

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

- 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



伊豆 哲也

サイバーセキュリティ



井上 均史

プロジェクトマネジメント



岩松 昇

ハイブリッドIT



海野 由紀

サイバーセキュリティ



炭田 佳彰

データ



大迫 剛史

サイバーセキュリティ

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

- 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 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、学术界と幅広い
- 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

- 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

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

- 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/conference/2022/FIRST2022-Conference-Program.pdf>

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

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

○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

Dashboard PasteSubmit Tags Terms frequency Browse important pastes Trending charts Modules statistics Sentiment Analysis

Search Paste

Total pastes since 10 min

Display queues

- Working queues
- Idling queues
- Stuck queues

Queue Name.PID	Amount
SentimentAnalysis.88374	0
Mail.87453	0
Phone.88039	0
WebStats.88152	32
Keys.87787	0
Web.87512	0
alertHandler.88215	0
Release.88044	0
Duplicates.87079	0

Feeder(s) Monitor:

Processed pastes

Filtered duplicated

Queues Monitor

Logs

10 | INFO WARNING CRITICAL

Time	Channel	Level	Script Name	Source	Date	Paste name	Message	Actions
11:17:19	Script	WARNING	Mails	pastebin.com_pro	20180620	K4THWgYj.gz	234 e-mail(s)	🔍
11:17:21	Script	WARNING	Credential	pastebin.com_pro	20180620	K4THWgYj.gz	234 credentials found.	🔍
11:33:38	Script	WARNING	CreditCard	pastebin.com_pro	20180620	5RQap0cM.gz	1 valid number(s)	🔍
11:46:22	Script	WARNING	CreditCard	pastebin.com_pro	20180620	b0cqWgWN.gz	1 valid number(s)	🔍
11:47:45	Script	WARNING	Mails	pastebin.com_pro	20180620	EGk7JK3h.gz	115 e-mail(s)	🔍
11:50:43	Script	WARNING	CreditCard	pastebin.com_pro	20180620	HHEF0tHf.gz	20 valid number(s)	🔍
11:50:47	Script	WARNING	Mails	pastebin.com_pro	20180620	HHEF0tHf.gz	17 e-mail(s)	🔍
11:51:24	Script	WARNING	CreditCard	pastebin.com_pro	20180620	c0B8huBy.gz	114 valid number(s)	🔍

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

○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

The screenshot displays the ATT&CK Workbench v1.9.0 interface. The main content area shows the details for the 'Screen Capture' technique (ID: T1113, Version: 1.1). The technique is categorized as 'enterprise-attack' and 'collection'. The description states: "Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as CopyFromScreen, xwd, or screencapture.^{[1][2]}" The 'DATA SOURCES' are listed as 'API monitoring, Process monitoring, File monitoring'. The 'NOTES' sidebar on the right contains a note titled 'Data Collection' dated '15 JUNE 2021, 9:04 AM' with the text: "Review data source information and create a plan to start collecting data required to detect this technique."

<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

○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

Search (Lucene query or hash)...

Quick query: [Only uploaded by me](#) [Exclude public](#) [Exclude feed:*](#) [Only ripped:*](#) [Add +](#)

Name/Hash	Size/Type	Tags	First seen
Name: 84867acf6698d97c05dd986a73b9a8d60... SHA256: 1055df2f38b4f540a89c23e..892b3db21cfe MDS: 52a0527e0d7cd086b1d04ccc00eb6595e	Size: 6043840 Type: PE32+ executable (GUI) x86-64, for ...	feed:malwarebazaar runnable:win64.exe	Thu, 08 Oct 20 GMT
Name: Ammendment_file_neft_returns_xlsx.html SHA256: 619eae83618943dbff10dde..04cfc3044d2 MDS: 3aba20506415ffa1dac836138e55a12	Size: 1053820 Type: HTML document, ASCII text, with ve...	misc:html	Thu, 08 Oct 20 GMT
Name: 200000_c SHA256: caa937e9 MDS: cdeb8bf5			
Name: 6.exe SHA256: 65e438e3 MDS: 1786af22			

File details

Details Relations Preview Static config **formbook** + Upload child Favorite Download

File name	33e4000_52f0ad333a614735
File size	177.5 kB
File type	data
md5	a1670f1417e221c45e154b08ec36c8a2
sha1	4ebd8971992435cd5f4ec0e613f7f4d38a3aa3b2
sha256	52f0ad333a61473583ae712d5a8664ee740f40cf786f108d84f25767e2eb0f60
sha512	93743d1e082027cea3b25c6696bbb15ed951d7ce70a1a4717eacacbe53fe826b7b5ec8a75ef1636e03610a30808775f198918a49b1843e7a0dee32bc2791e675
crc32	c8892e13
ssdeep	3072:zLU66mt0BWyc7VhvYUmr1wfrGoXBJ9w+Any313VX6AHvqR2pMGC9:nLssPvvDcrGoRjAdFoyMG
Upload time	Thu, 08 Oct 2020 14:17:33 GMT

Shares

Group name	Reason	Access time
Share with group Add		

Tags

[dump:win32.exe](#) [formbook](#)

Add tag [Add](#)

Related samples

[+ Add](#)

parent	3f8bef60842d6aa5827f315301d8b8b116a0938ed26f9da7eda3db51c104efb4	apivectors:formbook et:formbook feed:malwarebazaar feed:sample ripped:formbook runnable:win32.exe yara:win_formbook
--------	--	--

Related configs

[+ Add](#)

child	77cb660303d7509bc7de484957cc403582455cf42edddff6f8e769e7b80583d
-------	---

Attributes

[+ Add](#)

Karton analysis

[done](#) a4b78dc1-1023-42c5-a762-a747f8812e5d

Comments

画面例 : Karton ダッシュボード

karton home

binds

identity	filters	tasks	errors	replicas
karton.android-unpacker 🔗 v4.0.4	extension:apk kind:runnable platform:android stage:recognized type:sample	0	0	1
karton.archive-extractor 🔗 v4.1.0 v1.0.0	kind:archive stage:recognized type:sample	0	1	1
karton.asciimagic 🔗 v4.0.5	kind:ascii stage:recognized type:sample	0	0	1
karton.autoit-ripper 🔗 v4.0.4	kind:runnable platform:win32 stage:recognized type:sample kind:runnable platform:win64 stage:recognized type:sample	0	0	3
karton.avs 🔗 v3.1.0 non-persistent	platform:win32 stage:recognized type:sample platform:win64 stage:recognized type:sample	1	0	3
karton.classifier 🔗 v4.0.4	kind:raw type:sample	0	0	1
karton.config-extractor 🔗 v4.0.5	kind:runnable platform:win32 stage:recognized type:sample kind:runnable platform:win64 stage:recognized type:sample kind:runnable platform:linux stage:recognized type:sample kind:drakrun-prod type:analysis kind:drakrun type:analysis	0	0	1

- 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はいかかでしょうか
 - 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/
Dublin, IE
June 26, 2022-July 1, 2022

[Publications](#) [Program](#)

2021 FIRST Conference (Virtual)

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

[Program](#)

2020 FIRST Conference

www.first.org/conference/2020/
Virtual Event
November 15-18, 2020

[Publications](#) [Program](#)

2019 FIRST Conference

www.first.org/conference/2019/
Edinburgh, GB
June 16-June 21, 2019

[Publications](#) [Program](#)

Thank you

