１Ｃ１８

e-CSTI による研究分野分析：情報セキュリティ分野

○面和成（内閣府）※，井上瑶子（内閣府），寺田好秀（政策研究大学院大学），
七丈直弘（政策研究大学院大学），白井俊行（内閣府）
※kazumasa.omote.f6j@cao.go.jp

1. はじめに

政策において重要科学技術領域を説明する手段として，その領域の少数の専門家の個人的な見解を集めることを前提とする方法は偏った見解を示す恐れがある．また，このような方法では，大規模で多様な研究者のデータを収集･分析することは困難である.そこで重要なのが EBPM（Evidence Based Policy Making）という考え方である．EBPM とは，エビデンスに基づく政策立案を指し，政策の企画をその場限りのエピソードに頼るのではなく，政策目的を明確化したうえでエビデンスに基づくものである [9]．政策効果の測定に重要な関連を持つ情報や統計等のデータを活用した EBPM の推進は，政策の有効性を高め，国民の行政への信頼確保に資するものである．内閣府では，EBPM を推進するべく，様々な取組を進めており，科学技術イノベーション関連データを分析するプラットフォームである e-CSTI [8] を構築している．e-CSTI は科学計量学（サイエントメトリクス）の具体的な手段の一つである．

科学計量学とは，学術文献の測定と分析に関わる学問分野である [6]．特定のテーマや領域の成長について様々な側面を理解するのに役立ち，研究動向だけでなく，研究機関・研究者の定量的評価も行える．科学計量学の研究は，E. Garfield の研究 [1] が主な基盤となっており，様々な科学的領域を効果的に研究するための書誌学的手法である．研究者や政策立案者に対し，最新の研究動向や科学技術文献の様相を測る指標や可視化手法を提供することを目的としている．科学技術や学術に関する定量的データやその分析は，科学技術政策の立案のための欠かすことのできない基盤であるとともに，多岐に渡る科学技術･学術活動の状況を把握，また，政策の効果や影響を分析する上でも重要な役割を担っている．

情報セキュリティは，システムやサービスに安全・安心を与える科学技術の根幹をなす研究分野である．情報セキュリティ分野に関する分析結果は様々なところで公開されており，例えば，IPA は情報セキュリティ 10 大脅威を毎年公開している [7]．これは，前年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から，IPA が脅威候補を選出し，情報セキュリティ分野の研究者，企業の実務担当者など約 150 名のメンバーからなる「10 大脅威選考会」が脅威候補に対して審議・投票を行い，決定したものである．この結果により，インパクトある情報セキュリティの脅威を把握でき，その分析や対策に関する重要な研究テーマの選定にも役立つ．しかし，これは専門家の肌感覚により決定されていることから主観的な分析となっており，EBPM とは異なる性質のものである．

本稿では，科学計量学分析が扱う研究分野として情報セキュリティ分野を取り上げ，内閣府で構築している研究分野分析ツール e-CSTI，及び 2010 年から 2019 年までの 10 年間の書誌情報を用いて，情報セキュリティ分野の研究動向等の詳細な分析を行う．本分析は共引用情報 [1]のみに基づいて自動的に書誌情報を複数の論文クラスターに分類しており，時代に応じた動的なクラスター生成を実現できる特徴を持つ．情報セキュリティ分野は，本分析によって 4 つの分野（暗号系，サイバー攻撃系，認証系，ブロックチェーン関連）が抽出され，それぞれの研究分野について，世界各国の研究動向，注目テーマの動向について明らかにする．

2. e-CSTI

内閣府では，大学等の研究機関における「研究」,「教育」,「資金獲得」に関するエビデンスを収集し，インプットとアウトプットの関係性を「見える化」するための各種分析機能を開発し，関係省庁や国立大学・研究開発法人等の関係機関に対して分析機能・データを共有するプラットフォーム e-CSTI（Evidence data platform constructed by Council for Science, Technology and Innovation）を構築し

[1] 1 つの論文の参考文献に論文 A と論文 B が含まれているとき，A と B は共引用の関係にある．

ている [8]．また，e-CSTI の機能の一部として，重要科学技術領域の特定に向けたツールが試作されている．本ツールは，全研究分野の書誌情報を，共引用関係をもとにお互いに関連性の高い論文集合（論文クラスター）に分解して可視化できるものであり，政策立案者を含むユーザは SQL や Python などの知識がなくとも使うことできる．さらに，注目する論文や技術を含む論文クラスターを分析することにより，当該技術に関連する論文等の数，日本の論文シェアの推移，分野融合度，特許への引用度合い，国際研究ネットワーク，注目される研究者とその予算執行データを把握できる．その結果，e-CSTI は世界各国の動向や注目テーマの動向を把握できるだけでなく，日本の勝ち筋把握にも貢献することが期待できる．なお，本分析の結果はその一部である．

3. 先行研究

科学計量学の研究は数多く存在する．その中で情報セキュリティ分野に関する科学計量学の研究は，Lee [2] によって 2008 年に初めて行われた．Lee は，SCI (Science Citation Index)のデータベースを用いて重要キーワードを抽出し，Co-Word 分析を用いて情報セキュリティ分野の傾向やパターンを明らかにした．例えば，その中で情報セキュリティのテーマが急速に変容していることについて言及している．Olijnyk [3] は，Scopus 書誌情報を用いて，情報セキュリティ分野のプロファイル，ダイナミクス，構造の解析を行い，情報セキュリティ分野の知的構造を明らかにした．例えば，その中で情報セキュリティに高い影響を与えた研究機関や著者を明らかにしている．Rai ら [4] は，Scopus 書誌情報を用いてサイバーセキュリティを対象とした 2,720 件の論文のトレンド分析を行った．この研究では，国や機関，共同研究，研究資金に関する分析を実施している．しかし，これらの研究は，(1) 対象としている情報セキュリティ分野に偏りがある，(2) 研究テーマに関する詳細な分析がない，といった課題がある．

4. e-CSTI を活用した情報セキュリティ分野の分析

4.1 データ

Digital Science 社が提供する Dimensions の書誌情報 10 年分（2010～2019 年）のうち，Top10%論文 [2]を対象として論文情報を収集した．対象となる論文数は 2,224,645 本（著者数が 3,201,598 名）であった．専門分野の論文クラスターは論文同士の共引用関係をもとに 1,076 のクラスターに分類され，さらに論文クラスターは 12,445 のサブクラスターに分類された．

情報セキュリティ分野を代表する論文クラスターを特定するために，論文タイトルとアブストラクトを対象に「security」というキーワードを用いて，情報セキュリティに関連が深い上位 4 つの論文クラスター（サイバー攻撃系，暗号系，認証系，ブロックチェーン関連）を特定した．サイバー攻撃系を表すクラスターには 4,252 本，暗号系を表すクラスターには 2,908 本，認証系を表すクラスターには 1,412 本，ブロックチェーン関連を表すクラスターには 2,449 本の合計 11,021 本の本論文を分析の対象とする．なお，情報セキュリティ分野に属する共通鍵暗号，PUF（Physical Unclonable Function），生体認証は，これら 4 つの論文クラスターとは別のクラスターに分類されていることに注意されたい．また，書誌情報を視覚的に表示するためにソフトウェア Tableau を用いた．

4.2 分析方法

本研究では，情報セキュリティ分野に対して e-CSTI を用いた 3 種類の分析を行った．分析手法については，Small らの新興分野を分析する方式 [5] をベースとする．具体的には，共引用関係による論文ネットワークを作成した後，Node2Vec アルゴリズムによってネットワークをベクトル化し，t-SNE アルゴリズムによって二次元化し，論文を単位とするマップを作成する．さらに，Leiden アルゴリズムを用いて書誌情報をクラスタリングすることによって論文クラスターを生成する．論文数，国際共著数 [3] の推移の分析では，情報セキュリティに関係する 4 つの論文クラスターにおいて，論文数及び国際共著数の年別の論文件数を算出した．サブクラスター別の論文マップによる分析では，4 つのクラスターの論文をそれぞれ二次元でマッピングを行い，サブクラスター毎に色分けを行った．なお，各サブクラスターのキーワードラベルはワードクラウドを使った分析や個別論文の内容確認により著者が付与したものである．また，共引用情報でグルーピングしているため，サブクラスターはラベリングされたキーワードの研究だけでなく，その関連研究や関連技術も含まれることに注意されたい．最後に国別の論文

[2] 研究分野（FOR）ごと，年ごとに被引用数が上位 10%に含まれる論文
[3] 所在地が日本以外の研究機関に所属する著者が 1 人以上いる論文件数

マップによる分析では，4 つのクラスターの論文を二次元でマッピングを行い，国毎に色分けを行った．

4.3 分析結果と考察

4.3.1　論文数，国際共著数の推移

図 1 は，情報セキュリティに関係する 4 つの論文クラスターにおける論文数と国際共著数の 10 年間（2010 年～2019 年）の推移を示している．4 つのクラスター全てにおいて，論文数，国際共著数が共に増加傾向にあることがわかる．特に，ブロックチェーンは新しい技術であり，様々な分野への適用の可能性・将来性が示されており，論文数，国際共著数が急増している．

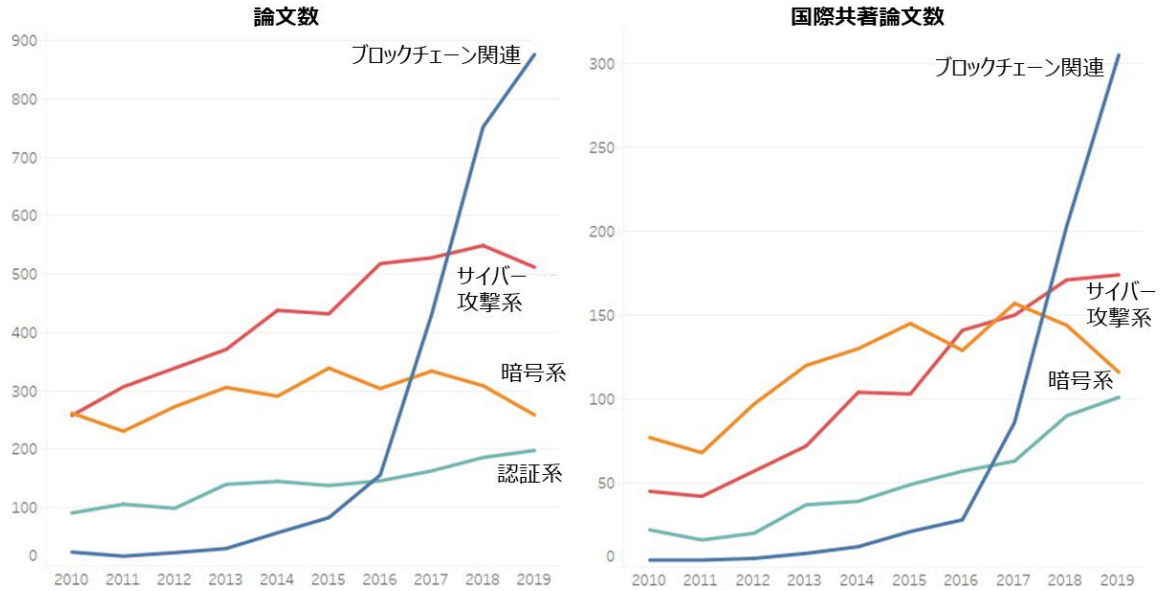

図 1 情報セキュリティに関係する 4 つの論文クラスターにおける論文数・国際共著論文数の推移

4.3.2　サブクラスター別の論文マップ

図 2 は，情報セキュリティに関係する 4 つのクラスターの論文マップを示しており，サブクラスターで色分けされている．サイバー攻撃系，暗号系，認証系の 3 つは各サブクラスターがより明確に区別されているのに対し，ブロックチェーン関連は新しい分野であることもあり，境界がぼやけていることが見て取れる．

サイバー攻撃系は 16 のサブクラスターから構成されており，具体的には，(0) 制御フロー攻撃，CFI（Control Flow Integrity），(1) サイドチャネル（ソフト），(2) フォレンジック，(3) IoT，(4) コード分析，(5) Web 利用，(6) 産業監視制御システム，(7) DDoS，SDN（Software Defined Networking），(8) 侵入検知，(9) Android セキュリティ，マルウェア検知，(10) Web 攻撃，(11) サイドチャネル（ハード），(12) 自動車，(13) ランサムウェア，(14) Botnet，(15) 標的型攻撃となっており，攻撃対象や手法によって特徴づけられている．この中で特に論文数の増加が顕著だったのは「(8) 侵入検知」であった．

暗号系は 17 のサブクラスターから構成されており，具体的には，(0) サイバーフィジカル，(1) 暗号理論（ID ベース暗号など），(2) 秘密分散，(3) クラウド向けセキュリティ手法，(4) 楕円曲線暗号，(5) 超特異楕円曲線，(6) 秘密計算（準同型暗号），(7) 耐量子計算機暗号，(8) プロトコル（電子投票，TSL など），(9) 秘密計算（その他），(10) クラウドストレージ，(11) 属性ベース暗号，検索可能暗号，(12) アクセス制御（クラウド），(13) アクセス制御（IoT ほか），(14) 異種クラウド，(15) 暗号理論（関数型暗号など），(16) 物理的暗号となっており，主に手法によって特徴づけられている．論文マップにおいて，左側のクラウドに関連する研究と右側の理論中心の研究に関する研究が重なり合う形で存在しており，この重なりに位置しているのが，(11) 属性ベース暗号，検索可能暗号である．この中で特に論文数の増加が顕著だったのは，暗号技術の基盤となる暗号理論，セキュアなクラウドサービス展開に重要な秘密計算，クラウドのきめ細かいアクセス制御やサービスの多様化に重要な「(11) 属性ベース暗号，検索可能暗号」であった．

認証系は 11 のサブクラスターから構成されており，具体的には，(0) Bluetooth，(1) アドホックネッ

トワーク，集約署名，(2) スマートグリッド，(3) ユーザ認証，鍵共有，(4) LTE，(5) IoT，(6) センサネットワーク，(7) RFID 認証，(8) グループ通信，(9) RFID 距離境界プロトコル，(10) ヘルスモニタリングとなっており，手法や対象によって特徴づけられている．この中で特に論文数の増加が顕著だったのは，IoT ネットワークに関連する「(5) IoT」と「(6) センサネットワーク」であった．

ブロックチェーン関連は 15 のサブクラスターから構成されており，具体的には，(0) スマートコントラクト，(1) ビットコイン，(2) IoT，(3) ICO（Initial Coin Offering），(4) IoT，(5) ビットコインアドレス，(6) サプライチェーン，(7) 電子投票，(8) 教育，(9) ヘルスケア，(10) IoT，(11) フォグコンピューティング，(12) エネルギー，(13) ブロックチェーン，(14) マネーロンダリングとなっており，ブロックチェーンの適用分野や関連技術によって特徴づけられている．ブロックチェーン関連はどのサブクラスターも論文数が増加傾向にあるが，特に(1) ビットコイン，(6) サプライチェーン，(10) IoT が急増している．なお，論文クラスターに登場する 3 つのサブクラスター「IoT」の差異は不明であった．

情報セキュリティに関係する 4 つの論文クラスターを外観して，まず「IoT」のキーワードが 4 つのクラスター全てに含まれており，情報セキュリティ分野において IoT が非常に重要なキーワードであることが分かる．さらに，IoT に関連するキーワードとして，暗号系の「サイバーフィジカル」，認証系の「センサネットワーク」，ブロックチェーン関連の「フォグコンピューティング」が出現している．

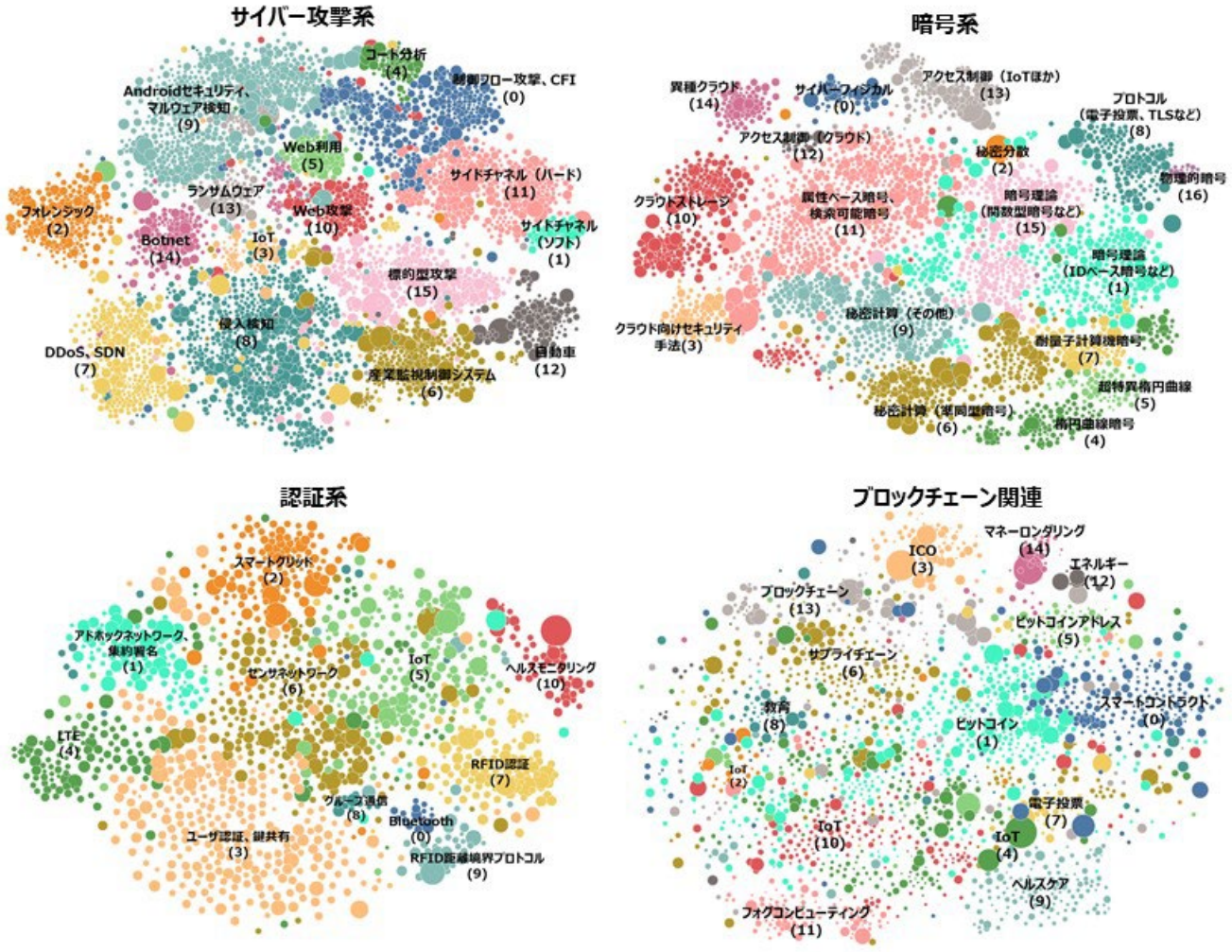

図 2 情報セキュリティに関係する 4 つの論文クラスターにおける論文マップ（サブクラスター別）

4.3.3 国別の論文マップ

図 3 は，情報セキュリティに関係する 4 つのクラスターの論文マップを示しており，国別で色分けされている．まず全体的な傾向としては，サイバー攻撃系と暗号系は米国が強く，認証系は中国が強く，ブロックチェーン関連は米中共に強いことが見て取れる．サイバー攻撃系では，右端のサイドチャネル（ハード）や中央のウェブ関連は米国が強く，左下のネットワーク関連は中国が強いことが読み取れる．

このことから，米国はハードウェア攻撃を脅威と捉える傾向にあり，中国はネットワーク攻撃を脅威ととらえる傾向にあることが読み取れる．暗号系では，米国は全体的に強いが，中国は左側のクラウド関連技術に力を入れていることが読み取れる．認証系では，中国がアドホックネットワーク，集約署名，IoT，センサネットワークなど IoT ネットワーク関連に力を入れていることが見て取れる．ブロックチェーン関連では，米国が中央のビットコイン，上部の ICO に力を入れているのに対し，中国が左下の IoT，フォグコンピューティングに力を入れていることが読み取れる．

全体的な傾向としては，米国は 4 つの分野全てにおいて強く，特に CPU のセキュリティや理論研究に力を入れていることが分かった．一方，中国は IoT やクラウドを含む応用技術に力を入れていることが分かった. なお, これらの分野における日本の論文数については, 暗号系の研究で強みはあるものの, 論文でみる限り全体的に世界の中でのプレゼンスは低い.

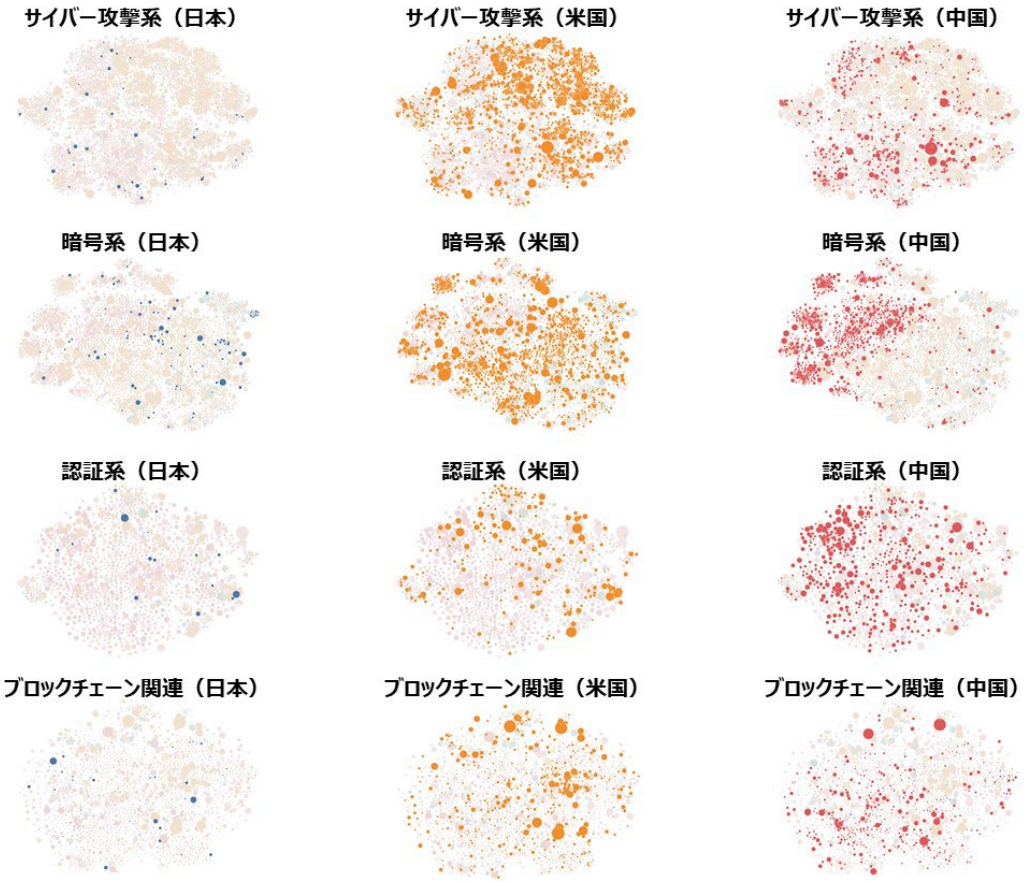

図 3 情報セキュリティに関係する 4 つの論文クラスターにおける論文マップ（国別）

5. 結論

本稿では，科学計量学分析が扱う研究分野として情報セキュリティ分野を取り上げ，内閣府で試作している研究分野分析ツール e-CSTI を用いて，情報セキュリティ分野の 4 つの分野（サイバー攻撃系，暗号系，認証系，ブロックチェーン関連）について研究動向等の詳細な分析を行った．特に，情報セキュリティ分野における世界各国の研究動向，注目テーマの動向について明らかにした．

謝辞

データの前処理や分析補助を行った加瀬豊氏（政策研究大学院大学）に感謝する．

参考文献

[1] E. Garfield, “Citation indexes for science: A New dimension in documentation through association of ideas. Science”, 122(3159), pp.108-111, 1955.
[2] W. Lee, “How to Identify Emerging Research Fields Using Scientometrics: An Example in the Field of Information Security”, Scientometrics, 76(3), pp.503–525, 2008.

[3] N.V. Olijnyk, “A Quantitative Examination of the Intellectual Profile and Evolution of Information Security from 1965 to 2015”, Scientometrics, 105(2), pp.883–904, 2015.
[4] S. Rai, K. Singh, and A.K. Vama, “Global Research Trend on Cyber Security: A Scientometric Analysis”, Library Philosophy and Practice (e-journal), 3769, 2019.
[5] H. Small, K.W. Boyack, and R. Klavans, “Identifying emerging topics in science and technology”, Research Policy, 43(8), pp.1450-1467, 2014.
[6] Wikipedia, “Scientometrics”, https://en.wikipedia.org/wiki/Scientometrics.
[7] IPA, 「情報セキュリティ 10 大脅威 2022」, https://www.ipa.go.jp/security/vuln/10threats2022.html, 2022 年 8 月.
[8] 内閣府, 「e-CSTI とは」, https://e-csti.go.jp/about.
[9] 内閣府, 「内閣府における EBPM への取組」, https://www.cao.go.jp/others/kichou/ebpm/ebpm.html, 2022 年 6 月.