企業の観点からのサイバーセキュリティ

ーサイバーセキュリティは情報技術の問題ではなく、企業経営の課題ー

PwC コンサルティング合同会社 パートナー
丸山　満彦

▌要　約▐

1. 2021 年 9 月に閣議決定された「サイバーセキュリティ戦略」において、「経済社会の活力の向上及び持続的発展」として「DX (Digital Transformation) with Cybersecurity の推進」が謳われている。企業の情報技術、デジタル技術の活用と情報セキュリティ対策の同時実施は当然のことであり、経営陣は経営課題として情報セキュリティ対策をとらえる必要がある。つまり、サイバーセキュリティはガバナンスの要素であるという認識が重要である。
2. サイバーセキュリティリスクに対して、経営陣としてすべきことは、サイバーセキュリティリスク対策を企業全体のリスクマネジメントの一環として組み込むことであり、経営者が自らのリーダーシップのもとで対策を進めることが重要である。また、ビジネスがサプライチェーンに支えられていることを鑑み、サプライチェーン全体への目配せも重要となる。
3. サイバーセキュリティリスクが組織活動に大きな影響を及ぼすことから、多様なステークホルダーとの平時、有事のコミュニケーションは重要となる。特に、米国ではすでに証券取引委員会（SEC）が新たな規則を設け、投資家へのリスク情報の開示を強化している点は、日本企業も注視しておく必要があるだろう。

Ⅰ 組織におけるサイバーセキュリティリスクの重要性

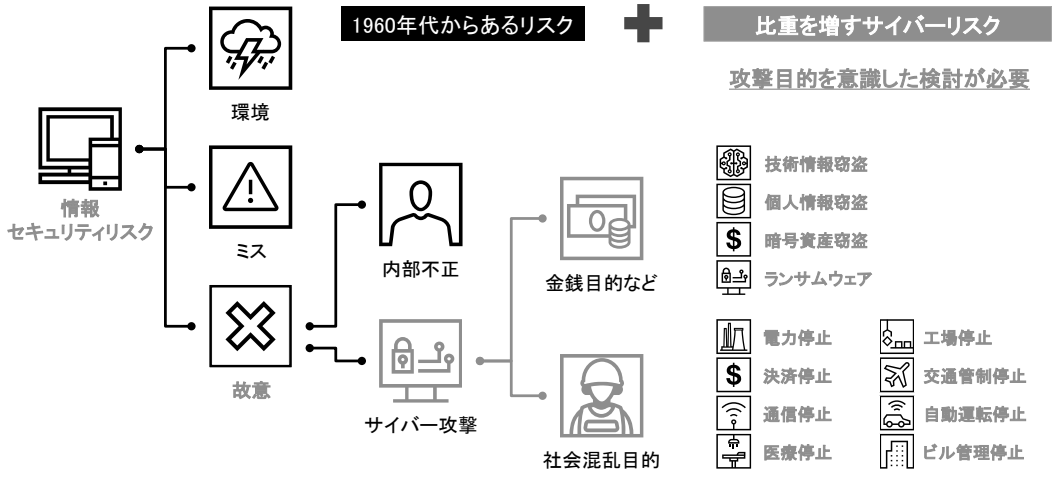
１．組織にとってサイバーセキュリティとは何か

1960 年代以降、コンピュータが社会的にも広く利用されるようになった。そして 1990 年代からのインターネットの普及、2000 年代からのスマートフォン、IoT（Internet of Things）製品を含むコンピュータデバイスの飛躍的な普及、クラウド環境の普及により、今や、多くの組織、個人が情報技術の恩恵を受ける環境となっている。この結果、情報技術（あるいは、デジタル技術）をうまく活用し、より高い付加価値を生み出せる組織が、競争に勝っていけるという社会になった。つまり、すべての企業にとって、情報技術の活用は競争優位を維持し、発展していく上でも不可欠ということである。

この情報技術、デジタル技術のうまい活用というのは、付加価値の提供とともに、適切なリスクコントロールができている状況のことである。2021 年 9 月に閣議決定された「サイバーセキュリティ戦略[1]」においても、「経済社会の活力の向上及び持続的発展」として「DX (Digital Transformation） with Cybersecurity の推進」が謳われていることからもそのことがわかる。企業の情報技術、デジタル技術の活用と情報セキュリティ対策の同時実施は当然のことである。

企業における情報セキュリティ対策は、災害（例えば、地震、洪水、落雷によるサージ〔過電圧・過電流〕、停電、火災など）、障害・ミス（ディスク破損、誤操作など）に起因するものが中心であったが、前述のように 1990 年代にインターネットが企業活動に不可欠なものとなり、また、近年のサイバー脅威の変化の速さもあり、企業にとって注目すべきリスクはサイバーセキュリティに関するリスクになってきた（図表 1）。ただ、従来から重要と言われていた内部不正対策についても、外部からの侵入者が内部の管理者のア

図表 1　サイバーセキュリティに関する脅威の動向



（出所）PwC 作成

[1] 内閣サイバーセキュリティセンター「サイバーセキュリティ戦略（閣議決定）」2021 年 9 月 28 日。

カウントになりすます（つまり、内部者を装うことになる）ので、引き続き重要である。

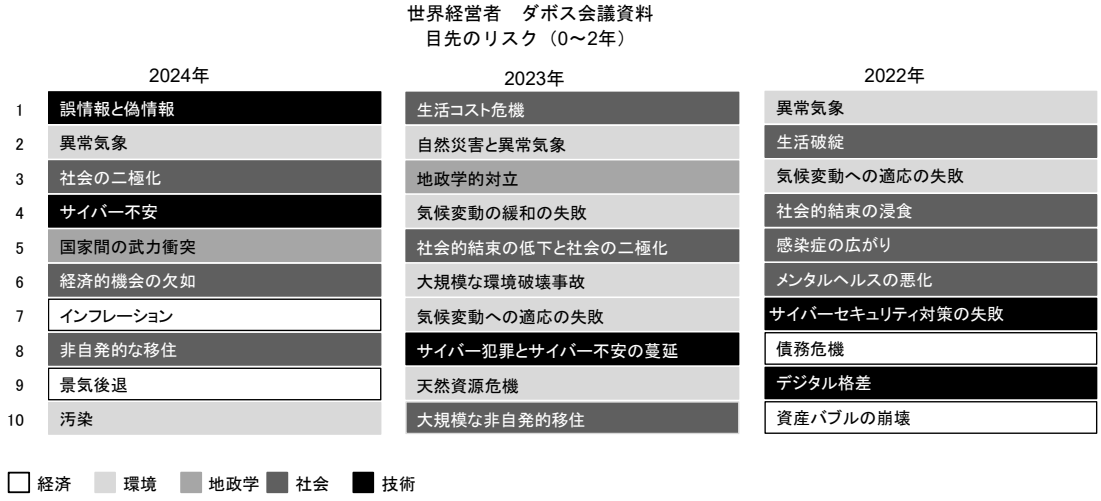
サイバー攻撃によるリスクは「情報漏えい」と「業務停止」である。情報漏えいは、「個人データ漏えい」と「技術情報の漏えい」が企業リスクとしては大きいと言えるだろう。また、「業務停止」という意味では、「ランサムウェア」によるシステムの暗号化が大きなリスクといえる。いずれも、業務活動の根幹に関わる問題であり、情報技術部門の問題というよりも、経営課題そのものである。このような背景を受けて、経済産業省でも、2015 年に「サイバーセキュリティ経営ガイドライン」が策定され、2023 年に Ver3.0[2]になっている。この改訂では、リスクマネジメントとの関係が強調されている。

また、気候変動リスク、人権リスクと同様に、組織のリスクとしてだけでなく、組織活動を通じて対応をしていかなければならない社会課題としても見ておく必要がある。

2．世界経済フォーラムのグローバルリスクレポートに見るサイバーセキュリティリスク

本節では、世界経済フォーラム（World Economic Forum）が毎年公開している、世界の経営者が重要と考えているリスクについて紹介する。今後 2 年間に予想される最も深刻なグローバル・リスクの中で、サイバーセキュリティに関連するリスクは、近年トップ 10 に入るリスクになっていることから、世界中の経営者が常に意識し、警戒しているリスクと言える（図表 2）。これと同様の傾向は、PwC が独自で調査している CEO グローバルサーベイ[3]でも窺える。

図表 2　世界の経営者が意識・警戒するリスク（2022～2024 年）



（出所）World Economic Forum, “The Global Risks Report 2024 19th Edition Insight Report,” January 10, 2024; World Economic Forum, “The Global Risks Report 2023 18th Edition Insight Report,” January 11, 2023; World Economic Forum, “The Global Risks Report 2022 17th Edition Insight Report,” January 11, 2022

[2] 経済産業省、独立行政法人情報処理推進機構「サイバーセキュリティ経営ガイドライン Ver3.0」2023 年 3 月 24 日。
[3] PwC「第 27 回世界 CEO 意識調査　絶え間ない変革の時代における成功」2024 年 3 月、PwC「第 26 回世界 CEO 意識調査　未来の成功を見据え、今日の勝機を掴む」2023 年 3 月、PwC「第 25 回世界 CEO 意識調査　目指すべき成果を再定義する」2022 年 3 月。

Ⅱ 経営陣として誰が何をすべきか

１．経営陣の中に責任者を任命する

経営課題となったサイバーセキュリティリスクに対して、経営陣はどのようにして対応をすべきか。これが経営陣にとっては重要となる。サイバーセキュリティのリスクは経営課題とはいえ、経営課題はその組織によって、様々である。数ある経営課題のひとつとして、サイバーセキュリティリスクへの対応をどの程度の優先度と考えるのかが最初の出発点である。

なお、経済産業省が 2023 年 3 月に公表した、「サイバーセキュリティ経営ガイドライン Ver.3.0」では、経営者がサイバーセキュリティリスクについての認識すべき 3 つの原則を以下のように示している（図表 3）。

図表 3　経営者が認識すべき 3 原則

	内容
1	経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要
2	サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先など、サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要
3	平時及び緊急時のいずれにおいても、効果的なサイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要

（出所）経済産業省、独立行政法人情報処理推進機構「サイバーセキュリティ経営ガイドライン Ver3.0」2023 年 3 月 24 日

２．経営陣によるサイバーセキュリティリスクへの関与

経営課題におけるサイバーセキュリティリスクの優先付けができれば、経営陣やその候補者の中から責任者（例えば、最高情報セキュリティ責任者〔CISO〕）を任命することになる。現在の経営陣やその候補者にその任に適切な人がいない場合は、新たに迎え入れるということも考えられるだろう。経営陣によるサイバーリスクへの関与の内容は前述の「サイバーセキュリティ経営ガイドライン Ver.3.0」では、次のように説明されている（図表 4）。詳細については、次節を参照されたい。

図表 4　サイバーセキュリティ経営の重要 10 項目

	内容
指示 1	サイバーセキュリティリスクの認識、組織全体での対応方針の策定
指示 2	サイバーセキュリティリスク管理体制の構築
指示 3	サイバーセキュリティ対策のための資源（予算、人材など）確保
指示 4	サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
指示 5	サイバーセキュリティリスクに効果的に対応する仕組みの構築
指示 6	PDCA サイクルによるサイバーセキュリティ対策の継続的改善
指示 7	インシデント発生時の緊急対応体制の整備
指示 8	インシデントによる被害に備えた事業継続・復旧体制の整備
指示 9	ビジネスパートナーや委託先などを含めたサプライチェーン全体の状況把握及び対策
指示 10	サイバーセキュリティに関する情報の収集、共有及び開示の促進

（注）　PDCA は「Plan〔計画〕、Do〔実行〕、Check〔実施状況の確認・評価〕、Act〔改善〕」の略。
（出所）経済産業省、独立行政法人情報処理推進機構「サイバーセキュリティ経営ガイドライン Ver3.0」
2023 年 3 月 24 日

３．他の CxO（Chief x Officer）との協力

CISO がサイバーセキュリティについての一義的責任を持つとはいえ、最高経営責任者（CEO）、最高財務責任者（CFO）、最高執行責任者（COO）、最高情報責任者（CIO）、最高リスク管理責任者（CRO）、最高人事責任者（CHRO）といった他の経営陣は、セキュリティについては CISO に任せきりというわけにはいかない。CFO はサイバーセキュリティ戦略に基づくセキュリティ対策が実行できるように財務面の支援、調整をする必要があるだろう。CHRO はサイバーセキュリティ人材の採用、育成、定着などの施策に協力することが重要となろう。また、CIO も、システム開発、運用において CISO との協力関係は欠かせないだろう。CRO もリスク対策の一環として全社リスクの観点からサイバーセキュリティリスクを評価し、その重要性を組織内外に浸透させる必要があるだろう。CEO は、最終的に全ての CxO の意見を踏まえて、組織のサイバーセキュリティリスク戦略などを承認し、その実行を支援していくことになるだろう。また、CEO 自らが取締役会でのサイバーセキュリティ戦略や取り組みを説明する必要もあるだろう。なお、組織によっては、CISO は CIO や CRO が兼務することもあり得るが、その際には組織全体のサイバーセキュリティリスクを一元的に管理できるようになっているかを確認することが重要である。

このようにサイバーセキュリティリスクは、組織が対応すべきリスクの中でも、影響が大きなリスクのひとつであり、組織経営の一環として、対応することが必要となってきている。特に DX を推進する組織ではなおさらである。ビジネスを成功に導くために必要な対応という意識で、経営陣は CISO を中心にサイバーセキュリティリスクに対応していくことが肝要である。

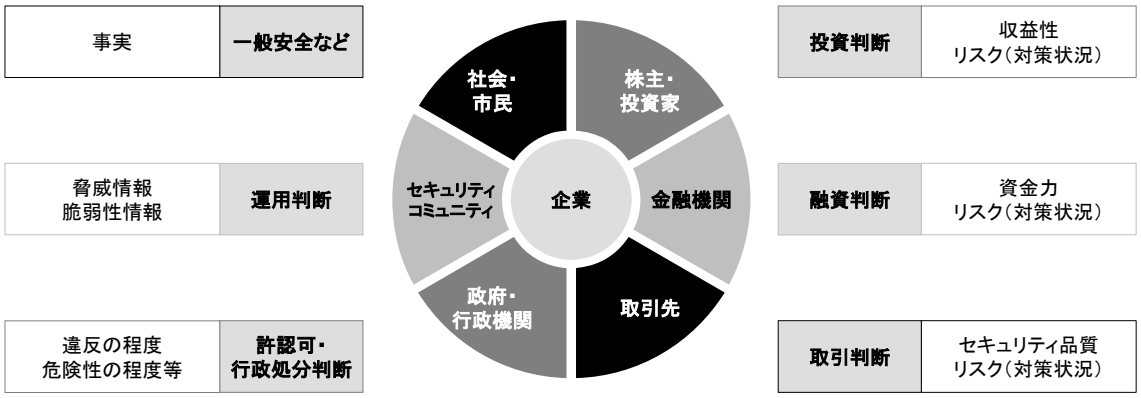
Ⅲ 経営陣とステークホルダーとのコミュニケーション

CxOの役割として、執行とともにステークホルダーへのアカウンタビリティを果たすことも重要である。

サイバーセキュリティに関わるステークホルダーとその関心事については例えば、図表5のような内容が考えられる。

ステークホルダーへのアカウンタビリティを果たす上では適切なコミュニケーションが必要である。適切なコミュニケーションには、適切な手段により、適切な内容を、適切なタイミングで伝達・共有することが必要となる。例えば、個人データの漏えいが生じた時は、関係する個人に対して、速やかにその事実を伝えることにより、可能な限り二次被害が生じないようにすることが重要となる。一方、投資家に対しては、インシデント発生時のみならず、定期的にリスク情報の開示ということも必要となるだろう。平時と有事のコミュニケーションの特質についてまとめると図表6のようになる。

図表5　サイバーセキュリティに関わる組織のステークホルダーとその関心事



（出所）PwC作成

図表6　平時と有事のコミュニケーションの特質

		期間比較可能性	組織間比較可能性	有益性	正確性	重要性	網羅性	適時性
平時	定期的	◎	◎	◎	◎	◎	◎	－
有事	イベントドリブン	－	○	◎	◎	◎	○	◎

組織間比較可能性：完全に同じインシデントはないが、影響等に関する情報は比較可能であり、比較により意味がある場合も多いかもしれない。

網羅性：インシデント時のコミュニケーションでは適時性が優先されるため、そのタイミングで一部不足している情報があっても、開示されることがある。

（出所）PwC作成

このようなステークホルダーとのコミュニケーションの設計、執行については、経営陣が最終判断することになる。

最近はサイバーセキュリティリスクが経営に与える影響が大きくなったことにより、米国の証券取引委員会（SEC）が新たに規則を設けるなど、投資家へのリスク情報の開示の一環としてのセキュリティリスクの開示が注目されるようになってきている。

Ⅳ まとめ

これまで、サイバーセキュリティは技術的な側面が目立っていたが、そのリスクの影響が企業全般に及ぶようになり、経営陣が対処すべきリスク課題と認識されるようになっている。経営陣はガバナンスの一環として、組織全体のリスクと一体となってサイバーリスクへの対応も考える必要がある。また、ステークホルダーを広く捉えると、一企業の活動は社会全体のエコシステムの一つとなっていることから、自らのリスクのみならず、サプライチェーンも含めたリスクとして意識することが重要である。そして、リスク対応の一環として、リスク情報を必要なステークホルダーと共有することも重要となってきている。人工知能（AI）の利活用を含め、サイバー空間における企業活動が今後もますます増大していくことが想定される。サイバーセキュリティリスクは今後もさらに重要な経営課題となるだろう。