

サイバー攻撃による産業毎の直接被害 及び波及被害の分析と考察

小梶 顯義*

概 要

一般に、国の施策立案にはマクロ経済的視野に立った定量的推計が必要である。しかし、現在、サイバー攻撃による一国における産業毎の経済的被害を分析する手法は確立されていない。そこで、筆者らは、マクロ経済分析モデルを用いて、サイバー攻撃による日本の産業毎の直接被害、攻撃を受けた産業から川上産業並びに川下産業に波及する被害額を定量的に推計するモデルを開発した。本稿では、総務省、経済産業省等が公表しているマクロ統計データ及び実際のサイバー被害データを用いて、被害額を定量的に推計した。本稿の貢献は、極めて限定的であっても、実際のサイバー攻撃による実被害データが得られれば、マクロ経済学モデル並びに総務省、経済産業省等が公表しているマクロ統計データを用いて、産業毎のサイバー攻撃による直接被害額及び波及被害額の推計が可能であることを示したことである。

1 まえがき

現在、サイバー攻撃による経済的被害の分析は、企業や組織が受けた被害を主な対象として行われている。一方で、サイバーセキュリティ戦略本部による「サイバーセキュリティ2024」[1]では、サプライチェーンでセキュリティが脆弱な部分が狙われ、サプライチェーン全体が影響を受ける事例が新たな脅威として顕在化しているとされる。このような状況を踏まえると、サイバー攻撃に対する国によるレジリエンス強化施策の立案の必要性が高まっていると考えられる。

一般に、国の施策立案のためには、国全体や産業毎等のマクロ経済的視野にたった定量的被害推計が必要である。しかし、現在、サイバー攻撃による国全体や産業毎の直接被害及び波及被害を分析する手法は確立されていない。この波及被害には、後方連関効果による被害と前方連関効果による被害がある。後方連関効果は、川下産業から川上産業への影響であり、ある産業の活動に必要な投入物を他産業が供給しようとするを誘発することである。前方連関効果は、川上産業から川下産業への影響であり、ある産業がその産出物を他産業の投入物として利用させようとするを誘発することである。この関係を図式化したのが、図1である。

* 博士(情報学)、情報セキュリティ大学院大学情報セキュリティ研究科 客員研究員

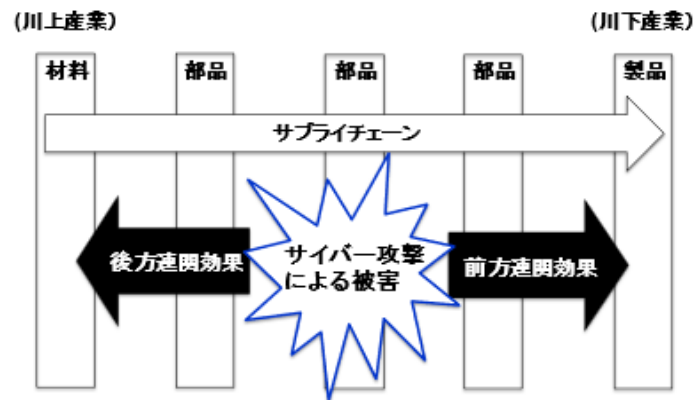


図 1：後方連関効果と前方連関効果（筆者作成）

Fig.1: Backward Linkage and Forward Linkage

筆者らは、マクロ経済分析モデルを用いて、サイバー攻撃による日本における産業毎の直接被害と攻撃を受けた産業から川上産業に波及する被害額を定量的に推計するモデルを開発した[2]。

更に、[2]で開発したモデルについて、攻撃を受けた産業から川下産業に波及する被害額についても定量的に推計するモデルに拡張した。具体的には、実際のサイバー攻撃被害データやマクロ経済統計データを使用して、サイバー攻撃を受けた産業におけるサイバー攻撃に起因する直接被害、サイバー攻撃を受けた産業から川上産業及び川下産業への波及被害額について、定量的な推計と分析を行った。

今回拡張したモデルは、全ての産業において推計が可能なモデルである。当モデル活用により、政策立案者が、日本における産業毎のサイバー攻撃による直接被害及び波及被害について、定量的に推計された被害額を掌握することが可能となる。その結果、サイバー被害の国レベルの施策立案に向けた定量的情報に基づく検討が可能となると考える。

また、今回のモデルは、自然災害等の国レベルでの分析において実績のあるマクロ経済学モデルである生産関数及び産業連関分析モデルを使用している。具体的には、まず、国全体の直接被害の推計にあたり、サイバー攻撃により失われた労働時間に着目し、実績のある生産関数を使用して国全体にわたる直接被害を推計している。サイバー被害の個別事案から国全体の被害額を積み上げて推計する際、データが少ないことから主観的な推測を加えることが避けられない。その結果、推計結果の信頼性確保が困難となることから、自然災害等の被害分析で実績のある生産関数を使用した。また、産業間で波及する被害の経済的分析については、自然災害による被災地から被災地以外への被害の波及分析等でも活用されている産業連関分析モデルを使用した。

本稿の貢献は、極めて限定的であっても、実際のサイバー攻撃による実被害データが得られれば、マクロ経済学モデル及び総務省、経済産業省等が公表しているマクロ統計データを用いて、産業毎のサイバー攻撃による直接被害額や波及被害額の推計が可能であることを示したことである。

なお、海外企業がサイバー攻撃を受けて国内企業が影響を受けるケースが想定され

るが、本稿では、データ収集上の制約から、国内へのサイバー攻撃により国内の経済が受ける経済的被害を分析対象としている。

2 先行研究

先行研究として、サイバー攻撃による被害に関するマクロ経済学モデルを用いた分析及び産業連関分析モデルの活用に関する動向を分析した。

2.1 サイバー攻撃による経済的被害のマクロ経済学モデルによる分析

サイバー攻撃による経済的被害分析に関する[3]～[22]について先行研究を実施した。

2.1.1 サイバー攻撃による直接被害の分析

現在、サイバー攻撃による国全体にわたる直接被害の分析は確立されていない。実際に発生したサイバー攻撃事案のうち公表された事案の被害を個別事案ごとに見積り、その額から国全体にわたる直接被害額を独自モデル(モデルを公表している場合と公表していない場合の双方を含む)で推計している場合が多い([3]～[17])。

[18]は、サイバー攻撃による企業価値の毀損額を推計している。[19]は、サイバー攻撃による被害ではないが、情報セキュリティ事案による被害について、生産関数を用いて情報セキュリティ事案の国全体の損失額を推計している。国全体にわたる情報セキュリティ事案の直接被害についてマクロ経済学モデルである生産関数を使用して推計している点は、筆者らのモデル[2]でも活用している。[20]は特定企業における川上産業への波及被害額を当該企業の財務データや産業連関表等に基づき推計、[21]は独自モデルでサイバー攻撃に関するインシデント毎に被害額を推計しているが、国全体にわたるサイバー攻撃による直接被害額は推計していない。

2.1.2 サイバー攻撃による波及被害の分析

[4]は、産業連関分析モデルを用いた国全体にわたるサイバー攻撃による波及被害推計モデルを提案している。ただし、直接被害を独自モデルで推計しており(モデル詳細は非公表)、モデル全体としての再現性がない。

また、[22]は、代表的な6つのシナリオを基に米国における産業毎の被害額を推計している。

一方、本稿では、実際のサイバー攻撃による被害データに基づき、実績のあるマクロ経済学モデルを使用して被害額を推計している。[22]と本稿の狙いは同じであるが、推計するプロセスに関して、[22]はシナリオを基に推計しているのに対し、本稿ではサイバー攻撃による実被害データを基に推計している。加えて、波及被害について、[22]は川上産業への波及被害のみを対象としているが、本稿では、川上産業への波及被害だけでなく川下産業への波及被害も対象としている。

上述のとおり、サイバー攻撃による産業毎の直接被害および波及被害について、産業

連関分析モデルを用いた先行研究は限定的である。この理由としては、企業単位での被害データは存在するが限定的であること、産業毎のサイバー攻撃による被害データが限定的であることにより産業連関分析モデルの利用が容易でないことがあげられる。また、サイバー攻撃の攻撃対象は、従来、個の企業や組織が主な対象となっていたため、被害の分析も個別の組織単位であったことも理由である。一方、最近になりサプライチェーンのなかでセキュリティが脆弱な部分が狙われるようになってきていることから、産業間の経済的波及効果や連関性を分析することが可能である産業連関分析モデルを使用する必要性が高まっていると考えられる。

2.2 産業連関分析モデル

2.2.1 産業連関表の概要

産業連関表は、一定の地域(国全体、都道府県など)における、一定期間(通常は1年間)の財・サービスの生産状況、産業相互間の取引状況を行列形式でまとめた、マクロ経済学における代表的統計である。

産業連関表で分かることのひとつに、各産業間の経済波及効果がある。経済波及効果には、前方連関効果と後方連関効果があり、前者は川上産業の生産が増加(減少)することで川下産業の需要が増加(減少)する効果であり、後者は川下産業が生産を増加(減少)することで、川上産業の需要が増加(減少)する効果である。産業連関表は、自然災害やビックイベント等の経済波及効果の分析に用いられているが、本研究においては、産業連関表を用いてサイバー攻撃による被害を推計、考察する。

2.2.2 産業連関表の概要

産業連関表の概観は図2のとおりである。

産業連関表の概観は図2のとおりである。

	中間財需要(Z_i)			最終需要 (F_i)	生産額 (Y_i)
	産業 ₁	...	産業 _n		
産業 ₁	a_{11}	...	a_{1n}	F_1	Y_1
...	...	...	...	...	...
産業 _n	a_{n1}	...	a_{nn}	F_n	Y_n
付加価値額	V_1	...	V_n		
生産額	Y_1	...	Y_n		

図2：産業連関表(筆者作成)

Fig.2: Input Output Table

Y_i は、産業_iの生産額

F_i は、産業_iの生産に対する最終需要

Z_i は、産業_iの生産に対する中間財需要

a_{ij} は、財_jの生産に用いられる財_iの生産額

V_i は、産業_iの付加価値を表す。

ただし、は中間財の投入行列の大きさ(国・地域×産業・分類数)を表す。

産業連関表は、以下を前提とした産業間の連関性を定量的に表現したすものであり、今回拡張したモデルにも以下の産業連関表の前提があてはまる。

- 1) 企業の生産能力に限界がない
- 2) 財・サービスの生産に必要な原材料等の投入(費用)構成は一定
- 3) 各産業が使用する投入量はその部門の生産量に比例(収穫一定)
- 4) 生産波及は途中段階で中断しない
- 5) 各産業の生産活動の和は各部門の総効果に等しい(各産業間の干渉がない)

なお、産業連表を使用した経済波及効果の分析においても、上述前提を基に各種経済効果の分析が実施されている。

また、産業業連関モデルで捉えられない動きは、今回拡張モデルでも捉えきれない。例えば、ランサムウェア攻撃により企業等が支払わざるを得なくなった身代金は捉えられない。

2.2.3 産業連関表を用いた波及被害推計

産業連関表をとおして、各産業間の経済波及効果、具体的には、前述の後方連関効果と前方連関効果を把握することができるが、ここでは、産業連関表を用いて後方連関効果と前方連関効果を推計する手法概要を説明する。

1) 後方連関被害の推計

産業連関表から得られる係数のひとつに投入係数がある。この投入係数とは、ある産業において1単位の生産を行う際に必要とされる原材料等の単位を示したものであり、投入係数は「ある産業に生じた需要が、各産業の需要を新たに導き出す係数」であり、後方連関被害を推計する際に用いられることが多い。

この関係を行列式に置き換える。

投入係数行列 $A:=(a_{ij}/Y_j)$ 、最終需要列ベクトル $F:=(F_1, \dots, F_n)^T$ 、国内生産額ベクトル $Y:=(Y_1, \dots, Y_n)^T$ 、および $n \times n$ の単位行列 I を用いると、産業連関表から以下の行列式が成立する。なお、産業連関表から投入係数を用いて $Y=AY+F$ が成立する過程については、付録1に記載している。

$$\begin{aligned} Y &= AY + F \\ \Leftrightarrow (I - A) Y &= F \\ \Leftrightarrow Y &= (I - A)^{-1} F \end{aligned}$$

ここで投入係数とは、ある産業において1単位の生産を行う際に必要とされる原材料等の単位を示したものであり、投入係数は「ある産業に生じた需要が、各産業の需要を新たに導き出す係数」である。上式において、レオンチェフ逆行列を $L:=(I-A)^{-1}$ と定義する。上式を用いて、産業間の相互連携を考慮した後方連関効果を推計することができる。また、本稿では、レオンチェフ逆行列を用いて前方連関効果を推計するモデルをレオンチェフモデルという。

一般に、波及効果といった場合は、このレオンチェフ逆行列を用いて後方連関効果のみを推計することが多く、本稿においても、後方連関効果についてはレオンチェフ逆行列を用いて推計する。

2) 前方連関被害の推計

また、産業連関表から得られる係数として産出(配分)係数がある。この産出(配分)係数とは、ある産業において1単位の生産を行う際に必要とされる原材料等の単位を示したものである。産出(配分)係数は「ある産業に労働力あるいは資本ストック(付加価値)の投入量を増加させた場合、各産業の生産量を新たに導き出す係数」であり、前方連関被害を推計する際に用いられることがある。

産出(配分)係数行列 $B:=(b_{ij}/Y_i)$ 、付加価値額行ベクトル $V:=(V_1, \dots, V_n)^T$ 、国内生産額ベクトル $Y:=(Y_1, \dots, Y_n)^T$ 、および $n \times n$ の単位行列 I を用いると、図2より以下の行列式が成立する。なお、連関表から産出(配分)係数を用いて $Y=BY+V$ が成立する過程については、付録1に記載している。

$$\begin{aligned} Y &= BY + V \\ \Leftrightarrow (I - B) Y &= V \\ \Leftrightarrow Y &= V (I - B)^{-1} \end{aligned}$$

上式を用いて、産業間の相互連携を考慮した生産波及効果(前方連関)を推計することができる。

上式において、ゴース逆行列を $G:=(I-B)^{-1}$ と定義する。を用いて、産業間の相互連携を考慮した前方連関効果を推計することができる。また、本稿では、ゴース逆行列を用いて前方連関効果を推計するモデルをゴースモデルという。

前方連関効果を推計する場合、このゴース逆行列を用いて推計することがあるが、その現実妥当性について以下の議論がなされており、使用されるケースは多くはない。代表的な論点としては、産出(配分)係数を一定と仮定している点があげられる[23]。しかし、例えば、サイバー攻撃による影響が大きいと考えられる情報通信産業では、長期契約が多く、サイバー攻撃により産出(配分)係数が影響を受ける程度は少ないと想定されることからゴースモデルを採用することに特段の問題は無いと考えられる。更に、情報通信産業は、各種情報の提供元であり川上産業に位置することが多いという産業特性から、情報通信産業のサービス提供が途絶した場合の影響は川上産業より川下産業への影響の方が大きいことが想定される。即ち、前方連関効果が大きいと考えられる。以上から、本稿では、前方連関効果についても推計対象とし、ゴースモデルを採用することとした。

3 サイバー攻撃による産業別の直接被害と波及被害を推計するモデル

サイバー攻撃による産業別の直接被害と川上産業への波及被害、川下産業への波及被害を推計するモデルを示す。概要は以下のとおりであるが、当モデルは、サイバー攻撃のミクロレベル(攻撃を受けた企業や組織)の被害に関する実被害データから、マクロレベル(国全体、産業毎)の被害額を推計している点に、特色がある。

3.1 生産関数を活用した直接被害推計モデル

生産関数を用いて国全体の直接被害を推計する前モデル[2]では、以下のとおり定式化を行っている。

公開済みのサイバー被害データから失われた時間を推計したうえで、マクロレベル(国全体)のサイバー攻撃による生産額の減少を直接被害額とするモデルであり、概観は図3のとおりである。

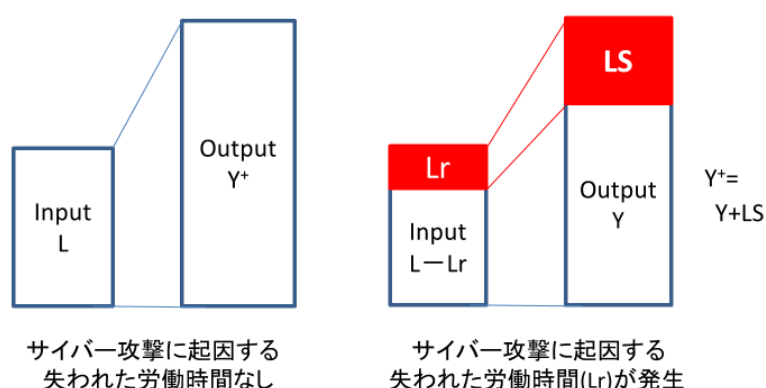


図3：生産関数によるサイバー攻撃に起因する
国レベルの被害額の推計(筆者作成)

Fig.3: National-level estimation of cyberattacks by production function

生産関数とは、労働と資本などの生産要素の投入量と、それによって達成される最大生産額(総付加価値)との間の関係を数式で表したものである。この生産関数を用いて、サイバー攻撃による実被害データから、国全体の失われた労働時間を推計のうえ、国全体の直接被害額を推計する。数式により表現すると次のとおりとなる。

$$Y = AK^{\alpha}(L - L_r)^{1-\alpha} \quad (1)$$

本来、サイバー攻撃がなければ投入された労働時間 (L) からサイバー攻撃に伴い国全体の失われた労働時間 (L_r) を差し引いた労働時間 ($L - L_r$) により「総付加価値 (Y)」が実現されると仮定し、生産関数を推計した (式(1))。また、サイバー攻撃がなければ達成された総付加価値額 (Y^+) と実際の (Y) の差を直接被害額 (LS) とした。 K は資本ストックである。

本稿では、サイバー攻撃によるインシデント、システム復旧またはデータリカバリに関係なく、資本ストック (K) は一定であると仮定した。また、式(1)は、サイバー攻撃により資本配分率 α と労働配分率 β の変動を推計できるデータがないことから、 $\alpha + \beta = 1$ (規模に関して収穫量が一定)の関係が成り立つことを前提とした。

式(1)の両辺を $L - L_r$ で割ると式(2)となる。

$$Y/(L - L_r) = AK^{\alpha} (L - L_r)^{-\alpha} = A(K/(L - L_r))^{\alpha} \quad (2)$$

式(2)から直接被害額を推計するため、式(1)の生産関数を推定することが必要となる。

A 、 α および β は、式(3)の対数変換に基づき算出した。

$$\ln Y/(L - L_r) = \ln A + \alpha \ln K/(L - L_r) \quad (3)$$

式(2)の Y^+ と Y の関係は、 $Y^+/Y=(L/(L-L_r))^{1-\alpha}$ であり、式(4)で直接被害額を推計することが可能となる。

$$LS=((L/L-L_r)^{1-\alpha}-1)Y \quad (4)$$

3.2 産業連関分析モデルを活用した波及被害推計モデル

波及被害には前方連関被害と後方連関被害の2つがあるが、まず、前モデル[2]で示した後方連関効果、続いて本稿で新たに示す前方連関効果について説明する。また、前モデル[2]では、後方連関効果のみを対象としているが、本稿では、前述の情報通信産業の特性を踏まえ、前方連関効果についても対象としている

3.2.1 後方連関効果(川上産業への波及効果)

ある生産者の生産水準が変化すれば、その生産者に中間財を供給している別の生産者の生産水準が変化する。産業連関分析においてある産業から見てサプライチェーン(あるいは産業連関)の川上産業の方向は後方連関(backward linkage)と呼ばれる。また、産業連関分析においてある産業の生産活動が後方連関に対して有する影響力は後述するレオンチェフ逆行列から計算される「影響力係数」と呼ばれる指標を利用して評価することができる。

産業連関表を用いた場合の「影響力係数」の計算方法について説明する。まず、影響力係数を計算する場合の基礎となる輪移入内生型のレオンチェフ逆行列の計算手法について説明する。式(5)において左辺は国内各産業の生産額ベクトルである。式(5)の右辺の $AY+F$ の部分は国内における各財への需要合計を示している。需要合計とは産業の中間投入需要と最終消費需要の合計である。需要合計の一部は国外からの輸入で賄われているので、需要合計から輸入を差し引き、さらに圏内産業の輸出を足し合わせる事で等式が成立する。

$$Y=AY+F+E-M \quad (5)$$

Y : 国内産業の生産額ベクトル

A : 投入係数行列

M : 輸入額ベクトル

F : 国内最終需要ベクトル

E : 輸出額ベクトル

国の各財の輸入額は、需要計の一定割合で固定と仮定すると輸入係数行列 $\hat{M}=M/(AY+F)$ を設定できる。式(5)に輸入係数行列を入れた形で表現すると以下の式(6)を得る。

$$Y=AY+F+E-\hat{M}(AY+F) \quad (6)$$

式(6)を整理することで、式(7)の表現を得る。なお、 I は単位行列である。

$$Y=(I-(I-\hat{M})A)^{-1}((I-\hat{M})F+E) \quad (7)$$

この $(I-(I-\hat{M})A)^{-1}$ は輸入競争型レオンチェフ逆行列と言われるが、ここで、式(7)の F は、式(4)で計算される直接被害額(LS)に相当し、式(4)の直接被害額(LS)は付加価値額ベース

の生産関数に基づいて推計される。一方、産業連関表では、生産額ベースで推計が行われている。このため、式(7)に F を代入する場合は、生産額ベースに修正する必要がある。また、本稿は、日本におけるサイバー攻撃による国内被害に着目しているため、自給率も考慮する必要がある。

したがって、この F は、産業毎に、 LS に国内生産額と付加価値との比率を乗じ、更に自給率を乗じて算出した。なお、付加価値は、産業毎に産業連関表の総付加価値額から家計外消費支出（宿泊費、日当費、交際費、福祉費）を減じて算出された値を用いた。また、自給率は1から輸入係数を減じて算出される係数であり、輸入係数は産業連関表の「総輸入（控除）」の絶対値を「総国内需要」で除して算出した。

また、式(5)で計算される Y には直接被害が含まれているため、波及被害から直接被害を除外する必要がある。これらの結果、後方連関効果の波及被害は式(8)を用いて推計した。

$$\begin{aligned} Y(\text{spillover damage only}) = \\ Y(\text{spillover damage including direct damage}) \\ - F(\text{direct damage}) \end{aligned} \quad (8)$$

3.2.2 前方連関効果(川下産業への波及効果)

続いて、前方連関指標について説明する。

産業連関分析において任意の生産者から見てサプライチェーンの川下産業の方向は前方連関 (forward linkage) と呼ばれ、本稿では前方連関指標としてゴーシュ逆行列 G から計算される指標を利用して計算される指標を利用する。

$$Y = YB + V \quad (9)$$

V : 付加価値額ベクトル

B : 産出（配分）係数行列

Y : 国内生産額ベクトル

式(9)を整理することで、式(10)の表現を得る。なお、 I は単位行列である。

$$Y = V(I - B)^{-1} \quad (10)$$

4 サイバー攻撃による被害額の推計

4.1 推計に使用したデータセット

本稿におけるサイバー攻撃による被害額の推計は、後述するデータセットが存在する2011年、2013年、2014年の3年分について実施した。

4.1.1 直接被害推計に使用したデータセット

日本における産業毎の直接被害の推計にあたっては、サイバー攻撃により失われた労働時間に着目して実績のある生産関数を使用し、産業毎の直接被害を推計している。

1) 総付加価値額(Y), 資本ストック(K), 労働時間(L)

純付加価値額(Y)は, JIP データ[24]の実質産出額から実質中間投入額を差し引いた額とし, 資本ストック(K) は実質純資本ストック, 総労働時間数(L)はマンアワー(従業者数×従業者一人当たり年間総実労働時間)に関するデータを使用した. なお, 当 JIP データにおける業種数は 100 業種であり, 2011 年価格で実質化されたデータである.

2) サイバー攻撃に伴い失われた労働時間(L_r)

サイバー攻撃に伴い投入された国全体及び産業別の失われた労働時間(L_r)のデータがないため, まず, A)で独立行政法人情報処理推進機構(IPA, Information-technology Promotion Agency, Japan. 以下, IPA)が実施したアンケート結果[25]から 1 企業当たりの失われた労働時間の平均時間を推計, 次に, B)で A)の結果と経済センサス[26]の企業数データから国全体の失われた労働時間を推計, 更に, C)で B)の結果と特定非営利活動法人日本ネットワークセキュリティ協会(JNSA(Japan Network Security Association. 以下,JNSA)のデータを用いて産業別の失われた労働時間を推計した. A), B), C)の具体的なデータセット及び推計手順は以下のとおりである.

A)1企業当たりの失われた平均労働時間

IPA アンケート結果[25]では, 情報管理部門がサイバー攻撃を受けた後に要した時間のアンケート結果が概説されており, この結果を本稿でも活用した. なお, この時間は情報管理部門で発生した失われた労働時間が主であり, 営業部門や管理部門など情報管理部門以外の部門での失われた労働時間は限定的である.

IPA のアンケートは, 従業員数が 300 人以上である企業と従業員数が 21 人から 300 人未満である企業に分けて実施している(従業員数が 20 人未満の企業はアンケートの対象としていない). アンケート結果の「(ア)情報管理部門が行った復旧時間作業人日」「(イ)復旧以外に発生した追加データ処理作業人日」「(ウ)復旧以外の作業人日」を基に, (ア)(イ)については, 従業員数が 300 人以上である企業と従業員数が 21 人から 300 人未満である企業に分けて, 1 企業当たりの被害時間を算出し, (ウ)については従業員規模別のアンケート結果になっていないため従業員規模に関係なく失われた平均労働時間を算出した. その際, 2~3 人/日等の幅のあるデータは「2.5 人/日」といった中央値の値, 無回答のデータは 0 人/日, また, 例えば 21 人/日以上等といったデータには, 25 人/日といった過大にならないと想定される値を適用した.

A) の推計結果は, 表 1 のとおりである.

表 1: 従業員数規模別企業の失われた平均労働時間(筆者作成)
Table1 : Average lost working hours for companies by employee size

(単位：時間)

従業員数規模	2011 年	2013 年	2014 年
300 人以上	62.6	80.1	47.7
21 人～300 人未満	44.0	44.9	40.0

B)国全体の失われた労働時間

A)で推計した1企業当たりの失われた平均労働時間を、経済センサス[26]から得られる従業員数が 300 人以上である企業数と 21 人～300 人未満である企業数にそれぞれ乗じ、その合計額を国全体のサイバー攻撃により失われた労働時間として推計した。

企業数については、経済センサス[26]には毎年度のデータがないため、平成 28 年度(2016 年)版から国全体の企業数を 3,856,457 社、従業員数が 300 人以上の企業数を 15,526 社(国全体企業数 3,856,457 社の 0.4%)、従業員が 21 人から 300 人未満の企業数を 320,085 社(国全体企業数 3,856,457 社の 0.83%)として、国全体の失われた労働時間を推計した。

B) の推計結果は、表 2 のとおりである。

表 2：国全体の失われた労働時間(筆者作成)

Table1：Lost working hours across the country

(単位：1,000 時間)

	2011 年	2013 年	2014 年
国全体	15,045	19,132	13,531

C)産業別の失われた労働時間

B)で推計されたサイバー攻撃による国全体の失われた労働時間数(L_r)と JNSA データからサイバー攻撃に伴い産業別の失われた労働時間を算出した。

この JNSA データには、公表日、業種名、漏えい原因区分、漏えい経路、被害人数、漏えい情報、被害件数、インシデント 一件当たりの想定損害賠償額及び一件当たりの想定損害賠償額等があり、年度別の個票が一覧となったデータであり、当該データのなかでサイバー攻撃のあった業種数は 14 である。

産業別失われた労働時間数の推計した手順は以下のとおりである。

まず、JNSA が JNSA データのなかで独自に算出している一件当たりの想定損害賠償額を JIP データの産業分類(100 業種)別に集計するとともに、その合計額を国全体の被害額として集計した。この産業別被害額と国全体の被害額との比率を求め、B)で算出した国全体の失われた労働時間数にこの比率を乗じることで、C)産業別(JIP データの 100 産業分類別)の失われた労働時間を推計した。

C)の推計結果は、付録 2 のとおりである。

また、この C)産業別失われた労働時間数を用いて、3.1 で示したモデルに基づき産業別(JIP データの 100 産業分類別)の直接被害を推計している。この産業別(JIP データの 100 産業分類別)の直接被害から 3.2 で示した産業連関分析モデルを用いて波及被害額を算出する際には、産業連関表の 54 産業業種に変換してうえで算出している。

4.1.2 波及被害(後方連関被害, 前方連関被害)推計に使用したデータセット

次に、波及被害推計については、産業別の直接被害を産業連関表から得られる逆行列を用いて、後方連関効果、前方連関効果を推計している。この際の、産業連関表は経済産業省が公開しているものを利用した[27](当産業連関表は、2011年から2012年にかけて産業分類が変更されたことから、2012年、2013年、2014分を使用した)。

なお、2011年、2013年、2014年の生産関数における A , α , β は表3のとおりと算出された。また、 A , α , β 算出時の決定係数(R^2)は0.5を上回っている。また、標準誤差等のその他の検定結果は、付録3に示すとおりである。

表3：生産関数における A , α , β , 決定係数(R^2)(筆者作成)

Table 3 : A, α, β , coefficient of determination (R^2) in Production Function

	2011年	2013年	2014年
A	0.340934	0.381121	0.388304
α	0.496841	0.494897	0.495205
β	0.503158	0.505102	0.504794
決定係数(R^2)	0.567585	0.580214	0.567529

4.1.3 波及被害(後方連関被害, 前方連関被害)推計に使用したデータセット

2011年、2013年、2014年の産業毎のサイバー攻撃による直接被害、波及被害(後方連関被害, 前方連関被害)及び総被害額は、付録4に示すとおりである。

5 むすび

本稿では、前モデル[2]で示した生産関数を用いた直接被害推計と産業連関分析モデルを活用した後方連関効果による川上産業への波及被害額を推計するモデルを、産業毎の前方連関効果による川下産業への波及被害額を推計するモデルに拡張した。

本稿の貢献は、極めて限定的であっても、実際の被害データ(JNSAのサイバー攻撃による被害データとIPAのサイバー被害に関するアンケートデータ)が得られれば、マクロ経済データ(産業連関表とJIPデータ)を用いる今回拡張したモデルを活用して、日本における産業毎の直接被害額と波及被害額、情報通信産業におけるサイバー攻撃による直接被害額と川上産業と川下産業への波及被害額について、定量的な数字を推計できるモデルを示したことである。また、後述のデータに関する制約が解消されることによって、より精緻な被害額推計が可能となり、レジリエンス政策等に活用可能な情報提供が可能となると考える。

本稿における制約として、モデルに関する制約とデータに関する制約がある。モデルに関する制約としては、2.2.1で述べた産業連関表そのものの制約があるが、経済波及効果において当該制約を踏まえたうえで各種分析が行われている。一方、データに関する制約は、本稿執筆時点において、日本ではサイバー攻撃による被害情報を報告する制度が整備中であり、本稿では、4.1.1の2)で述べたとおり、現時点で収集可能であるサイバー

攻撃に伴い主に情報管理部門での失われた労働時間のみを基に推計を行っている。上述のとおり、本稿で提案したモデルをより活用していくためには、サイバー攻撃に関する被害データの整備が課題である。例えば、本稿で提案したモデルを用いて分析する場合、被害データの産業分類は、現在の総務省が公表している産業連関表の大分類である 37 分類が最低限必要である。今回は JNSA のサイバー攻撃による被害データが 14 分類であったため、本稿では、直接被害を大括りに括むことしかできなかった。このサイバー攻撃による被害データについては、米国等では各種取組が進んでいる[†]。これらの動向を注視し、国全体のサイバー攻撃に関する被害データを収集し、政策に活用していく体制作りが求められる。

[†] 米国国土安全保障省（DHS）が保険会社にデータ収集および分析プラットフォーム（Cyber Incident Data and Analysis Repository）を提供し民間モデリング企業がモデリングのためにサイバーリスクの評価に活用する事例[28]、民間モデリング会社によるサイバー被害データの標準フォーマット化を推進する動き[29]等がある

付録1.レオンチェフモデルとゴースモデル

Appendix1. Leontief inverse matrix and Ghosh inverse matrix

本頁では、レオンチェフモデルとゴースモデルについて解説を行う。簡略化のために、1 国における4 産業のモデルを仮定する。以下の図4は簡略化した産業連関表である。

産業連関表では、タテ方向の計数の並びを「列」という。各列では、その部門の財・サービスの生産に当たって用いられた原材料、燃料、労働力などへの支払の内訳（費用構成）が示されており、産業連関表では、これを「投入」(input)という。一方、ヨコ方向の計数の並びを「行」という。各行では、その部門で生産された財・サービスの販売先の内訳（販路構成）が示されており、産業連関表では、これを「産出」(output)という。

		中間需要(Z_i)				最終需要 (F_i)	生産額 (Y_i)
		産業 1	産業 2	産業 3	産業 4		
中 間 投 入	産業 1	X_{11}	X_{12}	X_{13}	X_{14}	F_1	Y_1
	産業 2	X_{21}	X_{22}	X_{23}	X_{24}	F_2	Y_2
	産業 3	X_{31}	X_{32}	X_{33}	X_{34}	F_3	Y_3
	産業 4	X_{41}	X_{42}	X_{43}	X_{44}	F_4	Y_4
付加価値額(V_i)		V_1	V_2	V_3	V_4		
生産額(Y_i)		Y_1	Y_2	Y_3	Y_4		

図4: 産業連関表(筆者作成)

Fig.4: Input Output Table

Y_i は、産業 i の生産額

F_i は、産業 i の生産に対する最終需要

Z_i は、産業 i の生産に対する中間財需要

a_{ij} は、財 j の生産に用いられる財 i の生産額

V_i は、産業 i の付加価値を表す。

1. 後方連関被害を推計する行列式(レオンチェフモデル)

産業連関表の中間投入部分の列は、ある産業が生産に当たって用いられた原材料、燃料、労働力などへの支払の内訳（費用構成）を示したものである。図4を横方向に足し合わせると以下の式が得られる。

$$Y_1 = X_{11} + X_{12} + X_{13} + X_{14} + F_1 \quad (1)$$

$$Y_2 = X_{21} + X_{22} + X_{23} + X_{24} + F_2 \quad (2)$$

$$Y_3 = X_{31} + X_{32} + X_{33} + X_{34} + F_3 \quad (3)$$

$$Y_4 = X_{41} + X_{42} + X_{43} + X_{44} + F_4 \quad (4)$$

上記(1)～(4)の式は、各産業の生産の配分構造を示したものである。これらは、以下に書き換えられる。

$$Y_1 = \frac{X_{11}}{Y_1} Y_1 + \frac{X_{12}}{Y_1} Y_1 + \frac{X_{13}}{Y_1} Y_1 + \frac{X_{14}}{Y_1} Y_1 + F_1 \quad (5)$$

$$Y_2 = \frac{X_{21}}{Y_2} Y_2 + \frac{X_{22}}{Y_2} Y_2 + \frac{X_{23}}{Y_2} Y_2 + \frac{X_{24}}{Y_2} Y_2 + F_2 \quad (6)$$

$$Y_3 = \frac{X_{31}}{Y_3} Y_3 + \frac{X_{32}}{Y_3} Y_3 + \frac{X_{33}}{Y_3} Y_3 + \frac{X_{34}}{Y_3} Y_3 + F_3 \quad (7)$$

$$Y_4 = \frac{X_{41}}{Y_4} Y_4 + \frac{X_{42}}{Y_4} Y_4 + \frac{X_{43}}{Y_4} Y_4 + \frac{X_{44}}{Y_4} Y_4 + F_4 \quad (8)$$

さらに、式(5)から式(8)は、以下に書き換えられる.

$$Y_1 = a_{11} Y_1 + a_{12} Y_2 + a_{13} Y_3 + a_{14} Y_4 + F_1 \quad (9)$$

$$Y_2 = a_{21} Y_1 + a_{22} Y_2 + a_{23} Y_3 + a_{24} Y_4 + F_2 \quad (10)$$

$$Y_3 = a_{31} Y_1 + a_{32} Y_2 + a_{33} Y_3 + a_{34} Y_4 + F_3 \quad (11)$$

$$Y_4 = a_{41} Y_1 + a_{42} Y_2 + a_{43} Y_3 + a_{44} Y_4 + F_4 \quad (12)$$

ここで、 a_{ij} は、 i 産業から j 産業への投入係数であり、式(9)から式(12)を行列式で表記すると、以下の式が得られる.

$$\mathbf{Y} = \mathbf{AY} + \mathbf{F}$$

2. 前方連関被害を推計する行列式(ゴーストモデル)

産業連関表の中間投入部分の行は、その部門で生産された財・サービスの販売先の内訳(販路構成)を示したものである. 図4を縦方向に足し合わせると以下の式が得られる.

$$Y_1 = X_{11} + X_{21} + X_{31} + X_{41} + V_1 \quad (13)$$

$$Y_2 = X_{21} + X_{22} + X_{23} + X_{24} + V_2 \quad (14)$$

$$Y_3 = X_{31} + X_{32} + X_{33} + X_{34} + V_3 \quad (15)$$

$$Y_4 = X_{41} + X_{42} + X_{43} + X_{44} + V_4 \quad (16)$$

前述と同様の書き換えを行う.

$$Y_1 = \frac{X_{11}}{Y_1} Y_1 + \frac{X_{21}}{Y_1} Y_2 + \frac{X_{31}}{Y_1} Y_3 + \frac{X_{41}}{Y_1} Y_4 + V_1 \quad (17)$$

$$Y_2 = \frac{X_{12}}{Y_2} Y_1 + \frac{X_{22}}{Y_2} Y_2 + \frac{X_{32}}{Y_2} Y_3 + \frac{X_{42}}{Y_2} Y_4 + V_2 \quad (18)$$

$$Y_3 = \frac{X_{13}}{Y_3} Y_1 + \frac{X_{23}}{Y_3} Y_2 + \frac{X_{33}}{Y_3} Y_3 + \frac{X_{43}}{Y_3} Y_4 + V_3 \quad (19)$$

$$Y_4 = \frac{X_{14}}{Y_4} Y_1 + \frac{X_{24}}{Y_4} Y_2 + \frac{X_{34}}{Y_4} Y_3 + \frac{X_{44}}{Y_4} Y_4 + V_4 \quad (20)$$

さらに、式(17)から式(20)は、以下に書き換えられる.

$$Y_1 = b_{11} Y_1 + b_{21} Y_2 + b_{31} Y_3 + b_{41} Y_4 + V_1 \quad (21)$$

$$Y_2 = b_{12} Y_1 + b_{22} Y_2 + b_{32} Y_3 + b_{42} Y_4 + V_2 \quad (22)$$

$$Y_3 = b_{13} Y_1 + b_{23} Y_2 + b_{33} Y_3 + b_{43} Y_4 + V_3 \quad (23)$$

$$Y_4 = b_{14} Y_1 + b_{24} Y_2 + b_{34} Y_3 + b_{44} Y_4 + V_4 \quad (24)$$

ここで、 b_{ij} は、 i 産業から j 産業への産出(配分)係数であり、式(21)から式(24)を行列式で表記すると、以下の式が得られる.

$$\mathbf{Y} = \mathbf{BY} + \mathbf{V}$$

付録 2. 産業別失われた労働時間
Appendix2. Lost working hours by industry

(単位:1,000 時間)

JIP部門分類	2011	2013	2014
1 農業	0	0	0
2 農業サービス	0	0	0
3 林業	0	0	0
4 漁業	0	0	0
5 鉱業	0	0	0
6 畜産食料品	0	0	0
7 水産食料品	0	0	0
8 精穀・製粉	0	0	0
9 その他の食料品	0	0	0
10 飲料	0	0	0
11 飼料・有機質肥料	0	0	0
12 たばこ	0	0	0
13 繊維製品（化学繊維除く）	0	0	0
14 化学繊維	0	0	0
15 パルプ・紙・板紙・加工紙	0	0	0
16 紙加工品	0	0	0
17 化学肥料	0	0	0
18 無機化学基礎製品	0	0	0
19 有機化学基礎製品	0	0	0
20 有機化学製品	0	0	0
21 医薬品	0	0	0
22 化学最終製品	0	0	0
23 石油製品	0	0	0
24 石炭製品	0	0	0
25 ガラス・ガラス製品	0	0	0
26 セメント・セメント製品	0	0	0
27 陶磁器	0	0	0
28 その他の窯業・土石製品	0	0	0
29 鉄鉄・粗鋼	0	0	0
30 その他の鉄鋼	0	0	0
31 非鉄金属製錬・精製	0	0	0
32 非鉄金属加工製品	0	0	0
33 建設・建築用金属製品	0	0	0
34 その他の金属製品	0	0	0
35 はん用機械	0	0	0
36 生産用機械	0	0	0
37 事務用・サービス用機器	0	0	0
38 その他の業務用機械	0	0	0
39 武器製造業	0	0	0
40 半導体素子・集積回路	0	0	0
41 その他電子部品・デバイス	0	0	0
42 産業用電気機械器具	0	0	0
43 民生用電子・電気機器	0	0	0
44 電子応用装置・電気計測器	0	0	0
45 その他の電気機器	0	0	0
46 映像・音響機器	0	0	0
47 通信機器	0	0	0
48 電子計算機・同付属装置	0	0	0
49 自動車（自動車車体含む）	0	0	0
50 自動車部品・同付属品	0	0	0

JIP部門分類	2011	2013	2014
51 その他の輸送用機械	0	0	0
52 印刷業	0	0	0
53 製材・木製品	0	0	0
54 家具・装備品	0	0	0
55 プラスチック製品	0	0	0
56 ゴム製品	0	0	0
57 皮革・皮革製品・毛皮	0	0	0
58 時計製造業	0	0	0
59 その他の製造工業製品	222	151	6,973
60 電気業	357	1	0
61 ガス・熱供給業	0	0	0
62 上水道業	0	0	0
63 工業用水道業	0	0	0
64 下水道業	0	0	0
65 廃棄物処理	0	0	0
66 建築業	0	0	0
67 土木業	0	0	0
68 卸売業	0	0	0
69 小売業	1,664	4,187	1,523
70 鉄道業	0	0	0
71 道路運送業	32	5	704
72 水運業	0	0	0
73 航空運輸業	0	0	0
74 その他運輸業・梱包	0	0	0
75 郵便業	0	0	0
76 宿泊業	0	0	0
77 飲食サービス業	0	0	0
78 通信業	0	0	0
79 放送業	0	0	0
80 情報サービス業	1,589	14,639	3,725
81 映像・音声・文字情報制作業	0	0	0
82 金融業	1	3	20
83 保険業	0	0	0
84 住宅	0	0	0
85 不動産業	0	0	0
86 研究機関	321	3	182
87 広告業	0	0	0
88 業務用物品賃貸業	0	3	0
89 自動車整備業・修理業	0	0	0
90 その他の対事業所サービス	136	34	385
91 公務	28	1	19
92 教育	21	13	0
93 医療・保健衛生	10,670	60	0
94 社会保険・社会福祉	0	0	0
95 介護	0	0	0
96 娯楽業	0	0	0
97 洗濯・理容・美容・浴場業	0	0	0
98 その他の対個人サービス	3	32	0
99 会員制団体	0	0	0
100 分類不明	0	0	0
合計(1,000時間)	15,045	19,132	13,531

付録 3. 統計検定結果 Appendix3. Statistical test result

2011 生産関数における A, α, β の決定

回帰統計	
重相関 R	0.753442897
重決定 R ²	0.567676199
補正 R ²	0.566190550
標準誤差	0.632043095
観測数	293

分散分析表					
	自由度	変動	分散	観測された分散比	有意 F
回帰	1	152.6433579	152.6433579	382.1065907	6.33402E-55
残差	291	116.248236	0.399478474		
合計	292	268.8915939			

	係数	標準誤差	t	P-値	下限 95%	上限 95%
切片 (A)	0.340934692	0.075389925	4.522284549	8.91588E-06	0.192556045	0.489313339
X 値 1 (α)	0.496841655	0.025417085	19.54754692	6.33402E-55	0.446817031	0.546866278

2013 生産関数における A, α, β の決定

回帰統計	
重相関 R	0.761785360
重決定 R ²	0.580316934
補正 R ²	0.578879663
標準誤差	0.613604694
観測数	294

分散分析表					
	自由度	変動	分散	観測された分散比	有意 F
回帰	1	152.0211436	152.0211436	403.7631216	5.40149E-57
残差	292	109.9411302	0.37651072		
合計	293	261.9622738			

	係数	標準誤差	t	P-値	下限 95%	上限 95%
切片 (A)	0.381121433	0.073034785	5.218354967	3.43002E-07	0.237380109	0.524862757
X 値 1 (α)	0.494897156	0.024629275	20.09385781	5.40149E-57	0.446423752	0.54337056

2014 生産関数における A, α, β の決定

回帰統計	
重相関 R	0.753398422
重決定 R ²	0.567609183
補正 R ²	0.566128392
標準誤差	0.630818132
観測数	294

分散分析表					
	自由度	変動	分散	観測された分散比	有意 F
回帰	1	152.5331145	152.5331145	383.3149888	4.25302E-55
残差	292	116.1960026	0.397931516		
合計	293	268.7291171			

	係数	標準誤差	t	P-値	下限 95%	上限 95%
切片 (A)	0.388304644	0.075327407	5.154891979	4.68511E-07	0.240051162	0.536558125
X 値 1 (α)	0.495205882	0.02529344	19.57843172	4.25302E-55	0.445425321	0.544986442

付録 4. 2011 年, 2013 年, 2014 年の全産業の直接被害と波及被害(後方連関および前方連関)
(筆者作成, 単位: 百万円)

Appendix4. Direct damage and spillover damage (backward linkage and forward linkage) of whole industries in 2011, 2013, 2014 (M yen)

※後方連関は全産業への直接被害から当該産業が川上産業として受ける波及被害額,
前方連関は当該産業が川下産業として受ける波及被害額である.

産業（産業連関表54分類）		2011年				2013年				2014年			
		各産業のサイバー攻撃による直接被害額	全産業へのサイバー攻撃による波及被害額		総被害額	各産業のサイバー攻撃による直接被害額	全産業へのサイバー攻撃による波及被害額		総被害額	各産業のサイバー攻撃による直接被害額	全産業へのサイバー攻撃による波及被害額		総被害額
			後方連関	前方連関			後方連関	前方連関			後方連関	前方連関	
1	農林水産業	0	176	1,037	1,213	0	69	1,334	1,403	0	176	125	302
2	鉱業	0	10	1,374	1,384	0	6	1,280	1,286	0	13	178	191
3	石炭・原油・天然ガス	0	86	1,816	1,902	0	7	1,133	1,140	0	7	188	195
4	飲食品	0	328	1,155	1,483	0	59	1,742	1,801	0	90	167	257
5	繊維工業製品	0	38	1,705	1,743	0	47	1,756	1,803	0	69	181	250
6	衣服・その他の繊維既製品	0	55	1,592	1,648	0	42	2,145	2,187	0	31	192	223
7	製材・木製品・家具	0	235	1,392	1,627	0	266	1,998	2,263	0	323	202	524
8	パルプ・紙・紙加工品	0	607	2,847	3,454	0	1,065	2,347	3,412	0	2,203	222	2,424
9	化学基礎製品	0	1,000	2,646	3,646	0	225	1,596	1,821	0	391	219	609
10	化学最終製品	0	3,450	1,693	5,143	0	330	1,983	2,313	0	739	293	1,032
11	石油・石炭製品	0	2,595	1,498	4,093	0	726	953	1,679	0	731	154	885
12	プラスチック・ゴム	0	596	1,639	2,235	0	1,050	1,959	3,009	0	1,444	215	1,659
13	窯業・土石製品	0	171	1,841	2,012	0	84	1,457	1,541	0	134	192	326
14	鉄鋼	0	435	2,068	2,503	0	347	1,483	1,830	0	434	178	612
15	非鉄金属	0	174	1,900	2,073	0	97	1,777	1,875	0	289	204	492
16	金属製品	0	411	1,534	1,945	0	220	1,665	1,885	0	371	177	549
17	はん用機械	0	89	1,320	1,409	0	132	1,679	1,811	0	71	214	285
18	生産用機械	0	88	1,228	1,317	0	151	1,820	1,971	0	88	253	341
19	業務用機械	0	265	1,413	1,679	0	70	1,944	2,014	0	33	256	289
20	電子部品	0	143	1,783	1,926	0	218	2,109	2,327	0	168	302	469
21	産業用電気機器	0	53	1,469	1,523	0	77	2,333	2,410	0	43	345	388
22	民生用電気機器	0	10	1,489	1,499	0	18	1,971	1,988	0	8	216	224
23	その他の電気機械	0	24	1,419	1,443	0	30	2,275	2,305	0	27	351	379
24	民生用電子機器	0	2	1,435	1,436	0	2	2,433	2,436	0	1	321	322
25	通信機械	0	9	1,361	1,370	0	21	1,995	2,016	0	7	251	257
26	電子計算機・同附属装置	0	1	1,455	1,456	0	1	3,309	3,310	0	1	600	601
27	乗用車	0	0	1,591	1,591	0	0	2,097	2,097	0	0	239	239
28	その他の自動車	0	9	1,603	1,612	0	14	1,931	1,945	0	8	214	222
29	自動車部品・同附属品	0	345	1,561	1,907	0	550	1,899	2,449	0	245	193	438
30	その他の輸送機械	0	46	1,415	1,461	0	44	1,650	1,694	0	69	190	259
31	その他の製造工業製品	503	588	1,497	2,587	361	935	1,762	3,058	17,268	1,141	178	18,586
32	建築	0	0	992	992	0	0	1,484	1,484	0	0	143	143
33	建設補修	0	1,497	1,031	2,527	0	527	1,616	2,143	0	467	141	608
34	公共事業	0	0	884	884	0	0	1,308	1,308	0	0	147	147
35	その他の土木建設	0	0	895	895	0	0	1,293	1,293	0	0	154	154
36	電力	18,050	3,542	4,123	25,716	39	658	2,198	2,895	0	757	433	1,190
37	ガス・熱供給	0	198	1,529	1,727	0	119	1,485	1,604	0	104	251	356
38	水道	0	303	1,713	2,016	0	127	3,117	3,244	0	122	695	817
39	廃棄物処理	0	457	1,200	1,657	0	62	783	845	0	58	125	184
40	商業	2,813	3,238	781	6,833	7,825	2,136	1,629	11,591	2,813	3,082	302	6,197
41	金融・保険・不動産	0	2,854	373	3,227	24	4,216	1,137	5,378	166	2,112	253	2,532
42	運輸・郵便	71	1,924	741	2,735	12	1,457	957	2,426	1,570	2,395	180	4,145
43	通信・放送	0	692	837	1,528	0	1,376	2,276	3,652	0	433	538	971
44	情報サービス	5,595	982	809	7,386	54,323	1,815	2,060	58,198	13,759	735	461	14,955
45	その他の情報通信	0	602	1,113	1,715	0	1,797	3,193	4,990	0	733	643	1,376
46	公務	164	107	823	1,095	3	120	1,790	1,913	112	73	344	529
47	教育・研究	1,466	1,018	705	3,189	56	1,484	1,115	2,656	883	921	256	2,060
48	医療・福祉	29,053	954	1,764	31,771	166	11	1,427	1,604	0	7	196	203
49	その他の非営利団体サービス	0	148	730	878	0	130	2,378	2,507	0	72	438	510
50	物品賃貸サービス	7	997	495	1,499	34	1,358	1,183	2,574	0	918	234	1,153
51	広告	0	556	895	1,451	0	1,174	2,290	3,464	0	541	476	1,017
52	その他の対事業所サービス	369	5,964	648	6,981	85	10,812	1,382	12,279	931	4,309	242	5,482
53	対個人サービス	10	618	1,085	1,713	93	223	1,520	1,836	0	99	176	274
54	その他	0	587	1,352	1,939	0	656	1,876	2,532	0	408	227	635
合計		58,102	39,098	74,258	171,458	63,021	37,095	95,978	196,094	37,502	27,523	14,139	79,164

(筆者作成)

参考文献

- [1]サイバーセキュリティ戦略本部, “サイバーセキュリティ 2024”, Cybersecurity Strategic Headquarters,” Cybersecurity 2024”, <https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024.pdf>, Aug 2024.
- [2] A. Kokaji, A. Goto, ”An analysis of economic losses from cyberattacks: based on input–output model and production function. Journal: Journal of Economic Structures” , Journal of Economic Structures, DOI : 10.1186/s40008-022-00286-4, Dec 2022.
- [3]CSIS(Center for Strategic and International Studies) ,McAfee, ”The hidden cost of cybercrime”, <https://www.csis.org/analysis/hidden-costs-cybercrime>,Jan 2020.
- [4]RAND Cooperation, ”Estimating the global cost of cyber risk : methodology and examples”, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2299/RAND_RR2299.pdf, Jan 2023.
- [5]Cyber Security Ventures, ”Cybercrime to cost the world \$10.5 trillion annually”, <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>,Jan 2023.
- [6]Microsoft, Frost & Sullivan,” Cybersecurity threats to cost organizations in Asia Pacific US\$1.75 trillion in economic losses” <https://news.microsoft.com/apac/2018/05/18/cybersecurity-threats-to-cost-organizations-in-asia-pacific-us1-75-trillion-in-economic-losses> ,Jan 2023.
- [7]Accenture, Ponemon Institute, ”The cost of cybercrime”, <https://www.sciencedirect.com/science/article/abs/pii/S1353485819300327> ,Jan 2023.
- [8]JNSA, ” 情報セキュリティインシデントに関する調査報告” , JNSA, “Information security incident research report (Japanese Edition)” <https://www.jnsa.org/result/incident/2018.html>, Jan 2023.
- [9]トレンドマイクロ, “2020 年度 法人組織のセキュリティ動向” ,TrendMicro, “Enterprises security trend in 2020 (Japanese Edition)” . https://www.trendmicro.com/ja_jp/about/press-release/2020/pr-20201002-01.html, Jan 2023.
- [10]Security Incidents Organization , “RISI (Repository of Industrial Security Incidents”, <https://www.risidata.com>,Jan 2023.
- [11]Ponemon, “2015 Cost of cyber crime study :United States(cybercrime)” <https://www.ponemon.org/local/upload/file/2015%20US%20CCC%20FINAL%204.pdf>,Jan 2023.
- [12]Ponemon,”2015 Cost of data breach study:global analysis(cyberimpact)”, <https://www.ponemon.org/local/upload/file/2015%20US%20CCC%20FINAL%204.pdf>,Jan 2023.
- [13]CSIS, ”The economic impact of cybercrime and cyber espionage” <https://www.csis.org/analysis/economic-impact-cybercrime-and-cyber-espionage>, Jan 2023.
- [14]AFCEA(Armed forces communications and electronic association), <https://www.afcea.org/>, Jan 2023.
- [15]Center for Strategic and International Studies(CSIS),McAfee, “The hidden costs of cybercrime,” <https://www.csis.org/analysis/hidden-costs-cybercrime> ,Jan 2023.
- [16]Lloyd’s and Cambridge Centre for Risk Studies University of Cambridge Judge Business School, “Business blackout,” <https://www.lloyds.com/businessblackout>, Jan 2023
- [17]IPA “情報セキュリティ事象被害額調査,” 独立行政法人情報処理推進機構 (IPA) , IPA, “Information security incident damage survey (Japanese Edition)” <https://www.ipa.go.jp/security/products/products.html>,Jan 2014
- [18]三菱総合研究所,” 社会問題から見たサイバーセキュリティに関する技術課題” , MRI, “Technology issues in cybersecurity from social problems (Japanese Edition) ” <https://www.nisc.go.jp/pdf/council/cs/kenkyu/dai09/09shiryou03.pdf> , Jan 2023.
- [19]田中秀幸,竹村敏彦,飯高雄希,花村憲一,小松文子,”情報セキュリティインシデントによる経

- 済損失の推計に関する研究“，経済政策ジャーナル，vol.11,no.2, pp.59-62.2015 H. Tanaka, T. Takemura, Y. Iidaka, K. Hanamura, A. Komatsu, “A study about an estimation of economic loss by information security incidents (Japanese Edition)”, Journal of economic policy studies, vol.11,no.2, pp.59-62.2015
- [20]Lloyd’s, “Cloud down” <https://www.lloyds.com/businessblackout> ,Jan 2023.
- [21]JNSA, “情報セキュリティインシデントに関する調査結果 ～個人情報漏えい編～ (2018)” ,JNSA, “Information security incident survey – personal information leakage – (2018) (Japanese Edition)” <https://www.jnsa.org/result/incident/2018.html> ,Jan 2018.
- [22]Martin Eling, Mauro Elvedi & Greg Falco, “The Economic Impact of Extreme Cyber Risk Scenarios, North American Actuarial Journal”, 2022,DOI: 10.1080/10920277.2022.2034507 <https://www.tandfonline.com/doi/full/10.1080/10920277.2022.2034507>, June.2023
- [23]下田充,藤川清史, “産業連関分析モデルと東日本大震災による供給制約”, 産業連関 Vol. 20, No. 2 ,2012.
M.Shimoda, K.Fujikawa, ”I/O MODERU TO HIGASINIHONDAISHINSAI NIYORU KYOUKYUUSEIYAKU”,SANGYOHRENKAN Vol.20,No.2,2012
- [24]独立行政法人経済産業研究所, JIP データベース,
The Research Institute of Economy, Trade and Industry, “JIP databas (Japanese Edition) e”.
<https://www.rieti.go.jp/jp/database/jip.html> , Jan 2023.
- [25]IPA, “情報セキュリティ事象被害状況調査”, 2011,2013,2014. IPA,”JOHO SEKYURITHI JISYOU HIGAI JYOUKYOUTYOUSHA”.
(2011)調査報告書 P.81,P.84,P.85-88
<https://web.archive.org/web/20220812101254/https://www.ipa.go.jp/security/fy23/reports/isec-survey/index.html>,Apr 2024.
(2013)調査報告書 P.84,P.87,P.88-93
<https://web.archive.org/web/20220812101622/https://www.ipa.go.jp/security/fy25/reports/isec-survey/index.html>,Apr 2024.
(2014)調査報告書 P.85,P.89,P.91-101
<https://web.archive.org/web/20220812101419/https://www.ipa.go.jp/security/fy26/reports/isec-survey/index.html>,Apr 2024.
- [26]総務省統計局, “平成 28 年(2016 年)経済センサス - 活動調査 (確報) 産業横断的集計 <要約>” Statistics Bureau, Ministry of Internal Affairs and Communications, “2016 Economic Census - Activity Survey (Final Report) Cross-Industry Tabulation <Summary>”
https://www.stat.go.jp/data/e-census/2016/kekka/pdf/k_yoyaku.pdf ,Apr 2024.
- [27]経済産業省, “延長産業連関表”, Ministry of Economy, Trade and Industry, “Input Output table (Japanese Edition)” <https://www.meti.go.jp/statistics/tyo/entyoio/index.html> ,Jan 2023.
- [28]US Homeland Security Dedital Library,” DHS Cyber Incident Data and Analysis Working Group” .
<https://www.hsdl.org/c/dhs-cyber-incident-data-and-analysis-working-group/>,Apr 2024.
- [29]RMS(Risk Management Solutions), “RMS Redefines Today’s Data Standard With The Risk Data Open Standard “, <https://www.rms.com/newsroom/press-releases/press-detail/2019-05-14/rms-redefines-todays-data-standard-with-the-risk-data-open-standard>,Apr 2024.