研究報告

サイバー攻撃回避行動の経済モデルと実証分析
――情報セキュリティ事故被害規模と頻度から見る――

学習院大学経済学部　辰　巳　憲　一

1．はじめに

情報セキュリティ事故が頻繁に報道され、我々は様々なメディアを通じてよく目にし意識するようになった。それらのデータも収集され公表されるようになっている。辰巳［2014b］はそれらを展望し解釈している。本研究は、その被害規模と頻度の関係を考察し実証分析する。情報セキュリティ事故の生起のメカニズム、事故・災害被害の対象となる価値の大きさと事故や災害に対応する行動が関係することを示し、その解明に迫る。大規模事故・災害が生起するメカニズムを考慮すると、事故・災害に対応する経済行動が影響している証拠をあることを示す。

サイバー攻撃によって、組織は利益を失う、損失を被る、などの被害を受ける。それを防ぐために、お金を出して防御する、阻止する、のが極めて合理的な行動なのである。このような行動があって、我々が観察するイベントが存在しているのである。なお、このような方向への理論分析は別稿を予定している。

情報セキュリティ事故被害規模と頻度の関係を実証分析する本研究は、また、情報セキュリティ本来の問題とも強く関係している。情報セキュリティ一般については、様々な局面を持つが、辰巳［2011b］、辰巳［2011c］、辰巳［2012a］、辰巳［2012b］、などを参照。辰巳［2011a］と辰巳［2014a］はプライバシーがらみの問題を展開している。

さらには、Tatsumi and Goto［2010］、辰巳･後藤［2010］と Goto and Tatsumi［2012］はリアル・オプション理論を用いた情報セキュリティ投資行動の理論的分析である。そして、辰巳［2014b］は主として先行調査の展望であるが、様々な考察を加えていて、本稿の姉妹版である。

2. 事故・被害の発生確率計測の先行研究

企業内における事故・被害の発生確率を計測した先行研究は古くからある。その内いくつかは良く知られており、イベントの回避行動という観点とは共通部分が多く、それらの紹介から入るのが適切なように思われる。

2. 1　企業内の事故発生

2. 1. 1　ハインリッヒの法則

嚆矢となるのは、米国の損害保険会社で技術・調査部の副部長をしていたハーバート・ウィリアム・ハインリッヒ (Heinrich, Herbert William)（1886 あるいは 1881 年− 1962 年）が、労働災害の発

生確率を分析した結果を 1929 年 11 月に論文として発表した 90 年も前の研究に遡る。

ハインリッヒは 5000 件以上の労働災害を調べ、重傷以上の災害（major injury）が 1 件起きる背景には、軽傷を伴う災害（minor injuries）が 29 件起きており、さらには危うく惨事になるような「ヒヤリ」や「ハッと」するような出来事（no-injury accidents）が 300 件あるという「1：29：300 の法則」を見い出した。著書 Heinrich［1950］の p.24 には、有名なトライアングルの図がある。図表 1 には、以降で紹介する様々な法則と比較できるような図を描いた。

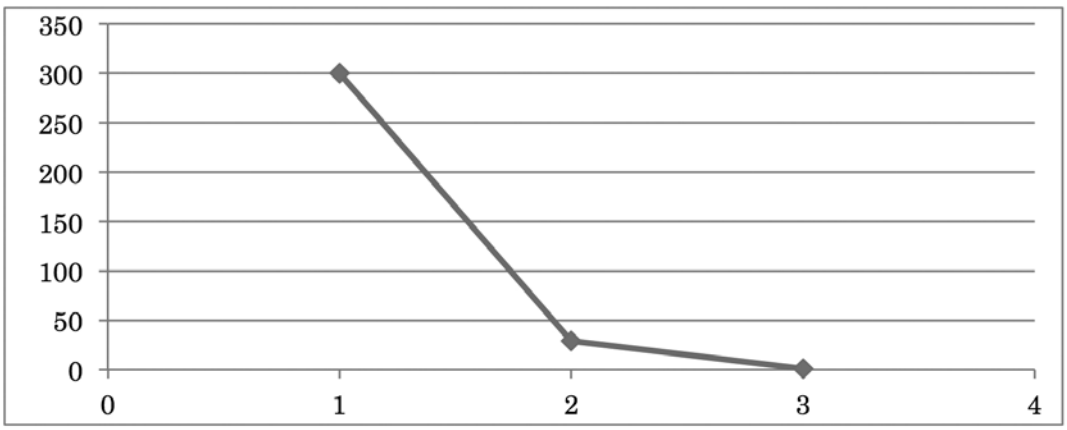
ハインリッヒは、この比率は同一人物が起こす同一種類の 330 の労働災害に適用可能である、と述べている。そして、労働災害全体の 98％は予防可能であり、予防可能な不安全な行動や状態をなくすことで重大事故のリスクを減少させることが出来ると指摘している。

この法則は、重大事故：軽度の事故：インシデントの比率と解釈され、ビジネスにおける失敗発生率、さらには企業へのクレーム発生率、などとしても利用されている。

2. 1. 2 バードの法則

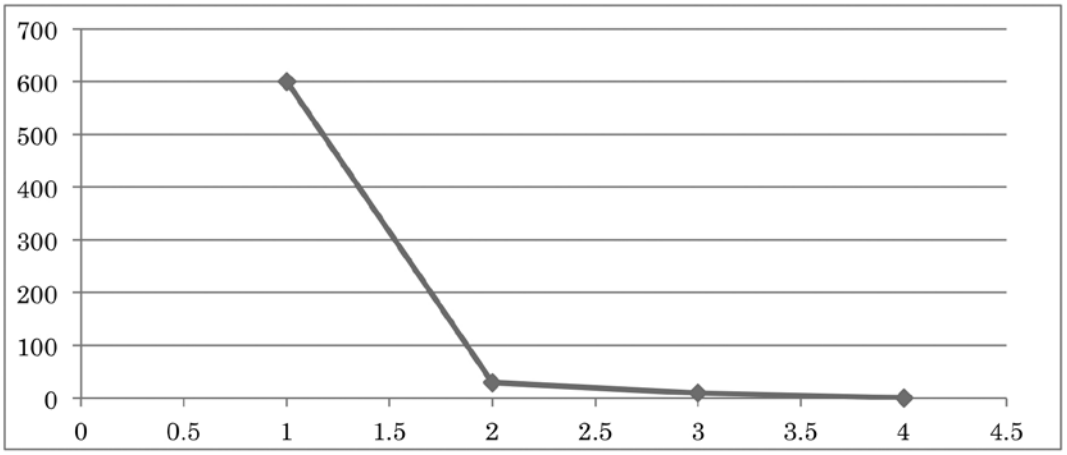
次の研究は 40 年後、保険会社の部長バード（Bird, Jr., Frank, E.）（1921 年− 2007 年）によって、なされた。1969 年に発表された彼の法則では、米国の 21 業種 297 社で働く 1,750,000 人の従業員（対象期間に累計 30 億時間働いた）に関する 1,753,498 件のデータから導き出された。ニアミス（non injury accidents）600: 物損事故（property damage accidents）30: 軽傷事故（minor injuries）10: 重大事故（serious injury） 1 、の比率が成り立つと主張する（図表 2 参照）。

図表 1　ハインリッヒの法則のイメージ



注）横軸は軽微の 1 から数字が大きくなれば重度になる事象概念、縦軸は正規化・標準化していない頻度・件数、をとっている。出典等は本文参照。

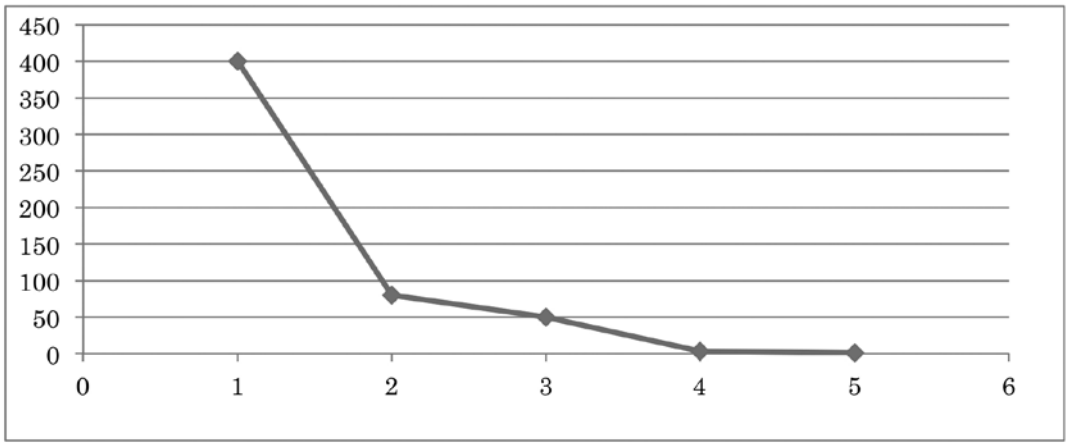
図表２　バードの法則のイメージ



注）横軸は軽微の１から数字が大きくなれば重度になる事象概念、縦軸は正規化・標準化していない頻度・件数、をとっている。出典等は本文参照。

正確には、重大事故とは致死（fatality）、身体障害（disability）に至る事故、就労中事故（労災事故、lost time injury）あるいは医療処置（medical treatment）が必要な事故を指す。ちなみに、物損事故の正確な率は、30 ではなく、30.2 である。なお、重大事故のなかの一部の比率について、95 社が報告しており、就労中事故１件につき医療処置事故 15 件が平均的に起こっていた。この重大事故１件につき､応急手当（first aid）だけで済む軽傷事故（minor injuries）が 9.8 件報告される。

図表３　タイ＝ピアソンの法則のイメージ



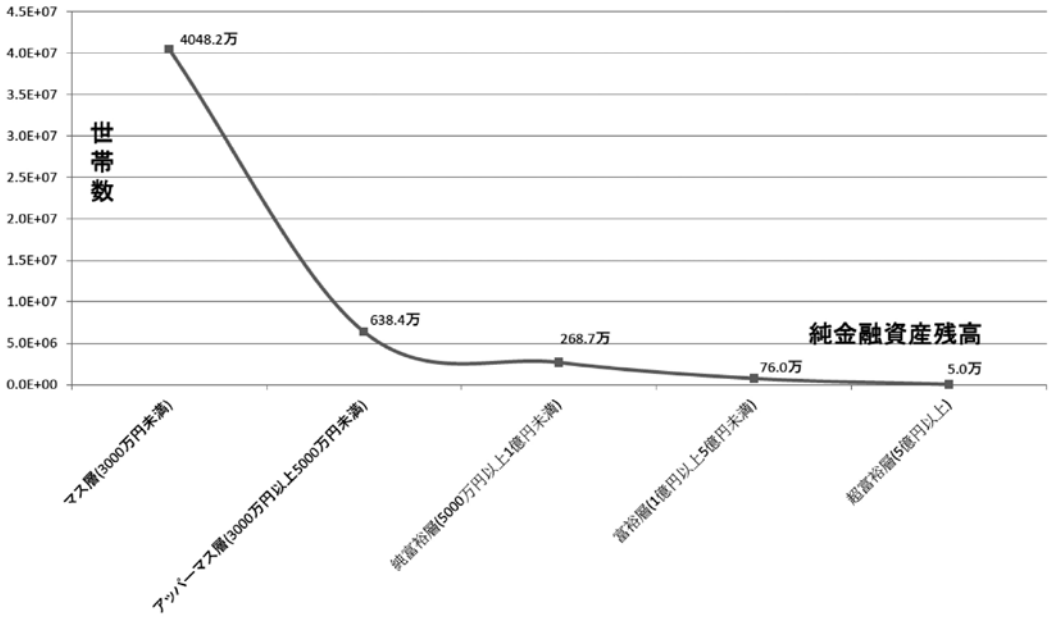
注）横軸は軽微の１から数字が大きくなれば重度になる事象概念、縦軸は正規化・標準化していない頻度・件数、をとっている。出典等は本文参照。

2. 1. 3　タイ＝ピアソンの法則

英国の保険会社のデータ約 100 万件から、1974 年、1975 年にタイ＝ピアソン（Tye および Pearson）によって導き出された結果がタイ＝ピアソンの法則であり、ニアミス 400：物損事故 80: 応急処置を施した事故 50: 軽中傷事故 3：重大事故 1、の比率が成り立つと主張される（図表 3 参照）。

以上はいずれも大規模データの研究で類似の法則ではあるが、国が違う、時期が違う、などの多様性の観点から法則の頑強性を保証する点が注目される。

図表 4　日本の純金融資産の世帯分布（2011 年）



注）純金融資産とは、資産から借金と不動産を除いた額。出所）野村総合研究所。

2. 2　事象の頻度と規模～１つの事例

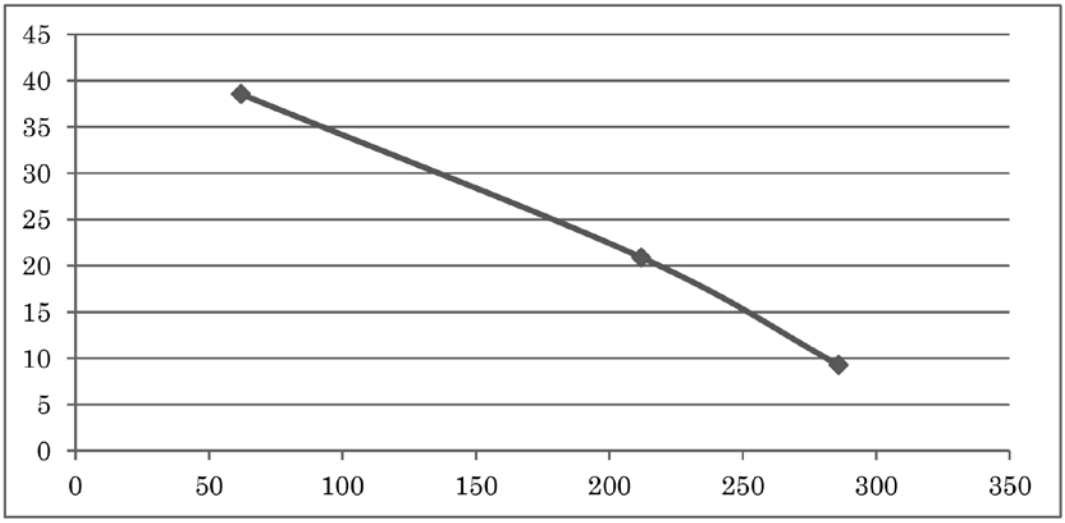
事象の頻度と規模の関係性を示す例として、日本の保有純金融資産の世帯分布（2011 年）を取り上げよう。図表 4 の横軸は、５分類した各層の「純金融資産残高」（最後は、５億円以上、５つの区分金額を目盛表示している）、縦軸は、世帯数（最後は 5.0 万、これらの数字は折れ線グラフの該当箇所に記入）である。

資産蓄積のプロセスは幾多の試練に挑むもので、成功するためには打ち勝ち続けることが条件になる。それは誰もが高い確率でなしえない。成金レースに勝ち続けるのは、十分な才能が必要である。才能だけでなく運も必要かもしれない。珍しい（度々観測しない）事象は希にしか起らない、ということである。

2. 3　自然災害の発生確率の計測結果

2014 年までの 10 年間に世界で起こった自然災害データを、国連の国際防災戦略（ISDR）が公表している。原データでは、2005 年から 2014 年の 10 年間で災害累積件数の多い国が選ばれている。そのなかから、被害総額（億ドル）上位３ヵ国（米国、中国、日本の順）を選び、横軸に１件当たり被害総額（億ドル）をとり、それに対する件数を縦軸にとり、図表５に図示した。１件当たり被害総額（億ドル）の順位は、日本、米国、中国の順に変わる。

図表５　自然災害の規模と発生件数



注）2014 年までの 10 年間に世界で起こった災害規模上位３ヵ国の一件当たり災害規模（億ドル、横軸）と件数（縦軸）。
出典）国連、国際防災戦略（ISDR）。

日本の高順位は東日本大震災が影響している。米国、中国も、それぞれハリケーンカトリーナ、四川地震が影響している。地震以外の災害の多くは洪水など気候変動に関連したものだったという。大災害の頻度は、自然災害でも、規模が大きくなる程低くなっていることがわかる。

小さい地震ほど発生数が多く、大きな地震ほど少ないという地震の規模と件数に見られる現象は、グーテンベルグ・リヒターの法則としても知られている。横軸を地震の規模の対数、縦軸をその規模を持つ地震の頻度の対数とすると、観測値はきれいな右下がりの直線上に乗る。大規模現象の頻度はやはり低い、のである。

2. 4　事故・被害の発生確率の調査・計測結果

以上で図示した関係性は事故のピラミッドやトライアングルとも呼ばれる。上記の法則などを発

展させたものが保険会社の「保険料率表」の根拠になっている。これらの比率は、主に大企業に適用され、業種や国や時期・時代によっても多少変わると考えられるが、共通要素が多い。

その原因、つまり事故や業務トラブルの元になるのはほとんどがヒューマンエラーであるが、事故・イベントには法則性がある、ように見える。その理由は、被害・影響を小さくしたい経済行動なのである。無限に対策費を出せば被害は小さく出来るが、利益が圧縮されるので、企業などの組織としては大きな経済問題になる。それぞれが最適と考えるレベルで阻止・回避行動を採っているようである。

2. 4. 1　分析

情報セキュリティや自然災害のリスクの大きさは、一般に、ハザード、エクスポージャー（曝露（ばくろ）と呼ぶ文献もある)、脆弱性の３つの要素の組み合わせによって決まる、とみられている。

ハザードは被害・災害を発生させる現象で、外部からもたらされる攻撃や自然の力の強さ・大きさである。エクスポージャーはハザードの影響を受ける被災組織、会社、個人、の価値の大きさである。自然災害の場合には地域に存在する人や資産などの該当のものであり、砂漠や原野が自然災害から受ける影響は小さい。脆弱性は、ハザードに対する人や資産の弱さであり、対策をどれ位とっているかが影響する。本稿が注目するのは、この点である。

（1）情報セキュリティの場合

情報セキュリティの場合、これら３つの要素のうちどれがどれ位影響するかは、業種や組織によって違うように思われる。同様に、システムトラブルと重要情報の漏洩は別の要因が影響している。

ハザードは、ランダムにやってくる、という考えが過去強かったように思われる。最近は、経済的要因を狙いにしてサイバー攻撃がなされるようになっている。

システムはビジネス社会の要求と技術進歩で益々拡大し複雑化している。当然、トラブルは増える。情報社会の進展で、情報の価値は上昇して、重要情報が増え、その結果重要情報の漏洩が増えた。それゆえ、最近はエクスポージャーにも関心が向くようになった。

脆弱性は、日本では漸く認識が高まり、対策はこれからであるようである。

（2）自然災害の場合

情報セキュリティでは「人対人」あるいは「人・マシーン対人・マシーン」の戦いである様相が、自然災害では「人対災害」あるいは「人・マシーン対災害」の戦いになる。競合相手を倒し、その失敗や脱落を狙うという要因が極めて小さくなり、人は助け合い、己を律し、やってくる災害を乗り越える試みに挑戦する、ことになる。

日本の自然災害の場合、主要な要素はハザードである、と考えられる。他方、新興国や発展途上国では、事情が違う。エクスポージャーと脆弱性が相乗的に影響している。人口の増加、経済発展に伴う都市化の進展、産業集積の拡大が進行している。これによってエクスポージャーが増える一

方で、十分な防災対策がなされないままに急速な地域開発がなされ、脆弱性が増す。このため、大規模なハザードに見舞われると、大きな被害が生じる可能性が高い。中国の自然災害の場合は、これらの要因が影響している。

2. 4. 2　本研究の意義

（1）技術者の研究で欠けている事柄

不正行為を行う者の行動を明らかにせずして、不正防止は実際上できない。不正防止を遂行する手段は無限にあり、それらを闇雲にすべて採用することはコスト的に不可能である。さらに、可能性の組み合わせは無限になり検討することさえも不可能になりつつある、からである。それゆえ、不正行為者の行動パターンがわかれば、防止手段の検討対象を限ることができ、防止方法を限ることもでき、より適切な対応ができる、のである。

不正行為者だけでなく、被害者の行動を知ることも重要である。不正行為者と被害者の行動が絡み合って事故が起きる、からである。その例として、被害者は不正になぜ気付かないのか、不正をなぜ受け入れてしまうのか、などの解明がある。

（2）技術か、ヒューマン（人間）か

技術だけでなく、ヒューマン（人間）な要素が事故・事件を引き起こしていることが注目されるようになっている。しかしながら、この２分法で物事がクリアになるとは思えない。両者の絡みがもっと重要であるように思われる。

3. 事故・被害の発生確率の実証分析

3. 1　事故・被害の発生確率調査の先行事例

被害の規模でクロスセクション分析している調査に関しては、規模の効果はあるという調査結果と必ずしも明瞭ではないという２つに分けられるようである。それらを紹介しておこう。

3. 1. 1　規模とともに大きくなるサイバー攻撃の発生確率調査

（1）規模別サイバー攻撃の発生率

日本情報システム・ユーザー協会（JUAS）が、東証１部上場企業とそれに準じる企業の計 4000 社（有効回答社数は 1030 社）の IT 部門長に調査票を郵送する形で企画・実施した 2012 年 10 月 29 日から 11 月 19 日が調査期間での「企業 IT 動向調査報告書 2013」では、攻撃を受けた割合は、1000 人以上の大企業の方が 1000 人未満の中堅・中小企業より高い。この背景には、大企業の方が標的になる情報を持っているため狙われやすいこと、不正侵入などを検知する仕組みが整備されているため攻撃を察知できること（つまり、中小企業では知らない間に侵入を受けているが、その認識がなく、報告もされない、ということであると解釈できる）、などが考えられる理由にあげられた

（2）企業規模に対する更なる考察

攻撃目標とユーザの属性の関係については、規模によって違いがあることが分かる。大規模企業が受ける外部からのデータ漏洩 / 侵害攻撃に関しては、金銭目的のものより、“意見の相違または抗議”や“遊び、好奇心、プライド”という理由による攻撃が増える傾向が指摘される（鵜沢［2012a］）。これはハクティビズム（hacktivism）という、社会的・政治的な主張の下に行うハッキング活動である。

攻撃手法についても、対象を大規模の企業・組織に限って傾向を見てみると、電子メール経由、Web/ インターネット経由の攻撃割合は高くなる（鵜沢［2012b］）。これは攻撃者が、大規模の企業・組織を真っ向から攻撃して防御を破るより、従業員にマルウェアをインストールさせるほうが簡単と考えているためだと考えられている（鵜沢［2012b］）。

3. 1. 2　規模に依存しないサイバー攻撃の発生確率調査

（1）サイバー犯罪の被害とその額の米国での Ponemon 調査～被害額分布と組織規模

サイバー犯罪の被害とその額などを企業データから体系的に調査した、筆者が知る限り、現時点までに公表された唯一のものは、Ponemon［2012b］であろう。Ponemon［2012b］は、1,000 以上の直接接続のネットワークを設けている米国における企業など 56 組織を対象に、2012 年に至る 3 ヵ年のサイバー犯罪を調査した。調査によると、3 年連続でサイバー攻撃への対策コストと発生頻度が増加していることが明らかになった。サイバー攻撃の発生件数は 3 年間で 2 倍以上に増加したという。

なお、英国、ドイツ、オーストラリア、日本については、2012 年から調査対象に加えられたが、サンプル数は更に小さい。しかも、詳細な調査はなされていない。それゆえ、ここでは米国の調査のみ紹介しよう。

56 組織の年間の平均被害額は 8.9 百万ドルで、最小は 1.4、最大は 46 百万ドル、であった。全体の 3 分の 2 に当たる 37 社は平均以下であるという偏った分布だった。ネットワークの規模と被害額は比例している。しかしながら、従業員一人当たりの被害額は逆転しており、小規模組織の方が有意に多い。

（2）規模別サイバー攻撃の発生率

2011 年にサイバー攻撃を受けた企業のうち、従業員数 250 名以下の会社は全体の 18％だったが、2,500 名以上の会社は 50％であった。ところが、2012 年に、2,500 名以上会社ではこの数字は変わらず、250 名以下会社は 31％へと跳ね上がったと、Symantec は 2013 年 4 月 16 日に発表した「Internet Security Threat Report 2013」2012 Trends, Volume 18, Published April 2013 で説明している。

「小規模企業に対する攻撃の見返りは大企業に対するそれより少ないという考えもあるが、小規模企業のサイバー犯罪に対する無防備さがそうしたマイナス面を相殺している」と推察している。

ちなみに、同時期に攻撃を受けた従業員数 251 名から 2,500 名までの組織は全体の 19%を、同じく 2,500 名以上の組織が残りの 50%を占めたという。同社はまた、2012 年は前年と比べてサイバー攻撃の総発生数が 42%増加したとも記している。

（3）サイバー犯罪と標的の企業規模

最近のサイバー犯罪者は、標的の企業規模には関心を寄せていないことが PwC Information Breaches Survey 2013 が明らかにしている。同調査によると、中小規模企業に対する不正な攻撃は 2012 年に 22%も増えたのに対し、大規模企業ではわずか５％の増加に留まった。理由としては、知的財産や企業機密の窃取による現金化傾向に加えて中小規模企業ではセキュリティに十分な予算をかけていないといったガードの甘さが犯罪者にとって好都合になっている、としている。

別の調査でも、SNS やモバイルを通した被害は、企業の規模とは無関係に起こる、という指摘もある。元来 SNS やモバイル・デバイスは、コンシューマー向けの製品やサービスであり、誰もが利用するもので、IT に十分な投資ができない中堅中小企業であっても、大手企業と同じようなセキュリティ対策が求められることになる。

3. 2　一件当たり漏洩人数と件数の関係～サイバー犯罪の被害

日本ネットワークセキュリティ協会『2011 incident survey』から、様々な組織における個人情報漏洩データを基に、横軸に一件当たり漏洩人数、縦軸には件数（100 単位）を取ったものが図表６である。大規模な情報漏洩件数になるほど、発生件数は減っている、ことがみてとれる。特徴的なことは､2008 年から 2011 年までは毎年極めて類似した傾向を示していることであろう。ちなみに、データはその後３年分入手可能であるが、これらの年次は多少ばらつく。

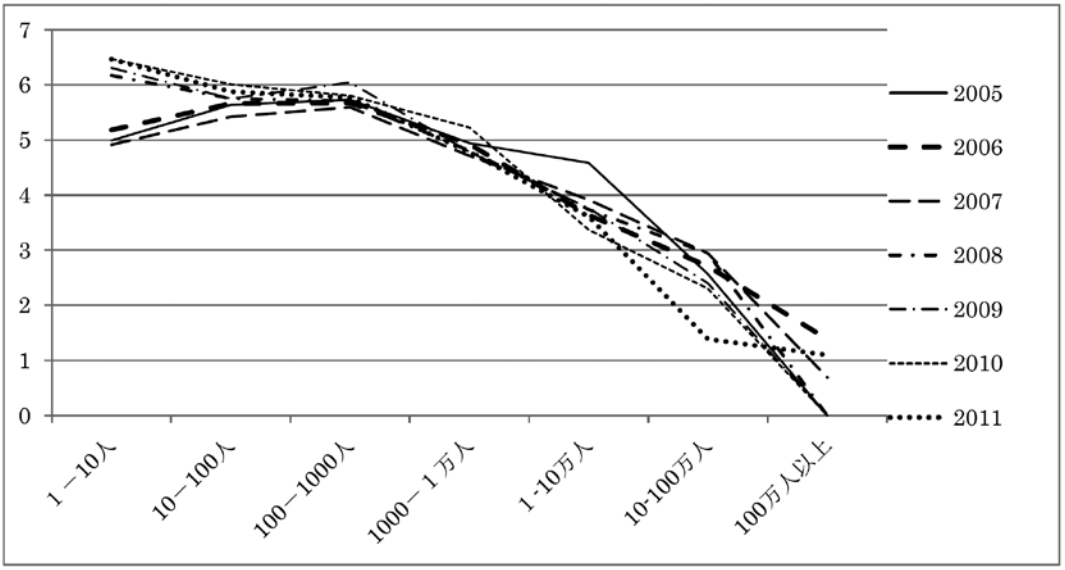
法制や規制の効果は、あるとすれば、すべてのセキュリティ・イベントに共通に現れるべきものである。それは、ここには、明瞭に出ていない。

図表中事故規模が小さい所で件数が減っているのは、2005 年から 2007 年である。2005 年から 2007 年については、世間の認識がまだ行き渡らず、個人情報漏洩を報告するまでもない、と考えられていたのである。

なお、本データでは、個人情報漏洩は必ずしもサイバー攻撃によるだけでなく、内部による犯行も含まれている。

この法則は、横軸の被害規模を価値額に代えると成立しないのではないか、という疑問がある。そもそも被害額は風評被害などの見えない部分があり、計測には論争がある。この法則は、被害と頻度の両方を実物で測ることで成り立っており、価値額のバージョンはこの法則を使って分析されるべき対象である。

図表６　一件当たり漏洩人数区分と件数の推移



出典）日本ネットワークセキュリティ協会『2011 incident survey』から。

3. 3　業種効果

このようなデータに業種の違いが毎年現れているのであろうか。企業調査の紹介の後、実証分析に進むことにしよう。

（1）日本の業種別サイバー攻撃の発生率

日本情報システム・ユーザー協会（JUAS）が、東証１部上場企業とそれに準じる企業の計 4000 社（有効回答社数は 1030 社）の IT 部門長に調査票を郵送する形で企画・実施した 2012 年 10 月 29 日から 11 月 19 日が調査期間での「企業 IT 動向調査報告書 2013」では、サイバー攻撃を受けた業種の比率もランク付けされている。攻撃が多いのは、製造業 24%、金融･保険･不動産 19%、サービス 17%の３産業の順である。政府（防衛を含む）、エネルギー・公益 10%、専門サービス８%が続く。

（2）サイバー犯罪の業種別被害とその額の米国での調査

サイバー犯罪の被害とその額などを調査した Ponemon［ 2012b ］では、被害を受けた企業の業種も分類されている。被害額が多いのは、防衛、電力・エネルギー、金融の３産業の順である。業種のリストの最後になるのが、同じ順で消費財、レストラン･観光業（hospitality industry）、小売、の３産業である。

分類されるのは総計 14 産業で、上記の他にあげられている業種には、被害額の少ない順に Industrial、Healthcare、Public sector、Services、Technology、Transportation、Communications、Education & research がある。この調査のサンプル・サイズが小さいにもかか

わらず、３ヵ年に渡り、同様な傾向が続いていることが特筆される。

（3）業種効果存在の証明

それでは、ハインリッヒに類似する前節の法則に業種効果は存在するのであろうか。Ln（１件当たり漏洩人数）を、年毎に、Ln（インシデンス件数）に線形回帰してみた。その推定誤差の相関係数を計算して次の図表７に載せた。

図表７　業種効果の相関係数

	2009 年	2010 年	2011 年
2009 年	1	0.4605	0.4438
2010 年	―	1	0.6118
2011 年	―	―	1

注）Ln（１件当たり漏洩人数）を、該当年毎に、Ln（インシデンス件数）に線形回帰した推定誤差の相関係数値。

いずれも高い相関係数値を示している。この事実は、ハインリッヒ類似法則には、その他の要因が作用していることを証明している。特に、それが業種効果と係わりがあると予想される。これら相関係数値が高ければ業種効果があることを示すものとまずは疑われるのである。しかしながら、計測式のなかに業種ダミーを入れることは、残念ながら、サンプル数が少なく出来ない。

4. 事故回避行動の実証例

4. 1　調査の先行事例紹介

先行する調査結果がいくつか報告されているので、紹介しておこう。

（1）セキュリティ対策の導入率

トレンドマイクロは、同社が Web 上で提供する企業向けセキュリティ無料診断ツールである「セキュリティアセスメントツール」の分析結果を 2012 年 10 月 10 日に発表した。2012 年 1 月 20 日の同ツール公開から８月末日までにアセスメントを実施した延べ 1,714 社の評価結果を集計し、スコアリング・数値化した結果である。

企業・団体に求められるセキュリティ体制は、約 50% が未整備であり、「サイバー攻撃対策」が 54.3%、「データセキュリティ」が 48.5%、「クラウドセキュリティ」が 47.0%、「モバイルセキュリティ」が 45.2% 未整備となっている。

セキュリティ強化を図る上で必要なユーザ教育も十分でない。セキュリティ課題を認識していても、具体的な対策の導入率は極めて低い、という結論になっている。

（2）情報漏洩リスクと被災時の想定対策費用

サイバー攻撃損害の補償をする保険を発売する AIU 保険が、潜在的ニーズを把握することを目的に、資本金 5000 万円以上で、従業員 100 人以上の日本企業の経営者・役員 200 人を対象に表記の件につきネットで調査している。田中［2013］の紹介記事参照。

情報漏洩の対応策をみると、「速やかな事実確認の徹底」（55.0％）と「原因の究明と把握」（21.0％）が最も重要だと認識している。情報漏洩の最も大きな原因には、全体では、定期的な状況把握やルールのマンネリ化といった「管理の不備」（33.5％）が挙がる。従業員数別だと、100 ～ 299 人規模の企業では「従業員の不正行為」（33.0％）が高く、「管理の不備」が全体よりも低くなる。1000 人以上規模の企業だと「サイバー攻撃」と「管理の不備」が高く、「従業員の不正行為」は低くなる。

サイバー攻撃の被害に遭った時、その対策にかかる想定費用は全体平均で約 1 億 2000 万円となっている。この想定費用は、従業員数が多くなればなるほど高くなっており、1000 人以上規模の大企業では約 3 億 4000 万円となり、100 ～ 300 人規模の企業と比較すると、約 10 倍の差となっている。

4. 2　事故回避行動の実証分析例

事故回避行動を、直接、分析した唯一の例を見てみよう。

（1）インターネットバンキングにおける不正送金

警察庁［2015］は、インターネットバンキングにおける不正送金犯罪を調べ、被害が増えている事実を報告している。被害対象が、メガ銀だけでなく、地方銀行や信用金庫・信用組合に拡大するとともに、法人名義口座に係る被害が拡大したことが、被害が増えている理由としている。

また、不正の技法は、資金移動業者を介して不法に国外送金する事犯から不正送金処理を自動で行うウイルスの利用等手口へ移行し、悪質・巧妙化していると指摘する。

警察庁［2015］データの一大特徴は、阻止行動によって得られた金額のデータが計算されていることで、「不正送金阻止」とは、事前に凍結された口座への送金指示に対する送金処理の取り消し、法人サービスにおける当日送金の停止等により、金融機関が不正送金を未然に阻止したものである。

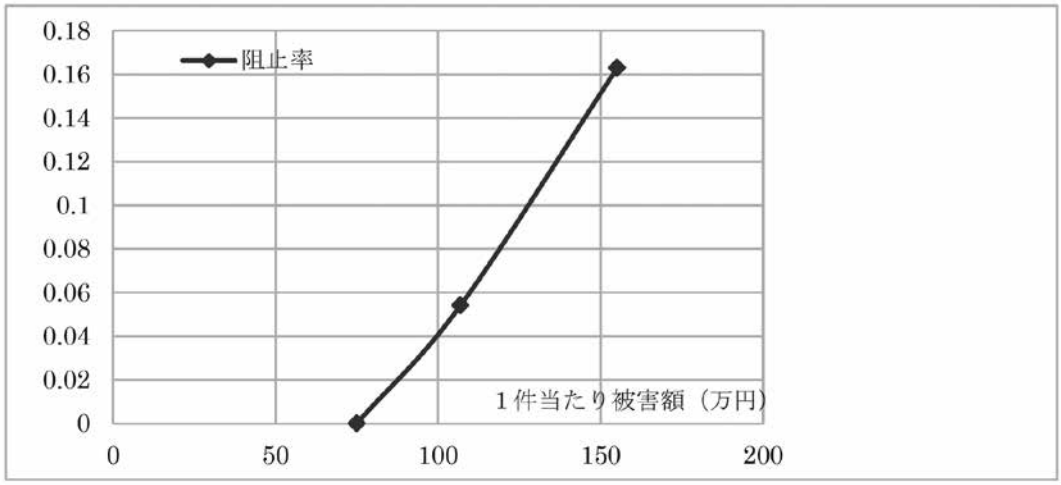
（2）不正送金阻止行動

金融機関が不正送金を未然に阻止したもので、阻止行動とは、金融関係団体やウイルス対策事業者等との連携、留学生・技能実習生関係団体に対する指導・啓発の要請、などである。これにより不正送金を阻止する効果はあったものと考えられる。

実際、被害額（犯人が送金処理を行ったすべての額）から実被害額（被害額から金融機関が不正送金を阻止した額を差し引いた実質的な被害額）を引いた額を不正阻止額とよび、阻止率をその額を被害額で割った比率としてみると、１件当たり被害額が増えれば、阻止率が高まる実態が図表７からわかる。

これらの阻止行動は、フィッシングやマルウェアへの対策をとって阻止したわけではない。それ以外の伝統的な手段がとられている。それでも、回避や阻止行動を分析している本稿にとっては、重要である。

図表７　インターネットバンキングにおける不正送金の規模と不正送金阻止率



注）警察庁［2015］から計算。横軸は１件当たり被害額（万円）、縦軸は阻止率、である。

4. 3　阻止行動の効果計測について

阻止行動の効果を適切に計測できるか、計測できているか、次のような理由で多少の疑問はある。

セキュリティ対策と一言でいっても、様々である。この分析では対策の中身は問うていない。セキュリティ対策の有効性については、さらに、不確かである。

さらに深刻な問題は、セキュリティ対策をとっていると、犯罪自体の存在がわからないかもしれない点である。

5. 被害額予測と対応策

5. 1　確率予測の公式

原田［2012］は、自身も係わる調査研究を要約して、情報漏えい事故件数と１件あたりで漏えいした個人情報の数の分布は裾が長く、べき（冪）乗則に従うことが分かったと報告している。べき乗則には、所得・収入の大きさと該当人口との分布についてのパレートの法則や、構造的自己相似性のフラクタル、がある。

べき乗則の興味深い性質は、スケール不変性にある。例えば、$f(x) = ax^k$ という関係が、$f(cx) = a(cx)^k = ac^k(x)^k = c^k f(x)$ という形で維持される。計測にあたっては、自然対数 Ln（ ）をとった形の

計測式、

Ln (f (x)) = Ln (a) + k Ln(x)、

を推定すればよい。係数 a と k がわかっていれば、ある地域で、ある期間に発生する事故の発生数を予測できるようになる、かもしれない。例えば、次のとおりである。

ある地域である期間内に発生した地震のマグニチュード x 毎の地震の件数 f (x) をグーテンベルグ・リヒターの式に当てはめ、係数 a, k を求める。推定された係数値 a と k から、大地震の発生率を計算すればよい。

5. 2　被害への対応策に使うためには

いくつか計測上残された課題があるので、述べておこう。

（1）サンプル数不足

係数を高精度で推定するためには、小さい事故から大きな事故まで含まれていなければならない。しかしながら、大きな事故は滅多に起こらない（ほとんど起こらないレア・ケースとして、10 万年に 1 度しか起こらない現象、などが例となる。）ため、サンプル期間が短ければ観察されないことになる。それゆえ、事故の発生数を精度よく予測するには、長期間の事故のデータが必要になる。

一方、小さな事故は、関係者の少なさ、その影響度の低さから、現場で独断的に対処されたり、もみ消されて、外部に報告されない可能性がある。事故を捉らえる検知能力を向上させる必要がある。

そこで、事故の大きさ毎に扱うサンプル期間を変え、大きな事故は長期間、小さい事故は最近だけの短期間のデータを使う、という統計学的方法が考えられる。

（2）多変量解析とサンプル・セレクション・バイアス

これまでの節で説明したように、事故発生確率に影響する要因は数多い。規模だけが変数ではないので、ハインリッヒの法則やグーテンベルグ・リヒターの法則のようなワンファクター・モデルでは実際の動きを説明するには弱い。多変量解析が必要になる。

もう 1 つの問題としてサンプルの質が重要になる。被害者側の事情として、攻撃対象となる企業や主体の数がサンプルとしてまだまだ少ないという事実がある。認証会社、セキュリティ・ベンダー、などの業界が最近攻撃される、などのケースに見られるように、特定の時期に特定の業種が狙われるというバラつきもある。攻撃者側の事情として、闇のなかで不確実であるとしても、資金・資源・能力を持つ攻撃者は世界を見渡しても極めて少ない。これらは、サンプル・セレクション・バイアスが大きいということを指している。その結果、予期せぬ要因が現れたり、する。

６．まとめ

本稿の研究は、保険会社が提供する商品をデザインするという観点からも、多くの関心を集めているテーマである。また、特定の組織が十分なサーバー攻撃対策をとっているかどうか、適切な指針・アドバイスを出せるか、などにも関心は高い。

被害を完全に防ぐことができないことも認識する必要がある。この点は厳粛な事実である。他方で、この考えを守り続けると、被害があっても許してしまうことになり、防御を怠りがちになる。「戦闘に敗れた指揮官は慰労するべきだが、警戒を怠った指揮官は許すべきではない」という戦いの諫言がある。事前の防御は大切であるということと「挑戦した結果の失敗なら構わない」ということでもある。

どこまでが許される被害なのか、どこまでが許されない被害なのか、具体的な境界線を設定するべきなのである。サイバー攻撃に対しては、セキュリティ事故のリスクを把握して、一部リスクを受容し、対策と効果の最適なバランスを考えた合理的なセキュリティ対策を考える必要がある。

脚注

＊）学習院大学経済学部教授。内容などの連絡先：〒171-8588 豊島区目白１－５－１学習院大学経済学部、TEL（DI）：03-5992-4382、Fax：03-5992-1007、E-mail: Kenichi.Tatsumi◎gakushuin.ac.jp（ご送信される場合◎は@に置き換えてご利用ください。）

本稿は多くの先行文献、ネットでの用語解説や研究者の口頭での発言に依存している。体系的でない記述をしている文献は引用できない、引用しなかった。それゆえ、ここで謝辞に代えたい。

参考文献

Goto, M. and Tatsumi, K.,［2012］“The Theory of Optimal Investment in Information Security and Adjustment Costs: An Impulse Control Approach,” pp.73-96 in Recent Advances in Financial Engineering 2011, Proceedings of International Workshop, edited by Takahasi, A., Muromachi, Y. and Nakaoka, H., World Scientific Publishing, 2012.

原田要之助［2012］「大規模な情報漏えい事件の特性と対策の考え方」『情報セキュリティ総合科学』、第４号、2012 年 11 月、pp.183-195。

Heinrich, H.W.,［1950］, Industrial Accident Prevention; A Scientific Approach, 3rd Edition (1st Edition, 1931), McGraw-Hill, 1950.

警察庁［2015］『平成 26 年中のインターネットバンキングに係る不正送金事犯の発生状況等について』、2015 年２月 12 日。

Ponemon Institute,［2012a］『2011 年情報漏洩のコストに関する調査：日本版』、2012 年。

Ponemon Institute,［2012b］, 2012 cost of cybercrime study: United States, Oct. 2012.
http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf

田中好伸［2013］「経営者が最も意識するリスクは情報漏洩―３割が BYOD を個人裁量に」、ZDNet Japan、2013 年１月 24 日。

辰巳憲一［2011a］「金融・経済活動における情報などの分割、バックアップと情報セキュリティ～金融セキュリティの経済学入門（I）～」『学習院大学経済論集』、2011 年１月、pp.301-321。

辰巳憲一［2011b］「個人情報信託の経済分析～プライバシー情報を保護しながら信託で一元管理する～」『学習院大学経済論集』、2011 年７月、pp.83-109。

辰巳憲一［2011c］「情報セキュリティ問題とその進化」『学習院大学経済経営研究所年報』、第 25 巻、2011 年 12 月、pp.15-26。

辰巳憲一［2012a］「情報セキュリティの階層型統合管理に関する経済分析（I）」『学習院大学経済論集』、2012 年４月、pp. ３-21。

辰巳憲一［2012b］「情報セキュリティの階層型統合管理に関する経済分析（II）」『学習院大学経済論集』、2012 年７月、pp.99-116。

辰巳憲一［2014a］「パーソナル情報の信託業務における価値創造～情報価値と非公開情報の補完の視点から～」『学習院大学経済論集』、2014 年７月、pp.81-101。

辰巳憲一［2014b］「情報セキュリティ事故発生確率の分析～サイバー攻撃を中心にした調査の展望と論評～」『学習院大学経済経営研究所年報』、2014 年 12 月、pp.75-101。

Tatsumi, K. and Goto, M.,［2010］“Optimal Timing of Information Security Investment,” in Moore, T., Pym, D. and Ioannidis, C. (eds.), Economics of Information Security and Privacy, Springer, 2010. (Chapter 11)

辰巳憲一・後藤 允［2010］「情報セキュリティとその投資の分析～研究報告書～」『学習院大学計算機センター年報』2010 年 12 月、pp.49-62。

http://ci.nii.ac.jp/els/110008148617.pdf?id=ART0009662982&type=pdf&lang=jp&host=cinii&order_no=&ppv_type=0&lang_sw=&no=1303796391&cp=

鵜沢裕一［2012a］「大規模企業向けに急増するハクティビズム攻撃、１年で過去４年分以上」『日経コミュニケーション』2012 年７月 31 日。

鵜沢裕一［2012b］「情報漏洩に使われるマルウェアの 95％は、感染ではなく犯罪者によるインストール」『日経コミュニケーション』2012 年９月５日。