資料６

一部非公表

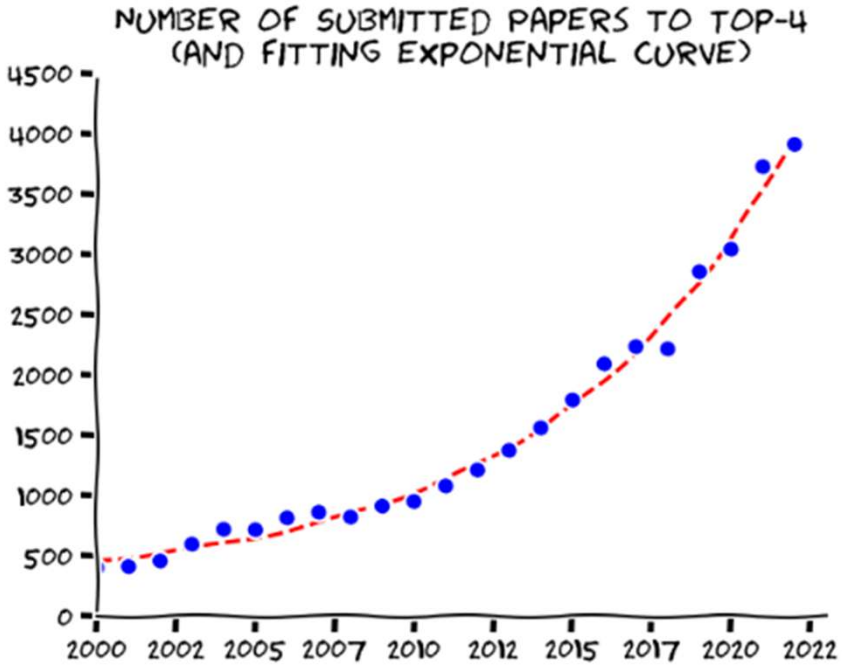
サイバーセキュリティ研究動向と社会実装に向けて

横浜国立大学
大学院環境情報研究院/先端科学高等研究院

吉岡克成

学界におけるサイバーセキュリティ研究外観

４大会議(最高峰国際会議：USENIX, ACM CCS, IEEE S&P, NDSS)における動向から学界におけるサイバーセキュリティ研究動向を概観



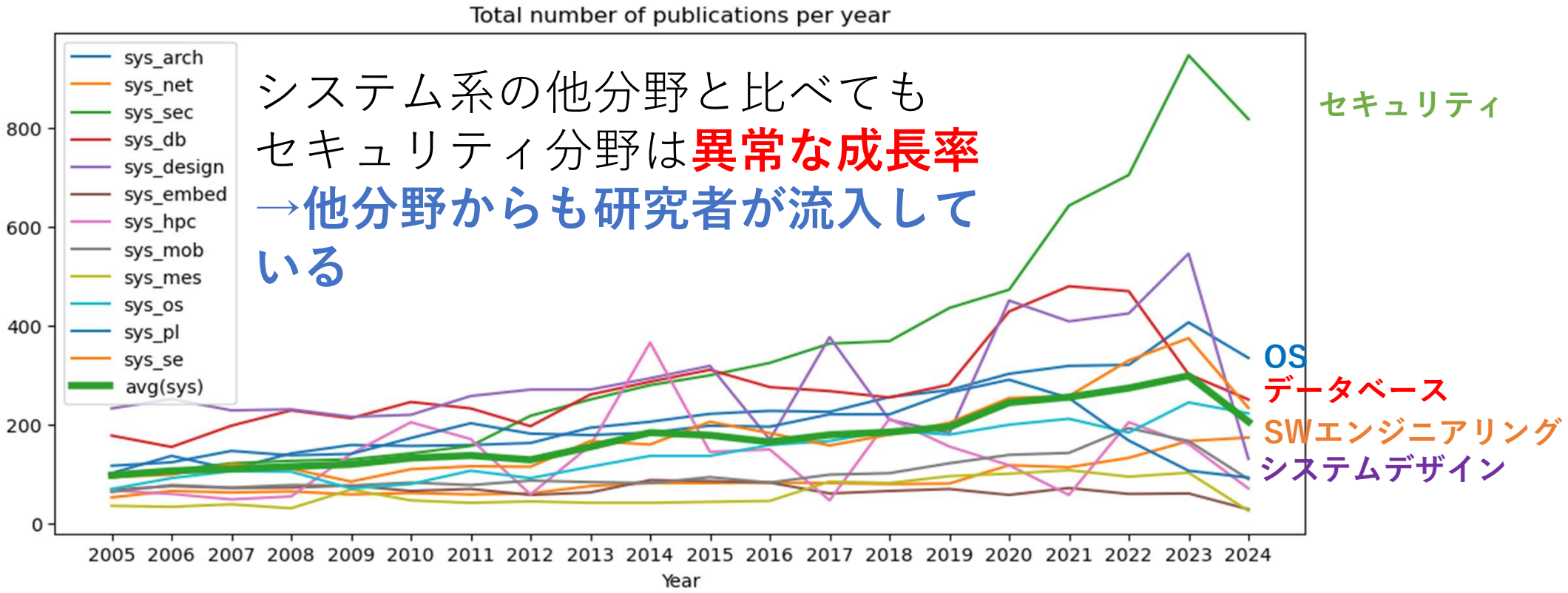
４大会議に投稿される件数は
2000→2022年で**約10倍**になった

近年は投稿数が**指数関数的に増加し**
競争激化

System Security Circus 2022, https://s3.eurecom.fr/~balzarot/security-circus/circus_stats.html
Systems Circus, https://nebelwelt.net/pubstats/

学界におけるサイバーセキュリティ研究外観

トップ会議での発表件数



システム系の他分野と比べても
セキュリティ分野は**異常な成長率**
→他分野からも研究者が流入している

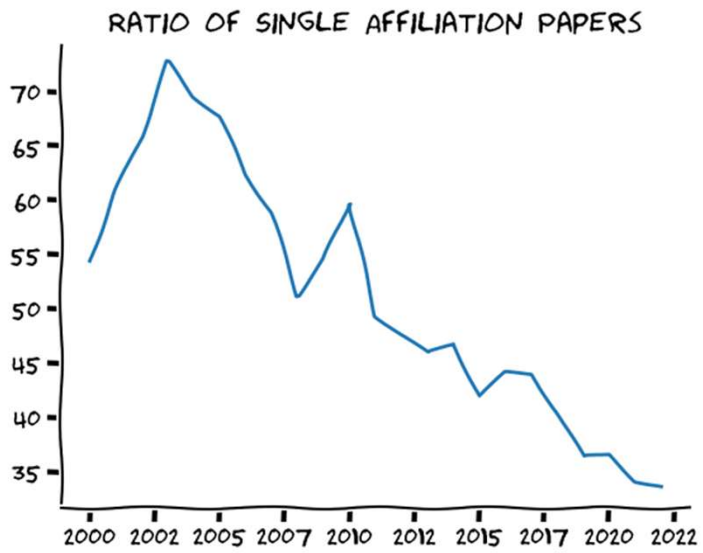
セキュリティ
OS
データベース
SWエンジニアリング
システムデザイン

System Security Circus 2022, https://s3.eurecom.fr/~balzarot/security-circus/circus_stats.html
Systems Circus, https://nebelwelt.net/pubstats/

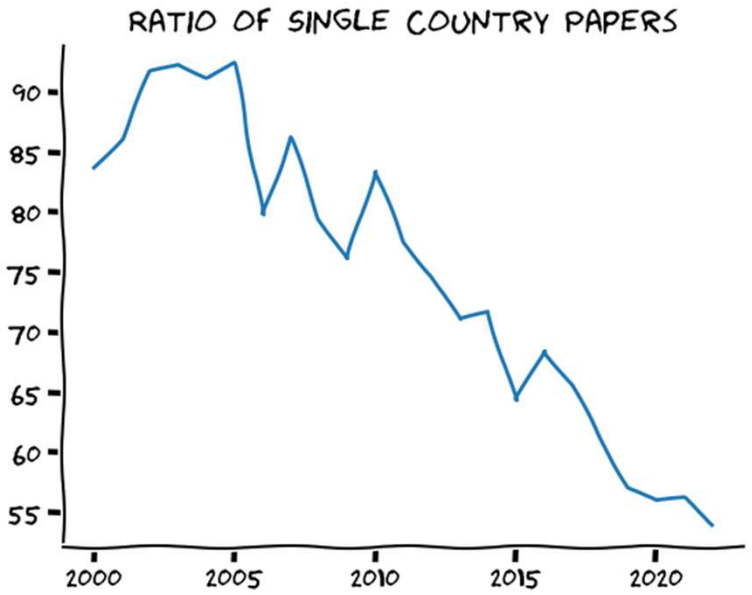
学界におけるサイバーセキュリティ研究外観

組織間連携、国際連携が進んでいる(テーマの多様化、競争の激化により研究の規模が大きくなり、単一組織で研究を行うことが困難になっていると予想)

１組織による論文の割合



１か国による論文の割合

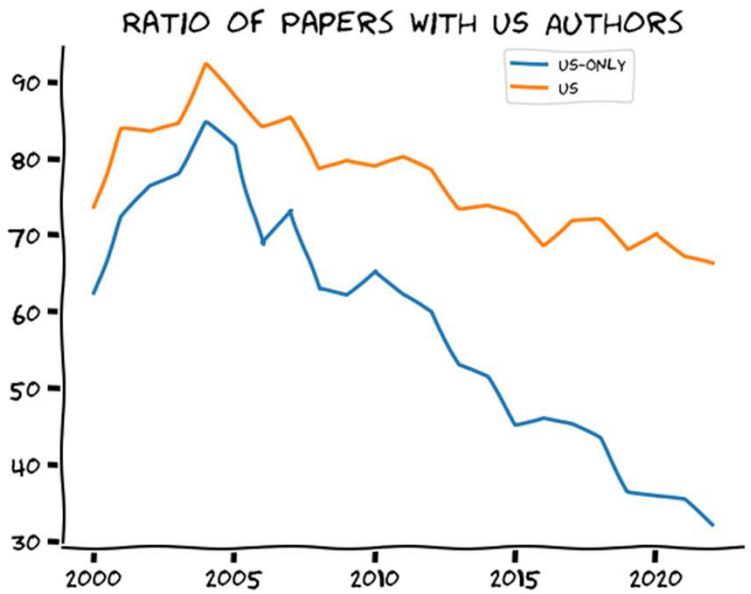


System Security Circus 2022, https://s3.eurecom.fr/~balzarot/security-circus/circus_stats.html
Systems Circus, https://nebelwelt.net/pubstats/

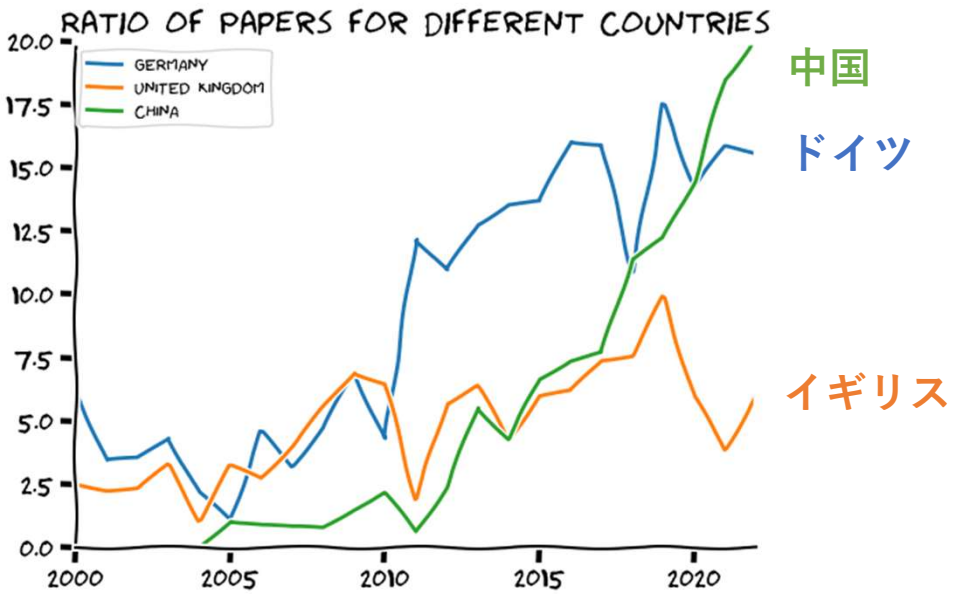
学界におけるサイバーセキュリティ研究外観

かつては米国の研究が支配的だったが、**ドイツ、中国**が急速に存在感を増している(2022年の論文発表数１位はドイツCISPA†)

米国関係の論文数



ドイツ、イギリス、中国の論文数



System Security Circus 2022, https://s3.eurecom.fr/~balzarot/security-circus/circus_stats.html
Systems Circus, https://nebelwelt.net/pubstats/
†CISPA Helmholtz Center for Information Security

日本の研究は？

- 2018年頃まで４大会議では存在感なし。**2019年頃から増加傾向**(予兆として準トップ会議では2013年頃から増加傾向あり)

- 若手研究者が海外で鍛えて成果を出す事例、海外研究者との連携で成果を出す事例が多い

- 分野：ハードウェアセキュリティ、IoTセキュリティ、ユーザブルセキュリティ、計測セキュリティなど

これらの技術は産業展開されるのでしょうか？

学術研究と産業展開(個人的な経験から)

- 2005年に(NICTに)就職し、サイバーセキュリティの研究を始めた頃、すでにネットワーク侵入検知(Network Intrusion Detection)技術は、学術界では「**レッドオーシャン状態**」または「**研究が一通りされた分野**」とされていた。

- 当時の研究のトレンドは**マルウェア対策技術**や、**Webセキュリティ**に移ろうとしていた。

世界のトップ研究者の活動からみる技術トレンド

Distributed pattern detection for intrusion detection C Kruegel, T Toth NDSS	80	2002
DPS: An Architectural Style for Development of Secure Software P Fenkam, H Gall, M Jazayeri, C Kruegel Infrastructure Security: International Conference, InfraSec 2002 Bristol, UK ...	7	2002
XGuide-A practical guide to XML-based Web engineering C Kerer, E Kirda, C Krügel Web Engineering and Peer-to-Peer Computing: NETWORKING 2002 Workshops Pisa ...	9	2002
Network alertness: towards an adaptive, collaborating intrusion detection system C Kruegel Technische Universität Wien	15	2002
Sparta: A Mobile Agent based Intrusion Detection System C Krügel, T Toth, E Kirda Advances in Network and Distributed Systems Security: IFIP TC11 WG11. 4 ...	47	2002
Connection-history based anomaly detection T Toth Proc. 3rd IEEE Information Assurance Workshop, 2002	101	2002
Decentralized event correlation for intrusion detection C Krügel, T Toth, C Kerer Information Security and Cryptology—ICISC 2001: 4th International ...	168	2002
Bayesian Event Classification for Intrusion Detection Reliable Software Group University of California K Christopher, DM William, RF Valeur Santa Barbara	12	2003
Topology-based detection of anomalous BGP messages C Kruegel, D Mutz, W Robertson, F Valeur Recent Advances in Intrusion Detection: 6th International Symposium, RAID ...	135	2003
On the detection of anomalous system call arguments C Kruegel, D Mutz, F Valeur, G Vigna Computer Security–ESORICS 2003: 8th European Symposium on Research in ...	299	2003
Evaluating the impact of automated intrusion response mechanisms T Toth, C Kruegel 18th Annual Computer Security Applications Conference, 2002. Proceedings ...	247	2002
Stateful intrusion detection for high-speed network's C Kruegel, F Valeur, G Vigna, R Kemmerer Proceedings 2002 IEEE Symposium on Security and Privacy, 285-293	416	2002
Service specific anomaly detection for network intrusion detection C Krügel, T Toth, E Kirda Proceedings of the 2002 ACM symposium on Applied computing, 201-208	538	2002
Flexible, mobile agent based intrusion detection for dynamic networks C Krügel, T Toth na	47	2002

カリフォルニア大学
サンターバーバラ校
Christopher Kruegel教授の例
４大会議発表100件を超える
トップ研究者の一人

実際、世界のトップ研究者は「**侵入検知(Intrusion Detection)**」の研究を2002-2003年頃までにおおむね終わらせていた

世界のトップ研究者の活動からみる技術トレンド

カリフォルニア大学
サンターバーバラ校
Christopher Kruegel教授の例
４大会議発表100件を超える
トップ研究者の一人

2005～2007年頃には、「**マルウェア解析・検知**」「**Webセキュリティ**」にシフトし、多数の成果．日本の学術成果はトップレベルではこの時期、ほぼ皆無．

世界のトップ研究者の活動からみる技術トレンド

研究で培った**マルウェア解析技術**を軸に２０１１年に**Lastline, Inc**を設立

2020年にLastlineがVMwareに買収され、**VP Security Services**に就任) 価格非公開も企業価値 1.14億$との報道 †

2023年にVmwareがBroadcomに買収され、**Distinguished Engineer**に就任

2024年にCISCO, Chief Scientist, Securityに就任

カリフォルニア大学
サンターバーバラ校
Christopher Kruegel教授の例
４大会議発表100件を超える
トップ研究者の一人

産業界で活躍しつつ、UCSBでの研究も継続

† https://news.crunchbase.com/startups/vmware-to-acquire-lastline-marking-thomvest-ventures-second-exit-in-a-weeks-time/

もっと早く産業展開した事例

censys　ASMサービス、広域スキャン、インターネットサービス

スタンフォード大
Zakir Durumeric助教
の例

ミシガン大での博士課程
学生時代に高速スキャン
技術Zmap開発

Censys Inc設立

これからの期待

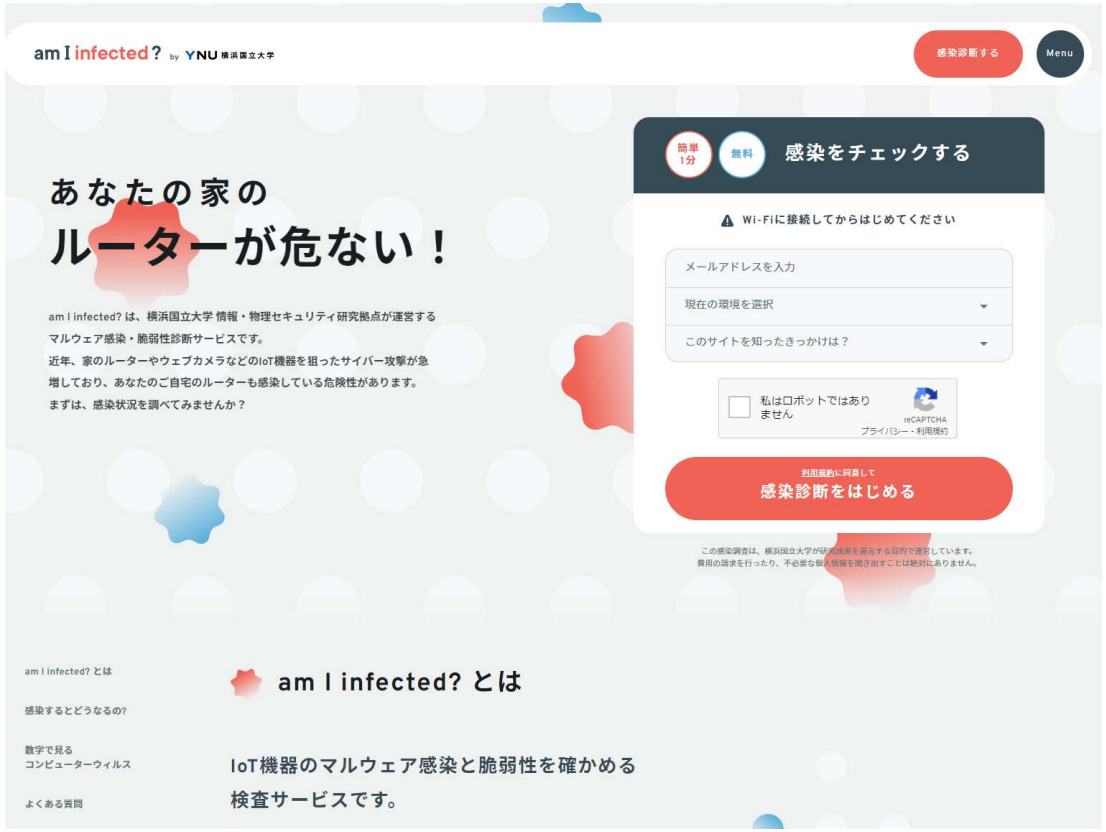
- 全ての産業技術が学術界での研究をベースにしているわけではないが、米国のセキュリティ技術の発展の根幹に学術研究があったことは確かであると考える
- 10年以上の準備期間を経て、世界で勝負できる日本のサイバーセキュリティ研究が少しずつ出てきており、その数は増加傾向にある。
- 現在、その兆候が見え始めているのは、ハードウェアセキュリティ、IoTセキュリティ、ユーザブルセキュリティ、計測セキュリティなどの分野であるが、今後、新たな分野での成果も期待される。
- これを続けていくことで人材の厚みを出すことが王道。

課題

- 新たな技術が創出されても、社会の要請とのマッチングが必要であったり、そのニーズに研究者側が気づかない場合もある。また、特に日本の大学研究者は起業家精神が旺盛とはいえず、また純粋な研究時間すら十分に確保できていないため、＋アルファの活動を行う余力・余時間が必要。そのためには起業のために**他負担をバイアウトする外部研究資金の仕組みの充実や起業のための人材紹介、雇用支援**が望ましい

- 一方、すでに大学で研究体制を構築している研究者だけでなく、Censysの事例のように、才能と時間とエネルギーのある若い世代の活動を後押しすべき。**若い研究者に早く世界の研究レベルを経験してもらい**、世界に通じる研究開発と（チャンスがあれば）それに基づくビジネスを構築する後押しとなる施策が必要。社会展開の経験、データがさらなる研究アイディアを生む、**正のスパイラル**を確立したい。

身近な(社会展開がうまくいかない)事例の紹介: IoT機器セキュリティ診断サービス:am I infected?



横浜国大が運営する無料のIoT機器セキュリティ診断サービス。

2022年開始後、累計10万人を超える利用があり、95%を超えるユーザが「役に立った」「また使いたい」と回答

本サービスの収集データに基づく研究が４大会議**USENIX Security2025に採録**

度々、有償化の提案を頂き、検討を繰り返すも、**毎回本務多忙で断念**

MCPC Award 2023 (サービス&ソリューション部門) 優秀賞

https://amii.ynu.codes/

日本のサイバーセキュリティ研究開発の課題 “負のスパイラル”

- 国際的な競争力をもつセキュリティ企業が存在しない

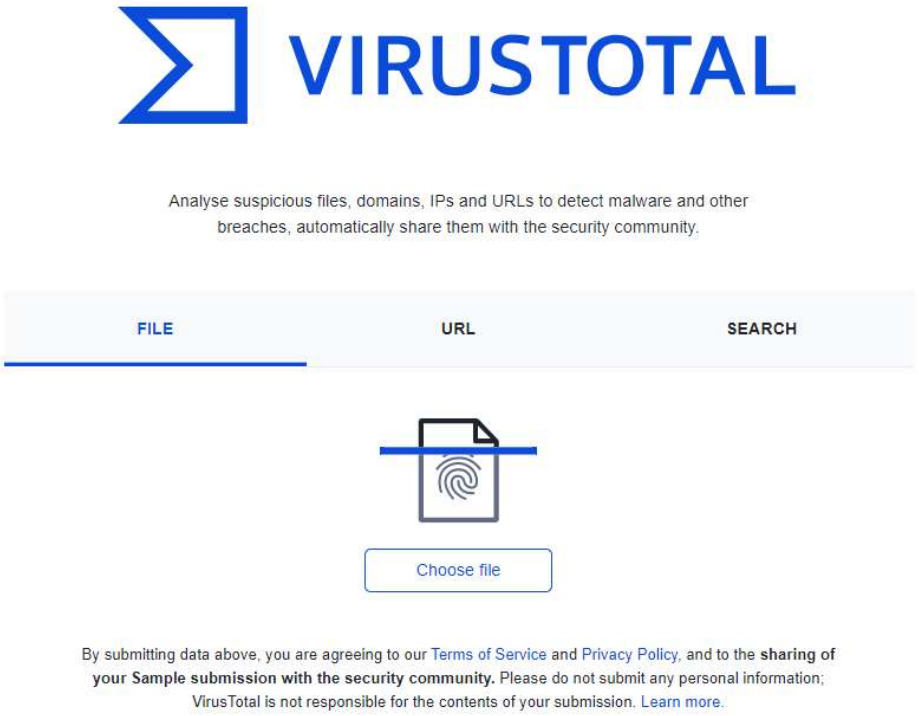
- 他国のセキュリティ技術、情報に頼らざるをえず、セキュリティに関するデータ、知識、ノウハウが蓄積しない

- **データ、知識、ノウハウが不足**しており、新たなセキュリティ技術のイノベーションがおきない。研究開発が進展しない。産学連携も進まない。大学も現場を見ない。

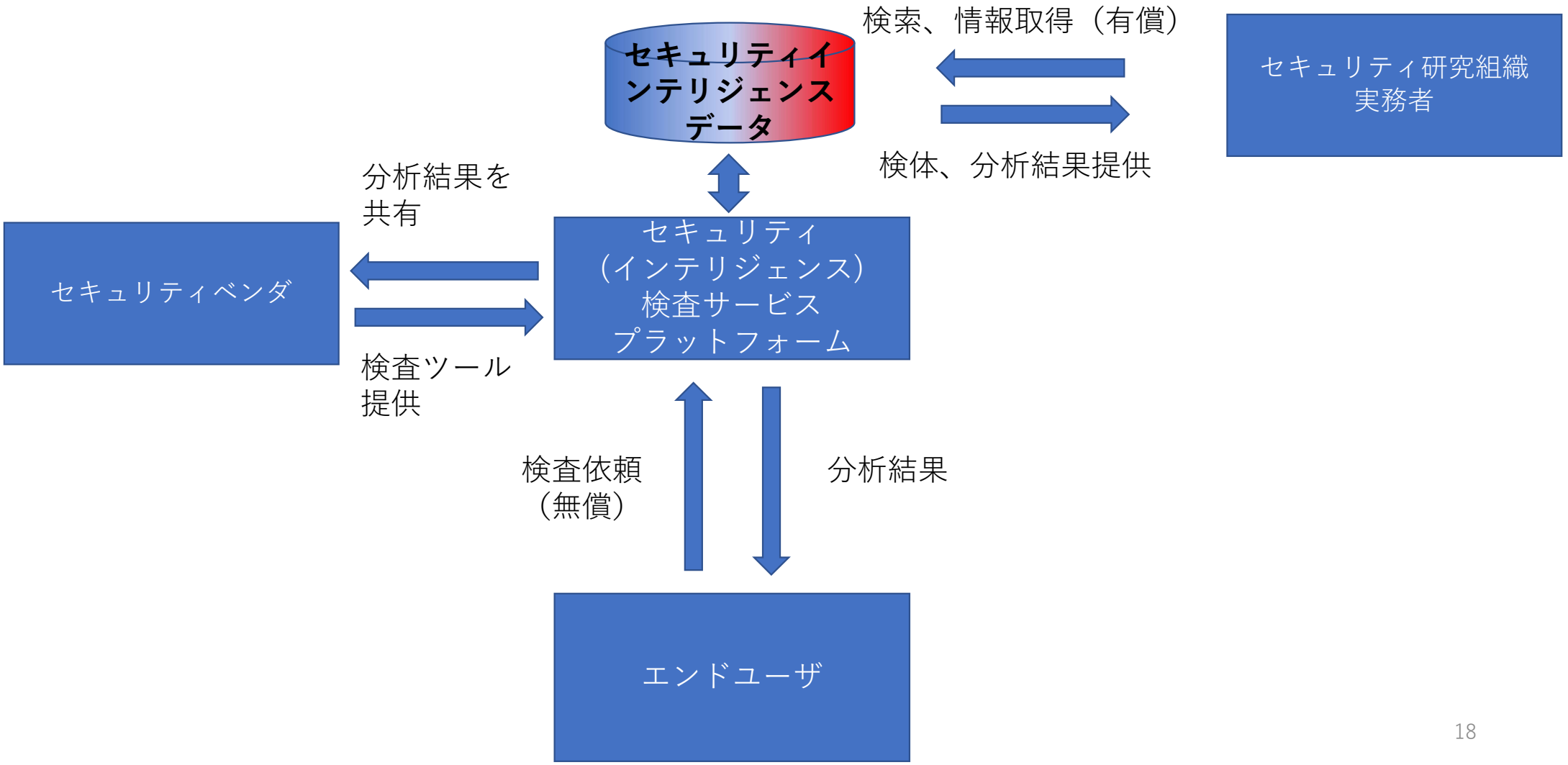
データ収集が研究開発を促進している好例（正のスパイラル）

- Google社 Virus Total
(ウイルストータル)

- 怪しいファイルやURLを投稿すると70を超えるセキュリティ製品で検査をして、結果を教えてくれる（利用は無料）



ウイルストータル全体像



提案：
日本版ウイルストータルを
作れないか？

データドリブンなサイバーセキュリティ研究開発エコシステム(日本版ウイルストータル)

- 本家ウイルストータルとの違いは？

1. 日本の研究組織の研究成果、日本に特化したサイバー攻撃に強い分析エンジンを提供する

2. ファイルやURLだけでなく、様々な入力の検査を行う（例：フェイクニュース診断、ディープフェイク検査、など）。

3. 信用された組織だけで情報を共有する「コントロールドシェアリング」モードを新たに設定する

1.日本の研究組織の研究成果、日本に特化したサイバー攻撃に強い分析エンジンを提供する

- 日本の企業、大学が分析エンジンを提供する

- なりすましメール、IoT機器への攻撃、フィッシング攻撃、SMS不正メッセージなど国内で特徴のある脅威について、検査対象に対する有益な情報を提供することで海外の検査サービスと差別化を図る

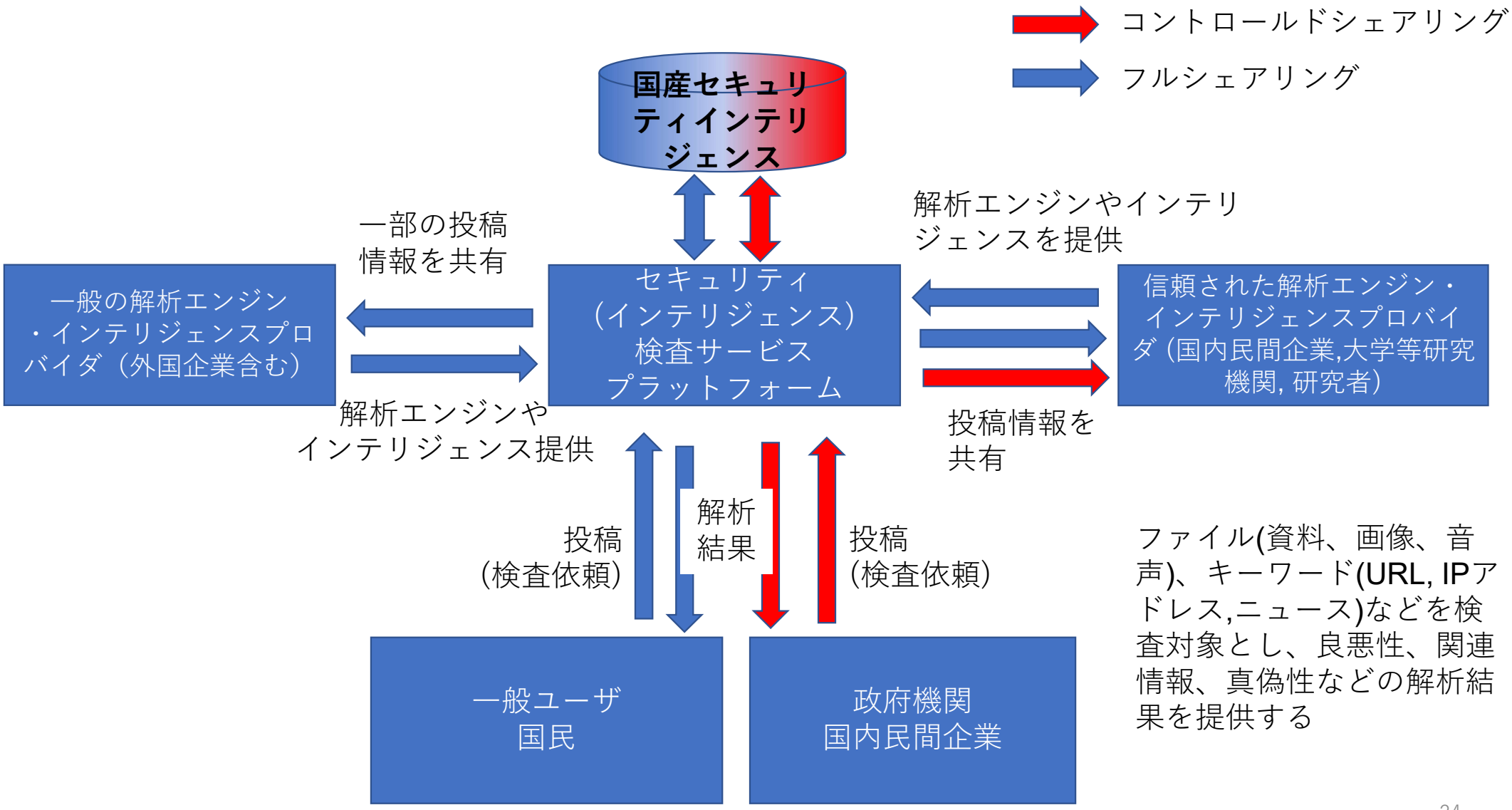
2. ファイルやURLだけでなく、様々な入力データの検査を行う

- ニュースや情報の信ぴょう性の検査
- 画像、動画、音声の真正性評価（ディープフェイク検知）
- 偽ショッピングサイト、不正に悪用されている電話番号
- なりすましメール、フィッシング検知

原理的には、専門家による判断が必要なすべての検査が対象となり得る。様々な分野の研究者を巻き込むことで多様な分析エンジンを用意する。研究者から見ると、サービスに投稿されたリアルなデータを使って研究を行うことができる。

3. 信用された組織だけで情報を共有する「コントロールドシェアリング」モードを新たに設定する

- 日本の企業、政府もこのサービスを利用してほしいが、ウイルストータルのように投稿したデータが自由に共有されるのでは安心してサービスが使えないため、コントロールドシェアモードを提供



ファイル(資料、画像、音声)、キーワード(URL, IPアドレス,ニュース)などを検査対象とし、良悪性、関連情報、真偽性などの解析結果を提供する

期待される効果

- 投稿された情報を蓄積することで**国産のセキュリティインテリジェンスを構築**し、経済安全保障に寄与することができる。

- 国民や政府機関、国内民間企業に対して国産の先端技術や学術界の研究成果に基づく**セキュリティサービスを提供**できる。

- 解析エンジン・インテリジェンスプロバイダ（大学や民間企業）に対して、開発した独自のセキュリティ技術をテストする環境と解析対象のデータを提供することで、**研究開発を促進**する。特に国内研究者が実サービス提供に耐える実用的なセキュリティ研究に取り組むことを促す。

- 上記の効果が相乗効果を生み、**負のスパイラルからの脱却**により、**国内セキュリティ産業、学術研究の育成と独自インテリジェンス蓄積**が推進される。

実現に向けた課題

- セキュリティ(インテリジェンス)検査サービスプラットフォームが現在存在しない。この新規構築、運用には多くのコストが掛かる

- 国産の解析エンジン、インテリジェンスを提供する技術、体力、能力のある研究組織（民間企業、大学）が限られる。何らかの資金面でのサポートが必要（大学研究室は外部資金がなければ大型プロジェクトに参画できない）