The Josai Journal of Business Administration (2022), Vol. 18, No. 1, 1−19

サイバーリスク管理の効率化と戦略的意思決定のための一考察

辻　智佐子・足立　照嘉・辻　俊一

要　旨

経済学におけるリスクの定義は一様ではないが，リスクが「危険」という負の側面だけでなく，「機会」という正の側面も内包するものとして理解されている。情報・デジタル技術の急速な進展は，それによって享受される機会と同時に，従来の外部環境および内部環境における情報すべてに新たなリスクを付加しようとしている。それがサイバー空間でのリスクであり，いわゆるサイバーリスクである。企業活動の国際化・ボーダレス化・ネットワーク化，それによるリスクの巨大化・複雑化の中で，企業は生き残りをかけて組織の舵取りをしなければならない。

本稿では海外の事例をとおして，サイバーセキュリティ対策を戦略的リスクマネジメントとして組み入れることを提案し，サイバーリスク管理を戦略的意思決定に取り入れるための方法について考え，そして経営戦略とリスクマネジメントの関係について新たな視点を提示した。

キーワード：サイバーリスク，リスクマネジメント，サイバーセキュリティ，経営戦略，クラウド・コンピューティング

1. はじめに

本稿は，日進月歩の高度情報化社会において企業のサイバーセキュリティを「対策」から「戦略」へと転換すべきであることを事例分析によって提案し，経営戦略とリスクマネジメントの関係について新たな視点を提示するものである。

そもそもリスクとは何か。リスクは，日本語では一般に「危険」と訳され「何か悪いことが起こる可能性」を意味しているため，負のイメージが強い。しかし，人類の歴史は自然現象や人間の行為に起因するリスクの連続であり，それを克服することで文明が誕生し，技術が進歩してきたとも言える。科学が発達を遂げるにつれて，リスクの概念は，甘んじて受け入れるものではなく，リスクを情報として定量的に評価し何か悪いことが起こる可能性を回避や軽減，あるいは移転，場合によっては受容することで，完全ではないがコントロールするものに変わってきた(1)。この意味で，リスクの概念は時代や風土によって影響を受けるが，情報が重要な鍵を握る。

封建社会から市場経済社会へ移行し，重商主義，重農主義をへて経済的自由主義が浸透する中で科学としての経済学が確立し，大量生産体制の確立と大企業の台頭をきっかけに企業組織を分析対象とした経営学が経済学から派生した。両学問においてリスクと情報がどう捉えられているかについては，市場経済の発達と経済のグローバル化と無関係ではなく，その度合いが増し社会が複雑化していく過程で議論が活発化してきた。

経済学では，とりわけ戦後においてリスクと情報に関する論考が積み重ねられていくが[2]，その中で，まず注目したいのはアローの「リスク負担に関する研究」（1951 年）である。アローは，社会の集団的選択における重要な定理を構築した経済学者であり，同論文はリスクや情報，不確実性を議論の中心に据え，個人の合理的行為と集団的選択の関連について考察している。次に，アカロフの「レモン市場：品質不確実性と市場メカニズム」（1970 年）である。アカロフは，市場の失敗を情報と関連付けて理論化した経済学者であり，同論文はレモン市場を事例に情報の非対称性がリスクを生むことを明らかにしている。いずれも経済学におけるリスクと情報に関する洞察に富む研究として，現在もなお繰り返し援用されている。

経済学におけるリスクの定義は一様ではないが，リスクが「危険」という負の側面だけでなく，「機会」という正の側面も内包するものとして理解されている。例えば，リスクと情報について経済学の視点から研究を行っている酒井泰弘は，「状態の如何によって，1 つの行為から複数個の結果が生まれることを指す。それは人間の生活維持や社会経済に対して，プラスとマイナスの両側面を持つ。リスクが大きいとは，複数の結果の間で変動の幅が大きく，また結果の程度が大きいことを意味する」と定義している（酒井［2004］）。

一方の経営学では，戦前にも企業の抱えるリスク問題に着目した研究は見られるが[3]，戦後に焦点を当てると，ギャラガーの「リスクマネジメント：コスト管理の新局面」（1956 年）は，企業を取り巻くリスクに対してどの程度のコストをかけるべきかを論じており，企業におけるリスク管理の問題に注目している。その後 1960 年代に入り，リスクを純粋リスクと投機的リスクの 2 つに分ける考え方が生まれ，その代表的研究がメアー＆ヘッジスの『企業におけるリスクマネジメント』（1963 年）とウィリアムス＆ヘインズの『リスクマネジメントと保険』（1964 年）である（亀井［2018］28-29 頁）。これらの研究をとおして純粋リスクをめぐる保険管理論の基礎が築き上げられた。1990 年代以降になると，リスクの概念がより広く定義されるようになり，投機的リスクを含めたリスクが企業の成長機会と結び付けられ[4]，また同時に「Value at Risk（VaR）」や「Key Risk Indicators（KRIs）」などのリスク評価における分析手法が登場した（Palermo［2017］p. 139）。こうした流れを経て，経営学ではリスクは企業価値を高め企業を発展させる上で重要なマネジメントの 1 つとして位置付けられ，その後もリスクマネジメントの機能や方法，理論について研究が重ねられている。

このように，経営学におけるリスクは，経済学と同様に「危険」と「機会」の両面を含んでおり，また企業のマネジメントの側面から捉えられている。その定義は様々であるが，例えば，米国の COSO[5] が 2004 年に「エンタープライズ・リスクマネジメント（ERM）」を公表した際の定義では，リスクは「ある事象が発生した場合に，目的の達成に不利な影響を及ぼす可能性」であり，リスクを統制する活動は「目的の達成に対するリスクを低減させる経営者の指示が確実に実行されるのに役立つ方針および手続を通して確立される行動」であるとしている（COSO［2013］11 頁）。COSO の取り組みは，エンロンの粉飾決算事件など一連の企業不正問題を背景に着手され，企業の内部統制にリスクマネジメントが盛り込まれる契機となった。

リスク統制にはリスク評価とその評価に基づいた意思決定が必要であるが，リスクを軽減するにしろ機会に転化するにしろ，その根拠となるのが情報である。では企業が考慮しなければならない情報にはどのようなものがあるのか。企業を取り巻く環境には大きく分けて外部環境と内部環境がある。まず外部環境は，PEST 分析に沿って整理すると 4 つの要素がある[6]。1 つに政治である。政治は，会計制度・税制度など多様な法制度や政治・外交・経済政策など社会全体のルールや目的を決定する。2 つに

経済である。経済は，景気動向や物価状況，為替，貿易収支，賃金・労働力など市場に影響を与える。3つに社会である。社会は，人口構成，文化・歴史，教育などの社会変化に関わっている。4つに技術である。技術は，生産・流通プロセスにおける新技術（イノベーション）のみならず，経済活動全体にインパクトを持つ情報技術（インターネット，デジタル，AI，シンギュラリティ等）に関連している。企業は，少なくともこれら4つの要素に係る情報に対応しなければならない。次に内部環境は，主に企業の経営資源である人（人材，組織等），モノ（製品，技術等），カネ（資金，資産等），情報（企業ノウハウ，顧客データ，無形資産等）に関わる要素のことである。これらの企業内部の複雑な情報を分析するための主な分析手法として，バリューチェーン分析やVRIO分析，PPM分析などがある(7)。

以上のように，企業のリスクマネジメントにおいて対象とする情報は多岐に渡るが，情報・デジタル技術の急速な進展は，従来の外部環境および内部環境における情報すべてに新たなリスクを付加しようとしている。それがサイバー空間でのリスクであり，いわゆるサイバーリスクである（図）。サイバーリスクとは，コンピューターウィルス，外部・内部からの不正アクセス，ソフトウェアの脆弱性，ネットワークセキュリティの脆弱性，IDおよびパスワードの漏えい，従業員などによる情報の持ち出しなどから生じるリスクのことである(8)。日本では2015年1月「サイバーセキュリティ基本法」(9)が施行され，これに基づいて2015年9月に「サイバーセキュリティ戦略」が閣議決定されたが，企業レベルで欧米諸国並みにサイバーリスクをリスクマネジメントし，企業価値を高めるべく戦略的かつ積極的に受け止めているところは少ない(10)。

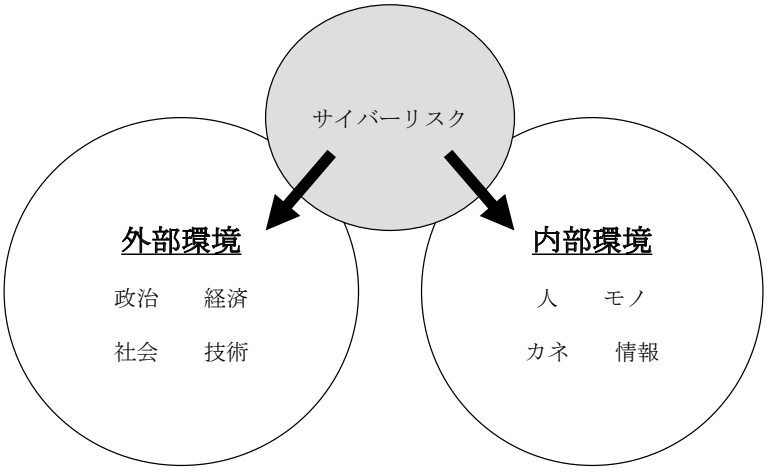

図　企業を取り巻く環境とサイバーリスク

サイバー空間におけるリスクは，他のリスクと同じように企業にとって「危険」と「機会」の両面を持ち合わせている。現状では「危険」の側面がクローズアップされており，実のところ昨今のサイバー攻撃による被害は年々増加傾向にある。東京商工リサーチの調べでは，2021年に上場企業とその子会社で個人情報漏えい・紛失の被害を受けたのは120社を数え，3年前の2019年に比べるとおよそ2倍の増加である。また，2012年から2021年の累計では496社となり，全上場企業の1割を占める（東京商工リサーチ［2022］）。間近の事例を挙げると，2020年に三菱電機，NEC，NTTコミュニケーションズで不正アクセスが原因で防衛関連情報が外部へ流出した可能性がわかっており，2021年には全日空で不正アクセスによりマイレージクラブのプレミアムメンバーの情報が漏えいしたり，デンソーのメキシコ工場でマルウェア被害を受けて多額の身代金を要求されたり，さらに2022年（3月時点）にはト

ヨタ自動車の取引先である小島プレス工業でマルウェア被害を受けたためトヨタ自動車の国内 14 工場が稼働停止したり，森永製菓で不正アクセスにより商品の製造や販売に使うシステムの一部に障害が起きたりした。防衛関連企業やグローバル企業においてより大きな被害が出ているが，今後他の産業分野や中小企業などにもサイバーリスクは及ぶと考えられている。

日本の現状を踏まえると，今のところサイバーリスクの「危険」の方に注意が払われているが，企業活動の国際化・ボーダレス化・ネットワーク化，それによるリスクの巨大化・複雑化の中で，企業は生き残りをかけて組織の舵取りをしなければならず，英国などのヨーロッパ諸国の事例に見るように，サイバーセキュリティ対策を企業の経営戦略，つまり競争優位の発揮として位置付けることが，これからの時代を生き抜くには不可欠である。

以上のことを踏まえ，本稿では海外の事例をとおして，サイバーセキュリティ対策を戦略的リスクマネジメントとして組み入れることを提案する。第 2 節では，ドイツおよび英国における事例分析を行い，サイバーリスク管理を戦略的意思決定に取り入れるための方法について考えていく。

2. サイバーリスク管理を戦略的意思決定に

組織や社会は，複雑でシステム化された災害リスクへの挑戦を強めており，その中でリーダーは不確実性の高い条件下で戦略的な意思決定を行わなければならない。しかし現状では，さまざまな形式の評価間のベンチマークを提供できる使いやすいモデルが欠けている。ペスカロリの研究では自然災害や防災を題材としているが（Pescaroli［2020］），サイバーリスクの評価とサイバーセキュリティの標準も同様ではないだろうか。各政府機関や米国国立標準技術研究所（NIST：National Institute of Standards and Technology，以下 NIST）などの標準化組織や団体(11)などから多様な評価手法や標準などが提示されており，これらを活用することで経営判断を効率化することができる。しかし，時としてこれらの評価や標準に対応していくことが，企業や組織にとって足枷となる状況もある。

なぜ多様な評価手法や標準などが足枷となってしまうのか。それは現代のビジネス環境がグローバルに相互接続され，企業や組織が参照または対応しなくてはならない標準や認証が複数要求されることがあり，このことで工数やコストの負担が増大しているからである。加えて，それら複数の標準や認証には重複した項目も多い。

このような問題は，ドイツの自動車産業においてもかつては存在していた。2014 年以降，アウディ，BMW，メルセデスベンツなどのドイツ自動車メーカーは，情報セキュリティ基準を満たしていることを定期的に証明するということをサプライヤーに対して要求するようになった。しかし，サプライヤーにおいては対応のための手間やコストが取引関係のある自動車メーカーごとに発生しており，さらに要求事項の重複もあるものの個別に対応する必要があった。

こうした状況の解決策として，ドイツ自動車工業会（VDA：Verband dear Automobilindustrie e.V.，以下 VDA）が，2017 年にすべての VDA 会員企業である自動車メーカーやサプライヤーが認める基準として，情報セキュリティの評価交換制度である情報セキュリティ審査基準（TISAX：Trusted Information Security Assessment Exchange，以下 TISAX）を策定した。TISAX では，VDA 情報セキュリティ評価（ISA：Information Security Assessment，以下 ISA）を共通の評価基準とし，情報セキュリティに関する管理の実装と成熟度をプラットフォーム上で共有することができる。その結果，サプライチェーン全体のセキュリティ基準を確保すると共に，サプライヤーが個別に対応することによる

工数やコスト，重複した評価項目へのその都度の対応といった工数の増加やコスト負担を軽減することに繋がった。また，サプライヤーが既存の取引として，例えばBMWと行なっており，新たにアウディとの新規取引を開始する場合などにも，TISAXでの評価をプラットフォーム上で共有するだけでよくなるため，新規取引先への対応が容易になるという利点もある。従来は，新規取引先のISAを満たしていることを証明するために，あらためて数ヶ月の期間を要して準備する必要があった。

自動車メーカー別に見ていくと，2017年2月にBMWが購買条件としてTISAXラベル取得をサプライヤーに求め始めた。2018年以降順次，TISAXはドイツのすべての自動車メーカーとの取引に必須の要件となっている。TISAXが要求されるサプライヤーの対象としてはドイツ系か，日系かということは問わない。

このような発想がドイツから生まれた背景について述べたい。ドイツでは，ドイツ工学アカデミーと連邦教育科学省によって「Industry 4.0」が2011年に提言されて以降，サプライチェーン全体のデジタル化，ネットワーク接続，自動化などが行われていくことを目指して，産業界で各種取り組みが行われてきた。しかし，サプライチェーンにおける上位レイヤーの企業では投資できているが，下位レイヤーにいくほど対応についていけないといった課題もあった。自動車業界においても自動車メーカーが異なればIT基盤も異なるが，「Industry 4.0」のデータモデルに自動車メーカーが準拠することで，サプライヤーはITへの二重投資を防ぐことが期待された。しかし，サプライヤーを含めたネットワークへの接続は，同時にサイバーリスクを抱えてしまう要因の1つにもなりえる。「TISAX Participant Handbook」においては，具体的に次のように記している（Gleich［2022］）。

> あなたのパートナーを想像してください。彼らは機密情報を持っています。彼らは，その情報をサプライヤーであるあなたと共有したいと考えています。あなたとパートナーとの間の協力関係は，価値を生み出します。パートナーがあなたと共有する情報は，この価値創造において重要な役割を果たします。したがって，パートナーはその情報を適切に保護することを望んでいます。そして，パートナーは，あなたが自分の情報を同じように慎重に扱っていることを確かめたいと考えています。
>
> しかし，自分の情報がきちんと管理されていると，どうすれば確認できるのでしょうか。ただあなたを「信じる」だけではだめなのです。パートナーは，何らかの証拠を見る必要があるのです。
>
> ここで，2つの疑問が生じます。情報の「安全な」取り扱いとは何か，誰が定義するのか。そして次に，それをどのように証明するのか？（日本語訳：筆者）

このように業界内で共通化した評価指標とそれを示すための仕組みにより，個別に評価を行うことによる工数やコストだけでなく，共通した基準によって効率的な意思決定をサポートすることが可能であると考えられる。

ドイツでのTISAXのように共通の評価制度を設けるものとして，英国では英国政府機関である国家サイバーセキュリティセンター（NCSC：National Cyber Security Centre，以下NCSC）とその運営委託を請け負っているIASMEコンソーシアムによって提供されているサイバーエッセンシャルズ（CE：Cyber Essentials，以下CE）や，日本ではサイバーリスク総合研究所の開発したCRRIC（Conflict and Resilience Research Institute）を産業別にカスタマイズし，自動車産業でのサプライチェーンの評価などに用いられているといった事例がある。

そこで本稿では，効率的なサイバーセキュリティ状況の評価と効果的な対策・対応に取り組むための意思決定に際し，TISAX および CE とその他の評価や標準などとの比較を通して，事例分析を行うこととする。

3. 事例分析：TISAX によるドイツ自動車産業での取り組み

TISAX における評価は，VDA ISA の 4 つの基準カタログに基づいて実施されている。

1） 情報セキュリティ
2） サードパーティへの接続
3） データ保護
4） 試作品の保護

情報セキュリティの基準カタログには，ISO/IEC27001（情報セキュリティマネジメント）に規定された情報セキュリティマネジメントシステム（ISMS：Information Security Management System）の必須要件が含まれている。一般に認められているセキュリティ基準に基づいてデータと情報を保護するための対策の共通フレームワークを作成することで，プロセスに関与するすべての関係者の総コストを削減できるためとしている。同時に，サイバーセキュリティに関する意思決定の効率化も実現できると考えられる。

ISA を行うための質問表は現在バージョン 5.1.0 が提供されているが（ENX［2022］），2019 年 5 月に更新されたバージョン 4.1.1 以降では「データ保護」モジュールとして，サービス・プロバイダが GDPR 第 28 条を適用することを求めている。なお，GDPR 第 28 条では「処理者」について定義している（European Union［2016］）。VDA ではこの基準カタログにおけるデータ保護の原則として，データ保護の原則は透明性，自律性，データセキュリティの 3 つのコアポイントを定義している（Scheibach［2017］）。また，すべての目的における TISAX の評価で，上記 1）の情報セキュリティは必須とされている。

VDA ISA のセキュリティコントロールは，「ISO27001 Annex A」の「情報セキュリティ管理」と非常に類似していると言われる。これは ISA のセキュリティコントロールが「ISO27001」の要素に加えて，サードパーティとの接続，試作品の保護，データ保護といったセキュリティ管理を追加したものとなっているためである。ただし，TISAX では要件ごとに成熟度レベルを使用して有効性を示し，さらに要件ごとに目標成熟度を定義しているが，「ISO27001」には成熟度レベルという概念そのものが存在しない。「ISO27001」では，リスク評価で特定されたリスクに必要なセキュリティコントロールだけを実装すればよいとしている。

逆に TISAX では，「ISO27001」のように PDCA は必須としていない。ISA の要求事項に焦点を当てるだけで十分であるとしている。

ここから見えてくることは，ドイツの自動車産業界で統一された共通の評価基準を構築するという試みにおいて，「ISO27001」と多くを共有した評価基準が設けられているということである。

4. 事例分析：CE による英国での取り組み

2014 年 6 月，英国政府は CE スキームの開始を発表した（National Cyber Security Centre［2014］）。このスキームは，政府と保険業界との共同作業によって以下の 2 つの機能を果たすために開発されている。

1） インターネットベースの脅威によるリスクを軽減するために，「すべての組織が実施すべき基本的な技術的コントロール」を明確に記述し奨励すること
2） 企業が顧客，取引先，保険会社などに対して，サイバーリスクに対する本質的な予防策を講じたことを証明するための担保となること

2015 年に英国政府が実施した調査によると，22％の中小企業においてサイバーセキュリティを「どこから始めるべきかわからない」との回答があった（Home Office, Cabinet Office［2015］）。このことからも，CE の活用による中小企業も含めたサイバーセキュリティ対策推進に期待が持たれており，サイバーリスクにおいて最重要課題の 1 つでもあるサプライチェーンリスクに対しても効果的な取り組みであることが考えられる。

英国政府では 2014 年 10 月以降，個人データの取り扱いや ICT 製品・サービスに関わる政府の調達案件において，入札企業への CE 認証の取得を義務付けている。また，2016 年 1 月以降，英国国防省（MoD）の請負業者についても入札の第一段階として CE 認証の取得を義務付けるとともに，250 人以上の従業員を抱え各自がネットワーク接続機器を使用している組織については，サイバーエッセンシャルズプラス（以下 CE+）認証の取得を強く求めている（Defence Contracts International［2014］）。

これらの取引において CE 認証の取得を求める理由の 1 つとしては，認証を実現するために必要な要件によって，一般的なサイバー攻撃の 8 割からビジネスを保護できるためとしている。また，CE+ については脆弱性への評価と組織的な対応まで含められていることから，前述した取引において認証取得が強く求められているという背景がある。

CE の評価プロセスでは，以下の 5 つの技術的な領域が存在している必要があり，認定を受けるために組織はすべての要件を満たす必要がある。ここで特定されている 5 つの領域は，企業における 80％以上，中小企業においては 99.3％におけるインシデントを引き起こす原因を生み出しているため（Brigantia［2014］p. 1），これらの課題に対する意思決定の負荷を軽減させるものとして考えられる。

1） ファイアウォール（Firewalls）：
　安全かつ必要なネットワークサービスだけが，インターネットからアクセスできるようにする
2） 安全な構成（Secure Configuration）：
　コンピュータとネットワークデバイスが，固有の脆弱性度合いを低下させられるように構成されていることを確認する
3） ユーザーアクセス制御（User Access Control）：
　ユーザーの役割を実行するために必要なアプリケーションにアクセスできるようにし，ユーザーアカウントが承認された個人にのみ割り当てられるようにする

4） マルウェア保護（Malware Protection）：
有害なコードが機密データにアクセスすることを防ぐために，既知のマルウェアおよび信頼できないソフトウェアの実行を制限する

5） 修正プログラム管理（Patch Management）：
デバイスやソフトウェアが，パッチや修正プログラムが利用可能となっている既知のセキュリティ問題に対して脆弱でないことを確認する

これらの観点からCEでは，内部のエンドユーザーデバイスに関して自己申告で評価を実施している。また，CE+では外部環境に面しているシステムすべてに対して，脆弱性スキャンツールによる外部からの診断と，内部のエンドユーザーデバイスを無作為に抽出してツールによる診断を実施する。後者はファイアウォールの内側であるため，ファイアウォール・スキャンと表記されていることもある。無作為での抽出は一般的に，全体の10%程度を対象とすることが多い。

CEとCE+との評価の違いであるが，日本語で公開されているCEに関する情報において「内部デバイスを自己診断」というところを，「内部スキャン」と「自己診断」の2つに分けてしまっている誤訳が散見されるため注意が必要である。

CEの評価を受けるにあたって，チェックリスト（National Cyber Security Centre［2022］）により，既にどの程度の進捗状況にあるのかを把握することができる。チェックリストの項目は次のとおりである。

1） インターネット接続を保護するためにファイアウォールを使用する
□ ファイアウォールとは何かを理解する
□ 個人と境界ファイアウォールの違いを理解する
□ 使用中のオペレーティングシステムに付属のファイアウォールを見つけてそれを有効にする
□ ルーターに境界ファイアウォール機能があるかどうかを調べ，それを有効にする

2） デバイスとソフトウェアに最も安全な設定を選択する
□「設定」の意味を理解する
□ 使用中のデバイスの設定を見つけ，必要のない機能を無効にする
□ 頻繁に使用するソフトウェアの設定を見つけ，不要な機能を無効にする
□ パスワードに関するNCSCのガイダンスを読む
□ 未だにパスワードで満足していないか確認する
□ 二要素認証に関する記事を読む

3） あなたのデータやサービスにアクセスできる人を管理する
□ アカウントと権限に関する記事を読む
□「最小権限」の概念を理解する
□ あなたのマシンで誰が管理権限を持っているのかを知る
□ 管理者の作業として何が重要かを知る
□ デバイスに最小限のユーザーアカウントを登録する

4） ウイルスやその他のマルウェアから身を守る

□ マルウェアとは何か，それがどのようにしてデバイスに侵入する可能性があるのかを知る
□ マルウェアから保護するための３つの方法を特定する
□ アンチウイルス・アプリケーションに関する記事を読む
□ デバイスの１つにアンチウイルス・アプリケーションをインストールし，ウイルスをテストする
□ Google Play や Apple App Store など，アプリを購入するための安全な場所を調査する
□「サンドボックス」とは何かを理解する

5） デバイスとソフトウェアを最新の状態に保つ

□「パッチ」とは何であるかを知る
□ すべての端末のオペレーティングシステムが自動更新に設定されていることを確認する
□ 定期的に使用する一部のソフトウェアを自動更新に設定するよう試みる
□ 現在サポートされていないすべてのソフトウェアをリストアップする

TISAX では「ISO27001」との類似性について触れたが，CE の場合は「ISO27001」にてカバーされている管理面での対応はカバーしていない。逆に，CE では脆弱性スキャンツールとして PCI ASV（Payment Card Industry Approved Scanning Vendor）[(12)] を用いていることや，PCI DSS（Payment Card Industry Data Security Standard）[(13)] の多くの要件にも適合しているため，CE と PCI DSS との違いについて注目されることが多い。いずれも，セキュリティ管理を明確に説明しており，最小限の管理措置を定めていること，外部からの技術的な脆弱性スキャンを実施することを求めていることなど，類似性もある。ただし，CE と PCI DSS とでは評価範囲に違いがあり，その点については認識しておく必要がある。CE と PCI DSS との要件の違いを整理すると，表１のようにまとめられる。

表１ Cyber Essentials と PCI DSS での対象領域の違い

CE	PCI DSS
1）境界ファイアウォールとインターネットゲートウェイ	1）カード名義人のデータを保護するためのファイアウォール設定をインストールして維持する
1）境界ファイアウォールとインターネットゲートウェイ 2）セキュアな設定 3）ユーザーアクセス制御	2）システム・パスワードおよびその他のセキュリティー・パラメーターには，ベンダー提供のデフォルトを使用しない
	3）保存されたカード名義人データの保護
	4）オープンなパブリックネットワークを介してカード名義人データの伝送を暗号化する
4）マルウェア対策	5）すべてのシステムをマルウェアから保護し，ウイルス対策ソフトウェアまたはプログラムを定期的に更新する
5）パッチ管理	6）安全なシステムとアプリケーションの開発と維持
3）ユーザーアクセス制御	7）企業が知る必要のあるカード会員データへのアクセスを制限する
3）ユーザーアクセス制御	8）システムコンポーネントへのアクセスを識別し，認証する

	9）カード名義人データへの物理的なアクセスを制限する
	10）ネットワークリソースおよびカード名義人データへのすべてのアクセスを追跡し，監視する
2）セキュアな設定 5）パッチ管理 技術的な脆弱性のスキャン	11）セキュリティシステムとプロセスを定期的にテストする
	12）すべての従業員の情報セキュリティに対応するポリシーを維持する

出典：筆者作成。

CE では，最も一般的なインターネット経由での脅威に対してコンピュータ，IT システム，ネットワークデバイスの保護に焦点を当てており，インターネットからアクセス可能なコンピュータや IT システムを保護する必要性を強調している。

PCI DSS では，重要なすべての情報資産を保護するのではなく，ペイメントカードデータに焦点を当てているため，技術的な制御だけでなく，物理的，手続き的または人に関連する脅威や脆弱性に対する保護に関するものも含まれており，「カード名義人データの機密性の確保のみ」に集中している。

5. 比較による一般化

TISAX と CE とを見ていく中で，TISAX と CE の内容を検討し，TISAX が「ISO27001」と，CE が PCI DSS と多くを共有していることが確認できた。この「ISO27001」と PCI DSS とが出揃った時に思い出されるのが GDPR である。

GDPR では全 99 条ある条文の中で，具体的な対策の仕方や要件などは定めていない。そこで一貫して説かれているのは，「技術的対応と組織的対応」の重要性であり，その具体的な対応については示していない。当然，GDPR への対応とは契約書を整備することだけで実現できるものでもない。

このことが GDPR への対応を難しくしている 1 つの要因でもあるが，GDPR には前身法となる EU Directive が 1995 年に施行されてから 30 年近い判例がある。これらに基づいて，GDPR 適用対象となる企業や組織では，技術的対応として PCI DSS の要件を参照，組織的対応として「ISO27001」の要件を参照するということが，在欧企業では広く慣例的に行われている。また，GDPR は在欧企業に限った話ではない。2019 年 1 月には欧州から日本へのデータ移転に関して，欧州委員会と日本政府との間で合意に至った。また，米国においてもプライバシーシールドを欧州との間で締結することで以前よりデータ移転が可能となっていた。

これらの合意の背景としては，データ移転先の対象国に GDPR と同等の法規制が整備されていることである。つまり，GDPR は現在，実質上の世界の基準として各国の法規制にも影響を与えている。さらに，2019 年 1 月には米国会計監査院（GAO）が，米国版 GDPR 立案の必要性についてその報告書（United States Government Accountability Office［2019］）の中で言及しており，米国では現在その議論が進行中である。これらのことから，本稿では GDPR をベンチマークとし，その条文と，PCI DSS および「ISO27001」との比較をしてみたのが表 2 である。

表 2　GDPR と ISO および PCI との比較

GDPR			ISO 27002 v2013	PCI DSS
第 1 章 一般規定				
	第 1 条	対象事項及び目的	18.1.1	
	第 2 条	実体的適用範囲	18.1.1	
	第 3 条	地理的適用範囲	18.1.1	
	第 4 条	定義		
第 2 章 基本原則				
	第 5 条	個人データの取扱いと関連する基本原則	8.2, 8.3, 8.3.3, 10.1.1, 14.1.3, 14.2.5, 18.1.3, 18.2.2	6.6, 12.1, 12.2
	第 6 条	取扱いの適法性	18.1.1	
	第 7 条	同意の要件		
	第 8 条	情報社会サービスとの関係において子どもの同意に適用される要件		
	第 9 条	特別な種類の個人データの取扱い		
	第 10 条	有罪判決及び犯罪と関連する個人データの取扱い		
	第 11 条	識別を要しない取扱い		
第 3 章 データ主体の権利				
第 1 節 透明性及び手順				
	第 12 条	データ主体の権利行使のための透明性のある情報提供，連絡及び書式		
第 2 節 情報及び個人データへのアクセス				
	第 13 条	データ主体から個人データが取得される場合において提供される情報		
	第 14 条	個人データがデータ主体から取得されたものではない場合において提供される情報		
	第 15 条	データ主体によるアクセスの権利		
第 3 節 訂正及び消去				
	第 16 条	訂正の権利		
	第 17 条	消去の権利（「忘れられる権利」）	18.1.1	
	第 18 条	取扱いの制限の権利		
	第 19 条	個人データの訂正若しくは消去又は取扱いの制限に関する通知義務		
	第 20 条	データポータビリティの権利	18.1.1	
第 4 節 異議を述べる権利及び個人に対する自動化された意思決定				
	第 21 条	異議を述べる権利		
	第 22 条	プロファイリングを含む個人に対する自動化された意思決定		
第 5 節 制限				
	第 23 条	制限	18.1.1	
第 4 章 管理者及び処理者				
第 1 節 一般的な義務				
	第 24 条	管理者の責任	18.1.1	
	第 25 条	データ保護バイデザイン及びデータ保護バイデフォルト	18.1.1	6.6, 12.1, 12.2
	第 26 条	共同管理者		
	第 27 条	EU 域内に拠点のない管理者又は処理者の代理人	18.1.1	
	第 28 条	処理者	13.2.4, 15.1.1, 15.1.2, 15.1.3	
	第 29 条	管理者又は処理者の権限の下における取扱い	13.2.4, 15.1.2	
	第 30 条	取扱活動の記録		
	第 31 条	監督機関との協力	6.1.3	
第 2 節 個人データの安全性				
	第 32 条	取扱いの安全性	5.1.1, 5.1.2, 6.1.5, 7.1.1, 7.2.2, 8.2, 8.3.3, 9.1.1, 11.1.4, 11.2.4, 11.2.9, 12.1.1, 12.1.2, 12.1.3, 12.4.1, 12.6.1, 13.1.1, 13.1.2, 13.1.3, 15.1.1, 16.1.1, 17.1.2, 18.1.1, 18.2.2, 18.2.3	1.1, 1.1.1, 2.2, 2.2.2.4, 6.6, 12.1, 12.2, 12.8
	第 33 条	監督機関に対する個人データ侵害の通知	16.1.2, 16.1.3	
	第 34 条	データ主体に対する個人データ侵害の連絡	16.1.2, 16.1.3, 16.1.4	
第 3 節 データ保護影響評価及び事前協議				
	第 35 条	データ保護影響評価	11.1.4	12.2
	第 36 条	事前協議	6.1.3	
第 4 節 データ保護オフィサー				
	第 37 条	データ保護オフィサーの指名	6.1.3, 18.1.4	
	第 38 条	データ保護オフィサーの地位	18.1.4	
	第 39 条	データ保護オフィサーの職務	18.1.4	
第 5 節 行動規範及び認証				
	第 40 条	行動規範	6.1.3, 6.1.4, 18.1.1	
	第 41 条	承認された行動規範の監視	6.1.3, 6.1.4	
	第 42 条	認証	6.1.3, 6.1.4, 18.1.1, 18.2.1	
	第 43 条	認証機関	6.1.4, 18.1.1	
第 5 章 第三国又は国際機関への個人データの移転				
	第 44 条	移転に関する一般原則		
	第 45 条	十分性認定に基づく移転		

	第 46 条	適切な保護措置に従った移転		
	第 47 条	拘束的企業準則		
	第 48 条	EU 法によって認められない移転又は開示		
	第 49 条	特定の状況における例外		
	第 50 条	個人データ保護のための国際協力	6.1.3, 18.1.1	
第 6 章 独立監督機関				
第 1 節 独立的地位				
	第 51 条	監督機関		
	第 52 条	独立性		
	第 53 条	監督機関のメンバーに関する一般的条件		
	第 54 条	監督機関の設置規定		
第 2 節 職務権限，職務及び権限				
	第 55 条	職務権限		
	第 56 条	主監督機関の職務権限		
	第 57 条	職務		
	第 58 条	権限		
	第 59 条	活動報告書		
第 7 章 協力と一貫性				
第 1 節 協力				
	第 60 条	主監督機関とその他関係監督機関との間の協力		
	第 61 条	共助		
	第 62 条	監督機関の共同作業		
第 2 節 一貫性				
	第 63 条	一貫性メカニズム		
	第 64 条	欧州データ保護会議の意見		
	第 65 条	欧州データ保護会議による対立の解決		
	第 66 条	緊急の手続		
	第 67 条	情報交換		
第 3 節 欧州データ保護会議				
	第 68 条	欧州データ保護会議		
	第 69 条	独立性		
	第 70 条	欧州データ保護会議の職務		
	第 71 条	報告書		
	第 72 条	手続		
	第 73 条	議長		
	第 74 条	議長の職務		
	第 75 条	事務局		
	第 76 条	機密性		
第 8 章 救済，法的責任及び制裁				
	第 77 条	監督機関に異議を申立てる権利		
	第 78 条	監督機関を相手方とする効果的な司法救済の権利		
	第 79 条	管理者又は処理者を相手方とする効果的な司法救済の権利		
	第 80 条	データ主体の代理人		
	第 81 条	訴訟手続の停止		
	第 82 条	賠償の権利及び法的責任		
	第 83 条	制裁金を科すための一般的要件		
	第 84 条	制裁		
第 9 章 特定の取扱いの状況と関係する条項				
	第 85 条	取扱いと表現の自由及び情報伝達の自由		
	第 86 条	公文書の取扱い及び公衆のアクセス		
	第 87 条	国民識別番号の取扱い		
	第 88 条	雇用の過程における取扱い		
	第 89 条	公共の利益における保管の目的，科学調査若しくは歴史調査の目的又は統計の目的のための取扱いと関連する保護措置及び特例		
	第 90 条	守秘義務		
	第 91 条	教会及び宗教団体の既存のデータ保護規則		
第 10 章 委任される行為及び実装行為				
	第 92 条	委任される行為の執行		
	第 93 条	委員会の手続		
第 11 章 最終規定				
	第 94 条	指令 95/46/EC の廃止		
	第 95 条	指令 2002/58/EC との関係		
	第 96 条	既に締結された協定との関係		
	第 97 条	欧州委員会の報告書		
	第 98 条	データ保護に関する EU の他の法的行為の見直し		
	第 99 条	発効及び適用		

出典：Article of GDPR より作成。また，条項の日本語訳は JETRO 資料より引用。

表2から読み取れることは，PCI DSSによって技術的対応，「ISO27001」によって運用面など組織的対応に該当する項目をカバーできていることが分かる。日本の企業や組織においては，NISTの標準が参照されることも多い。そこで，NISTの「NIST Cyber Security Framework, NIST SP800-171, NIST SP800-53」といった日本の企業や組織において参照されることの多い標準との比較を追加したものが表3である。

表3　GDPRとISO，PCIおよびNISTフレームワークとの比較

GDPR			ISO 27002 v2013	PCI DSS	NIST CSF	NIST 800-171 rev1	NIST 800-53 rev4
第1章 一般規定							
	第1条	対象事項及び目的	18.1.1		ID. GV-3, PR. IP-5		PM-8
	第2条	実体的適用範囲	18.1.1		ID. GV-3, PR. IP-5		PM-8
	第3条	地理的適用範囲	18.1.1		ID. GV-3, PR. IP-5		PM-8
	第4条	定義					
第2章 基本原則							
	第5条	個人データの取扱いと関連する基本原則	8.2，8.3，8.3.3，10.1.1，14.1.3，14.2.5，18.1.3，18.2.2	6.6, 12.1, 12.2	DE．DP-5，PR. DS-1，PR. DS-2，PR. DS-8, PR. IP-7	3.8.6, 3.12.1, 3.12.2，3.12.3，3.12.4，3.13.1，3.13.2，3.13.8，3.13.11，3.13.16，13.2.3，NFO	AP-1, AR-7, CA-2, CA-7, CA-7(1), DI-2, DM-1, DM-2, DM-3, MP-1, MP-6(9), MP-7, PL-9, PM-8, PM-14, SA-8, SA-13, SC-7(18), SC-8, SC-8(2), SC-9, SC-13, SC-13(1), SC-16(1), SC-28(1)(2), SC-42(2)(4)(5), SI-1, SI-2(7), SI-7(6), SI-12, UL-1
	第6条	取扱いの適法性	18.1.1		ID. GV-3, PR. IP-5		AR-3, IP-1, SA-9(5), SC-36, UL-2
	第7条	同意の要件					IP-1
	第8条	情報社会サービスとの関係において子どもの同意に適用される要件					IP-1
	第9条	特別な種類の個人データの取扱い					UL-1
	第10条	有罪判決及び犯罪と関連する個人データの取扱い					UL-1
	第11条	識別を要しない取扱い					DM-1，DM-3，TR-1，UL-1
第3章 データ主体の権利							
第1節 透明性及び手順							
	第12条	データ主体の権利行使のための透明性のある情報提供，連絡及び書式					IP-1，IP-2，IP-3，TR-1
第2節 情報及び個人データへのアクセス							
	第13条	データ主体から個人データが取得される場合において提供される情報					IP-2, TR-1, AP-2
	第14条	個人データがデータ主体から取得されたものではない場合において提供される情報					IP-1, IP-2, IP-3, TR-1, AP-2
	第15条	データ主体によるアクセスの権利					IP-2, UL-2
第3節 訂正及び消去							
	第16条	訂正の権利					IP-2, IP-3
	第17条	消去の権利（「忘れられる権利」）	18.1.1		ID. GV-3, PR. IP-5		PM-8
	第18条	取扱いの制限の権利					DM-1, DM-2, DM-3, IP-3, IP-4, UL-1
	第19条	個人データの訂正若しくは消去又は取扱いの制限に関する通知義務					IP-4
	第20条	データポータビリティの権利	18.1.1		ID. GV-3, PR. IP-5		PM-8, UL-2
第4節 異議を述べる権利及び個人に対する自動化された意思決定							
	第21条	異議を述べる権利					DM-2, IP-4
	第22条	プロファイリングを含む個人に対する自動化された意思決定					IP-4
第5節 制限							
	第23条	制限	18.1.1		ID. GV-3, PR. IP-5		PM-8
第4章 管理者及び処理者							
第1節 一般的な義務							
	第24条	管理者の責任	18.1.1		ID. GV-3, PR. IP-5		PL-9, PM-8
	第25条	データ保護バイデザイン及びデータ保護バイデフォルト	18.1.1	6.6, 12.1, 12.2	ID. GV-3, PR. IP-5		PL-9, PM-8
	第26条	共同管理者					AR-3, IP-2, IP-3, IP-4, SA-9(5), SC-36, TR-1, UL-2
	第27条	EU域内に拠点のない管理者又は処理者の代理人	18.1.1		ID. GV-3, PR. IP-5		PM-8

	第 28 条	処理者	13.2.4, 15.1.1, 15.1.2, 15.1.3		ID. SC-1, ID. SC-3, ID. SC-4	NFO	AR-3, SA-4, SA-9(3), SA-9(5), SA-12, SC-36
	第 29 条	管理者又は処理者の権限の下における取扱い	13.2.4, 15.1.2		ID. SC-3		AR-3, SA-9(3), SA-9(5), SC-36
	第 30 条	取扱活動の記録			ID. AM-3		AR-8, PL-2, SA-5 (1)(2)(3)(4)
	第 31 条	監督機関との協力	6.1.3				AR-6, IR-6
第 2 節 個人データの安全性							
	第 32 条	取扱いの安全性	5.1.1, 5.1.2, 6.1.5, 7.1.1, 7.2.2, 8.2, 8.3.3, 9.1.1, 11.1.4, 11.2.4, 11.2.9, 12.1.1, 12.1.2, 12.1.3, 12.4.1, 12.6.1, 13.1.1, 13.1.2, 13.1.3, 15.1.1, 16.1.1, 17.1.2, 18.1.1, 18.2.2, 18.2.3	1.1, 1.1.1, 2.2, 2.2.2.4, 6.6, 12.1, 12.2, 12.8	DE. CM-1, DE. DP-1, DE. DP-2, ID. BE-2, ID. GV-1, ID. GV-3, ID. GV-4, ID. RA-1, ID. SC-1, ID. RM-1, ID. RM-2, ID. RM-3, PR. AT-1, PR. AT-3, PR. AT-4, PR. DS-4, PR. IP-5, PR. IP-9, PR. IP-11, PR. IP-12, PR. PT-1, PR. PT-4RC. RP-1	3.9.1, 3.9.2, NFO	AC-1, AR-4, AT-1, AU-1, CA-1, CA-2, CM-1, CM-3, CM-9, CP-1, CP-2, IA-1, IR-1, IR-4(3), MA-1, MP-1, MP-2, PE-1, PL-1, PL-9, PM-1, PM-5, PM-8, PM-9, PM-10, PM-13, PM-16, PS-1, PS-3, RA-1, SA-4, SC-1, SC-5, SC-5(3), SC-38, SI-2, SI-3(2), SI-4, SI-9
	第 33 条	監督機関に対する個人データ侵害の通知	16.1.2, 16.1.3		RS. CO-2, RS. CO-3, RS. CO-5	3.6.1, 3.6.2	IR-6, SE-2
	第 34 条	データ主体に対する個人データ侵害の連絡	16.1.2, 16.1.3, 16.1.4		RC. CO-1, RC. CO-2, RC. CO-3, RS. CO-1, RS. CO-2, RS. CO-3, RS. CO-4, RS. CO-5	3.6.1, 3.6.2	IR-6, IR-7(2), IR-10
第 3 節 データ保護影響評価及び事前協議							
	第 35 条	データ保護影響評価	11.1.4	12.2	ID. RA-4, ID. RA-5	3.11.1	AR-2, PL-5, RA-3
	第 36 条	事前協議	6.1.3		ID. RA-4		IR-6
第 4 節 データ保護オフィサー							
	第 37 条	データ保護オフィサーの指名	6.1.3, 18.1.4				AR-1, IR-6
	第 38 条	データ保護オフィサーの地位	18.1.4				AR-1
	第 39 条	データ保護オフィサーの職務	18.1.4				AR-1
第 5 節 行動規範及び認証							
	第 40 条	行動規範	6.1.3, 6.1.4, 18.1.1		ID. GV-3, PR. IP-5		IR-6, AT-5, PL-9, PM-15, PM-8
	第 41 条	承認された行動規範の監視	6.1.3, 6.1.4				IR-6, AT-5, PM-15
	第 42 条	認証	6.1.3, 6.1.4, 18.1.1, 18.2.1		ID. GV-3, PR. IP-5		IR-6, AT-5, PM-15, PM-8
	第 43 条	認証機関	6.1.4, 18.1.1		ID. GV-3, PR. IP-5		AT-5, PM-8, PM-15
第 5 章 第三国又は国際機関への個人データの移転							
	第 44 条	移転に関する一般原則					SA-9(5), SC-36, UL-2
	第 45 条	十分性認定に基づく移転					SA-9(5), SC-36, UL-2
	第 46 条	適切な保護措置に従った移転					SA-9(5), SC-36, UL-2
	第 47 条	拘束的企業準則					SA-9(5), SC-36, UL-2
	第 48 条	EU 法によって認められない移転又は開示					SA-9(5), SC-36, UL-2
	第 49 条	特定の状況における例外					SA-9(5), SC-36, UL-2
	第 50 条	個人データ保護のための国際協力	6.1.3, 18.1.1		ID. GV-3, PR. IP-5		IR-6, PM-8
第 6 章 独立監督機関							
第 1 節 独立的地位							
	第 51 条	監督機関					
	第 52 条	独立性					
	第 53 条	監督機関のメンバーに関する一般的条件					
	第 54 条	監督機関の設置規定					
第 2 節 職務権限，職務及び権限							
	第 55 条	職務権限					
	第 56 条	主監督機関の職務権限					
	第 57 条	職務					
	第 58 条	権限					
	第 59 条	活動報告書					
第 7 章 協力と一貫性							
第 1 節 協力							
	第 60 条	主監督機関とその他関係監督機関との間の協力					
	第 61 条	共助					
	第 62 条	監督機関の共同作業					
第 2 節 一貫性							
	第 63 条	一貫性メカニズム					
	第 64 条	欧州データ保護会議の意見					
	第 65 条	欧州データ保護会議による対立の解決					
	第 66 条	緊急の手続					
	第 67 条	情報交換					
第 3 節 欧州データ保護会議							
	第 68 条	欧州データ保護会議					

	第 69 条	独立性					
	第 70 条	欧州データ保護会議の職務					
	第 71 条	報告書					
	第 72 条	手続					
	第 73 条	議長					
	第 74 条	議長の職務					
	第 75 条	事務局					
	第 76 条	機密性					
第 8 章 救済，法的責任及び制裁							
	第 77 条	監督機関に異議を申立てる権利					
	第 78 条	監督機関を相手方とする効果的な司法救済の権利					
	第 79 条	管理者又は処理者を相手方とする効果的な司法救済の権利					
	第 80 条	データ主体の代理人					
	第 81 条	訴訟手続の停止					
	第 82 条	賠償の権利及び法的責任					
	第 83 条	制裁金を科すための一般的要件					
	第 84 条	制裁					
第 9 章 特定の取扱いの状況と関係する条項							
	第 85 条	取扱いと表現の自由及び情報伝達の自由					
	第 86 条	公文書の取扱い及び公衆のアクセス					
	第 87 条	国民識別番号の取扱い					
	第 88 条	雇用の過程における取扱い					
	第 89 条	公共の利益における保管の目的，科学調査若しくは歴史調査の目的又は統計の目的のための取扱いと関連する保護措置及び特例					
	第 90 条	守秘義務					
	第 91 条	教会及び宗教団体の既存のデータ保護規則					
第 10 章 委任される行為及び実装行為							
	第 92 条	委任される行為の執行					
	第 93 条	委員会の手続					
第 11 章 最終規定							
	第 94 条	指令 95/46/EC の廃止					
	第 95 条	指令 2002/58/EC との関係					
	第 96 条	既に締結された協定との関係					
	第 97 条	欧州委員会の報告書					
	第 98 条	データ保護に関する EU の他の法的行為の見直し					
	第 99 条	発効及び適用					

出典：Article of GDPR より作成。また，条項の日本語訳は JETRO 資料より引用。

ここで比較に用いた NIST Cyber Security Framework は元々，米国の重要なインフラストラクチャに関連するリスク管理を改善するために開発されたもので，既存の標準，ガイドラインおよびベストプラクティスに基づいて，サイバーリスクに対処および管理するための一連の明確なガイドラインを提供している。そして，この NIST Cyber Security Framework と「ISO27001」とでの対象領域として重複する項目が多い。

6. まとめ

今やサイバーリスクはキャッシュフローの健全性や信用格付けにも影響し，事業継続性に直接的な影響をおよぼしている。収益性や業務効率の観点からサイバーリスクを完全に排除することはできないが，損失へのエクスポージャーを最小限に抑えていかなくてはならない。

将来の不確実性を管理するには多くのツールが必要であるものの，そのうちのいくつかは同様の機能や重複する機能さえも持っており，工数やコストの増加に繋がっている。また，取締役会へのサイバーセキュリティ報告が行われている場合，さまざまな方法，ツール，プロセスが使用されているものの，報告の内容や取締役会から効果的なフィードバックを得る方法に苦労している。残念ながら多くの場合，特定のサイバーセキュリティツールの展開に焦点を合わせたツール中心のメトリクスになりがちと

いった問題もある（Dezeure et al.［2022］）。また個別企業の経営体力に応じたサイバーセキュリティが実施されないと，サプライチェーン，バリューチェーン全体のセキュリティを持続的に維持・向上させることが難しい側面もある。企業の規模や体力を勘案した戦略構築が必要になっている。ロシアのウクライナ侵攻により東アジアでも地政学的リスクが高まる中，サプライチェーン等の脆弱性攻撃対象となる可能性が高い中小企業が，持続可能で効果的なセキュリティ施策を実施できることが，国家安全保障の観点からも重要になっている。

従来の意思決定ツールは，完全で信頼できる情報にアクセスできる前提だったが，ほとんどの戦略的な意思決定は不確実性の多い中で行われている（Courtney, Lovallo and Clarke［2013］）。そして，成功を決定する変数をどの程度理解しており，重要な成功要因のどの組み合わせが意思決定を良い結果へと導くのかを理解する必要がある。

このことから，さまざまな形式による評価間のベンチマークを提供できる使いやすいモデルを確立することで，サイバーリスク管理の効率改善やコスト削減へと繋がることが考えられ，本稿では既存の標準をベースにビジネスの信頼性を確立するために開発された TISAX と CE について見てきた。サイバーリスク管理がビジネスのパラメータと直結していくことで，経営における意思決定の効率化に寄与し，企業価値を高め，持続可能な成長の源泉となる。これらのことからも，サイバーセキュリティとは対策ではなく戦略であると言える。

［文責：第 1 節 辻（智），第 2・3・4・5 節 足立，第 6 節 辻（俊）］

謝　辞

Dr. Emma Philpott MBE（英 IASME Consortium），中島一樹氏（一般社団法人 Japan Automotive ISAC），高橋秀行氏（CISSP，NTT セキュリティ・ジャパン株式会社），大河内智秀氏（CISSP，東京海上ディーアール株式会社），衣川俊章氏（CISSP，米 Security Scorecard 社）には，本研究の遂行にあたり多大なご助言，ご協力頂きました。厚く御礼申し上げます。

注

（1） 例えば，科学が発達した現代社会において地震などの自然災害から生じるリスクは，過去のデータを蓄積しそれを分析することによってある程度回避，軽減することが可能である。また，そうしたリスクに備えて保険に入り，リスクを移転することもできる。

（2） 戦前については，ナイトが「リスク，不確実性，利益」（1921 年）においてリスクを不確実性とリンクさせ，リスクを確率分布がわかるもの（リスク）とわからないもの（真の不確実性）の 2 つに分類している（ナイト［1959］）。その後，ケインズが不確実性について「雇用・利子および貨幣の一般理論」（1936 年）の中で論じているが，ナイトの学説には触れていない。

（3） 企業のリスクマネジメントの起点とされるのは戦前に発刊されたファヨールの「産業ならびに一般の管理」（1916 年）であるとされており（亀井［2018］28 頁），ファヨールは鉱山会社の技師として働いていた経験から，企業経営において自社の財産や従業員を自然災害や事故，ストライキなどの危害から守る「保全活動」が必要であることを説いた。

（4） 日本におけるリスクマネジメントの先駆者とされる片方善治と亀井利明がそれぞれの著書においてリスクを純粋リスクのみならず投機的リスクも考慮に入れるべきことを述べている（片方［1978］，亀井［1978］）。また，純粋リスクと投機的リスクの区別について武井勲は，両者間には密接な関係があるため明確に区別することは難しいが，従来のリスクマネジメントが純粋リスクを主な対象にしてきたこと，純粋リスクの方が予知しやすいこと，純粋リスクの場合企業の損失は社会全体の損失になること（投機的リスクの場合企業の損失は必ずしも社会全体の損失にはならず利益になることがある）を理由に，両者を分ける必要があると述べている（武井［1982］74 頁）。

（5） Committee of Sponsoring Organizations of the Treadway Commission の略。日本語ではトレッドウェイ委員会支援組織委員会と呼ばれ，「組織の業績や監督を改善するとともに組織における不正を減らすために立案された内部統制，全社的リスクマネジメントおよび不正抑止に関する包括的なフレームワークとガイダンスの開発を通じて先導的な考え方を提供する」ことを目的に活動している。米国会計学会（American Accounting Association），米国公認会計士協会（American Institute of Certified Public Accountants），国際財務担当経営者協会（Financial Executives International），管理会計士協会（Institute of Management Accountants），内部監査人協会（The Institute of Internal Auditors）の5つの民間団体によって支援されている（COSO［2013］）。

（6） PEST 分析は，1967 年に当時ハーバード大学教授であったアギュラーが提起したものであり，その後コトラーが体系化した（Aguilar［1967］，Kotler［1998］）。外部環境の分析手法には，PEST 分析の他に 5 フォース分析（ポーター）などがある。

（7） ポーターが考案したバリューチェーン分析は雑多にある企業活動を 1 つの価値連鎖として考え，活動ごとに強みや弱みを見つけて戦略を立てるためのフレームワーク。バーニーが提唱した VRIO 分析は Value（価値），Rarity（希少性），Imitability（模倣可能性），Organization（組織）の 4 つの視点から経営資源の強みと弱みを分析するフレームワーク。ボストンコンサルティンググループが理論化した PPM（Product Portfolio Management）は市場成長性と市場シェアの 2 つを軸として資源配分を考えるためのフレームワーク。

（8） 独立行政法人情報処理推進機構（IPA）が発表した「情報セキュリティ 10 大脅威 2021」にサイバー空間における脅威について整理されている（独立行政法人情報処理推進機構［2021］6 頁）。

（9） これを受けて 2016 年 12 月 7 日に「官民データ活用推進基本法」が成立し，また「個人情報の保護に関する法律」および「行政手続における特定の個人を識別するための番号の利用等に関する法律」の一部が改正され 2017 年 5 月 30 日に全面施行された。

(10) 日本の企業は他のアジア諸国や欧米諸国の企業に比して，サイバーリスクに対する意識は低い（総務省［2020］268-275 頁）。

(11) NIST などの標準規格を策定する公的および民間の組織の総称。

(12) クレジットカード業界のセキュリティ基準のこと。

(13) クレジットカード会員の情報を保護することを目的に定められたクレジットカード業界の情報セキュリティ基準のこと。

参考文献

〈日本語文献〉

片方善治［1978］『リスク・マネジメント：危険充満時代の新・成長戦略』プレジデント社。

亀井克之［2018］「リスクマネジメントの新たなフレームワークの試み」日本情報経営学会『日本情報経営学会誌』第 38 巻 3 号，2018 年，28-39 頁。

亀井利明［1997］『危機管理とリスクマネジメント』同文舘出版。

亀井利明［1978］『危険と安定の周辺：リスク・マネジメントと経営管理』同朋舎。

COSO，八田進二他監訳，日本内部統制研究学会他訳［2013］『内部統制の統合的フレームワーク』日本公認会計士協会出版局。

ケインズ，塩野谷祐一訳［1983］『ケインズ全集第 7 巻　雇用・利子および貨幣の一般理論』東洋経済新報社。

酒井泰弘［2004］「古くて新しい『リスクの経済学』」『経済セミナー』594 号（2004 年 7 月号），日本評論社，2004 年 6 月，14-19 頁。

総務省［2020］「第 3 章 5G 時代を支えるデータ流通とセキュリティ 第 4 節 5G 時代のサイバーセキュリティ」『令和 2 年版 情報通信白書』（https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/pdf/n3400000.pdf）。

武井勲［1982］「経営におけるリスクの性質とリスク・マネジメントの対象」富山大学経済学部『富大経済論集』第 27 巻 2 号，1982 年 2 月，202-223 頁。

東京商工リサーチ［2022］「上場企業の個人情報漏えい・紛失事件は，調査開始以来最多の 137 件 574 万人分（2021 年）」（公開日付：2022 年 1 月 17 日）（https://www.tsr-net.co.jp/news/analysis/20210117_01.html）。
独立行政法人情報処理推進機構［2021］「情報セキュリティ 10 大脅威 2021」2021 年 2 月（https://www.ipa.go.jp/files/000088835.pdf）。
ナイト，奥隅榮喜訳［1959］『危険・不確実性および利潤』文雅堂書店。
ファヨール，佐々木恒男訳［1972］『産業ならびに一般の管理』未来社。

〈英語文献〉

Aguilar, F. J., *Scanning the Business Environment*, Macmillan, 1967.
Akerlof, G., 'Market for Lemons: Quality Uncertainty and the Market Mechanism,' *Quarterly Journal of Economics*, Vol. 84, No. 3, Aug. 1970, pp. 488–500.
Arrow, Kenneth J., 'Alternative Approaches to the Theory of Choice in Risk-Taking Situations,' *Econometrica*, Vol. 19, No. 4, Oct. 1951, pp. 404–437.
Brigantia, 'What is Cyber Essentials?,' *Cyber Smart*, 2014.
Courtney, H., Lovallo, D. and Clarke, C., 'Deciding How to Decide,' *Harvard Business Review,* Nov. 2013 (https://hbr.org/2013/11/deciding-how-to-decide).
Defence Contracts International, 'What Is Cyber Essentials?,' 2014 (https://www.dcicontracts.com/cyber-essentials/).
Dezeure, F., Webster, G., Trost, J., Leverett, E., Gonçalves, J. P., Mana P., McCord, G. and Magri, J., 'Reporting Cyber Risk to Boards. CISO Edition,' *ResearchGate*, 2022, (https://www.researchgate.net/profile/Eireann-Leverett/publication/359338731_Reporting_Cyber_Risk_to_Boards_CISO_Edition/links/624189a17931cc7ccfff9ace/Reporting-Cyber-Risk-to-Boards-CISO-Edition.pdf).
ENX, 'Current Version of ISA (5.1.0),' 1 May 2022 (https://portal.enx.con/isa5-en.xlsx).
European Union, 'Article 28 Processor,' in the GDPR, *Official Journal of the European Union*, 2016 (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e3150-1-1).
Gleich, F., 'TISAX Participant Handbook,' ENX Association, 1th Feb. 2022.
Gallagher, R. B., 'Risk Management: New Phase of Cost Control,' *Harvard Business Review*, Vol. 34, May 1956, pp. 75–86.
Home Office, Cabinet Office, The Rt Hon Karen Bradley MP, and Ed Vaizey, 'Cyber security "myths" putting a third of SME revenue at risk,' gov.uk, 2015, (https://www.gov.uk/government/news/cyber-security-myths-putting-a-third-of-sme-revenue-at-risk).
Kotler, P., *Marketing Management: Analysis, Planning, Implementation, and Control* (9th ed.), Englewood Cliffs: Prentice-Hall, 1998.
National Cyber Security Centre, 'About Cyber Essentials,' 2014, (https://www.cyberessentials.ncsc.gov.uk/).
National Cyber Security Centre, 'Cyber Essentials: Requirements for IT infrastructure,' 2022 (https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure-3-0.pdf).
Palermo, T., 'Risk and Performance Management: Two Sides of the Same Coin?,' Wood, M., and Linsley, P., eds., *The Routledge Companion to Accounting and Risk*, Routledge, 2017, pp. 137–149.
Pescaroli, G., Velazquez, O., Alcántara-Ayala, I., Galasso, C., Kostkova, P. and Alexander, D., 'A Likert Scale-Based Model for Benchmarking Operational Capacity, Organizational Resilience, and Disaster Risk Reduction,' *International Journal of Disaster Risk Science*, 2020, pp. 404–409.
Scheibach, R., 'Three principles for data protection with autonomous and networked driving,' VDA, Mar. 2022 (reference date) (https://www.vda.de/en/Topics/digitization/data/datenschutz).
United States Government Accountability Office, 'Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility,' *GAO-19-52*, 2019.

Measure for Measurement: how to connect efficient cyber risk management with strategic decision-making

Chisako TSUJI・Teruyoshi ADACHI・Shunichi TSUJI

Abstract

Risk is understood as encompassing not only the negative aspect of ‘danger’ but also the positive aspect of ‘opportunity.’ The rapid development of information and digital technologies is adding new risks to all information in the traditional external and internal environment. These are the risks in cyber-space, the so-called “cyber risks.” In the context of internationalization, borderlessness and networking of business activities, and the consequent growth and complexity of risks, companies must manage their organizations to survive.

Through examples, this paper proposes incorporating cyber security measures as strategic risk management, considers ways to integrate cyber risk management into strategic decision-making, and presents a new perspective on the relationship between management strategy and risk management.

Keywords: Cyber risk, Risk management, Cyber security, Management strategy, Cloud computing