サイバー攻撃の動向と
サイバーセキュリティ研究・人材育成の最前線

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ネクサス ネクサス長
井上 大介

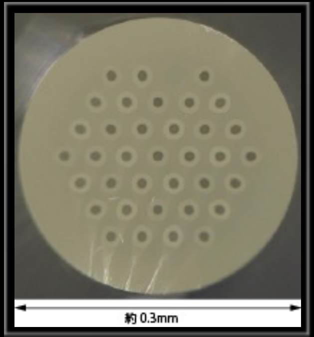
NICT National Institute of Information and Communications Technology

CYNEX CYBERSECURITY NEXUS

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）

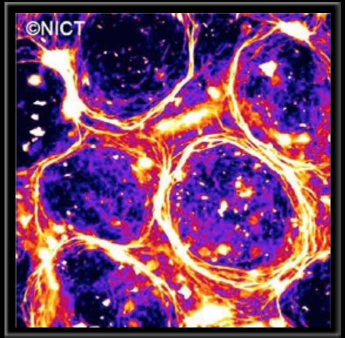


光通信システム
（ペタbps級 マルチコアファイバ）

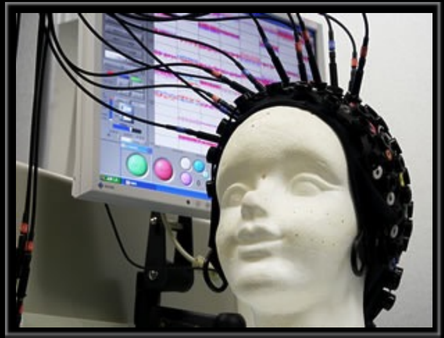
宇宙通信システム
（超高速インターネット衛星きずな）

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）



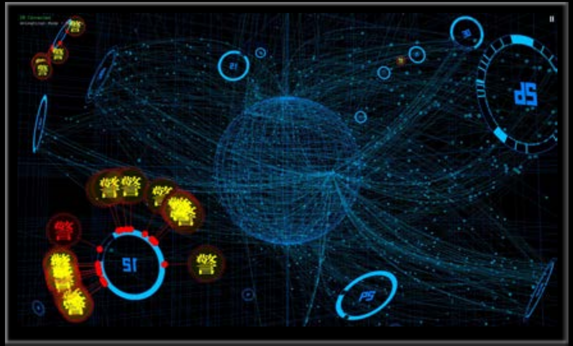
バイオ・ナノICT
（生体分子の自己組織化）



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）

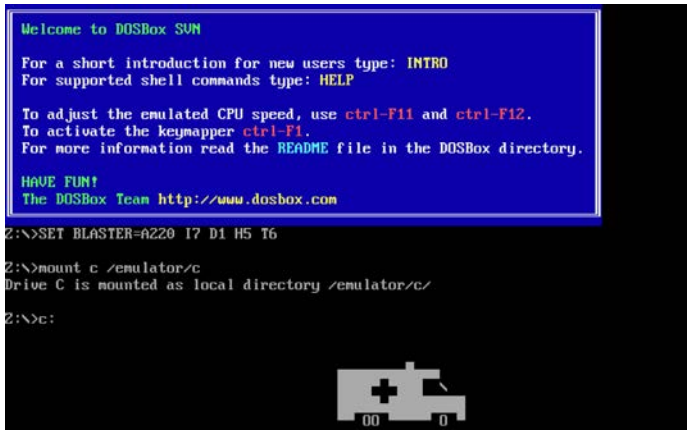


サイバーセキュリティ
（対サイバー攻撃アラートシステムDAEDALUS）

サイバー攻撃の動向

サイバー攻撃の変遷

- 20世紀：愉快犯



ウイルス Ambulance（1990）

感染すると画面上を救急車が走る

https://archive.org/details/malware_AMBULANC.COM

- 21世紀：経済犯

示威活動
諜報活動

ランサムウェア（2019）

身代金要求型ウイルス
米国の年間被害額75億ドル以上？

https://www.technologyreview.jp/nl/ransomware-may-have-cost-the-us-more-than-7-5-billion-in-2019/

過去14年間の主なセキュリティ事案

発生年	事案名
2008	Downadup (a.k.a. Conficker)
2009	Gumblar (a.k.a. GENO)
2010	Stuxnet
2011	標的型攻撃
2012	バンキングマルウェア
	遠隔操作ウイルス
2013	リフレクター攻撃
	アカウントリスト攻撃
2014	Heartbleed, Shellsock
	ベネッセ 個人情報漏洩
2015	Sony Pictures Entertainment への攻撃
	日本年金機構 年金情報漏洩

発生年	事案名
2016	JTB 顧客情報漏洩
	超大規模DDoS攻撃
2017	Apache Struts2
	WannaCry ①
2018	パスワード大量流出
	仮想通貨マイニングツール設置
2019	NASAへのサイバー攻撃 ②
	Emotet
2020	医療機関を狙った標的型ランサムウェア ③
	SolarWindsへのサプライチェーン攻撃 ④
2021	米石油パイプライン企業のランサムウェア感染
	Kaseya VSAへのサプライチェーン攻撃

リモート感染型ランサムウェア

WannaCry (1/2)

- **2017年3月14日 Microsoft セキュリティ情報 MS17-010公開**
  - SMBv1にリモートコード実行可能な脆弱性
  - 感染対象：Windows Vista/7/8.1/10
    Windows Server 2008/2008 R2/2012/2012 R2/2016
    Windows XP/XP Embedded/8, Windows Server 2003（サポート終了）

- **2017年5月12日 WannaCry感染キャンペーン開始**

WannaCry感染画面（英語版出典：Symantec）

https://www.symantec.com/security_response/writeup.jsp?docid=2017-051310-3522-99

WannaCry感染画面（日本語版出典：IPA）

https://www.ipa.go.jp/security/ciadr/vul/20170514-ransomware.html

リモート感染型ランサムウェア

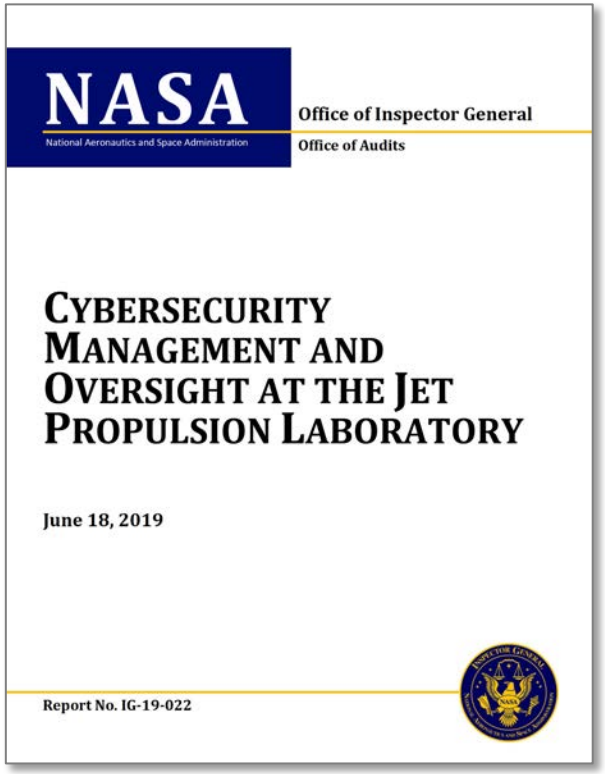
WannaCry (2/2)

- **感染後の挙動**（出典： https://piyolog.hatenadiary.jp/entry/20170513/1494700355 ）
  - 166種類の拡張子のファイルを暗号化
  - 暗号化処理後、ボリュームシャドーコピーの削除
  - デスクトップに下記の身代金要求を表示（300 US$）
  - 3日以内に支払いがなければ要求金額は倍に
  - 7日以内に支払いがなければデータ削除と脅迫
  - LANとInternetにCVE-2017-0145を用いた感染活動

出典：BLEEPINGCOMPUTER “People Are Photoshopping WannaCry Ransom Notes on Everything with a Screen”
https://www.bleepingcomputer.com/news/security/people-are-photoshopping-wannacry-ransom-notes-on-everything-with-a-screen/

NASAへのサイバー攻撃

- NASAのジェット推進研究所（JPL）から機密データ漏洩
- 無許可接続されたRaspberry Piが原因（野良IoT）



NASA
National Aeronautics and Space Administration

Office of Inspector General
Office of Audits

CYBERSECURITY MANAGEMENT AND OVERSIGHT AT THE JET PROPULSION LABORATORY

June 18, 2019

Report No. IG-19-022

itmedia.co.jp

NASA、サイバー攻撃で機密データ流出　侵入口は無許可接続の「Raspberry Pi」 - ITmedia NEWS

ITmedia NEWS > セキュリティ > NASA、サイバー攻撃で機密データ流出　侵入口は無許...

NASA、サイバー攻撃で機密データ流出　侵入口は無許可接続の「Raspberry Pi」

2019年06月23日 07時45分 公開　[ITmedia]

印刷　1905　Share　B!　828

米航空宇宙局（NASA）のジェット推進研究所（JPL）の研究データが昨年、サイバー攻撃により盗まれていたことが、米連邦政府の監察総監室（OIG）が6月18日付で公開した報告書（リンク先はPDF）で明らかになった。

2018年4月にJPLのネットワークに侵入した攻撃者が約10カ月の間ネットワーク内の多数の脆弱性を利用して行動範囲を広げ、火星科学研究探査機のデータを含む約500MBの機密データを盗んだ。深宇宙通信情報網DSN（ディープスペースネットワーク）のデータにもアクセスした痕跡があるため、JPLのネットワークからDSNの宇宙飛行関連システムを切断したという。

DSNのパラボラアンテナ（画像：NASA）

攻撃者の侵入口はJPLのネットワークに無許可で接続していたRaspberry Pi端末だった。本来ならば最高情報責任者室（OCIO）がネットワークに接続するすべての端末を管理しているはずだが、正常に機能していなかった。管理者の1人はOIGに対し、新たに端末を接続する際はセキュリティデータベースに手動で登録することになっているが、更新機能がうまく動かないことがあり、そのまま登録を忘れることがあると語ったという。

gigazine.net

NASAの機密データがRaspberry Piを侵入口として盗まれたと判明 - GIGAZINE

GIGAZINE

19万点超 著作権フリー音楽
日本最大級のBGM・効果音販売サービス「オーディオストック」 - Audiostock

2019年06月25日 19時00分　セキュリティ

NASAの機密データがRaspberry Piを侵入口として盗まれたと判明

by Les Pounder

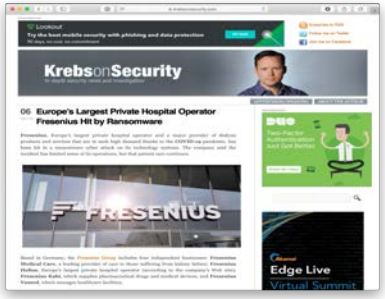
アメリカ航空宇宙局(NASA)は、2018年にジェット推進研究所(JPL)のネットワークがハッキングされたことを確認しました。報告によると、ハッキングをしかけたクラッカーは、JPLのネットワークに無許可で接続されたRaspberry Piを侵入口として、データを盗み出したとのことです。

"https://www.flickr.com/photos/biglesp/14234773312/"を新規タブで開く

https://oig.nasa.gov/docs/IG-19-022.pdf
https://www.itmedia.co.jp/news/articles/1906/23/news012.html
https://gigazine.net/news/20190625-nasa-hacked-raspberry-pi/

医療機関を狙った標的型ランサムウェア

- **ランサムウェア**：感染端末のデータを暗号化し**復号の見返りに金銭を要求するマルウェア**
- 医療機関をターゲットにした**標的型ランサムウェア**の出現
  - ✓ 2016年：米国Hollywood Presbyterian Medical Center ➡ 1万7000ドルの身代金を支払いデータ復旧
  - ✓ 2018年：奈良県宇陀市立病院 ➡ 電子カルテシステムの利用が不可能に
- 欧州最大の**民間病院運営会社『Fresenius』**がランサムウェアに感染（2020年5月）
  - ✓ Freseniusは過去にもマルウェア感染し150万ドルを支払ったことがあるらしい[#1]
  - ✓ INTERPOL[#2]とDHS[#3]から医療機関を狙った標的型ランサムウェアに注意喚起[#4]
- デュッセルドルフ大学病院で**ランサムウェアによる初の死亡例**？（2020年9月）
  - ✓ 院内のITシステムへのマルウェア感染で患者の緊急搬送を受け入れられず移送先で死亡

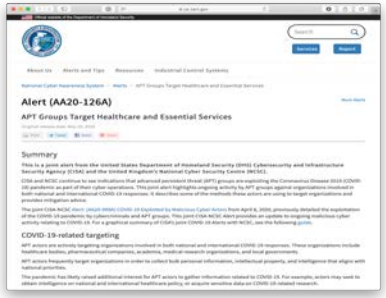


[#1] Krebs on Security

https://krebsonsecurity.com/2020/05/europes-largest-private-hospital-operator-fresenius-hit-by-ransomware/

[#2] INTERPOL

https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware



[#3] DHS

https://www.us-cert.gov/ncas/alerts/AA20126A

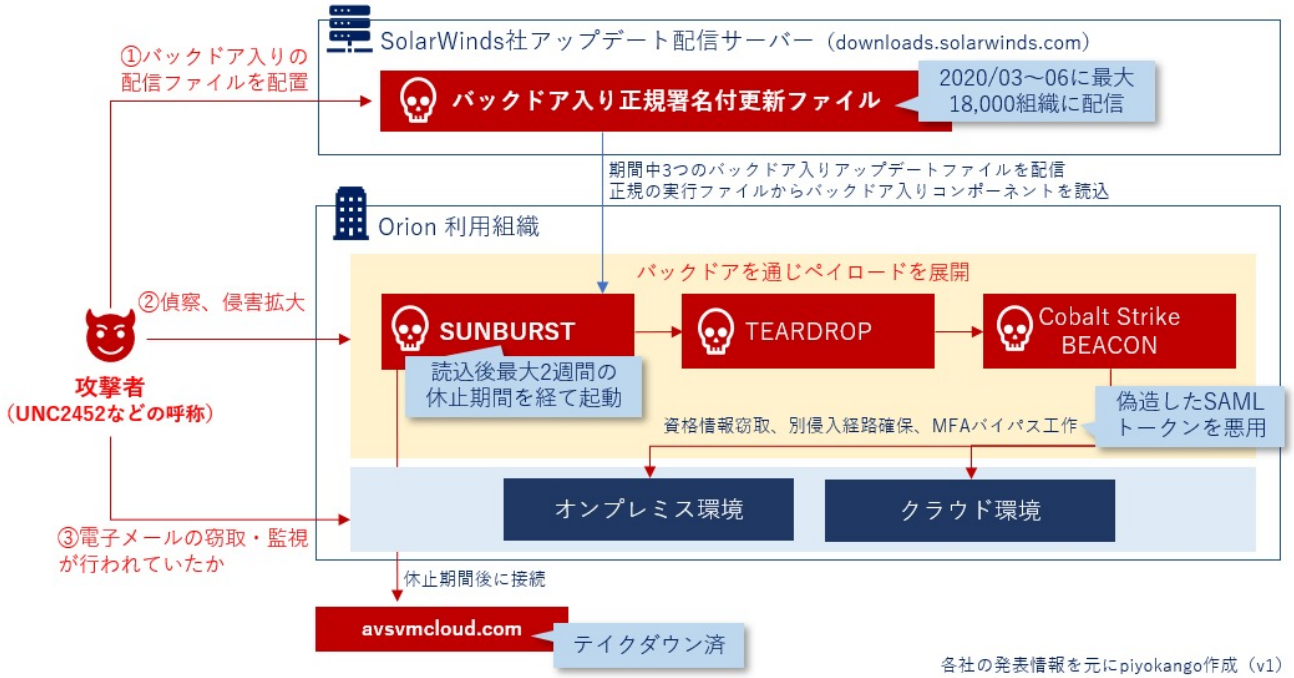
[#4] ZDNet

https://japan.zdnet.com/article/35159781/

SolarWindsへのサプライチェーン攻撃

- 米国SolarWinds社のリモート監視ツール『Orion Platform』にバックドアが仕込まれる
  - ✓ 2020年3月～6月：同社のアップデート配信サーバからバックドア入り更新ファイルが配布される
  - ✓ 2020年12月8日：FireEye社が当該バックドア経由のRedTeam用ツールの窃取を公表

- 米国の多数の組織に影響
  - ✓ Cisco, Nvidia, Intel, Deloitte, VMware, 米国財務省, 商務省, 国防総省, 国土安全保障省, 国務省, 司法省, etc.



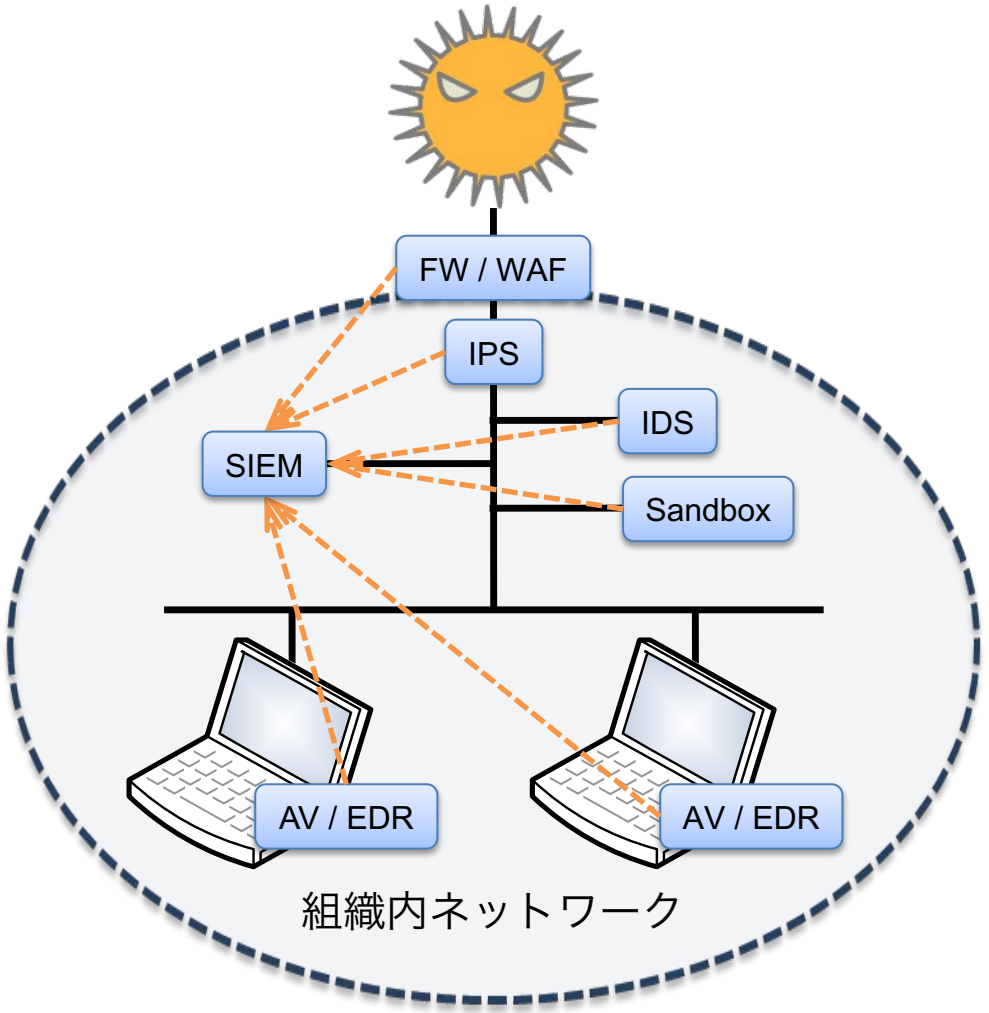
出典： https://piyolog.hatenadiary.jp/entry/2020/12/20/045153

近年のセキュリティ事案のまとめ

- **攻撃手法は多様化**
  - ✓ 無差別型攻撃、標的型攻撃、ドライブバイダウンロード
  - ✓ ランサムウェア、サプライチェーン攻撃、etc.
- **攻撃対象も多様化**
  - ✓ 一般ユーザ、企業、重要インフラ、政府官公庁、etc.
- **インターネットの根幹技術を攻撃に転用**
  - ✓ DNS、NTP、etc.
- **どの攻撃も根絶に至っていない**
  - ✓ 依然Ongoingな脅威

セキュリティ対策技術の動向

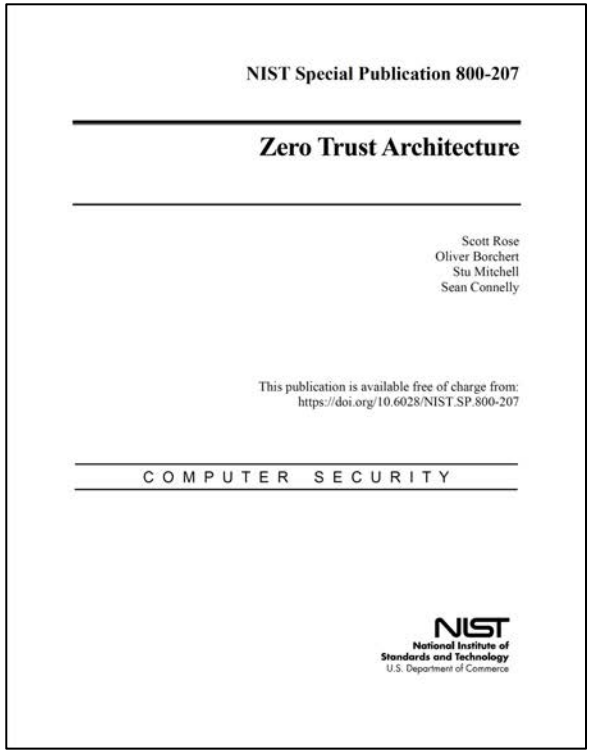
- **FW / WAF**（ファイアウォール / Webアプリケーションファイアウォール）
  - ✓ Network層/Transport層/Application層で**パケット通過の可否**を判定
  - ✓ 導入方法：インライン
- **IDS**（侵入検知システム：Intrusion Detection System）
  - ✓ シグネチャで攻撃を**検知（アラート）**
  - ✓ 導入方法：ポートミラーリング or TAP
- **IPS**（侵入防止システム：Intrusion Prevention System）
  - ✓ シグネチャで攻撃を**防止（遮断）**
  - ✓ 導入方法：インライン
- **Sandbox**（箱庭環境）
  - ✓ 仮想環境でファイルを実行し**マルウェア検知**
  - ✓ 導入方法：ポートミラーリング or TAP
- **AV / EDR**（アンチウイルス / Endpoint Detection and Response）
  - ✓ シグネチャベースで**マルウェア検知**、端末内の**各種情報を収集・対応**
  - ✓ 導入方法：PC等の端末内にインストール
- **SIEM**（Security Information and Event Management）
  - ✓ 各種セキュリティ機器からの**ログやアラートを集約して一元管理**
  - ✓ 導入方法：組織内ネットワークに適宜設置



ゼロトラスト・アーキテクチャ

- **従来型：境界防御**
  - ✓ ネットワークを内と外で分け、組織内のネットワークという場所を静的に保護
  - ✓ 問題点：攻撃者の侵入をネットワーク境界で完全に防ぐことは難しい
  - ✓ 問題点：クラウドや仮想環境の利用拡大でネットワーク境界が曖昧に

- **ゼロトラスト・アーキテクチャ（ZTA）**
  1. データソースや計算サービスなどのリソースが保護対象
  2. 全ての通信の安全性確保
  3. セッション単位のリソースへのアクセス許可
  4. 動的なポリシによるリソースへのアクセス判断
  5. 全ての機器の監視と計測
  6. アクセス前の認証・認可の動的・厳格な実施
  7. 機器の状態やインフラ・通信状態の情報収集


NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST, “SP 800-207, Zero Trust Architecture,” August, 2020.
https://csrc.nist.gov/publications/detail/sp/800-207/final

サイバーキュリティ研究の最前線

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
(ア) データ駆動型サイバーセキュリティ技術
(イ) エマージングセキュリティ技術

(2) 暗号技術
(ア) 安全なデータ利活用技術
(イ) 量子コンピュータ時代に向けた暗号技術の安全性評価

(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


盛合 志帆 所長


中尾 康二 主管研究員

セキュリティ基盤研究室


野島 良 室長

サイバーセキュリティ研究室


井上 大介 室長

CYNEX
サイバーセキュリティネクサス


井上 大介 ネクサス長

ナショナルサイバートレーニングセンター


園田 道夫 センター長

サイバートレーニング研究室


花田 智洋 室長

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


盛合 志帆センター長

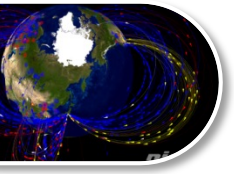
サイバーオブザベーション運用室


井上 大介 室長

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

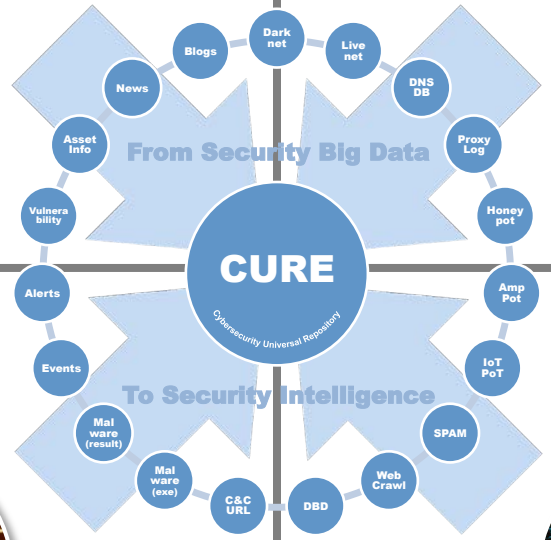
脆弱性管理プラットフォーム（ニルヴァーナ・カイ・ニ）
NIRVANA改弐

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

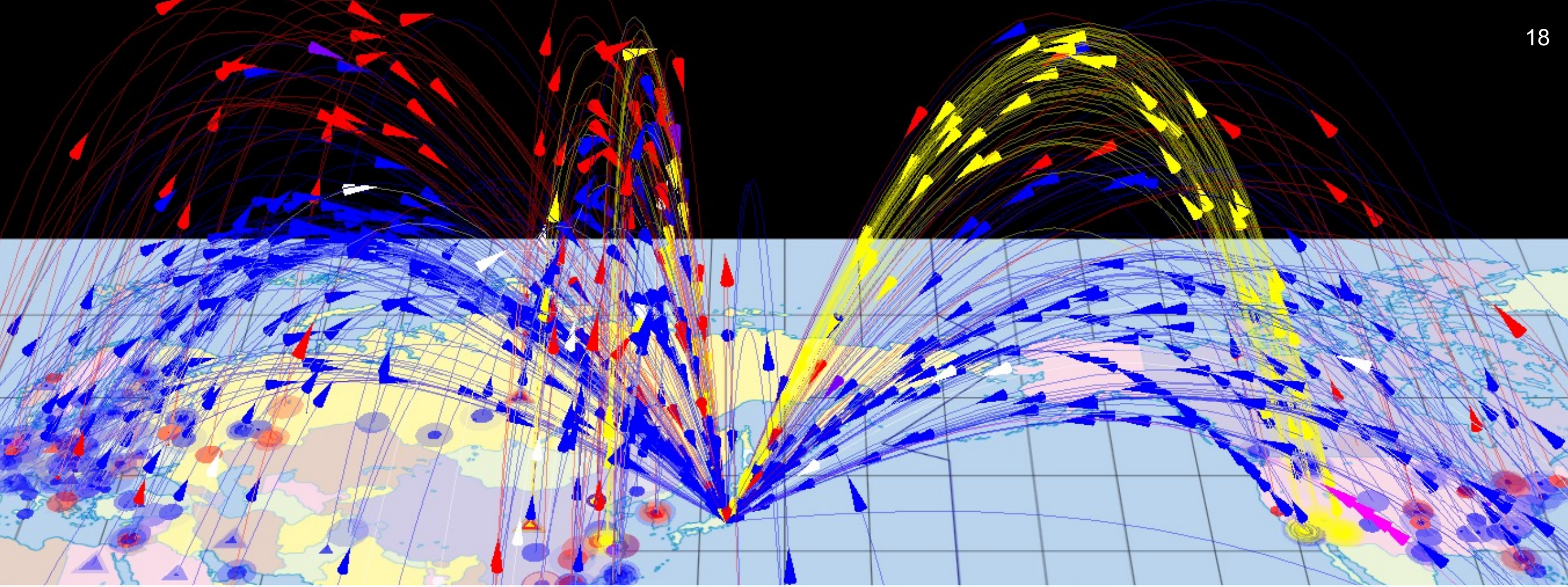
Active

NICT National Institute of Information and Communications Technology

CYNEX CYBERSECURITY NEXUS

インシデント分析センター

Network **I**ncident analysis **C**enter for **T**actical **E**mergency **R**esponse



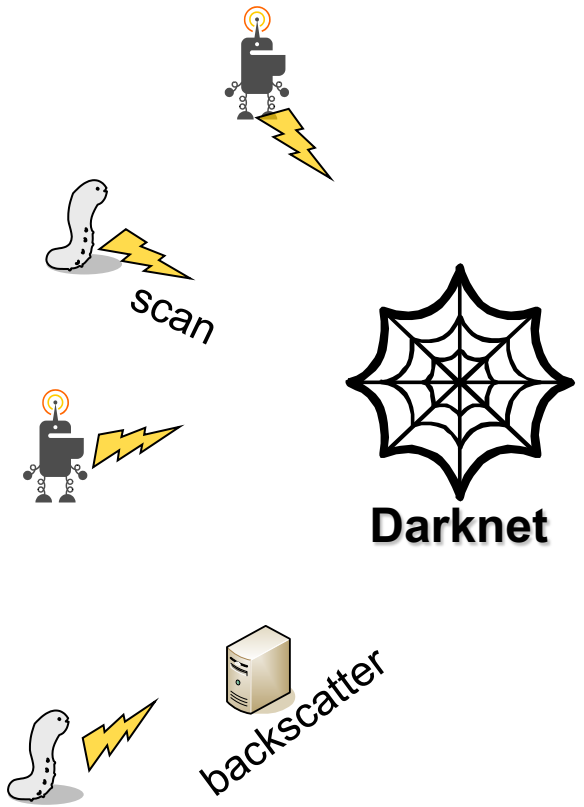
NICTER

- 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

ダークネットとは？

- **ダークネット = 未使用IPアドレスブロック**
  - ✓何もない所にパケットが飛んでくること自体おかしい

- **ダークネットで見えるもの**
  - ✓インターネット上で何かを探す行為
    - ワーム型マルウェアによるスキャン
    - DRDoSのリフレクタ探索（DNS Open Resolver、NTP etc.）
    - セキュリティ関連組織等による調査
  - ✓DoS攻撃の跳ね返り
    - DDoSバックスキャッタ
      ※ 送信元IPアドレス偽装されたSYN Floodへの応答
    - DNS水責め攻撃のバックスキャッタ
      ※送信元IPアドレス偽装されたランダムサブドメイン攻撃
  - ✓設定ミス



NICTERダークネット観測統計（過去10年）

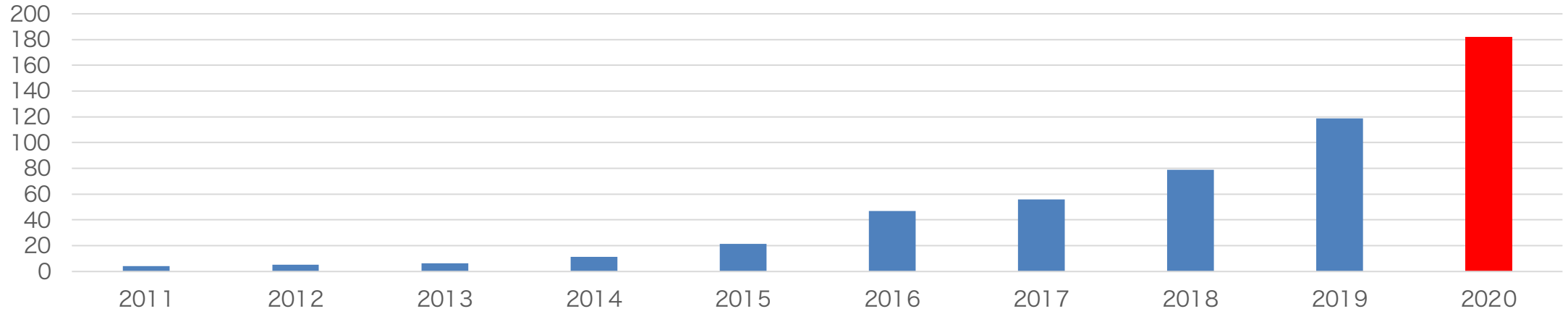
年	年間総観測パケット数	ダークネットIPアドレス数	1 IPアドレス当たりの年間総観測パケット数
2011	約45.4億	約12万	40,654
2012	約77.8億	約19万	53,085
2013	約128.8億	約21万	63,655
2014	約256.6億	約24万	115,323
2015	約545.1億	約28万	213,523
2016	約1,281億	約30万	469,104
2017	約1,504億	約30万	559,125
2018	約2,121億	約30万	789,876
2019	約3,220億	約30万	1,187,935
2020	**約5,001億**	**約30万**	**1,820,722**

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）

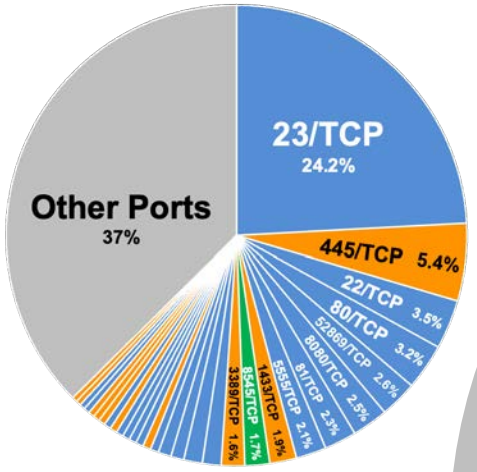


1 IPアドレス当たりの年間総観測パケット数

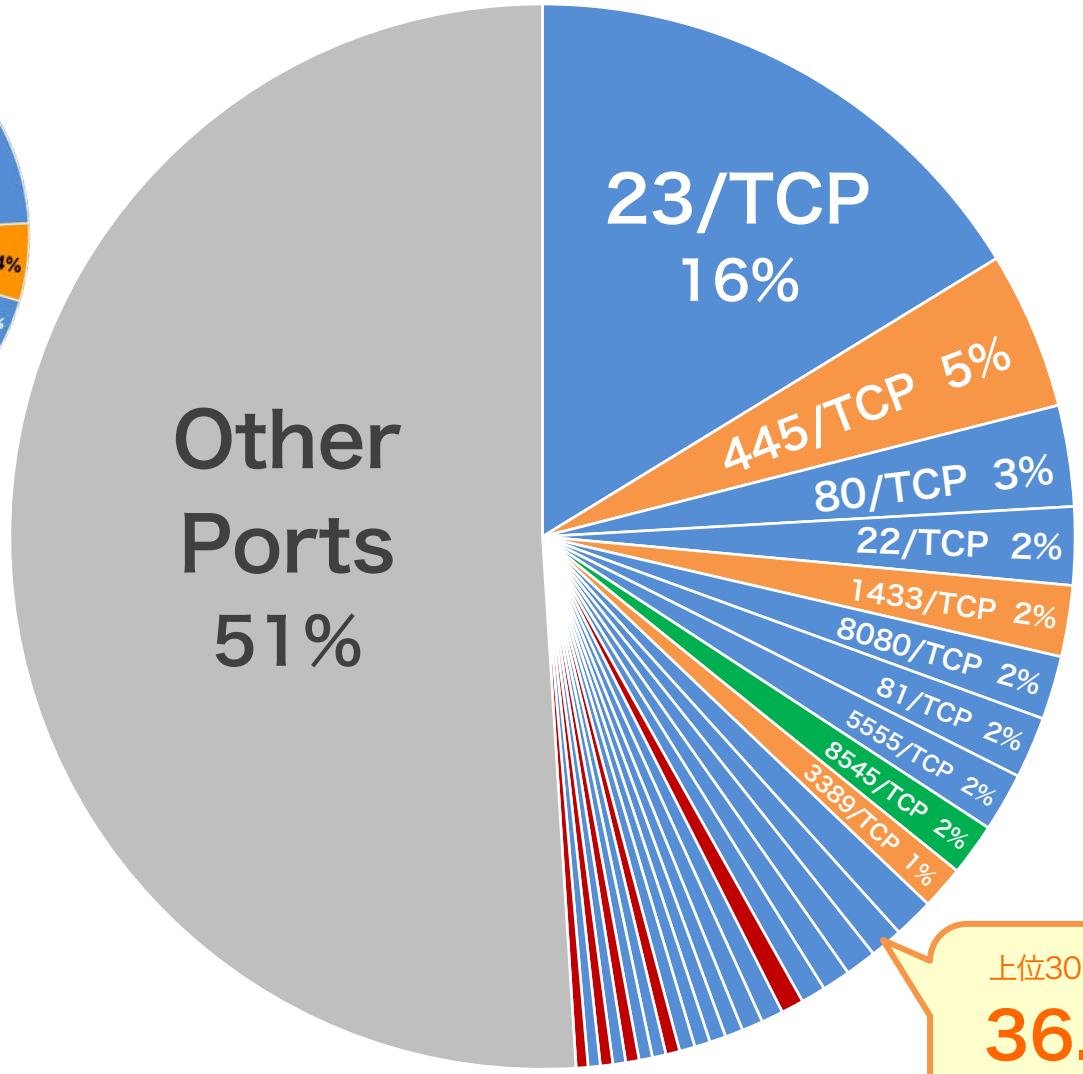
横浜国立大学
吉岡研究室による調査

感染機器の分布（2020年）

- NICTER 観測レポート 2020：宛先ポート番号別パケット数分布 -



2019年



2020年

ポート番号	攻撃対象
23/TCP	IoT機器 （Webカメラ等）
445/TCP	Windows（サーバサービス）
80/TCP	Webサーバ（HTTP） IoT機器（Web管理画面）
22/TCP	IoT機器（ルータ等）
1433/TCP	Windows (MS-SQL)
8080/TCP	IoT機器（Webカメラ等）
81/TCP	IoT機器（ホームルータ等）
5555/TCP	Android 機器 (セットトップボックス等)
8545/TCP	イーサリアム（仮想通貨）
3389/TCP	Windows (リモートデスクトップ)

上位30ポート中
36.9%
がIoT機器への攻撃

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）

NICT National Institute of Information and Communications Technology

CYNEX CYBERSECURITY NEXUS

NICTER 観測情報の利活用

nicter.jp

● セキュリティ関連組織への観測情報提供

- ✓ **定点観測友の会（SIGMON）**
  - JPCERT/CC、IPA、@Police等との観測結果共有（2004年～）
- ✓ **DoS攻撃即応-WG**
  - ICT-ISAC JapanとのDoS攻撃関連情報共有（2011年～）
- ✓ **オリパラ体制検討会**
  - NISC、オリパラ組織委員会等との攻撃関連情報共有（2015年～）
- ✓ **サイバーセキュリティ協議会**
  - NISC、関連組織との情報共有に第二類構成員として参画（2019年～）

● 観測情報一般公開

- ✓ NICTER Web (http://www.nicter.jp/)
- ✓ NICTER Blog (http://blog.nicter.jp)
- ✓ NICTER 観測レポート (http://www.nict.go.jp/cyber/report.html)

NICTERWEB

CYNEX CYBERSECURITY NEXUS

NICT National Institute of Information and Communications Technology

今すぐできる！ IoT機器セキュリティ対策 6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）

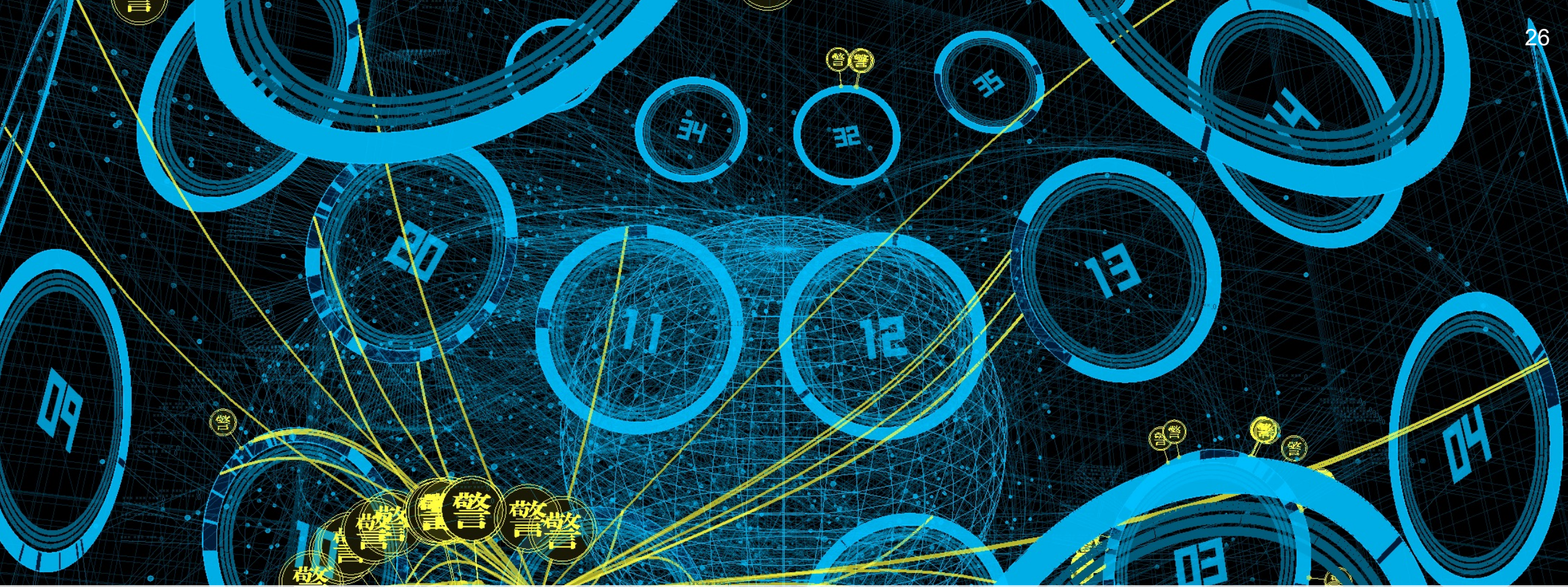
4. インターネット側からのアクセス拒否設定（外から繋がせない）
5. ゲートウェイ機器の内側に設置（直接インターネットに繋がない）
6. 古い機器は買い換える（自動アップデート機能がない機器はNG）

GOOD DESIGN AWARD 2013

対サイバー攻撃アラートシステム

DAEDALUS

Direct **A**lert **E**nvironment for **D**arknet **A**nd **L**ivenet **U**nified **S**ecurity



DAEDALUS

- 大規模ダークネット観測に基づく“アラートシステム”
- 組織内のウイルス感染端末からの攻撃を検知
- 約600の地方自治体にアラート無償提供中

境界防御技術とDAEDALUS

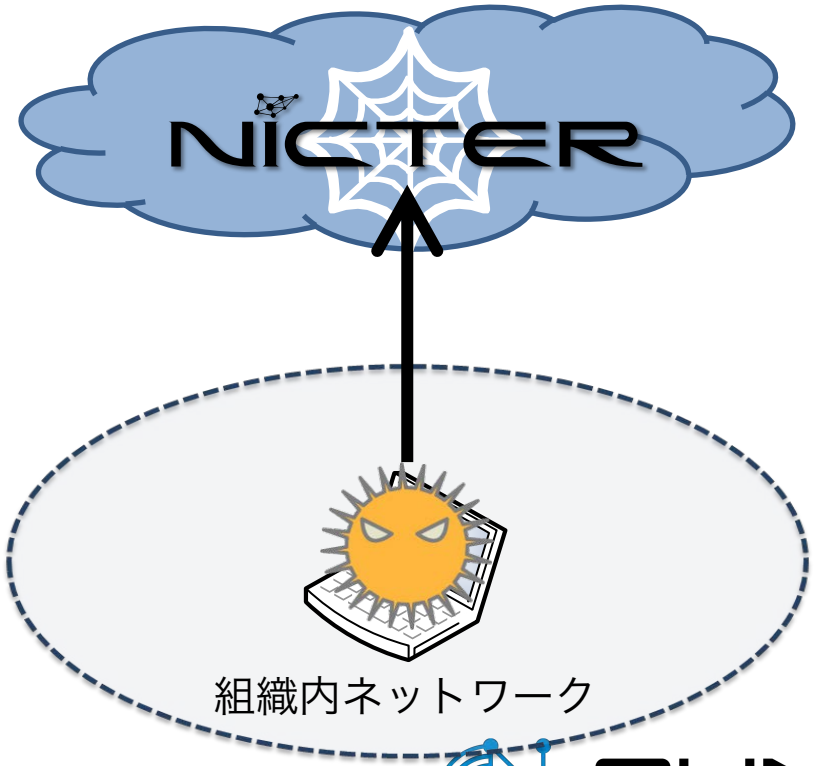
境界防御技術（従来技術）

組織外からの攻撃をネットワーク境界で検出

相補的

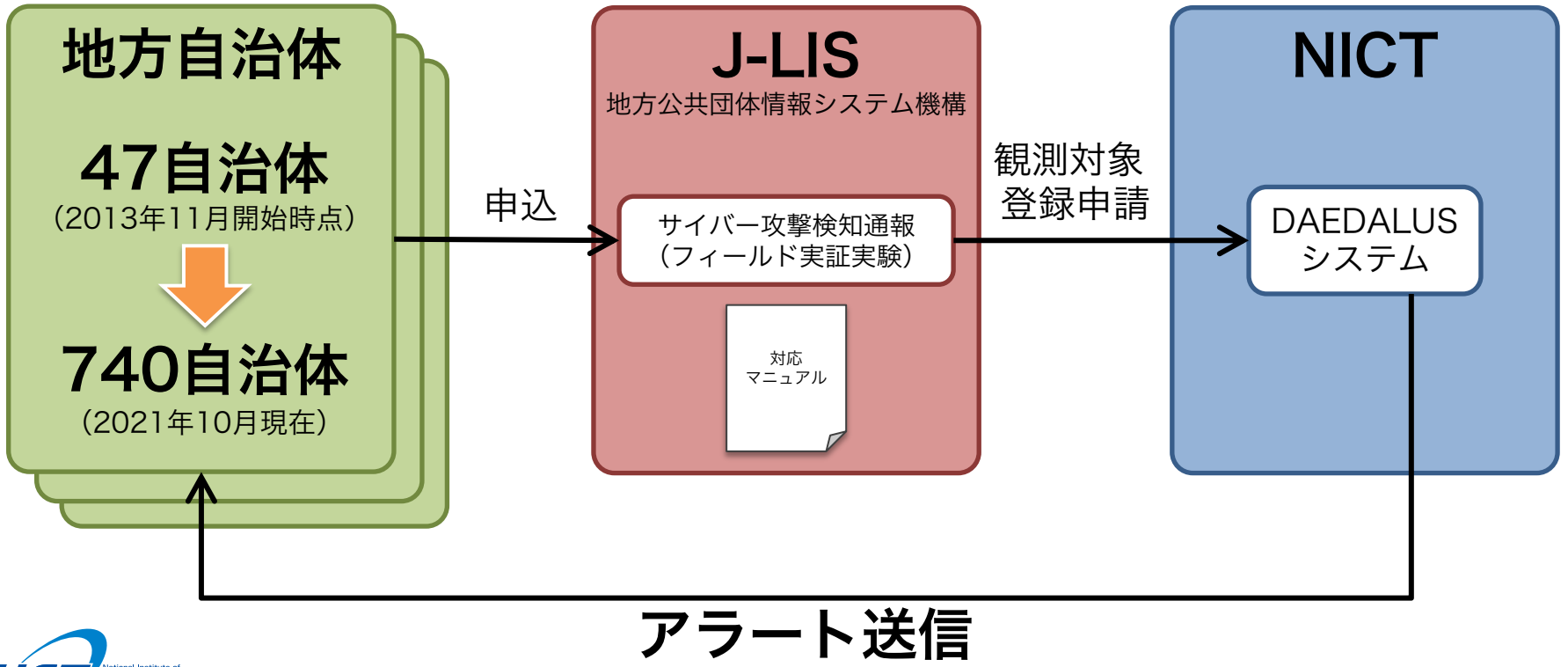
DAEDALUS

組織内からの攻撃をネットワーク広域で検出



地方自治体へのアラート提供

- **2013年11月1日より、地方自治体に向けてアラート送信開始**
  - ✓地方公共団体情報システム機構（J-LIS）を窓口として自治体より申込受付
  - ✓アラート発生時の対応マニュアルをNICTとJ-LISで整備



サイバー攻撃検知通報

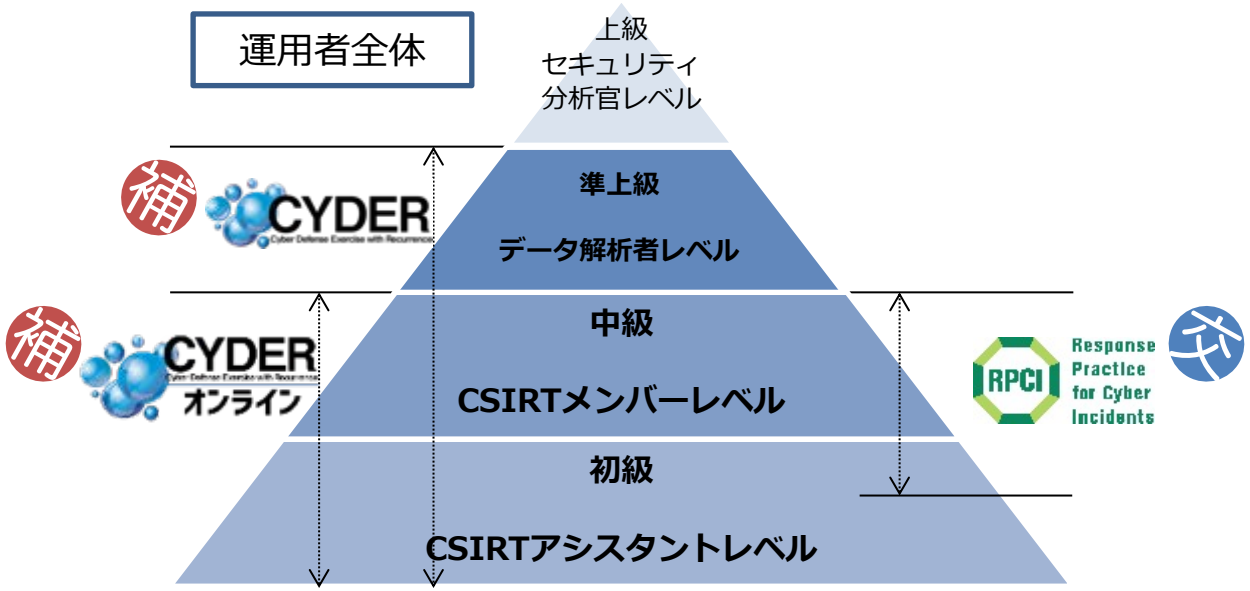
ナショナルサイバートレーニングセンター

ナショナルサイバートレーニングセンターにおける人材育成

情報通信分野を専門とする我が国唯一の公的研究機関である**NICTの技術的知見、研究　成果、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、「ナショナルサイバートレーニングセンター」を設置（2017年4月1日）

セキュリティオペレーター（実践的運用者）の育成

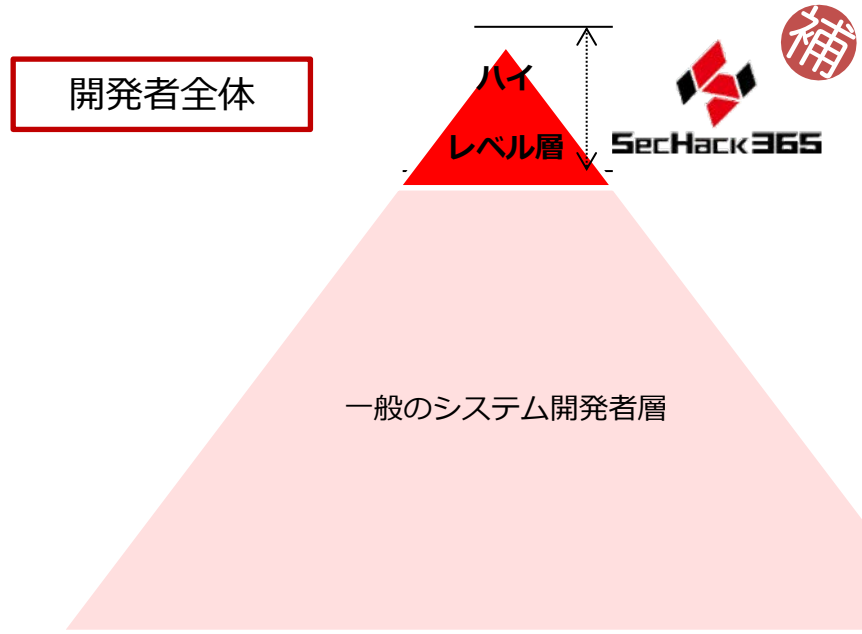
- **行政機関や民間企業等の組織内のセキュリティ運用者（情報システム担当者等）を対象**
- **所属組織が深刻なサイバー攻撃を受けた段階等（＝「有事」）における実践的なインシデント対応能力を育成**



※CSIRT（シーサート）：Computer Security Incident Response Team

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**



交 運営費交付金による事業　　補 補助金による事業

National Cyber Training Center

実践的サイバー防御演習「CYDER」 2021年度概要

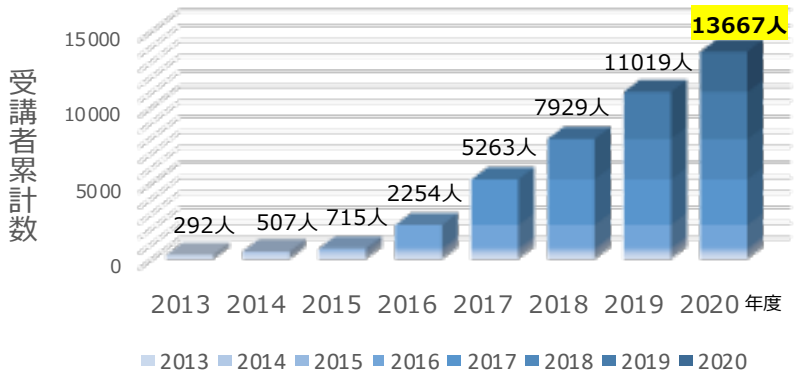
国の機関、地方公共団体及び重要インフラ事業者等の情報システム担当者等が、組織のネットワーク環境を模擬した環境で、実践的な防御演習を行うことができるプログラムを提供することにより、数千人規模でセキュリティオペレーターを育成

2021年度コース概要

- 毎年 **約 3,000人が受講**
- 演習は1日間 (Cコースは2日間)
- 集合 (実地) 演習のほか、**オンライン演習コース (個人演習) を新設**
- 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/オンラインAコース … 77,000円 (税込)
  Cコース … 121,000円 (税込)

CYDER受講者数の推移 (累積数)



2021年度実施内容および対象組織

	コース	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
	A	集合演習	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	65回
	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	21回
	B-2				地方公共団体以外	全国4都市	13回
新規	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	2回
新規	オンラインA	オンライン演習	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	受講者職場等	-

※CYDERは、(ISC)² が提供する資格の認定継続に必要なCPEクレジット (継続教育単位) 付与対象の演習

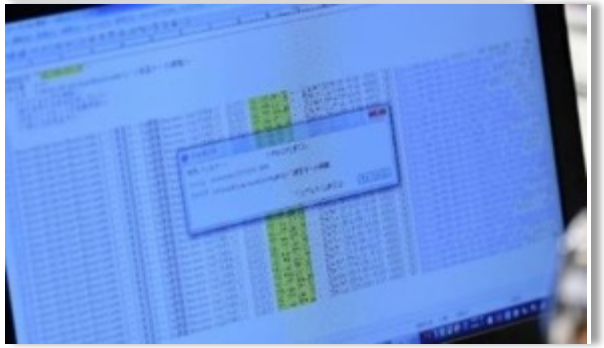
National Cyber Training Center

実践的サイバー防御演習「CYDER」の演習風景（2019年度）

オリエンテーション

演習フロー説明

インシデント発生～事実確認



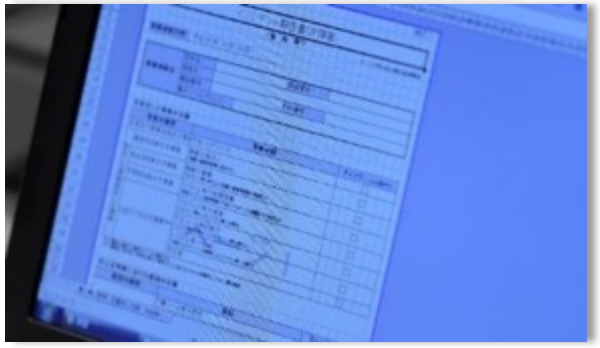
チューターによるサポート

マルウェア挙動調査

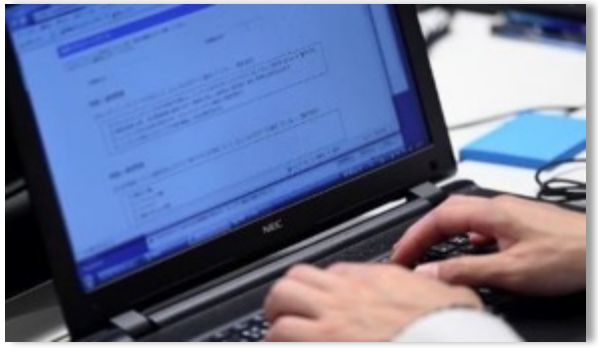
グループワーク

発表

報告書作成



確認テスト



National Cyber Training Center

実践的サイバー防御演習「CYDER」の演習風景（コロナ対策後）

National Cyber Training Center

情報処理安全確保支援士向け特定講習　実践サイバー演習「RPCI」概要

NICTが持つ大規模演習環境を活用してリアリティを高めたインシデントハンドリング演習。
公的機関初の**情報処理安全確保支援士向け特定講習**[*1]として、提供開始予定。

[*1]特定講習: セキュリティに係る最新の知識・技能を備えた専門人材の国家資格「情報処理安全確保支援士（登録セキスペ）」の更新にあたり、3年に1回受講が必要となる講習で、経済産業大臣が定めるもの。（詳細：https://www.meti.go.jp/policy/it_policy/jinzai/tokutei.html）

講習名称	実践サイバー演習「RPCI（リプシィ）」 ～大規模演習環境を活用してリアリティを高めたインシデントハンドリング演習～		
対象者	情報処理安全確保支援士、その他サイバー防御演習に関心のある方など		
講習形態	事前オンライン学習と集合演習（ハンズオン＆グループワーク形式）		
受講日数	1日間	定員（1回あたり）	16名[*2]
受講料	88,000 (円/税込)	受講時間	8.5時間
対象分野	主な分野：デジタルプロダクト運用	関連分野	脆弱性診断・ペネトレーションテスト
開催日程	8月・・・25日（水）、28日（土） 9月・・・2日（木）、4日（土）、7日（火）、11日（土）、16日（木）、18日（土）、28日（火） 10月・・・8日（金）		
開催会場	NICTイノベーションセンター（千代田区大手町）		

[*2] 新型コロナ感染症対策等により、1回あたりの定員を減らして実施

習得できるスキル

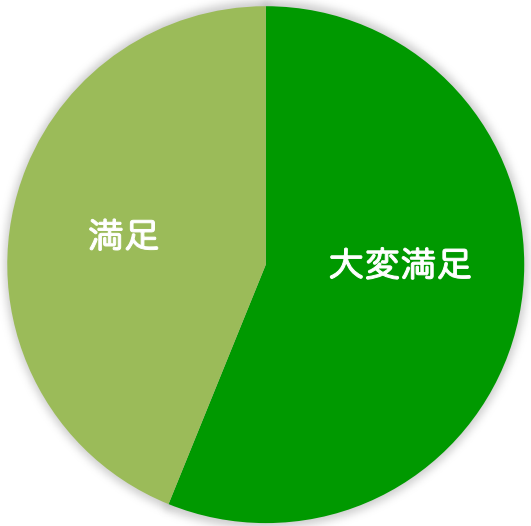
- **Wiresharkを利用した特定のプロトコルのパケット解析**
- **Nmapを利用したネットワークアクセスコントロールの適正動作確認**
- **Hydraを利用した、自らが管理するネットワーク機器への侵入試験**
- **ネットワーク機器への侵入リスク軽減策等の説明能力**
- **CISOに対する優先度をつけた再発防止策の提案**

新型コロナ感染症対策

- **会場入り口での検温**
- **新型コロナの代表的症状がないことを確認、誓約書の提出**
- **CO2センサーにて換気状況を測定**
- **サーキュレーターを使用した室内の換気**

[参考] 実践サイバー演習「RPCI」アンケート結果

講習の満足度をお聞かせください（大変満足 5 – 4 – 3 – 2 – 1 不満足）



満足度

100%

受講者全員が大変満足・満足と回答

- **普段の業務では行うことのできない実習（ハンズオン）**は、非常に貴重な経験となった。
- 実際にインシデントが起こった場合に行う手順・操作を把握することができた。
- 事前学習、当日の資料、解説がわかりやすかった。
- 個人的に難しいと感じる課題もあったが、**同じチームの方々や講師の方と会話することで、学びながら実践的な経験を積むことができた**。
- IR対応について知識として把握している部分はあるが、**実践に近い形で経験することができ**、どのようなことについて考えておく必要があるのか（決めておく必要があるのか）などを理解することができた。

若手人材育成プログラムSecHack365 2021年度概要

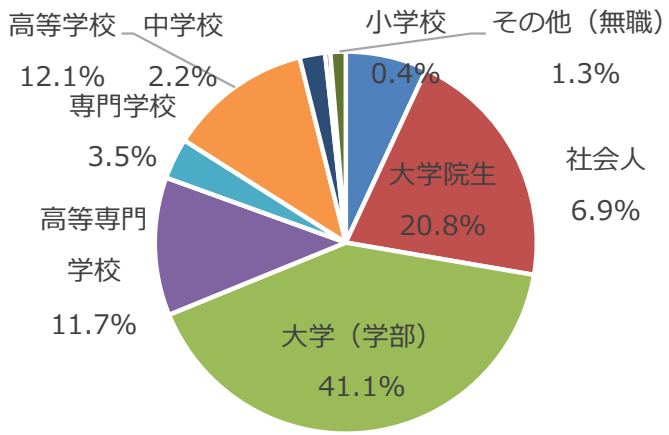
自ら手を動かし、セキュリティに関わる新たなモノづくりができる人材（セキュリティイノベーター）の育成に向けて、若年層のICT人材を対象に、NICTの持つ長年の研究開発のノウハウや、実際のサイバー攻撃関連データとそれらを安全に利用して研究開発が行える環境を活かした、**1年をかけて**本格的にセキュリティ関連技術の**指導を行う**プログラム

対象者

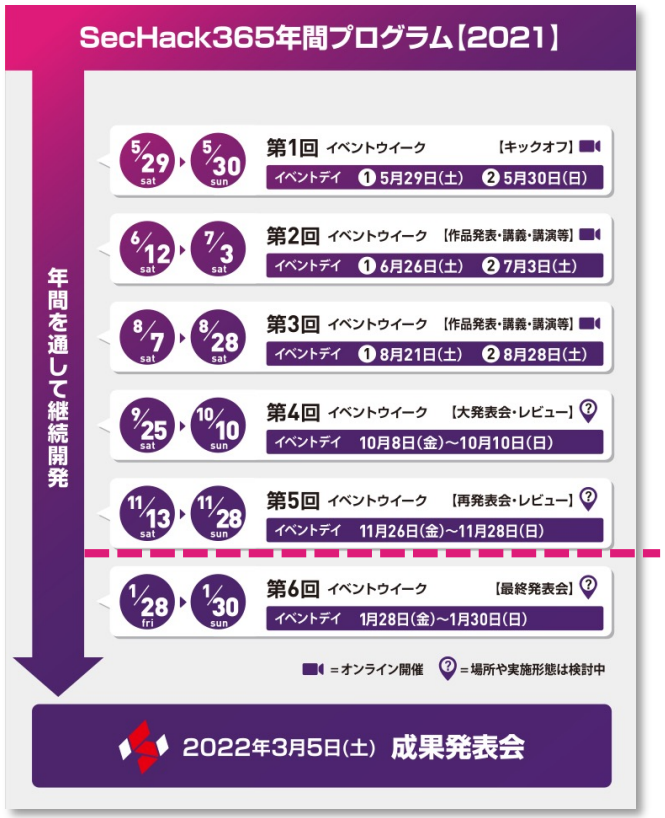
- **日本国内に居住する**
  25歳以下の若手ICT人材
  （学生、社会人、無職等※）

※2021年度より25歳以下の無職・無収入者へも補助

受講生属性（2017～2021年度）



年間プログラム例(2021年度)



ここまで終了

特長

年6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6回実施し、継続的に開発指導します。

学生向け支援

学生は受講費用等※を全額補助。学業との両立についての相談や指導も実施。
※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、攻撃データ等を活用できる“NONSTOP”が利用可能。

最先端技術の体験

ゲスト講演や先端企業の見学で発想力やプレゼンテーションスキルを強化。

オンラインでの指導

オンラインで利用可能な開発環境を提供。チャットやタスク管理ツールを活用した継続的な指導。

[参考] SecHack365 修了生の継続支援

➢ 修了後の活動状況と成果

2017年度から2020年度の修了生の活動については、修了生からの報告、修了生ポータルへの登録などで情報を得たものに限られるが、こうした修了後の呼びかけに対して8割近い回答がある。

種別	件数
他事業採択	27
出版・執筆	13
研究発表・論文登録	21
学会・論文等受賞	47
新聞・テレビ・ネット掲載	26

【受賞の例】
情報処理学会全国大会 中高生情報学研究コンテスト 中高生研究賞 最優秀賞
情報処理学会全国大会 中高生情報学研究コンテスト 中高生研究賞 優秀賞
情報処理学会 優秀論文発表賞
コンピュータセキュリティシンポジウム　奨励賞
情報危機管理コンテスト 文部科学大臣賞・経済産業大臣賞
情報通信システムセキュリティ（ICSS）研究賞

【他事業採択の例】
未踏IT人材発掘・育成事業　採択
未踏IT人材発掘・育成事業　スーパークリエータ選出
異能ベーションプログラム　採択
ITスーパーエンジニアサポートプログラム“すごうで”　採択

【起業の例】
株式会社 Riparia (リペリア) 2017年度修了生
株式会社Cyship(サイシップ) 2017年度修了生
HarvestX株式会社（ハーヴェストエックス） 2017年度修了生

riparia

【セキュリティ専門業への進路例】
NRIセキュアテクノロジーズ株式会社
株式会社サイバーディフェンス研究所
サイバートラスト株式会社
株式会社セキュアブレイン
株式会社 Flatt Security
三井物産セキュアディレクション株式会社
株式会社ラック

サイバーセキュリティ
統合知的・人材育成基盤

背景

● 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

CYBERSECURITY NEXUS

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

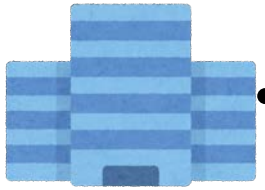
説明可能な国産脅威情報の生成・提供

高度SOC人材育成（Online自主学習＆OJT）

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
CYBERSECURITY NEXUS



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

CYNEXのタイムライン

まとめ

- サイバー空間は『人 対 人』の戦い
- サイバーセキュリティは最大の経営課題
- 優秀なセキュリティ人材の確保・育成が
  サイバーセキュリティの近道
- CYNEXに関するご連絡先 → cynex@ml.nict.go.jp