大阪大学 社会技術共創研究センター
Research Center on Ethical, Legal and Social Issues

ELSI NOTE No.51

2025 年 1 月 6 日

サイバーセキュリティリスクの定式化と非技術的要因に関する文献調査

Authors

岸本 充生　大阪大学 社会技術共創研究センター　センター長（2024年12月現在）
D3センター　教授

本ノートの作成は、セコム科学技術振興財団 特定領域研究助成 情報セキュリティ分野「超スマート社会の『悪』の研究」「サイバー攻撃の被害者予測システムと内部犯罪に強力な機械学習モデルの構築」研究代表者：宮地 充子（大阪大学）の一環として行ったものである。

大阪大学

目次

1. はじめに：サイバー脅威の現状

●サイバー空間における脅威は、サイバー空間におけるリスクのうち、意図的、すなわち悪意に基づくものを指す。本 NOTE ではその中でも組織に対する脅威を取り上げる。

●独立行政法人情報処理推進機構（IPA）による「情報セキュリティ脅威 2024」の脅威ランキングでは、「組織」向け脅威の 1〜5 位は次のとおりであった[1]。これはセキュリティ専門家や企業のシステム担当等から構成される「10 大脅威選考会」が投票して決定される。上位 5 位までは前年度とほぼ同じであった。

1 位　ランサムウェアによる被害

2 位　サプライチェーンの弱点を悪用した攻撃

3 位　内部不正による情報漏えい

4 位　標的型攻撃による機密情報の窃取

5 位　修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

●2024 年 3 月に公表された、警察庁による「令和 5 年におけるサイバー空間をめぐる脅威の情勢等について」では、前年度に続いて令和 5 年における脅威の動向として 1 番目にランサムウェアが取り上げられた[2]。ランサムウェアとは「感染すると端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価（金銭又は暗号資産）を要求する不正プログラム」と説明されている。ランサム（ransom）とは身代金のことであり、対価を払わなければ当該データを公開すると脅すことは二重恐喝（ダブルエクストーション）と呼ばれている。令和 5 年に警察庁が把握した件数は 197 件であり、7 割以上が二重恐喝であった。また、直接的な対価を要求されたケースのほとんどで暗号資産による支払いを要求されたという。ランサムウェアへの感染経路は、有効回答 115 件のうち 6 割を「VPN 機器からの侵入」が、2 割を「リモートデスクトップからの侵入」が占める。調査・復旧に要した費用として 1000 万円以上要したものが 4 割であった。

●本 NOTE では、上記 2 つの報告書においても組織へのサイバー脅威の 1 位に挙げられている「ランサムウェア」と、前者で 3 位に入っている「内部不正」に焦点を当て、組織がこれらの

[1] https://www.ipa.go.jp/security/10threats/10threats2024.html

[2] https://www.npa.go.jp/publications/statistics/cybersecurity/

サイバーリスクへの備えができることを目的に、ランサムウェアと内部不正のリスクを事前に予測するにあたり、技術以外の重要な因子を探究した既存研究のいくつかを紹介する。第 2 章では、サイバーセキュリティのリスク一般について、リスク（事後的には被害）を定式化する既存の試みを拡張することを試み、サイバー脅威の分類を整理する。第 3 章ではランサムウェア、第 4 章では内部者脅威に関する非技術的なリスク因子の探究を行った文献調査を行う。第 5 章では残された課題を整理する。

2．サイバーリスクの定式化

2.1　サイバーリスクの構成要素

●サイバーセキュリティのリスクは ISO/IEC 27000 シリーズにおいて定式化されている[3]。「リスク」の定義の 6 番目の注釈に「情報セキュリティリスクは、脅威（Threat）が情報資産（Asset）・・・の脆弱性（Vulnerability）を悪用し、それによって組織に損害を与える可能性と関連している」と記載されており、リスクは、脅威（T）と脆弱性（V）と資産（A）の関数であると読める。事前の観点からみるとリスクであるが、被害が顕在化したあとは損害（damage）となる。

リスク（R）or 損害（D）＝ f （脅威（T）、脆弱性（V）、資産（A））　　式 1

脅威（T）とは「システムまたは組織に損害をもたらす可能性のある、望ましくないインシデントの潜在的な原因」、脆弱性（V）とは「一つまたは複数の脅威によって悪用される可能性のある、資産または管理の弱点」と定義されている。資産（A）はデータや金銭といった守るべきもの（攻撃者からしたら盗みたいものの価値）を表している。

●米国国土安全保障省では、サイバーに限らない広い意味でのセキュリティリスクの定義について、その「拡張定義」において「インシデント、イベント、または発生に関連する脅威（Threats）、脆弱性（Vulnerabilities）、および帰結（Consequences）の関数として評価される、好ましくない結果の可能性」と記載している[4]。上記の資産（A）に代わって帰結（C）が用いられているが、考え方はほとんど同じである。

---

[3] ISO/IEC 27000 ファミリー規格は、ISO（国際標準化機構）と IEC（国際電気標準会議）の合同専門委員会 ISO/IEC JTC 1 の分科委員会 SC 27 おいて標準化が進められている。ISO/IEC 27000:2018(en) Information technology — Security techniques — Information security management systems — Overview and vocabulary.

[4] U.S. Department of Homeland Security, Risk Steering Committee - DHS Risk Lexicon. https://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf

●要するに、脅威（T）は、悪の主体が攻撃する確率である。脆弱性（V）は、攻撃があった場合に突破される確率である。資産（A）は、攻撃が成功した際に奪われる価値である。ここでは、T と V と A はそれぞれが独立ではなく、脅威（T）は、脆弱性（V）と資産（A）のそれぞれが大きいほど大きくなるという、式 2 のような関係にあることが想像できる。ただし、攻撃がランダムである場合に限りこの関係は当てはまらない。

脅威（T）＝ f （脆弱性（V）、資産（A））　　式 2

脆弱性（V）は、大企業よりも中小企業が、中央政府よりも地方自治体が、営利企業よりも教育機関や医療機関などの非営利企業が大きくなることが予想される。また、資産（A）は逆に、大企業（資産やデータ）、プラットフォーム事業者（顧客情報）、ヘルスケア産業（プライバシー情報）、政府機関（機密情報）の方が大きくなることが予想される。

●脅威（T）、すなわち攻撃確率を決める鍵となる情報は、客観的な、すなわち真の脆弱性（V）と資産（A）というよりは、悪の主体による主観的な脆弱性（V*）と資産（A*）である。そのため、脅威（T）を減らすための方策として、真の脆弱性（V）や真の資産（A）を減らすことに加えて、悪の主体からみた主観的な脆弱性（V*）や資産（A*）（場合によってはそれらだけ）を減らす、という選択肢もありうる。

脅威（T）＝ f （脆弱性*（V*）、資産*（A*））　　式 3

式 3 を式 1 に代入すると、式 4 のようになる。

リスク（R）/損害（D）＝ f （脆弱性*（V*）、資産*（A*）、脆弱性（V）、資産（A））　式 4

●ランサムウェアの場合は、パソコンやサーバ内のデータが暗号化され、元に戻す見返りとして「身代金（ランサム）」が要求される。つまり、資産（A）は「データ」そのものではなく、そのデータへのアクセスを取り戻すために支払われる「身代金」となる。逆に言うと、身代金を払ってもらえない場合は、悪の主体にとって資産（A）は（データそのものが闇で高価で売れない限り）限りなく小さくなってしまう。そのため、主観的な資産（A*）は、攻撃対象が身代金を支払ってくれる主観確率で重みづけられた期待値となる。そのため、身代金を断固支払わないという姿勢（A*を限りなくゼロに近づかせる）を見せることが、脅威（T）を減らす対策の 1 つとなりうる。

●サイバー保険に入っているかどうかも重要な要素になりうる。サイバー保険に入る際の審査を通るために、技術的に脆弱性（V）を削減したり、データのバックアップをとったりする必要があるとしたら、保険に加入するだけで V が減ることもありうる。サイバー保険で身代金がカバーされる場合はそのことがある種のモラルハザードを引き起こし、脆弱性（V）が放置されてしま

ったりする可能性がある。逆に、サイバー保険で身代金がカバーされない場合（日本の場合がそうである）の影響については第 5 節で改めて考察する。

●内部者脅威（Insider threat）の場合は、立場によっては自組織の脆弱性（V）や資産（A）については客観的に把握している場合もあるため、動機さえ強ければ脅威（T）（攻撃確率）も高くなり、リスク（R）/被害（D）も大きくなりうる。また、金銭目的の場合ももちろん多いと考えられるが、動機が恨みや不満であれば、被害を与えることそのものが目的となる場合もありえる。IPA の脅威ランキングの 3 位に「内部不正」が入っているように、悪の主体は外部とは限らない。内部者脅威としては、後述するように、不注意による非意図的なものと、意図的な（悪意ある）攻撃がある。

●近年では、複数の組織同士がネットワーク化されていることが多いため、サイバーリスクもいわゆるサプライチェーン全体で考える必要があり、サプライチェーン上で最も脆弱な部分（例えば、中小企業など）が狙われる可能性がある。業界・企業ごとにサプライチェーンの構造・特徴は異なる。

2.2　サイバーリスクの分類

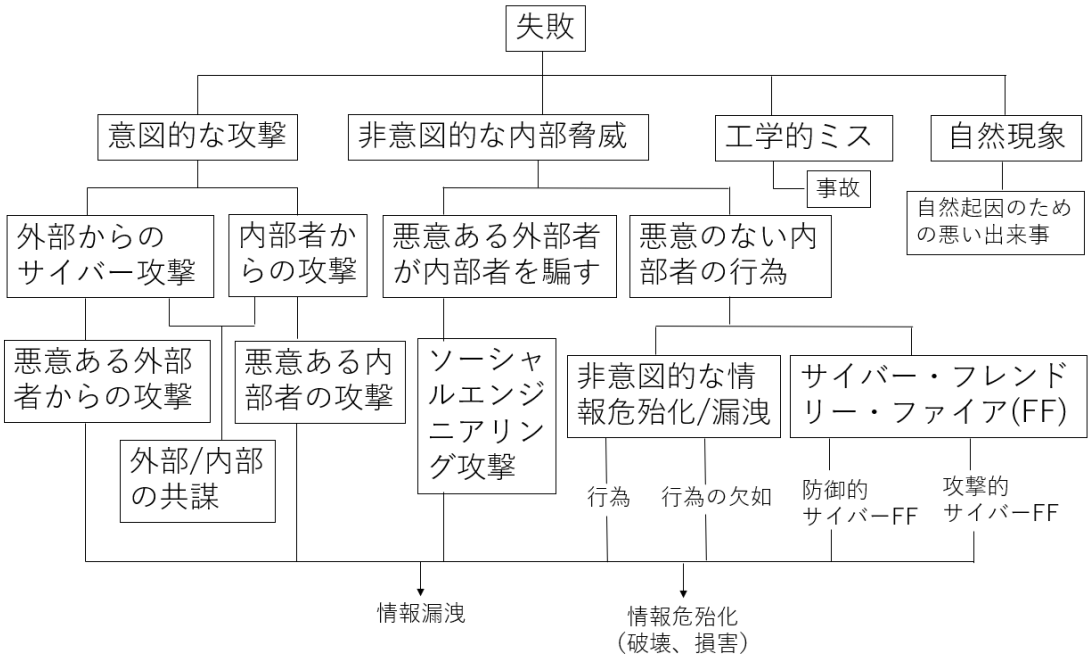

図 1　情報セキュリティの失敗の全体像（特に内部者の脅威に焦点を当てたもの）

●情報セキュリティの失敗の全体像については、Gretizer（2019）による図 1 の分類図が便利で

ある[5]。他の分野のリスクと同様、「工学的なミス」や「自然現象」といった意図しない原因によるものに加えて、「意図的な攻撃」があり、さらに「非意図的な内部者脅威」がある。

●「意図的な攻撃」は外部からのものと内部からのものに分かれる。また、外部者と内部者の共謀によるものもある。「非意図的な内部者脅威」は、悪意ある外部者が内部者を騙すものと悪意のない内部者の行為が結果として情報漏洩につながるものに分かれる。「悪意ある外部者が内部者を騙すもの」はソーシャルエンジニアリング攻撃と呼ばれ、人間の心理的な隙や弱点につけ込むもので、フィッシング・メールによる詐欺などはその典型である。「悪意のない内部者の行為」としては、非意図的な情報危殆化（compromise）や漏洩（leak）とサイバー・フレンドリー・ファイア（FF）がある。危殆化は必ずしも情報漏洩ではないセキュリティレベルの低下を指す概念である。サイバー・フレンドリー・ファイア（FF）とは、サイバー誤爆とも呼ばれ、防御、あるいは、攻撃のためのアクションが意図せずに、味方あるいは中立の第三者に害を与えることを指す。

●本 NOTE ではこれらのうちの「意図的な攻撃」に含まれる「悪意ある外部者からの攻撃」としてランサムウェア攻撃を、「悪意ある内部者からの攻撃」として内部者脅威を取り上げる。

3．ランサムウェアによるリスク

3.1　ランサムウェアによる被害の特徴

●毎年ランサムウェア攻撃の状況について調査している Sophos 社は 2023 年 1 月から 3 月にかけて、日本を含む 14 か国の組織（従業員数 100～5,000 人）に所属する 3,000 人の IT/サイバーセキュリティ部門のリーダーを対象とする調査を実施した[6]。過去 1 年間の経験に基づいて回答してもらった結果、ランサムウェア攻撃を受けたと回答した組織は 66％であり、業種別では教育機関が最も高かった。データが暗号化された割合は 76％であった。暗号化された比率は過去 4 年間で最高値だという。また暗号化された攻撃の 30％でデータも盗まれている。データが暗号化された組織の 97％がデータを取り戻すことに成功しており、方法としてはバックアップによ

[5] Frank L. Greitzer. 2019. Insider Threats: It's the HUMAN, Stupid! In Proceedings of the Northwest Cybersecurity Symposium (NCS '19). Association for Computing Machinery, New York, NY, USA, Article 4, 1–8. https://doi.org/10.1145/3332448.3332458

[6] Sophos，ランサムウェアの現状 2023 年版、ソフォスホワイトペーパー2023 年 5 月．https://www.sophos.com/ja-jp/content/state-of-ransomware

るものが70%を占めているが、身代金を払ってデータを取り戻した割合も46%に上ったという。

●サイバー保険に加入している組織では 97～98%が暗号化されたデータを取り戻しているが、サイバー保険に加入していない組織では 84%にとどまった。この差の要因の 1 つは保険加入時にバックアップとリカバリ計画を作成する必要があることであるが、保険金が得られるために身代金を払う確率が高くなっていることも課題として挙げられている。スタンドアロン型のサイバー保険に加入している組織では 58%が、サイバー攻撃への補償が含まれるパッケージ型の保険に加入している組織では 36%が身代金を払っているのに対して、サイバー保険に未加入の組織では 15%にとどまっている。売上高が多い組織ほど、身代金の支払い額も多くなっているという。例えば、売上高が 50 億ドル超の組織の平均値は約 250 万ドル、中央値は 300 万ドルであった。また復旧するためのコストは（身代金を除いて）平均 182 万ドルであった。復旧にかかる時間は「最大 1 週間」が最も多かったが、6%の組織は「3～6 カ月」と回答した。

●日本の組織では、過去 1 年間にランサムウェア攻撃を受けた割合は 58%（回答者数 300）であった。14 カ国の平均値 60%とほぼ同じである。また、データを取り戻すことができたかという質問（回答者数 125）に対しては、52%が身代金を支払って、60%がバックアップを利用して取り戻したと回答したとのことである。22%が複数の方法を利用したと回答した。結果として95%は何らかの方法でデータを取り戻したと回答している。

3.2　ランサムウェア攻撃によるリスク要因の探索

●ランサムウェア攻撃の増加に伴って、ランサムウェアに関する研究も増加しているが、多くは技術的解決策を探るものである。しかし、攻撃者はある種のビジネスモデルを確立しており、ソーシャルエンジニアリングのための心理的なトリック、技術的な欠点、セキュリティ領域の専門知識の欠如、リーダーシップの欠如、組織の資金不足といった弱点を組み合わせて悪用している。要求する身代金額も、対象企業の規模や売上高などをもとにある種のアルゴリズムに基づいて決定しているとも言われている。そのため、技術的手段だけでは防ぐことは困難であることから、非技術的側面に焦点を当て、関係者へのインタビューを含めた質的研究や、実際の被害ケースを集めて統計的に分析する量的研究が複数実施されている。ここではこれらの中からいくつかを紹介する。

●Connolly and Wall (2019)は、英国において 2014 年から 2018 年の間に行われた 26 件の暗号化ランサムウェア攻撃に関与した被害者と捜査官（警察官を含む）への半構造化インタビューを

実施した[7]。下記の囲みはインタビュー内容のサンプルである。対象は 22 人（フォーカス・グループに 5 人、個別インタビューに 17 人）であった。

ランサムウェア事件の経験について教えてください。
ランサムウェアが感染したことをどのようにして知りましたか？
ランサムウェアの配送方法はどのようなものでしたか？
ランサムウェアがネットワークに感染するのに効果的だったのはなぜだと思いますか？
あなたの組織には、ランサムウェアに関する具体的なポリシーやトレーニングがありますか？
組織にはバックアップがありますか？
攻撃前にすべてのアプリケーションは最新のものでしたか？
あなたの組織はアンチウイルスソフトウェアを使用していますか？
この経験から何を学びましたか？
攻撃後、組織内でどのような変更が行われましたか？

得られたテキストデータは、5 つの段階で詳細に分析・分類された。第 4 段階では、「回復を支援する要因」「暗号化ランサムウェア攻撃に続く変化」「感染とさらなる拡散を可能にする要因」「回復を妨げる要因」の 4 つに集約され、最終の第 5 段階では対応ツール（ユーザのセキュリティ教育、セキュリティ・ポリシーとセキュアな実践、技術的対策、インシデント対応戦略、ネットワークセキュリティ）と変革の実現者（フロントライン管理、上級職によるマネジメント）からなる分類法が形作られた。このように、ランサムウェアへの対応は、攻撃の技術的側面と人的側面、組織的側面の間の関係によって複雑化することが明らかになった。成功する攻撃には、心理的な策略、技術的な欠点の悪用、上級管理職による怠慢、熟練した献身的で適応力のあるフロントラインの管理者の不足などといった要因が挙げられた。逆に言うと、対策のためにはこれらを包括する多層的なアプローチが必要であることを意味する。

●Connolly et al. (2020)は、ランサムウェア攻撃の被害にあった英国と北米の 50 の組織から抽出した 55 のランサムウェア攻撃事例について、定量的・定性的データに基づいて、暗号化ランサムウェア攻撃の深刻度を評価し、様々な要因が深刻度に影響を与えるかどうかを 2 つのフェーズ（質的データを集める探索的なフェーズと量的データを集めるフェーズ）に分けて調査した[8]。研究にあたり、下記のような仮説が立てられ統計的に検証された。またこの研究では、攻撃による損害の大きさを定量的に表現するための「影響評価尺度（Impact Assessment Instrument）」も開発された。事業継続中断期間、回復時間、影響を受けたデバイス、暗号化された重要情報、

[7] Connolly, L. and Wall, D., 2019. The rise of crypto-Ransomware in a changing cybercrime landscape: taxonomising Countermeasures. Comput. Secur. (87) 1–18. https://doi.org/10.1016/j.cose.2019.101568

[8] Connolly, A. Y., Wall, D. S., lang, M. and Oddson, B., 2020. An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability. Journal of Cybersecurity 6.1.: tyaa023.

情報喪失、総体としての影響の大きさという 6 種類の影響項目に対して、55 の事例が低（1）、中（2）、高（3）に分類された。各仮説には右側の矢印横に結果も追記した。

仮説 1a：組織の規模は、ランサムウェア攻撃の影響の大きさに影響する。⇒NO

仮説 1b：組織の種類は、ランサムウェアの攻撃に耐えられるかどうかに影響する。⇒YES

仮説 1c：組織のセキュリティ態勢は、ランサムウェア攻撃の影響の大きさに影響する。⇒YES

仮説 2a：暗号ランサムウェアの世代は、ランサムウェア攻撃の影響の大きさに影響する。⇒NO

仮説 2b：攻撃タイプが日和見的か標的型かは、ランサムウェア攻撃の影響の大きさに影響する。⇒YES

仮説 2c：攻撃対象が人間か機械かは、ランサムウェア攻撃の影響の大きさに影響する。⇒NO

●Hack et al. (2021)は、2019 年から 2020 年にかけて発生した 700 件以上のランサムウェアの攻撃者と被害者の交渉内容を収集し、データセットとして整理した[9]。交渉事例の分析から、攻撃者は被害者企業の財務情報などを調べ、年間収益に基づいて価格差別を行っていることが示唆され、（交渉の余地があるという意味でそのことを知っていれば）交渉で優位に立てる可能性がある一方で、被害者は不利な立場に置かれていることが明らかにされた。ただし、被害者側にも交渉を優位に進めるため、例えば、時間稼ぎをする、身代金を支払う能力がないと訴える、サイバー保険の存在を明かさないなどの戦略もありうるのではないかと指摘された。

●Connolly et al. (2022)は、標的となった個人や組織が身代金の支払いに応じているという事実がランサムウェア攻撃を魅力的なビジネスにしてしまっているという悪循環ともいえる状況を打破するためには、身代金の支払いに影響を与える要因を探るべく、被害者は身代金を支払うかどうかを決める前に状況を慎重に分析しているという仮説を検証した[10]。調査対象は、2014～2018 年に発生したランサムウェア攻撃から、多様な組織を含むように選んだ、36 の組織に対する 41

[9] P. Hack, Cybersecurity Analyst, Fox-IT, part of NCC Group, “We wait,because we know you.” Inside the ransomware negotiation economics.Research Blog, 12 Nov. 2021. NCC group

[10] Connolly, L. Y., and Borrion, H., 2022. Reducing ransomware crime: analysis of victims’ payment decisions. *Computers & Security* 119: 102760.

件とした。11 人のランサムウェア被害者との半構造化インタビューを実施したが、それ以上、対象者を見つけるのが困難であったため、英国サイバー犯罪対策課の警察官英国の組織やサイバー犯罪課の警察官 8 人から半構造化インタビューとフォーカルグループインタビューを実施した。その結果、被害者は最終的な決断を下す前に、介入のコストとベネフィットを比較検討することが多く、その決断はさまざまな理由に基づいていることが確認された。また、一般データ保護規則（GDPR）のような法律による、情報漏洩に対する罰金が、犯罪者が求める身代金よりもはるかに大きい場合、被害者は当局に報告せずに身代金を払ってなかったことにすることを選ぶかもしれないという問題提起も行っている。

●Lang et al. (2022)は、COVID-19 パンデミックの発生がランサムウェア攻撃の戦術をどのように変化させたかを理解するために、直接インタビューと二次資料をもとに、COVID-19 パンデミックの発生直前に発生した 26 件とパンデミック中に発生した 13 件のランサムウェア攻撃、合計 39 件の定性的比較分析を行った[11]。方法は次の通り 4 段階で実施された。

①複数のランサムウェア被害者と、英国のサイバー犯罪ユニットの専門警察官へのインタビュー

②2 人のサイバーセキュリティ専門家から、COVID-19 の流行時に発生した 7 件のランサムウェア攻撃に関するデータを提供してもらい、3 回の半構造化インタビューを実施

③攻撃被害者へのインタビューがこれ以上できなかったために、公開文書（二次資料）により補完（6 件分）

④比較対象のパンデミック前の 26 件は Connolly and Wall (2019)を利用

これらからいくつかの重要なテーマが見えてきたことが報告された。

(1)ランサムウェアの攻撃者は、より邪悪な戦術を採用し、リターンを最大化するために複数の犯罪を行うようになった。

(2)従業員の在宅勤務による攻撃機会の拡大が、悪意のある侵入のリスクを大幅に悪化させた。

(3)優先する攻撃ベクトルが変化し、フィッシングや VPN 悪用が前面に出てきた、

[11] Lang, M., Connolly, A. Y., Taylor, P. and Corner, P. J., 2022. The Evolving Menace of Ransomware: A Comparative Analysis of Pre-pandemic and Mid-pandemic Attacks. Digital Threats Just Accepted (August 2022). https://doi.org/10.1145/3558006

(4)オフラインからオンラインへの一般的なビジネスプロセスの適応に失敗し、脆弱性が生じた。

(5)サイバーセキュリティに対する放任主義の継続と準備不足が見られた。

●Meurs et al. (2023)は、2019 年から 2022 年の間にオランダ警察に報告されたオランダにおける 453 件のランサムウェア攻撃調査報告に基づくデータセットを構築し、3 つの仮説を回帰分析によって検証した[12]。

1．要求される身代金額は、データ流出、RaaS[13]の利用、被害者の年間収益・業種、保険の有無と相関がある→支持（サイバー保険に加入している企業はより高額の身代金を要求される傾向があった）

2．身代金の支払い確率は、要求された身代金額、データ流出、個別化ターゲット、追加の脅迫、バックアップ状態、交渉日数と相関がある→部分的に支持

3．被害者の経済的損失額は、支払われた身代金、データ流出、RaaS の利用、被害者の年間収益、バックアップ状態、季節と相関がある。→支持

4．内部者からの攻撃リスク

4.1　内部者脅威の分類

●proofpoint 社（本社：米国カリフォルニア州）は 2022 年 1 月、「2022 年内部者（インサイダー）脅威のコスト：グローバルレポート」を発表し、内部者脅威の件数が 2 年間で 44%増加し、影響を受けた組織は、全体的な修復に年間平均 1,540 万ドルを費やし、各インシデントの封じ込めに 85 日を要したことを明らかにした[14]。また、報告された内部者脅威事案の 56%は、不注意な従業員や請負業者によるもので、26%は「悪意のある内部者」であり、1 件あたりの平均コストは 648,062 ドルであったという。「悪意のある内部者」とは、データアクセスを有害、非倫理

[12] T. Meurs, M. Junger, E. Tews and A. Abhishta, "Ransomware: How attacker's effort, victim characteristics and context influence ransom requested, payment and financial loss," 2022 APWG Symposium on Electronic Crime Research (eCrime), Boston, MA, USA, 2022, pp. 1-13, doi: 10.1109/eCrime57793.2022.10142138.

[13] RaaS とは、Ransomware as a Service の略称であり、ランサムウェア攻撃に必要な一式を「サービス」として提供するものを指す。

[14] 2022 Ponemon Cost of Insider Threats Global Report. https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats https://www.globenewswire.com/news-release/2022/01/25/2372208/35374/en/Global-Cybersecurity-Study-Insider-Threats-Cost-Organizations-15-4-Million-Annually-up-34-Percent-from-2020.html

的、または違法な活動に使用する従業員または権限を与えられた個人を指している。

●内部者脅威は、組織の資産へ簡単にアクセスでき、それゆえ一定の信頼を受けた内部者によって実行されることが多いことから事前に検知することが難しい。また、検知されるとしても、組織のセキュリティ部門ではなく、同僚などによって検知される可能性が高い。そういった場合には組織外部からの攻撃を防御するために設計された、侵入検知システムなどの技術的な対策は役に立たないことになる。こうした背景から、これまで内部者脅威についての研究は十分に進展してこなかった。しかし、内部者脅威の検知も、技術的アプローチと非技術的アプローチに分けることができる。前者は直接的に不正な活動を検知することと内部者脅威につながりそうな（間接的な）行動の変化を特定することに分かれる。後者は関連しそうな心理的・社会的なリスク因子（変数）を特定する必要があるが、検証することはなかなか難しい。

●米国 CISA（Cybersecurity and Infrastructure Security Agency）は内部者脅威（insider threat）を、「内部者が意図的または非意図的に、許可されたアクセス権を使用して、部門のミッション、リソース、人員、施設、情報、機器、ネットワーク、またはシステムに危害を加える脅威」と定義している[15]。行動としては、スパイ活動、テロ行為、情報の不正開示、国際的な組織犯罪への参加を含む汚職、妨害行為、職場での暴力、部門リソースまたは能力の意図的または非意図的な損失または低下が挙げられている。内部脅威のリスクを軽減するためには、検知・特定、評価（アセスメント）、管理（マネジメント）というアプローチが必要となる。2020 年に公表された「内部者脅威緩和ガイド（Insider Threat Mitigation Guide）」は効果的な内部者脅威緩和プログラムのための実行可能なフレームワークを詳述したものである[16]。

4.2　内部者脅威リスク要因の探索

●上記ガイドでは、組織内で何らかの不満を持った個人が敵対的な行為に至るまでには一定の経緯と時間がかかることが強調されている（図２）。この図から分かるように、個人的な観察可能な行動に着目することで内部者脅威を早期に検出・特定することができる可能性がある。本NOTEでは触れないが、管理（マネジメント）の局面では、「何もしない」から法的措置まで様々な戦略がある。また、リスクレベルをあらかじめ定めておくことで、管理（マネジメント）につなげやすくなる。CISA（2020）では、9 段階に分けて、軽度のリスク（1 と 2）、中程度のリスク（3

[15] Cybersecurity and Infrastructure Security Agency (CISA) (2020). Insider Threat Mitigation Guide. https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

[16] https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide

と４）、高められたリスク（5 と 6）、深刻なリスク（7 と 8）、極度のリスク（9）の 5 種類が示されている。

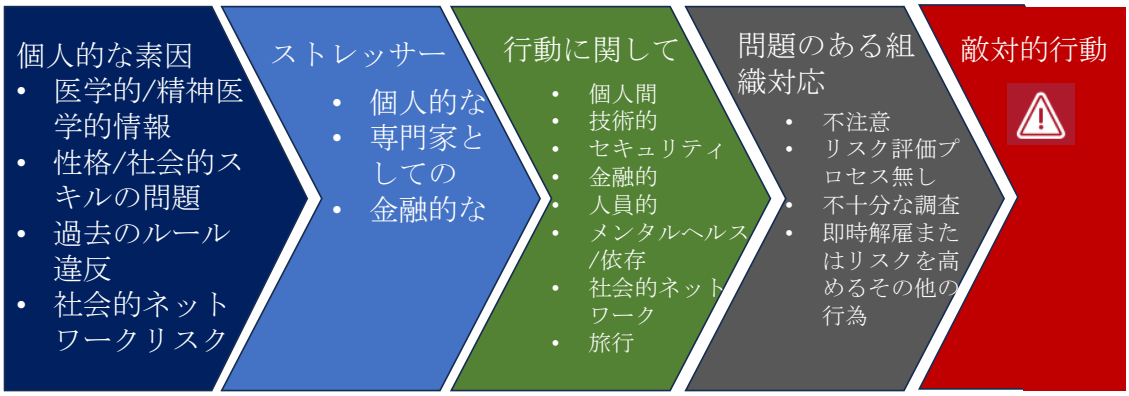

図２　内部者リスクに至るまでで重要な経路に沿ったファクター

出典）Cybersecurity and Infrastructure Security Agency（CISA）(2020). Insider Threat Mitigation Guide. Figure 10.を引用

●Greitzer et al. (2019)は内部者脅威を対象とした SOFIT（内部者脅威のための社会技術的及び組織的要因）と名付けられたオントロジー（概念）を開発した[17]。内部者からの脅威は、アクター（行為者）、ファクター（要因）、インテンション（意図）からなるとされる。アクターは個人と組織、インテンションは悪意と非悪意からなる。

ファクターは図３のように、個人的要因と組織的要因に分けられ、さらに個人的要因には境界違反（個人的なことと職業上のこととの境目があやふやになることに起因する様々な問題）、心理的ファクター、仕事のパフォーマンス、サイバーセキュリティ違反、人生における様々な出来事という 5 つからなるものとされた。他方、組織的要因には、セキュリティ慣行、コミュニケーション問題、マネジメントシステム、作業計画とコントロールの 4 つが挙げられた。ここでは詳細には触れないがこれらはさらに細分化されている。

[17] Frank L. Greitzer, James D. Lee, Justin Purl, Abbas K. Zaidi, Design and Implementation of a Comprehensive Insider Threat Ontology, Procedia Computer Science, 153, pp. 361-369. 2019. https://doi.org/10.1016/j.procs.2019.05.090

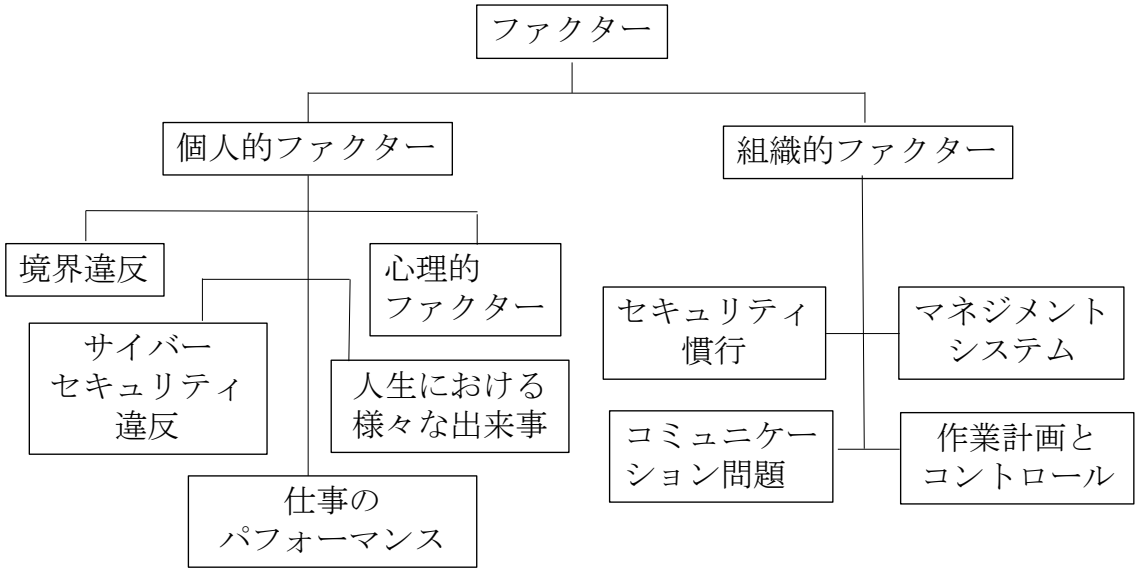

図３　SOFIT オントロジーによる「ファクター」の分類

5. おわりに

●本 NOTE ではサイバー攻撃、特にランサムウェア攻撃と内部者脅威について、非技術的な側面に関する研究をいくつかとりあげて紹介した。本稿で取り上げた非技術的要因以外に、サイバー保険とサイバーリスク・デュー・デリジェンス（DD）が重要である。

●サイバー保険を提供する保険会社は、組織が保険に加入する際に何らかの査定を行い、場合によってはデータのバックアップをとる等の条件を付けて加入させる場合もあるだろう。また、サイバー保険に加入することは、組織にとってのインセンティブ構造を変えることで組織の行動変容を引き起こすことになる。特に、日本のサイバー保険は、欧米のものと違って、最初から身代金は支払いの対象外であったという。欧米ではサイバー保険に入っている組織が安易に身代金を支払ってしまうこと、そしてそれを攻撃者が見込んで攻撃対象にすることが問題視されていた。その点、日本のサイバー保険に入っていること、すなわち身代金が支払われる可能性が低いことが知られることで、悪の主体による主観的な資産（A*）を減らし、脅威（T）を減らす可能性が示唆される。

●サイバーリスク DD は、財務 DD などの他の種類の DD と同様、M＆A（企業の合併・買収）や出資といったタイミングで行われる査定のことである。サイバーリスク DD の場合の査定ポイントがまさに本 NOTE で議論した、非技術的な側面とおおよそ重なると考えられる。そうした実務情報を収集する必要もあるだろう。

●脆弱性（V）が高い対象として、近年攻撃が増している病院に加えて、教育機関も目を付けられている可能性がある。米国では学校を標的としたサイバー攻撃が増えていることを受けて、2023年8月7日にはホワイトハウスで、教育省長官、国土安全保障省長官、ジル・バイデン大統領夫人とともに、学校管理者、教育関係者、民間企業が招集され、学校のサイバーセキュリティを強化するための会合が開催された[18]。2022年12月に公表された米国GAO（政府アカウンタビリティ局）の報告書によると、学校へのサイバー攻撃によって学習ができなくなる期間は3日から3週間で、復旧には2カ月から9カ月かかるという[19]。さらに、サイバー攻撃後の学区の金銭的損失は5万ドルから100万ドルに及ぶ。代表的な攻撃には、フィッシング、ランサムウェア、分散型DoS攻撃、ビデオ会議の妨害が挙げられた。ミネアポリスの公立学校がランサムウェア攻撃にあった際には、身代金の支払いを拒否した後にオンライン上に30万以上のファイルが流出し、生徒に関するプライバシー情報が多数含まれていたことがあったという[20]。しかし被害者に対して行政当局からの説明はないようで、理由は病院と違って、米国では学校に対してそういった通知を義務付ける連邦法が存在しないことが指摘されている。

●本NOTEでは体系的なレビューを実施したわけでなく、あくまでも予備的な調査を行い、いくつかの仮説検証の取り組みを紹介したに過ぎない。今後はサイバー保険やデューデリジェンス（DD）の調査も行い、現実と理論のギャップを埋めていく予定である。

[18] https://www.whitehouse.gov/briefing-room/statements-releases/2023/08/07/biden-harris-administration-launches-new-efforts-to-strengthen-americas-k-12-schools-cybersecurity/

[19] https://www.gao.gov/blog/cyberattacks-increase-k-12-schools-here-whats-being-done

[20] https://apnews.com/article/schools-ransomware-data-breach-40ebeda010158f04a1ef14607bfed9b0

令和 7 年 1 月 6 日

ELSI NOTE No. 51

サイバーセキュリティリスクの定式化と非技術的要因に関する文献調査

岸本 充生　　大阪大学 社会技術共創研究センター　センター長（2024 年 12 月現在）
D3 センター　教授

Formulation of cybersecurity risk and literature review on non-technical factors

Atsuo KISHIMOTO　　Osaka University

大阪大学 社会技術共創研究センター
Research Center on Ethical, Legal and Social Issues

〒565-0871 大阪府吹田市山田丘 2-8
大阪大学吹田キャンパステクノアライアンス C 棟 6 階
TEL 06-6105-6084
https://elsi.osaka-u.ac.jp

大阪大学

Osaka University
Research Center on
Ethical, Legal and
Social Issues