ソシオネットワーク戦略ディスカッションペーパーシリーズ ISSN 2434-9445
第 84 号　2020 年 3 月
RISS Discussion Paper Series
No.84　March, 2020

イベントスタディによる IT サプライチェーン上のセキュリティインシデントが株価に与える影響の測定

竹村敏彦・小山明美・小川隆一

文部科学大臣認定　共同利用・共同研究拠点

関西大学ソシオネットワーク戦略研究機構

Research Institute for Socionetwork Strategies,
Kansai University
Joint Usage / Research Center, MEXT, Japan
Suita, Osaka, 564-8680, Japan
URL: http://www.kansai-u.ac.jp/riss/index.html
e-mail: riss@ml.kandai.jp
tel. 06-6368-1228
fax. 06-6330-3304

イベントスタディによるITサプライチェーン上のセキュリティインシデントが株価に与える影響の測定*

竹村敏彦† 小山明美‡ 小川隆一‡

概要

IT システム・サービスに関する業務の一部を系列企業やビジネスパートナーなどに外部委託し、その業務委託が、さらに委託先から再委託先、再々委託先へと連鎖する委託形態（「IT サプライチェーン」と呼ばれる）は一般的なものとなりつつある。この IT サプライチェーン上においてインシデントが発生すれば、その影響は 1 つの企業だけではなく、そのサプライチェーン上の他の企業にも波及することが容易に想像できる。本研究では、IT サプライチェーン上でインシデントが発生したとき、そのことがサプライチェーン上の企業の株価のリターンに与える影響について検証を試みる。具体的には、イベントスタディの手法を用いて、公開情報から収集した IT サプライチェーン上で発生した国内の主なインシデント事例をもとに、2012～2017 年におけるインシデントの公表の効果に関する分析を行った。その結果、インシデントの発生は委託先企業よりも委託元企業の企業価値を低下させてしまうことや、原因が不正アクセスの場合や 5000 件を超える個人情報の漏洩が発生した場合は継続的に企業価値が低下し続けることなどを明らかにした。

キーワード：IT サプライチェーン、セキュリティインシデント、イベントスタディ、株価、FF3（Fama-French 3 ファクター・モデル）

---

* 本研究の一部は、独立行政法人日本学術振興会の科研費（17K03827 および 17K00463）の助成、文部科学大臣認定共同利用・研究拠点 関西大学ソシオネットワーク戦略研究機構に対する文部科学省助成を得て行った研究成果である。

また、本研究の意見は、著者たち個人に帰属し、所属機関の公式見解を示すものではないことをことわっておく。

† 城西大学経済学部 教授

関西大学ソシオネットワーク戦略研究機構 ネットワーク分析ユニット研究員

E-mail: tkmrtshk@josai.ac.jp

‡ 独立行政法人情報処理推進機構

E-mail: a-koyama@ipa.go.jp

E-mail: r-ogawa@ipa.go.jp

Measuring the Impact of Security Incidents over IT Supply Chain on the Stock Price of Firms by Fama-French 3 Factors Model*

Toshihiko TAKEMURA † Akemi KOYAMA ‡ Ryuichi OGAWA ‡

Abstract

At recent the consignment of business activities with respect to IT systems and/or services becomes more complicated. The reason is that IT supply chains are constituted with multiple firms such as family firms or their business partners If the security incident occurs over an IT supply chain, the negative effects of the incidents would spread to the multiple firms over the IT supply chain. In this article, we measure and verify the impact of security incidents over an IT supply chain on the stock value of firms by using the methodology called "event study." We adopt a Fama-French 3 factors model and use the Japanese security incidents cases from Oct. 2012 to Oct. 2017 which are taken up by IPA's report. As a result of analyses, we found the following. (1) even if the incidents occur in the trustees, to disclose the occurrence of the security incidents would decrease the stock value of the firms which would be especially entrusters rather than trustees. (2) in a case that the cause of the incidents is illegal access and a case that the number of individual information leakage is over 5000, the stock value of the firms would continue to decrease for about one month.

Keywords: IT Supply-Chain, Security Incidents, Event Study, Stock Price, FF3 (Fama-French 3 Factors Model)

---

* This work was supported by Japan Society for the Promotion of Science: Grant-in-Aid for Scientific Research (C) (17K03827 and 17K00463) and by Kansai University and Matching Fund Subsidy from MEXT (Ministry of Education, Culture, Sports, Science and Technology).

Note that the opinions of this study belong to the authors and do not represent the official views of their institution.

† Professor, Faculty of Economics, Josai University

Researcher, The Research Institute for Socionetwork Strategies, Kansai University

E-mail: tkmrtshk@josai.ac.jp

‡ Information-technology Promotion Agency, Japan (IPA)

E-mail: a-koyama@ipa.go.jp

E-mail: r-ogawa@ipa.go.jp

1. はじめに

IT システム・サービスに関する業務の一部を系列企業やビジネスパートナーなどに外部委託し、その業務委託が、さらに委託先から再委託先、再々委託先へと連鎖する委託形態（「IT サプライチェーン」と呼ばれる）は一般的なものとなりつつある（図 1)。この IT サプライチェーン上においてインシデントが発生すれば、その影響は 1 つの企業だけではなく、そのサプライチェーン上の他の企業にも波及する。近年、 IT サプライチェーンリスク（業務の委託元や委託先、再委託先に対するサイバー攻撃、調達したソフトウェアの未知の脆弱性、システム停止・情報流出・不正アクセスなどによる IT システム・サービスにおける情報セキュリティに係るリスク）の顕在化により、多くの企業はビジネスパートナーや委託先も含めた IT サプライチェーン上のセキュリティ対策について考えなければならない。例えば、同じ企業・グループ内であれば、セキュリティガバナンスを効かせることが可能であるものの、IT サプライチェーン上にはセキュリティガバナンスの及ばない企業も存在するため，必要なセキュリティ対策がとられていない企業を踏み台として攻撃が仕掛けられたり、不正侵入されたりする恐れがある。また、IT サプライチェーンリスクに対する認識や業務委託契約やこれに類する取り決めに関する考え方について、委託元と委託先の間で必ずしも一致していないことが明らかになっており、両者の間には（深刻な）理解の不一致（認識の齟齬）が存在しがちである（小山他, 2019a; 森他, 2019; 森他, 2020）[1]。

情報処理推進機構（IPA）は、2016 年度から IT サプライチェーンに注目し、その上で発生するインシデントや情報セキュリティ上のリスクならびに企業における当該リスクの防止・低減のためのマネジメント（IT サプライチェーンリスクマネジメント）について調査・分析を継続的に行っている。2017 年度には、過去 5 年間における IT サプライチェーン上で発生した国内の主なインシデント事例を公開情報から収集し、典型パターンについて整理を行っている（情報処理推進機構, 2018)。

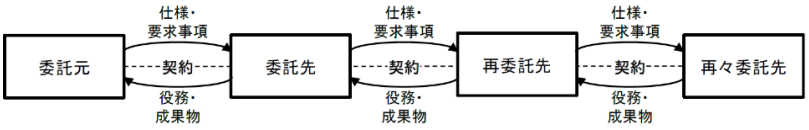


図 1：IT サプライチェーン

本研究では、情報処理推進機構（2018)で収集された事例をもとにイベントスタディと呼ばれる手法を用いて、関連企業の株価に与える影響について分析を行う。イベントスタディとは、企業に関連したイベント（本研究では、IT サプライチェーン上のインシデント発生の公表）前後の株式の平均（累積）超過リターンの動きを検証することで、そのイベントが

[1] 業務委託契約やこれに類する取り決めにおいて必要なセキュリティ要件を提示し、合意しておくことが重要となることも併せて指摘されている。

企業価値に与える影響や情報の効率性を検証する手法である。この手法は、会計学やファイナンスの分野において個別企業や経済全体の多くの出来事（企業の合併・買収、負債や株式の新規発行、マクロ経済変数の公表など）の分析に広く利用されている（Campbell , et al., 1997)。

2. 関連研究

イベントスタディの手法を用いて、企業価値に対する情報セキュリティインシデントの影響を検証する研究は海外において早くから進められている。Konchitchki and O'Leary (2011)や Arcuri, et al. (2017)、Malliouris and Simpson (2019)などはこれらの先行研究を整理しているので参照されたい。また、日本においてもこれらの関係を検証している研究がある（Ishiguro, et al., 2006; 河路, 2006; 廣松, 2011; 田中・中野, 2016; 中村, 2016; 竹村他, 2020)。これらの研究の多くにおいて、情報セキュリティインシデントに関する公表が企業の株価変動に負の影響を与えていることが統計的に確認されている。一方で、両者の間には必ずしも関連性が見られないことを指摘する研究もある（Kannan, et al., 2007）[2]。

また、先行研究の共通点として、イベントスタディはいずれもシングルファクター・モデル（市場ポートフォリオのリターンの変動だけで企業のリターンの変動を説明しようとするモデル）によって行われている。しかしながら、近年では、イベントスタディのポピュラーな手法として 3 ファクター・モデル（Fama and French, 1993）や 5 ファクター・モデル（Fama and French, 2015）などが提唱されており、シングルファクター・モデルでは、情報セキュリティインシデントに関する公表に対する株価の反応が特定できていない可能性は否定できない。竹村他（2020)では，5 ファクター・モデルを用いて IT サプライチェーン上のインシデント発生に対する株価の反応の測定ならびに分析を試みている。その結果、インシデントの発生は委託先企業よりも委託元企業の企業価値を低下させてしまうことや、原因が不正アクセスの場合は継続的に企業価値が低下し続けることなどを確認している。竹村他（2020)は、分析の対象を東証一部上場企業としたため、東証二部や新興市場に上場している企業は分析の対象から外していた。しかしながら、本研究では、市場拡張版の 3 ファクターデータを用いて、これらの企業も分析対象として含めた分析を試みる。

本研究では、3 ファクター・モデルを用いて IT サプライチェーン上のインシデント発生に対する株価の反応の測定ならびに分析を行う。また、竹村他（2020)で試みられているグルーピングに「個人情報漏洩件数」の視点によるものを加えて更なる分析などを試みている。

3. 検証方法

3.1 イベントスタディ

[2] その理由として、事前に（日頃から）リスク評価を行っていることや、早急かつ適切な事後対応を行っていることを挙げている。

本研究では、ITサプライチェーン上のインシデント発生に対する株価の反応を測定するために、Fama and French (1993)による3ファクター・モデルを利用する。

3ファクター・モデルは、企業価値に与える要因として、市場リスク・プレミアムの他に、サイズ・プレミアム（SMB）とバリュー・プレミアム（HML）を組み入れたモデルである。SMBは、時価総額を指標として作成する分位ポートフォリオの平均リターンから計算されるスプレッド・リターンである。SMBは、時価総額の小さい（小型株）ポートフォリオの平均リターンから時価総額の大きい（大型株）ポートフォリオの平均リターンを差し引いて求められ、大型株に比べて小型株は倒産リスクが高く流動性が低い傾向が強いことに対してプレミアムが要求された一つの結果としてその値がプラスとして観測されるものと解釈できる。一方で、HMLは、実績自己資本の時価総額に占める比率（簿価時価比率）に基づいて作成する分位ポートフォリオの、最高位と最低位のポートフォリオの横断的平均リターンの差として得られるスプレッド・リターンであり、将来の成長が期待される成長株と見なされる。HMLは割安株と成長株のリターンの差を表していることから、経験的に割安株の方が成長株よりもパフォーマンスがよく、プラスのプレミアムが期待できるものである。図2に示したように、SMBで2分割、HMLで3分割することで6 つのグループが作成され、これらが分析に用いられる。詳しくは、久保田・竹原（2007)などを参照されたい。

		簿価時価比率		
		Low	Medium	High
時価総額	Big	Big / Growth B/L	Big / Neutral B/M	Big / Value B/H
	Small	Small / Growth S/L	Small / Neutral S/M	Small / Value S/H

図2：Fama-Frenchモデルのグルーピング

3 ファクター・モデルによる推定では、イベント公表の影響を受けていない（イベント公表日以前の）推定期間（estimation window）として、140 日前から 21 日前までの 120 日間を推定期間として想定する [3]。また、対象となる企業 i の日次リターン $R_i(t)$と日次の市場ポートフォリオのリターン $R_M(t)$は以下のように計算される。

$$R_i(t)=[P_i(t)-P_i(t-1)]/[P_i(t-1)]$$
$$R_M(t)=[P_M(t)-P_M(t-1)]/[P_M(t-1)]$$

これらの日次リターンデータなどを用いて、対象企業ごとに、式 (1)の 3 ファクター・モ

[3] 本研究では、推定期間を 140 日前から 21 日前までの 120 日間としているが、この期間の設定は研究によって異なる。また、イベント日はインシデント発生日ではなく、インシデントが発生したことを公表した日としている。

デルを推定する。

$$R_i(t) = \alpha_i + \beta_i R_M(t) + \varepsilon_i(t)$$
$$R_i(t) - R_F(t) = a_i + b_i [R_M(t) - R_F(t)] + s_i SMB(t) + h_i HML(t) + \varepsilon_i(t) \quad (1)$$

ここで、$R_F(t)$は無リスク利子率、SMB(t)はサイズ・プレミアム（SMB)、HML(t)はバリュー・プレミアム（HML)、$\varepsilon_i(t)$は誤差項である[4]。また、b_i、s_i、h_iはそれぞれのプレミアムに対する感応度を表している。得られた係数推定量を a_i^、b_i^、s_i^、 h_i^とすると、t 日における企業 i の超過リターン（AR; abnormal return）は式 (2)より計算される。

$$AR_i(t) = R_i(t) - R_F(t) - [a_i^ + b_i^ (R_M(t) - R_F(t)) + s_i^ SMB(t) + h_i^ HML(t)] \quad (2)$$

平均的なイベント公表の効果を検証するために、個別企業について算出された $AR_i(t)$をもとに t 日における平均超過リターン（AAR; average abnormal return）は式(3）によって計算される。

$$AAR(t) = 1/N_t \times \Sigma AR_j(t) \quad (3)$$

ここで、N_t は t 日における対象企業数である。

各イベント期間に対する検定統計量は、

$$AAR(t)/S^ \quad (4)$$

で与えられる。S^は推定期間における AAR(t)の標準偏差である。なお、AAR(t)が i.i.d.の正規分布に従うとき、超過リターンがゼロという帰無仮説の下では、式 (4)の検定統計量は t 分布に従う。

次に、サプライチェーン上のインシデント発生に関するイベント日（t=0）を含むイベント期間（event window）$[t_1, t_2]$（$t_2 > t_1$）を設定して、その累積平均超過リターン（CAAR; calculated average abnormal return）を式(5）により計算する。

$$CAAR[t_1, t_2] = \Sigma AAR(t) \quad (5)$$

イベント期間$[t_1, t_2]$における累積平均超過リターンに対する統計検定量は

[4] 式(1)における$[R_M(t) - R_F(t)]$は市場リスク・プレミアムと呼ばれるものである。

$CAAR[t_1, t_2]/ [(t_2\text{-}t_1+1)S^{\wedge}]$ (6)

で与えられる。式 (6)の検定統計量も t 分布に従う（Brown and Warner, 1985)。

3.2 分析対象企業および分析期間

情報処理推進機構（2018)は、2012 年 10 月から 2017 年 10 月における IT サプライチェーン上で発生した国内外のインシデント事例をもとに、委託元の業種および原因区分の網羅性、インシデント被害のインパクトの観点で 52 件を抽出し、それらの特徴・典型パターンについてまとめている [5]。表 1 は収集したインシデント事例の委託元業種と原因区分の属性をまとめたものである。

表 1：インシデント事例集の属性

委託元の業種	不正アクセス	ウイルス	SW のバグ	内部不正	人的ミス	盗難紛失
製造業	1				1	
電気・ガス・熱供給・水道業		1				1
情報通信業	1			1		1
運輸業, 郵便業					1	
卸売業, 小売業	8		2			
金融業, 保険業	1			1		
その他サービス業	7	1			1	1
教育, 学習支援業				2		
医療, 福祉	1					
国家・地方公務	8	1			3	1
公益法人等			1			
教育機関	2				3	

これらの事例に関して、インシデントが発覚する主体（委託元、委託先、顧客）による発覚経緯や、事業分野ごとのインシデント原因が特徴的であること、またインシデントの発生箇所として委託先（再委託先や再々委託先も含む）が多いことが指摘されている [6]。また、インシデントの発生箇所が委託先や再委託先であったとしても、ウェブページ等でこれらのインシデントについて委託元のみが公表した事例数は 37 件、委託先のみが公表した事例数は 10 件であった（3 件は委託元・委託先がともに公表していた)。さらに、その公表された内容には（リスク管理の一環として）必ずしもインシデントの発生箇所となった企業名は明記されず、例えば HP 管理委託業者といった記載にとどまっているという特徴もあった。

表 1 を見てわかるように、委託元の業種には国家公務・地方公務や公益法人等（公益法

[5] 情報処理推進機構（2018)にも記載されているように、これらの整理は公開情報のうち意図的に抽出したものに対して実施されており、発生したインシデント全体の傾向ではないことを断っておく。

[6] 52 件のインシデント事例のうちインシデントの発生箇所が委託先（再委託先や再々委託先も含む）であったものは 50 件であった。委託先で発生するケースとして、委託元から運営委託された WEB サイトや EC サイトに対する不正アクセスの事例、再委託先で発生するケースとして、再委託先以降の社員による内部不正で、顧客の個人情報を窃取する事例が挙げられている。

人、社団法人、財団法人、NPO 法人）が含まれているが、イベントスタディの対象企業は株式上場している必要があるため、これらの業種はイベントスタディの分析対象とならない。そのため、インシデント発生を公開した上場企業もしくは上場企業の連結子会社を対象とすることになる。また、事例によっては委託元だけでなく IT サプライチェーン上にある委託先や再委託先などの企業についての情報が公開されていることもあり、これらの企業についても同様に取り扱うことにする。　厳密に言えば、廣松 (2011)などで行われているように、全国紙または主要な地方紙に記事として掲載されたケースを選択基準として、分析対象ならびにインシデント発生の公表日（報道日）を特定すべきである。これは、株式市場への影響という観点からは新聞等のマスメディアによって、インシデントが報道された時点を公表日とすることが望ましいと考えられるためである。しかしながら、本研究においては、当該企業のホームページやネットニュース等で公表された日をイベント日として設定している。なお、1 つの企業が短期間に複数のインシデント発生に直面することや情報を何度かに分けて公表することがある。その場合、最初に公表された日をイベント日とする。

整理の結果、分析に用いることができる東証一部・二部ならびに新興市場上場企業数は 37 社となった。内訳は、委託元の企業数が 17 社、委託先の企業数が 20 社であった（再委託先は委託先の企業数の中に含めている）[7]。また、原因区分が不正アクセスかそれ以外のインシデントかに分けたところ、前者の企業数が 14 社、後者の企業数が 23 社となった。さらに、個人情報の漏洩件数が 5000 件を超えるケースとそれ以外のケースに分けたところ、前者に該当する企業数が 17 社、後者に該当する企業数が 20 社となった [8]。

3.3　データおよび変数の定義

分析に用いる株式データなどは日本経済新聞社が提供する『日経 NEEDS-Financial QUEST2.0』ならびに、金融データソリューションズが提供する『日本上場株式 Fama-French 関連データ』の 3 ファクターデータ（市場拡張版）を利用する。このデータセットは，構成銘柄ユニバースとして、東証 1 部に東証 2 部に加え、新興市場銘柄を追加して計算した市場拡張版である。なお、市場リスク・プレミアム、サイズ・プレミアム、バリュー・プレミアムに関するデータの構築の仕方については金融データソリューションズ (2016)を参照されたい。

4.　分析結果

イベント期間については、営業日ベースでイベント日の 5 日前（イベント日の 1 週間前）

---

[7] なお、上述したように、これらの計数は 1 つの事例においても複数の企業（委託元や委託先）が関わっていることことを断っておく。

[8] 2017 年 5 月 30 日に改正された個人情報保護法では、保有している個人情報が 5,000 件以下の事業者であっても適用の対象であるものの、それ以前は 5,000 件を超える個人情報を保有する事業者のみが個人情報保護法の適用対象であった。そのため、本研究では、5000 件を 1 つの目安として採用した。

から 20 日後（イベント日から約 1 か月）の期間を設定して分析を試みる。イベント期間の設定については明確な基準は存在しないものの、株価に対するイベント以外の影響を極力排除するために、一般的にはイベント期間は短い方が望ましいとされる。一方で、イベントに関する情報が投資家に十分に伝わりにくいと考えられる場合には、イベント期間を多少拡大することで株価に対する影響を拾い上げることも行われる。本研究では、イベント公表日前にも株価が変動する可能性があることを考慮してイベント 5 日前から計測する。

4.1　全体

図 3 にはイベント日の 5 日前からの平均超過リターン AAR[-5, t]を時系列的にプロットしたものを示している。また、全サンプル（37 社）を対象としたものである。なお、図 3 をはじめとする図表における横軸の座標 0 はイベント（IT サプライチェーン上のインシデント発生の）公表日を表している。また、図 3 は平均超過リターンの検定統計量をまとめたものである。

図 3：平均超過リターンの推移 I

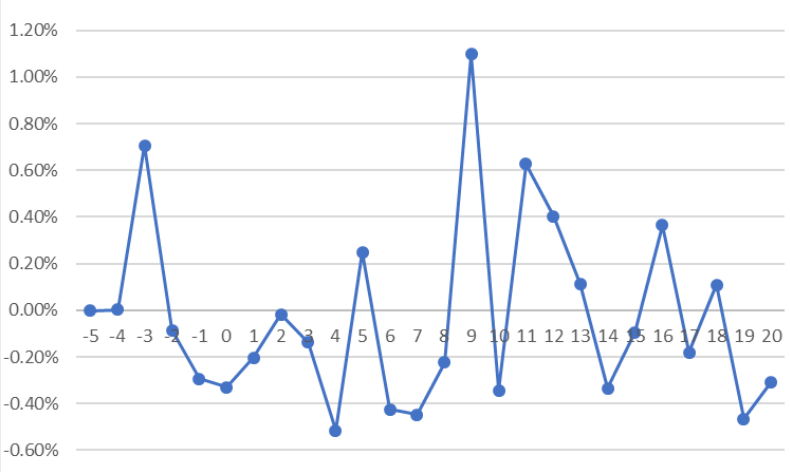


表 2：平均超過リターン I

	全サンプル	t 値		全サンプル	t 値
-5	-0.001	-0.394	8	-0.225	-0.761
-4	0.002	0.829	9	1.098**	3.717
-3	0.706**	2.389	10	-0.343	-1.163
-2	-0.085	-0.287	11	0.628*	2.125
-1	-0.295	-0.998	12	0.403	1.365
0	-0.330	-1.116	13	0.114	0.385
1	-0.204	-0.689	14	-0.336	-1.136
2	-0.018	-0.060	15	-0.094	-0.318
3	-0.137	-0.465	16	0.365	1.237
4	-0.516*	-1.748	17	-0.180	-0.609
5	0.248	0.841	18	0.109	0.368
6	-0.424	-1.436	19	-0.467	-1.581
7	-0.447	-1.514	20	-0.307	-1.041

$**: p < 5\%, *: p < 10\%$

図 3 と表 2 から全サンプルを対象とした平均超過リターンは-0.516%～1.098%の範囲で上下に変動していることが見てとれる。続いて、平均超過リターンの検定統計量（表 2）を確認したところ、全サンプルではイベント 3 日前、イベント 4 日後・9 日後（3 日間）となり、統計的に有意となったイベント 3 日前とイベント 9 日後における平均超過リターンの符号はプラス、イベント 4 日後のその符号はマイナスとなっていることがわかる。なお、ここから平均超過リターンの明確な傾向を読み取ることはできなかった。

次に、図 4 を見てわかるように、全サンプルの累積平均超過リターンはイベント日から 8 日後あたりまでいずれもマイナスの値をとっており、マイナスの傾向に陥っていることが見てとれる。そこで、この動きを統計的に確認するために表 3 を確認したところ、イベント 3 日前と イベント 8 日後における累積平均超過リターンの符号のみがマイナスになっていることがわかった。ここからも、累積平均超過リターンの明確な傾向を読み取ることはできなかった。

図 4：累積平均超過リターンの推移 I

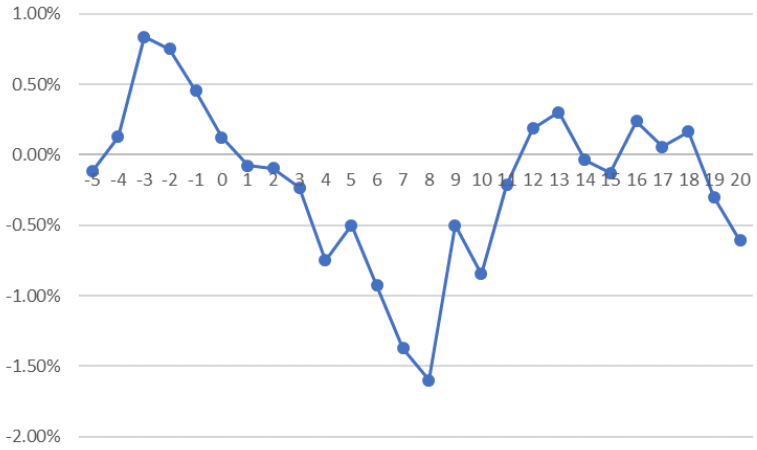


表 3：累積平均超過リターン I

	全サンプル	t 値		全サンプル	t 値
-5	-0.116	-0.394	8	-1.598*	-1.446
-4	0.128	0.308	9	-0.500	-0.437
-3	0.834*	1.630	10	-0.844	-0.714
-2	0.749	1.268	11	-0.216	-0.177
-1	0.455	0.688	12	0.187	0.149
0	0.125	0.173	13	0.301	0.234
1	-0.079	-0.101	14	-0.035	-0.026
2	-0.096	-0.115	15	-0.129	-0.095
3	-0.234	-0.264	16	0.237	0.171
4	-0.750	-0.803	17	0.057	0.040
5	-0.502	-0.512	18	0.166	0.114
6	-0.926	-0.905	19	-0.301	-0.204
7	-1.373	-1.289	20	-0.609	-0.404

$*: p < 10\%$

4.2　委託元企業・委託先企業

図 5 にはイベント日の 5 日前からの平均超過リターン AAR[-5, t]を時系列的にプロットしたもので、サンプルを委託元企業（17 社）と委託先企業（20 社）に分けたものを示している。また、表 4 は平均超過リターンの検定統計量をまとめたものである。

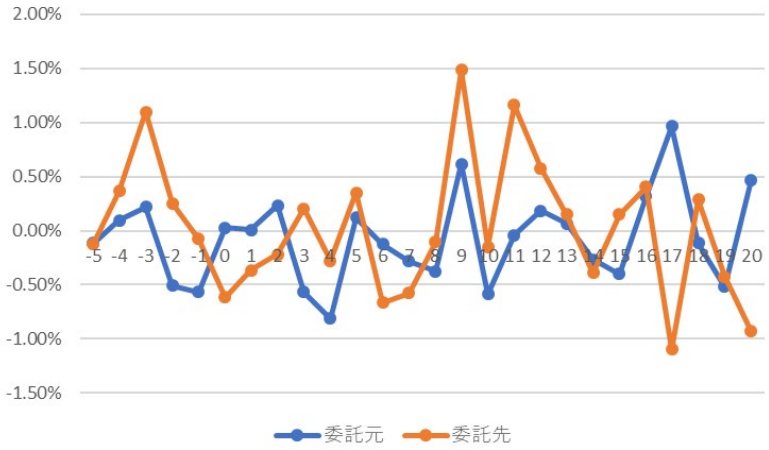


図 5：平均超過リターンの推移 II

表 4：平均超過リターン II

	委託元	t 値	委託先	t 値
-5	-0.113	-0.266	-0.119	-0.252
-4	0.094	0.221	0.366	0.775
-3	0.218	0.513	1.096**	2.322
-2	-0.508	-1.198	0.254	0.538
-1	-0.569	-1.341	-0.076	-0.160
0	0.029	0.069	-0.617	-1.307
1	0.008	0.018	-0.365	-0.772
2	0.233	0.550	-0.218	-0.463
3	-0.566	-1.335	0.206	0.436
4	-0.814*	-1.919	-0.278	-0.590
5	0.119	0.280	0.352	0.746
6	-0.123	-0.290	-0.665	-1.410
7	-0.284	-0.669	-0.578	-1.225
8	-0.373	-0.880	-0.106	-0.225
9	0.616	1.452	1.483**	3.144
10	-0.588	-1.386	-0.148	-0.314
11	-0.042	-0.100	1.164**	2.466
12	0.184	0.434	0.578	1.225
13	0.065	0.154	0.152	0.323
14	-0.268	-0.631	-0.390	-0.827
15	-0.398	-0.939	0.150	0.317
16	0.315	0.743	0.406	0.860
17	0.964**	2.273	-1.095**	-2.320
18	-0.115	-0.270	0.287	0.609
19	-0.519	-1.225	-0.425	-0.901
20	0.469	1.106	-0.929*	-1.968

$**: p < 5\%, *: p < 10\%$

図 5 と表 4 から，委託元企業グループと委託先企業グループに分けて見てみると、前者は-0.815%～0.964%の範囲、後者は-1.095%～1.483%の範囲で変動しており、後者の振れ幅が若干大きいことがわかる。続いて、平均超過リターンの検定統計量（表 4）を確認したところ、委託元企業グループではイベント 4 日前、イベント 17 日後（2 日間)、委託先企業グループではイベント日 3 日前、イベント 9 日後・11 日後・17 日後・20 日後（5 日間）となり、統計的に有意となった平均超過リターンの符号の大半はプラスとなっていることがわかる。しかしながら、ここから平均超過リターンの明確な傾向を読み取ることはできなかった。

続いて、図 6 にイベント日の 5 日前からの累積平均超過リターン CAAR[-5, t]を時系列的に委託元企業と委託先企業に分けてプロットしたものを示している。また、表 7 は累積平均超過リターンの検定統計量をまとめたものである。

図 6 を見ると、委託元企業グループと委託先企業グループの累積平均超過リターンの推移は異なることがわかる。イベント後ともに 8 日後あたりまでともに低下し続けるが、その後、委託先企業グループの累積平均超過リターンはプラスに転じる。一方で、委託元企業グループの累積平均超過リターンは引き続き低下傾向にある。この動きを統計的に確認するために、表 5 を確認したところ、委託先企業グループの累積平均超過リターンは概ねイベント 4 日後から 16 日後にかけて、マイナスの値をとり、それらは統計的に有意なものとなっている。他方、委託先企業グループに関しては、イベント 3 日前から 1 日前にかけてプラスの値をとっている（統計的に有意なものとなっている）が、それ以降は統計的に有意となっていない。図 6 ではイベント日以降、概ねプラスとなっているが、統計的に見るとこれらはゼロと判断できる。これらの結果から、委託元企業グループの累積平均超過リターンはイベント 4 日後（約 1 週間後）以降、ほぼ明確にマイナスの傾向に陥っていることが見てとれる。委託先企業よりも委託元企業にサプライチェーン上のインシデント発生に関するイベントが影響を与えることがわかる。

図 6：累積平均超過リターンの推移 II

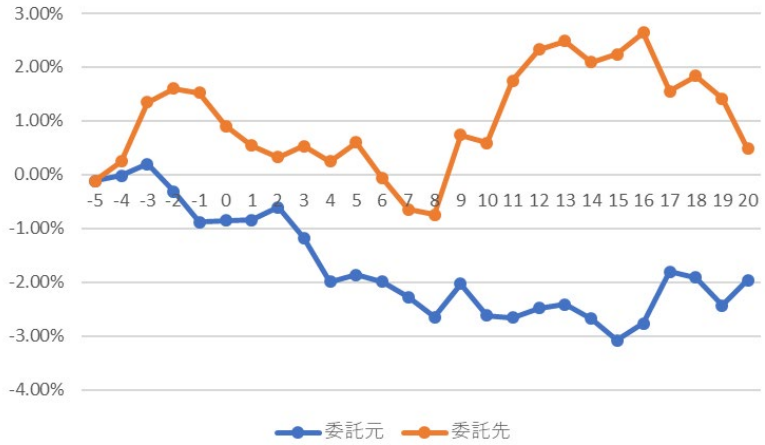


表 5：累積平均超過リターン II

	委託元	t 値	委託先	t 値
-5	-0.113	-0.266	-0.119	-0.252
-4	-0.019	-0.032	0.247	0.370
-3	0.199	0.270	1.343*	1.643
-2	-0.310	-0.365	1.596*	1.692
-1	-0.878	-0.926	1.521*	1.441
0	-0.849	-0.817	0.904	0.782
1	-0.842	-0.750	0.540	0.432
2	-0.608	-0.507	0.321	0.241
3	-1.174	-0.923	0.527	0.372
4	-1.988*	-1.482	0.249	0.167
5	-1.869	-1.329	0.601	0.384
6	-1.992*	-1.356	-0.065	-0.039
7	-2.276*	-1.489	-0.643	-0.378
8	-2.649*	-1.670	-0.749	-0.424
9	-2.033	-1.238	0.735	0.402
10	-2.621*	-1.545	0.586	0.311
11	-2.663*	-1.523	1.750	0.900
12	-2.479*	-1.378	2.328	1.163
13	-2.414*	-1.306	2.481	1.206
14	-2.681*	-1.414	2.091	0.991
15	-3.080*	-1.585	2.240	1.036
16	-2.764*	-1.390	2.646	1.195
17	-1.801	-0.885	1.551	0.685
18	-1.915	-0.922	1.838	0.795
19	-2.435	-1.148	1.413	0.599
20	-1.965	-0.909	0.485	0.201

$*: p < 10\%$

4.3 原因（不正アクセス）

図 7 には、サンプルを原因が不正アクセスであった企業（14 社）とそれ以外であった企業（23 社）に分けて、イベント日の 5 日前からの平均超過リターン AAR[-5, t]を時系列的にプロットしたものを示している。また、表 6 は平均超過リターンの検定統計量をまとめたものである。

図 7：平均超過リターンの推移 III

表 6：平均超過リターン III

	不正アクセス	t 値	その他インシデント	t 値
-5	-0.424	-1.160	0.071	0.168
-4	-4E-06	0.000	0.383	0.906
-3	0.140	0.382	1.025*	2.426
-2	-0.367	-1.004	0.075	0.177
-1	-0.710*	-1.940	-0.060	-0.142
0	-0.652*	-1.782	-0.147	-0.349
1	-0.365	-0.998	-0.105	-0.249
2	0.428	1.169	-0.269	-0.637
3	0.007	0.019	-0.219	-0.518
4	-0.569	-1.555	-0.487	-1.151
5	0.363	0.993	0.184	0.434
6	-0.867**	-2.371	-0.174	-0.411
7	-0.514	-1.404	-0.410	-0.969
8	-0.283	-0.773	-0.192	-0.455
9	0.888**	2.427	1.216**	2.878
10	-0.306	-0.836	-0.365	-0.863
11	0.928**	2.537	0.458	1.083
12	-0.092	-0.253	0.683	1.616*
13	-0.106	-0.289	0.238	0.563
14	-0.711*	-1.943	-0.124	-0.293
15	-0.331	-0.905	0.040	0.095
16	0.937**	2.562	0.042	0.100
17	0.072	0.197	-0.322	-0.762
18	-0.126	-0.344	0.241	0.571
19	-0.489	-1.335	-0.455	-1.076
20	0.161	0.440	-0.572	-1.353

$**: p < 5\%, *: p < 10\%$

原因が不正アクセスであった企業グループの平均超過リターンは-0.867%～0.937%の範囲、それ以外の企業グループのそれは-0.572%～1.216%の範囲で変動しており、前者の振れ幅が若干大きいことがわかる。また、平均超過リターンの検定統計量（表 6）を確認したところ、原因が不正アクセスであった企業グループではイベント 1 日前、イベント日、イベント 6 日後・9 日後・11 日後・14 日後・16 日後、それ以外の企業グループではイベント 3 日前、イベント 9 日後となった。この結果についても特に、平均超過リターンの明確な傾向を読み取ることはできなかった。

続いて、図 8 に、サンプルを原因が不正アクセスであった企業とそれ以外であった企業に分けて、イベント日の 5 日前からの累積平均超過リターン CAAR[-5, t]を時系列的にプロットしたものを示している。また、表 7 は累積平均超過リターンの検定統計量をまとめたものである。

図 8 を見てわかるように、不正アクセスについてはイベント 5 日前から累積平均超過リターンの値はマイナスとなり、それは 20 日後まで続いている。一方で、その他のインシデントの場合はイベント 7 日後･8 日後のみ累積平均超過リターンの値はマイナスとなっているが、それ以降は非負に転じているように見てとれる。この動きを統計的に確認するために表 7 を確認したところ、原因が不正アクセスであった企業グループの累積平均超過リターンはイベント 1 日前から 20 日後まで（継続的に）統計的に有意にマイナスの値をとっていることがわかる。一方で、原因がそれ以外の企業のグループの累積平均超過リターンはイベント

3 日前から 1 日前まで統計的に有意にプラスの値をとっているが、それ以外の期間は統計的に有意となっていないことがわかった。つまり、原因が不正アクセスかどうかによって企業に与える影響が異なり、とりわけ原因が不正アクセスの場合、その影響は継続的に続くことがわかる。

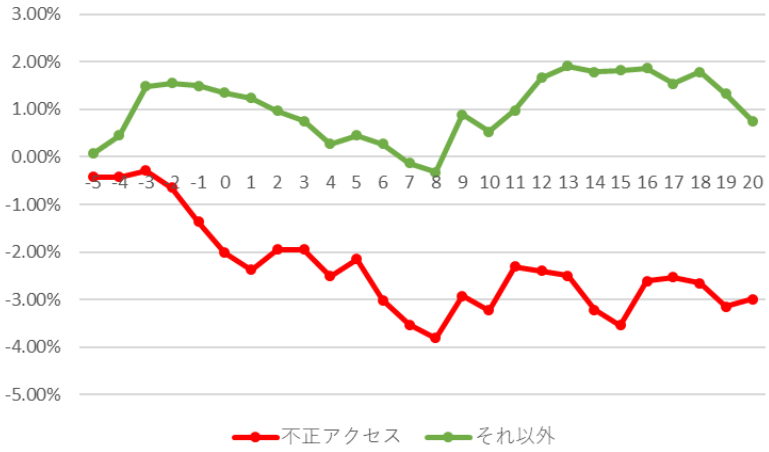


図 8：累積平均超過リターンの推移 III

表 7：累積平均超過リターン III

	不正アクセス	t 値	その他インシデント	t 値
-5	-0.424	-1.160	0.071	0.168
-4	-0.424	-0.820	0.454	0.760
-3	-0.285	-0.449	1.480*	2.021
-2	-0.652	-0.891	1.555*	1.839
-1	-1.362*	-1.665	1.495*	1.581
0	-2.014**	-2.247	1.347	1.301
1	-2.379**	-2.458	1.242	1.110
2	-1.951**	-1.886	0.972	0.813
3	-1.944*	-1.771	0.754	0.594
4	-2.513**	-2.172	0.267	0.200
5	-2.150**	-1.772	0.451	0.321
6	-3.017**	-2.381	0.277	0.189
7	-3.531***	-2.677	-0.133	-0.087
8	-3.814***	-2.786	-0.325	-0.206
9	-2.926**	-2.065	0.891	0.544
10	-3.232**	-2.208	0.527	0.311
11	-2.303*	-1.527	0.984	0.565
12	-2.396*	-1.543	1.668	0.930
13	-2.502*	-1.569	1.905	1.034
14	-3.212**	-1.963	1.782	0.943
15	-3.543**	-2.113	1.822	0.940
16	-2.606*	-1.519	1.864	0.940
17	-2.534*	-1.444	1.542	0.760
18	-2.660*	-1.484	1.783	0.861
19	-3.148**	-1.721	1.328	0.628
20	-2.987*	-1.601	0.756	0.351

$***: 1\%, **: p < 5\%, *: p < 10\%$

4.4　個人情報の漏洩件数

図 9 は、5000 件を超える個人情報の漏洩が発生した企業（17 社）とそれ以外の企業（20 社）に分けて、イベント日の 5 日前からの平均超過リターン AAR[-5, t]を時系列的にプロットしたものを示している。また、表 8 は平均超過リターンの検定統計量をまとめたものである。

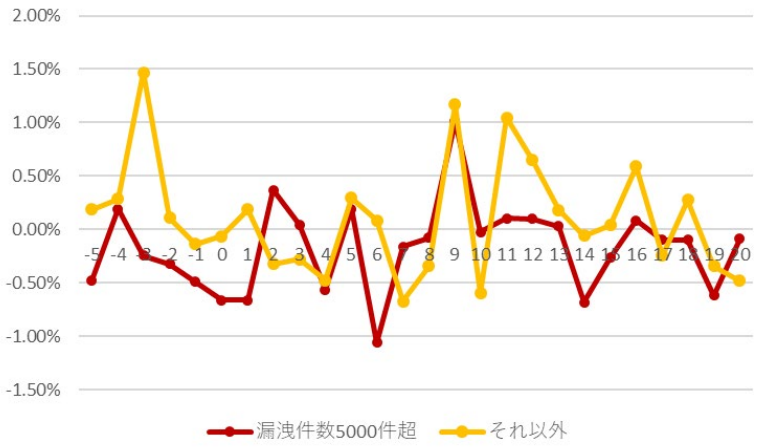


図 9：平均超過リターンの推移 IV

表 8：平均超過リターン IV

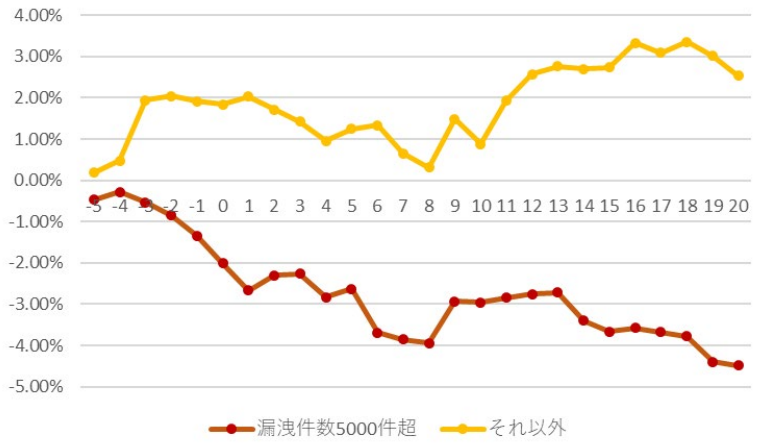
	漏洩件数 5000 件超	t 値	それ以外	t 値
-5	-0.475	-1.201	0.188	0.425
-4	0.193	0.489	0.286	0.646
-3	-0.246	-0.623	1.467**	3.313
-2	-0.325	-0.821	0.107	0.242
-1	-0.491	-1.242	-0.138	-0.312
0	-0.662*	-1.675	-0.064	-0.144
1	-0.665*	-1.682	0.188	0.426
2	0.366	0.925	-0.324	-0.733
3	0.042	0.107	-0.281	-0.634
4	-0.564	-1.428	-0.478	-1.080
5	0.194	0.490	0.292	0.660
6	-1.061**	-2.685	0.085	0.193
7	-0.164	-0.415	-0.674	-1.522
8	-0.079	-0.201	-0.341	-0.771
9	1.011**	2.557	1.168**	2.637
10	-0.024	-0.060	-0.599	-1.353
11	0.104	0.263	1.047**	2.364
12	0.096	0.244	0.648	1.465
13	0.032	0.080	0.179	0.405
14	-0.681*	-1.724	-0.059	-0.134
15	-0.263	-0.665	0.041	0.093
16	0.084	0.212	0.591	1.335
17	-0.100	-0.253	-0.244	-0.551
18	-0.099	-0.249	0.274	0.620
19	-0.621	-1.570	-0.344	-0.777
20	-0.089	-0.225	-0.482	-1.089

$***: p < 1\%, **: p < 5\%, *: p < 10\%$

5000 件を超える情報漏洩が発生した企業グループの平均超過リターンは-1.061%～1.011%の範囲、それ以外の企業グループのそれは-0.674%～1.467%の範囲で変動しており、前者の振れ幅はほぼ同じであるが、後者の方が前者よりも上振れしていることがわかる。また、平均超過リターンの検定統計量（表 8）を確認したところ、イベント日、イベント 1 日後・6 日後・9 日後・14 日後、それ以外の企業グループではイベント 3 日前、イベント 9 日後・10 日後となった。この結果についても特に、平均超過リターンの明確な傾向を読み取ることはできなかった。

続いて、図 10 に、に分けて、イベント日の 5 日前からの累積平均超過リターン CAAR[-5, t]を時系列的にプロットしたものを示している。また、表 9 は累積平均超過リターンの検定統計量をまとめたものである。

図 10 を見てわかるように、5000 件を超える個人情報の漏洩が発生した企業グループの累積平均超過リターンは全期間にわたってマイナスの値をとり続けている一方で、それ以外の企業グループの累積平均超過リターンは全期間にわたってプラスの値をとり続けており、両者の推移は大きくことがわかる。この動きを統計的に確認するために表 7 を確認したところ、5000 件を超える個人情報の漏洩が発生した企業グループの累積平均超過リターンはイベント 1 日前から 20 日後まで（継続的に）統計的に有意にマイナスの値をとっていることがわかる。一方で、それ以外の企業のグループの累積平均超過リターンはイベント 3 に前からイベント 2 日後、イベント 12 日後からイベント 19 日後まで断続的ではあるが、統計的に有意にプラスの値をとっていることがわかった。このことから、漏洩した個人情報の件数によって企業の株価に与える影響が異なり、5000 件を超える個人情報の漏洩が発生した場合、その影響は継続的に続くことがわかる。



図表 16：累積平均超過リターンの推移 IV

図表 17：累積平均超過リターン IV

	漏洩件数 5000 件超	t 値	それ以外	t 値
-5	-0.475	-1.201	0.188	0.425
-4	-0.281	-0.503	0.474	0.758
-3	-0.528	-0.771	1.941**	2.532
-2	-0.852	-1.078	2.048**	2.313
-1	-1.343*	-1.519	1.910*	1.930
0	-2.005**	-2.071	1.846*	1.703
1	-2.669**	-2.553	2.035*	1.737
2	-2.304**	-2.061	1.711*	1.366
3	-2.262**	-1.907	1.430	1.076
4	-2.826**	-2.261	0.952	0.680
5	-2.632**	-2.008	1.244	0.847
6	-3.694***	-2.698	1.329	0.867
7	-3.858***	-2.707	0.655	0.411
8	-3.937***	-2.662	0.314	0.190
9	-2.926**	-1.912	1.482	0.864
10	-2.950**	-1.866	0.882	0.498
11	-2.846**	-1.746	1.929	1.057
12	-2.749*	-1.640	2.578*	1.372
13	-2.718*	-1.578	2.757*	1.429
14	-3.399**	-1.923	2.698*	1.363
15	-3.662**	-2.022	2.739*	1.350
16	-3.578**	-1.930	3.330*	1.604
17	-3.678**	-1.941	3.086*	1.453
18	-3.777**	-1.951	3.361*	1.549
19	-4.397**	-2.225	3.016*	1.363
20	-4.486**	-2.226	2.534	1.123

$***: p < 1\%, **: p < 5\%, *: p < 10\%$

4.5 考察

前節にて、(1) 委託元企業と委託先企業と分けた分析、(2) 原因が不正アクセスの場合とそれ以外の場合と分けた分析, (3) 5000 件を超える個人情報の漏洩が発生した場合とそれ以外の場合と分けた分析、を行った。その結果、興味深いことがわかった。

(1)について、多くの事例において委託先や再委託先企業でインシデントが発生しているにも関わらず、委託先企業よりも委託元企業に負の影響が与えられていることがわかった。一方で、委託先企業は統計的に見ると、累積平均超過リターンはゼロとなっており、インシデントが発生したとしてもその影響はそれほど大きくないと判断することができる。この理由としては、委託先企業が連結子会社であることが多いことに加えて、IT システム・サービスを専門とするがゆえにインシデント発生直後に早急な技術的対応を施したことにより、株価に対して大きな影響を受けなかったと考えられる。

(2)について、原因が不正アクセスの場合、累積平均超過リターンはインシデント発生後継続して負の値をとり続けている、つまり不正アクセスが発生した場合は継続的な企業価値の低下につながることがわかった。他方、不正アクセス以外のインシデント発生の場合, 累積平均超過リターンはゼロとなっており、これらのインシデントが発生したとしてもその影響はそれほど大きくないと判断することができる。

(1)と(2)については、竹村他 (2020)で試みられた 5 ファクター・モデルの検証結果と整

合的な結果となっている。

(3)について、5000 件を超える個人情報の漏洩が発生した場合、累積平均超過リターンはインシデント発生後継続して負の値をとり続けている、つまり不正アクセスが発生した場合は継続的な企業価値の低下につながることがわかった。他方、それ以外の場合（5000 件以下の個人情報の漏洩や個人情報漏洩事例以外のもの）には、累積平均超過リターンはゼロからプラスに転じていることが確認された。このことから両者において、インシデント公表後の株価の動向は大きく異なることがわかる。

5. おわりに

本研究では、IT サプライチェーン上でインシデントが発生したとき、そのことがサプライチェーン上の企業の株価のリターンに与える影響について、イベントスタディの手法を用いて、公開情報から収集した IT サプライチェーン上で発生した国内の主なインシデント事例をもとに分析結を試みた。その結果、その結果、インシデントの発生は委託先企業よりも委託元企業の企業価値を低下させてしまうことや、原因が不正アクセスの場合や 5000 件を超える個人情報の漏洩が発生した場合は継続的に企業価値が低下し続けることなどを明らかにした。

2020 年 4 月 1 日から施行されることが決定している民法の一部を改正する法律（平成 29 年法律第 44 号）では、従来の瑕疵担保責任の考え方が変わり、また請求できる期間についても長くなることから、各企業の契約書雛形の見直しの要否を検討する契機となると考えられる。しかしながら、小山他（2019b, 2020)によれば、これらの見直しが多くの企業において行われているとは 2019 年 8 月時点では言いがたい。とりわけ、委託先企業は見直しが進んでおらず，民法改正に関する情報も十分届いていない恐れがあることが指摘されている。すでに触れたように、この民法の改正を契機として委託元企業と委託先行の間の（深刻な）理解の不一致（認識の齟齬）を解消することで、IT サプライチェーン上でたとえインシデントが発生したとしても，それに対して早急な対応ができ、IT サプライチェーン上の影響を小さくできることも予想できる。

最後に、本研究の課題と今後の展望について述べる。本研究では、情報処理推進機構(2018)で取り上げられた事例をもとに分析を試みたが、これらの事例は意図的に抽出されたものであるため（脚注 5 参照)、発生したインシデント全体の傾向とは言えない。そのため、インシデント全体の傾向を捉えるために、より多くの事例の収集ならびそれらの分析を行う必要があり、これを今後の課題としたい。

参考文献

1. Arcuri, M.C., Brogi, M., Gino Gandolfi, G. (2017) How Does Cyber Crime Affect Firms? The Effect of Information Security Breaches on Stock Returns, The Proceedings of the First Italian Conference on Cybersecurity (ITASEC17), 175-193

2. Brown, S., Warner, J. (1985) Using Daily Stock Returns: The Case of Event Studies, Journal of Financial Economics, 14, 3-31
3. Campbell, J., Lo, A.W., MacKeinlay, A.C. (1997) The Econometrics of Finance, Princeton University Press,
4. Fama, E.F., French, K.R. (1993) Common Risk Factors in the Returns on Stocks and Bonds, Journal of Financial Economics, 33(1), 3-56
5. Fama, E.F., French, K.R. (2015) A Five-Factor Asset Pricing Model, Journal of Financial Economics, 116, 1-22
6. Ishiguro, M., Tanaka, H., Matsuura, K., Murase, I. (2006) The Effect of Information Security Incidents on Corporate Values in the Japanese Stock Market, Workshop on Economics of Information Security (WEIS2006), (http://citeseerx.ist.psu.edu/viewdoc/download$?$doi=10.1.1.212.4556$$rep=rep1$$type=pdf)
7. Kannan, K., Rees J., Sridhar, S. (2007) Market Reactions to Information Security Breach Announcements: An Empirical Analysis, International Journal of Electronic Commerce, 12(1), 69-91
8. Konchitchki, Y., O'Leary, D.E. (2011) Event Study Methodologies in Information Systems Research, International Journal of Accounting Information Systems, 12, 99--115
9. Malliouris, D.D., Simpson, A.C. (2019) The Stock Market Impact of Information Security Investments: The Case of Security Standards, Workshop on Economics of Information Security (WEIS2019), 2019 (https://weis2019.econinfosec.org/wp-content /uploads/sites/6/2019/05/WEIS_2019_paper_22.pdf)
10. 河路武志（2006）「個人情報漏えい事件に対する株式市場の反応」管理会計学, 15(1), 35-56
11. 金融データソリューションズ（2016)「日本上場株式 FF 関連データ: FF 3 ファクター市場拡張版モデル」(https://fdsol.co.jp/doc/ FF3 ファクターデータ_市場拡張版.pdf)
12. 久保田敬一・竹原均（2007）「Fama-French ファクターモデルの有効性の再検証」現代ファイナンス, 22, 3-23
13. 小山明美・小川隆一・竹村敏彦（2019a)「IT サプライチェーン上の情報セキュリティリスク認識に関する分析」2019 年暗号とセキュリティシンポジウム（SCIS2019）予稿集, 4D1-5
14. 小山明美・森淳子・小川隆一・竹村敏彦（2019b)「企業の民法改正対応への取組みに関する一考察」2019-EIP-86, 10, 1- 6
15. 小山明美・森淳子・小川隆一・竹村敏彦（200)「企業の民法改正対応への取組みに関する一考察（2)」情報処理学会第 82 回全国大会予稿集, 2G-01, 2020 年
16. 情報処理推進機構（2018)「IT サプライチェーンの業務委託におけるセキュリティイ

ンシデント及びマネジメントに関する調査報告書」(https://www.ipa.go.jp /files/000065162.pdf)
17. 竹村敏彦・小山明美・小川隆一（2020)「IT サプライチェーン上のセキュリティインシデントが企業価値に与えるインパクト～イベントスタディによる検証～」2020 年暗号とセキュリティシンポジウム（SCIS2020）予稿集, 2D3-3
18. 田中秀幸・中野邦彦（2016)「サイバー・セキュリティ・インシデントが企業価値に与える影響」東京大学大学院情報学環紀要（情報学研究）, 91, 1-11
19. 中村政美（2016)「リスク開示の有無が株式市場の評価に与える影響～情報セキュリティ・リスク発生を対象にしたイベント・スタディを通じて」中央大学大学院研究年報（戦略経営研究科篇）, 4, 1-23
20. 廣松毅（2011)「情報セキュリティ事故が企業価値に与える影響の分析～イベント・スタディ法を用いたリスク評価の試み」情報セキュリティ総合科学, 3, 91-106
21. 森淳子・小山明美・小川隆一・竹村敏彦（2019)「IT サプライチェーンの責任範囲の実態から見た対策強化のための提案」CSS2019 Proceedings, 1B3-5
22. 森淳子・小山明美・小川隆一・竹村敏彦（2020)「IT サプライチェーンのセキュリティ要求事項に関する分析～責任範囲の取り決めに対する考え方～」2020 年暗号とセキュリティシンポジウム（SCIS2020）予稿集, 2D3-4