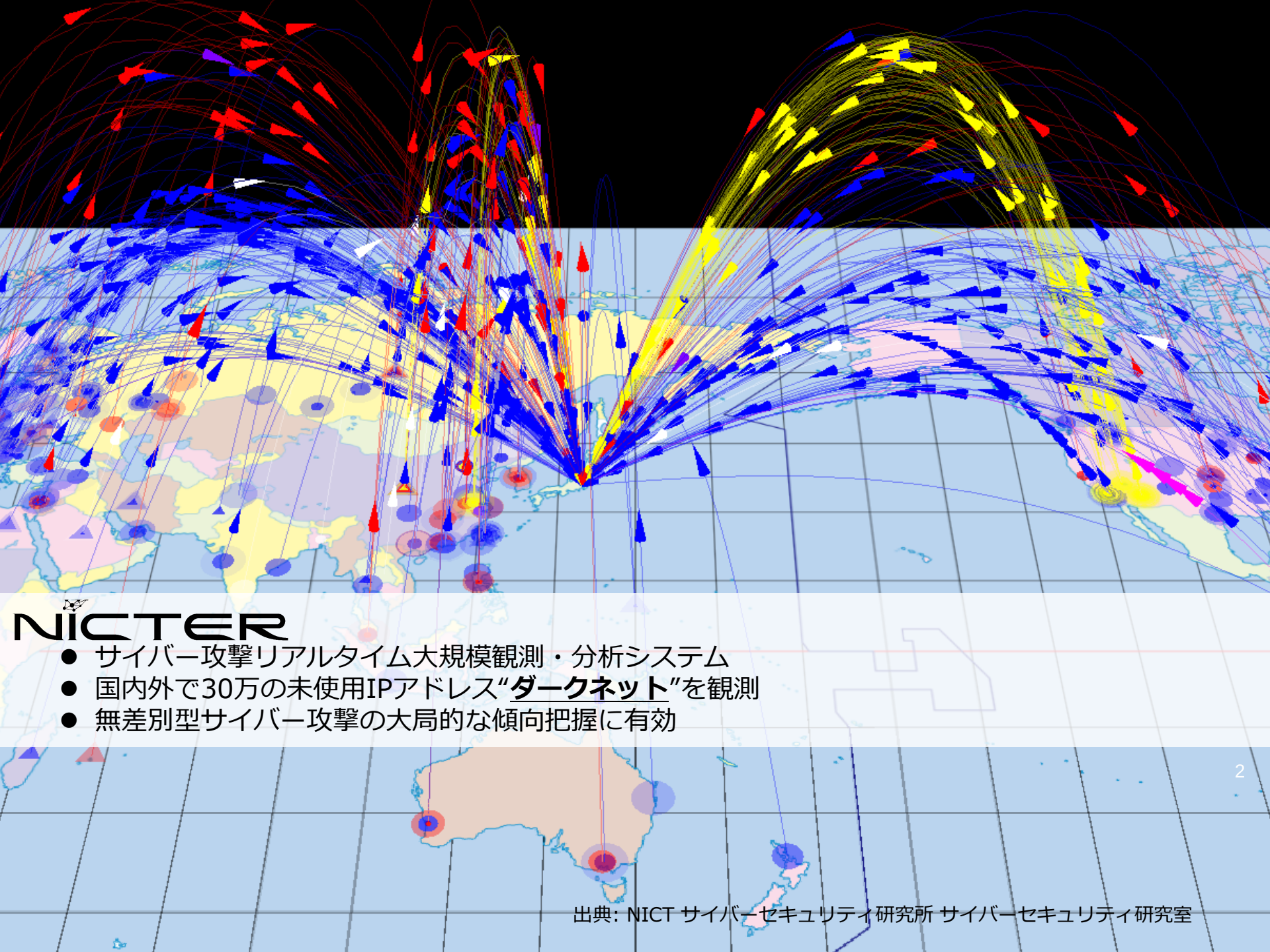
NICT におけるセキュリティ人材育成について

(2019 年 11 月 22 日)

国立研究開発法人情報通信研究機構
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長
衛藤 将史



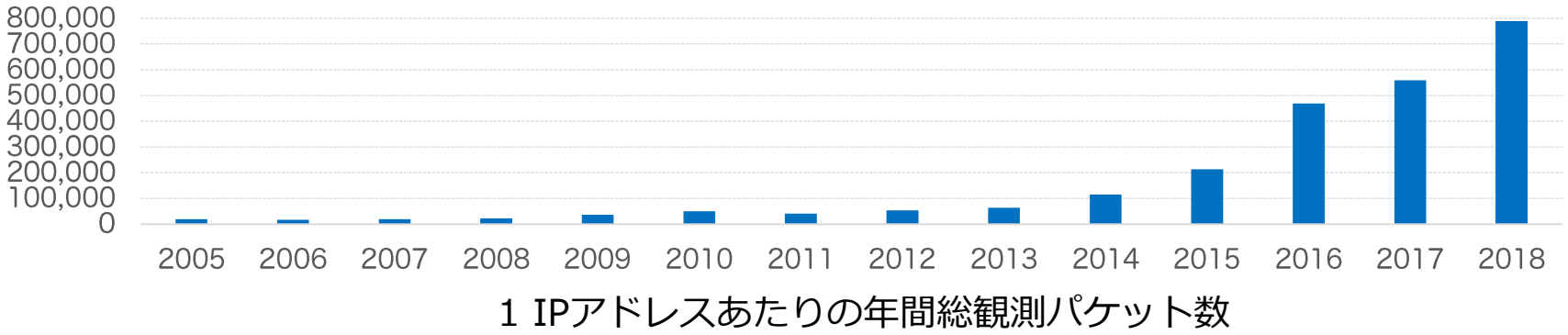
NICTER

- 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

出典: NICT 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

NICTER観測統計（2005-2018）

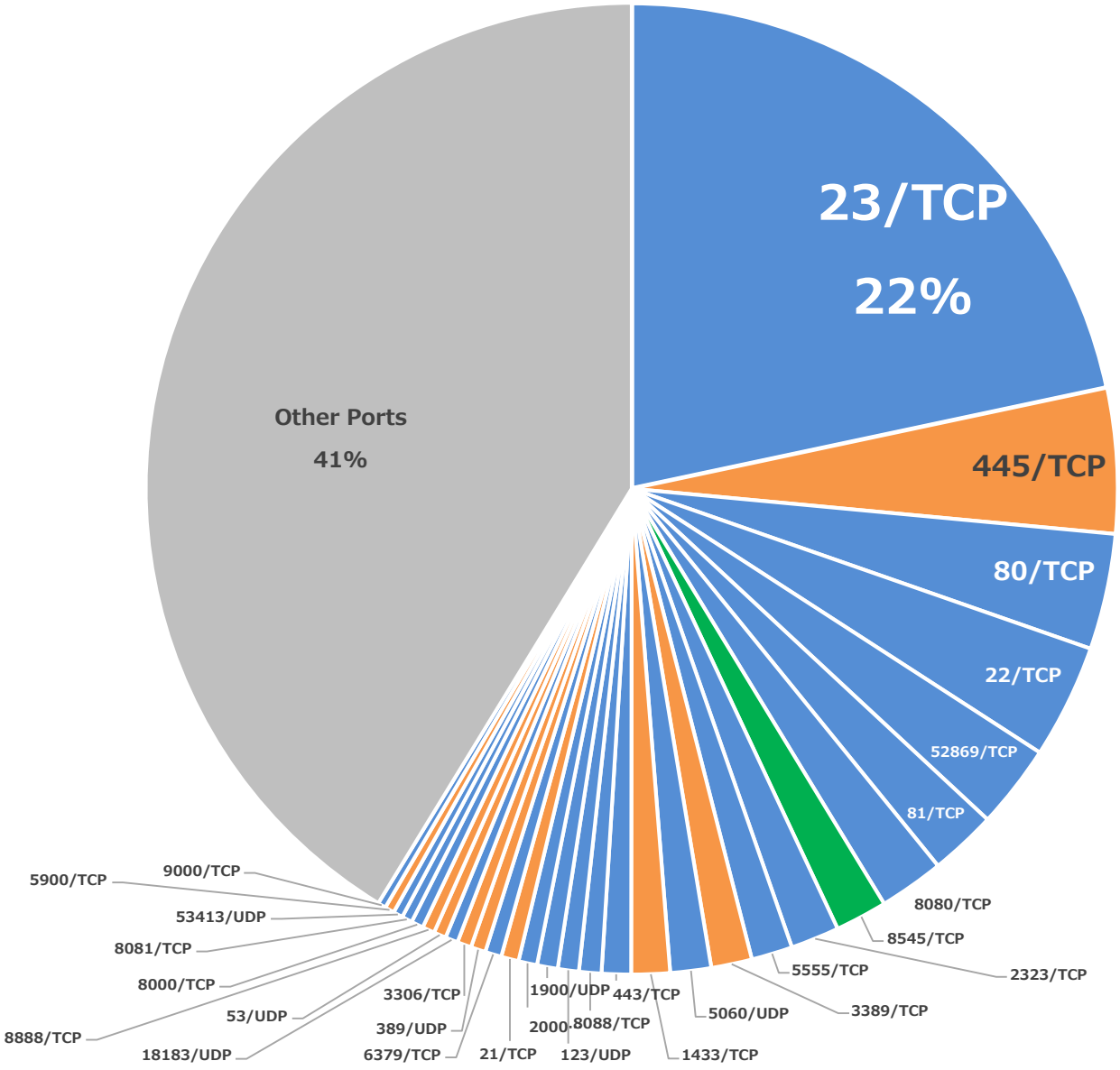
年	年間総観測パケット数	観測IPアドレス数	1 IPアドレス当たりの年間総観測パケット数
2005	約 3.1億	約1.6万	19,066
2006	約 8.1億	約10万	17,231
2007	約19.9億	約10万	19,118
2008	約22.9億	約12万	22,710
2009	約35.7億	約12万	36,190
2010	約56.5億	約12万	50,128
2011	約45.4億	約12万	40,654
2012	約77.8億	約19万	53,085
2013	約128.8億	約21万	63,655
2014	約256.6億	約24万	115,323
2015	約545.1億	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**



1 IPアドレスあたりの年間総観測パケット数

出典: NICT 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

感染機器の分布（2018年）
- NICTER 観測レポート 2018：宛先ポート番号別パケット数分布 -



IoT = 47.7%

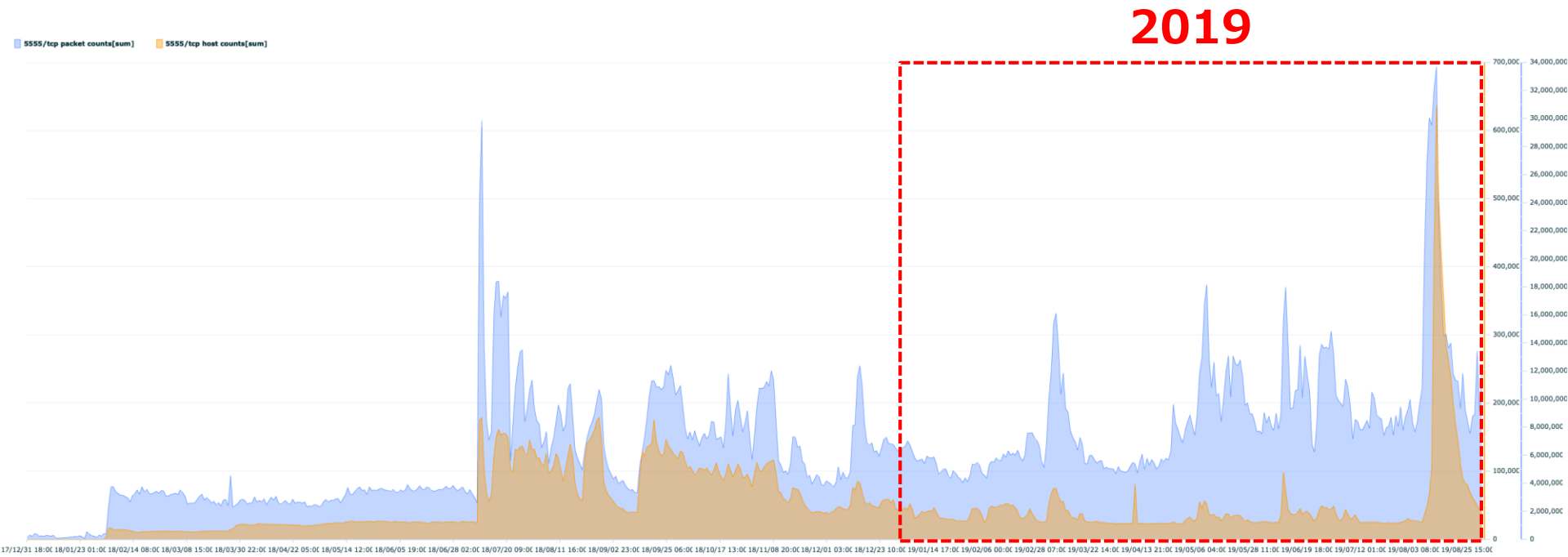
（上位30ポート中）

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）
22/TCP	IoT機器（ルータ等） 認証サーバ（SSH）
52869/TCP	IoT機器（ホームルータ等）
81/TCP	IoT機器（ホームルータ等）
8080/TCP	IoT機器（Webカメラ等）
8545/TCP	イーサリアム（仮想通貨）
2323/TCP	IoT機器（Webカメラ等）
5555/TCP	Android機器 （セットトップボックス等）

出典: NICT 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

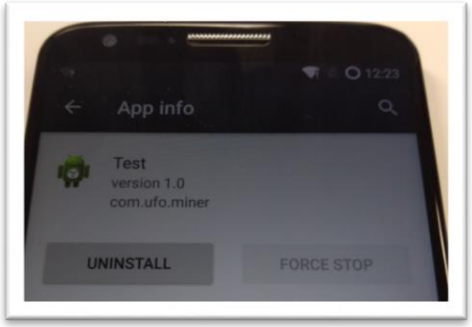
2019年上半期の大規模感染事例

- 5555/tcp（ADB: Android Debug Bridge）を狙う攻撃が高水準で推移



5555/TCP経由で感染するマルウェア

- 仮想通貨採掘 Android アプリ（apkファイル）
  - ✓ 同一 apk ファイル（com.ufo.miner）を1年以上継続的に観測
  - ✓ マイニングプール Coinhiveのサービス終了後もapkの送信が続く



- DDoS攻撃を行うマルウェア
  - ✓ 攻撃命令を出すC&Cサーバは１か月以上稼働
  - ✓ Android端末から1日26GBの通信が派生するケースも

- ADBポート等のパケットフィルタリングを行うマルウェア
  - ✓ 他のマルウェアによる感染を防止し感染を永続化

```
[dhcp161:Downloads yoshiki$ strings initdz | grep DROP
 iptables -A OUTPUT -p tcp --dport 3333 -j DROP
 iptables -A OUTPUT -p tcp --dport 5555 -j DROP
 iptables -A OUTPUT -p tcp --dport 7777 -j DROP
 iptables -A OUTPUT -p tcp --dport 9999 -j DROP
 iptables -A OUTPUT -p tcp --dport 14444 -j DROP
```

NASAへのサイバー攻撃（2019年6月）

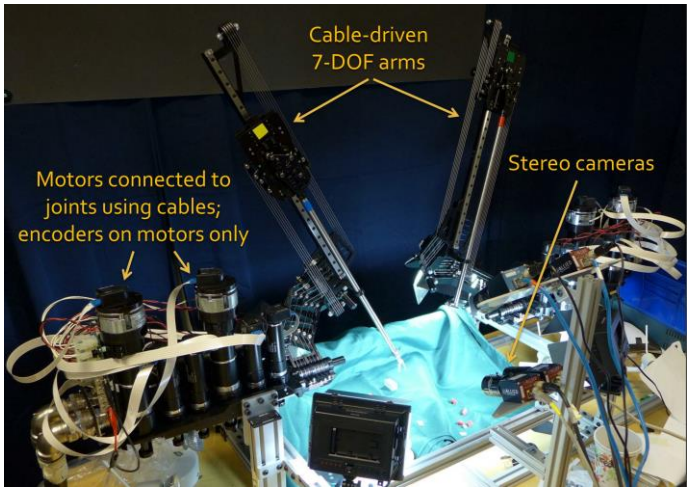
- NASAのジェット推進研究所（JPL）から機密データ漏洩
- 無許可接続されたRaspberry Piが原因（野良IoT）

https://www.itmedia.co.jp/news/articles/1906/23/news012.html
https://gigazine.net/news/20190625-nasa-hacked-raspberry-pi/
https://www.gizmodo.jp/2019/06/nasa-hacker-raspberry-pi.html

外科手術ロボットへの攻撃（国際会議 RAID 2019）

- Smart Malware that Uses Leaked Control Data of Robotic Applications: The Case of Raven-II Surgical Robots
  - ✓ 外科手術ロボットRaven-IIに感染するマルウェア
  - ✓ 感染後、潜伏し手術の挙動を学習
  - ✓ 手術中の最も重要な局面でROS※にエラー注入

※ROS: Robot Operating System



Raven-II

http://rll.berkeley.edu/surgical/control/state_estimation.html

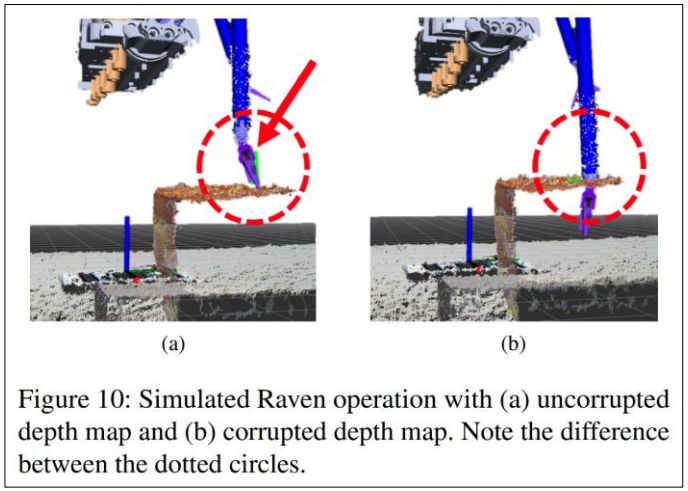


Figure 10: Simulated Raven operation with (a) uncorrupted depth map and (b) corrupted depth map. Note the difference between the dotted circles.

エラー注入による誤動作

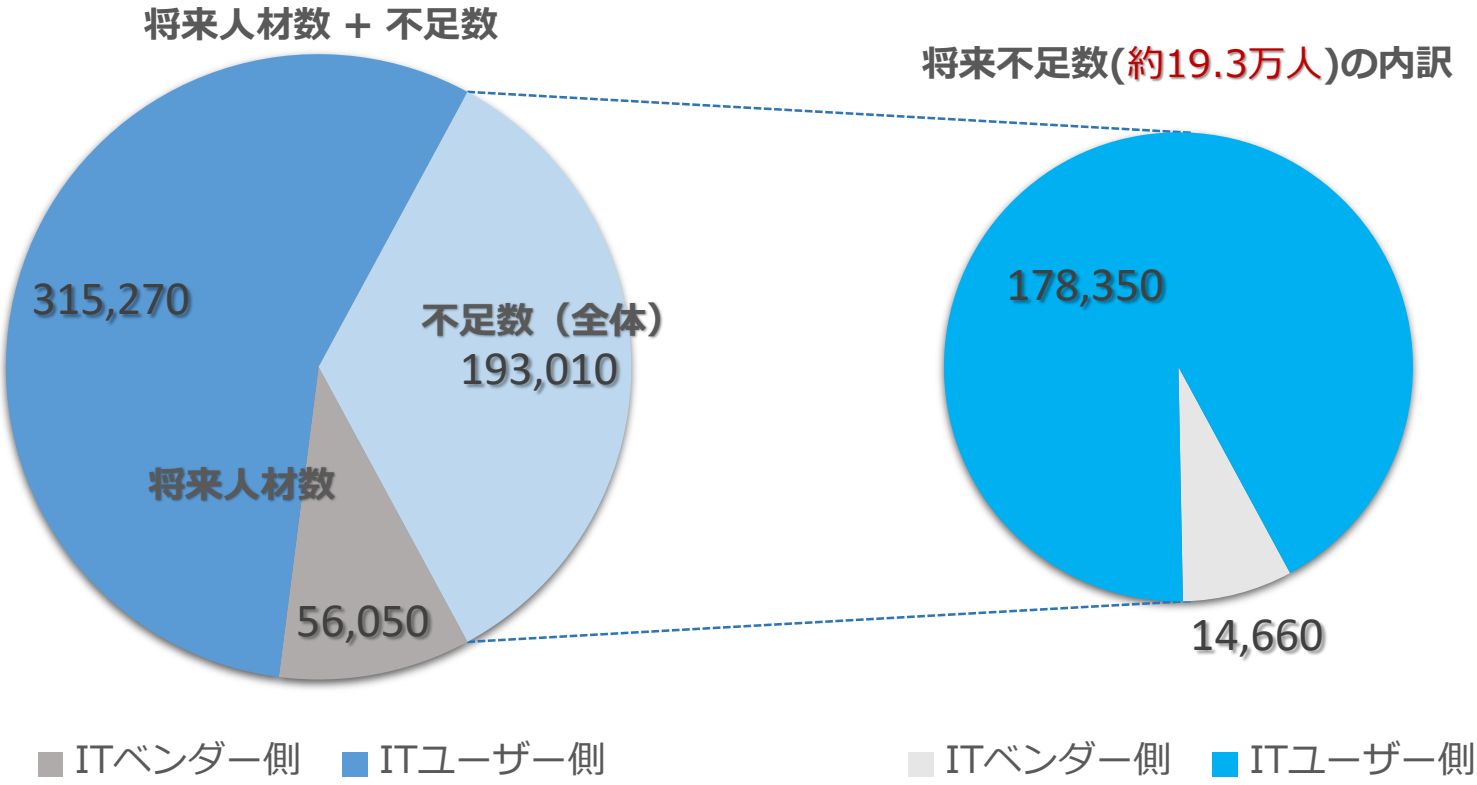
https://www.usenix.org/conference/raid2019/presentation/chung

情報セキュリティ人材の不足数の規模

- 我が国の情報セキュリティ人材は、 2020年の時点において 約19.3万人 不足するといわれている ※「IT人材の最新動向と将来推計に関する調査結果」経済産業省商務情報政策局 2016.6.10付
- このうち、 ITベンダー・WEB企業等「ITベンダー側」を除く、 **「ITユーザー側」**の不足数は約17.8万人 となることが推計される

※不足数に関する数字は、NICTにおいて、前記報告書等を参考とするなどして算出

情報セキュリティ人材数/不足数の内訳（2020年推計値）

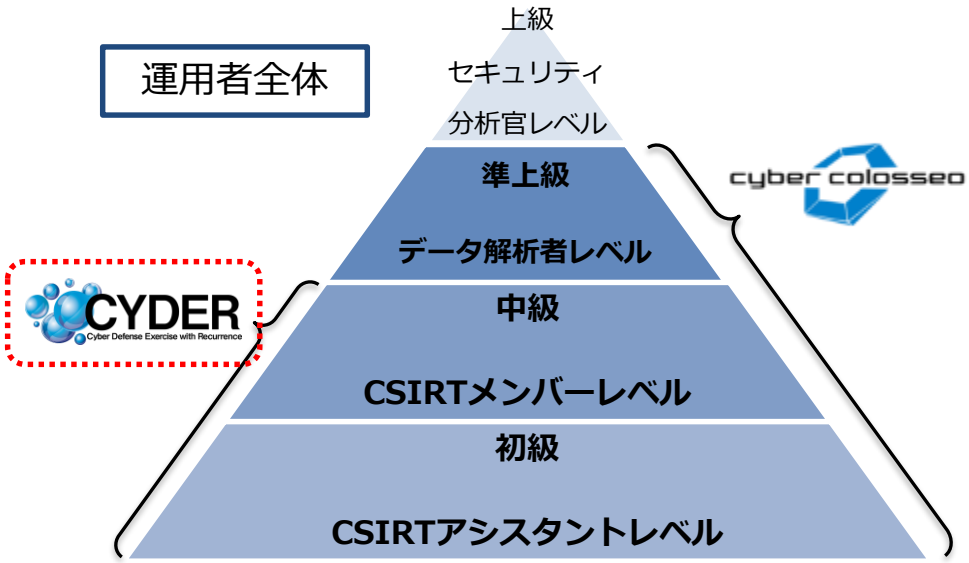


NICT ナショナルサイバートレーニングセンター

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
(2017.4.1 設置)

セキュリティオペレーター（実践的運用者）の育成

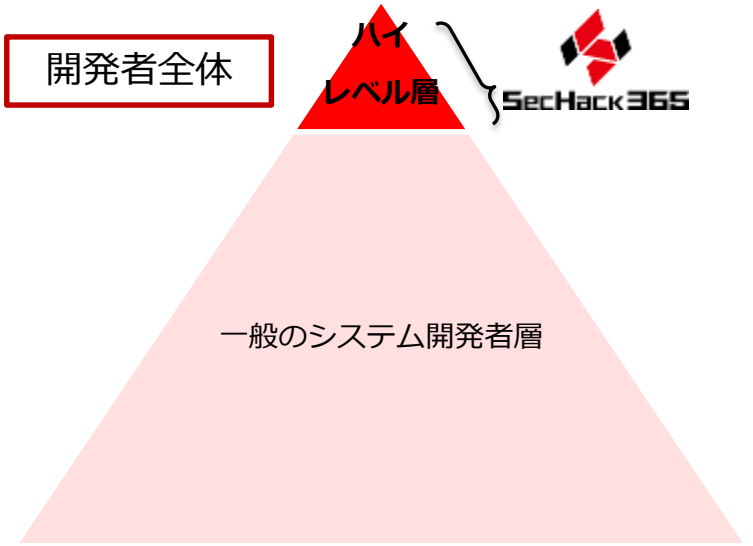
✓ 行政機関や民間企業等の組織内のセキュリティ運用者 (情報システム担当者等) を育成



※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

✓ セキュリティマインドを有した創造的人材 (セキュリティイノベーター) を育成



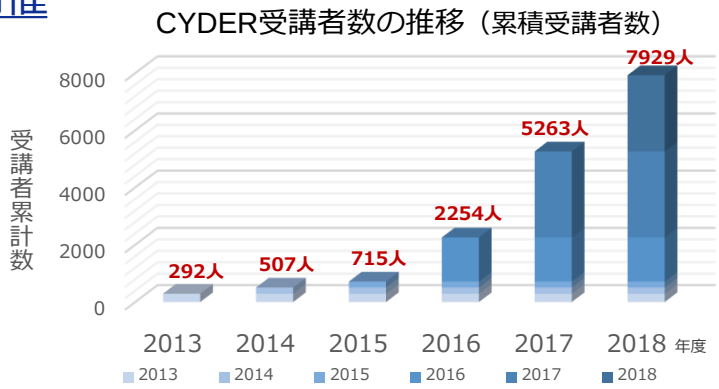
実践的サイバー防御演習「CYDER」 の概要

(CYDER：CYber Defense Exercise with Recurrence)

行政機関、重要インフラ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

2019年度コース概要

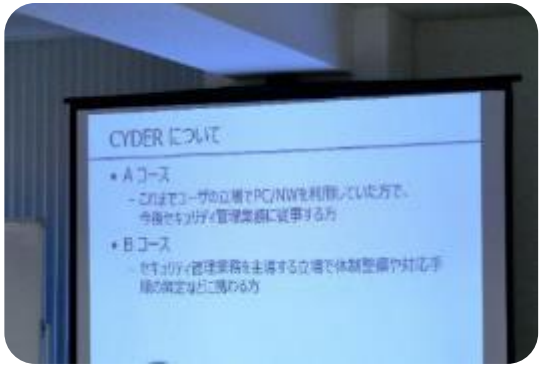
- ✓ 受講者の習熟度に応じてAコース及びBコースを開催
  - 事前オンライン学習（１時間程度）
  - 実機演習・グループワーク（１日間）
- ✓ 年間100回程度開催、3,000人以上の受講が可能
  - 全国47都道府県、100回程度開催
  - 重要社会基盤事業者、民間企業等は、受講料を徴収（7万円/人（税別））



コース	難易度	主な対象組織	開催予定地	開催回数
A コース（初級）	CSIRT アシスタントレベル	（全組織共通）	47都道府県	60回程度
B-1コース（中級）	CSIRT メンバーレベル	地方公共団体向け	全国11地域	20回程度
B-2コース（中級）		国の行政機関 (28組織)、独立行政法人等 (87 法人)、指定法人 (9 法人)、重要社会基盤事業者、民間企業等向け	東京 名古屋・大阪	20回程度

CYDER演習風景例（Aコース）

オリエンテーション



スキルチェックテスト

CYDER演習風景例（Aコース）

演習フロー説明

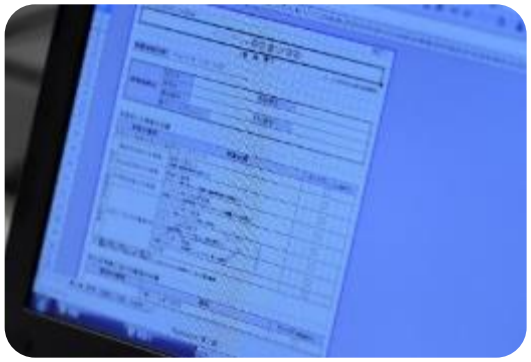
端末特定

マルウェア挙動調査

グループワーク

発表

報告書作成



[2019 年度 B-1 コース] 攻撃シナリオ例

演習受講効果の維持のため、受講者以外には非公開

[2019 年度 B-1 コース] 事案対処の流れの例

演習受講効果の維持のため、受講者以外には非公開

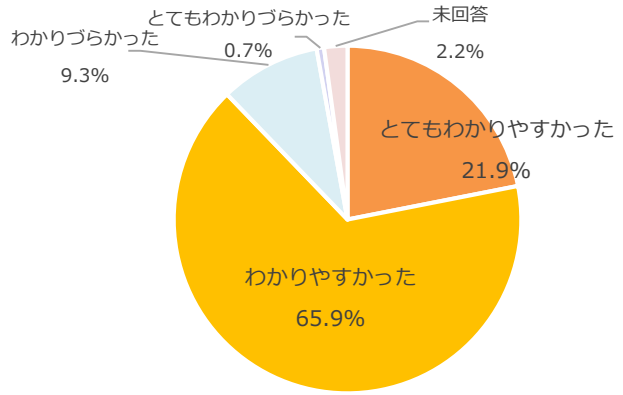
[2019 年度 B-1 コース] 事案対処の実例

演習受講効果の維持のため、受講者以外には非公開

CYDER受講結果 (アンケート等)

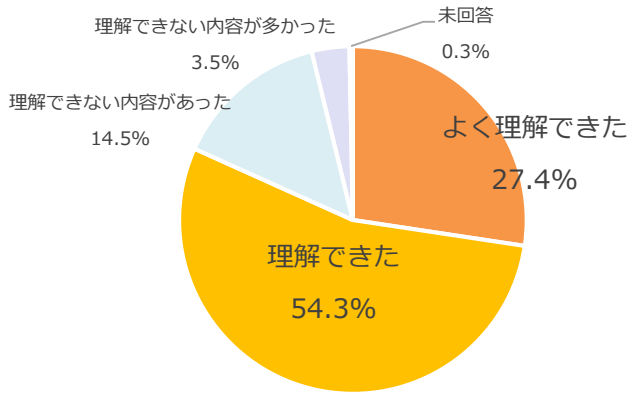
集合演習＆事前オンライン学習の理解度調査（受講者アンケート） 2018年度結果

「事前オンライン学習」の内容や説明はわかりやすかったですか？



n=2173

集合演習は，理解できましたか？

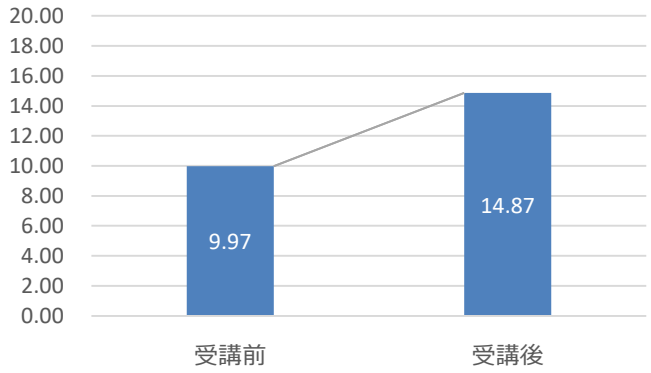


n=2173

スキルチェックテスト得点の変化 2017年度結果

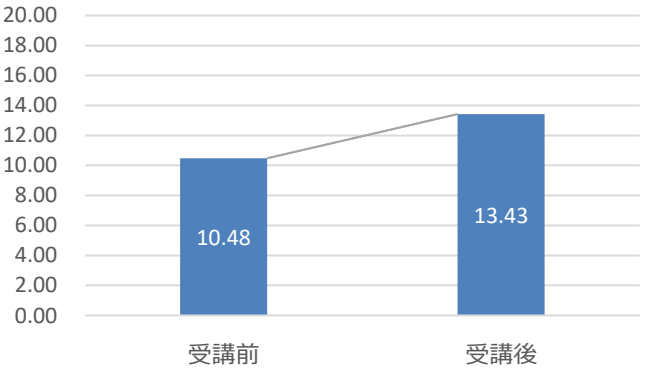
B-1コース

20点満点



B-2コース

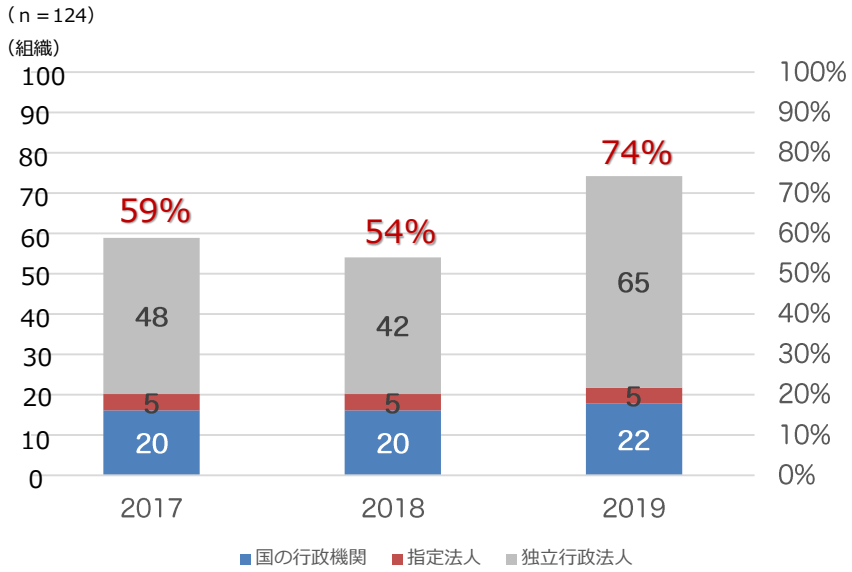
20点満点



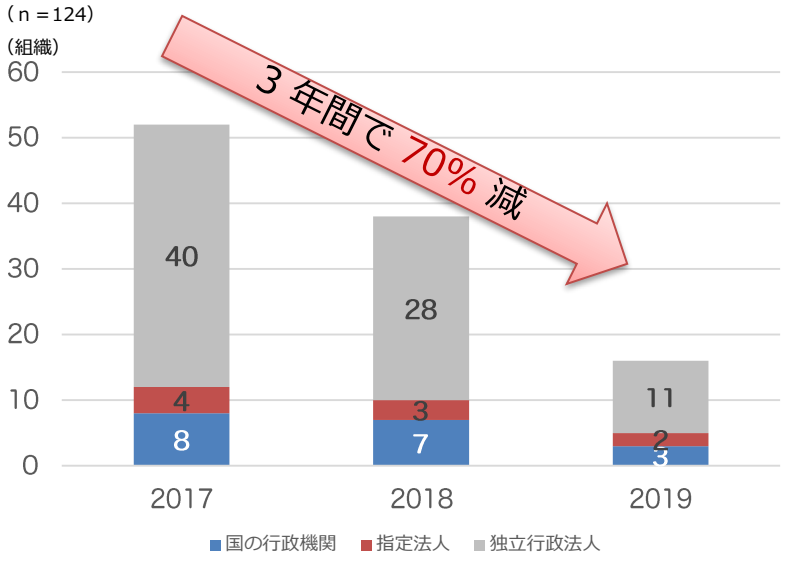
CYDER 参加状況（国の行政機関等）(2017 年度 ～)

＜国の行政機関・指定法人・独立行政法人※＞
- 国の行政機関・指定法人においては、受講組織数が継続して全組織の**半数以上を維持**。
- 独立行政法人においては、2019 年度に初めて受講した組織が増加するなど、受講組織数が**拡大傾向**。
- 一度も受講したことがない組織は**急減傾向** (3 年間で 70% 減)。

国の行政機関等における受講組織数と全組織数に対する参加率



一度も受講したことがない
国の行政機関等の組織数

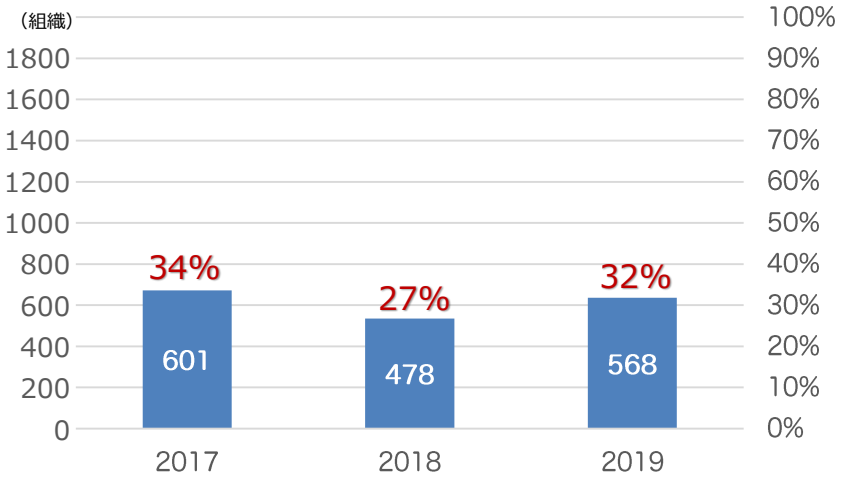


※受講対象者：サイバーセキュリティ基本法第13条の規定される組織（国の行政機関（28組織）・指定法人（9法人）・独立行政法人（87組織））
※2019 年度は 11 月 14 日現在

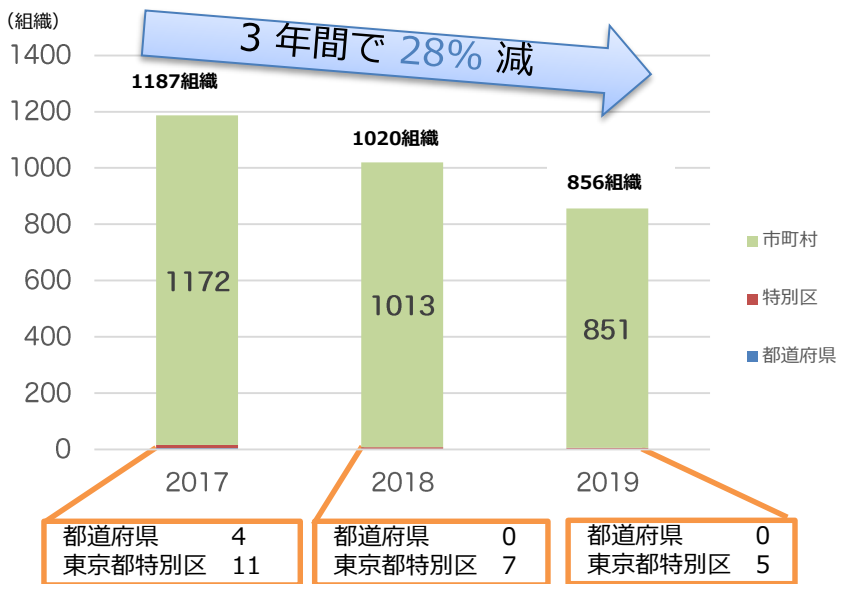
CYDER 参加状況（地方自治体） (2017 年度 ～)

＜地方自治体＞
✓ 受講組織数が概ね横ばい状態で、一度も受講したことがない組織数は毎年減少しているものの、その程度は、国の行政機関等に比べれば穏やかな状況 (現時点で 48% の地方自治体が未受講)。

地方自治体受講組織数と全組織数に対する参加率



一度も受講したことがない地方自治体組織数

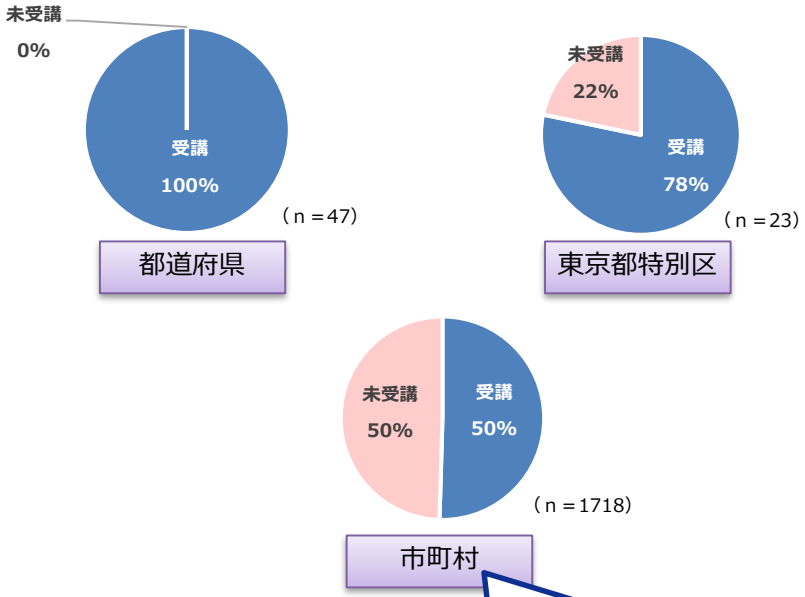


※地方自治体 (都道府県 市区町村) の総数は 1788
※2019 年度は 11 月 14 日現在

未受講の地方自治体の状況

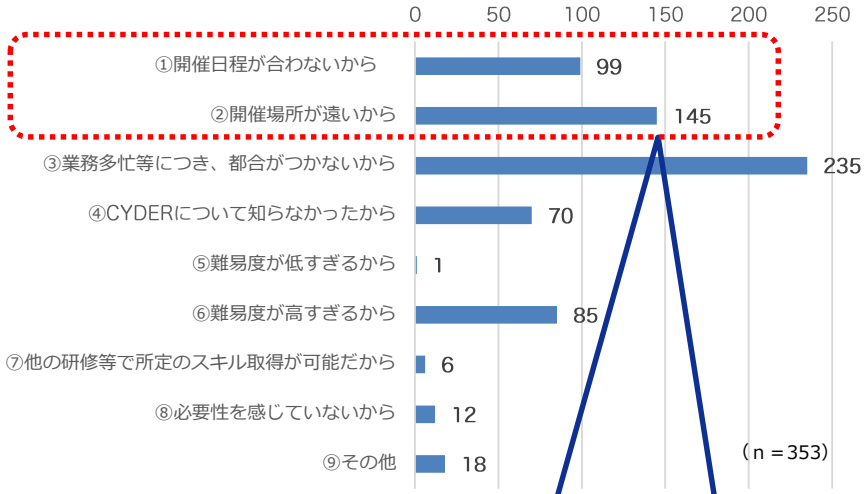
＜地方自治体＞
✓ 未受講の理由としては、地方自治体の半数以上が業務多忙の他、演習会場が遠方であること、日程が合わないこと等を挙げる。

組織別受講割合（2017 ~ 2019年度）



✓ 特に市町村において、未受講組織の割合が大きい傾向

CYDERを受講しない理由



✓ 開催日程、開催場所が合わないことを理由に受講しない組織の割合が比較的高い

(ナショナルサイバートレーニングセンター調べ)

CYDER の開催地変更による受講の利便性改善の取り組み (県の例)

- ✓ の自治体の参加を促すため、2019 年度に開催地を 市に変更したところ、近隣の 4 自治体が初めて参加するなど、**未受講自治体の減少 (16 → 9) に効果を発揮** (開催地・開催日程の設定にあたっては、地元の事情に詳しい総務省各総合通信局とも事前に調整)
- ✓ 一方、一部の自治体が近隣県の開催地を選択するなど、県全体の受講機会確保の観点からは課題が残る

個別の自治体に関する情報のため非公開

まとめ

- 地方自治体は、国の行政機関等と比較して未受講組織数の割合が高い傾向。

- 開催地を県庁所在地から変更・追加する等の事業運営上の工夫による一定の効果や意義が認められる一方、未受講組織数の抜本的な解消には未だ至っていない。

- 東京 2020 大会の開催に先立ち、社会的なセキュリティ対応力を強化するため、特に地方公共団体を対象として、より効果的な取り組みを検討する必要があるのではないか。

- 開催場所が遠方にあることを主な理由として挙げる未受講組織が多いことから、その対策として、受講場所に依存しにくい訓練機会の検討も進める必要があるのではないか。