サイバー脅威インテリジェンスにおける会計的なコントロールと心理的なコントロールの関係性
―コミュニケーション活動と仕事満足度の関連から―

佐藤　正隆（武蔵野大学 経営学部 専任講師）

要約

A 社のサイバー脅威インテリジェンスの業務は、分業では成り立たず、すべての業務を最初から最後までやり遂げている。これが A 社のサイバー脅威インテリジェンスの仕事における第一の経営理念である。サイバー脅威の解消は、短時間で解消しなければならないという第二の経営理念である。

サイバー脅威インテリジェンスの業務は、密接な関係でしかも少ない時間でのコミュニケーション活動を行う必要がある。受注を受けるか否かについては、請負価格に関して、損益分岐点の思考で判断している。サイバー脅威インテリジェンス事業は、事業者の人件費と高級ホテルの一室を事務所とした賃借料が主要なコストであるので、約 90％を利益として見込める高利益率の業種であり、良好な経営業績を上げているという。A 社によれば、政治的な観点を除いて接しているので、サイバー脅威インテリジェンスの仕事を楽しくこなし、仕事への満足度は高いという。

１．問題提起

佐藤（2023）では、中小企業の経営者がどのようにして従業員の満足度を昂揚させ、企業業績を向上させているのかを考察している。先行研究として、澤邉・飛田（2009）の見解をもとに、中小零細企業の経営者への訪問調査を実施し、それらの会社の現状を調査している。その結果、中小零細企業では、企業業績を向上させるためには、会計的な側面よりのコントロールと心理的な側面よりのコントロールの併用が必要であることを確認している。しかし、従業員の業務の範囲と責任の所在が明確という会計的な側面よりのコントロールである要件は、従業員の仕事に対する満足度を高めるといった結果には至らなかっ

た。佐藤（2023）の研究対象は、製造業を中心とした企業であるため、本研究ではサービス業の会計的な側面よりのコントロールと心理的な側面よりのコントロールが業績に及ぼす影響について検討する。

かつて、ネット注文で、商品購入の支払い手続きに入った時、クレジットカードによる決済をしようとすると、「長らくカードを使用していないので、カードの再登録をして下さい」といった旨の要求がパソコン上に表示された。うかつにもカード情報を打ち込んでしまった。その後、何日が経つと、高額なコンピュータ付属用品が次々に送られてくることになり、大変な迷惑を被ったことがある。ネット犯罪の一つである。

この度、訪問調査の機会を頂いたA社は、「サイバー脅威インテリジェンス」というネットワークに係る犯罪を防御するために、犯罪者の情勢を密かに探り、依頼者である企業の担当者に、その危険な状態を知らせる仕事に携わっている。その「サイバー脅威インテリジェンス」というサービス提供型の事業経営に関して、経営理念、会計的な側面よりのコントロール、心理的な側面よりのコントロール、経営業績および仕事満足度などについて、その内容を明らかにすることを目的としている。

2．外部志向型企業と内部指向型企業の検討

（1）サイバー脅威インテリジェンスの必要性

サイバー脅威インテリジェンスは、2015年頃から日本に入ってきた。当初、弁護士や法律事務所がマンパワー（人、専門性、時間の拘束）で、コンサル業務を請け負う監査法人などでサイバー脅威インテリジェンスの仕事を行っていた。A社の代表取締役は、個人事業主として、サイバー脅威インテリジェンスというサイバーセキュリティのサービス提供を行っている。これはネットワークに係る犯罪を防御するために、犯罪者の情勢を密かに探り、依頼者である企業の担当者にその危険な状態を知らせる仕事である。これにより、依頼企業のサイバー脅威の危険を解消して、依頼企業の安全確保が保障されることになる。

私たちがインターネットにアクセスできるレベルをサーフェスレベルという。これはインターネットの表面上のレベルである。このサーフェスレベルといった表向きの領域は、インターネット全体の5%程度に過ぎない。インター

ネット領域の残りの95%程度は、一般の人々が通常アクセスできない闇の領域である。このアクセスできない闇の領域は、誰かによって制御されている。

それは国家としての制御、または闇を支配する犯罪集団の制御である。そこでのサイバー脅威に係る犯罪に対しては、それらの犯罪を防御するために、犯罪集団の情勢を密かに探り、依頼者である企業の担当者にその危険な状態を知らせる仕事が必要になってくる。そのために、インテリジェンス事業としては、犯罪集団の情勢を密かに探るためにクローリング（Crawling）作業を行う。このクローリング作業とは、Web上で様々なサイトを巡回し、情報の保存や複製などの様々な処理を行う作業のことである。このWeb上でのサイトの巡回は、特定の企業に絞り込むこともあれば、官公庁、警察が警戒する犯罪組織などに絞り込むこともあるという。

例えば、B銀行に係る仕事でWebサイト上の巡回作業を行っていた時期に、B銀行のホームページをコピーして、B銀行を装い、偽のホームページやアプリを作成しているものがあった。一般に、日本人は、アプリやネットワーク情報を見ることには関心が薄い。しかし、諸外国の人々はアプリやネットを頻繁に閲覧し、それらを様々な目的で活用している。いずれの場合にしても、本来、顧客となるべき人々が誤って偽のアプリやネットにアクセスし、個人情報を盗まれるという事件が数多く発生している。特に、最近、「インターネット社会」といわれ、このような事件が社会問題となっている。それ故に、このサイバー脅威インテリジェンスの仕事は、このような偽サイトを削除する必要性から、最近、注目されてきている。

（2）外部志向型企業と内部指向型企業

A社は、外部志向型の特徴を有している。澤邉・飛田（2009）では、外部志向型企業の特徴として、大家族型や官僚組織型よりも起業家型や競争原理型を中心にもつことを示している。創業時の企業は外部志向型であることが多いと考えられる。会社を創業したときは、安定性を求めるよりも挑戦していく意識の方が強く働くため、起業家型や競争原理型を中心にもつことになる。榊原ほか（1989）では、内部志向型企業は既存事業から切り離されたものに多くあることを指摘している。外部志向型企業は、スタートアップ企業の特徴を有して

いるとしている。2015年にスタートアップ企業として創業したA社は、外部志向型の企業の特徴を有している。創業から5年を過ぎると内向志向型の企業の特徴を有するといわれる。しかし、A社ではSaaSを通じてサービスを提供しており、クラウド上で商品を取り扱い、時代の変化に応じ、即座にカスタマイズを実施している。犯罪集団の新たな手口に対して柔軟な対応をしていくため、A社は安定性の追求よりも新たに挑戦していくため、外部志向型の企業の特徴を有していると考えられる。

3．経営理念とコミュニケーション活動

（1）先行研究におけるコントロールの必要性

澤邉・飛田（2009）では、内部志向型の企業では、経営理念の浸透度が高まれば従業員の仕事に対する満足度が高まることが示されている。また、外部志向型の企業では、内部統制制度による業務範囲の明確化と社会関係の重要性が高まることで、従業員の仕事に対する満足度が高まるという結果が述べられている。会計的な側面よりのコントロールと心理的な側面よりのコントロールに分類している。会計的な側面よりのコントロールは、①目標管理や予算管理を達成しているのか、②業務範囲が明確化されているのかという点を意識している。心理的な側面よりのコントロールは、①経営理念の浸透をしているのか、②コミュニケーション活動がなされているのかという点を意識している。両者のコントロール通じ、従業員満足度が高まり、企業業績の向上が見込まれる。佐藤（2023）では、会計的な側面よりのコントロールと心理的な側面よりのコントロールの両コントロールが必要であることを指摘している。

（2）サイバー脅威インテリジェンスの業務内容および制約

次章で、サイバー脅威インテリジェンスの業務範囲の明確化を議論する必要がある。そのため、サイバー脅威インテリジェンスの業務内容と業務の必要性を明示する。

ダークウエッブ（dark web）とは、インターネット上の闇の領域にある闇の閲覧システムであり、一般的な検索エンジンでは見ることができない領域である。これは匿名性が高く、違法な取引や犯罪などで悪用されている場合が多い。

例えば、このサイトは、武器、麻薬、人間などの売買などに使われている。この種のサイトは削除してもすぐに復活するので、このサイトを完全に削除することは難しい。

ダークウエッブ上では、偽物のパスポートの売買だけではなく本物のパスポートの売買も行われている。これは違法取引である。また、正当なクレジットカードも通用しているが、ダークウエッブ上では、このようなクレジットカードは不正に利用されている、というのが実態である。しかし、クレジット会社ではこの実態がわかっていても、自社の企業イメージの低下に繋がるといった理由で、何ら対策を講じることもなく、さらにその事実を公表もしていない場合もあるという。

ダークウエッブ上のサイトでサイバー脅威インテリジェンスの仕事をする時に、一つの障害がある。それは日本には、弁護士法第 72 条 (弁護士でない者は、報酬を得る目的で訴訟事件、非訟事件及び審査請求、異議申立て、再審査請求等行政庁に対する不服申立事件その他一般の法律事件に関して鑑定、代理、仲裁若しくは和解その他の法律事務を取り扱い、又はこれらの周旋をすることを業とすることができない。) が存在していることによる。そのため、サイバー脅威インテリジェンスの仕事では、日本国籍を有し、弁護士資格を有していないと、解決できないネット上の問題が絡んでくるというのである。その理由は、ネットを保存しているサーバーが日本に存在せず、ほとんどが日本ではない諸外国にあるからである。そのため、我々がサーバーと連絡をするにあたっても、電話のやりとりができない、またメールでの返信も来ない、といった状態であるという。これがサイバー脅威インテリジェンスの仕事におけるひとつの障害となっている。

一方で、ダークウエッブを監視する場合に、ダークウエッブに精通している情報があると効果的なことがあるという。依頼企業をネット上で監視する場合、ネット上から全てを見ることができる部分と見ることができない部分とがある。そこで、機械学習機能を通じて、企業の何らかの領域を集中的に監視することになる。この場合、国家の諜報活動を行っていた人々や財務捜査官などの警察勤務の経験がある人々の機密情報が、ダークウエッブを監視する場合に有効になるという。すなわち、これらの人々の情報は彼らしか持ち得ないもので

あり、信頼性の高い機密情報であるからである。

（３）サイバー脅威インテリジェンスを必要とする背景

サイバー脅威インテリジェンスの仕事を行っていると、フィッシングメール詐欺をよく見かけるという。このフィッシングメール詐欺として見かけるのは、銀行、宅配会社、Amazon、Apple などを装ったメールであるという。フィッシングメール詐欺では、送信者を偽って電子メールを送りつけ、偽の電子メールから偽のホームページに接続させたりするなどの方法で、クレジットカード番号やユーザ ID やパスワードなどのアカウント情報といった重要な情報を盗み出す行為である。そのような偽メールによって偽のホームページにアクセスすると、個人情報や会社情報が盗みとられ、それらが流出することになるので、サイバー脅威インテリジェンスとしては、そうならないように防御策を講じているのであるという。その防御策の一つとして、サイバー脅威のレベルをコンピュータの液晶画面上で、注意喚起の段階が判断できるように可視化しているという。段階レベルとしては、(1) 最も危険、(2) 危険、(3) 中程度、(4) 低い、(5) 今後危険になる可能性がある、といった内容である。

サイバー脅威インテリジェンスを必要とする背景には、このところのインターネットを利用した企業経営が目立つようになってきたことである。その一つが、銀行、生命保険会社、損害保険会社、製薬会社、医療機関などである。例えば、損害保険会社は社会基盤として存在する必要がある。しかし、いずれの損害保険会社であってもこのところ経営状態が思わしくない状態が続いている。そこで、損害保険会社では、損害保険事業以外の何らかの事業で、利益を生み出すという経営を行っている。それがネットワーク上の安全確保のためのサイバーセキュリティ保険の事業であるという。次に、インターネットを利用した企業経営としては、小売業、ブランドファッション業、流通業といった企業がある。その具体例が家具およびインテリア用品小売業の大手ニトリである。ニトリの場合、かつては店舗販売を中心とした企業経営を行っていた。しかし、時代の変化に伴いインターネットを利用した企業経営に主軸を移行してきている。

他にも、新聞社や出版社を含むメディア系企業、エンターテイメント系企業、ハイテク系企業もインターネットを頻繁に利用する企業経営を行っている。こ

こでは、一般的なITが利用され、コンピュータやインターネットなどを使っている。製造業もインターネットを利用しているが、製造業の場合は、OT（Operational Technology；工場やプラント、ビルなどの制御機器を制御し運用するシステムやその技術のことである。例えば。原発や資源に関係する閉じたITなどである。）を利用している。また、官公庁や警察などの政府系の機関や教育機関でも、ほとんどすべての業務分野でインターネットを利用した運営（インターネット経営）を行っている。このように、多くの企業がインターネットを利用した企業経営（インターネット経営）を取り入れることにより、そこでの犯罪が数多く発生するようになった。そして、その犯罪を防御するために、サイバー脅威インテリジェンスの仕事が必要となった、という背景がある。

４．会計的な側面よりのコントロール

（１）目標管理や予算管理

佐藤（2023）では、目標管理や予算管理の会計的な側面によるコントロールが従業員満足度に影響を与え、会社の企業業績を高めることを示している。内部志向型の企業では、目標管理や予算管理が機能していたが、外部志向型の企業では、目標管理や予算管理が機能していなかった。

A社の代表取締役は、若手従業員に対して多くの経験をして欲しいと考えている。そのために、すべてのメンバーが国際的な価値観の異なる人々と接することを奨励している。若さが社会を変えることができるのは、体力だけではなく、仕事に対する勢いがあるからでもあるという。失敗しても挑戦するという気風は、企業にとって必要であるとともに、我が国全体に対しても欲しい心がけである。サイバー脅威インテリジェンスの仕事は、社会的にもてはやされる仕事であるが、瞬時に状況判断が求められるといった機敏性の求められるきつい仕事でもある。

新たな人材を投入する場合には、人の能力は失敗をしないと高まらないので、20代の若い頃にメンバーの代表として仕事に就かせることで、大きく成長することが見込まれる。また、年配のメンバーは社会経験があるので、指導者としての地位を与え、活躍の場を確保しておいてやることが重要であるという。サイバー脅威インテリジェンスの仕事には定年がないので、能力のある人材には

常に活躍の場が確保されているという。

A 社では、予算管理や目標管理を厳格に実施すると、挑戦する姿勢が損なわれると考え、これといった予算編成と予算執行は実施されていない。

さらに、利益率 90％であり、仮に、月収（請負収入）500 万円であるとすると、その 10％が賃借料 50 万円という損益計算をしている。つまり、請負収入 500 万円として会費を受け取り、営業費としての賃借料 50 万円を差し引いた残額 450 万円をすべて利益と考えている。単純な損益計算であるので、予算編成や予算執行といった会計的な側面よりのコントロールは、実施されてはいなかった。この結果は、製造業とサービス業では異なるが、佐藤（2023）と同じ結果を示している。外部志向型の企業では、目標管理や予算管理が機能していなかった。

（２）業務範囲の明確化

佐藤（2023）では、業務範囲の明確化の会計的な側面によるコントロールが従業員満足度に影響を与え、会社の企業業績を高めることは示されていない。しかし、澤邉・飛田（2009）では、外部志向型の企業では、内部統制制度による業務範囲の明確化と社会関係の重要性が高まることで、従業員の仕事に対する満足度が高まるという結果が述べられている。

一般的な企業では、業務の役割を分担した分業が行われている。しかし、A 社のサイバー脅威インテリジェンスの仕事では、収益（請負収入）の観点からすると、１人でやれることは１人でやった方がよいと考えている。人数が増えると人件費が増えることになる。サイバー脅威インテリジェンスの仕事は、分業では成り立たず、すべての仕事を最初から最後までやり遂げるといった職人のような仕事であると考えている。すなわち、ここでは業務範囲は明確に区分されずに、すべてが A 社の代表取締役の業務範囲となっている。

A 社は外部志向型の企業であるが、業務範囲の明確化はなされていない。会社経営全般に関わる知識を持った少人数の従業員で業務を遂行していることもあり、業務範囲の明確化を必要としていないと考えた。

５．心理的な側面よりのコントロール

（１）経営理念の浸透

佐藤（2023）では、経営理念の浸透である心理的な側面によるコントロールが従業員満足度に影響を与え、会社の企業業績を高めることは示されていない。サイバー脅威インテリジェンスの仕事では、収益（請負収入）の観点からすると、１人でやれることは１人でやった方がよいと考えている。人数が増えると人件費が増えることになる。これはサイバー脅威インテリジェンスの仕事におけるA社の第一の経営理念である。

サイバー脅威を無償で解消してくれるサービスもあるが、その解消能力は極めて低く、サイバー脅威の解消はほとんど期待できない。この種のサービスにサイバー脅威の解消を委ね、その結果を待っていると、多くの時間あるいは日数を費やしてしまうことになる。また、たとえサイバー脅威が一時的に解消できたとしても、根本的な解消には至らず、違法サーバーはすぐに復活してしまう。サイバー脅威の解消は、短時間で、例えば１時間や２時間で解消していかなければならない。長くとも１日以内で解消策を出していく必要がある。つまり、サイバー脅威を解消するには時間の速さが重要なポイントなのである。これがサイバー脅威インテリジェンスの第二の経営理念であるという。そうしないと、例えば、サイバー脅威の原因となる企業の悪い噂は、一瞬で広まることになるので、企業としてはすぐに削除したい代物なのである。

サイバー脅威インテリジェンスの仕事で、ダークウェブでの巡回捜査には通常のパソコンを利用している。ダークウェブに通常のパソコンでアクセスするとパソコン内にある情報やデータが抜き取られる可能性がある。この防御策としては、大規模な情報機関や教育機関がダークウェブでの巡回捜査するための指導書を作成し、これを利用できる体制を創る必要性があるという。現在でもダークウェブを巡回捜査するための指導書はあるが、10年から20年前の内容での指導書であるので、即時的な内容が取り上げられていない。ダークウェブに係る関係者全員がこの即時性を理解して、問題解決に取り組んでいく必要がある。このような即時性に対応して指導サイトを立ち上げているのは、やはり20代の若者が行っているという。その理由としては、「失敗しても良いからやってみよう」という行動方針を持っているからである。かつては、「失敗は許されない」という風潮があったが、現代では「失敗を恐れずにやってみる」という考えが、このサイバー脅威インテリジェンス業界では広まっているという。

外部志向型の企業では、経営理念の浸透が大きな影響を与えるわけではないが、A 社では経営理念の浸透が行われていた。

（2）コミュニケーション活動

佐藤（2023）では、コミュニケーション活動を通じた心理的な側面によるコントロールが従業員満足度に影響を与え、会社の企業業績を高めることが示されている。また、澤邉・飛田（2009）では、外部志向型の企業では、内部統制制度による業務範囲の明確化と社会関係の重要性が高まることで、従業員の仕事に対する満足度が高まるという結果が述べられている。

1 人でできる仕事を 10 人でやる必要はないと考えている。大人数で仕事をするというのは大企業の作業のやり方であり、10 人、50 人、100 人といった多くの作業者がいれば､その人数分のコミュニケーション活動が必要となる。コミュニケーション活動を円滑に行おうとすれば、メンバー同士でのメールでのやり取りや会合が必要となり、メンバー全員が共通の認識に至るまでには多くの時間を費やしてしまうことになる。しかし、メンバーが少なければ、少ない時間で共通の認識をもつことができる。サイバー脅威インテリジェンスにおいては、この種の密接な関係でしかも少ない時間でのコミュニケーション活動を行う必要がある、と A 社の代表取締役は述べている。サイバー脅威インテリジェンスは、時間との勝負であるともいう。

大企業で、コンピュータに精通し、その実績を上げた指導者であっても、コンピュータ技術のめまぐるしい変化に対応するのは難しい。なぜなら､サイバー脅威インテリジェンスの仕事では、従来のコンピュータ技術と知識では通用しない領域が確実に増えているからである。サイバー脅威インテリジェンスの仕事では、一つの達成目標に専念し、数多くの作業をこなさなければならない。そこで、A 氏は、サイバー脅威インテリジェンスの仕事に新たな人材を投入するにあたり、その人々がどのようにすれば成長できるのかを常に考えているという。ここではメンバー間の円滑なコミュニケーション活動が必要となるので、困ったときにすぐに支援できる体制をつくることが大切であるという。

少人数での仕事であるため、A 社は密接な関係でのコミュニケーション活動を実施している。これは先行研究と同様の結論を得ている。

６．従業員満足度と業績への影響について

（１）サイバー脅威インテリジェンス事業の高い利益率と仕事満足度

A 社のサイバー脅威インテリジェンスの事業は、事業者の人件費と高級ホテルの一室を事務所とした賃借料が主要なコストであった。収益（請負収入）については、前受けで年会費を受け取り、サイバー脅威インテリジェンスのサービスを提供する受注型の事業である。この場合、受注を受けるか否かについては、請負価格に関しては、損益分岐点の思考で判断しているという。サイバー脅威インテリジェンス事業は、事業者の人件費と高級ホテルの一室を事務所とした賃借料が主要なコストであるので、約 90％を利益として見込める高い利益率の業種であり、良好な経営業績を上げているという。ただし、誰でもできる仕事ではなく、サイバー脅威インテリジェンスの仕事で能力を発揮できる人のみが得られる経営業績であると判断した。A 社の代表取締役によれば､サイバー脅威インテリジェンスの仕事では、最先端のコンピュータを操れるデータバンクをやることが最大の利益追求に繋がるという。

サイバー脅威インテリジェンスの仕事は、初年度の実績が評価対象となり、２年度以降の請負価格は初年度の実績次第で請負価格の計算式が変わり、それにより請負価格も変動する仕組みになっているという。また、サイバー脅威インテリジェンスの仕事は時間給で決められており、1 時間あたりの賃率が高く、例えば、1 人あたりおよそ月 500 万円程度の請負収入になるという。しかし、昼夜問わず仕事に掛かりきりでいるので、本当の意味での時間給計算はできていないという。長時間労働でも苦しいと感じることはなく、楽しい仕事である。飲む、食べるといったことよりも、サイバー脅威インテリジェンスの仕事が楽しいという。A 社の代表取締役によれば、政治的な観点を除いて接しているので、サイバー脅威インテリジェンスの仕事を楽しくこなし、仕事への満足度は高いという。仮に、政治的な観点から、サイバー脅威インテリジェンスの仕事をするとなると、複雑な問題が発生することになると推察された。そこで、「そのような仕事をしていると、恨まれることはありませんか」という問いに対しては、「あるとしたら、犯罪組織ぐらいしかない」といわれた。

（２）会計的な側面および心理的な側面よりのコントロールの関係

サイバー脅威インテリジェンスの業務について、会計的な側面よりのコントロールと心理的な側面よりのコントロールなどの関係を示すと、図表１のように整理することができる。

図表１ 会計的な側面よりのコントロールと心理的な側面によるコントロール

評 価 項 目	サイバー脅威インテリジェンスの事業活動
１．会計的な側面よりのコントロール	
①予算編成と予算執行	これといった予算編成と予算執行は実施されていない。
②業務範囲の明確化	サイバー脅威インテリジェンスの仕事は、分業では成り立たず、すべての仕事を１人で行っており、仕事のすべてが業務範囲となっている。
２．心理的な側面よりのコントロール	
①経営理念の浸透	サイバー脅威インテリジェンスの仕事は、１人でやれることは１人でやった方がよい。サイバー脅威を解消するには時間の速さが重要なポイントである。
②コミュニケーション活動	１人の仕事であるので、密接な関係でのコミュニケーション活動と少ない時間でのコミュニケーション活動が、実践されている。
３．経営業績	前受けで年会費を受け取り、経費としては人件費と賃借料が発生する高い利益率の業種である。在庫を持たない仕事である。
４．仕事に対する満足度	仕事を楽しく感じ、仕事への満足度は高い。

出所：筆者作成

佐藤（2023）では、会計的な側面よりのコントロールと心理的な側面によるコントロールの必要性を示していた。本研究では、心理的な側面によるコント

ロールである経営理念の浸透とコミュニケーション活動が従業員満足度に影響を与え、結果として利益率が高い事業を遂行し、業績が向上していた。対象が製造業ではない点も影響している可能性はあるが、従業員が経営理念を理解し、事業全体を把握していた。そのため、業務範囲を明確化しなくても、従業員が事業全体に責任をもつと同時に、報酬としてのインセンティブもあり、企業の全体最適化がなされていたと考えている。

7．仕事の達成目標と機密情報の漏えい防止策

（1）業績を維持するうえで意識するべきこと

顧客によって異なるが、顧客が解決したいサイバー上の脅威が何であるのか分かれば、その脅威を解消するための目標達成が可能になる。目標達成をするプロセスで注意するべき点は、顧客との認識を合わせることと、どのようにすればサイバー脅威を解消する方法を提供できるのかという調整である。そこで先ず、その依頼会社がサイバー脅威の危険性にある機密情報や電子資産をどの程度保有しているかを知ることから始める。このサイバー脅威の対象が決まれば、依頼企業にはサイバーセキュリティの部署があるので、そのサイバーセキュリティの部署にサイバー脅威の情報を提供することになる。この時、依頼企業がどのようなサイバー脅威の解消を期待しているのか、またそれが可能となる適切な解消方法を提供することができるのかが重要な接点となる。

例えば、技術者によくある事例であるが、その会社の機密情報をもって他社に移籍することがある。機密情報を持っての転職である。このようにして企業の顧客情報や従業員の個人情報などの機密情報が社外に流出した場合、サイバー脅威インテリジェンスの関係者である我々がサイトを閲覧した事実があると、次のような問題が起きる。それは企業の内部者が仕事上で閲覧した情報を悪用した場合には、それは刑事事件となり、サイバー脅威インテリジェンスとして閲覧できる環境にいたという条件だけで、その犯人の可能性があるとして我々が疑われることになる。依頼企業の視点から見て、サイバー脅威インテリジェンスの関係者である我々が疑われる可能性をゼロにするために、サイトを閲覧できないような仕組みに変えておかなければならない。そのためには、機密情報の漏洩をさせないためのサイトの防御システムを設定する必要がある。

フランスにおいては、例えば、旅行会社の支社が旅行の顧客名簿が流失した場合には、欧州連合 (EU) 域内の各国に適用される個人データ保護やその取り扱いについて詳細に定められた法令である GDPR（General Data Protection Regulation、EU 一般データ保護規則）に違反する行為となり、最低でも 23 億円の罰金が科せられることになる。このようにヨーロッパの法規制は、機密情報の社外流出に関しては整備されている。しかし、我が国の法制度では、この種の法整備は不完全である。一応、個人情報保護法はあるが、ヨーロッパほどの厳格さはない。それは国家自体が企業を守るという姿勢をとっているからであるという。例えば、以前、大手インターネット通販会社 C 社の顧客情報が流出したことがあったが、その時、罰金は科せられなかったとう事実をみればわかることである。

日本企業は、企業の機密情報が中国に漏れると分かっていても、中国に進出することがある。中国に大規模な工場設備を建設する日本企業は、年々、その数が減少している。例えば、日本で精密機械の部品を製造し、その部品を中国で組み立てて製品にする。そして、この製品を中国で販売するといったやり方が、高額となる輸送コストを考慮すると、安い製品の製造に繋がると考えられているからである。このような理由で、中国に工場設備を建設する日本企業もある程度存在している。その際に、特に配慮しなければならない点は、製品の製造が完了したら、次に重要なことは機密情報を盗み取られないように防御策を講じることであるという。現地中国の従業員から中国の関係者に、日本企業の機密情報が漏れるといったことは簡単に起こりうることである。日本企業が機密情報を盗まれないように防御策を講じたとしても、その防御網を超えて盗む方が勝っているのが実情であるという。しかし、当面の利益を確保したいと考える日本企業は、この機密情報の抜き取りという現実を念頭に置きながらも、中国への海外進出をしてしまうと言われている。

（２）新たなクラウド上の商品

新しいコンピュータウイルスが出てきたら、クラウド上で対策することができるが、それに伴い、サイバー脅威インテリジェンス請負契約も変更されることになる。製造企業の場合には、新しいコンピュータウイルス対策として、部

品を追加投入したり、新しい人材を投入したりして多額のコストがかかる。それに対して、クラウド上で、新しいコンピュータウイルスへの対策ができる企業については、そのような変化への対応を１人で行うことができ、少ない作業と少ないコストで済むといった利点がある。さらに、サイトについても月に何度ものバージョンアップが可能となる。

アメリカ企業の中には、このようなサイバー脅威インテリジェンスにおけるクラウド契約の変化について説明しない企業がある。BtoB 企業は理解しているが、BtoC 企業はあまり理解していないことが多い。A 社では、以前、韓国企業へのハードウェアやソフトソフトウェアの販売取引を行っていた。しかし、買い手側の韓国では、ハードウェアやソフトソフトウェアをすぐに複製できてしまうので、販売取引が成立しない、といった仕事上のやりにくさがあった。それと同時に、韓国との販売取引では利益率が低いので、その後、日本企業を顧客とする販売取引に移行することになったという。

８．結び

サイバー脅威インテリジェンスは、インターネット上のダークウエッブに存在する企業を脅威に陥れる可能性のあるサイトを削除することを目的とする仕事である。A 社は､外部志向型企業の特徴を有していた。澤邉･飛田(2009)では、外部志向型の企業では、内部統制の制度による業務範囲の明確化と社会関係の重要性が高まることで、従業員の仕事に対する満足度が高まるという結果が述べられている。また、佐藤（2023）では、会計的な側面よりのコントロールと心理的な側面によるコントロールの必要性を示していた。

本研究では、心理的な側面によるコントロールである経営理念の浸透とコミュニケーション活動が従業員満足度に影響を与え、結果として利益率が高い事業を遂行し、業績が向上していた。対象が製造業ではない点も影響している可能性はあるが、従業員が経営理念を理解し、事業全体を把握していた。そのため、業務範囲を明確化していなくても、従業員が事業全体に責任をもつと同時に、報酬としてのインセンティブもあり、企業の全体最適化がなされていたと考えている。

本研究は、中小零細企業を対象としているため、コントロールの一般化には

限界がある。しかし、特殊な業種のインタビュー調査を通じ、心理的な側面よりのコントロールを中心としたコントロールを提示できたことに、先行研究への貢献があると考えている。

謝辞

A 社への訪問調査については、千葉商科大学土屋清人准教授にご配慮頂き、感謝しております。

参考文献

Anthony, R.1965.Planning and Control Systems: A Framework for Analysis. Division of Research, Graduate School of Business Administration, Harvard University, Boston. 高橋吉之助訳. 1968. 『経営管理システムの基礎』ダイヤモンド社 .

Simons, R. 1995. Levers of Control: How Managers Use Innovative Control Systems to Drive Strategic Renewal. Harvard Business School Press, Boston. 中村元一・黒田哲彦・浦島史恵訳.

榊原清則・大滝精一・沼上幹 .1989.『事業創造のダイナミクス』白桃書房 .

佐藤正隆 .2022.「制約管理に基づく中小企業経営の一考察－最適利益のための在庫管理と原価管理に係る意思決定－」『武蔵野大学経営研究所紀要』(6)：43-57.

佐藤正隆 .2023.「中小零細企業における会計的な側面によるコントロールの有効性－経営理念の浸透とコミュニケーション活動の関連から－」『産業経理』83(3)：107-122.

澤邉紀生・飛田努 .2008.「経営理念・社会関係・管理会計と企業業績に関する実態調査」『企業会計』60(12)：133-141.

澤邉紀生・飛田努 .2009.「中小企業における組織文化とマネジメントコントロールの関係についての実証研究」『日本政策金融公庫論集』（３）：73-93.

新藤晴臣・秋庭太 .2014.「外部指向型コーポレートベンチャリングに関する考察 ―ソフトバンク株式会社による関係会社創出の分析―」『日本ベンチャー学会誌』（24）：27-42.

牧野功樹 .2020.「中小企業の管理会計研究―システマティック・レビューによる統合の試み―」『管理会計学』28(1)：71-95.
牧野功樹 .2021.「中小企業におけるマネジメント・コントロール・システムの導入要因とその経済的帰結」『原価計算研究』45（2）：53-67.
横尾陽道 .2004.「企業文化と戦略経営の視点：「革新志向の企業文化」に関する考察」『三田商学研究』47 (4)：29-42.
横田絵理・乙政佐吉・坂口順也・河合隆治・大西靖・妹尾剛好 .2016.「マネジメント・コントロールの分析枠組みから見た管理会計研究－文献分析による検討」『原価計算研究』40（2）：125-138.