

令和 5 年 6 月 14 日現在

機関番号：34428

研究種目：基盤研究(C)（一般）

研究期間：2018～2022

課題番号：18K11593

研究課題名（和文）サイバー犯罪のリスク発見・判別支援の為に統計的プロファイル分析モデルに関する研究

研究課題名（英文）Research on statistical analysis models for assessing the risk of cybercrime victimization and their practical implementation

研究代表者

針尾 大嗣 (hario, daiji)

摂南大学・経営学部・教授

研究者番号：80386672

交付決定額（研究期間全体）：（直接経費） 1,800,000円

研究成果の概要（和文）：本研究は、サイバー関連犯罪の犯行特徴をまとめたデータベース構築と犯行テーマ（犯行プロファイルセット）分類のための統計的プロファイリング・アプローチ、及びその活用方法を検討することを目的として、(1)サイバー関連犯罪に関わる犯行特徴（実行犯の特徴、犯行ツール、犯行手口、被害内容等）のデータベース化、(2)データベースから犯行テーマを分類・抽出するための統計的分析アプローチの検討、(3)当該成果に基づいた防犯用教材の制作に取り組む。

研究成果の学術的意義や社会的意義

一般犯罪の犯行行動と犯行者の属性推定を主な目的とした従来の統計的プロファイリング研究に対し、本研究は、情報通信ネットワークを介して実行される新たな犯罪であるサイバー犯罪を対象として、その多様な犯行形態を可視化分析するための統計的プロファイリングアプローチを検討した。世界的に遅れている我が国のサイバー関連犯罪を対象とした統計的プロファイリング研究の学術的発展に大きく貢献すると同時に、当該犯罪に向けた警察活動の課題解決に寄与するとともに、その成果を市民社会に実践的に還元するという点で意義のあるものである。

研究成果の概要（英文）：The purpose of this study is to build a database that summarizes the characteristics of cyber-related crimes and to examine a statistical profiling approach for classifying crime themes (crime profile sets), as well as its utilization methods. The study aims to: (1) Database construction of crime characteristics related to cyber-related crimes (characteristics of perpetrators, crime tools, operation, the damage, etc.) (2) Investigation of statistical analysis approaches for classifying and extracting crime themes from the database. (3) Development of crime prevention materials based on the aforementioned findings.

研究分野：情報学

キーワード：サイバー犯罪 プロファイル分析 防犯教育

1. 研究開始当初の背景

犯罪情報分析は「行動科学を応用して犯罪に関連する情報を分析し、犯罪捜査や犯罪予防等の警察活動に寄与する知見を得る技術」と定義され、戦略的目的と戦術的目的に分類される。我が国の警察等機関においては、中長期間にわたる犯罪予防対策などのマネジメントを行う戦略的目的の分野において地域防犯マップや犯罪データベース、個別事件の犯人検挙など戦術的目的の分野においては、犯罪前歴者の記録を基にした犯行パターンや犯行地点の抽出を行う情報分析支援システムが導入されている。しかしながらサイバー犯罪に関しては、日々進化する IT の技術的知識が必要であることや事象件数が顕在的・潜在的にも膨大であること、また匿名性が高く地理的制約を受けにくいいため発生時期、犯行位置の特定が困難であることなど、犯行ツールの特殊性や被害リスクを含めこれまでの犯罪とは異なる特徴を持つことから、従来の犯罪情報分析によるアプローチの限界も指摘されている。そのためサイバー関連犯罪の犯行特徴等情報を迅速に取り入れ、リスク判別し、関係者間での迅速な情報共有を可能にする新たな犯罪情報分析法の開発が急務となっている。犯行抑止と犯人検挙の捜査支援のための犯罪情報分析は、オフエンダープロファイリングと呼ばれ、方法論の違いにより臨床的プロファイリングと統計的プロファイリングに分けられる。前者は心理学や精神医学に基づいて犯罪者の犯行動機に着眼した質的分析を行い、犯罪者のパーソナリティに関する個別的理解を深めることを重視するアプローチであり、後者は犯人像と犯行内容の関連性に関して犯罪統計データを用いた量的分析を行い、犯行行動の予測を主に目的としたアプローチである。我が国においては、科学警察研究所が犯罪者プロファイリング研究会を開催して両プロファイリングに関する同様の研究が進められているものの、犯罪統計データの整備が遅れていることもあって実証事例は、(研究着手前時点において)確認できるもので 328 件と米英両国に比べて少ない。またサイバー犯罪を対象とした研究事例は、申請者が調査した限りにおいて一桁台と同様に少なく、未発展分野と言える。

2. 研究の目的

そこで本研究は、サイバー関連犯罪の犯行特徴をまとめたデータベース構築と犯行テーマ(犯行プロファイルセット)分類のための統計的プロファイリング・アプローチ、及びその活用方法を検討することを目的として、サイバー関連犯罪に関わる犯行特徴(実行犯の特徴、犯行ツール、犯行手口、被害内容等)のデータベース化、データベースから犯行テーマを分類・抽出するための統計的分析アプローチの検討、当該成果に基づいた防犯用教材の制作に取り組む。

3. 研究の方法

初年度から翌年度にかけて地元警察、自治体、学校関係者へのヒアリング調査や事件記録等文献調査を基にサイバー関連犯罪に関する事件情報を収集し、サイバー関連犯罪の各種構成要素及び被害件数等をまとめたデータベース構築を行った。これをもとに翌々年度以降、多次元尺度構成法による犯行テーマの抽出ならびに事件分類に用いる分析モデルの検討を行った。最終年度は、当該分析モデルを用いて各種サイバー関連犯罪の特徴をまとめたサイバー防犯学習カード(犯行プロファイルセットを罪種別にまとめたカード)を作成し、地元開催の小学生向け防犯ワークショップにおいて、防犯教材として活用し、その有用性について評価を行なった。

4. 研究成果

サイバー関連犯罪に関わる犯行特徴(犯人特徴、犯行ツール、犯行手口、被害内容等)のデータベース化

地元警察、自治体、学校関係者ならびに被害者に対するヒアリング調査および事件記録・報道等文献調査をもとにネットワーク利用犯罪に定義される各種事件情報を収集し、各事犯を構成する犯行要素(実行犯の特徴、目的、ソフトウェアや端末などの犯行ツール、犯行手口、被害者の特徴、被害内容等)となる 75 の変数からなるデータベースを構築した。図 1 は、事件情報をもとにストーキング犯罪に関する犯行要素をまとめたもの。

犯行テーマを分類・抽出するための統計的アプローチの検討

各事犯(ケース)を 23 の罪種別分類し、犯行要素の発生状況を 0 と 1 のダミー変数化したデータセットを作成した。同一罪種内の犯行テーマを分類する方法として、これらのデータセットについて多次元尺度構成法を用いた分析アプローチについて考案した。図 2 は、多次元尺度構成法によりサイバーストーカーの 3 タイプ(犯行テーマ: Dominant Type、

Operational Type、Violence Type) とそれを特徴づける犯行要素をマッピングした犯行プロファイルセット。

当該成果に基づいた防犯用教材の制作

地元小学生を対象としたサイバー防犯教室を開催し、 の犯行プロファイルセットを簡易にまとめた学習カードを作成し、サイバー犯罪の特徴及び被害内容を解説する教材として活用した。

Variables reflecting stalking actions and their definitions

#	Variable	N	%	Definition
A1	SMS	143	64.1	Sends frequent Short Message or SNS Message
A2	Entice friend of LINE	102	45.7	Entices friend(follower) of LINE by online *LINE is most popular SNS in Japan
A3	Backbiting on LINE	98	43.9	Posts backbitings to LINE *LINE is most popular SNS in Japan
A4	eMail	95	42.6	Sends frequent email
C1	Invaide Privacy	68	30.5	Invaides the victim's privacy outside his/her home
A5	Follow SNS account	68	30.5	Continues following SNS account persistently even though prohibited
C2	Insult	54	24.2	Insults the victim
D1	Threat violence	47	21.1	Threatening to cause physical violence/danger to health to the victim
A6	Not clear logs	45	20.2	Refuses to delete logs (photo, diary,tweet) on SNS
E2	Telephone	43	19.3	Makes frequent telephone calls
D2	Threaten to destroy	36	16.1	Threatening to destroy the victim's possessions
A7	Re-follow	35	15.7	Requesting to re-register as a friend of SNS, persistantly
C4	Sextortion	34	15.2	Distributes sexually explicit image and video
A9	Blackmail	32	14.3	Sends frequent mail under an alias
A10	Fabrication on twitter	23	10.3	Distributes fabrication on Twitter
C3	Rummage	23	10.3	Rummages through victim's belongings
D3	Threaten suicide	23	10.3	The restraineed threatens to commit suicide
D4	Threat to kill	17	7.6	Threatening to kill the victim
A11	Backbiting on twitter	16	7.2	Backbits on Twitter
F1	Follow	16	7.2	Follows or trails the victim
B6	Assault	15	6.7	Physically assaults or attempts to physically assault the victim by hand(kick, punch, strangle)
F2	Visit to home	14	6.3	Visits the victim's home
A12	Fabrication on Facebook	13	5.8	Distributes fabrication on Facebook
B1	Stolen valuables	13	5.8	Steals valuable items from the victim(credit cards, money,etc)
B2	Damage	12	5.4	Destroys or damages victim's belongings
E1	Unwanted object	8	3.6	Delivers unwanted objects,gifts,photos
A8	Entice friend of Facebook	7	3.1	Entices friend(follower) of Facebook by online
E3	Letter	5	2.2	Sends letters
B3	Intrude	4	1.8	Intrudes or tries to intrude into the victim's home without permission
B4	Stolen belongings	4	1.8	Steals victim's personal belongings(diary, letters, etc)
B5	Attempt to kill	3	1.3	Attempts to kill the victim
D5	Threat other	3	1.3	Threatening to arrange for some other person to damage the victim
F3	Stay against wish	3	1.3	Stays in the victim's home against their wishes
F4	Visit to office or school	3	1.3	Visit teh victim's office or school
D6	Threat to harm family or friend	1	0.4	Threatening to harm victim's family or friends

図 1: ストッキングの犯行要素と該当件数

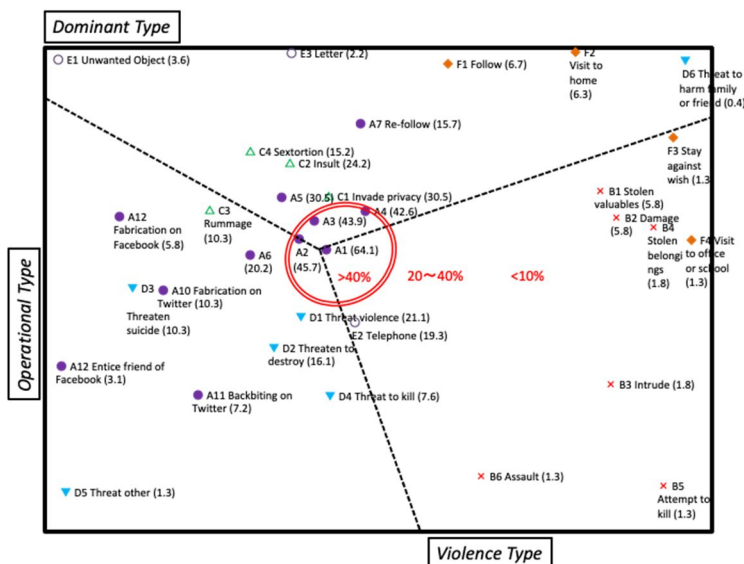


図 2: サイバーストッキングの犯行プロファイルセット

5. 主な発表論文等

〔雑誌論文〕 計1件（うち査読付論文 1件 / うち国際共著 0件 / うちオープンアクセス 0件）

1. 著者名 上田祥二、松井亮治、針尾大嗣	4. 巻 39
2. 論文標題 プレステーション5の転売者プロフィール	5. 発行年 2021年
3. 雑誌名 情報通信学会誌	6. 最初と最後の頁 83-90
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

〔学会発表〕 計3件（うち招待講演 0件 / うち国際学会 3件）

1. 発表者名 Daiji HARIO
2. 発表標題 Behavioral profiling to detect potential threats in cyberspace
3. 学会等名 EUROCRIM2019（国際学会）
4. 発表年 2019年

1. 発表者名 Daiji HARIO
2. 発表標題 Cyber risk assessment
3. 学会等名 The 46th Annual Conference of the WSC（国際学会）
4. 発表年 2019年

1. 発表者名 Daiji HARIO
2. 発表標題 Behavioral taxonomy of cyber offender
3. 学会等名 EUROCRIM2018（国際学会）
4. 発表年 2018年

〔図書〕 計0件

〔産業財産権〕

〔その他〕

-

6. 研究組織

	氏名 (ローマ字氏名) (研究者番号)	所属研究機関・部局・職 (機関番号)	備考
--	---------------------------	-----------------------	----

7. 科研費を使用して開催した国際研究集会

〔国際研究集会〕 計0件

8. 本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関
---------	---------