# 資料：OECD のサイバーセキュリティ政策
## ～経済・社会的影響の強調と情報共有の重視～

●本稿は OECD のサイバーセキュリティ政策を概観するための資料的意味合いを有すものであり、「概要」をお読みいただくと、OECD の政策の大まかな流れが把握できる構成になっている。

**概要：**

経済・社会分野の調査・分析、政策提言を行い、先進的な課題のグローバル・スタンダード、ルール作りを行う国際組織である OECD（経済開発協力機構）は、産業構造の変化に伴い、デジタル分野を重視している。サイバーセキュリティについても積極的にコミットする姿勢を打ち出し、ガイドライン、レポート等を公開してきた。本稿は主に 2015 年に発表されたレポートである「経済と社会の繁栄のためのデジタル・セキュリティ・リスク・マネジメントに関する提言」及び 2019 年に発表された「企業におけるデジタル・セキュリティ・リスク・マネジメント調査」に依拠し、近年の OECD のサイバーセキュリティのとらえ方、取り組み等を見ていくものである。

本稿の構成は、上記レポートを踏まえ、大きく以下の 3 点からなっている。1. OECD がなぜ「サイバーセキュリティ」という文言を使わず、「デジタル・セキュリティ」という用語を使用するのかを OECD の組織のあり方を交えて考察した後、2. デジタル・セキュリティに関して OECD が重視するポイントについて確認する。その後、3. 今後各国が、あるいはグローバルで実施する調査の原型になるであろう、2018 年に実施された、情報共有に向けたデジタル・セキュリティに関する予備調査について、反省点も含めてその内容を検証する。

OECD では現在、「サイバーセキュリティ」という文言を使わず、「デジタル・セキュリティ」という文言を使っている。サイバーセキュリティが経済・社会面に与える影響を重視し、企業にとっても IT 部門の問題ではなく経営の根幹に関わる問題であり、企業経営全体のリスクととらえるべきと考えているからである。だからこそ、ともすれば技術的な印象を与える「サイバー」ではなく、より広範かつ全体的な印象を与える「デジタル」という文言を選択している。この考え方に基づけば、デジタル・セキュリティのステークホルダーは経済・社会活動においてデジタル環境に部分的にでも依拠している組織・個人となり、ほぼすべての組織・人がそれに当てはまることになり、「自分事」となる。

OECD は、8 つの原則として①意識の向上、②責任、③人権、④連携、⑤リスク・アセスメント、⑥セキュリティの方策、⑦イノベーション、⑧準備と継続性を掲げているが、この原則に通底するのが、アクティブな経済・社会活動を行う上で、ある程度のリスクはやむを得ないという、「リスクの受容」である。経済・社会活動を重視することで、ベネフィットとリスクのバランスを考えながらのマネジメントが必要になってくる。OECD は、「すべてのステークホルダーは経済的・社会的目標の達成のためにはある程度のデジタル・セキュリティ・リスクは受容されるべきであることを理解すべき」としているが、「リスクの受容」のレベルについて判断しうるのは、企業であれば IT 部門ではなく、経営陣ということになろう。

OECD ではまた、すべてのステークホルダーが国内外問わず連携、ベスト・プラクティス、バッド・プラクティスも含めた情報共有を行うことで、それぞれが実行するリスク・マネジメントがブラッシュアップされると考えている。2018 年には欧州各国の企業のリスク担当責任者を対象とした予備調査を行った。大企業に偏り、回答率も低いなど、国際比較としてはまだ不十分なものではあったが、これを基点として、より広範に企業のデジタル・リスク・マネジメントを測定するためのフレームワークや指標が開発され、それが各国・グローバルに実施される調査のベースとなっていくことが期待されている。OECD としては、企業が他社比較を通じて自社のレベル感を知ることができるような「成熟度モデル」が必要と考えている。本モデルの開発はまだ緒に就いたばかりだが、2018 年末には、バーチャル、リアル両方でステークホルダー達が集い、情報共有を行うためのプラットフォームである「繁栄のためのデジタル・セキュリティに関するグローバル・フォーラム」が創設された。これによりデジタル・セキュリティのステークホルダー達の横のつながりがグローバルに広がり、深まることが期待される。これらの活動を通じ「成熟度モデル」がさらに議論されることで洗練され、よりよいマネジメント手法が開発・普及することが期待されている。

【はじめに：OECD とは何か】

OECD（Organization for Economic Cooperation and Development：経済協力開発機構）は 1961 年に創設された、経済・社会分野にフォーカスした国際機関である。2020 年 3 月現在、加盟国は欧米諸国、ロシア、日本、韓国など 36 カ国。OECD 加盟国が世界の GDP に占める割合は 6 割となっている。経済政策・分析、規制精度・構造改革、貿易・投資、環境・持続な開発、公共ガバナンスなど、多岐に渡る経済・社会分野において調査、分析、政策提言を行っている。OECD の活動形態は、「交渉」ではなく「議論」による政策協調や国際ルール作りを主体としており、1700 人を超える専門性の高い職員を擁した「世界最大のシンクタンク」とも呼ばれている。その存在が重要視される理由の一つは，OECD が経済・社会分野の国際的な政策協調の場であり、政策的な議論を通じて先進的な課題の「世界標準」を醸成、ルール作りがなされていくところにある（「世界のスタンダード・セッター」）。最近では，政策提言を実行に移す側面を重視し，「シンク・ドゥー・タンク」と自ら称している。加盟各国はフランス・パリにある OECD 本部に代表部を置いており、日本からは外務省、財務省、経済産業省など複数の省庁から職員が出向、これらの議論に参加している。OECD には経済、貿易、開発援助、金融、租税、企業、科学技術、環境、教育、エネルギー等に関する委員会があり、委員会と関連会合の数は 200 以上に及ぶが、近年ではデジタル分野も重視している[1]。

【OECD とデジタル】

世界標準を創り出す立場にある OECD の役割はデジタル分野においても同様であり、産官共に議論の動向を注視し、議論にも積極的に関与しようとしている。特にデジタル分野においては、1980 年に OECD 理事会が採択した『プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告』、いわゆる「OECD プライバシーガイドライン」は、個人データ（個人情報）のプライバシー保護と適正な流通のためのルールであり、このガイドラインが、日本の最初の個人情報保護法である行政機関個人情報保護法につながったという経緯がある。日本の個人情報保護のベースとなったのが OECD のガイドラインだったという事実は、OECD の影響力の大きさを日本の産業界においてもひときわ認識させるきっかけであった。1982 年には「デジタル経済政策委員会」が発足し、持続的な経済社会の発展に資する情報通信技術（ICT）政策について議論を行っている[2]。

**【OECD によるサイバーセキュリティ関連レポート】**

OECD は 1990 年代初頭からサイバーセキュリティについても積極的な姿勢を打ち出してきた。近年の OECD のレポートは邦訳がされておらず、OECD の具体的な考え方、姿勢などが日本ではわかりづらい面があったが、主なガイドライン、レポートを挙げると、1992 年の「情報システムのセキュリティのための OECD ガイドライン」（OECD Guidelines for the Security of Information Systems）[3]、2002 年の「情報システム及びネットワークのセキュリティのための OECD ガイドライン：セキュリティ文化の普及 に向けて」（OECD Guidelines for the Security of Information

---

[1] 外務省『経済協力機構と日本』https://www.mofa.go.jp/mofaj/files/000471199.pdf

[2] OECD デジタル経済政策委員会については、下記参照。なお現在の議長は総務省出身の飯田陽一氏が務めている。https://oecdgroups.oecd.org/Bodies/ShowBodyView.aspx?BodyID=1837&Lang=en

[3] https://www.oecd.org/internet/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm

Systems and Networks ： Towards a Culture of Security）[4]、2008 年の「重要通信インフラの防御に関する提言」（Recommendation of the Council on the Protection of Critical Information Infrastructures）[5]、2015 年の「経済と社会の繁栄のためのデジタル・セキュリティ・リスク・マネジメントに関する提言」（Recommendation of Council on Digital Security Risk Management for Economic and Social Prosperity）などがある（以下、「提言」と記載）[6]。また 2015 年の「提言」に基づき、議論・情報共有・協働の場としての「繁栄のためのデジタル・セキュリティに関するグローバル・フォーラム」（The Global Forum on Digital Security for Prosperity）が創設された[7]。

**【「サイバーセキュリティ」ではなく「デジタル・セキュリティ」】**

上述のレポートのタイトルには、「サイバーセキュリティ」という言葉が登場してこない。その代わりに、OECD では「デジタル・セキュリティ」という言葉を前面に打ち出している。2015 年の「提言」では、その理由が明示されている。

「提言」はまず、序文でこう書き始める。「デジタル・セキュリティに関する脅威やインシデントは近年増加し、公的機関、民間機関、個人を問わずに重大な経済・社会的帰結をもたらすようになってきた。いくつかの事例はオペレーションの破綻（サービスの拒否やサボタージュを通じるなど）、直接的な財政的損失、訴訟、レピュテーションの失墜、競争力の喪失（通商機密の盗難の場合など）、また顧客の信頼の喪失などにつながっている」。そして、「デジタル・リスクは技術的なものではなく、経済的なリスクとして扱われるべき」だと説明している。この「提言」で示された、「2 つの主要メッセージ」を確認してみよう。

1. 本提言は、公的機関及び民間機関の経済的・社会的目的に焦点を当てている。また、リスク・マネジメントをベースとするアプローチを導入する必要性にも焦点を当てている。デジタル・リスクは技術的な問題ではなく、経済的なリスクとして扱われるべきであり、それ故、組織全体のリスク・マネジメントと意思決定のプロセスと一体となっているべきである。他のカテゴリーのリスクとなんら違いはない。その意味で、本報告書では、特別感、特殊感を出してしまう「サイバーセキュリティ」や「サイバー」といった文言を使っていない。

2. このようなマネジメントをすれば、リスクは経済活動から得られる利益に比して受容できるレベルにまで抑えることができる。その意味で、デジタル・セキュリティは、その他の利益を必ず考慮し、直面するリスクに対して適切であるように、また、守ろうとしている経済的・社会的活動を

---

[4] OECD (2002), Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security, www.oecd.org/internet/ieconomy/15582260.pdf.

[5] OECD (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures, http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=121&InstrumentPID=117.

[6] OECD (2015), Recommendation of Council on Digital Security Risk Management for Economic and Social Prosperity, https://www.oecdilibrary.org/docserver/9789264245471en.pdf?expires=1585215107&id=id&accname=guest&checksum=C185835932735AE95716FE564A9FF340

[7] https://www.oecd.org/internet/global-forum-digital-security/

損なわないようにデザインされるべきである[8]。

OECD としては、より広範かつ一般的な「デジタル」という文言を使い、この問題が経済・社会活動や繁栄を阻害するものであること、経営全体としてのリスク・マネジメントの一環として考えるべきであることを打ち出し、経営戦略に見合った、守りに偏りすぎないバランスの取れたデジタル・セキュリティを促しているのである。

なお、この「提言」では、デジタル・セキュリティに関係を持つステークホルダー像が次のように述べられている。「経済活動・社会活動のすべて、あるいは一部でもデジタル環境に依拠している政府、公的機関、民間組織、そして個人はステークホルダーである」[9]。パソコンもスマートフォンも使わない、使うのはハンコと電話。そういう数少ない組織、人を除けば、ありとあらゆる人たち、組織がステークホルダーなのである。それを今一度強調し、だからこそこの問題はほぼすべての人たちが考えるべき問題であることを示している。

2015 年の「提言」に基づき 2018 年 12 月に創設された「繁栄のためのデジタル・セキュリティに関するグローバル・フォーラム」(The Global Forum on Digital Security for Prosperity) は、デジタル・セキュリティに関係する世界中のあらゆるステークホルダーが参加する場として位置づけられているが、この「グローバル・フォーラム」のウェブサイトでは、改めて、「サイバーセキュリティ」と「デジタル・セキュリティ」の違いが説明されている。サイバーセキュリティは 1．経済・社会、2．技術、3．法の執行、4．国家及び国際安全保障の 4 つの重なり合う側面を持つとし、「デジタル・セキュリティはサイバーセキュリティの経済的・社会的側面」であると整理している[10]。徐々に説明が洗練されて行っていることがわかる。「デジタル・セキュリティは、ハードウェア、ソフトウェア、ネットワークやデータの有効性や統合性、機密性を阻害するような事案から、ステークホルダーの資産、安全、評判、様々な機会、経済的・社会的活動の継続性をどう守るかまでカバーして」おり、「デジタル・セキュリティはデジタル・エコノミーにおける持続可能な信頼を構築し、経済・社会のデジタル・トランスフォーメーションをサポートするための、より広範な政策アジェンダの一環」なのである[11]。

「経済協力開発機構」という名前を有する組織なればこそだが、OECD としては、世界中がデジタル化された現在、サイバーセキュリティの問題は国家から個人にいたるまで、あらゆるレベルの経済・社会活動に大きな影響を与えること、そして誰しもがこの問題に関わっていることをより明確に打ち出したい。そのために、技術的な問題として処理されてしまい、全体に関わる問題としてとらえられない危険性がある「サイバー」という文言より、より広範に訴求する「デジタル」という文言を使うという判断をしているのである。この問題は科学技術の話ではなく、経済・社会の話なのである。

---

[8] OECD, 2015, pp 6
[9] OECD, 2015, pp 10
[10] https://www.oecd.org/internet/global-forum-digital-security/about/
[11] Ibid.

**【「提言」が掲げた原則：OECD の重視するポイント】**

2015年の「提言」では、これを実行に移すことでデジタル・セキュリティ・リスク・マネジメントのより包括的な公共政策的アプローチが進むことを期待し、また、政府内部、官民、そして国内・地域内・国際的な新たな協働メカニズムが生まれることを期待すると記されている。「提言」では、以下の8つの原則が示されている。これらの指針はOECDの考え方を明確に示しているため、重要と思われる部分を紹介する[12]。

**1. 意識の向上・スキル・強化：すべてのステークホルダーはデジタル・セキュリティ・リスクを理解し、またそのリスクをどうやってコントロールするかを理解するべきである**

デジタル・セキュリティ・リスクが経済的また社会的な目標の達成に影響を及ぼし得ること、またこのマネジメントが他に影響を及ぼしうることを認識すべきである。そしてこのリスクを理解し、これをコントロールするために必要な教育やスキル、また、このリスク・マネジメントに関する決定がそれぞれの活動や全体的なデジタル環境にどう影響するかを評価できる教育やスキルを与えられるべきである。

**2. 責任：すべてのステークホルダーはデジタル・セキュリティ・リスクの管理について責任を負うべきである**

すべてのステークホルダーが、デジタル・セキュリティ・リスクのマネジメントについて責任を負い、かつ自分たちの下す決定が他者にどのような影響をもたらすか考慮することについて責任を負うべきである。すべてのステークホルダーは、経済的・社会的目標の達成のためにはある程度のデジタル・セキュリティ・リスクは受容されるべきであることを理解すべきである。

**3. 人権と基本的価値：すべてのステークホルダーは透明性を持ってデジタル・セキュリティ・リスクを管理するべきであり、また人権と基本的価値に沿うように管理するべきである**

デジタル・セキュリティ・リスクのマネジメントは、表現の自由、情報の自由な流れ、情報やコミュニケーションの秘匿性、プライバシーや個人データの保護、開放性、フェアなプロセスと言った民主主義社会で認められている人権や基本的価値に則った形で行われるべきである。また、組織はデジタル・セキュリティ・リスクのマネジメントやその手続きについて、透明性に関する基本的方針を持つべきである。

**4. 連携：すべてのステークホルダーは国内だけでなく国境を越えて連携するべきである**

**5. リスク・アセスメントと対応のサイクル：リーダーや意思決定者達はデジタル・セキュリテ**

---

[12] OECD, 2015, pp 11-13

ィ・リスクが不断のリスク・アセスメントに基づいて対応されるよう徹底すべきである

デジタル・セキュリティ・リスクのアセスメントは、システマチックかつ循環的に行われるべきである。このアセスメントは危機に瀕した経済・社会活動の脆弱性とあいまった脅威がもたらしうる結果について判定すべきであり、またそのリスクに対応するための意思決定プロセスを公表すべきである。リスクへの対応は、経済・社会活動から期待される便益に比して受容できるレベルまでリスクを減らすことを目指すべきであり、他方で、他者の合法的な利益に影響を及ぼす可能性を考慮すべきである。リスク対応には多くの選択肢が含まれる。たとえばリスクの受容、減少、移転、予防、あるいはそれらのミックスである。

**6. セキュリティの方策：リーダーや意思決定者達は、セキュリティのための方策が適切で、リスクに釣り合ったものであるよう徹底すべきである**

デジタル・セキュリティ・リスクのアセスメントは、受容レベルまでリスクを減らすためのセキュリティの手段の選択、実行、改善の手引きを示すべきである。セキュリティの方法はリスクに見合った適切なものであるべきであり、その選択は、リスクから守ろうとしている経済・社会的活動や、人権・基本的価値、そして他者の合法的な利益に及ぼしうるプラスの影響、マイナスの影響を考慮すべきである。

**7. イノベーション：リーダーや意思決定者達は、イノベーションが考慮されているかを徹底すべきである**

イノベーションは、デジタル・セキュリティ・リスクをリスク・アセスメント及び対応において決められた受容可能レベルまで減少させるために不可欠なものと見なされるべきである。イノベーションは、セキュリティの手段の設計・開発、デジタル環境に依拠した経済・社会活動の設計・実行、この双方において育まれるべきである。

**8. 準備と継続性：リーダーや意思決定者達は、準備と継続のためのプランの採用を徹底すべきである**

セキュリティ・インシデントによるマイナス効果を減少させるため、また経済・社会活動の継続性と回復力を守るための、デジタル・セキュリティ・リスク・アセスメントに基づいた準備及び継続プランが採用されるべきである。このプランではデジタル・セキュリティ・インシデントを防ぎ、見破り、対応し、インシデントから復活するための方法を特定・識別すべきである。このプランはインシデントの影響の大きさ、深刻度、デジタル環境において他者に影響が及ぶ可能性に基づいたレベル化のためのメカニズムを提示する必要がある。通知のための適切な手続きは、このプラン実行の一部とみなされるべきである。

以上８つの指針に通底するのは、アクティブな経済・社会活動を行う上で、ある程度のリスクは

やむを得ないという、「リスクの受容」である。ブレーキばかり踏んでいたら、スピードは出ない。守りばかり重視していたら、攻めることが出来ず、成長につながらない[13]。そのために、リーダーや意思決定者が徹底的に己の組織を日常的に繰り返し精査し、活動の便益を損なわない、受容できるリスクのラインを見極め、そのラインまでリスクを減らすよう、セキュリティ対策を徹底していくことが求められる。この一連の流れは、人権や基本的価値に沿うことはもちろん、透明性も必要とされる。

そしてデジタル・セキュリティ・リスクに関係のあるあらゆるステークホルダーは、一国内だけでなく、国境を越えて協力することが必要とされている。リスクは受容するがぎりぎりまで軽減させ、経済・社会の進展を促す、進展を阻害させてまでもリスク潰しに邁進する選択は取らない。そのためにあらゆるステークホルダーが協力し合うことが必要だというOECDの確固たる意思が、この原則から見えてくる。

**【デジタル・セキュリティ・リスク・マネジメントに関する国際調査】**

2019 年 6 月に発表されたのが「企業におけるデジタル・セキュリティ・リスク・マネジメント調査」 (Measuring Digital Security Risk Management Practices in Businesses)である。これは、2015 年の提言で示された原則にのっとった、企業のデジタル・リスク・マネジメントを測定するためのフレームワークや指標を開発するためのプロジェクトについてまとめたものであるが、その一環として、2018 年 7 月から 9 月にかけて国際的に実施された予備調査の内容も含んでいる。

調査の背景：

この調査の背景には、OECDの以下のような問題意識がある。以下、調査の冒頭に示されている概要から引用する。「デジタル・セキュリティに関するインシデントは、企業のイメージや財務力、運営や有形資産、そしてバリュー・チェーンにおけるパートナーやその他の関係者に影響を与える。インシデントは企業の競争力やイノベーションの能力、市場でのポジションを揺るがすこともできる。インシデントの頻度を減らし、負のインパクトを軽減し、デジタル・トランスフォーメーションをうまく活用できるようにするためにも、効果的なデジタル・セキュリティ・リスク・マネジメントは企業にとってきわめて重要である。そのため、OECD各国の行政担当者たちは、企業のデジタル・セキュリティ・リスク・マネジメントを理解し、計測することにより大きな関心を寄せるようになった」[14]。経済・社会的側面を重視するOECDとしては、これらの分野への影響をコントロールし、かつ成長につなげるための打ち手を考えるために、効果的なリスク・マネジメントのやり方を広く調査し、広く情報を得ることが必要と考えたのである。

2016 年、OECD はまず、デジタル・セキュリティ・リスクに関連するデータを提供してきたこれまでの調査のレビューからスタートした。このレビューを通じ、これまでの調査では多くの場合設問が技術的なものに偏っており、企業のリスク・マネジメントに関するものが少ないことが判明した。2015 年の「提言」で強調されたデジタル・セキュリティ・リスクの経済的・社会的側面を見て

---

13 「攻め」の重要性については、JCIC の公開した各レポートでも言及しているので参照いただきたい https://www.j-cic.com/reports.html

14 OECD, 2019, pp 6

いなかったのである。

調査手法：

こういった不備についての反省を踏まえ、OECD は企業のデジタル・セキュリティ・リスク・マネジメントを計測するフレームワークを開発することで、改善を試みた。このフレームワークは 2015 年の「提言」に依拠し、6 つのモジュールと 18 の指標から構成されている[15]。6 つのモジュールとは：A. 分布、B. デジタル・セキュリティ・リスクに関するガバナンス、C. デジタル・セキュリティ・リスクの評価事例、D. デジタル・セキュリティ・リスクを減少させる事例、E. デジタル・セキュリティ・リスクの移転事例、F. デジタル・セキュリティ・リスク意識（認識）及びトレーニングである。これら６つのモジュールの下に、指標がぶら下がる形になっている（表１）[16]。

【表１：調査のフレームワーク】

| モジュール | 指標 |
|---|---|
| A. 分布 | A-1 所在地<br>A-2 企業規模<br>A-3 経済活動の種類<br>A-4 売上高<br>A-5 デジタル化への依存度 |
| B. デジタル・セキュリティ・リスクに関するガバナンス | B-1 デジタル・セキュリティ・リスクについて責任を負う特定の任務が社内にある企業<br>B-2 デジタル・セキュリティ・リスクのマネジメントに関する方針が定まっている企業<br>B-3 デジタル・セキュリティ・リスクのマネジメントに関するレビューとモニタリングの手順が定まっている企業<br>B-4 デジタル・セキュリティ・リスクのマネジメントに関する協力とレポーティングを可能にする組織構造と手順が社内にある企業 |
| C. デジタル・セキュリティ・リスクの評価事例 | C-1 会社全体の経営リスクのマネジメントの一環としてデジタル・セキュリティ・リスクを評価している企業<br>C-2 デジタル・セキュリティ・リスクの評価の一環として定期的になんらかの活動を行っている企業 |
| D. デジタル・セキュリティ・リスクを減少させる事例 | D-1 リスク軽減のための措置を講じた企業<br>D-2 脅威や脆弱性、インシデント、リスク・マネジメント事例やセキュリティ対策などの情報を共有している企業 |
| E. デジタル・セキュリティ・リスクの移転事例 | E-1 デジタル・セキュリティ・リスクの移転のために保険を活用している企業 |

15 OECD, 2019, pp 23

16 Ibid., pp 24

| | |
|---|---|
| | E-2　保険証券を購入しなかった企業とその理由<br>E-3　保険証券を購入してリスク移転を行った企業と移転したリスクの種類<br>E-4　その他のリスク移転を行った企業 |
| F. デジタル・セキュリティ・リスク意識（認識）及びトレーニング | F-1　デジタル・セキュリティ・リスクのマネジメントに関する意識啓発及びトレーニングを行った企業 |

各モジュールの論拠は次のようになっている。A)分布：回答を階層化し、分析する。B)企業が適切なデジタル・セキュリティ・リスクに関するガバナンスの枠組みを定めているかを評価する。こういった枠組みは、特に、デジタル・セキュリティ・リスクのマネジメントが複雑化する比較的大規模な組織にとって重要である。企業のあらゆる側面に関係する包括的な概念であり、企業におけるデジタル・セキュリティ・リスクのマネジメントが成功するための決定的要素として企業がガバナンスをとらえているかを見る。C)セキュリティに関わる決定がリスクと経済・社会活動の双方を鑑みて適切かつバランスが取れているかどうかを決めるのは持続的なリスク評価と対応次第である。本モジュールで、適切なリスク評価を行うための事例を測定する。D)リスク軽減は、リスク対応の際に企業のリスク・マネジメントの責任者が選択しうる選択肢のうちの１つである。E)リスク移転も D)のリスク軽減と同様、リスク対応の選択肢のうちの１つである。リスク移転には、「活動目的における不確実性による望まない効果を他者に移転させる」ことが含まれる。F)「デジタル・セキュリティ・リスクのマネジメントにまず必要なのは、リスクが存在するのを理解すること」である。故に「認識」はすべての基礎になる。リスクが存在することを認識しないステークホルダーは、リスクを評価し、対応する代わりに、無意識のうちにうっかりリスクを受け入れてしまうことになる。認識することは、責任をとることの第１歩である（「提言」における第２の原則)。責任ある決定を下す能力に必要なのは、それを行うスキルを身につけることである。それ故、社内にデジタル・セキュリティ・リスクに関する意識及びそのマネジメントについての意識を醸成するための事例（トレーニングを含む）について調べるのが本モジュールである[17]。

予備調査：

15 年の「提言」で示された「原則」が企業のリスク担当責任者によってどの程度、またどのように実行されているかを明らかにする予備調査が、FERMA(European Federation of Risk Management Associations)の協力の下、上記の調査枠組みを用いて 2018 年 7 月から 9 月にかけて行われた[18]。調査対象は欧州 14 カ国の企業のリスク担当責任者約 2,600 人である。リスク担当責任者がいない企業については、内部監査担当者、経理担当者、リスク管理委員会の委員長もしくはメンバー、CEO、COO、CFO が回答するよう依頼している。回答者として、技術、IT 担当者が含まれていない。これは「提言」において、デジタル・セキュリティ・リスクは技術的なものではなく経済的リスクであると示されていることを踏まえている。

---

17 OECD, 2019, pp 24-28

18 Ibid., pp 29-31

この方法には構造的な不備も見出された。たとえば、デジタル・セキュリティ・リスク・マネジメント事例が会社全体のリスク構造に組み込まれず、技術的なリスクとして対応されていた場合には、調査の回答者であるリスク担当責任者はIT部門で下される技術上のセキュリティに関する決定についてよく知らず、正確に回答することができない。この予備調査を通じ、企業の多くが、デジタル・セキュリティを会社全体のリスク・マネジメントの枠組みに組み込んでいないことがわかった。デジタル・セキュリティ・リスク・マネジメントのより包括的な全体像を見るためには、セキュリティ担当責任者の視点とITの視点の双方を組み込むことが必要である。また、FERMAを通じた回答者の多くが、比較的リスク・マネジメントについての理解が進んでいる大企業に属しており、OECDが重要と考えている中小企業をカバーできなかった[19]。

また、このパイロット調査の回答率は約3%と極めて低く、欧州の正確な傾向をこの調査から測ることは難しいが、示された結果を次項で見ていきたい[20]。

調査結果：

モジュールA：多くの回答者は従業員1,000人以上の企業に属し、産業としては製造業、金融業、運輸・倉庫業の順である。ほぼすべての回答企業がウェブサイト、イントラネットを有している。欧州ではブロードバンドが広く張り巡らされているが、この利用率は76%と案外低い。

モジュールB：回答があった企業のうち85%に、会社全体のリスク・マネジメントを担当する部署もしくは役職が置かれていたが、このうち、デジタル・セキュリティ・リスクを担当する部署もしくは役職が置かれている企業は全体の32%にとどまった。そのかわり、CIOもしくはITマネジャーが任を負っているのが43%、CISOなのが38%となった。デジタル・セキュリティ・リスクの受容レベルを決定するのはCIOやITマネージャー（19%）よりCEO（33%）が多かった。数は少ないが（4%）、取締役会のメンバーというケースもあった。

回答があった企業のうち84%が、デジタル・セキュリティに関する対応策があると答え、そのうちの91%がデジタル・セキュリティ・リスク・マネジメントに関する役割と責任を割り当てており、93%が啓発とトレーニングも実施している。一方、リスク移転が対応策の中に入っているのは37%であり、またこの設問と「リスク対応のプロセス」について「わからない」と答えた率も15%に上ることから、これらについては理解が進んでいないことがうかがえる。また、セキュリティ対応策がどれくらい深掘りされているかについては、B2の設問「デジタル・セキュリティ・リスクのマネジメントに関する方針が定まっているか」で示されている9つの分野（①役割・責任、②協力のプロセス、③監査・レビュー・改善サイクル、④リスク評価、⑤リスク対応プロセス、⑥デジタル・セキュリティの方法、⑦ビジネスの継続と復元性、⑧リスク移転、⑨啓発とトレーニング）をどれだけカバーしているかで見ることが出来るが、平均は6.6分野と比較的高い数値であった。B3の「レビューとモニタリング」については、ほとんどが「年1回」と回答している。70%の企業が、デジタル・セキュリティ・リスクに関して経営部門とICT間のミーティングを行っており、協力とコミュニケーションが行われていることがわかる。

---

19 OECD, 2019, pp 29

20 Ibid., pp32-45

モジュールC：81%の回答企業が、自社のビジネスが直面するデジタル・セキュリティ・リスクを評価するシステムを有しており、そのうちの88%がデジタル・セキュリティ・リスクを自社の全体のリスクの中に統合していた。この評価の担当者はビジネス・マネジャー、ITマネジャー、リスク・マネジャーなど様々であった。評価は年1回の企業が58%と多くを占めた。

モジュールD：81%の企業がデジタル・セキュリティに関する評価の結果としてなんらかの対応策を定めていた。そのうち、企業活動の変革を目的とする対応策を定めている企業は42%と半分以下だが、インシデントの発生の対応策を定めている企業は80%に達した。D2の設問については、社内で経営陣とIT部門がデジタル・リスクについて情報共有を行っている企業が全体の70%に達したのに対し、外部関係者との情報共有については、ITサプライヤーが48%、保険会社が45%であり、顧客との情報共有は22%、また、情報共有・分析のための組織と情報共有している割合はわずか8%であった。

モジュールE：約半数の企業がリスク移転を行っている。移転方法は、保険（55%）、その他の法的契約（53%）、外部委託（59%）などがあった。しかし、リスク移転を行っていても、「風評被害」についてはカバーできないと考えている企業が半数近くを占めている。

モジュールF:啓発とトレーニングに関しては、多くの企業がこれを実施している。69%の企業で部門会議の際にリスクについて議論し、61%の企業がトレーニングを提供している。一方で、リスクを軽減する活動を行った社員への報酬を出す企業は22%しかなかった。トレーニングは取締役クラスに対して実施している企業が89%、事業部のマネージャークラスには95%、セキュリティ部門の社員には91%、IT部門の社員には95%の企業が提供していた。外部の請負業者に対してなんらかのトレーニングを行っていると回答した企業は18%で、「わからない」と答えた企業が31%にのぼった。

今後の改善に向けて：

他組織がどういうリスク・マネジメントを行っているか、自社の取り組みは適切なのかを知るために、情報の共有はきわめて重要である。そのためのデータ収集は、常に改善されていくべきである。予備調査を顧みて、改善すべき点も挙げられている[21]。主要な点をいかに挙げる。

1. 回答率の改善

回答率がきわめて低かったことを踏まえ、忙しい担当者達の時間を奪わぬよう設問をシンプルにすること、また必ずしもリスク・マネジメントの専門家でなくても設問が理解しやすいように、言葉づかいをより一般的なものにすることが改善としてあげられている。例示されているのは、表１より設問をかなり絞ったリストである。

---

[21] OECD, 2019, pp 47-50

【表２】

| モジュール | 指標 |
|---|---|
| A. 分布 | A-1　所在地<br>A-2　企業規模<br>A-3　経済活動の種類<br>A-5　デジタル化への依存度 |
| B. デジタル・セキュリティ・リスクに関するガバナンス | B-1　デジタル・セキュリティ・リスクについて責任を負う特定の任務を社内で誰が担当しているか |
| C. デジタル・セキュリティ・リスクの評価事例 | C-2　企業活動に影響を与える可能性があったインシデントについて、その結果をどのくらいの頻度で評価しているか |
| D. デジタル・セキュリティ・リスクを減少させる事例 | D-1　デジタル・セキュリティの評価の結果、リスク軽減のための措置<br>を講じたか |
| E. デジタル・セキュリティ・リスクの移転事例 | E-1　デジタル・セキュリティ・リスクをカバーする保険に加入しているか、<br>E-3　カバーするリスクの種類 |
| F. デジタル・セキュリティ・リスク意識（認識）及びトレーニング | F-1　デジタル・セキュリティ・リスクのマネジメントに関する意識啓発及びトレーニングを行った企業 |

2.「成熟度モデル」への転換

調査を通じて明らかになったのは、この調査のフレームワークを改良・拡張した、企業のデジタル・セキュリティ・リスク・マネジメントの「成熟度」を評価するためのモデルの必要性である。このモデルは、デジタル化への依存度や産業規模を前提として、あるべき姿、重要性、効果などの尺度からある種の事例を重点的に見たり、事例のランク付けをするものである。ただし、一般的に「成熟」「未成熟」が与えるイメージに引きずられないように設計されるべきである。会社の規模、産業、あるいはデジタルへの依存度などで共通点を持つ企業のデジタル・セキュリティ・リスク・マネジメント事例が、他社比較でき、自社のレベルが適切かどうかわかるようになる。この成熟度のスコアが他のリスク要因（脅威、脆弱性、インシデント等）についての情報と連結できれば、各社の政策立案者たちは、用意周到な企業がデジタル・セキュリティ・リスクにいかにうまく対応できるかについて、詳細に理解できるだろう。

この他、より各組織の対応について、より「深く」見るべきであること、インシデントとその経済的インパクトをしっかり見ることも重要であることが挙げられている。

**【まとめ：より効果的なデジタル・セキュリティ・リスク・マネジメントを目指して】**

この予備調査では、欧州14カ国の企業のリスク担当責任者に同一の質問を行っている。調査への回答数はごく少数であり、大企業に絞られているなど、様々な改善すべき点が見出されているが、

経済・社会の進展のために、より効果的なデジタル・セキュリティ・リスク・マネジメントが必要であり、そのためにはさまざまなステークホルダーが自社・自組織のマネジメント方法について、ベスト・プラクティス、バッド・プラクティスも含めて情報公開し、共有していくべきだというOECDの姿勢は揺るぎない。

デジタル化の技術的変化のペースは速く、技術的専門家でなければそのリスクについて深く理解することはやはり難しいだろう。OECDは「デジタル・リスクは技術的なものではなく、経済的なリスクとして扱われるべき」としているが、であればこそなおさら、社内的には経営層とIT部門との連携が重要になってくる。また、デジタル・リスクへの感度を通常より高いレベルで有する「プラス・セキュリティ人材」の存在もきわめて重要と言えるだろう。社外的には、自社・自組織と似た業種、規模感を有する企業・組織と比較し、己のレベルが妥当であるか確認、改善できるシステムが必須である。そのためにはOECDが今回行った予備調査のような国内外の比較の他、成熟度をスコア化し、見える化していくことはやはり重要である。

2018年末に発足した「グローバル・フォーラム」は、デジタル・セキュリティに関係する世界中のあらゆるステークホルダーが参加する場として位置づけられている。提言に書かれた原則を実現していくにあたり、やはり自分以外の組織がどうやっているかは気になるところであるし、互いの知見を合わせ、よりよいやり方を模索していくことも望まれる。本フォーラムを介し、専門家や政治家がデジタル・セキュリティ・リスク及びそのマネジメントにまつわるベスト・プラクティス、バッド・プラクティスを共有し、共に学び、経済・社会の繁栄のためのデジタル・セキュリティについての見方・対応策を収斂させていくことが期待されている。そしてここでの議論が国際的な公共政策の議論に影響を与え、OECDやその他の国際的な場での分析や指針、政策提言につながることが期待されている。

この分野において、「こうやったらうまくいく」という簡単な処方箋はおそらくありえない。ただ、決定的なダメージを受けるようなマネジメント上の失敗がもしあるのであれば、ダメージ・コントロールのためにもその失敗から学ぶことは意味がある。より効果的、効率的な手法を見出していくためにも、デジタル・セキュリティに関係があるステークホルダー達の積極的な情報開示・共有は欠かせない。OECDはグローバル・フォーラムを通じ、ステークホルダー達の議論の場を構築したが、これにより意識が高まることが期待される。特に「成熟度モデル」については、どのような内容になっていくのかも期待されるところである。「成熟度モデル」が作り込まれ、よりよいマネジメント手法が編み出され、広まっていくことが期待される。今後もOECDの動きに着目していきたい。