# FIRST Annual Conferenceの発表を紹介します

富士通株式会社 富士通研究所
データ&セキュリティ研究所
主管研究員 / Global Fujitsu Distinguished Engineer
海野 由紀

# 自己紹介

- 海野 由紀（うんの ゆき）
- 主務：D&S研 サイバーセキュPJ
  - サイバーセキュリティ対策技術の研究
  - 最近はAIセキュリティの研究
- 兼務：情セキ本）IHC
  - インシデントハンドリングにまつわるエトセトラ
- その他：GFDE



https://www.fujitsu.com/jp/about/global-fde/

# はじめに

- 主に学生やセキュリティ業界の新人向け
- セキュリティの現場（実際の業務）を知る手がかり
- 研究テーマを決める手がかり

# FIRSTとは？

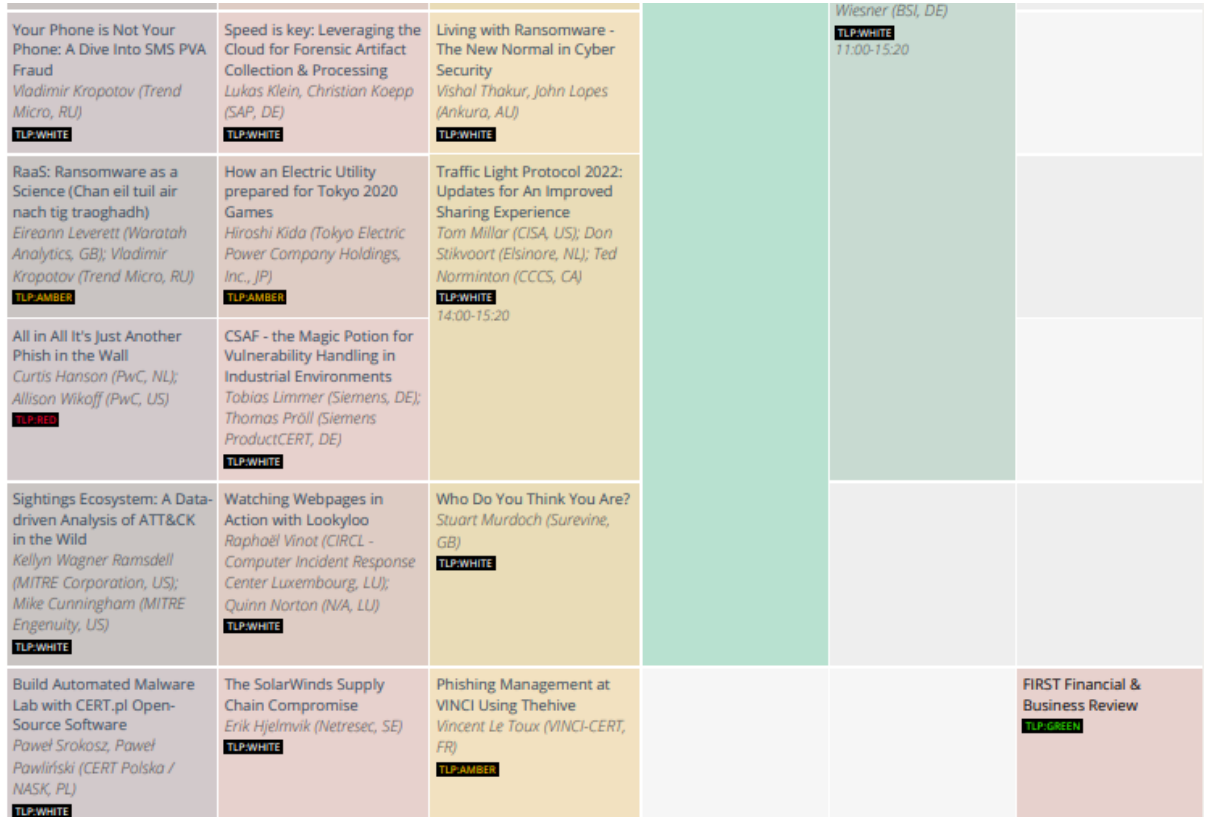
FUJITSU

- FIRST is the **F**orum of **I**ncident **R**esponse and **S**ecurity **T**eams.
- 1990年設立
  - CERTコーディネーションセンターが設立された1年後
- セキュリティチーム，インシデントレスポンスチームにおいて相互の関心事に関する情報交換や協力が重要課題
  - 新しい脆弱性，広範囲に及ぶ攻撃など
- 参加者のセクタは政府、民間、学術界と幅広い
- FIRST Annual Conferenceを開催し，コンピュータ・セキュリティとインシデントレスポンスチームの世界的な連携と協力を促進

# TLPについて

FUJITSU

- 各発表にはどのように情報が共有されるべきなのかを示すTLPが記されている



| | | | | | |
|---|---|---|---|---|---|
| Your Phone is Not Your Phone: A Dive Into SMS PVA Fraud<br>*Vladimir Kropotov (Trend Micro, RU)*<br>TLP:WHITE | Speed is key: Leveraging the Cloud for Forensic Artifact Collection & Processing<br>*Lukas Klein, Christian Koepp (SAP, DE)*<br>TLP:WHITE | Living with Ransomware - The New Normal in Cyber Security<br>*Vishal Thakur, John Lopes (Ankura, AU)*<br>TLP:WHITE | | *Wiesner (BSI, DE)*<br>TLP:WHITE<br>*11:00-15:20* | |
| RaaS: Ransomware as a Science (Chan eil tuil air nach tig traoghadh)<br>*Eireann Leverett (Waratah Analytics, GB); Vladimir Kropotov (Trend Micro, RU)*<br>TLP:AMBER | How an Electric Utility prepared for Tokyo 2020 Games<br>*Hiroshi Kida (Tokyo Electric Power Company Holdings, Inc., JP)*<br>TLP:AMBER | Traffic Light Protocol 2022: Updates for An Improved Sharing Experience<br>*Tom Millar (CISA, US); Don Stikvoort (Elsinore, NL); Ted Norminton (CCCS, CA)*<br>TLP:WHITE<br>*14:00-15:20* | | | |
| All in All It's Just Another Phish in the Wall<br>*Curtis Hanson (PwC, NL); Allison Wikoff (PwC, US)*<br>TLP:RED | CSAF - the Magic Potion for Vulnerability Handling in Industrial Environments<br>*Tobias Limmer (Siemens, DE); Thomas Pröll (Siemens ProductCERT, DE)*<br>TLP:WHITE | | | | |
| Sightings Ecosystem: A Data-driven Analysis of ATT&CK in the Wild<br>*Kellyn Wagner Ramsdell (MITRE Corporation, US); Mike Cunningham (MITRE Engenuity, US)*<br>TLP:WHITE | Watching Webpages in Action with Lookyloo<br>*Raphaël Vinot (CIRCL - Computer Incident Response Center Luxembourg, LU); Quinn Norton (N/A, LU)*<br>TLP:WHITE | Who Do You Think You Are?<br>*Stuart Murdoch (Surevine, GB)*<br>TLP:WHITE | | | |
| Build Automated Malware Lab with CERT.pl Open-Source Software<br>*Paweł Srokosz, Paweł Pawliński (CERT Polska / NASK, PL)*<br>TLP:WHITE | The SolarWinds Supply Chain Compromise<br>*Erik Hjelmvik (Netresec, SE)*<br>TLP:WHITE | Phishing Management at VINCI Using Thehive<br>*Vincent Le Toux (VINCI-CERT, FR)*<br>TLP:AMBER | | | FIRST Financial & Business Review<br>TLP:GREEN |

https://www.first.org/conference/2022/FIRST2022-Conference-Program.pdf

- 4種類のTraffic Light Protocol (TLP)

| | |
|---|---|
| TLP:RED | 公開不可，関係者限定 |
| TLP:AMBER | 限定公開，関係者が所属する組織内で共有可能 |
| TLP:GREEN | 限定公開，コミュニティ内で共有可能 |
| TLP:WHITE | 制限なく共有可能 |

https://www.first.org/tlp/docs/tlp-v1-jp.pdf

# 本日ご紹介する発表（#FIRSTCON21より）

FUJITSU

1. AIL Framework: Practical and Efficient Data-Mining of Suspicious Websites, Forums and Tor Hidden-Services

2. Extending ATT＆CK with the ATT&CK Workbench

3. Build Your Own Malware Analysis Pipeline using New Open Source Tools

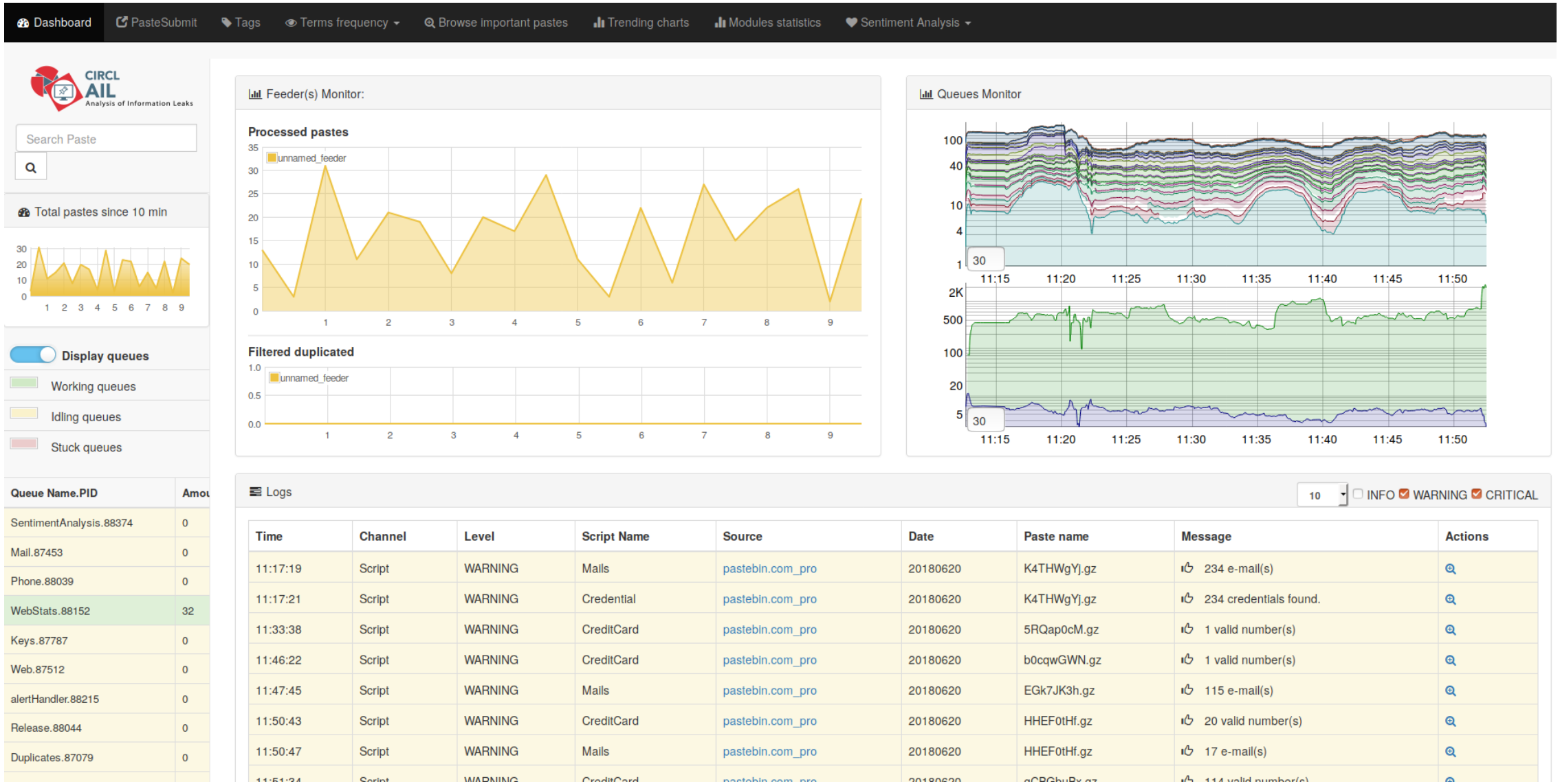
# 1. AIL Framework: Practical and Efficient Data-Mining of Suspicious Websites, Forums and Tor Hidden Services

FUJITSU

- 背景・課題
  - CSIRT (Computer Security Incident Response Team)は機微情報が外部に漏洩したかどうかを知りたい
  - 専門家が人手で分析するとコスト（時間）がかかる
- 解決方法・特徴
  - 情報漏洩分析フレームワーク（AIL framework）を開発，情報漏洩と不審な活動の発見が可能
  - Torの隠れサービス，フォーラム，Pastebinなどをクロールして分析
  - フレームワークの機能拡張が容易
- その他
  - AIL framework ソースコード
  - AIL トレーニング素材

# 画面例：AILのダッシュボード

FUJITSU



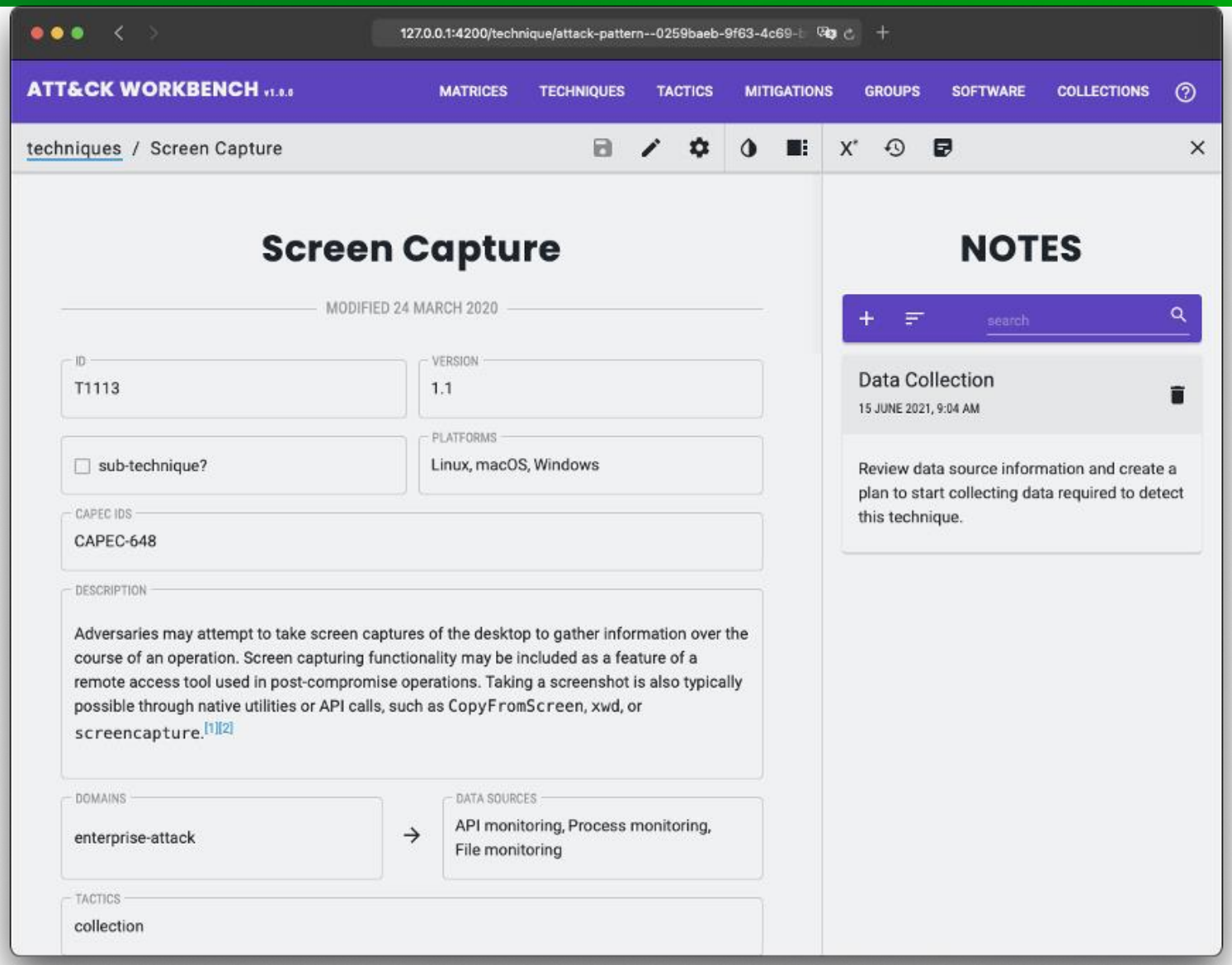
# 2. Extending ATT&CK with The ATT&CK Workbench

FUJITSU

- 背景・課題
  - サイバー攻撃への防御において，攻撃者に関する自組織のローカルなナレッジやTTP (Tactics, Techniques and Procedures)をMITRE社のATT&CK※のナレッジベースと統合するのが困難
- 解決方法・特徴
  - ATT&CKのローカルバージョンを管理・拡張するATT＆CK workbenchを開発
  - MITRE社のATT&CKナレッジベースと同期させ整合性を確保
  - 防御する側の障壁を大幅に削減
- その他
  - ATT＆CK workbench ソースコード
  - プロジェクトからのアナウンス

※･･･実際の攻撃を戦術，技術，手法で分類したナレッジベース

# 画面例：ノート追記




https://medium.com/mitre-engenuity/att-ck-workbench-a-tool-for-extending-att-ck-e1718cbfe0ef

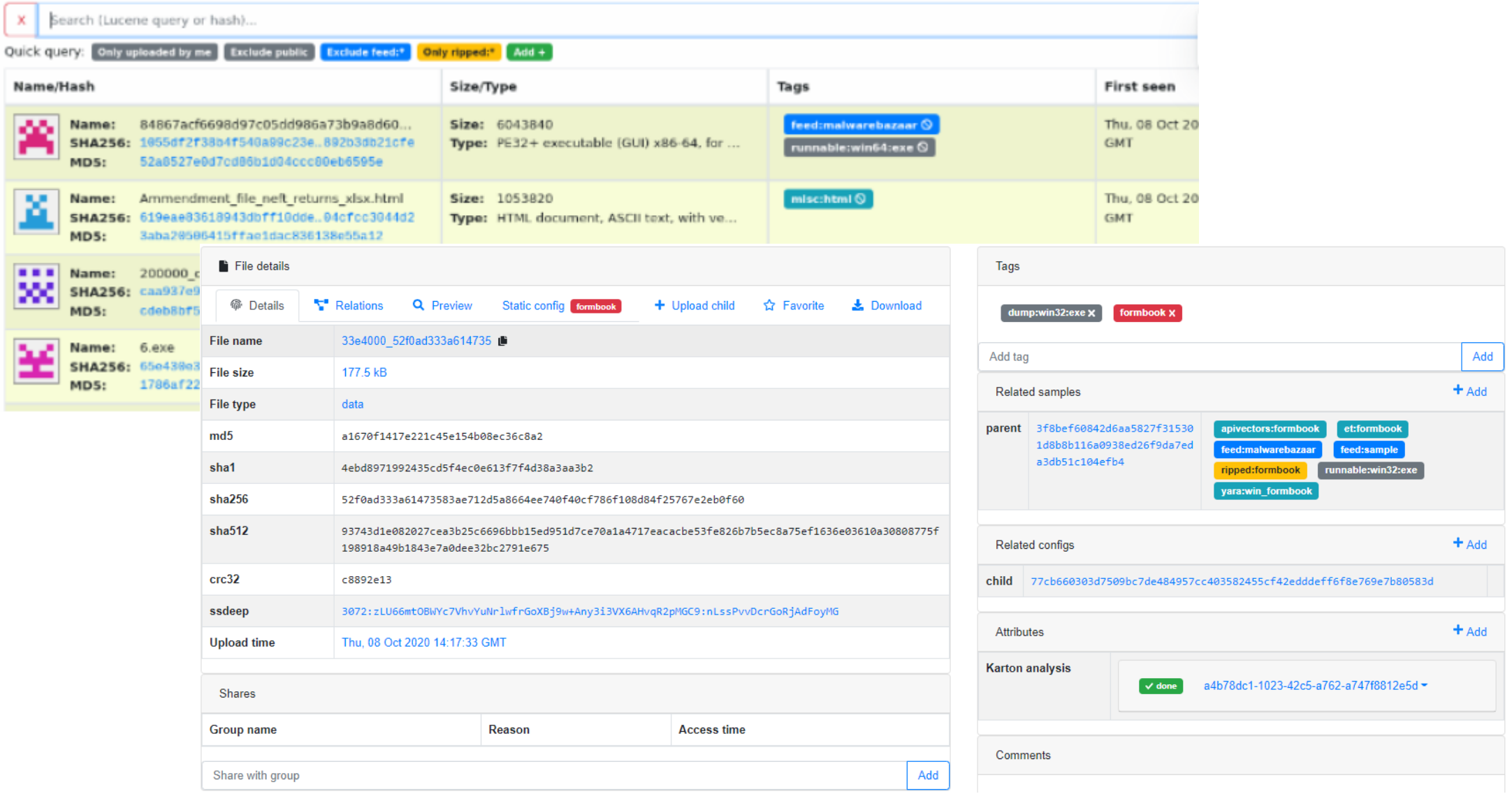
# 3. Build Your Own Analysis Pipeline Using New Open Source Tools

FUJITSU

- 背景・課題
  - 個人がマルウェア解析における失敗から得た知見の共有・活用ができていない
- 解決方法・特徴
  - マルウェアリポジトリと解析プラットフォームを開発
    - MWDB：マルウェアサンプルの解析と共有のためのコミュニティベースのオンラインサービス．マルウェア抽出とボットネットの追跡を自動化
    - Malwarecage：マルウェアのサンプルやコンフィギュレーションなど、マルウェアに関連するあらゆる技術情報のリポジトリ
    - Karton：拡張性・耐障害性に優れたマルウェア解析ワークフローのためのマイクロサービス・フレームワーク
    - Malduck：マルウェアの抽出と解析のためのライブラリ
  - その他
    - ソースコード一式

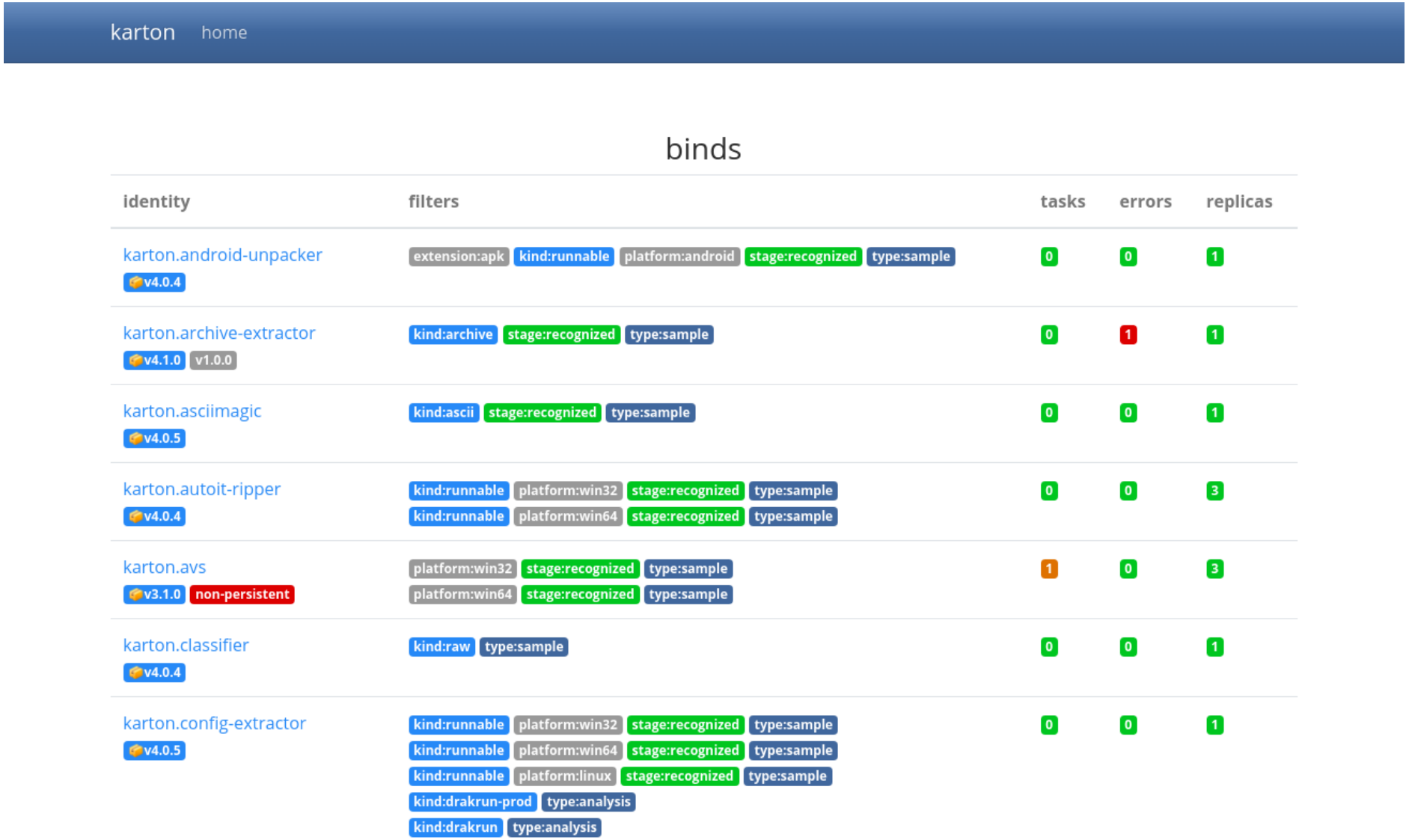
# 画面例：MWDBのクエリ

FUJITSU



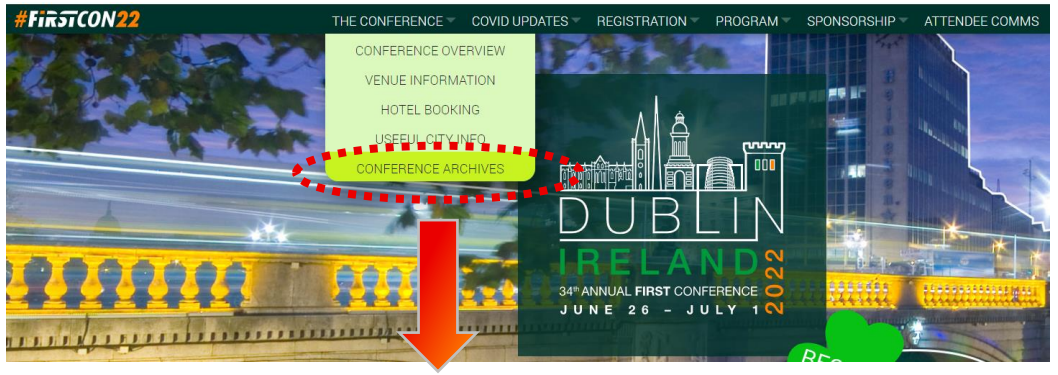
# 画面例：Karton ダッシュボード

FUJITSU



# おわりに

- Annual Conferenceの発表スライド，動画は公開されています
  - 34th Annual FIRST Conferenceの発表は8月末頃に公開予定
- その他の発表もご覧になってはいかがでしょうか
  - セキュリティの現場（実際の業務）を知る手がかり
  - 研究テーマを決める手がかり




**2022 FIRST Conference**

www.first.org/conference/2022/ Publications Program
Dublin, IE
June 26, 2022–July 1, 2022

**2021 FIRST Conference (Virtual)**

www.first.org/conference/2021/ Program
Virtual Event
June 6–June 9, 2021

**2020 FIRST Conference**

www.first.org/conference/2020/ Publications Program
Virtual Event
November 15–18, 2020

**2019 FIRST Conference**

www.first.org/conference/2019/ Publications Program
Edinburgh, GB
June 16–June 21, 2019

# Thank you