サイバーセキュリティセミナー’23 in 東北

サイバー攻撃の動向とサイバーセキュリティの結節点

サイバーセキュリティ研究所 サイバーセキュリティネクサス
安田 真悟

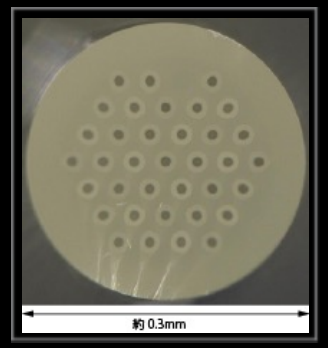
CYNEX
CYBERSECURITY NEXUS

NICT 国立研究開発法人 情報通信研究機構

国立研究開発法人 情報通信研究機構とは？

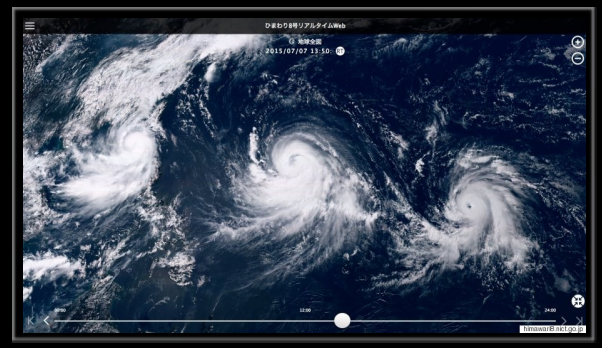
- 情報通信分野を専門とする日本で唯一の公的研究機関

日本標準時の生成・配信
（うるう秒挿入）

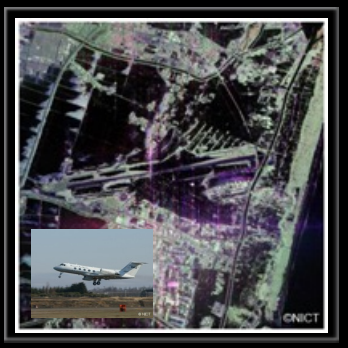


光通信システム
（ペタbps級 マルチコアファイバ）

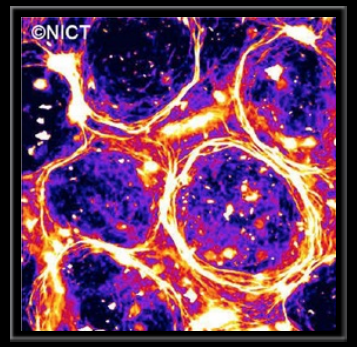
宇宙通信システム
（超高速インターネット衛星きずな）



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）

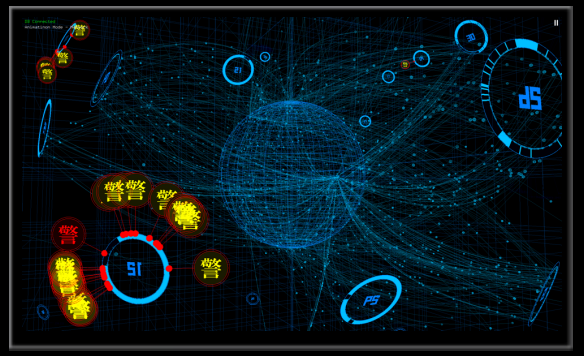


バイオ・ナノICT
（生体分子の自己組織化）

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 サイバーセキュリティ分野の体制図

【第5期中長期計画　サイバーセキュリティ分野】

- (1) サイバーセキュリティ技術
- (2)　暗号技術
- (3) サイバーセキュリティに関する演習
- (4) サイバーセキュリティ産学官連携拠点形成
- (5) パスワード設定等に不備のあるIoT機器の調査

サイバーセキュリティ研究所

セキュリティ基盤研究室
- 暗号技術

サイバーセキュリティ研究室
- 基礎研究

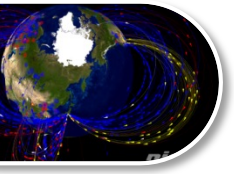
サイバーセキュリティネクサス（CYNEX）

ナショナルサイバートレーニングセンター
- サイバートレーニング研究室
  - 人材育成
- サイバートレーニング事業推進室

ナショナルサイバーオブザベーションセンター
- サイバーオブザベーション運用室
  - IoT調査
- サイバーオブザベーション事業推進室

総合企画室

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

Passive 受

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）

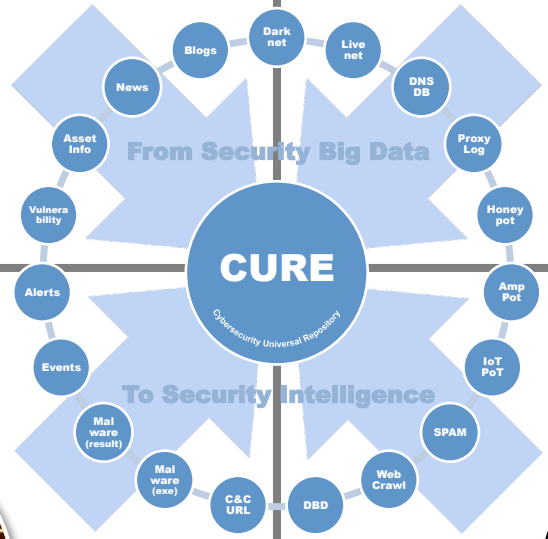
NIRVANA改弐

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

ナショナルサイバートレーニングセンター　事業概要

NICTナショナルサイバートレーニングセンターは、主に以下の4つの事業を推進してまいります。

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）

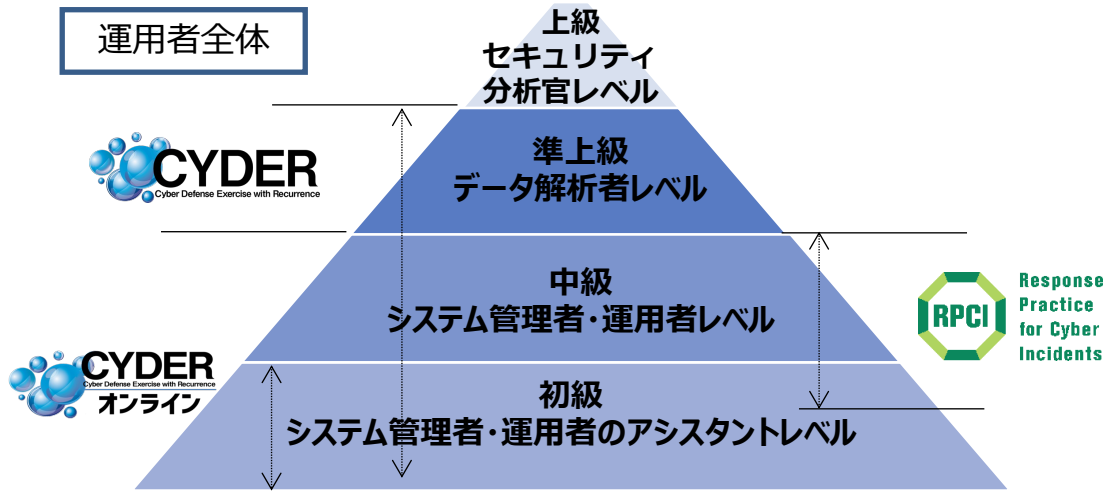
セキュリティイノベーター育成を目的として、NICTが若年層のICT人材を対象に、セキュリティの技術研究・開発を本格的に指導する新規プログラム

ナショナルサイバートレーニングセンターの概要

- NICTの技術的知見、研究施設等を最大限に活用し、実践的なサイバートレーニングを企画・推進する組織として設置（2017年4月1日）
- 日本全体のサイバーセキュリティエコシステムの能動的な発展のため、インシデント対応の実務に携わる運用者及び革新的なセキュリティサービス等を開発するハイレベルな人材の育成を実施

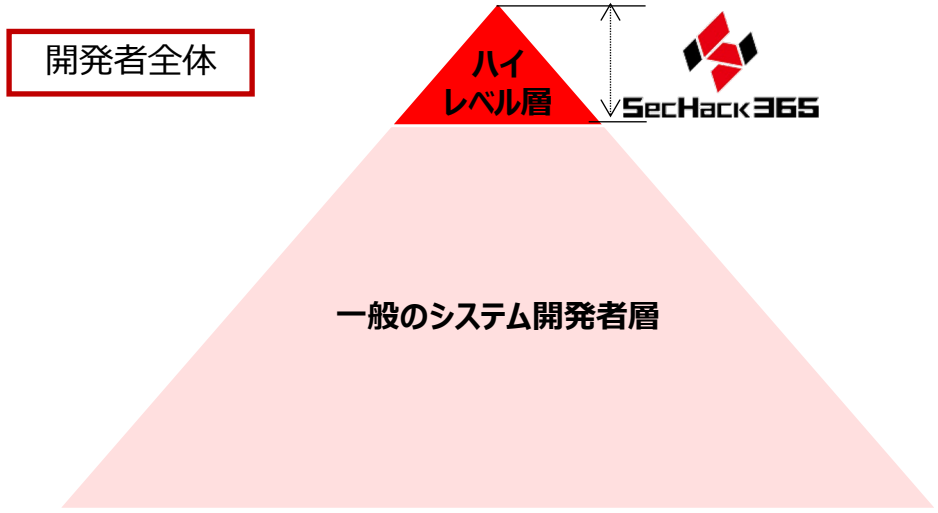
セキュリティオペレーター
（実践的運用者）の育成

- 行政機関や民間企業等の組織内のセキュリティ運用者（情報システム担当者等）を対象
- 年間約3000名の規模で、所属組織がサイバー攻撃を受けた段階等（＝「有事」）における実践的なインシデント対応能力を育成



セキュリティイノベーター
（革新的研究・開発者）の育成

- 単なる「ユーザー」として既存ツールを利用するだけではなく、セキュリティマインドを持ち、革新的なセキュリティソフトウェア等を自ら「研究・開発」していくことができるハイレベルな人材を育成（年間約40名）



（CYDER：Cyber Defense Exercise with Recurrence）

実践的サイバー防御演習「CYDER」の概要

- 国の機関、自治体及び重要インフラ事業者等を対象として、**NICTの技術的知見を活用**し、仮想空間上に　組織のネットワーク環境を再現し、一連のインシデント対応を模した**実践的な防御演習**を行うプログラム。
- 自治体、関係府省庁、重要インフラ事業者等多くの組織が毎年受講

概要（2023年度）

【受講対象】 国の機関、指定法人、独立行政法人、自治体**（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)	自治体
B-2				自治体以外
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
入門	オンライン演習	入門	情報システム担当経験1年前後で 知識のアップデートをお考えの方	全組織共通
プレCYDER		-	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	国の機関等 自治体

CYDER受講者数の推移（累積数）

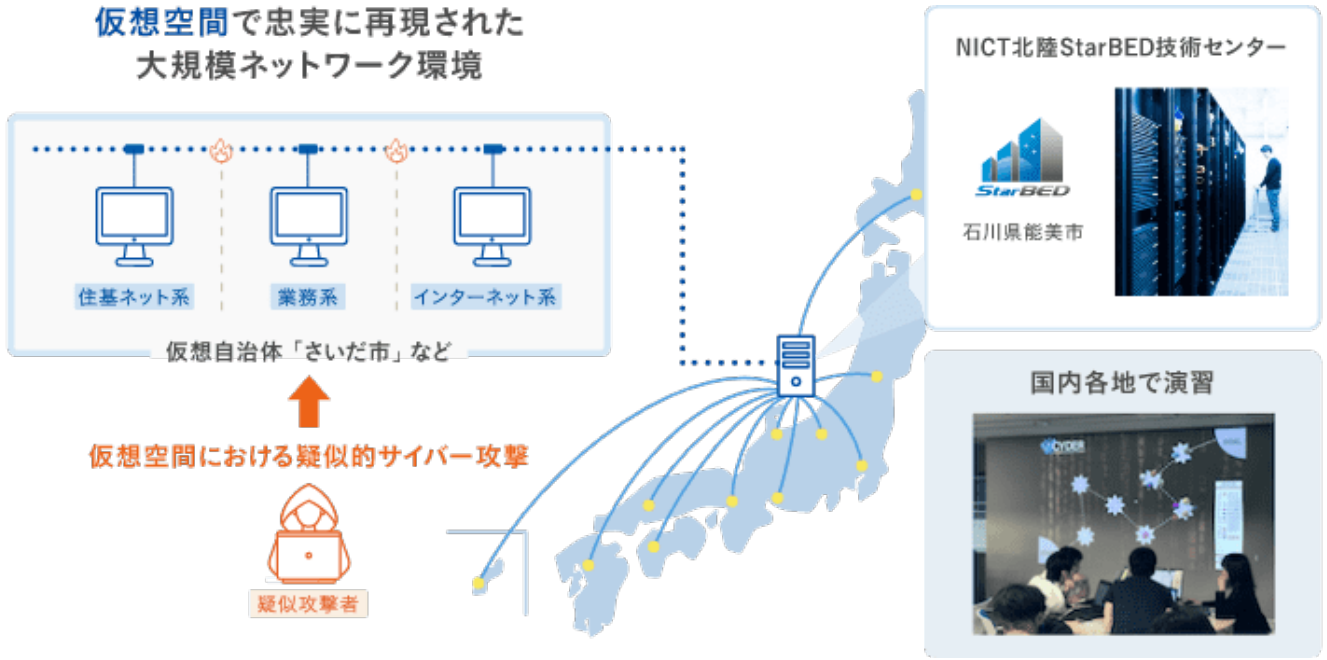
CYDERのトレーニング内容（集合演習）

- 仮想空間上に再現した自治体等のネットワーク環境で、インシデントハンドリングをロールプレイ形式で体験
- 最近のサイバー攻撃事例分析に基づいた、リアリティある演習シナリオ
- 演習会場での、経験豊富な講師・チューターによるサポートや、受講者間のグループワークを通じた高い学習効果

演習シナリオの例

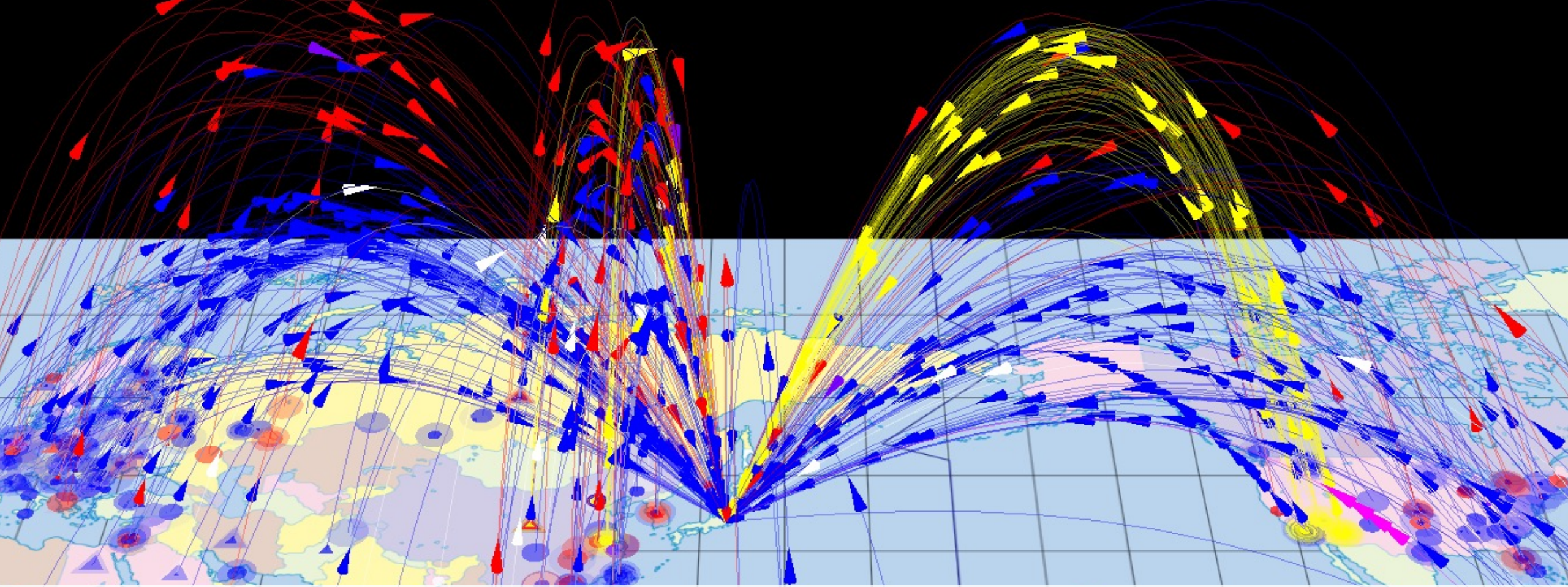
- **標的型攻撃**
  職員が標的型メール（Emotet）を開き感染が拡大し、Web管理者の端末からWebが改ざんされる
- **踏み台攻撃**
  リモートワーク端末を踏み台としてLGWAN内に侵入され、情報を窃取される
- **ランサムウェア攻撃**
  乗っ取られた外部アカウントからのメールを職員が開き、そこを踏み台に組織内システムがランサムウェアに感染

演習舞台設定演習イメージ



※ 地理的・時間的要因等により集合演習の受講が困難な受講者への対応として、自職場から受講可能なオンライン演習も提供中。

サイバー攻撃の動向



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）

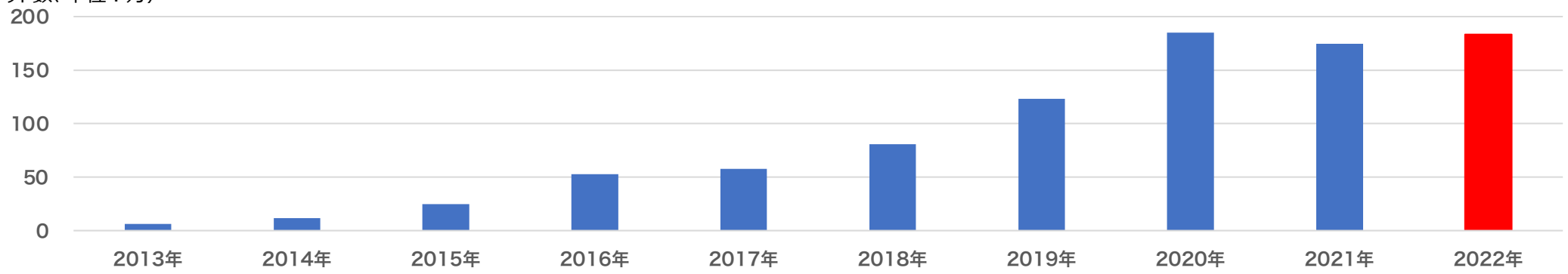
年	年間総観測パケット数	ダークネットIPアドレス数	1 IPアドレス当たりの年間総観測パケット数
2013	約128.8億	209,174	63,682
2014	約241.0億	212,878	115,335
2015	約631.6億	270,973	245,540
2016	約1,440億	274,872	527,888
2017	約1,559億	253,086	578,750
2018	約2,169億	273,292	806,877
2019	約3,756億	309,769	1,231,331
2020	約5,705億	307,985	1,849,817
2021	約5,180億	289,946	1,747,685
2022	**約5,226億**	**288,042**	**1,833,012**

1アドレスあたり

17秒に1回

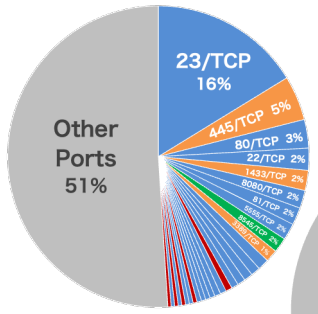
攻撃関連通信受信

（パケット数、単位：万）

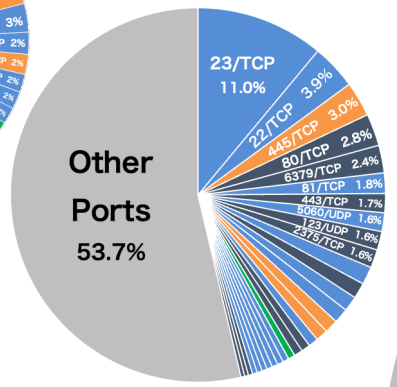


1 IPアドレス当たりの年間総観測パケット数

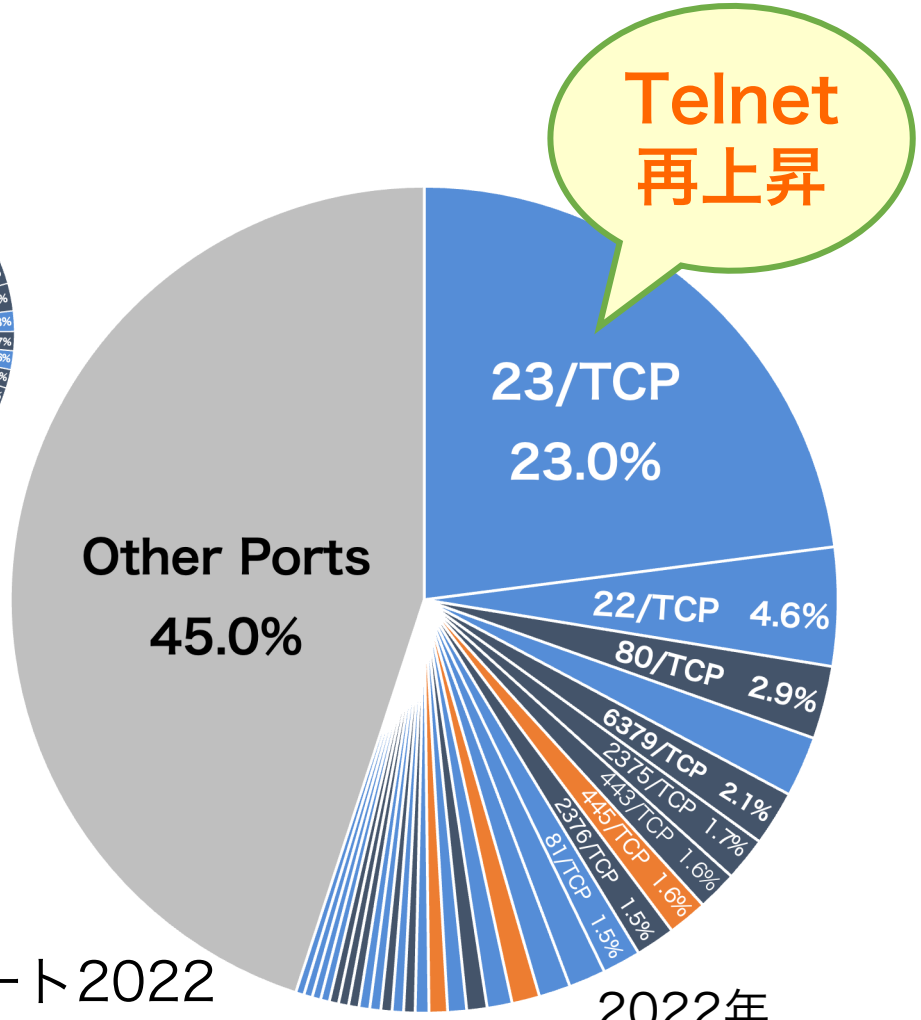
感染機器の分布（2022年）



2020年



2021年



2022年

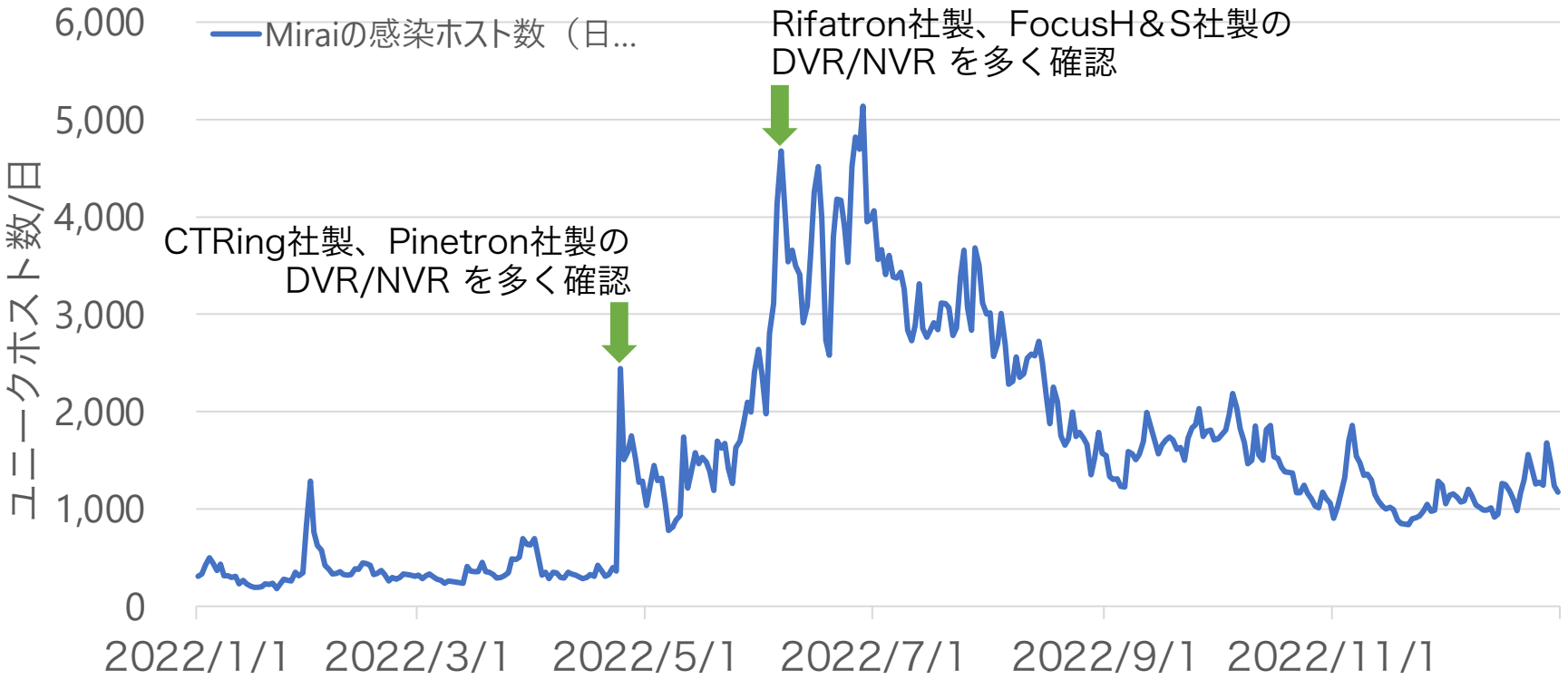
ポート番号	主な攻撃対象
23/TCP	Telnet （ルータ，Webカメラ等）
22/TCP	SSH（サーバ，ルータ等）
80/TCP	HTTP（Web管理画面）
5555/TCP	ADB（Android Debug Bridge）
6379/TCP	Redis
2375/TCP	Docker REST API
443/TCP	HTTPS (Webサーバ)
445/TCP	Microsoft-DS（SMB, Samba等）
2376/TCP	Docker REST API
81/TCP	HTTP（ホームルータ等）

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）

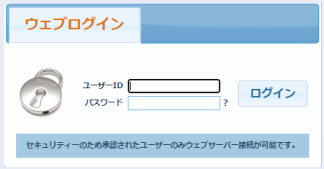
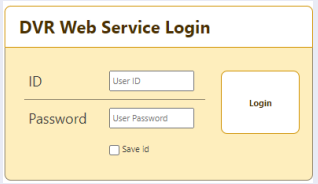
出典：NICTER観測レポート2022
https://csl.nict.go.jp/report/NICTER_report_2022.pdf

Mirai 感染ホスト数の推移（日本）

- 数百～5千ホスト/日で推移（2021年と比較すると増）
- 複数の**韓国製 DVR/NVR 機器**がMiraiに感染

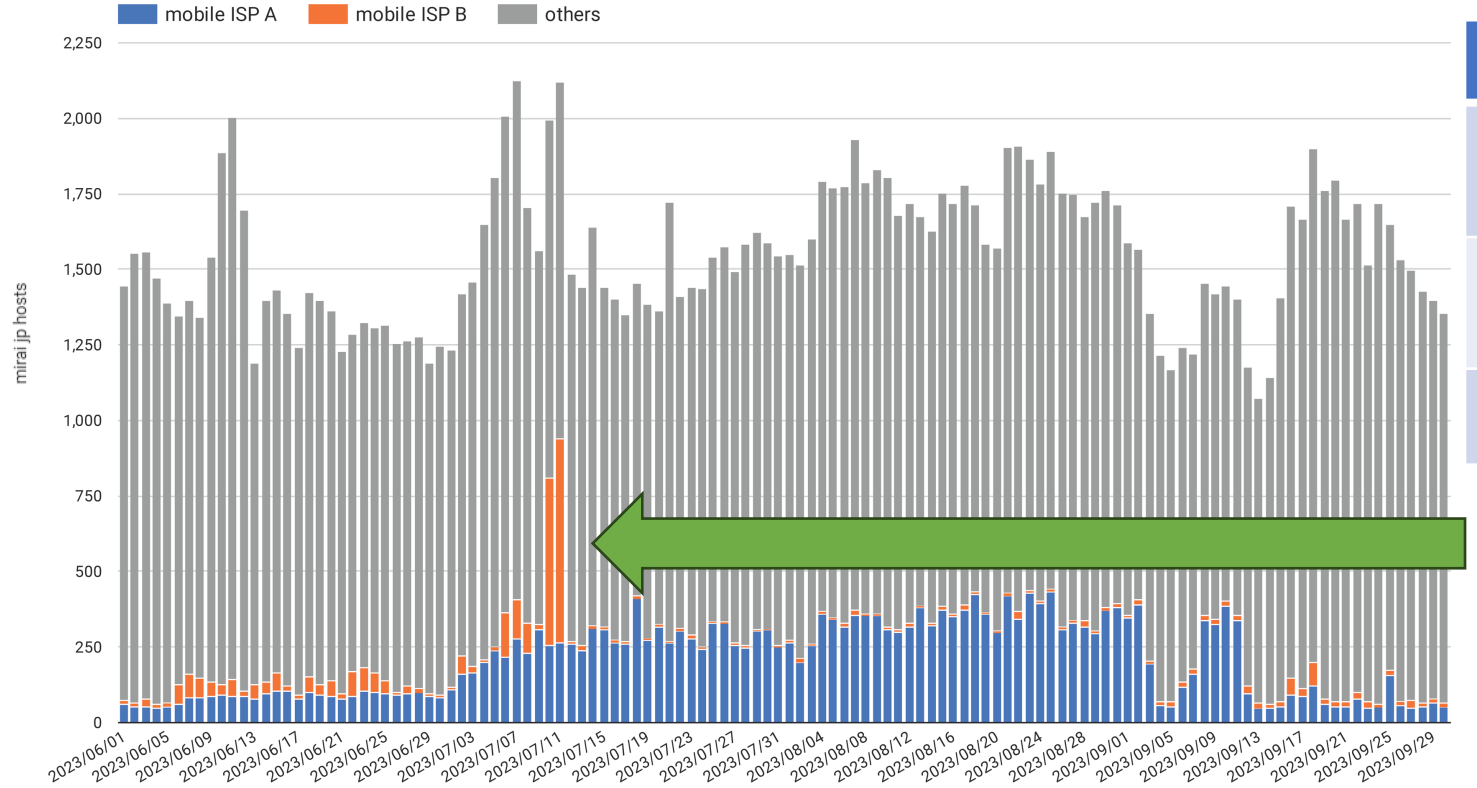


NICTで脆弱性を確認したDVR/NVR（一部抜粋）

製造元	筐体	管理画面	有効なポート （※FWにより異なるため参考情報）	観測したマルウェア
FocusH&S			80/TCP 8002/TCP 9010/TCP 10801/TCP	・Moobot（スキャン機能あり） ・Fodcha
Rifatron			21/TCP 23/TCP 80/TCP 1998/TCP 50100/TCP	・fbot（rippr gang） ・Mirai亜種（スキャン機能あり）
Pinetron			7000/TCP	・Moobot（スキャン機能あり）
CTRing			23/TCP 80/TCP 5920/TCP	・Mirai亜種（スキャン機能あり）

Mirai 感染ホスト数の推移#2（日本）

- 2023 年第 3 四半期に観測した事象
- 日本国内における LTE 対応ルータの Mirai 感染事例



NICTで特定した機器	
サン電子製 LTE 対応ルータ Roosterシリーズ	ハイテクインター製 LTE 対応ルータ HWL-2511-SS
	
※運用上の設定によるもの 初期設定ではない	※脆弱性対応済

回線種別がモバイル回線と判定される国内 Mirai 感染ホスト数の増加を観測（2023年7 月以降）

今すぐできる！ IoT機器セキュリティ対策 7選

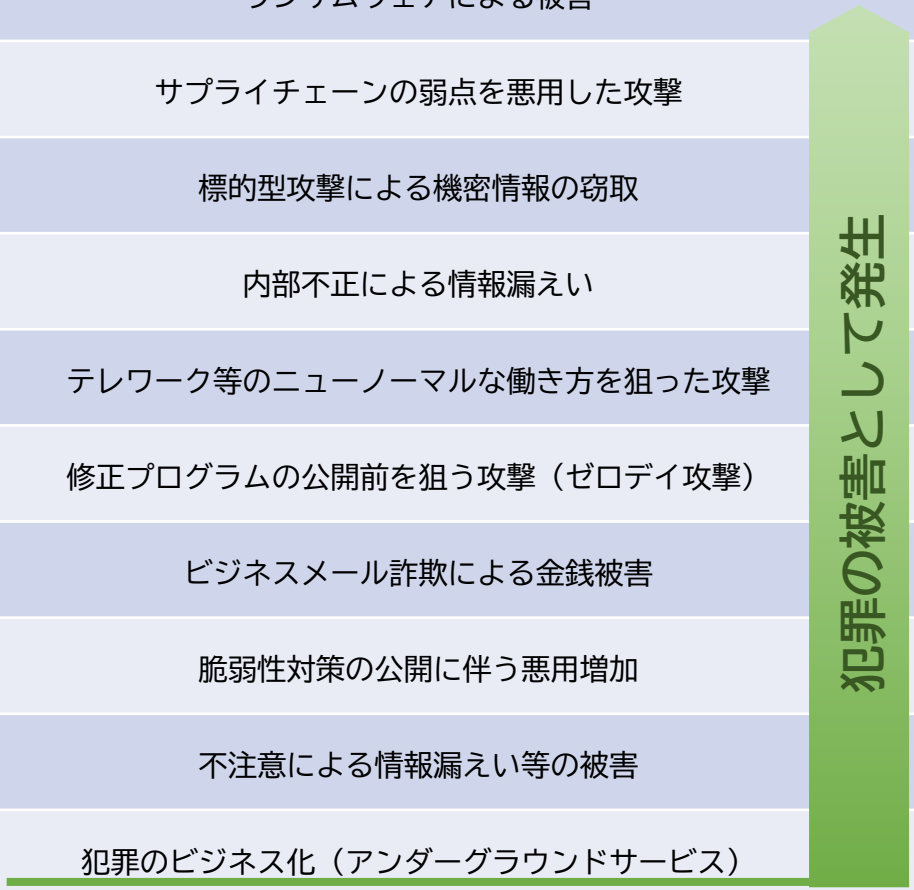
1. IoT機器の再起動（揮発型のマルウェアを消滅させる）
2. ファームウェアのアップデート（脆弱性を塞ぐ）
3. ID/パスワードを変更（初期パスワードでの侵入を防ぐ）
4. インターネット側からのアクセス拒否設定（外から繋がせない）
5. **ゲートウェイ機器の内側に設置**（直接インターネットに繋がない）
6. **古い機器は買い換える**（自動アップデート機能がない機器はNG）
   - 病院・工場など機器更新が困難な場合は資産管理とNW構成を再確認！
7. **NOTICEから注意喚起があれば即対応！**

NOTICE
National Operation Towards IoT Clean Environment

セキュリティ10大脅威2023：組織に注目

順位	個人
1位	フィッシングによる個人情報等の詐取
2位	ネット上の誹謗・中傷・デマ
3位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求
4位	クレジットカード情報の不正利用
5位	スマホ決済の不正利用
6位	不正アプリによるスマートフォン利用者への被害
7位	偽警告によるインターネット詐欺
8位	インターネット上のサービスからの個人情報の窃取
9位	インターネット上のサービスへの不正ログイン
10位	ワンクリック請求等の不当請求による金銭被害

順位	組織
1位	ランサムウェアによる被害
2位	サプライチェーンの弱点を悪用した攻撃
3位	標的型攻撃による機密情報の窃取
4位	内部不正による情報漏えい
5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
6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
7位	ビジネスメール詐欺による金銭被害
8位	脆弱性対策の公開に伴う悪用増加
9位	不注意による情報漏えい等の被害
10位	犯罪のビジネス化（アンダーグラウンドサービス）



組織のセキュリティインシデントのはなし

サイバー攻撃のボリュームゾーンは~~ビジネス~~金銭目的

攻撃対象は星の数

技術は手段
弱いところが狙われる

何が弱いのか？

ITガバナンスの欠如

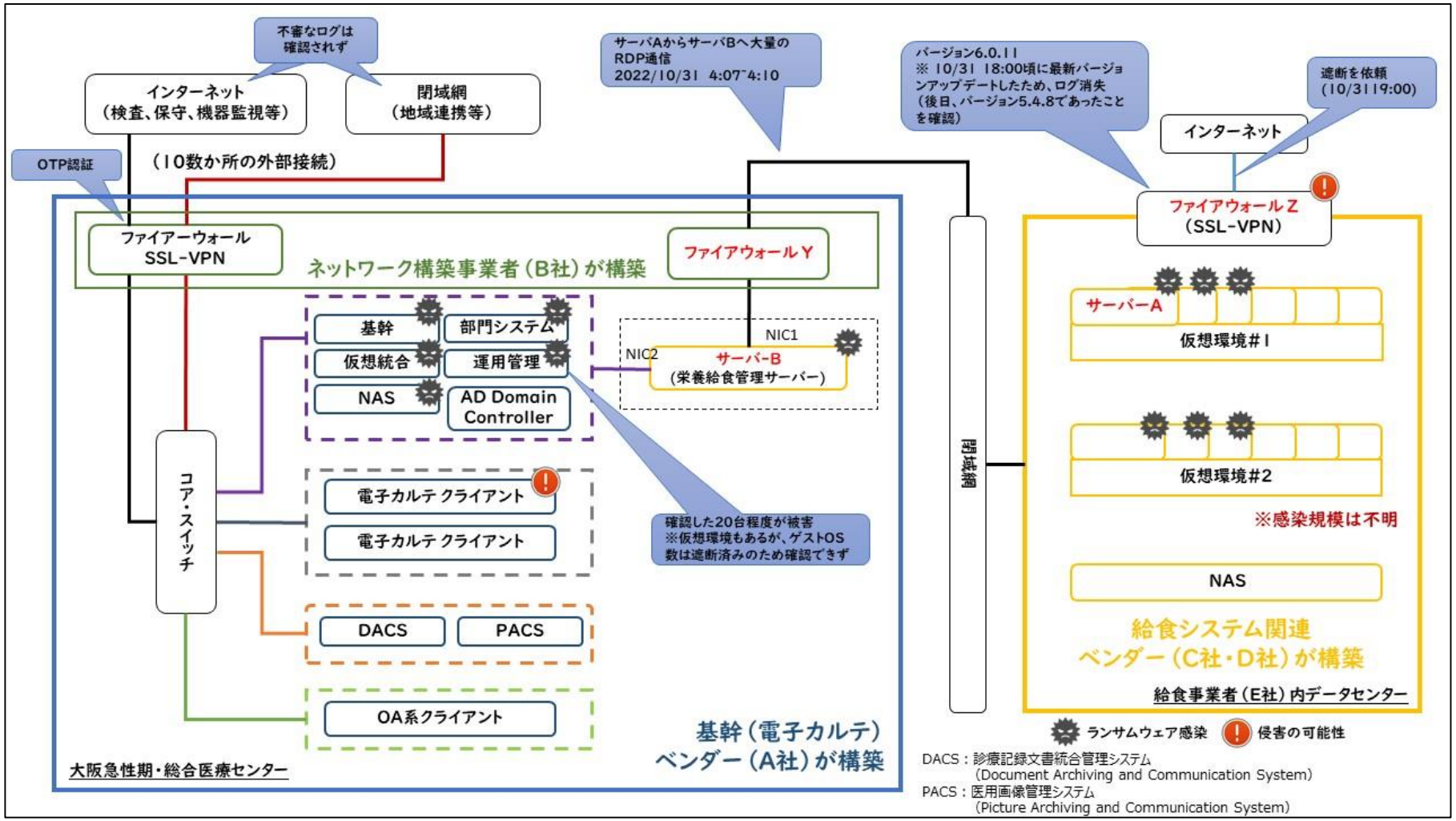
- 大阪急性期・総合医療センター 調査報告書（2023/3/28）

4.2.1. 組織的発生要因のサマリー

① ITガバナンスの欠如

システムや機器を使用する病院において、情報資産が把握されていないことに始まり、契約におけるセキュリティポリシーの不一致や責任分界点の不明瞭さ、脆弱性管理の役割分担など、組織的な ITガバナンスが欠如していた。ITガバナンスとは「経営陣がステークホルダーのニーズに基づき、組織の価値を 高めるために実践する行動であり、情報システムのあるべき姿を示す情報システム戦略の策定及び実現 に必要となる組織能力」のことである。

ネットワーク構成図と感染状況（大阪急性期・総合医療センター）



閉域網神話

ベンダ横断の統制の不備

資産管理の不備

組織のITガバナンス は 信仰とベンダ丸投げ では実現しない

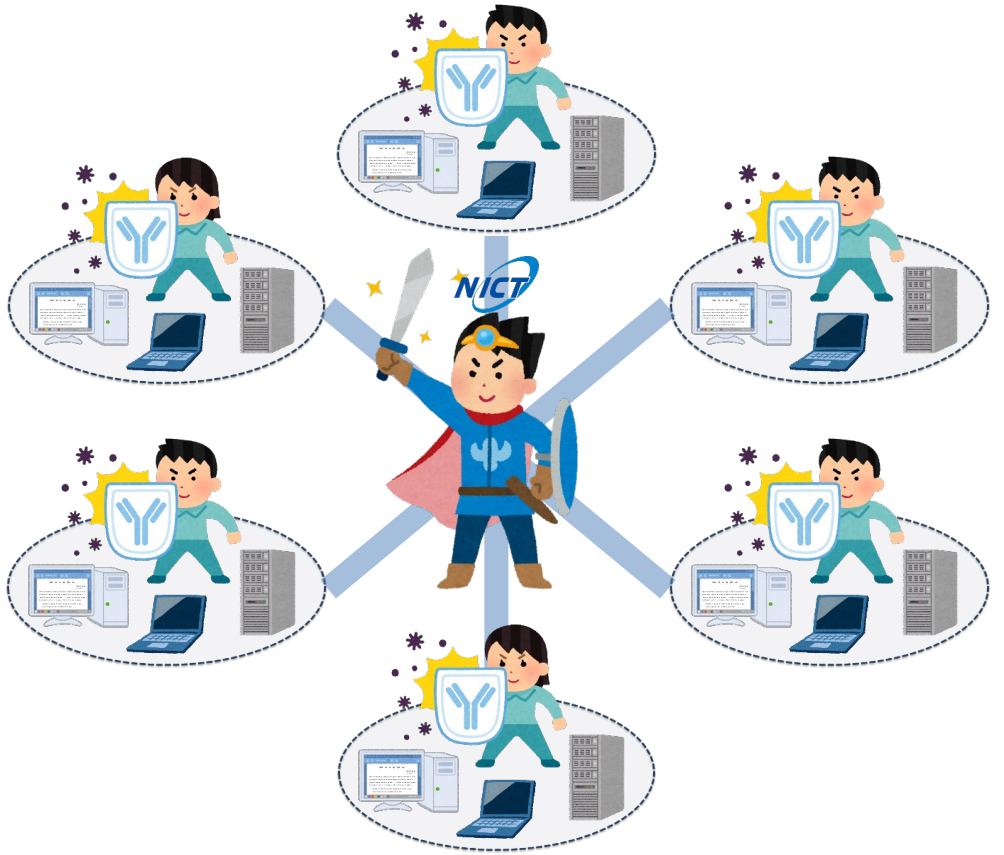
国内サイバーセキュリティの結節点

スタンドアロン型からネクサス型の対策へ

スタンドアロン型

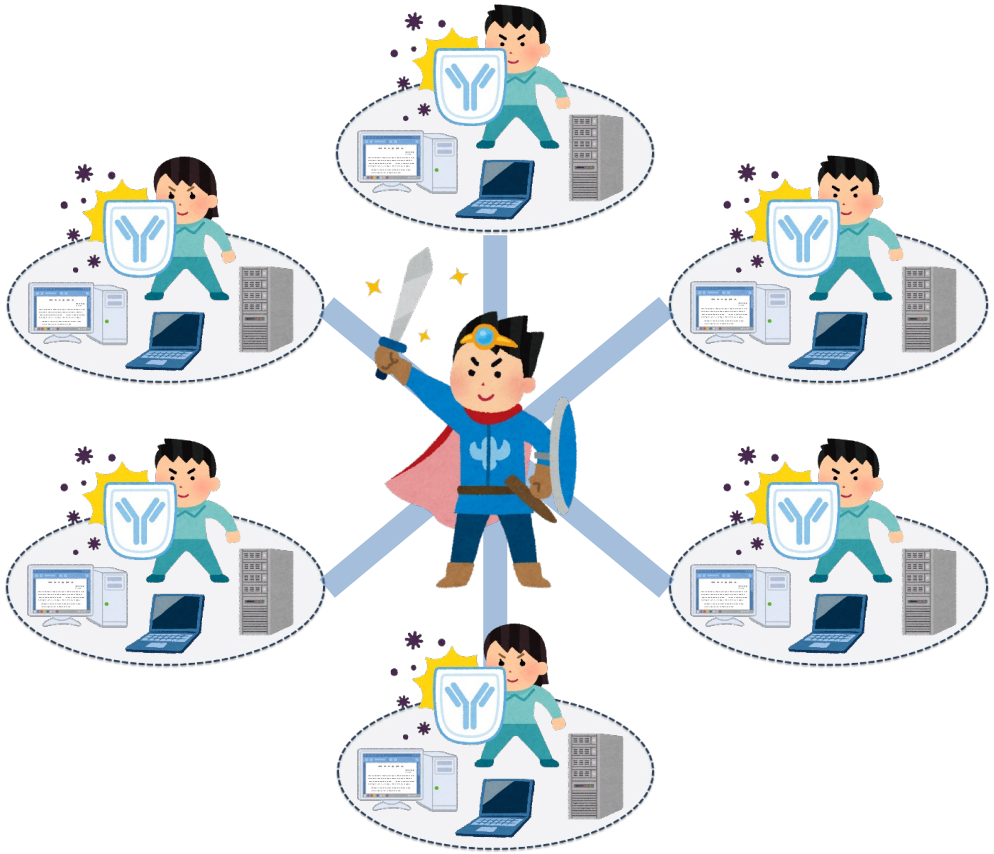
組織単独でのセキュリティ対策には限界が

ネクサス型



中小ユーザー企業のネクサス型

相談相手をみつける



IPA サイバーセキュリティお助け隊サービス

独立行政法人 情報処理推進機構（IPA）

サイバーセキュリティお助け隊サービス　IPA Better Life with IT

IT導入補助金で
「サイバーセキュリティお助け隊サービス」の
サービス利用料が支援対象となります！

サイバーセキュリティ CSお助け隊

IT導入補助金とは？

中小企業・小規模事業者のみなさまが
ITツール導入に活用いただける補助金です。
IT導入補助金で「サイバーセキュリティお助け隊サービス」
のサービス利用料の支援が受けられます。

▼ くわしくはこちら ▼

クイックアクセス

- サイバーセキュリティお助け隊 サービスリスト
- 紹介用 チラシ/パンフレット
- サイバーセキュリティ 対策カルタ
- お問い合わせ

事実　中小企業はサイバー攻撃の脅威にさらされている！

出典：令和２年度中小企業サイバーセキュリティ対策支援体制構築事業（サイバーセキュリティお助け隊事業）成果報告書（全体版）

CYNEX

CYBERSECURITY NEXUS

2023年10月1日 CYNEXアライアンス 発足

4つの“Co-Nexus”によるプロジェクト推進

47組織
参画中

CYNEX ALLIANCE

Co-Nexus A (Accumulation & Analysis)

28組織

- ✓各種観測機構によるデータ収集・蓄積
- ✓解析者コミュニティ醸成と共同分析の実現

Co-Nexus S (Security Operation & Sharing)

12組織

- ✓高度SOC人材育成（Online自主学習＆OJT）
- ✓国産脅威情報の生成・提供・情報発信

Co-Nexus E (Evaluation)

4組織

- ✓国産セキュリティ製品の長期運用・検証
- ✓国産セキュリティ製品へのフィードバック

Co-Nexus C (CYROP)

21組織

- ✓サイバーセキュリティ演習基盤のオープン化
- ✓演習環境の運用と演習教材の継続的開発

*CYROP: Cyber Range Open Platform

Co-Nexus Chairs


安田 真悟
NICT


毛利 公一
立命館大学


佐藤 隆行
日立製作所


久保 正樹
NICT


piyokango
セキュリティインコ

Walküre
CYNEX Red Team


安部 小百合
NICT

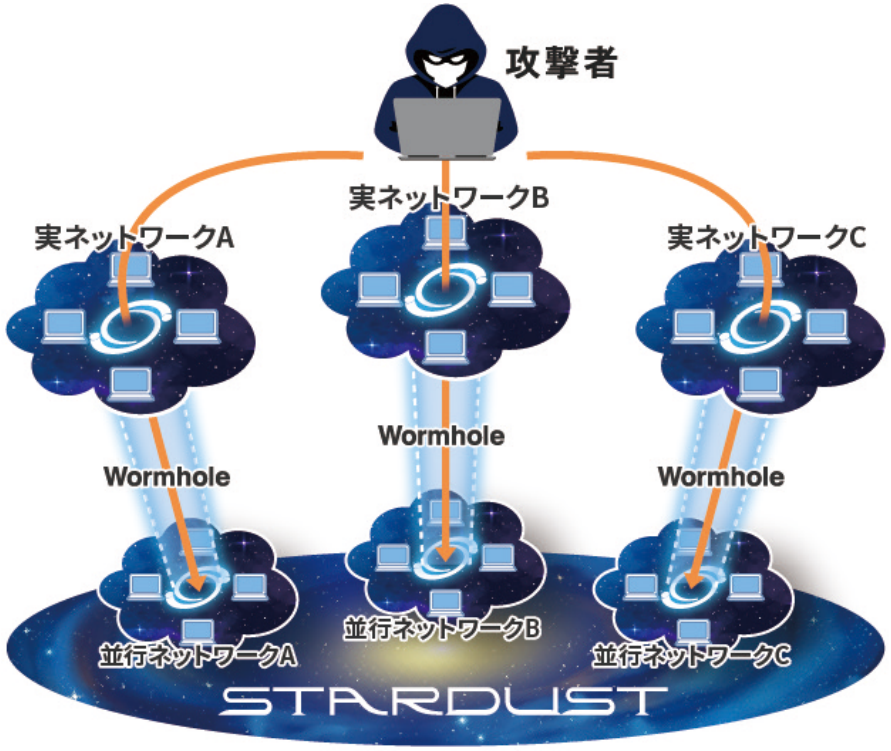

佐藤 公信
NICT


島 成佳
長崎県立大学


井田 潤
トレノケート

Co-Nexus A：STARDUST＆解析者コミュニティ形成

- STARDUST：人間の攻撃者を誘い込むサイバー攻撃誘引基盤
- 定常的な攻撃誘引の試行と解析結果を共有する解析者コミュニティの形成



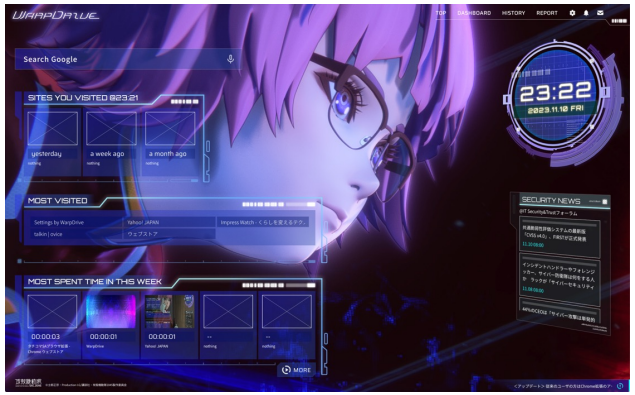
サイバー攻撃誘引基盤STARDUST NxtGen

● 活動状況

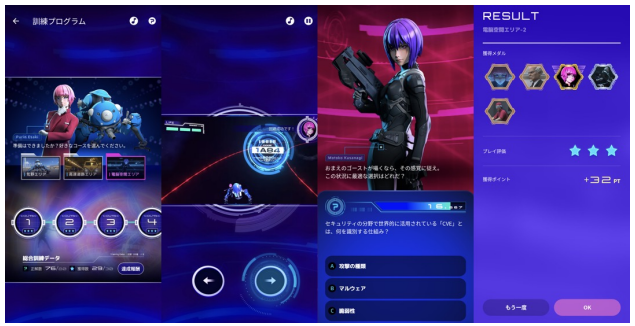
- ✓ STARDUST NxtGen 貸与
  - ✓ 参画組織が独自に標的型等マルウェア検体解析
- ✓ 年間300日以上の攻撃誘引実験
  - ✓ NICTの解析結果は積極的にコミュニティへ共有
- ✓ 解析者コミュニティ会合定期開催
  - ● 年4回開催+オンラインコミュニケーション基盤
  - ● 毎回90名程度の参加者

Co-Nexus A：WarpDriveプロジェクト

- WarpDrive：ユーザ参加型のWeb媒介型攻撃大規模観測プロジェクト
  - Web媒介型攻撃の対策確立のためのデータ収集・分析
  - タチコマ・セキュリティ・エージェント（PC/Android版）を無償配布



PC版
タチコマSA



Android版
タチコマモバイル

● 活動状況

✓ **第2弾アップデート**（2023/10/16 リリース）
- Android向けタチコマモバイルに**ゲーム機能を開発**
- クイズゲームでセキュリティやITの知識を反復学習

✓ **第3弾アップデート**（2024/1 リリース予定）
- PC向けタチコマSAにゲーム機能を追加
- Android向けに**ローカルスキャン機能を開発**
  - ➡ 家庭内のネットワークデバイスを発見可能に

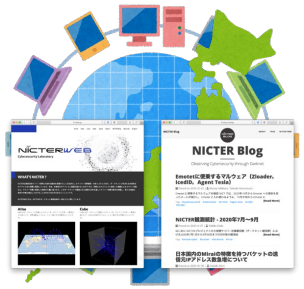
✓ **WarpDriveコミュニティ発足**
- 産学の研究機関が複数参画、データ解析や対策展開を加速

Co-Nexus S：高度SOC人材育成と国産脅威情報発信

- 自主学習型オンラインSOC研修とCYNEX解析チームでのOJT
- サイバーセキュリティ関連情報の発信と収集・生成データの外部提供

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

自主学習型オンラインSOC研修

am I infected?
横浜国立大学

● 活動状況

✓ **オンラインコース＆OJTコース**
- オンラインコース：3期生6名 修了、**4期生16名 研修中**
- OJTコース：CYNEX解析チームで1名修了、**1名育成中**

✓ **NICTERレポート, Blog, Twitter**
- NICTER観測レポートQ1, Q2, Q3, Q4
- NICTER観測レポート2023（2024/2 公開予定）
- NICTER Blog：5件、Twitter 随時更新

✓ **am I infected?***への情報提供

*横浜国立大学 情報・物理セキュリティ研究拠点が運営するマルウェア感染・脆弱性診断サービス

Co-Nexus E：国産セキュリティ製品の運用・検証

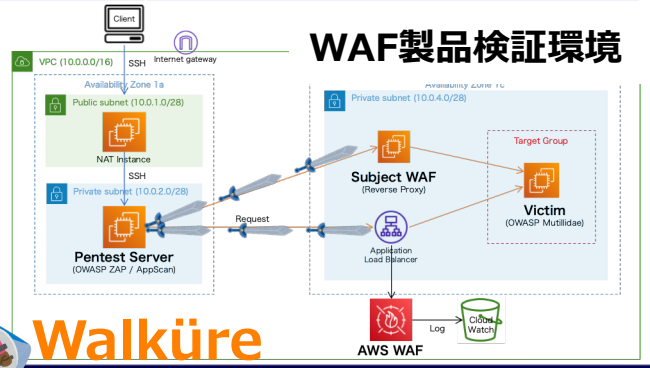
- 国産セキュリティ製品のテスト環境提供による実用化支援
  - NICT内部ネットワークにおける国産セキュリティ製品の長期運用・検証
  - Walküre（CYNEX Red Team）の模擬攻撃によるセキュリティ機能検証

国産セキュリティ製品検証リスト

製品種別	製品フェーズ	運用・検証の概要
ペネトレーションツール	商用化前技術	ツールの高度化及び長期運用
ファジングツール	商用化前技術	アルゴリズムの精度検証
IPレピュテーションサービス	商用化済技術	運用されている製品の精度検証 新たな分析軸の検証
ランサムウェア対策ソフト	商用化済技術	新たなマルウェアへの適応検証

IoT機器検証環境

WAF製品検証環境



Walküre

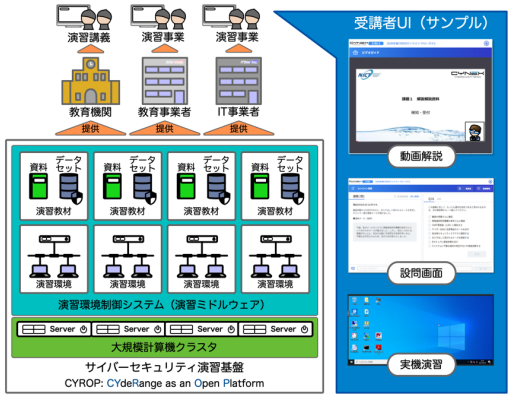
● 活動状況

- ✓ **国産製品の長期運用・検証**を実施
- ✓ 各製品ごとに**カスタム検証環境構築**
  - IoT機器検証環境、WAF製品検証環境、etc…
- ✓ **Walküre**による模擬攻撃の実施
- ✓ 海外有力製品群との**比較検証**
- ✓ 開発企業への**フィードバック**

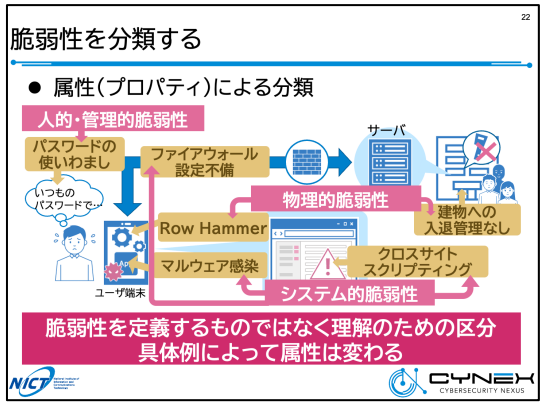
CYNEX CYBERSECURITY NEXUS

Co-Nexus C：人材育成オープンプラットフォーム

- 演習基盤開放による国内セキュリティ人材育成事業活性化
  - サイバーセキュリティ演習に必要となる演習環境と演習教材をオープン化
  - 産学官のニーズに基づき、NIST NICE Frameworkに沿って演習教材整備



サイバーセキュリティ演習基盤
CYROP (Cyber Range Open Platform)



CYNEXオリジナル演習教材

大学での演習教材利用事例

● 活動状況

✓ **CYROP基盤本格稼働開始**

✓ **３組織**が商用演習サービスを開始
- CYDER Aコース由来 演習教材（順次受け入れ）
- CYDER Bコース由来 演習教材（順次受け入れ）
- CYNEX オリジナル 演習教材（拡充中）

✓ **新規演習教材の共同開発**を実施
- 2021年：CYDERコンテンツ、パケット解析等（18種）
- 2022年：セキュリティ管理、ペンテスト等（18種）
- 2023年：**フォレンジック、OTセキュリティ（29種）**


CYNEX
CYBERSECURITY NEXUS


NICT
国立研究開発法人
情報通信研究機構