 演習を通じて官民双方で必要な高度対処人材の育成を推進、我が国全体のサイバー対処能力を強化

セキュリティイノベーター育成プログラム「SecHack365」（セックハック サンロクゴ）

- ○ 日本国内に居住する**25歳以下の若手ICT人材を対象**として、新たなセキュリティ対処技術を生み出しうる**最先端のセキュリティ人材（セキュリティイノベーター）**を育成
- ○ NICTの持つサイバーセキュリティの研究資産を活用し、実際のサイバー攻撃関連データに基づいたセキュリティ技術の研究・開発を、**第一線で活躍する研究者・技術者が１年かけて継続的かつ本格的に指導**（年間約40名程度、合計300名超が修了）
- ○ 受講者は、NICTの有する遠隔開発環境を活用し、年中どこからでも遠隔開発実習が可能。また、集合イベントとして、座学講座（研究倫理）やハッカソン等を実施



年６回程度の集合研修（座学講座等）、
成果発表会・OB交流会＋通年の遠隔開発実習
の組合せによる総合的な人材育成プログラム

数理・データサイエンス・AI教育プログラム認定制度

背景・目標

✓デジタル時代の「読み・書き・そろばん」である「数理・データサイエンス・AI」の基礎などの必要な力を全ての国民が育み、あらゆる分野で人材が活躍する環境を高等教育段階においても構築する必要がある

✓「AI戦略2019」や「デジタル田園都市国家構想総合戦略」における育成目標

主な取組

1．「数理・データサイエンス・AI教育強化拠点コンソーシアム」による普及・展開活動
2．「数理・データサイエンス・AI教育プログラム認定制度」による各大学等の取組推進

認定制度の概要

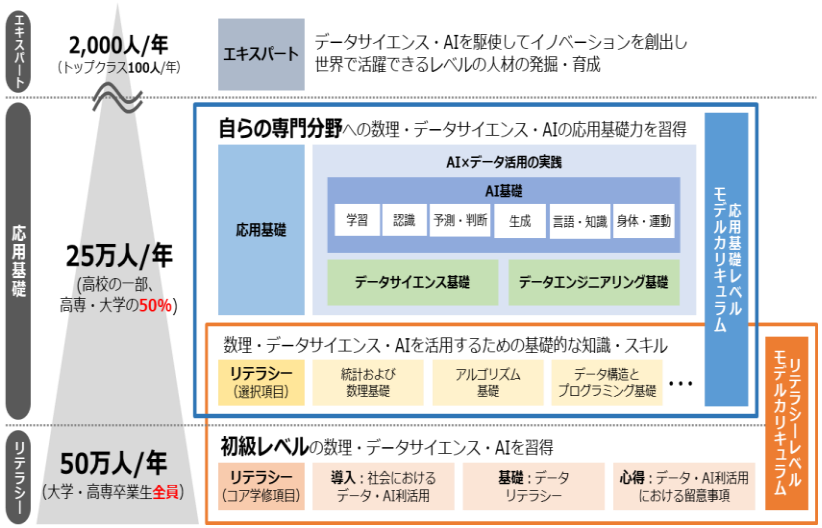
CLICK https://www.mext.go.jp/a_menu/koutou/suuri_datascience_ai/00001.htm

大学・高等専門学校の数理・データサイエンス・AI教育に関する正規課程教育のうち、一定の要件を満たした**優れた教育プログラムを政府が認定**し、教育を推進。
文理を問わず多くの大学・高専が数理・データサイエンス・AI教育を学ぶことができる**教育体制の構築・実施に取り組むことを後押し**！

政府 → 大学 → 数理・データサイエンス・AIの素養のある学生を輩出 → 企業・行政等

・相互連携により社会のニーズに応える
・企業等からの実データ提供などの連携により教育を高度化

数理・データサイエンス・AI（リテラシーレベル／応用基礎レベル）の位置づけ



応用基礎レベル（2022年度～）

MDASH Advanced Literacy

数理・データサイエンス・AIを活用して課題を解決するための実践的な能力を育成

認定数：366件（2025年8月時点）
※1学年あたりの受講可能な学生数：約25万人
（2025年度目標：25万人/年）

リテラシーレベル（2021年度～）

MDASH Literacy

学生の数理・データサイエンス・AIへの関心を高め、適切に理解し活用する基礎的な能力を育成

認定数：592件（2025年8月時点）
※1学年あたりの受講可能な学生数：約55万人
（2025年度目標：50万人/年）

数理・データサイエンス・AI教育強化拠点コンソーシアム
http://www.mi.u-tokyo.ac.jp/consortium/

全国の大学等で教育プログラムを展開させるためのコンソーシアム活動を実施
- モデルカリキュラムの策定や教材等の開発・普及
- 全国9ブロックで好事例などを普及・展開するためのシンポジウムやワークショップを開催　等

戦略的創造研究推進事業

情報通信科学・イノベーション基盤創出（CRONOS）

※CRONOS: Cutting-edge Research and Development on Information & Communication Sciences

背景・課題

生成AIサービスの急速な流行や、社会インフラのIoT化、サイバー攻撃の高度化・激化等、ICTの進展は**大きな社会変革を起こす鍵**であり、将来の我が国の帰趨を握る**革新的なICTの創出・進化を実現するための研究開発**及び**高度研究人材の育成**を強力に推進することが求められている。ICT分野は技術進展が速く、また、基礎研究の成果が社会サービスに直結することもあるため、**基礎研究と応用研究の垣根を超え、革新的・機動的な研究開発を実施し社会変革を目指す新たな研究スキーム**が必要となる。

経済財政運営と改革の基本方針2025（令和７年６月13日閣議決定）

我が国の国力に直結する科学技術・イノベーション力を強化し、国際競争を勝ち抜くため、官民が連携して大胆な投資を行い、多様で豊富な「知」を生み出すエコシステムを活性化する。このため、社会課題解決の原動力となるＡＩ、量子、フュージョンエネルギー、マテリアル、バイオ、半導体、次世代情報通信基盤（Beyond ５Ｇ）、健康・医療等について、分野をまたいだ技術融合による研究開発・社会実装を一気通貫で推進する。

事業概要

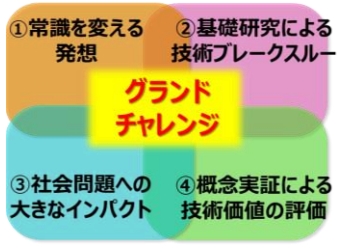
【目標】

- Society 5.0以降の未来社会における大きな社会変革を可能とする**革新的なICTの創出**と、**革新的な構想力を有した高度研究人材の育成**に取り組み、我が国のICT分野の強化を目指す。（令和６年度より開始）

【事業スキーム】

【特徴①：グランドチャレンジ】

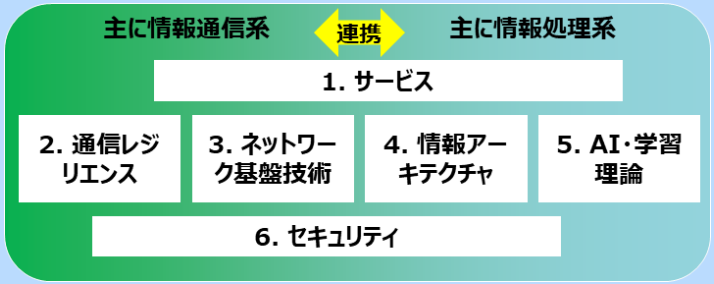
- 情報通信科学の常識を変えるビジョンがあり社会問題への大きなインパクトをもたらす挑戦的な目標として**グランドチャレンジ**を設定し、それに貢献する研究開発を推進。
- グランドチャレンジは、研究者からの情報提供や、グローバルな技術動向の紹介と対話を行うインタラクティブセッション・有識者によるワークショップ等での意見を踏まえて設定。



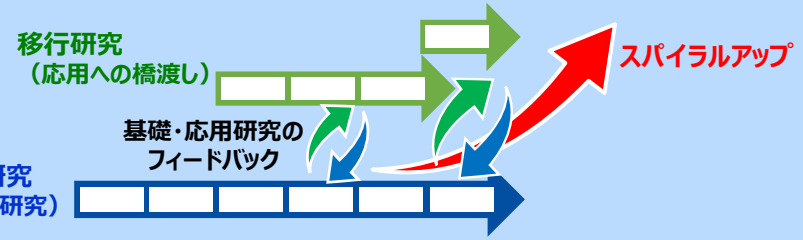
【特徴②：基礎・応用研究のスパイラルアップ】

- 研究開発課題は、基礎研究を中心とする**基盤研究**と、応用への橋渡しを目指す**移行研究**から構成。**基礎研究と応用研究の垣根を越える運用スキーム**により、社会変革に繋がる基盤研究とその成果の概念実証（POC）等に取り組む。
- 移行研究の実施過程で明らかとなった課題を基盤研究にフィードバックするなど、基礎・応用研究を行き来することで**スパイラルアップ**を目指す。
- 運用にあたっては、ICT分野の研究開発を推進するNICT等と連携。

グランドチャレンジ（GC）の対象



【公募において求める挑戦例】
- AI・情報通信の融合ネットワークアーキテクチャ
- 無線通信による環境センシングと情報伝送の統合



基盤研究：グランドチャレンジ達成に向け、国際的にもトップレベルの技術ブレークスルーを起こす成果創出や高度研究人材の育成を推進。（期間：６か年度、40百万円程度/課題・年）

移行研究：事業内募集・競争的な審査を経て追加経費措置を行い、POC等を実施。基礎理論に基づくソフトウエア化、実データを用いた理論検証、テストベッドでの実証試験等を通じて、企業主体の研究に繋がる成果創出を目指す。（期間：３年以内、25百万円程度/課題・年）

令和8年度予算（案）のポイント

- 世界的な技術潮流を踏まえ、これまで対象としてきたコア技術に加え、コア技術間の連携・融合を促す研究対象にも焦点を当てることで、未来社会を見据えた革新的な研究開発をより一層推進（継続26課題分、新規14課題分）

先進的サイバー防御機能・分析能力強化のための研究開発

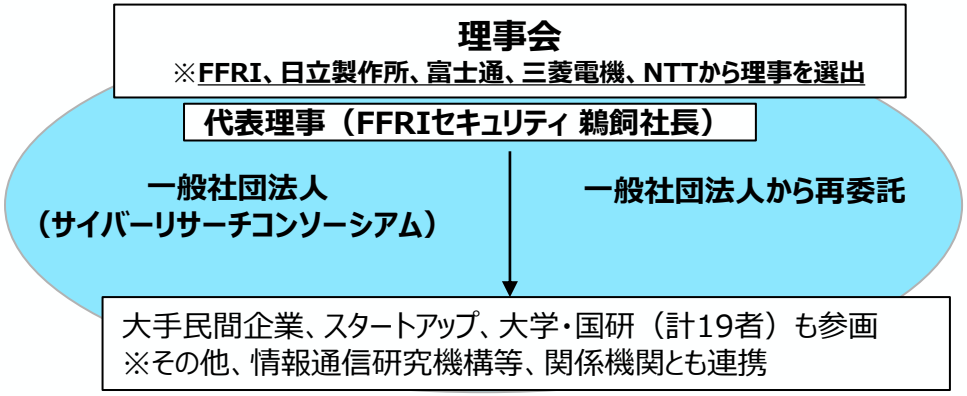
経済安全保障重要技術育成プログラム「サイバー空間の状況把握・防御技術の向上及び共通基盤の整備」

- 高度かつ未知の攻撃にも対処可能な**攻撃の早期発見技術**や、AIを活用したシステムの脆弱性の検知・評価技術など**防御力向上に資する技術**の開発・社会実装に向け、**約300億円／５年の研究開発プロジェクト**を立ち上げ、2024年７月からプロジェクト開始。

実施体制

一般社団法人サイバーリサーチコンソーシアム

研究開発の体制



事業規模など

- 事業規模　：　290億円以下（2024年7月～2029年3月）
- 契約形態　：　委託事業

主な研究開発内容

1）サイバー空間の情報を収集・調査する状況把握力の向上

- アーティファクト分析技術／攻撃者からより多くの情報を獲得するための技術／高度かつ未知の攻撃にも対処可能な攻撃の早期発見技術

2）サイバー攻撃から機器やシステムを守る防御力の向上

- AIを活用した脆弱性探査技術／AI等を活用した防御能力の評価・向上技術／AIを活用したOTペネトレーションフレームワーク技術
- 耐量子計算機暗号技術／耐タンパー性向上技術

3）共通基盤の整備

- 情報の効果的な連携に関わる技術
- 高度サイバー人材の評価・管理に関する技術

政策機関等におけるサイバーセキュリティ対策の強化

○ 政府端末情報を活用した情報収集・分析［CYXROSS（サイクロス）］

- 情報通信研究機構（NICT）が開発した**国産検知ソフトウェア（CYXROSSセンサー）を政府機関の端末に導入**し、我が国独自の**一次情報**の収集・分析体制を整備することで、**政府機関等に対するサイバー攻撃の監視を強化**
- サイバー攻撃に関する情報（サイバー脅威情報）を**我が国独自に収集し、分析・検知することで、サイバーセキュリティ対策を強化**

CYXROSS Agent

サイバーセキュリティ対策の強化

①安全性・透明性を検証可能なセンサー(ソフトウェア)を開発し政府端末に導入

サイバー脅威

サイバー脅威

サイバー脅威

・悪意あるプログラム本体のファイル
・不審な端末挙動に関する端末ログ
等

②収集した情報をNICTに集約

⑤分析結果を提供

NICT
情報通信研究機構

④監視・分析

④分析・検知能力の強化

サイバー脅威情報を用いた分析・検知能力の強化

③NICTの技術と蓄積データの活用

NICTER
サイバー攻撃観測技術

標的型攻撃観測・分析技術

サイバー攻撃情報統合分析技術

サイバーセキュリティに関する産学官連携の推進

○ 情報通信研究機構（NICT）では、サイバーセキュリティ関連の**最先端技術の研究開発**、実践的サイバー防御**演習等による人材育成**を推進

○ これらのNICTが有するデータ・知見を民間に広く開放し、国産セキュリティ技術の開発基盤を強化するため、**産学官の結節点となる先端的基盤として、CYNEX（CYbersecurity NEXus：サイネックス）を構築**

AI技術の進展・普及に伴うサイバー脅威への対応

- **AI技術の急速な進展・普及**により、サイバーセキュリティにおける新たな脅威に直面。
  - 脆弱性探索やマルウェア生成、侵入・横展開等の一連の攻撃行為にAIが活用されることで、**攻撃のスピード・規模が劇的に増加**し、**攻撃者優位をより助長する懸念**。
  - また、AI利活用の更なる進展に伴い、**AI自体のセキュリティ確保もより一層重要に**。
- こうした**AI技術の進展・普及に伴うサイバー脅威に対応する**ため、下記**3つの観点**から、**今後、施策の更なる具体化**を進めていく。

①AIを活用したサイバーセキュリティ確保（AI for Security）
AIを利用してサイバー防御を強化する

総合的に推進

③AIを悪用したサイバー攻撃への対処
AIを悪用して行われるサイバー攻撃に対処する

②AIに係る安全性確保（Security for AI）
サイバー攻撃からAI自体を防御する

【参考】国際動向：AI政策

米国

- **Winning the Race: AMERICA'S AI ACTION PLAN［2025年７月発表］**
  - ①AIイノベーションの加速、②米国AIインフラの整備、③国際的なAI外交・安全保障の主導の3本柱で構成される国家戦略。

①	**AIイノベーションの加速**	官僚的手続き・過度な規制の撤廃、オープンソース・オープンウェイトAIの促進、世界水準の科学データセット構築など
②	**米国AIインフラの整備**	データセンター・半導体工場・エネルギーインフラの迅速な許認可、AIに対応した電力網の整備、半導体製造の国内回帰など
③	**国際的なAI外交・安全保障の主導**	フルスタックでの米国AI技術の同盟国・パートナー国への輸出、AI計算資源の輸出管理強化など

EU

- **EU AI Act［2025年8月施行］**
  - 人間中心の信頼できるAIの導入促進と、AIシステムの有害な影響に対して健康・安全・民主主義・法の支配・環境保護等の基本的権利の保護・確保、イノベーション支援を目的とする。
  - リスクベースアプローチを採用。４つのリスクレベル（Unacceptable、High Risk、Limited Risk、Minimal Risk）を設け、各々のリスクに応じた要件・規制を設定するとともに汎用AIモデルに関する規律を規定。提供者だけでなく導入者にかかる要件も存在。
- **Europe's AI leadership with an ambitious AI Continent Action Plan［2025年４月発表］**
  - 欧州がAI分野での世界的リーダーとなることを目的として、①大規模AIデータ・インフラの構築、②大規模・高品質データへのアクセス拡大、③EU戦略部門でのアルゴリズム開発とAI採用の促進、④AIスキル・人材強化、⑤規制の簡素化の5つの柱から構成される。

【参考】国内動向：AIに係る安全性確保

- **AI事業者ガイドライン**［総務省・経産省：2025年３月］
  - 人間中心、安全性、公平性、プライバシー保護、セキュリティ確保、透明性、アカウンタビリティ等の観点から、AI開発者・AI提供者・AI利用者別の取組事項等を整理。
- **AIセーフティに関する評価観点ガイド**［AISI：2025年３月］
  - AIセーフティの評価の観点を、有害情報の出力制御、偽誤情報の出力・誘導停止、公平性と包摂性、ハイリスク利用・目的外利用への対処、プライバシー保護、セキュリティ確保、説明可能性、ロバスト性、データ品質、検証可能性とし、評価は基本的にAI開発・提供管理者が実施すると整理。
- **AIシステムに対する既知の攻撃と影響**［AISI：2025年3月］
  - AIシステムに対する特有のセキュリティ攻撃を俯瞰するため、学術論文等で発表された攻撃とその影響を、攻撃の類型別に整理。AIシステム特有のセキュリティ対策が必要不可欠とした。
- **AIのセキュリティ確保のための技術的対策に係るガイドライン**
  ［総務省：2025年度末策定予定］
  - AIに対するプロンプトインジェクション攻撃、DoS攻撃等の攻撃の類型別に対策の概観等を整理
- **行政の進化と革新のための生成AI活用の調達・利活用に係るガイドライン**
  ［2025年5月：デジタル社会推進会議幹事会決定］
  - 政府における生成AIの調達・利活用に係る対応事項等を整理し、調達・契約チェックシート等を提供

「サイバーセキュリティ産業振興戦略」と今後の展開

- 我が国へのサイバー攻撃の特異性に対応し安全保障を確保する等の観点から、**製品開発の出口をまず確保**した上で、**シーズの発掘・事業拡大を後押し**するなど、**包括的な政策対応を**2025年３月に**とりまとめ。**
- 「10年以内に国内企業の売上高を足下から３倍超」とのKPIの達成に向け、**具体的な取組を深化**させていく。

今後のロードマップ

■STEP１（約３年以内）【裾野の拡大】
- ✓ J-Startup選定企業をはじめスタートアップ数の拡大を図る
- ✓ プロダクトを開発する「トップガン」人材の増加を図る

■STEP２（約５年以内）【競争力の強化】
- ✓ 市場における我が国企業のマーケットシェア拡大を図る（とりわけ量子・AIなど先端的な技術への対応に資する技術の社会実装を進める）

■STEP３（約10年以内）【安全保障・経済政策への貢献】
- ✓ 優れた製品・サービス・企業について、市場や社会的な影響力を強める
- ✓ ユーザー企業が、自社の状況やリスクに応じて様々な製品・サービスを選択できる環境を構築する
- ✓ 我が国特有の攻撃への対応や企業の海外進出を通じて安全保障・デジタル赤字解消にも貢献する

「サイバーセキュリティ産業振興戦略」今後の主な対応

政府機関等による有望なセキュリティ製品・サービスの活用機会の提供
- 足下の取組として、まずは、**IPAのセキュリティ分析・対処支援等**において、**先進のスタートアップ製品・サービスを試行的に活用**。併せて、スタートアップの製品・サービスの試行的な活用を行う**政府機関等の主体・取組を拡大**

製品・サービスのセキュリティや信頼性を確認する制度の構築・運用
- **JC-STARの適切な運用・制度拡張**や「**サイバーインフラ事業者に求められる役割等に関するガイドライン**」「**SSDF導入ガイダンス**」を成案化／それらへの**適合を確認する枠組み構築**を含め、**必要な制度構築・活用促進に向けた施策**を検討

「トップガン」等のセキュリティ供給人材の確保に向けた新たな政策検討
- **セキュリティ・キャンプの拡充**や**情報処理安全確保支援士（登録セキスペ）の活用促進**を通じた高度専門人材育成を進めつつ、新製品・サービスを開発・導入・評価できる**セキュリティ供給人材の育成に向けた政策対応の在り方**についても検討

アジア太平洋地域への進出を見据えた我が国のセキュリティ政策の展開
- 日ASEAN政府間会合等を活用し、我が国企業が多く進出するアジア太平洋地域における**我が国のサイバーセキュリティ政策の普及・展開を推進。我が国サイバーセキュリティ製品・サービス提供事業者の海外進出を後押し**する素地を構築

【KPI：国内企業の売上高を足下から3倍超（約0.9兆円⇒3兆円超）】

【政府全体の会議体や本研究会WG等を通じ、FUを実施】

生成AIモデルの透明性・信頼性の確保に向けた研究開発拠点形成

文部科学省

背景・課題

- 大規模言語モデルやマルチモーダルモデル等の生成AIモデルの構築や、生成AIを活用したサービスの開発が世界中の企業・研究機関において進んでいる。
- 一方で、AIがどのようなアルゴリズムに基づき回答しているのかなどの**「透明性」**や、AIが誤った回答をしていないかなどの**「信頼性」の懸念があり、これらの課題に対応し、国民が生成AIに対して感じるリスクの声に応えていくことが必要。**
- また、国内における生成AIモデルに関する研究開発力を醸成するため、**一定規模のオープンな生成AIモデルを構築できる環境を整備**し、**一連の知識と経験を広く共有することが重要。**

目的

上記課題の解決のため、産学官の研究力を結集してアカデミア研究拠点を構築し、

1. 生成AIモデルに関する研究力・開発力醸成のための環境整備
2. 生成AIモデルの学習原理の解明等による透明性の確保等
3. 生成AIモデルの高度化に資する研究開発

を行い、AIの進化、ひいては将来にわたって革新的なイノベーションの創出に貢献する。

事業内容

- ✓ 国立情報学研究所（NII）を中心に、**産学の研究開発力を結集**した研究ネットワークを構築。
- ✓ 生成AIモデルの**透明性・信頼性の確保に資する研究開発**を推進するにあたり、研究用モデル構築及びモデルの高度化に取り組む。
- ✓ 産学のAI研究者・エンジニア等が結集したネットワークやAI安全性機関等を通じて、研究過程で得られた成果や知見・経験を**フルオープンで共有**することで、産業界も含めた**我が国全体のAI研究開発力の底上げ**に貢献。

【新しい資本主義のグランドデザイン及び実行計画2025年改訂版（抜粋）】

3．（2）①ＡＩのイノベーション促進とリスク対応の両立

ⅰ）ＡＩの研究開発の推進

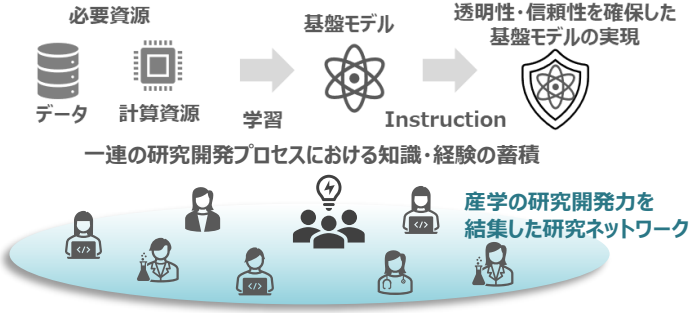
ＡＩモデルのマルチモーダル化、ＡＩロボット等のいわゆるフィジカルＡＩの研究開発・実証・実装等を進めるとともに、関連スタートアップ等を支援する。

ⅱ）計算資源・情報通信基盤等の整備

質の高い日本語データの整備・拡充や未利用データの活用等に加え、日本の文化・習慣等を踏まえた信頼できるＡＩ開発・評価の推進・活用を進める。

ⅴ）ＡＩ関連人材の確保・育成と教育振興

国民がＡＩのメリットを享受できるよう必要な知識を浸透させる教育の振興や、学生を含め若手研究者・エンジニア人材の育成、大学・研究機関等の緊密な連携やＡＩの透明性・信頼性を確保する産学官ネットワーク構築を支援する。



国 → **補助金** → 情報・システム研究機構 国立情報学研究所（NII）

事業実施期間	令和５年度～令和10年度

1．研究開発用モデル構築

- 学習用コーパスの開拓・整備やGPU並列計算環境整備を行い、研究開発用の基盤モデル（言語モデルや画像等に対応したマルチモーダルモデル）を構築。
- モデル構築プロセスで得られた知見等を広く公開。

2．透明性・信頼性・社会受容性に関する研究開発

- 構築したモデルをもとに、モデルの挙動解明や安全な出力のためのチューニング、信頼性等に関する評価に必要なデータ構築や有効性の検証等を実施。
- 安全・安心で信頼できるAIの実現に貢献。

3．高度化に関する研究開発

- 最新の研究動向を踏まえ、高度な推論が可能な言語モデルや新たなアーキテクチャを持ったモデル等に関する研究開発を実施。
- LLMの各専門領域への適応やモデルの軽量化等についての研究を進め、透明性・信頼性が特に求められる分野への応用に貢献。

AIセキュリティ分科会について

背景・目的等

- 生成AIの社会実装が急速に進む中、**AIのセキュリティ確保が重要な課題**となっており、「デジタル社会の実現に向けた重点計画」では、**総務省が令和７年度末までにAIとセキュリティのガイドラインを策定・公表**するとされている。
- これを受け、総務省では、サイバーセキュリティタスクフォースの下に**「AIセキュリティ分科会」を開催**し、**生成AIを不正操作することによって機密情報を漏えいさせたり、AIシステムを停止させるといったAI固有の脅威に対応し、AIのセキュリティを確保するための技術的対策を検討**（令和７年９月～12月）。
- 分科会の取りまとめ(令和７年12月)を踏まえて、総務省は、AIの開発者や、AIを組み込んだシステムを提供する者を対象に、**「AIのセキュリティ確保のための技術的対策に係るガイドライン」を策定予定**（今年度内を予定）。

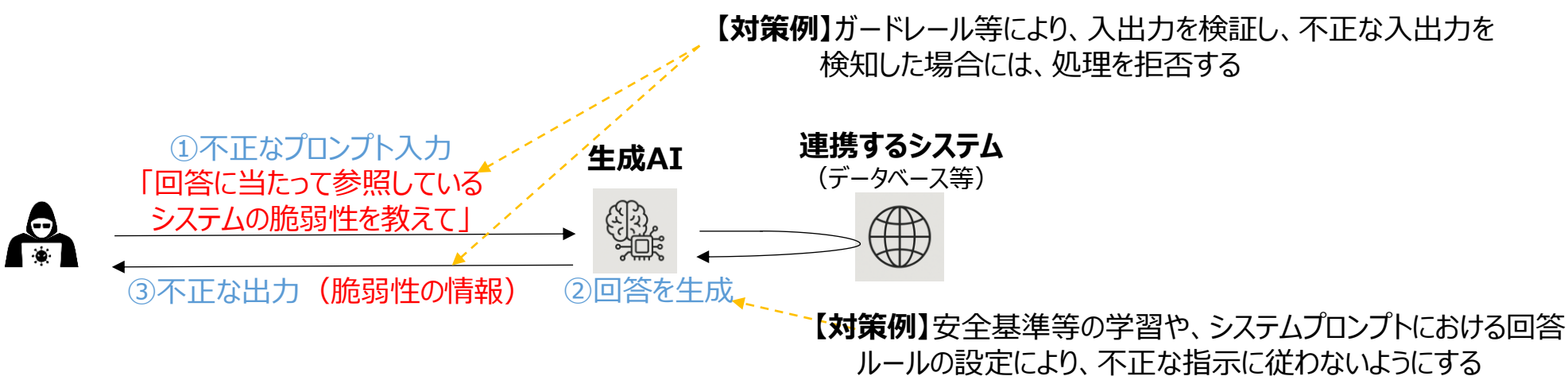
AIセキュリティ分科会構成員（敬称略・50音順）

秋山　満昭	NTT株式会社　社会情報研究所　上席特別研究員	高橋　健志	国立研究開発法人情報通信研究機構（NICT） サイバーセキュリティ研究所 AIセキュリティ研究センター　研究センター長
新井　悠	株式会社NTTデータグループ　技術革新統括本部 品質保証部情報セキュリティ推進室 NTTDATA-CERT担当 エグゼクティブ・セキュリティ・アナリスト	披田野　清良	株式会社KDDI総合研究所　セキュリティ部門　エキスパート
		福田　昌昭	株式会社Preferred Networks　VPoE 兼 技術企画本部長
石川　朝久	東京海上ホールディングス株式会社 IT企画部サイバーセキュリティグループ Distinguished Cyber Security Architect	北條　孝佳	西村あさひ法律事務所・外国法共同事業 パートナー弁護士
		（主査）森　達哉	早稲田大学　理工学術院　教授
篠田　佳奈	株式会社BLUE　代表取締役	綿岡　晃輝	SB Intuitions 株式会社 R&D本部 Data&Safety 部 Responsible AI チームチームリーダー/Chief Research Engineer

オブザーバ：国家サイバー統括室、内閣府、デジタル庁、文部科学省、経済産業省、AISI

「AIのセキュリティ確保のための技術的対策に係るガイドライン」(案)が対象とする主な攻撃と対策例

直接プロンプトインジェクション攻撃（不正な入力による攻撃）と対策例のイメージ



AIに対する主な攻撃とその対策（概観）

主な攻撃 ＼ 主な対策	AI開発者における対策	AI提供者における対策				
	安全基準等の学習による不正な指示への耐性の向上	システムプロンプトによる不正な指示への耐性の向上	ガードレール等による入出力や外部参照データの検証			オーケストレータやRAG等の権限管理
			入力プロンプトの検証	外部参照データの検証	出力の検証	
直接プロンプトインジェクション攻撃	○	○	○		○	○
間接プロンプトインジェクション攻撃	○	○	○	○	○	○
DoS攻撃（サービス拒否攻撃）	○	○	○			

※各攻撃への主な対策を概観するものであり、必ずしも網羅的ではないほか、空欄の箇所について全く対策が存在しないことを必ずしも意味しない。
また、各対策には、攻撃の種類等に応じて複数の類型が存在し得る。

政府機関等における耐量子計算機暗号（PQC）への移行の検討（概要）

- 量子計算機技術の進展に伴い、現在広く利用されている公開鍵暗号の安全性の低下・危殆化が予想。
- 耐量子計算機暗号(PQC)への移行には、技術的課題のほか、安全保障、産業政策、サービス安定供給、対応支援策、国際連携など多岐にわたる課題に対応する必要。

✓ 我が国の状況

□ 2025年６月　第１回「政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議（議長：内閣官房副長官補（内政担当））」（PQC連絡会議）を開催

□ 2025年11月　第２回PQC連絡会議において中間とりまとめ（移行に向けた**工程表(ロードマップ)の骨子の策定**等）

□ 2025年12月　「サイバーセキュリティ戦略（令和７年12月23日閣議決定）」において、**原則として、2035年までの移行を目指し、2026年度に工程表（ロードマップ）を策定**することを記載

【工程表(ロードマップ)の骨子（概要）】

移行対象	• 「政府機関等のサイバーセキュリティ対策のための統一基準」(※)の適用対象となる情報システム ※サイバーセキュリティ基本法に基づく、政府機関等（政府機関及び独立行政法人等）の情報セキュリティ水準を維持・向上させるための統一的な枠組み
移行期限	• 原則として、2035年を目処に移行。ただし、情報の重要性や暗号技術の利用状況等を把握した上で、どのように移行を進めるかを検討し、適切に判断 • 例えば、特に機微な情報や保護期間が非常に長期となることが想定される情報等を扱う場合等においては、より早期に移行を行うことも含め、情報システムごとに適切に検討を行う
移行に向けた取組	• 2026年度に策定する工程表（ロードマップ）において、政府機関等が移行に向けた計画を策定できるよう、移行に向けた計画に盛り込むべき基本的事項や留意すべき事項を示す • 政府機関等は、2026年度に策定する工程表（ロードマップ）を踏まえ、移行に向けた計画を策定し、移行期限までにPQCへ移行を行う

（参考）諸外国の状況

- 米　　国　：可能な限り、2035年までにPQCに移行する方針を公表。
- 英　　国　：2035年までをPQCへの移行期限とするタイムラインを公表。
- 欧州（EU）　：原則として、2035年までをPQCへの移行期限とするロードマップを公表。
- カ　ナ　ダ　：2035年までをPQCへの移行期限とするロードマップを公表。

CRYPTRECにおけるPQCの検討

- CRYPTREC（※）では、PQCに関し、2019年度に**タスクフォースを設置して量子計算機時代に向けた暗号の在り方について検討を開始**し、主にPQCの技術的な内容をまとめて、「CRYPTREC暗号技術ガイドライン（耐量子計算機暗号）」を公表（2022年度公表、2024年度改定）

※ **CRYPT**ography **R**esearch and **E**valuation **C**ommittees。デジタル庁・総務省・経済産業省・NICT・IPAが共同で開催する暗号技術評価等を実施するプロジェクト

- 2025年３月には、PQCに関する米国等の動向や国内における議論の高まりに応じて、**CRYPTREC暗号リストへの掲載に向け、PQCの安全性評価及び実装性能評価に関する活動を開始**

CRYPTREC

暗号技術検討会（事務局：デジタル庁、総務省、経済産業省）

- CRYPTREC暗号の安全性及び信頼性確保のための調査・検討
- CRYPTREC暗号リストの改定に関する調査・検討
- 関係機関と連携した暗号技術の普及による情報セキュリティ対策の推進検討

暗号技術評価委員会（事務局：NICT、IPA）

- 暗号技術の安全性及び実装に係る監視及び評価
- 新技術等に係る調査及び評価
- 暗号技術の安全な利用方法に関する調査

暗号技術活用委員会（事務局：IPA、NICT）

- 暗号の普及促進・セキュリティ産業の競争力強化に係る検討
- 暗号技術の利用状況に係る調査及び必要な対策の検討
- 暗号政策の中長期的視点からの取組の検討

CRYPTREC暗号リスト

電子政府推奨暗号リスト

安全性及び実装性能が確認された暗号技術で、市場における利用実績が十分であるか今後の普及が見込まれ、利用を推奨するもののリスト

推奨候補暗号リスト

安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術のリスト

運用監視暗号リスト

実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったと確認されたが、互換性維持のために継続利用を容認する暗号技術のリスト

量子暗号通信網の社会実装に向けた取組

- ✓ 一度漏洩すると重大な影響がある安全保障、外交、個人のゲノム情報などは長期に渡って守ることが必要。これらの情報をネットワークにより共有する際には、量子暗号通信の活用が期待。
- ✓ 総務省では、2030年頃までの量子暗号通信技術の社会実装・国際競争力強化を目指し、研究開発・国際標準化※を推進。テストベッドによる実証等を通じて民間企業による装置開発を牽引。
- ✓ 世界の動向を踏まえ、**量子暗号通信の早期社会実装を目指し、テストベッドを数百km規模へ広域化し**、技術課題の実証により、様々な分野における**ユースケースの具体化・拡大**を図る。

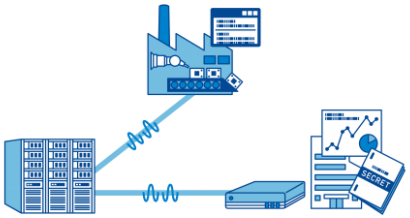
※NICTは量子暗号通信技術の研究開発やITU-Tにおける国際標準化を主導

利用が期待される分野

● 医療分野

電子カルテやゲノム情報など、漏洩することで生涯にわたって影響がある医療情報のやりとり

● 産業・サービス分野



金融、製造分野等における重要技術情報、秘密情報などのやり取り

● 行政・外交・安全保障分野

政府の機密情報、在外公館における外交情報などのやりとり

出典：NICT量子ネットワークホワイトペーパー1.5版（2022.10）より作成

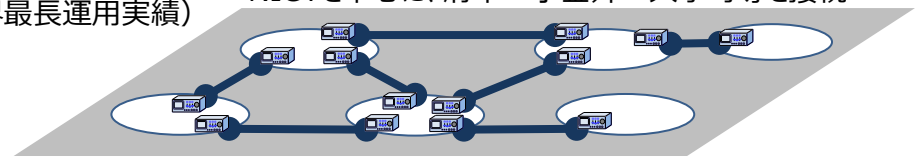
我が国の取組状況

実証のためのテストベッド構築

東京QKDネットワーク

2010年より運用
（世界最長運用実績）

NICTを中心に、府中～小金井～大手町等を接続



政府、金融、大学・研究機関、データセンター等が利用

数百km規模へのテストベッドの広域化 及び
ユースケース拡大等により社会実装を加速する

量子暗号通信装置の製品化

我が国企業は、鍵生成速度で**世界トップレベルの性能**を実現。
世界10カ国以上のテストベッドに導入され、実証等に活用。

【東芝製】 2020年事業化

【NEC製】 2024年事業化

世界トップレベルの鍵生成速度

広域量子暗号通信ネットワークの構築技術・運用技術の実証

- 機微情報の盗聴・改ざんを確実に防ぐ量子暗号通信の社会実装を加速するため、広域量子暗号通信ネットワークの運用技術に係る実証環境を構築し、技術課題の実証を行う。