SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

MITRE ATT & CK Techniques の関連性に基づく攻撃検知の検討
Study on Attack Detection Based on Relevance of MITRE ATT & CK Techniques

葛西　裕紀 *　　岡田　怜士 *　　満永　拓邦 *
Yuki Kasai　　Satoshi Okada　　Takuho Mitsunaga

キーワード キーワード MITRE ATT & CK 階層型クラスタリング 攻撃検知

あらまし

米国 MITRE 社が開発したフレームワークである ATT & CK [1] は攻撃者による行動を体系化したものであり、攻撃シナリオの策定やそれに対する防御手法の検討に有用である．4 種類ある ATT & CK の要素の一つである Technique は、攻撃者が目標を達成するために実行する個別の攻撃手法として定義されている．2020 年に発表された論文 [2] では, MITRE ATT & CK によって報告された APT およびソフトウェア攻撃データをグルーピングする研究を行っている．本研究では, 現在 MITRE ATT & CK で公開されている APT グループをグルーピングし, その結果を用いて攻撃の検知率を向上させる手法を提案する．

参考文献

[1] The MITRE Corporation,“ATT & CK, Available: https://attack.mitre.org/

[2] Rawan Al-Shaer, Jonathan M. Spring, Eliana Christou, “Learning the Associations of MITRE ATT & CK Adversarial Techniques,” IEEE Conference on Communications and Network Security (CNS)， pp. 1–9

* 東洋大学, 〒 115-8650　東京都北区赤羽台 1-7-11 INIAD HUB-1, TOYO University, INIAD HUB-1, 1-7-11 Akabanedai, Kita-ku, Tokyo 115-8650,