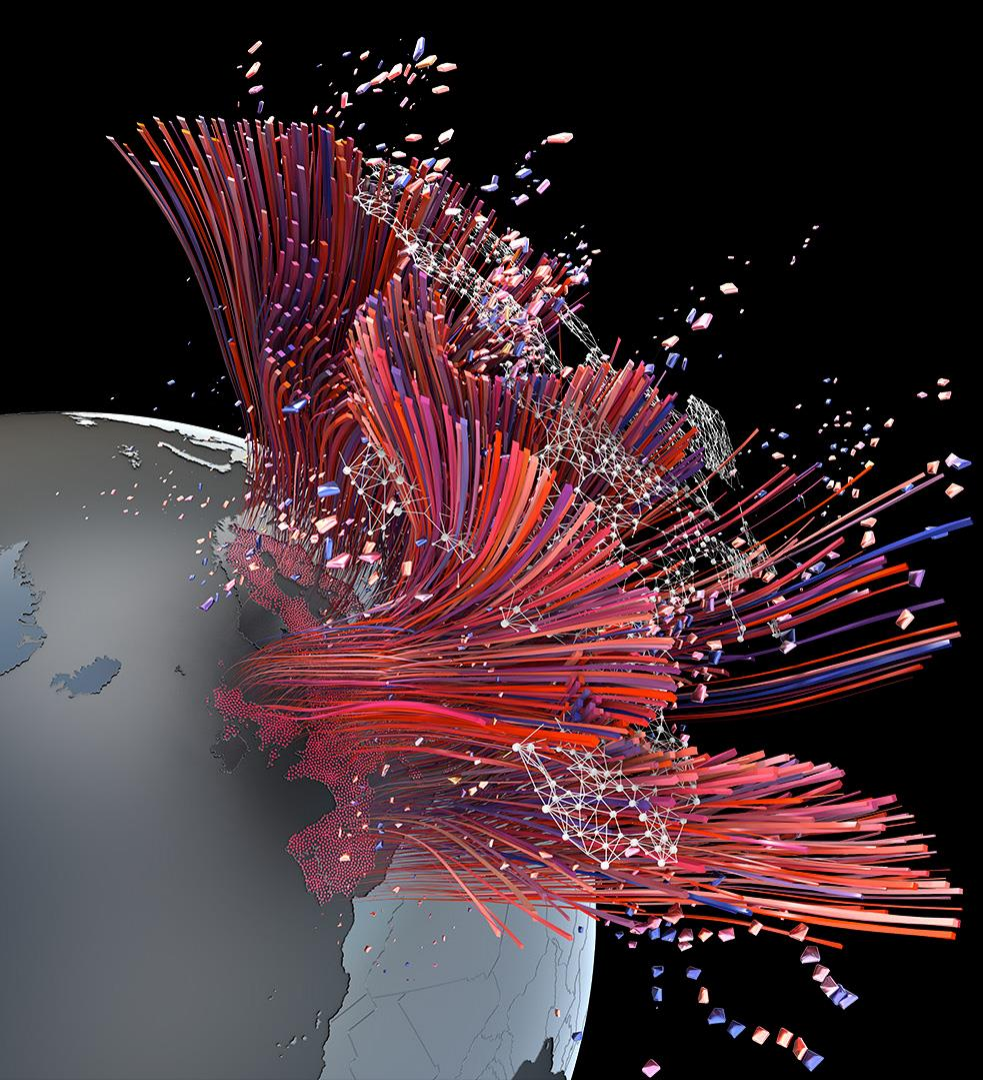


お仕事紹介
- インシデントハンドラー

トレンドマイクロ株式会社
インシデントレスポンスチーム
日本Region代表　田中 啓介

Agenda

- 自己紹介
- 仕事紹介
- 職種のやりがいや魅力

自己紹介

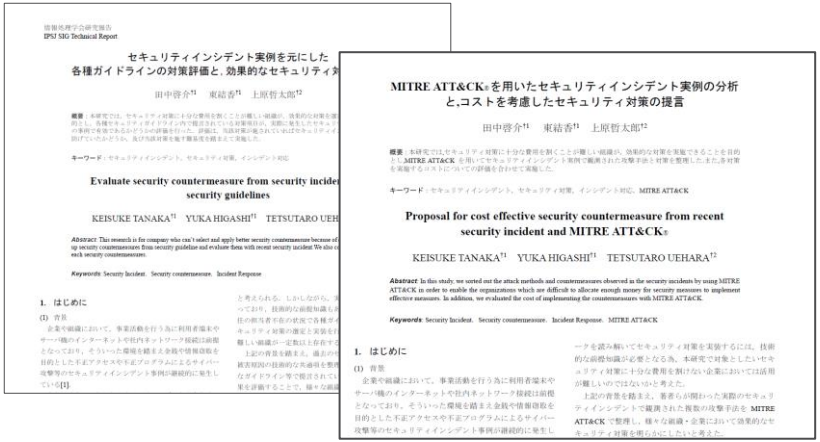
田中 啓介
アプライドサイバーセキュリティラボ部
インシデントレスポンスチーム　日本Region代表
情報処理安全確保支援士,SANS GIAC GCFA,GDAT

期間	所属/業務	役割	備考
2007年-	個人製品サポート	サポートエンジニア	・ウイルスバスター担当(技術/更新)
2009年-	法人製品サポート	サポートエンジニア	・グループウェア製品担当
2012年-	インシデントレスポンス	インシデントハンドラ	・お客様先CSIRTのリード ・ログ監視、端末調査、対策立案 （1000件以上未知のマルウェア発見）
2017年-		マネージャ	
2019年-	法人 製品提案SE	コンサルタント・ インシデントハンドラ	・インシデントレスポンス業務を兼務
2021年-	インシデントレスポンス		・国内のインシデント対応サービスをリード

自己紹介 - 研究活動

- 2020年：2件の論文投稿、研究会発表
  1. セキュリティインシデント実例を元にした各種ガイドラインの対策評価と，効果的なセキュリティ対策の提言(2020/7)
  2. MITRE ATT&CKを用いたセキュリティインシデント実例の分析と,コストを考慮したセキュリティ対策の提言(2020/10)

- 2021年：9月より立命館大学 後期博士課程 入学 (上原研究室)



セキュリティインシデント実例を元にした
各種ガイドラインの対策評価と，効果的なセキュリティ対

田中啓介[1]　東結香[1]　上原哲太郎[2]

Evaluate security countermeasure from security incide
security guidelines

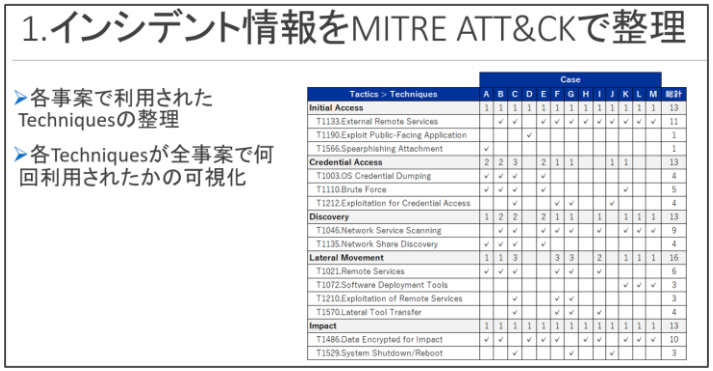
KEISUKE TANAKA[1]　YUKA HIGASHI[1]　TETSUTARO UEH

MITRE ATT&CK®を用いたセキュリティインシデント実例の分析
と,コストを考慮したセキュリティ対策の提言

田中啓介[1]　東結香[1]　上原哲太郎[2]

Proposal for cost effective security countermeasure from recent
security incident and MITRE ATT&CK®

KEISUKE TANAKA[1]　YUKA HIGASHI[1]　TETSUTARO UEHARA[2]



1.インシデント情報をMITRE ATT&CKで整理

- 各事案で利用されたTechniquesの整理
- 各Techniquesが全事案で何回利用されたかの可視化

	Case												
Tactics > Techniques	A	B	C	D	E	F	G	H	I	J	K	L	M	総計
Initial Access	1	1	1	1	1	1	1	1	1	1	1	1	1	13
T1133.External Remote Services		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	11
T1190.Exploit Public-Facing Application				✓										1
T1566.Spearphishing Attachment	✓													1
Credential Access	2	2	3		2	1	1			1	1			13
T1003.OS Credential Dumping	✓	✓	✓		✓									4
T1110.Brute Force	✓	✓	✓		✓						✓			5
T1212.Exploitation for Credential Access			✓			✓	✓		✓					4
Discovery	1	2	2		2	1	1		1		1	1	1	13
T1046.Network Service Scanning			✓	✓		✓	✓		✓		✓	✓	✓	9
T1135.Network Share Discovery	✓	✓	✓			✓								4
Lateral Movement	1	1	3			3	3		2		1	1	1	16
T1021.Remote Services	✓	✓	✓			✓	✓		✓					6
T1072.Software Deployment Tools											✓	✓	✓	3
T1210.Exploitation of Remote Services				✓		✓	✓							3
T1570.Lateral Tool Transfer				✓		✓	✓		✓					4
Impact	1	1	1	1	1	1	1	1	1	1	1	1	1	13
T1486.Data Encrypted for Impact	✓	✓		✓	✓	✓		✓	✓		✓	✓	✓	10
T1529.System Shutdown/Reboot				✓			✓		✓					3

1)https://ipsj.ixsq.nii.ac.jp/ej/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=206131&item_no=1&page_id=13&block_id=8
2)https://ipsj.ixsq.nii.ac.jp/ej/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=208491&item_no=1&page_id=13&block_id=8

Agenda

- 自己紹介
- 仕事紹介
- 職種のやりがいや魅力

仕事紹介 (インシデント対応)

お客様から相談

何が起きているかヒアリング

ツールの設置（ネットワーク,端末上）

攻撃手法・侵入原因を究明

調査結果・再発防止策を報告・提案

担当者

- 営業
- 製品エンジニア
- 製品エンジニア
- マルウェア解析者
- フォレンジック解析者
- インシデントハンドラー

インシデントハンドラーが提供するもの

インシデントに対するお客様のニーズ

- 侵入経路
- 侵入原因
- 安全宣言の条件
- 情報漏洩有無

Incident Handlerが提供するもの

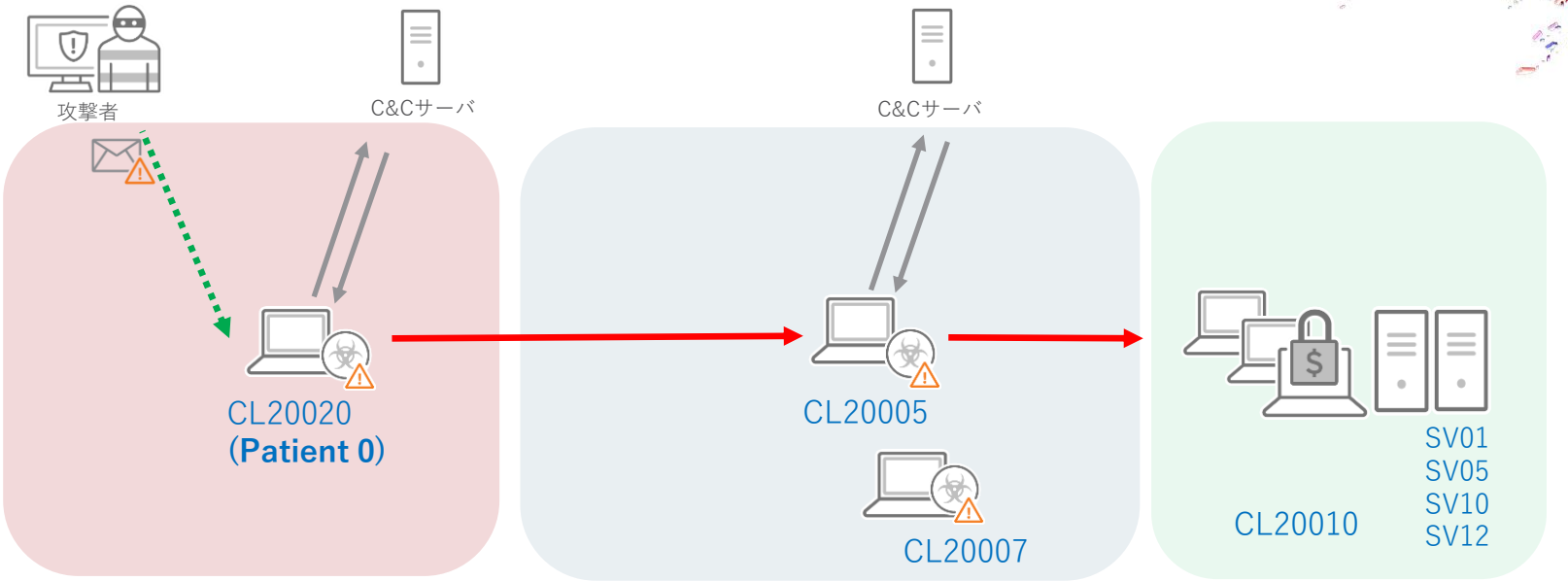
- 様々な確定・未確定情報から現状を把握し、整理
- Scoping（ゴール設定）
- 当社が支援可能かどうか及び、当社支援内容を確定

インシデントハンドラーが提供するもの

インシデントに対するお客様のニーズ	Incident Handlerが提供するもの
• 侵入経路 • 侵入原因 • 安全宣言の条件 • 情報漏洩有無	• 確定情報か 、整理 （コール設定） • 当社が支援可能かどうか 及び、当社支援内容を確定

- 技術的に可能？
- 実施することでお客様の期待が満たせそう？
- 社内で解析エンジニアはアサイン出来るか？

参考：フェーズ毎にクリアになるポイント



端末調査で明確になるエリア

ウイルス検知ログや周辺ログで明確になるエリア

ヒアリングで明確になるエリア

Agenda

- 自己紹介
- 仕事紹介
- 職種のやりがいや魅力

仕事のやりがいや魅力

勉強になること

- 日々、様々な攻撃の手法とその痕跡を見ることが出来る
  - 特段目新しい手法ではなくても、「今本当に利用(悪用)されている」攻撃手法を自分の目で見れることに魅力を感じる

やりがい

- 自身が判断・決定した調査・対応方針を提示することで、当初曇っていたお客様の顔が晴れやかになり、対応終了後お客様と共に達成感を得られる
- インシデントをきっかけにお客様のIT環境を強固にする提案が出来、お客様や社会に貢献できている実感が得られる


TREND MICRO
THE ART OF CYBERSECURITY