[ポスター発表] 研究報告

OSINTによる中小企業のサイバーセキュリティ対策向上

田中 啓介[1]　上原 哲太郎[2]

Improving cyber security countermeasure of SMEs through OSINT

1. はじめに

1.1 背景

昨今中小企業において，ランサムウェア等によるサイバー攻撃・セキュリティインシデントが継続発生している．昨今のランサムウェアによる被害件数は 2 年前の約 6 倍程度であったとされており，ランサムウェア被害の内 52 % が中小企業の被害であるとされている [1].

著者らの先行研究では，中小企業におけるサイバーセキュリティ対策の現状や課題を整理する為にインタビュー調査と分析を実施し，担当者が自社のセキュリティ対策を推進する為には，自社セキュリティ状況を客観的に分析し，正しい現状理解を行うことがセキュリティ対策レベル向上において重要な点であると考察した [2], [3].

中小企業の現状理解を外部から支援するにはヒアリング，診断ツールや IDS 等によるアセスメント等が考えられるが，いずれもそれなりのコストが必要であり, 安価にリスクが可視化出来, セキュリティ対策行動を促せるような仕組みが出来ないかと考えた.

1.2 概要

本研究では, 中小企業のリスクを可視化し，対策行動を促す為の手法として OSINT(Open Source INTelligence) が利用可能かを検証する．OSINT とは，インターネット上に公開された情報を整理・深堀し，ターゲットに関する必要な情報を得る為の手法であり，サイバー攻撃者がターゲット組織の脆弱な侵入口の特定に用いたり，セキュリティリサーチャが不正プログラム情報や不正通信先等を元に，攻撃団体の特定等を行う際などに用いられる．本研究では，対策行動に結びつくであろう OSINT 情報源と, その具体的な利用手順を確立し, その後効果の実証や活用を目指す.

1.3 貢献

本研究で目指す貢献は以下のとおりである.

- 中小企業が OSINT を活用した調査手法を理解し, 安価に利用できるようになる
- 中小企業が OSINT で得られた情報を元に追加のセキュリティ対策を行う動機を得る

2. 関連研究

OSINT に関する先行研究では，攻撃者がターゲット企業や個人の情報を収集する過程をモデル化し対策に活かそうとする上原ら [4] の研究や，セキュリティアナリストが行っている OSINT 調査をモデル化・自動化を試みた川北ら [5] の研究が存在するが，いずれも本研究とは目的や調査対象が異なる．中小企業のリスク可視化や注意喚起の手法として OSINT を利用している公表された論文は確認されなかったが，OSINT を利用して企業のリスクアセスメントを行うサービスがいくつか存在していた [6], [7]．本研究と目的や調査手法が近いが，サービス費用が 250 万円程度からと高価であり，調査範囲や調査項目も多岐に渡っている為，本研究では調査項目を限定し，実施コストを下げた提供手法や，企業担当者が自ら実施可能な手法を検討したい.

3. 手法

3.1 概要

研究は以下のステップで実施する．まずは OSINT 情報源の整理, 具体的な調査手法の確立を行い，中小企業が調査結果を受けてセキュリティ対策行動を行えるかを検証し，最終的には自動化や手順化などを経て，企業自身で OSINT 調査を行い結果を確認出来るような状態を目指す.

(1) OSINT 情報源を整理し・対策行動に結びつき得る情報源を選定する
(2) 具体的な調査手法を確立し手順化する
(3) セキュリティ対策向上に寄与できるものかを複数社で

[1] 立命館大学 大学院 情報理工学研究科, トレンドマイクロ株式会社
[2] 立命館大学 情報理工学部

検証する

(4) 自動的な調査システム，あるいは容易な調査手順を確立する

本ポスター発表では, 研究全体の内, 図 1 の赤枠内における進捗内容を発表する.

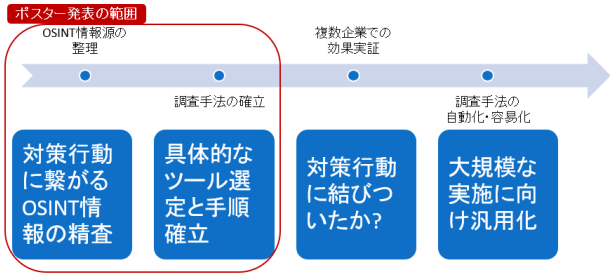

図 1 研究概要

3.2 調査内容

本ポスター発表では, 主に以下の調査目的に対して簡易的な手法を検証する.

- 外部公開メールアドレスの洗い出し
- グローバル IP アドレスの公開ポート調査
- Web サイト上の脆弱性や個人情報の調査

例として「E Mail Hunter」というサービスを利用して特定のメールドメインに紐づくメールアドレスを洗い出したものが図 2 である. 実際のサイバー攻撃者もこういったサービスを利用して標的型メールを送る先のメールアドレスを収集する為，当該メールアドレスについては不審メールの着弾を警戒する必要がある.

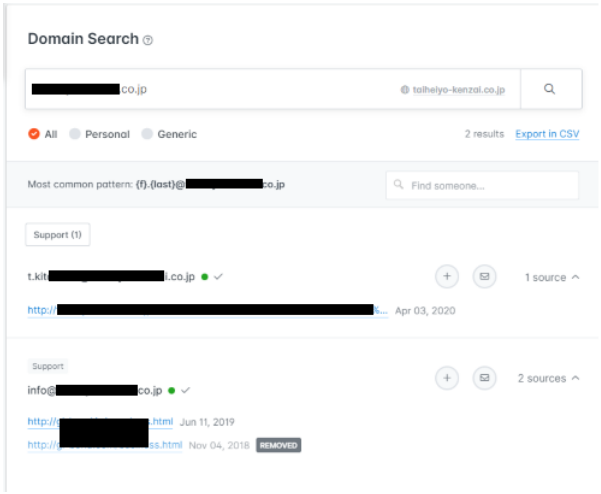

図 2 E Mail Hunter による調査

4. おわりに

ポスター発表による有識者との議論やフィードバックを経て，技術的な実施内容を検討・検証し，複数の中小企業への試験提供，最終的にある程度の効果が認められればシステム化により多数の中小企業が利用できるような状態にすることを検討していきたい.

参考文献

[1] 警察庁，“令和 4 年上半期におけるサイバー空間をめぐる脅威の情勢等について” https://www.npa.go.jp/publications/statistics/cybersecurity/ (2022/9/15).
[2] 田中啓介, 上原哲太郎, 古川佳和, 野田幹稀,” 中小企業における情報セキュリティ対策状況のインタビュー調査”, 研究報告インターネットと運用技術（IOT）, 2022-IOT-56, 43 号, p1-8, (2022-02-28)
[3] 田中啓介, 上原哲太郎, 古川佳和, 野田幹稀,” 中小企業における情報セキュリティ課題の抽出- M-GTA を用いたインタビュー分析”, 信学技報, vol. 122, no. 85, IA2022-12, pp.67-70, (2022-06-16)
[4] 上原航汰, 向山浩平, 藤田真浩, 西川弘毅, 山本匠, 河内清人, 西垣正勝. “OSINT を利用した標的型メール攻撃手法に関する基礎検討”. コンピュータセキュリティシンポジウム 2017 論文集, 2017(2).
[5] 川北将, 島成佳. “オープンソースインテリジェンスと深層強化学習によるサイバー脅威分析手法の検討”. コンピュータセキュリティシンポジウム 2017 論文集, 2017(2).
[6] ソリトンシステムズ株式会社，“サプライチェーンセキュリティリスク調査サービス” https://www.soliton.co.jp/news/2022/004703.html, (2022/3/2).
[7] 株式会社ユービーセキュア，“Attack Surface 調査サービス” https://www.ubsecure.jp/assessment/attack-surface-assessment, (2022/10/10 時点).