ESG経営発展の鍵となるCybersecurity Strategy

-欧米のESG・先進デジタル動向から考察する日本企業の課題と対策-

2024年1月４日

株式会社日本総合研究所　先端技術ラボ
株式会社三井住友フィナンシャルグループ
シリコンバレー・デジタルイノベーションラボ

＜本件に関するご照会先＞
田谷洋一　株式会社日本総合研究所 シニアエキスパート 兼 JRI America, Inc. Executive Director（Ytaya@jri-america.com）
緒方雄二　株式会社三井住友フィナンシャルグループ 部長代理　（yuji.ogata@smbcgroup.com）

はじめに

➢近年、事業の持続可能性や環境問題への対策、従業員の労働環境の改善等、企業を取り巻く様々なテーマを対象にしたESG（環境・社会・ガバナンス）経営を推進する動きが国内外ともに拡大しており、投資家からの関心も高まっている。

➢ESG経営において、日本では自然災害などの環境問題への対策が注目を集める一方で、GDP上位国などの諸外国ではイノベーションやサイバーセキュリティをESG経営の注力領域として定める傾向がある。グローバルにDX（デジタルトランスフォーメーション）が進むなか、事業の持続可能性を大きく左右する要素として、システムリスクマネジメントやサイバーセキュリティ対策など、ESGにおけるガバナンス施策が近年注目を集めている。

➢サイバー攻撃の手口が巧妙化するにつれて、大規模な情報漏洩やシステム凍結など、企業の事業継続を揺るがす深刻なサイバー事件も増加しており、企業のセキュリティ対策には顧客やユーザー、投資家も厳しい目を向け始めている。実際に、ESG投資では、サイバーセキュリティ対策を新たな評価軸に加える動きも広がっており、同対策は企業の事業を評価する上での重要な指標になりつつある。

➢本稿ではこのようなESG経営とデジタルの先進動向に着目し、ESG評価の中で近年特に注目されているガバナンスやサイバーセキュリティに関連するトピックにフォーカスして、日本企業が直面している課題や対策について論じていく。具体的には、ESG経営で先行する欧米の事例を整理しながら、日本企業が今後ESG経営を一層発展させていく上での課題や対策について、デジタルやDXなどの観点を含めながら考察を進めていく。

目次

目次

第１章
ESG経営の推進で一層注目される
ガバナンス関連施策とサイバーセキュリティ戦略

１．グローバル企業が最も注力するESG経営におけるガバナンス関連施策

- 近年、国内外ともに環境問題や企業の持続可能性、労働環境の改善等に配慮したESG経営を推進する動きが拡大している。
- 国内では自然災害などの環境問題などへの対策がESGの主要トピックとして注目を集める一方、GDP上位国などの諸外国では、イノベーションやサイバーセキュリティなどの施策がESG経営の注力領域とされている。特に近年は、著しいデジタル化の進展とともにサイバー攻撃の脅威も大幅に増加しており、サイバーセキュリティ対策はESGにおける重要分野の一つとして位置づけられている。

近年注目されるESGとしてのサイバーセキュリティ対策

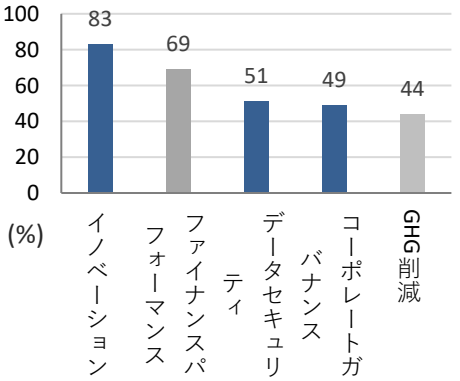
- 近年注目されるESG経営において、日本国内の動向からは、気候変動やウェルビーイング（労働環境）などの、主に環境や社会に関連する施策へ注力している様子が見られる。
- 一方で**GDP上位国の動向に目を向けると、ESG施策の中でも、特にイノベーションやサイバーセキュリティに関連する取組への優先度が高い**点が指摘されている（右図表）。
- 一般的に、**イノベーションやサイバーセキュリティに関連する施策は、ESGの中でも特にガバナンス（G）との関連が大きい。**グローバルにDXが拡大するなか、様々な業界において業務の自動化やデジタル技術を活用した新規事業の創出などが進んでおり、ガバナンス関連施策は、事業を継続的に発展させていく上で不可欠な要素となっている。
- デジタル化の著しい進展とともに、サイバー攻撃の種類も複雑かつ多様化している点が指摘されており、**企業にはDXと並行して、高度なサイバーセキュリティ対策を施すことが求められている。**実際に投資家などが企業のESG経営を評価する要素として、サイバーセキュリティへの対策は最も注目されるトピックの一つとなっている（次頁参照）。

（参考）欧米諸国と日本におけるESG注力施策の違い

図表１：GDP上位国と日本のESG注力分野比較（2016年～2018年）

順位	GDP上位10か国（日本を除く）			日本		
	2016年	2017年	2018年	2016年	2017年	2018年
1	規制等の影響	規制等の影響	イノベーション	気候変動	規制等の影響	気候変動
2	イノベーション	イノベーション	規制等の影響	規制等の影響	気候変動	ウェルビーイング
3	サイバーセキュリティ	サイバーセキュリティ	サイバーセキュリティ	ウェルビーイング	ウェルビーイング	イノベーション
4	気候変動	気候変動	気候変動	イノベーション	イノベーション	サイバーセキュリティ

図表２：グローバルのESG施策優先順位(2022年)



図表３：欧米と比較した日本のESG評価(2023年)

ESGの要素に関する評価で業界水準以上のスコアを出している業界の数。**日本はガバナンスのスコア(G Score)が特に低い。**

E score			S score			G score		
S&P 500	Stock Euro 600	TOPIX 500	S&P 500	Stock Euro 600	TOPIX 500	S&P 500	Stock Euro 600	TOPIX 500
12	11	4	10	12	3	22	13	0

参考：000212.pdf (meti.go.jp), ESG priorities for investors 2022 | Statista, Japan's Corporate Governance Enters New Phase (citigroup.com) を基に作成

２．サイバーセキュリティ対策は機関投資家が最も注目するESG評価のテーマの一つ

➢ 近年、ESG経営の観点でサイバーセキュリティ対策やガバナンス強化関連施策が企業価値を大きく左右する要素として位置づけられている。企業には、ビジネス戦略立案の段階からセキュリティ施策を策定するなど、組織の主要な戦略の一つとして、サイバーセキュリティを組み込むことが求められている。

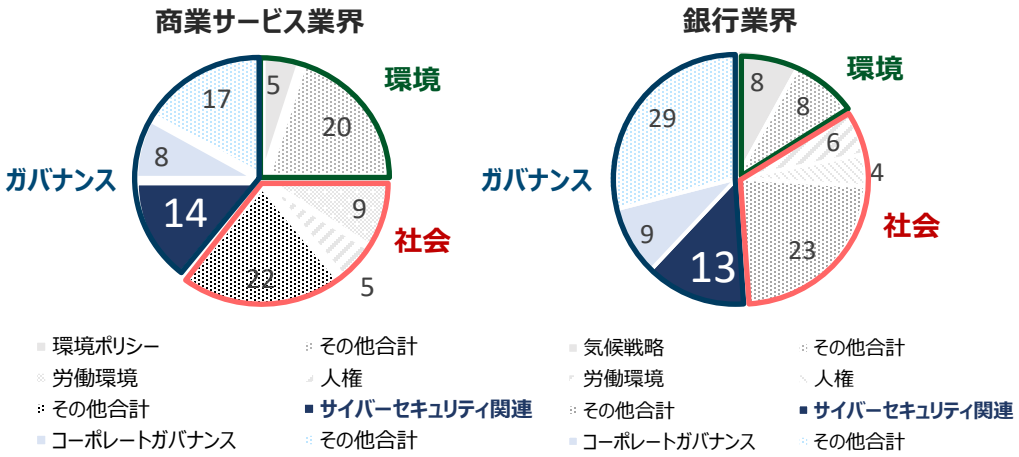
企業価値を左右するガバナンス施策

- ESG投資への注目が集まるなか、ガバナンス施策やサイバーセキュリティ関連施策への対応の充足度が、企業の経営評価を大きく左右する要素になりつつある。
- 実際にESG経営の対応レベルを評価するグローバルの指標を見ると、**ガバナンス関連施策に対する評価がESGの評価項目の中で最も大きな割合を占めている**ことが分かる。特に、情報セキュリティやシステムリスク管理など、**サイバーセキュリティ関連施策は他の項目と比較して重みづけが大きい**（下図）。

サイバーセキュリティは機関投資家が注目する主要テーマ

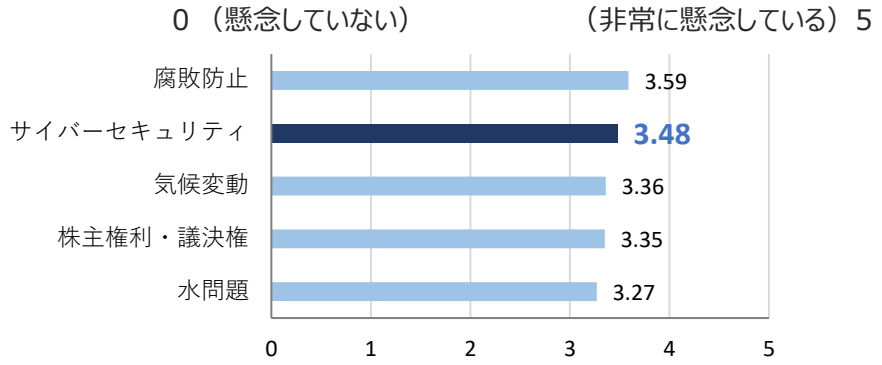
- RBC Global Asset Managementの調査によると、機関投資家が懸念しているESG関連テーマは、1位の「腐敗防止」に次いで、「**サイバーセキュリティ」が2位**となっている。**機関投資家の多くが企業を評価する主要な要素として、サイバーセキュリティ対策に着目している**点がうかがえる（下図）。
- また、PwCの調査レポート「24th Annual Global CEO Survey 」によると、**自社の成長見通しに対する懸念材料の第1位として、欧米のCEOが挙げたのがサイバー脅威**であった。

ESG評価におけるサイバーセキュリティ関連施策の割合（S&Pグローバルの例）



参考：Weights Overview Corporate Sustainability Assessment 2022 (spglobal.com)を基に作成。
＊Morgan Stanley Capital Internationalの指標ESG Investing: ESG Ratings - MSCIを見ても、商業サービスや金融などの業界で、ESG評価におけるサイバーセキュリティ施策への重みづけが大きいことが分かる。

機関投資家が懸念しているESG関連テーマ



参考：なぜESG格付けにおいてサイバーセキュリティの重要性が高まっているのか | PwC Japanグループを基に作成

３．　ESG経営における重要な開示項目としてのサイバーセキュリティ対策

- サステナビリティに関するグローバル基準のSASBやGRIでは、 企業の経営を判断する重要な項目としてサイバーリスクを挙げており、サイバーセキュリティ戦略の有無が企業の財務や評価に長期的な影響を与えると指摘している
- 企業には、サイバーセキュリティ対策に関する情報をステークホルダーに開示することが求められている

ESGに関するグローバル基準の例①　SASB

- ESGに関するグローバル基準の一つがSASB（Sustainability Accounting Standards Board）である。SASB は、企業がESG経営を推進する上での情報開示に関する業界固有の基準を提供している。
- SASBが定める基準は企業の財務評価を行う上でも重要な基準として示されているほか、投資家が企業の経営に関する様々な情報に基づいて、投資の意思決定を行うのに役立つ基準として位置づけられている。
- SASBは、一連の基準の中で組織の重要なデータやセンシティブ情報を侵害する可能性のあるサイバー脅威を取り上げるとともに、サイバー危機管理に関するガイダンスを提供している。
- **SASBが対象とするサステナビリティの重要なトピックの1つがサイバーリスク**であり、サイバーセキュリティ施策は**様々な業界に共通する横断的な企業の評価項目**として示されている。
- サイバーリスクとその対策に関する内容は、企業が積極的に情報開示を行う必要があり、**データセキュリティへの対策などはステークホルダーへの開示トピックにも含まれている**。

ESGに関するグローバル基準の例②　GRI

- ESGに関するグローバル基準としてGRI（Global Reporting Initiative)も挙げられる。GRIはサステナビリティの活動や事業の報告にも広く使用される基準であり、同基準には、**サイバーセキュリティとデータプライバシーに関する運営を開示するためのガイダンスが含まれている**。

サイバーセキュリティ対策はESGにおける重要な開示項目

- SASBとGRIはともに、**サイバーリスクをサステナビリティに関する情報として開示することを求めており、サイバー脅威が企業の財務や風評、および長期的な事業継続性に大きな影響を与える**可能性があることを指摘している。
- **近年、サステナビリティの要素としてサイバーセキュリティ対策の立案は企業が着手すべき重要な項目として示されている**。サイバー危機管理のプラクティスを開示し、セキュリティポリシーや対策に関する情報を提示することは、投資家や顧客、監督当局など、**企業を取り巻くステークホルダーに対する説明責任や透明性の証明に繋がる**。

参考：Cybersecurity in ESG - KPMG Globalなどを基に作成

４．サイバーセキュリティやガバナンスの情報開示に関する各国の規制・ルール

- 欧米では、サイバーセキュリティのリスク管理や戦略、ガバナンスの開示に関する各種法規制が強化されている
- サイバーセキュリティ対策やガバナンス管理の強化は企業が果たすべき重要な役割として示されており、サイバーセキュリティ対策やリスク管理、ガバナンスに関する情報をステークホルダーに開示することが強く求められている

国	法律・業界の規制	発行元	内容
米国 	US’ Cybersecurity Risk Management for Investment Advisers	Federal Register	ファンドの顧客に影響を及ぼす**重要なサイバーセキュリティインシデントを委員会に報告する**ことをアドバイザーに要求する
	Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure	SEC(U.S. SECURITIES AND EXCHANGE COMMISSION)	**重要なサイバーセキュリティインシデントや、サイバーセキュリティのリスク管理、戦略、ガバナンスを年次開示**する
	Regulation S-K Items 106	米国規制	**サイバーセキュリティに関するリスク管理、戦略、ガバナンスに関する情報を開示**する
欧州 	Digital Operational Resilience Act (DORA)	規則 (EU) 2022/2554	主な目的は、サイバー脅威の防止と緩和。企業がICT関連の混乱や脅威に対応し、回復できるようにするために、デジタル業務のレジリエンスに関する規制の枠組みを構築。
	the revised Network and Information Systems Directive(NIS2)	EU-wide legislation	EUにおけるサイバーセキュリティの全体的なレベルを高めるための法的措置を実施。
	Corporate Sustainability Reporting Directive (CSRD)	the European Commission and the European Parliament	大企業には、**欧州で確立された基準に従って非財務報告（社会、環境、ガバナンスに関連するリスク、重大な影響に関する詳細な情報）を公表する**ことが義務付けられる。

参考：Federal Register :: Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies; Reopening of Comment Period、SEC.gov | Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosureなどを基に作成

５．日本国内におけるサイバーセキュリティ対策への認識と現状

- 日本国内においても、DXの推進などによるデジタル技術活用の拡大やリモートワークの拡充などに伴い、従来以上に企業のセキュリティリスクが増大する点が指摘されている
- 一方で、ESG経営とサイバーセキュリティ対策との関係性は薄く、企業が事業を継続する上でサイバーセキュリティ対策を立案し、ステークホルダー向けに情報を開示していく重要性が十分に示されていないように見える

DXやデジタル化推進とともに増加するセキュリティリスク

- 国内では様々な業界においてDX推進の重要性が示されており、**企業は業務のデジタル化に向けた施策を強化**している。変化のスピードが著しい市場へ迅速に対応していくためには、クラウドなどのデジタル技術の活用が有効である点が指摘されている。
- 経済産業省が公開しているDXレポート 2.1では、デジタル社会の実現に向けて求められる産業構造について、市場の変化に迅速に対応し、他社との連携によって多様な価値を生み出していく必要性から、**固定的ではないネットワーク型の構造となる点**が示されている。
- 業務のデジタル化が急速に進むとともに、**システムを運用する場所やデータを管理する場所の多様化も進んでいる。**また、近年は働き方改革やリモートワークの拡充によって、**外部から企業の内部環境へアクセスする機会も従来以上に増加**している。
- クラウドやAPI、IoTなど新たなデジタル技術を活用するシステム環境や、データにアクセスする端末などが急速に増加すると、これに伴い、**セキュリティリスクが発生する箇所も大幅に増加**する点が指摘されている。

参考：https://usknet.com/dxgo/contents/dx-trend/increased-security-risks-with-dx/を基に作成

ESG経営とサイバーセキュリティとの関連性は示されていない

- **セキュリティリスクの増加に伴い、日本国内でもサイバーセキュリティ対策の重要性が指摘されている。**実際に、経済産業省が公表する「サイバーセキュリティ経営ガイドライン」では、企業の経営者を対象にサイバーセキュリティ対策を推進するためのガイドラインが示されている（4章に詳細記載）。
- ただし、ESG経営という観点においては、**サイバーセキュリティ対策に関連する国内の具体的な評価指標や、日本企業向けのガイドラインなどは公表されていない**（次頁参照）。
- また、欧米のように**ESG経営とサイバーセキュリティ対策との密接な関連性や、ESGの評価項目として情報を開示することについて、具体的な議論が十分になされていない。**
- ESGとサイバーセキュリティに関する法規制については、欧米と比較すると国内では十分に整備が進んでいない状態であるが、今後、**経済安全保障法の施行などにより、日本企業にもサイバーセキュリティ対策が本格的に求められる**ことが予想される（2章に詳細記載）。

参考：http://www.sompo-ri.co.jp/issue/quarterly/data/qt57-2.pdfなどを基に作成

【参考】サイバーセキュリティやESG経営に関連する日本のガイドライン・法規制

- **日本国内で公表されているサイバーセキュリティに関するガイドラインやESGに関する法規制において、ESG経営としてサイバーセキュリティ戦略や対策に関する具体的な情報の開示を義務付けているものはない**
- 一方で、近年多発するサイバーセキュリティの脅威を受けて、2022年より経済安全保障推進法が施行されており、企業にはサイバーセキュリティやガバナンスの観点で、今後対策を強く求められることが予想される。

１．サイバーセキュリティ経営ガイドライン（詳細は4章に記載）

- 経済産業省が、独立行政法人情報処理推進機構（IPA）とともに、ITに関するシステムやサービス等を供給する企業の経営者を対象に、サイバーセキュリティ対策を推進するための枠組みを策定したガイドライン。
- **経営層が取り組むべき施策などが示されているものの、ESG経営との明確な関連性については記載されていない。**

２．「企業内容等の開示に関する内閣府令」改正

- 開示原則には、「**サステナビリティ情報には**、国際的な議論を踏まえると、（中略）**サイバーセキュリティ、データセキュリティなどに関する事項が含まれ得ると考えられる**」と記載がある
- しかし、上記コメントに対する金融庁の考え方では「サステナビリティ情報については、**開示原則に示された全ての項目を記載する必要はなく、各企業が重要性を判断して情報を開示する**」という旨の記載がある。

３．ESG評価・データ提供機関に係る行動規範（金融庁）

- **金融機関向けのESG評価に関するガイドラインであるが、サイバーセキュリティの情報開示に関する具体的な記述はない**（以下抜粋）
  - ✓ ESG 評価・データ提供機関は（中略）サービス提供に当たっての基本的考え方を一般に明らかにするべきである。また、提供するサービスの策定方法・プロセス等について、十分な開示を行うべきである。
  - ✓ 投資家は、自らが投資判断等に用いている ESG 評価・データについて（中略）ESG 評価・データ提供機関や企業と対話を行うべきである。

４．経済安全保障推進法

- 国際情勢の複雑化や社会経済構造の変化等に伴い、安全保障の対象が急速に拡大するなか、国家や国民の安全を経済面から確保する取組を強化するための法律として成立
- 同法ではインフラ企業が管理する重要設備等について、政府が事前に審査する制度が導入されており、**対象企業にはサプライチェーンを強化するための対応や基幹インフラを安定的に提供することなどが求められる**（P18,19に詳細記載）。

参考：01.pdf (fsa.go.jp)などを基に作成

６．ESG経営の主要な評価軸として注目されるサイバーセキュリティ対策

- 欧米を中心にESG経営におけるサイバーセキュリティ施策の立案と強化の重要性が示されており、ステークホルダーに対してサイバーセキュリティ戦略の内容やポリシー等を示すことが企業の評価を大きく左右する要素となっている
- 近年のESG経営に関するグローバルの動向を鑑みると、日本企業にとってもESGの中心施策としてサイバーセキュリティ施策を確立するとともに、ステークホルダーに情報を開示するための準備を進めていくことが求められる

グローバル

- これまで述べたように、**欧米を中心にESG経営の主要施策として、サイバーセキュリティ対策やセキュリティリスクの管理強化などが挙げられており、企業を取り巻くステークホルダーへ十分に情報を開示する必要性が示されている**
- **背景として挙げられるのは、欧米におけるサイバーセキュリティのリスク管理やガバナンスの情報開示に関する各種法規制の強化である。**サイバーセキュリティ戦略を立案して、システムや事業を安全に運営していくための方針や手順などを整備していくことが、投資家や顧客、監督当局などに対する透明性の証明や説明責任へと繋がる。
- 実際にサイバー攻撃の多様化や増加に伴い、近年、投資家が企業のセキュリティ対策にも厳しい目を向け始めている。**ESG投資では、ESG（環境・社会・ガバナンス）の概念に加え、「サイバーセキュリティ（C）」対策を新たな評価軸に加える動きも広がりつつある*。**

日本

- 様々な業界でDXが推進されるなか、システム環境の多様化やリモートアクセス端末の利用拡大などが急速に進み、セキュリティリスクが大幅に増加している点が指摘されている。
- 近年多発するサイバー攻撃の脅威を受けて、経済安全保障推進法の施行やサイバーセキュリティ経営ガイドラインの改訂など、日本企業におけるサイバーセキュリティ施策の強化を促すための施策も立案されている。
- しかし、ESG経営における日本企業の注力領域や、サイバーセキュリティ施策との関連性を見ると、**国内ではサイバーセキュリティ戦略がESGの主要な要素として認識されておらず、十分な議論が進んでいない**ようにも見える。

⇒ **欧米のサイバーセキュリティ対策に関する動向や近年のESG経営に対する投資家の関心を鑑みると、日本企業もESGの中核施策としてサイバーセキュリティ戦略を立案し、予算の拡充や推進体制の強化を図っていく必要があるのではないだろうか。**

* サイバー攻撃被害、株価戻り鈍く　対策がESGの評価軸に - 日本経済新聞 (nikkei.com)
(2023年2月21日)

７．まとめ

➢グローバルにデジタル化の動きが加速するなか、企業にはDXの推進と併せてガバナンス関連施策の推進強化を図る必要性が指摘されている。特にサイバーセキュリティ戦略は、ESG経営の根幹をなす要素として近年大きく注目されており、企業はサイバー危機管理のプラクティスを立案し、セキュリティポリシーや対策に関する具体的な情報を投資家や顧客などのステークホルダーに提示することが求められている。

➢実際に欧米では、ESGに関する法規制として、環境や社会などへの事業方針の開示に加え、ガバナンスに関する投資やシステムリスクマネジメント、システムセキュリティに関する情報の開示が義務化されているほか、組織のガバナンス対策や管理体制に関する評価基準を示すガイドラインも公表されている。

➢システム環境の多様化に伴いサイバー攻撃の脅威も急速に増加している。欧米のESG経営に関する先進の動向やESG経営に対する投資家の関心を鑑みると、企業の事業継続という観点において、日本企業もESGの中核施策としてサイバーセキュリティ戦略を明確に位置づけるとともに、予算の拡充や推進体制の整備を早急に図っていく必要があると考えられる。

➢2章では、 1章で整理した内容を基に、欧米や日本のサイバーセキュリティに関連する法規制に着目して、グローバルな動向を整理するとともに、日本政府が推進する施策との比較などを行い、日本企業が直面している状況について考察を進める。

第２章
サイバーセキュリティに関する欧米日の法規制動向

１．サイバーセキュリティ対策に関する欧米の主な法規制

- 欧米ではサイバーセキュリティに関連する様々な法規制の対応整備が進められている
- 特に米国では、世界的に深刻な影響を及ぼした情報漏洩事件を受けて、大統領令や国家のサイバーセキュリティ戦略などが公表されており、サイバーセキュリティが国家の運営に不可欠なものとして位置づけられている

国	年月	法律	内容
欧州	2020年12月	「ネットワークおよび情報システムのセキュリティに関する指令（NIS指令）」改訂	**企業によるサプライチェーンセキュリティ対策の強化などを後押し**
ドイツ	2021年5月	「ITセキュリティ法2.0」を施行	**重要インフラの部品使用に関する事前届け出制を導入**
米国	2019年5月	「情報通信技術・サービス（ICTS）のサプライチェーン安全確保」の規則に関する大統領令が署名	過度もしくは容認できないリスクをもたらすICTS取引の中止やリスク軽減措置を行える
	2021年5月	国家のサイバーセキュリティ向上に関する大統領令（EO 14028）が公表	連邦政府および連邦政府と連携する民間業者が満たすべき高度なセキュリティ基準が7つの側面から示される
	2021年5月	**バイデン大統領が「国家のサイバーセキュリティ改善に関する大統領令」**に署名　（次頁に詳細を記載）	米サイバーセキュリティ・インフラストラクチャーセキュリティ庁（CISA）と米国立標準技術研究所（NIST）に、**重要インフラのサイバーセキュリティに関する実績目標を策定するよう命じた**
	2022年10月	**「CPGs（サイバーセキュリティ・パフォーマンス・ゴールズ）」**を公表　（次頁に詳細を記載）	**重要インフラ事業者が取るべき基本的なサイバーセキュリティ対策を示した**
	2023年3月	国家サイバーセキュリティ戦略を公表	**「サイバーセキュリティは経済の基盤的機能、重要インフラの運営、民主主義と民主的機関の強靭さ、個人のデータと通信のプライバシー、国家防衛に不可欠なもの」とその重要性を指摘**

参考：基幹インフラのサイバーセキュリティ保護 | 特集3 | 三菱総合研究所（MRI）、 バイデン米政権、重要インフラ向けのサイバーセキュリティー対策目標を策定(米国) | ビジネス短信 ― ジェトロの海外ニュース - ジェトロ (jetro.go.jp)などを基に作成

２．米国における主要なサイバーセキュリティ施策

- 米国では一連の大規模セキュリティ事件を受けて国家のサイバーセキュリティ改善に関する大統領令やサイバーセキュリティ・パフォーマンス・ゴールズ（CPGs）が公表されている
- 両施策では連邦政府および連邦政府と連携する民間業者が満たすべきセキュリティ基準や、重要インフラ事業者が取るべきセキュリティ対策が示されている

国家のサイバーセキュリティ改善に関する大統領令（2021年5月）

- SolarWinds社の大規模な情報漏えい事件（次頁参照）など、一連のセキュリティ事件を受けて発表された。
- 連邦政府および連邦政府と連携する民間業者が満たすべきセキュリティ基準が7つの側面(以下)から示されている。

1. 脅威情報の共有を阻む障害を取り除く
2. 連邦政府のサイバーセキュリティの近代化
3. **ソフトウェアのサプライチェーンセキュリティの強化**
4. 政府が運営するサイバー安全審査委員会の設立
5. **サイバーセキュリティの脆弱性等に対する対応の標準化**
6. 政府のネットワークにおける脆弱性と問題の検出強化
7. **調査および修復能力の向上**

⇒ **特に注目されるのが３となる**

- **「各製品のソフトウェア部品表(SBOM*1)を購入者に直接または公開Webサイトで提供すること」を要求**
- **「製品に使用されているOSS(*2)の完全性と出所を実行可能な範囲で確保し、証明すること」が必要となる**

参考：https://thinkit.co.jp/article/18611を基に作成

*1：SBOMについてはP26で内容を説明、*2：OSS（オープンソースソフトウェア）

サイバーセキュリティ・パフォーマンス・ゴールズ（CPGs）（2022年10月）

- 重要インフラ事業者が取るべき基本的なサイバーセキュリティ対策を示した
- 重要インフラに広く適用する対策をまとめ、事業者が対策の成熟度を測定・改善するための基準を示す

1. アカウントセキュリティ
2. 機器のセキュリティ
3. データセキュリティ
4. **ガバナンスおよびトレーニング**
5. **脆弱性の管理**
6. **サプライチェーン管理**
7. 事案対応および回復　、等

⇒ 重要インフラとして、**通信やエネルギー、金融サービス、医療・公衆衛生、情報技術、輸送システムなど16部門**が挙げられている

参考：https://www.jetro.go.jp/biznews/2022/11/c8e9ac6f668db081.htmlを基に作成

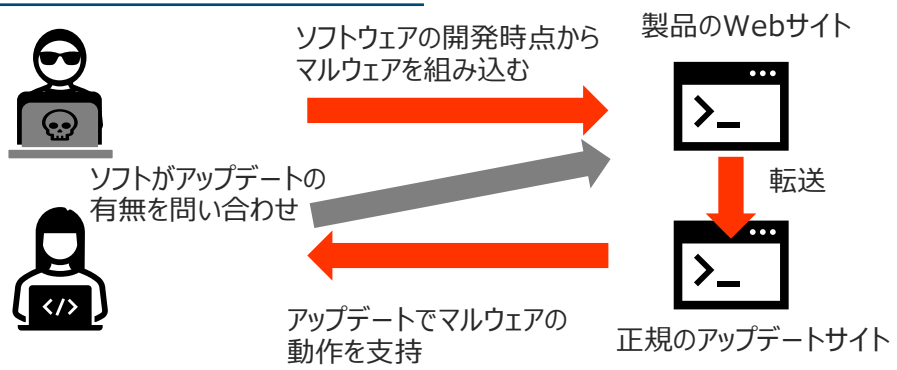
【参考】Solarwinds, Log4jの脆弱性をついた情報流出事件について

- 近年、ソフトウェアプロダクトの脆弱性を狙った大規模なサイバー攻撃が起こり、多くの組織に影響を与えている
- ソフトウェアはデータのやり取りやソフトウェア間の機能連携などにおいて相互依存していることが多く、脆弱性が発覚した場合の対応が難しい。ソフトウェアのサプライチェーン管理は多くの組織にとっての喫緊の課題となっている

Solarwindsのサプライチェーン攻撃

- 2020年12月、IT管理やリモート監視ツールの開発を行うSolarWindsは同社が開発するOrionにバックドア（悪意のあるコンポーネント）が含まれていたことを公表した。
- Orionは、企業のサーバーを遠隔から管理できるソフトウェアであり、**サプライチェーンに潜り込んだ攻撃者はサーバーのデータに容易にアクセスしたり、マルウェアを仕込むことができた**。
- 同製品は**米国の多数の政府機関や企業(18,000の組織)で導入されていたため影響範囲が非常に広く**、Microsoftなど大手企業のほか、日本でも被害が確認されている。

SolarWindsの攻撃の例



参考：SolarWinds社のサプライチェーン攻撃に見るDevSecOpsの重要性｜大塚商会（otsuka-shokai.co.jp）などを基に作成

Log4jの脆弱性

- システムのログを記録するためのソフトウェアApache Log4j（Log4j）に見つかった脆弱性。Log4jはオープンソースソフトウェアとして提供されており、Javaで開発されている。
- JavaはWebサーバーの開発などで広く利用されている言語であり、Log4jはOSSに標準で組み込まれていたため、非常に多くのソフトウェアに影響があった。
- 本脆弱性は、取り込まれたログに特定の文字列があると、攻撃者が仕込んだ悪意のあるプログラムをシステム内で実行できてしまうというものであった。脆弱性が発覚した直後から、本脆弱性を狙った無差別の攻撃がインターネット上で多数観測された。
- **システム上で稼働するソフトウェアはデータのやり取りやソフトウェア間の機能の連携などにおいて相互に依存し合っている状態であることが多く**、脆弱性が発覚した場合も、**該当のソフトウェアを単純に削除したり、すぐに取り換えることが難しい**という特徴がある。この問題は、システム特有の構成や特徴などから、**ソフトウェアのサプライチェーン問題**と言われている。

参考：「Log4shell」は何故これだけ騒がれたのか ｜ コラム (ipa.go.jp)、【Infostand海外ITトピックス】「Log4j」脆弱性発見から1年　OSSセキュリティの努力は続く- クラウド Watch (impress.co.jp)などを基に作成

３．日本におけるサイバーセキュリティ関連法規制（経済安全保障推進法）

- 国際情勢の複雑化や社会経済構造の変化等に伴い、安全保障の対象が急速に拡大するなか、国家や国民の安全を経済面から確保する取組を強化するための法律として、2022年5月に経済安全保障推進法が成立した
- 同法ではインフラ企業が管理する重要設備等について、政府が事前に審査する制度が導入されており、対象企業にはサプライチェーンを強化するための対応や基幹インフラを安定的に提供することなどが求められる

経済安全保障法制の4分野

目的	制度の概要
①重要物資のサプライチェーン強化	▪ 海外への依存度が高く、国民の生活に必要不可欠で重要な物資の安定供給確保を図るため、助成金や利子補給により事業者の取り組みを支援 ▪ 支援のみで安定供給が困難な場合、政府備蓄、価格安定化措置を実施 ▪ **サプライチェーンの実態を把握するため関係者に対し調査を実施**
②基幹インフラの信頼性確保	▪ **基幹インフラ（通信、電力、運輸、金融ほか14事業*次頁参照）の安定的な提供を妨害する手段に使用される恐れがある設備を、導入計画に基づき審査** ▪ **インフラの構成設備（機器、プログラムを含む）が、妨害行為の手段に使用される恐れが大きいときは、防止策を勧告または命令**
③重要先端技術の開発推進	▪ 先端技術のうち、外部により悪用された場合は利用を制限された場合に、国家および国民の安全が脅かされる恐れがある技術の研究開発について支援（情報提供、資金確保、調査研究など）し、技術的な優位性を確保 ▪ 官民協議会を設置し研究開発を進めるとともに、技術情報や成果を管理 ▪ 研究開発戦略を支援するためシンクタンクによる調査研究を実施
④非公開特許制度	▪ 公開により国家、国民の安全を損なう恐れが大きい発明の特許出願について、発明の開示や実施を制限する制度を創設 ▪ 特定技術分野に関する特許出願について、内閣府が保全審査を実施し非公開化

参考：外交・安全保障　第2回：経済安全保障推進法の成立と今後の注目ポイント｜三菱総合研究所（MRI）を基に作成

４．経済安全保障推進法で求められるセキュリティ対策とサプライチェーン管理

➢ 経済安全保障推進法で特に注目されるのは、基幹インフラサービスを提供する事業者へのサプライチェーン管理やセキュリティ対策への強化である。同法では、サイバー攻撃によるシステム障害や情報流出のリスクなどが審査され、事業運営やサプライチェーンの見直しなど、企業にはリスク低減に必要な措置を勧告・命令することが想定される

基幹インフラ事前審査制度（次頁に詳細記載）

- 前頁「②基幹インフラの信頼性確保」に関して、インフラ企業が重要設備（システムを含む）の導入等を行う場合に、**政府が事前に審査する制度（基幹インフラ事前審査制度）が導入**された
- 審査においては、**サイバー攻撃によるシステム障害や情報流出のリスクなどが検討され、審査の結果、リスク低減に必要な措置（設備の導入・維持管理の内容の変更・中止など）を勧告・命令される**場合がある
- 対象事業者はその義務を履行するために、**対象設備（設備・機器類、プログラムなど）、供給者・委託先などに関する届出事項の把握やデータマネジメント、リスク管理措置を実施し、場合によっては委託先などの見直しが必要**となる

スケジュール	内容
2023年5月	基本方針の策定
2023年11月17日	14業種210の対象事業者（企業や団体）を指定
2024年5月17日	制度運用開始

対象インフラ事業者と審査義務

- 基幹インフラサービス14業種（以下）に関して、対象事業者に**重要設備の導入・維持管理などの委託に関する計画書の届出をさせて、国による審査を受ける義務**を課している
- **重要設備を提供する企業や、対象企業に部品等を提供する企業、特定重要設備を管理する企業**も影響を受ける

1. 電気事業
2. ガス事業
3. 石油精製業および石油ガス輸入業
4. 水道業および水道用水供給事業
5. 第一種鉄道事業
6. 一般貨物自動車運送事業
7. 貨物定期航路事業および一定の不定期航路事業
8. 国際航空運送事業および国内定期航空運送事業
9. 空港設置・管理事業および空港にかかる公共施設等運営事業
10. 電気通信事業
11. 基幹放送を行う放送事業
12. 郵便事業
13. 保険業、第一種金融商品取引業その他一定の金融にかかる事業
14. 包括信用購入あっせんの業務を行う事業

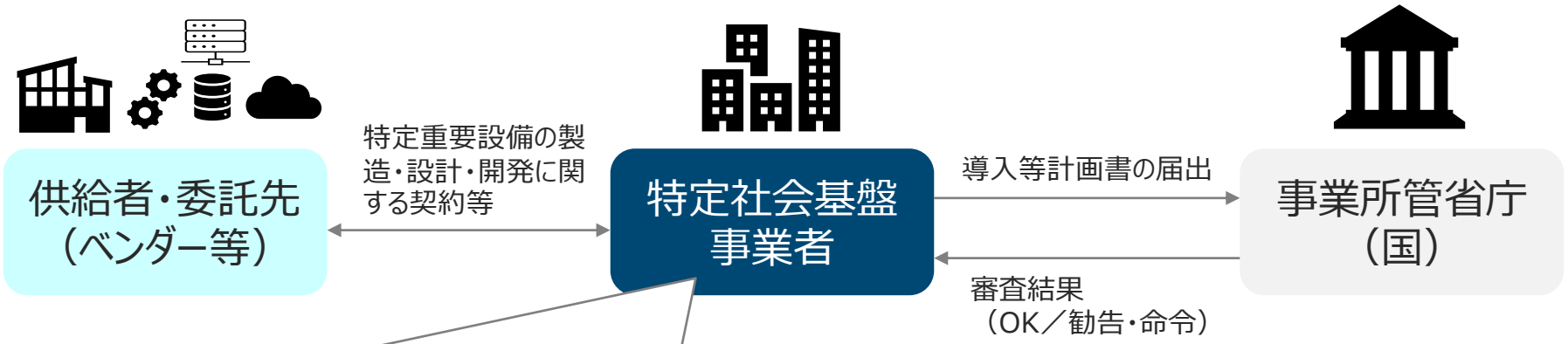
参考：経済安全保障リスク対応の現在地　Part1 - KPMGジャパン, 政府 基幹インフラ設備導入の事前審査対象に210事業者を指定 | NHK | サイバー攻撃などを基に作成

【参考】経済安全保障推進法「基幹インフラ事前審査制度」の概要

- 基幹インフラ事前制度における政府の審査内容については、未だ未確定な要素も多く、**政府への提示する情報や対象企業のリスク評価については、統一された基準や取り決めはなく当面は個社ごとの判断になる模様**
- 政府からは対象の事業者の評価を実施する過程で、必要な情報の提示を随時求められることが予想される

基幹インフラ事前審査制度の概要

- 国が一定の基準のもと、規制対象とする事業者（特定社会基盤事業者）を指定し、同事業者が、国により指定された重要設備（特定重要設備）の導入・維持管理の委託をする際に、事前に国に届け出をして審査を受ける制度
- 国は、届け出られた計画書に係る特定重要設備がサイバー攻撃などの妨害行為の手段として使用される恐れが大きいと認めるときは、妨害行為を防止するために必要な措置を講じた上で重要設備の導入等を行う事を勧告（命令）できる



基幹インフラサービス14業種

１．電気	２．ガス	３．石油	４．水道	５．鉄道
６．貨物自動車運送	７．外航貨物	８．航空	９．空港	１０．電気通信
１１．放送	１２．郵便	１３．金融	１４．クレジットカード	

参考：231006_商工会議所「経済安全保障推進法」に関するセミナー.pdf、経済安全保障推進法基幹インフラ役務提供に伴う事前審査対応支援サービス｜PwC Japanグループを基に作成

５．日米の法規制に関する比較・共通点と注目されるサプライチェーン管理

- 米国では、国家のサイバーセキュリティ改善に関する大統領令やCPGsなど、セキュリティに関連する法規制が大幅にアップデートされている。特に注目されるのがソフトウェアのサプライチェーンセキュリティ強化に関する施策である
- 一方、日本国内でも経済安保推進法によって企業のサプライチェーンに関する審査が義務化されるなど、米国と類似した施策が提示されている。先行する米国の事例を参考に日本企業も対策を施していく必要があるだろう

米国の動向

- 米国では、ソフトウェアの脆弱性をついた大規模なサイバー被害が多発しており、近年、**国家のサイバーセキュリティ改善に関する大統領令やCPGsなど、サイバーセキュリティに関連する法規制が大幅にアップデート**されている。
- **特に注目されるのがソフトウェアのサプライチェーンセキュリティの強化に関する内容**であり、企業には自社が運用しているシステムやソフトウェアを適切に管理して、その情報を当局やステークホルダーに開示することが求められるなど、サイバーセキュリティに関する対策や管理体制の強化が義務化されている。
- サイバーセキュリティに関連する法規制への対応は、企業の評価にも大きく影響を与えるほか、**十分な対策がなされない企業にはサプライチェーンやサプライヤーの見直しも求められる可能性がある**など、事業継続にも大きな影響を与えることが想定される。
- **法規制への対応やサイバーセキュリティ対策の強化は、グローバル企業にとって喫緊の課題**である。

日本の現状と今後の動向

- 国際情勢の複雑化や欧米の法規制強化の流れを受けて、**日本では企業や組織のサイバーセキュリティ対策の強化を目的とした経済安全保障推進法が施行**されている。
- 同法では、主要なインフラ事業を担う14業種に関する設備の導入や維持管理に関する審査が義務化される予定であり、**企業のサプライチェーンに関する安全性の審査が行われるなど、米国と同様の施策が提示**されている。
- 今後、**企業にはサプライチェーンに関するセキュリティの強化施策や管理が強く求められることになり、十分に対応できない企業にはサプライチェーンの見直しなど、厳格な措置がとられる**ことが予想される
- グローバルの動向を鑑みると、**米国のようにソフトウェアの構成を含めたサプライチェーンの情報や管理体制について、政府から情報の提示を求められる可能性**がある。先行する米国の事例を参考に日本企業も対策を検討していく必要があるだろう。

６．まとめ

➢ソフトウェアサプライチェーンの脆弱性をついた攻撃が深刻化するなか、欧米ではサイバーセキュリティに関する様々な法律やガイドラインが施行されている。法規制への対応は、企業の戦略立案や事業内容にも大きく影響を与えることが想定され、サイバーセキュリティ対策の見直しや強化はグローバル企業にとって喫緊の課題となっている。

➢一方、日本国内でも経済安保推進法が施行され、今後、様々な業界にサプライチェーン管理やセキュリティへ対策の強化が求められると予想される。現時点では法規制が拘束力を十分に発揮していないものの、対象事業者の審査が進み、制度運用が本格的に始まると、国内においてもサイバーセキュリティ関連施策への対応や議論が急速に加熱すると考えられる。

➢グローバルの動向を鑑みると、企業にはソフトウェアの構成を含めたサプライチェーンの情報や管理体制について、政府から情報の提示を求められる可能性がある。安全性が十分に証明されない企業にはサプライチェーンの見直しなど厳格な対応が求められる場合もあるため、先行する米国の事例などを参考に、日本企業も対策を十分に検討していく必要があるだろう。

➢3章ではセキュリティ対策の強化が加速する米国について、近年のサイバーセキュリティ市場の動向や米国企業が取り組む施策を紹介するとともに、日本企業が今後取り組んでいくべきサイバーセキュリティ施策のヒントを探る。

第３章
米国のサイバーセキュリティ動向と米国企業が推進するサイバーセキュリティ戦略
-ソフトウェアサプライチェーンとデータ保護対策が鍵-

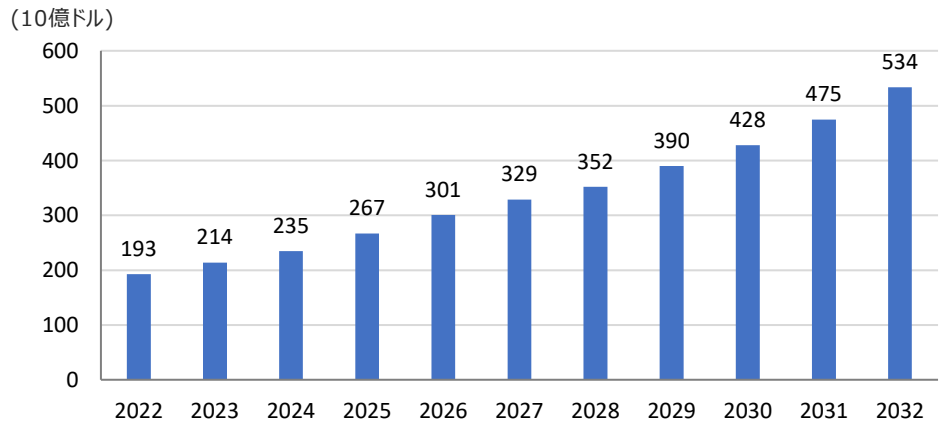
１．サイバーセキュリティサービスに関するグローバルの市場動向

- 世界のサイバーセキュリティ市場は、2022年以降の10年間で約3,400億米ドルを超える成長となる見込み
- 近年は、クラウドやAI、ブロックチェーンなどインターネットを通して利用できるサービスが大幅に増加している一方、外部から攻撃を受けるポイントも増加しており、多様化する攻撃に対応するソリューションへの需要が高まっている

サイバーセキュリティの市場はグローバルで大きく成長

- 世界のサイバーセキュリティ市場は、2022年の1,930億米ドルから**2032年までに5,340億米ドル**を超えると予想されており、**2023年から2032年までのCAGRは11%**に達する見込み。
- 新興企業によるECプラットフォームやIoT 、クラウド、AIを対象にしたセキュリティ製品が、サイバーセキュリティ市場の成長を推進する主要な要素となっているほか、大手企業はAIを活用したインターネットセキュリティソリューションの開発に注力している。

グローバルのサイバーセキュリティ市場推移



参考：https://finance.yahoo.com/news/cyber-security-market-size-valued-104600974.htmlを基に作成

サイバーセキュリティ市場成長の主な要因

サイバーセキュリティ市場を牽引する主な要素は以下の3つ

1. 技術の進歩

クラウド、AI、ブロックチェーンなどのデジタル技術の進歩や新技術を活用したECプラットフォームの増加によって、**企業がサイバーセキュリティ対策を施す対象が拡大。**

2. クラウドコンピューティングの台頭

SaaSの利用拡大やハイブリッド環境（クラウドとオンプレミスを接続するシステム環境）の構築などによって、**インターネットと社内のシステム環境の接点が大幅に増加（外部からの攻撃リスクが増加）。**

3. 北米市場が世界の市場を牽引

北米は世界のセキュリティ市場の成長を大きく牽引している。**市場全体に占める北米の売上シェアは36%**にものぼり、**米国内におけるIT企業数やビジネスの多様性、資本量**などが、セキュリティ市場成長の主要な要素となっている。

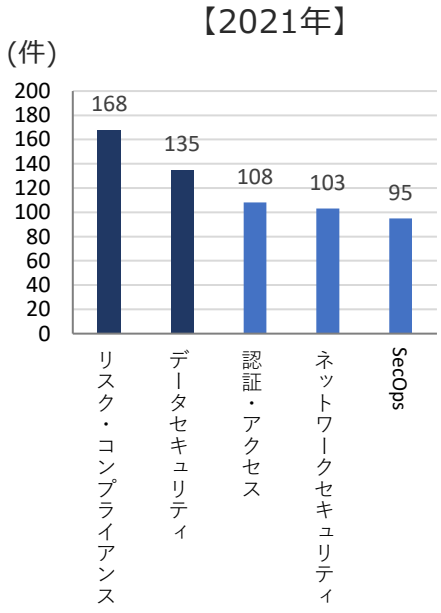
参考：http://www.sompo-ri.co.jp/issue/quarterly/data/qt57-2.pdfなどを基に作成

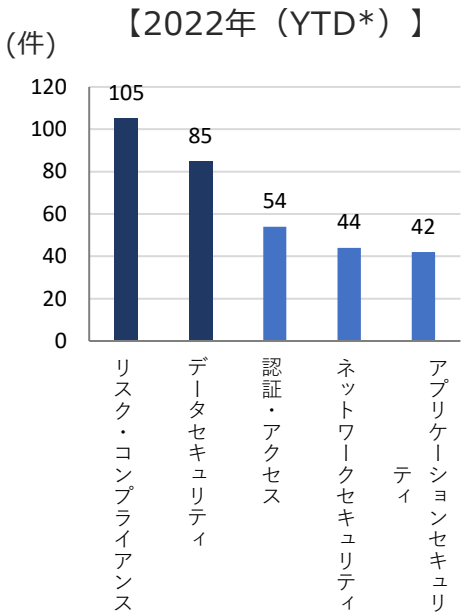
２．サイバーセキュリティ市場で特に注目されるリスク・コンプライアンスとデータセキュリティ

- サイバーセキュリティ市場の中でも、特に資金調達の動きが活発化しているのがサプライチェーンの管理やデータ保護に関するデジタルソリューションやサービスである
- 近年、サプライチェーンの脆弱性をついた大規模な攻撃がグローバルに増加するなか、企業内のシステム環境に留まらず、サードパーティを含めたソフトウェアやデータを統合的に管理して対策を施す重要性が指摘されている

セキュリティ市場において特に注目される2つの領域

- 不安定な市場の状況下においても、特に**リスク・コンプライアンスとデータセキュリティに関連する製品やサービスの取引の割合は、全体の取引件数の中でも最も多く**、近年、市場の上位を占めている（下図）





参考：momentumcyber.com/docs/Quarterly/Cybersecurity_Market_Review_1H_2022.pdfを基に作成

*Year To Date（2022年初日から当レポート集計直近の日付までの期間）

リスク・コンプライアンス（サプライチェーンの可視化・管理）

- リスク・コンプライアンスに関連するソリューションとして注目されるのが**ソフトウェアサプライチェーンの可視化や管理機能**である。
- P16で述べたように、**米国の大統領令で情報開示が求められているSBOM（サードパーティーも含めたソフトウェア全体を一元的に管理する概念、次頁参照）は関連ソリューションの数も多く**、グローバルに見ても大きい市場分野である。

データセキュリティ

- **データセキュリティに関連ソリューションとして近年注目される概念の一つがDSPM**（次頁参照）である。DSPMはオンプレミスやクラウドなど、企業が管理するすべてのシステム環境を含めたデータを統合的に管理するためのソリューションである。

⇒ リスク・コンプライアンスやデータセキュリティに共通して求められるのは、サードパーティを含めたシステムやデータの統合的な管理の強化である。近年は**企業内のシステム環境に留まらず、企業がオペレーションを実行しているクラウドやサードパーティ環境も含めた包括的なセキュリティ対策の重要性**が指摘されている。

【参考】SBOMとDSPM

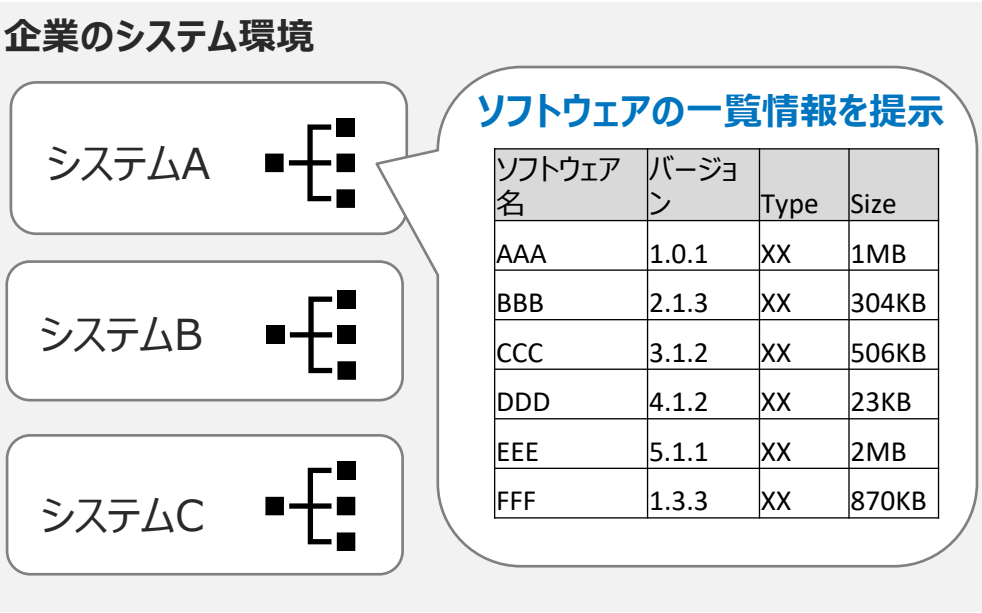
SBOM

- SBOM（Software Bill of Materials：ソフトウェア部品表）は、ソフトウェアを構成するOSSや商用ソフトウェアなどのライブラリやモジュールの情報を統合的に管理するソリューション
- ソフトウェアを構成するコンポーネントやソフトウェア同士の依存関係、ライセンスデータなどをリスト化した一覧表であり、OSSのライセンス管理や脆弱性の管理、ソフトウェアサプライチェーンのリスク管理等の用途で利用（下図参照）
- ソフトウェアサプライチェーンにおける透明性の証明やトレーサビリティの管理に有効な手段として世界的に普及が進んでいる

DSPM

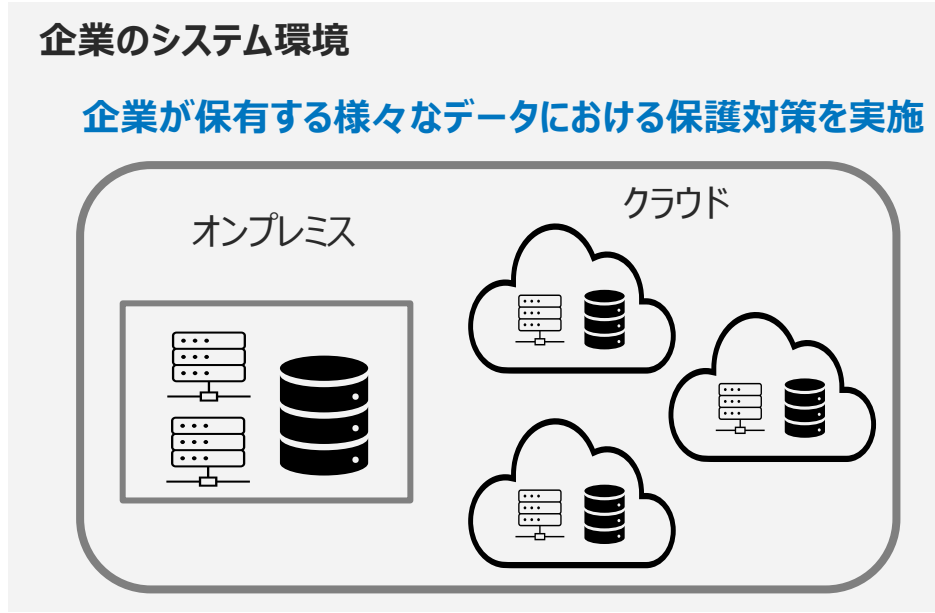
- DSPM（Data Security Posture Management、データセキュリティ態勢管理）は、オンプレミスやクラウドに存在する社内データや顧客データなどの機密情報をモニタリングし、そのデータが適切なセキュリティ対策や保護を受けているかどうかをチェックする仕組み
- Gartnerの定義によると、組織が保有するデータの可視化や分類(データのリスクやデータ保護の優先順位付け)、データにアクセスできる権限の可視化、データの取り扱いに関するユーザの行動の監視などを行う管理・運用などを指す

SBOMの概要図



ソフトウェア名	バージョン	Type	Size
AAA	1.0.1	XX	1MB
BBB	2.1.3	XX	304KB
CCC	3.1.2	XX	506KB
DDD	4.1.2	XX	23KB
EEE	5.1.1	XX	2MB
FFF	1.3.3	XX	870KB

DSPMの概要図



３．米国ベンチャーキャピタルが見る米国のサイバーセキュリティに関する最新動向

- 米国企業の経営層の多くが、近年サイバーセキュリティソフトウェアへの投資を一層増加させている
- 背景には、複雑化するサイバー攻撃への対応やデータ保護規制、ソフトウェアサプライチェーン管理などへの対応が挙げられており、サイバーセキュリティ戦略は新興企業から大企業に至るまで立案が不可欠な要素となっている

サイバーセキュリティへの投資増加と求められるデータ保護強化

- 米国企業のCISOの多くが、**近年サイバーセキュリティ対策を最優先事項にしている。**サイバー攻撃が複雑化するなか、企業にはより洗練された防御ツールの導入が求められており、**サイバーセキュリティ対策への投資は増え続けている。**
- サイバーセキュリティへの投資が増加する背景のひとつは、**データ保護に関する規制への対応**である。グローバル企業にとって、GDPRやPII(*1)への順守は、企業が事業を継続する上で不可欠な施策である。
- TargetやHome Depotのような大企業で発生した情報漏えいは企業や顧客に与えた影響も深刻であり、近年のサイバー攻撃は米国企業にとって事業の存続を揺るがす事態となっている。
- **サイバーセキュリティ戦略は、新興企業から大企業に至るまで、企業の規模に関わらず立案が欠かせない要素**である。新興企業であっても、SOC2やISO27001、PIIの認証取得など、十分なセキュリティ対策を講じなければ、米国の市場でユーザーにサービスを売り込むことはできないだろう。

ソフトウェアサプライチェーンへの対策は過熱傾向

- 近年ソフトウェアサプライチェーンセキュリティが注目されており、**多くの企業が自社やサードパーティを含めたサプライチェーン管理の強化のために、多額の投資をしている。**
- とくに政府機関からの委託を基に業務を行うベンダーには、SBOMの提示が求められており、システムの安全性やセキュリティ対策を十分に検証しなければならない。
- **自社の製品やサービスにサイバー攻撃を受ける可能性があったり、悪意のあるコードが含まれている場合、組織はサプライチェーン全体を見直す必要に迫られる(*2)。**
- 米国のサイバーセキュリティに関連する法案（P16参照）は、政府関連の事業者だけでなく、より広範な組織や企業に対象が拡大されることになるだろう。
- 今後様々な業界で、**SBOMを通して組織内のソフトウェアに関するセキュリティレビューを行うことが義務化される**だろう。

参考： Geodesic CapitalのDivya Sudhakar(Partner), Will Horyn(Vice President)からヒアリングした内容(2023年10月20日)を基に作成
*1 PII(Personally Identifiable Information):特定の個人を識別するために使用される一連のデータ。個人情報。
*2 米国ではソフトウェアサプライチェーンの安全性を確保できない企業に対して罰則や罰金を科す法案も検討されているほか、ソフトウェアの十分なセキュリティ対策が取れない企業は米国市場からの撤退を余儀なくされる点が指摘されている。https://www.activestate.com/blog/how-to-avoid-software-supply-chain-fines/

４．コストセンターからプロフィットセンターへとシフトする米国のサイバーセキュリティ戦略

- 米国でサイバーセキュリティが重視されるのは、グローバル市場で大きな影響力を持つ企業の割合が多い点にある
- サイバーセキュリティへの投資が急増する米国では、セキュリティ機能が競争上の優位性を確立して他社との差別化要因になるなど、サイバーセキュリティ対策がコストセンターからプロフィットセンターへとシフトする動きも見られる

米国でサイバーセキュリティ対策が重視される背景

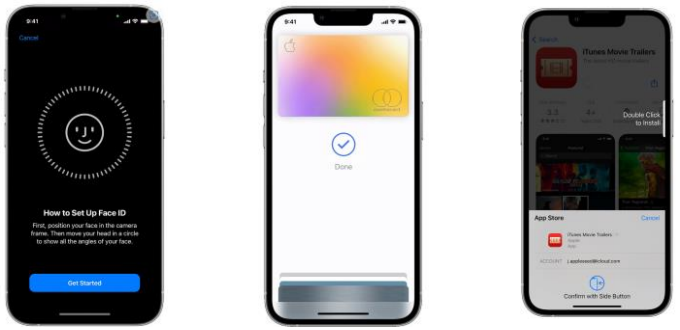
- 米国企業はサイバー攻撃を受ける機会が多い反面、サイバーセキュリティ対策もいち早く発達し、同対策が企業の主要施策の一つとして位置づけられている。これは、米国で設立された企業が、**グローバル市場において大きな影響力や多数の顧客データを持ち、攻撃者にとって価値の高い情報として認識されているためである。**
- これまで米国企業はWebやクラウド、AIなど、先進テクノロジーの導入や越境サービスの展開を通して、**デジタルを活用したインフラの構築において国際的に先陣を切ってきた**経緯がある。
- 一方で、**デジタルインフラへのパラダイムシフトは**組織のシステム環境をよりオープンな状態にするとともに、**組織の脆弱性を広く晒すことにも繋がる。**またグローバル化の加速によって、GDPRのような**他国の規制にも迅速に対応する必要も出てくる。**
- **企業の事業拡大とともにデジタル技術の活用度も上がり、国際的なプレゼンスが高まった**ことで、米国企業は他国と比較して、**迅速かつ厳格なセキュリティ対策を講じる必要に迫られた。**

セキュリティ機能を活用した付加価値の向上

- 近年、米国では**サイバーセキュリティ対策が、コストセンターからプロフィットセンターへとシフトしている**動きが見られる。セキュリティ機能が競争上の優位性を確立し、**製品がセキュアであることが差別化要因になっているケース**がある。
- 例えば、**Appleは個人のプライバシーやデバイス、システムに関する一連のセキュリティ機能を当社独自の売りにしている。**これはセキュリティを守りの観点ではなく、製品を一層魅力的に見せるアプローチへと置き換えた事例であると言える。

セキュリティ機能を製品の差別化要因としている例（AppleのFaceID）

AppleのFaceIDは本来セキュリティ機能であるものの、ユーザーにとってはデジタル体験を向上させるiPhoneの魅力的なユーザーインターフェースの一つとして見られている



参考：Geodesic CapitalのDivya Sudhakar(Partner), Will Horyn(Vice President)からヒアリングした内容(2023年10月20日)を基に作成

出典：Use Face ID on your iPhone or iPad Pro - Apple Support

５．まとめ

➢米国においてサイバーセキュリティは成長率の高い市場であり、多くの経営層がサイバーセキュリティへの投資を最優先事項として挙げている。GDPRやPIIなどに関連する各国の法規制への準拠は、グローバル企業にとって対応が不可欠であり、迅速かつ厳格なセキュリティ対策が企業のプロダクトの評価や信頼を大きく左右する。サイバーセキュリティ対策や戦略の立案は、業種や事業規模にかかわらず、様々な企業において欠かすことができない要素となっている。

➢法規制のアップデートや大規模なセキュリティ被害の増加に伴い、セキュリティ分野の中でもリスク・コンプライアンスやデータセキュリティは近年資金が大きく投入される領域である。特にサードパーティを含めたソフトウェアサプライチェーン管理やデータの保護対策など、組織のシステム運用状況やIT資産状況を統合的に可視化・管理する対策は、米国において取り組みが一層進んでいる領域である。

➢米国では、企業のセキュリティ戦略がコストセンターからプロフィットセンターへと変わるパラダイムシフトが進んでいる。セキュリティ対策は企業にとって競争上の優位性を示す要素でもあり、近年はセキュリティ機能の充実性を示すことがユーザーにサービスを提供する上での差別化要因になりつつある。システムセキュリティやプライバシー保護を製品の主力機能として位置づけるような戦略への転換も起きている。

➢1章から3章まで考察した内容を参考に、最終章となる４章では、日本のサイバーセキュリティ対策に関する概況や法規制の動向を整理して、日本企業の現状を把握するとともに、日本企業が直面している課題や将来対策が求められる事項などについて考察・検証を行う。

第４章
サイバーセキュリティ戦略の発展に向けた日本企業の課題と対策

１．日本企業におけるサイバー攻撃の被害件数及び被害総額

- 日本国内でもサイバー脅威は深刻化しており、2012年以降の10年間でサイバー攻撃の通信が約66倍増加している
- また、2022年に日本国内で起こったサイバー攻撃の被害額は1,045億円にものぼり、前年と比較して約3.3倍増加している

直近10年間にわたるサイバー攻撃の増加

- 近年、日本国内でもサイバー攻撃の数が急増している。情報通信研究機構（NICT）の調査によると、**サイバー攻撃に関連する通信は2012年からの10年間で66倍増加した**。
- 2021年の1年間では、サーバ攻撃に関する通信が5,180億パケットにまで到達している。平均計算で1IPアドレスあたりに、年間174万パケットのサイバー攻撃が観測されており、**国内でもサイバー脅威が急拡大している状況**である。

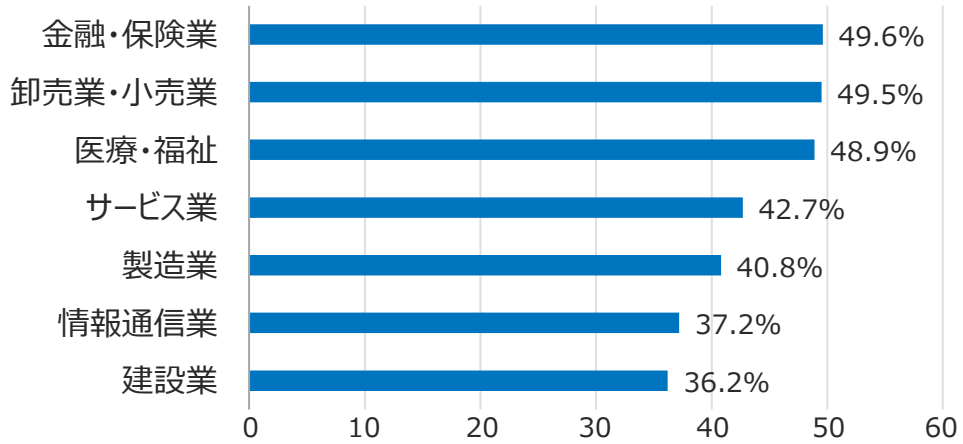
サイバー攻撃に関連する通信（年／パケット数）

出典：国立開発研究法人情報通信研究機構「NICTER観測レポート」

サイバー攻撃による被害総額

- サイバー攻撃による金銭的被害も決して少なくない。**2022年の1年間に日本国内で起こったサイバー攻撃の被害額は1,045億円であり、前年と比較して約3.3倍増加している**。
- サイバー攻撃に対する不安が大きくなったと回答する業種のトップは、金融業や卸売業・小売業など、顧客の機密情報や個人情報を多く扱う業種である。また、後述するように、近年は医療機関においても、大規模なサイバー攻撃を受けて診療サービスの停止などに追い込まれる深刻な被害が発生している。

1年前に比べてサイバー攻撃に対する不安が大きくなったと回答した割合



参考：https://scan.netsecurity.ne.jp/article/2023/04/13/49202.html, https://www.cybersolutions.co.jp/news/20230412/」などを基に作成

２．日本企業におけるサイバー攻撃の発生率及び対策状況

- 2023年に実施したアンケートによると、日本国内では一年以内に８割以上の企業がサイバーインシデントを経験している
- 一方、セキュリティ対策にかける予算不足などの理由により、サイバー攻撃への対策を十分に講じている企業は半数以下に留まる

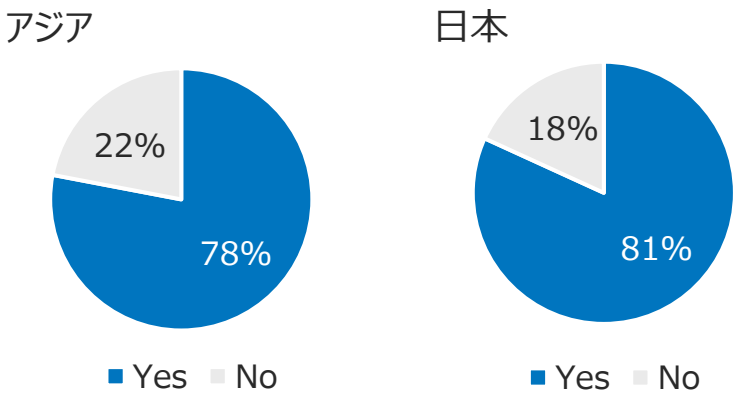
日本国内では8割以上の企業がサイバーインシデントを経験

- 日本を含むアジアで実施したサイバーセキュリティ対策に関する2023年の調査では、**回答者の78%が、過去12カ月の間に1回はサイバーセキュリティインシデントを経験している**
- また、日本企業単体の回答結果では、**81%が過去12カ月の間に少なくとも1件のサイバーセキュリティインシデントを経験している**
- 日本で最も被害が多いサイバーセキュリティインシデントは、マルウェアや、ビジネスメール詐欺、ランサムウェア・スパイウェアなどである

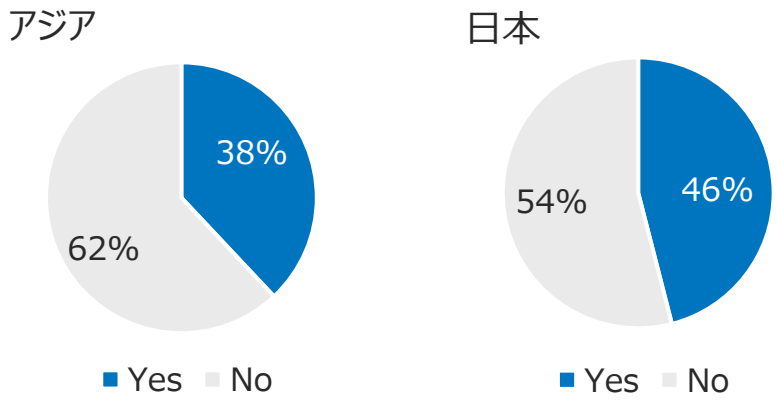
半数以下がサイバーセキュリティへの対策を不十分と回答

- アジアではサイバーセキュリティインシデントが増大しているにもかかわらず、**サイバー攻撃への対策を十分に講じていると回答したのはわずか38%**であった
- 日本においても、**サイバー攻撃への対策を十分に講じていると回答したのは半分以下の46%**にとどまっている
- 背景として挙げられるのは、**セキュリティ対策に割り当てられる予算が十分でない、慢性的な人材不足が発生しているなどの点**である

過去12ヶ月の間に１回はサイバーセキュリティインシデントを経験したことがあるか（2023年）



自社はサイバー攻撃への対策を十分に講じていると思うか（2023年）



参考：アジア太平洋地域の企業、セキュリティ対策が万全は38%--Cloudflare調査 - ZDNET Japanを基に作成

第４章

３．日本国内でも増加するサプライチェーンの脆弱性をついたサイバー攻撃

➢ 近年、企業を取り巻くサプライチェーンの脆弱性をついたサイバー攻撃が急増しており、自社のセキュリティ対策のみならず、委託先や調達先などのサードパーティを含むサプライチェーン全体におけるセキュリティ対策の強化が求められている。

セキュリティ脅威の裏に潜むサプライチェーンリスク

- 2023年の国内のセキュリティ脅威には、ランサムウェアや標的型攻撃など様々な脅威が挙げられている。**これらに共通するのは、委託先などを含むサプライチェーンの構成やソフトウェア、データ管理の脆弱性などを突いた攻撃**という点である。
- 実際に近年はサプライチェーン管理体制の不備などに起因するサイバー被害や情報漏洩が多発しており（右側に事例を記載）、**サードパーティや委託先との業務連携を行う組織や企業にとって、サプライチェーンの管理強化が急務**となっている。
- 政府もこの点を懸念しており、経産省が公表したサイバーセキュリティ経営ガイドライン(次頁)では、**サプライチェーン管理の重要性が強調されている他、**経済安保推進法では**サプライチェーン管理の審査が厳格化される見込み**(2章)である。

IPAが公表した2023年の国内セキュリティに関する10大脅威

順位	脅威の種類	順位	脅威の種類
1	ランサムウェアによる被害	6	修正プログラムの公開前を狙う攻撃
2	サプライチェーンを悪用した攻撃	7	メール詐欺による金銭被害
3	標的型攻撃による情報の窃取	8	脆弱性対策の公開に伴う悪用増加
4	内部不正による情報漏洩	9	不注意による情報漏えい
5	ニューノーマルな働き方を狙った攻撃	10	犯罪のビジネス化

参考：情報セキュリティ10大脅威 2023 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構を基に作成

近年の大規模サプライチェーン攻撃の事例

- 近年、サプライチェーンの脆弱性を狙った大規模な攻撃が国内でも発生している（以下）。サプライチェーン攻撃に対しては、自社のセキュリティ対策だけでなく、委託先や調達先等、サプライチェーン全体を考慮したセキュリティ対策が必要となる。

事例1）三菱電機の不正アクセスによる情報流出

2020年11月、中国にある子会社への不正アクセスをきっかけに、三菱電機本社が保存する取引先口座などの情報が外部に流出。三菱電機や子会社が利用するOffice 365のアカウント情報が第三者に窃取され、それらの情報をもとにOffice 365や関連サーバに対して攻撃が行われた。

事例2）マルウェア被害によるトヨタの工場停止

2022年3月、トヨタ自動車の主要サプライヤーの1社として自動車の内外装部品を生産する小島プレス工業がマルウェア￥（悪意のあるプログラム）の感染被害をに公表。この影響からトヨタは国内全工場（14工場28ライン）の稼働を停止し、サプライチェーン攻撃による点検や対策を行った。

事例3）大阪急性期・総合医療センターの医療サービス停止

2022年10月、ランサムウェアによる攻撃でシステム障害が起き、大阪急性期・総合医療センター（病床数800以上）のサービスが2ケ月停止。電子カルテが暗号化されただけでなく、病院システム全体に影響があった。給食を委託するサプライチェーン企業経由で病院システムに侵入されたのが原因。

参考：サプライチェーン攻撃事例　2022年から2023年の最新事例と対策を紹介 (isid.co.jp)、三菱電機、新たに1115件の情報漏えい明らかに　中国経由で不正アクセス - ITmedia NEWSなどを基に作成

４．サイバーセキュリティ戦略の立案には経営者のリーダーシップが重要

➢ 経済産業省が公表しているサイバーセキュリティ経営ガイドラインでは、深刻化するサイバー攻撃や社内の対策の実態を経営者が正確に把握するとともに、トップダウンでサイバーセキュリティ戦略の立案や対策の見直しを図る必要性が強調されている。

サイバーセキュリティ経営ガイドラインVer3.0

- 経済産業省は、経営者のリーダーシップの下で、**サイバーセキュリティ対策を推進・実践するためのプラクティス集やツールなどをまとめた「サイバーセキュリティ経営ガイドラインVer3.0(*1)」（以下、経営ガイドライン）を策定し公表**した。
- 本ガイドラインでは、**サイバー攻撃から企業を守る観点で経営者が認識・実践すべき「3原則」**や、経営者が情報セキュリティ対策を推進する上でCISO(*2)等に指示すべき「重要10項目」などが示されている(以下)。

３原則	経営者は、（中略）**組織のリスクマネジメントの責任を担う経営者が自らの役割として実施方針の検討、予算や人材の割当、実施状況の確認や問題の把握と対応等を通じてリーダーシップを発揮することが必要**である
重要10項目	CISO等は、経営者の指示に基づき、（中略）**セキュリティ対策の取組みを、セキュリティ担当者に対してより具体的に指示をし、推進することが必要**である。さらに、経営者に対して適宜状況報告を行うことを通じ**経営者が適切な判断を行うために必要な情報を提供**する。

企業経営者が認識・実践すべき3原則

- 経営ガイドラインで示される3原則では、特にセキュリティ対策において**経営者が果たす役割が重要視**されている。
- 後述するように、近年は**クラウドサービスやIoTなどの普及や導入により、サイバー攻撃の対象が増加しており、サプライチェーンのリスクが一層高まっている**。経営者には**サプライチェーンを取り巻く構造の大きな変化を認識するとともに、適切なセキュリティ対策を立案していく**ことが求められる。

1）経営者による強いリーダーシップ

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）サプライチェーン全体のセキュリティ強化

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等、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）関係者との積極的なコミュニケーション

平時及び緊急時のいずれにおいても、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

参考：経済産業省 サイバーセキュリティ経営ガイドライン Ver 3.0を基に作成
*1：2015年に「サイバーセキュリティ経営ガイドライン Ver1.0」が公開、その後2017年にVer2.0に改訂された。そして2023年3月に、約6年ぶりに3.0に改訂された
*2：CISO（Chief Information Security Officer：最高情報セキュリティ責任者）、企業における情報セキュリティを統括する責任者を指す

第４章

【参考】サイバーセキュリティ経営ガイドラインと関連資料の概要

➢ 経営ガイドラインの重要10項目では、サイバーセキュリティ対策を実施する上での責任者（CISO）や担当部署への指示を通じて組織に適した形で確実にセキュリティ施策を実行させる必要性が示されているほか、同ガイドラインの付録では、サイバーセキュリティ施策の実践における具体的な手段や事例が紹介されている

経営ガイドラインの重要10項目

- 経営者は、経営ガイドラインの重要10項目（以下）について、サイバーセキュリティ対策を実施する上での責任者（CISO）や担当部署（サイバーセキュリティ担当者等）への指示を通じて組織に適した形で確実に実施させる必要がある。

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
2	サイバーセキュリティリスク管理体制の構築
3	サイバーセキュリティ対策のための資源（予算、人材等）確保
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
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
6	関係者との積極的なコミュニケーション
7	経営者のリーダーシップ発揮
8	サプライチェーンセキュリティの強化
9	委託先等を含めたサプライチェーン全体の状況把握及び対策
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

付録（重要10項目の実施にあたって参考となる手引き）

- 経営ガイドラインでは、重要10項目の実施にあたって、参考となる情報を付録として提示している。付録の中でも、サイバーセキュリティ施策の実践における支援手段として挙げられている３つについて紹介する。

付録	内容
サイバーセキュリティ経営可視化ツール	経営ガイドラインで定める**重要10項目の実施状況を5段階の成熟モデルでレーダーチャート表示**できるツール（**ただし、Excel**）。セキュリティに関する現状の運営内容（方針策定の有無、CISOを含むサイバーセキュリティ体制の構築、等）について、定量的に自社の状況を把握することが可能。
付録F サイバーセキュリティ体制構築・人材確保の手引き	サイバーセキュリティ管理体制の構築や**サイバーセキュリティ対策のための資源確保について検討を行う際のポイントが記載**されている。具体的には、サイバーセキュリティに関して「やるべきこと」の明確化やセキュリティ統括機能の検討、「プラス・セキュリティ」の取り組みなどに関する内容が挙げられている。
サイバーセキュリティ経営ガイドライン Ver3.0実践のためのプラクティス集	経営者やCISO等、セキュリティ担当者を主な読者とし、経営ガイドラインの重要10項目を実践する際に参考となる考え方や実践事例等を記載。**事例の妨げとなる課題やセキュリティ担当者の悩みに対し、実際に試みられた工夫の事例を紹介している。各種付録の中でも最も有用な内容**となっている。

参考：経済産業省 サイバーセキュリティ経営ガイドライン Ver 3.0を基に作成。なお、関連法律として2015年に施行されたサイバーセキュリティ基本法があるが、同法はサイバーセキュリティ戦略をはじめとする施策の基本となる事項や基本理念を規定した法律であり、企業が具体策を検討するための参考にはなりにくい内容であるため、本稿では解説を割愛する。

第４章

５．事業成長への投資として認識すべきサイバーセキュリティ戦略

➢ サイバーセキュリティ戦略の立案は、企業活動におけるコストや損失を減らすために不可欠な投資であり、サイバーセキュリティのリスクを十分に把握した上で対策を実施していくことが、企業として果たすべき社会的責任となる。政府には、日本企業がサイバーセキュリティ戦略の立案に向けた投資や人材確保を十分に行うための環境づくりや法規制を整備していくことが期待される。

サイバーセキュリティ経営ガイドラインで強調される投資としてのサイバーセキュリティ対策(＊)

- サイバーセキュリティ経営ガイドラインで強調されるのは、**サイバーセキュリティ対策を企業にとって重要な投資（将来の事業活動や成長に必須な費用）として位置付ける重要性である**。同ガイドラインでは、サイバーセキュリティ対策が**企業の価値を維持あるいは増大し、企業活動におけるコストや損失を減らすために不可欠な投資であり、サイバーセキュリティのリスクを把握した上で対策を実施していくことが、企業として果たすべき社会的責任**である点が示されている。

日本企業のサイバーセキュリティ戦略立案を加速させるために

- 経営ガイドラインには、企業経営者がセキュリティ戦略を立案する上で認識すべき３原則や、セキュリティ施策の推進において念頭に置くべき重要10項目などが示されており、様々な企業にとって活用が期待できる内容である。一方で、次頁に示すように、日本企業の実態を見ると、**経営者のセキュリティ関連施策への関与や、日本企業がサイバーセキュリティ対策にかける予算の割合は米国等と比較しても依然として低い状態**である。
- これまで繰り返し述べたように、サイバー攻撃が急増する中、グローバルにおいてはサイバーセキュリティ戦略の立案がESG経営を担う柱の一つとして位置づけられており、このような動向は日本においても経営者を含めて強く認識する必要がある。ESGとデジタルに関する先進の動向を十分に把握し、まずは政府が、**経営ガイドラインで記されている3原則や重要10項目などの要素について、ESG経営との関連性を明確に示していくことが、経営者の関心やセキュリティ関連施策への関与を高める**ことに繋がるだろう。
- 併せて、日本企業が**サイバーセキュリティ戦略の立案に向けた投資や人材確保を十分に行えるように、サイバーセキュリティに関連する法規制の整備やガイドラインの定期的なアップデートによって、経営者のセキュリティ施策への関与を一層促す仕組みを作る**など、政府には日本企業の取り組みを積極的に後押ししていくことも期待される。

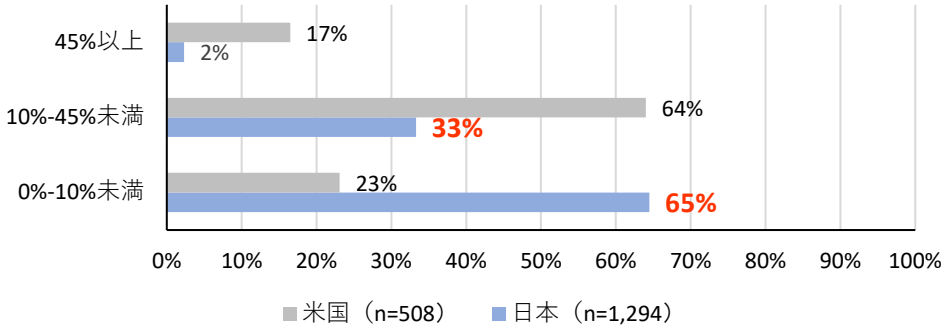
＊ 経済産業省 サイバーセキュリティ経営ガイドライン Ver 3.0を基に作成

【参考】日米のサイバーセキュリティ分野にかける予算比較

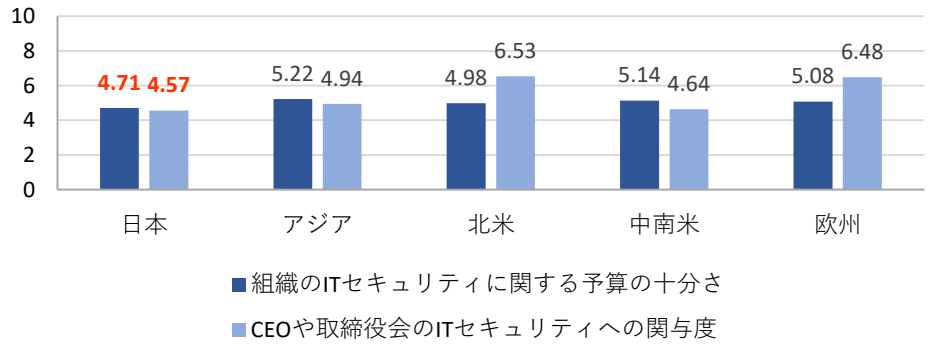
- 海外企業と比較して、**日本企業はサイバーセキュリティにかける予算や、経営層が戦略の立案や施策に関与する割合が低く、サプライチェーンへのセキュリティ対策や先進セキュリティ技術への投資などが十分に進んでいない**
- 背景として挙げられるのは、多くの日本企業にとって**セキュリティ対策が経営の主軸として認識されていない、ROIが測りにくく全社的にセキュリティ施策に対する予算が十分に確保しにくい**、などの理由である。

セキュリティ対策に投資する予算（グローバル比較）

１．IT予算に占めるセキュリティ関連予算の割合

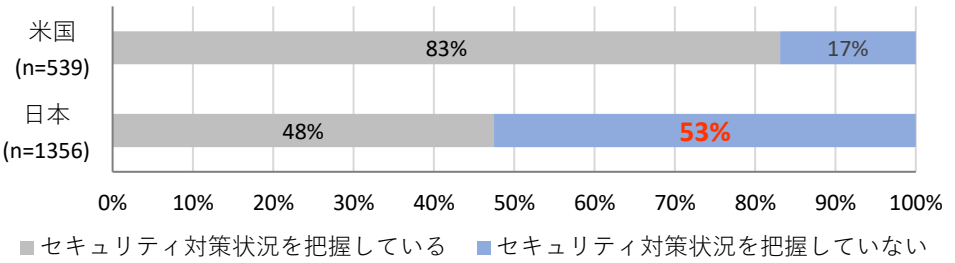


２．セキュリティに関する予算とセキュリティへの経営関与

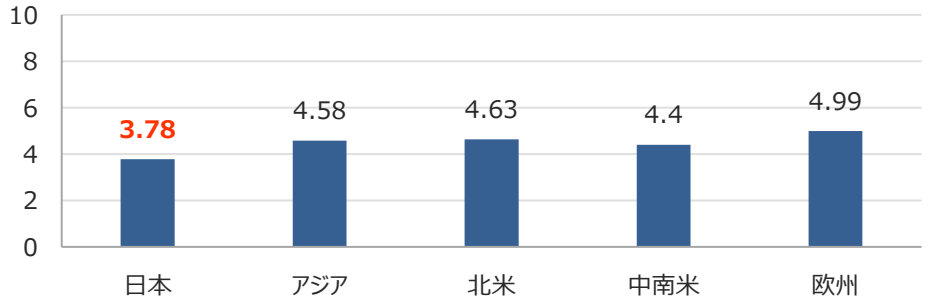


セキュリティ対策に関する予算、CEOの関与度他（グローバル比較）

３．サプライチェーンのセキュリティ管理（国内パートナー・委託先への統制状況）



４．先端のセキュリティ技術への投資



参考：「NRI Secure Insight 2022」、m471_サイバーセキュリティリスク_意識調査レポート（日本）.pdf (trendmicro.com)、日本と世界のトップ企業のCISO設置率とセキュリティ意識の差 | NordVPNを基に作成

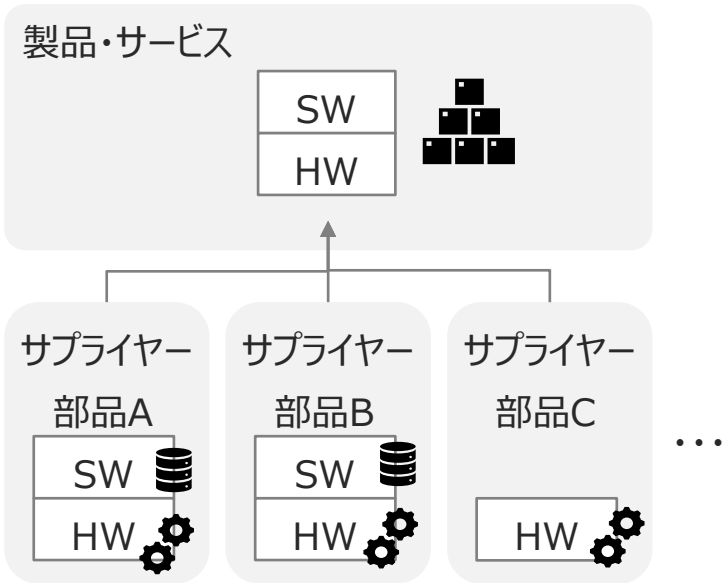
６．サイバー攻撃増加の背景にあるサプライチェーンの複雑化

以降のページでは、近年のサイバー攻撃増加における主要な要因の一つとされるサプライチェーンの複雑化とその対策について触れる

- 近年、需要変動のスピードの増加やサービスのグローバル展開、テクノロジーの進歩などに伴い、サプライチェーンがグローバル化
- ハードウェアやソフトウェア、クラウドサービス、IoT製品など様々なサプライヤーと連携するサプライチェーンによって管理が複雑化したほか、サイバー空間と物理空間の接点が急増し、サイバー攻撃の対象が増加するなど、サプライチェーンのリスクが一層高まっている。

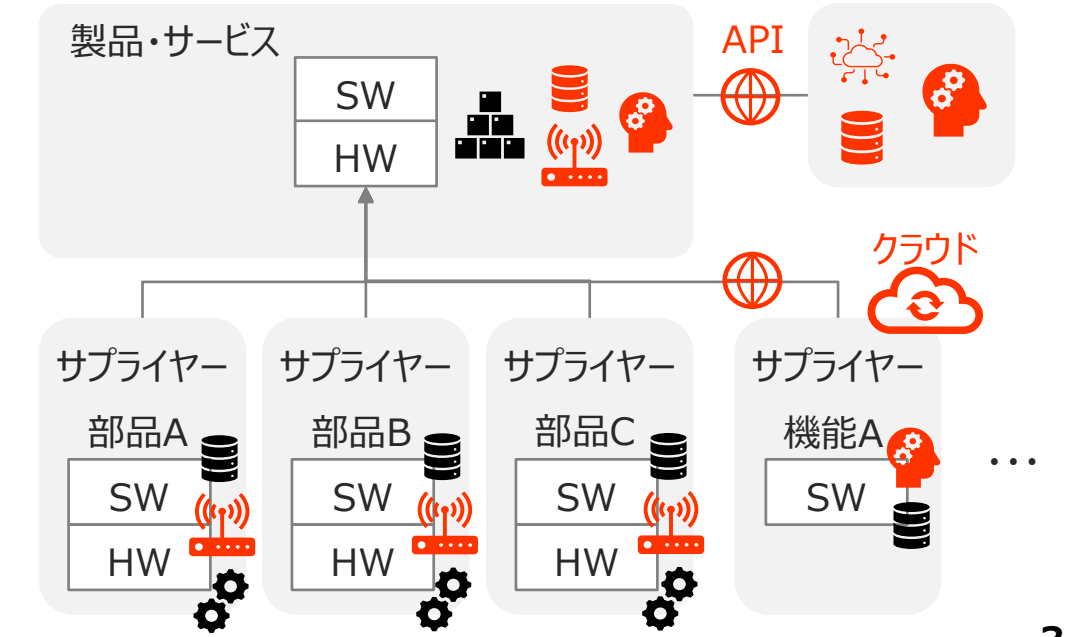
従来のサプライチェーン

- 主に物理製品や部品などのハードウェアが対象
- 環境、開発ラインごとに情報を管理
- サプライチェーン担当者、企業などにより管理が俗人的に行われる傾向あり
- オンプレミスなどのクローズドな環境で主に管理
- 需要に応じたリアルタイムな生産の増減等は困難



近年のサプライチェーン

- ハードウェアやソフトウェア、クラウドサービス、IoT製品など、**インターネットを介した様々なサプライヤーの活用による製品・サービスの開発**
- サプライチェーン全体の**情報共有・連携がリアルタイムで可能に**
- 一方で、製品を製造する**サプライチェーン全体の管理は複雑化**
- インターネットを利用したサードパーティとの接続や外部との情報共有の拡大などによって、**セキュリティリスクも大きく増加**

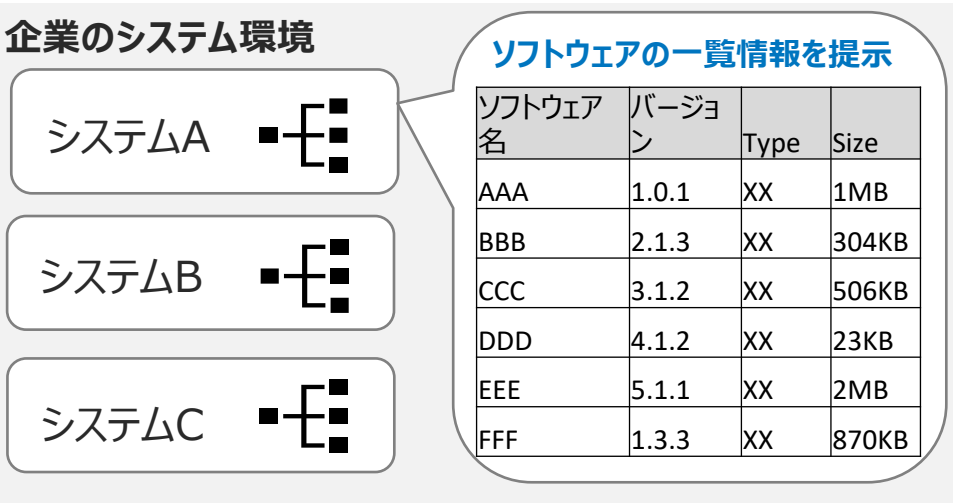


７．【再掲】複雑化するサプライチェーン管理に有効なSBOMとDSPM

- 複雑化するサプライチェーンの管理に関して、経営ガイドラインなどの活用が参考になるが、**社内のセキュリティ戦略の立案と併せて具体的にサイバーセキュリティ対策を行っていく上で有効になるのが先進のデジタルセキュリティソリューションの活用**である。
- 以降のページでは、近年特に注目されるサプライチェーンとデータセキュリティの領域(*)について代表的なソリューションを紹介する

SBOM（Software Bill of Materials）

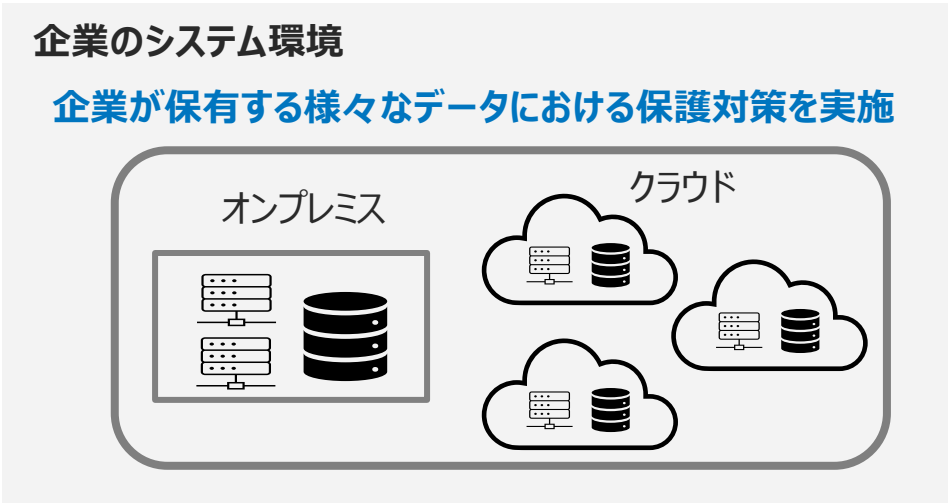
- ソフトウェアを構成するOSSや商用ソフトウェアなどのライブラリやモジュールの情報を構成情報として記したもの
- 製品に含むソフトウェアを構成するコンポーネントや互いの依存関係、ライセンスデータなどをリスト化した一覧表であり、ソフトウェアサプライチェーンのリスク管理等の用途で利用
- **ソフトウェアサプライチェーンにおける透明性とトレーサビリティの管理に有効な手段**として世界的に普及が進んでいる



ソフトウェア名	バージョン	Type	Size
AAA	1.0.1	XX	1MB
BBB	2.1.3	XX	304KB
CCC	3.1.2	XX	506KB
DDD	4.1.2	XX	23KB
EEE	5.1.1	XX	2MB
FFF	1.3.3	XX	870KB

DSPM（Data Security Posture Management）

- オンプレミスやクラウドに存在する社内データや顧客データなどの機密情報をモニタリングし、そのデータが適切なセキュリティ対策や保護を受けているかどうかチェックする仕組み
- 組織が保有するデータの可視化や分類、データにアクセスできる権限の可視化やデータの取り扱いに関するユーザのアクティビティの監視など、**サードパーティを含めたサプライチェーン全体のデータ管理を行う**



*サイバーセキュリティ対策には、サーバやサービスを利用する際のログイン認証の高度化やネットワークや各種デバイスのセキュリティ対策、セキュリティリテラシーを向上させるための従業員教育等、多岐に渡る施策が挙げられるが、本稿では近年特に注目されるサプライチェーンとデータセキュリティの領域にフォーカスしてソリューションを紹介する

８．デジタルソリューション事例（SBOM・サプライチェーン管理）

Anchore

- https://anchore.com/sbom/
- 本社カリフォルニア州、2016年設立
- オンプレミスやクラウド、コンテナなど様々な環境におけるソフトウェアの資産に関する統合的なSBOMを自動的に作成する。同社のSBOMでは、各ソフトウェア間の依存関係やリスクのチェック、継続的な脆弱性の監視等を行うことが可能。
- 新しい脆弱性が確認された場合もSBOM内を検索して、影響を受けるソフトウェアやアプリケーションを特定し、脆弱性に対する修正などを行うことが可能。

【Anchoreのホームページより】

OS | Files | NPM | Gems | Python | Java | NuGet | Binary | Golang | Malware

Package Name	Version	Type	Size
.otp-run-deps	20210803.033168	APKG	NaN
alpine-baselayout	3.2.0r15	APKG	404
alpine-keys	2.3r-1	APKG	116
apk-tools	2.12.5-r1	APKG	304
bash	5.1.4-r0	APKG	1 M
busybox	1.33.1-r2	APKG	928
car-certificate-bundle	20191127-r5	APKG	228

Scribe Security

- https://scribesecurity.com/
- 本社イスラエル、2021年設立
- 企業が保有するソフトウェア資産、ソフトウェア同士の依存関係、脆弱性のリスクなどを全て可視化して提示
- ソフトウェア開発のライフサイクルに合わせて、開発のプロセス毎に自動的にソフトウェアの安全性やリスクを検証することが可能
- Cyber Security Excellence Awards 2023、Global Infosec awardsなど多数の賞を受賞

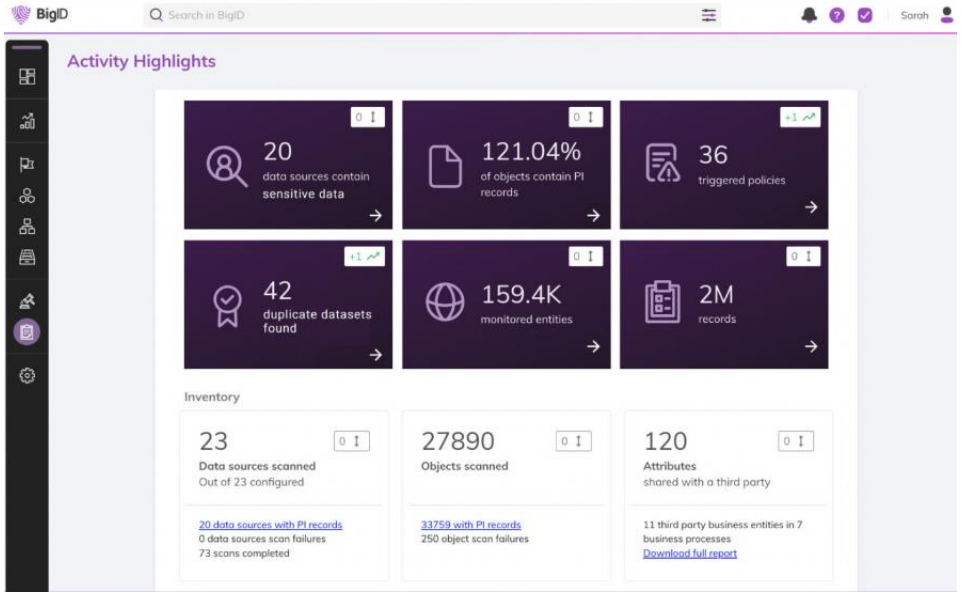
【Scribe Securityのホームページより】

９．デジタルソリューション事例（DSPM・データセキュリティ）

BigID

- https://bigid.com/
- 本社ニューヨーク、2016年設立
- オンプレミスやクラウド環境を含む企業のシステム環境全体におけるデータの可視化、管理、保護ソリューションを提供
- 同製品では、データが存在する場所を特定して分類するほか、リスクの高いデータを特定し、セキュリティやコンプライアンス、プライバシー、ガバナンス等の様々な対策を行うことが可能。
- DSPMのリーダー企業として注目される

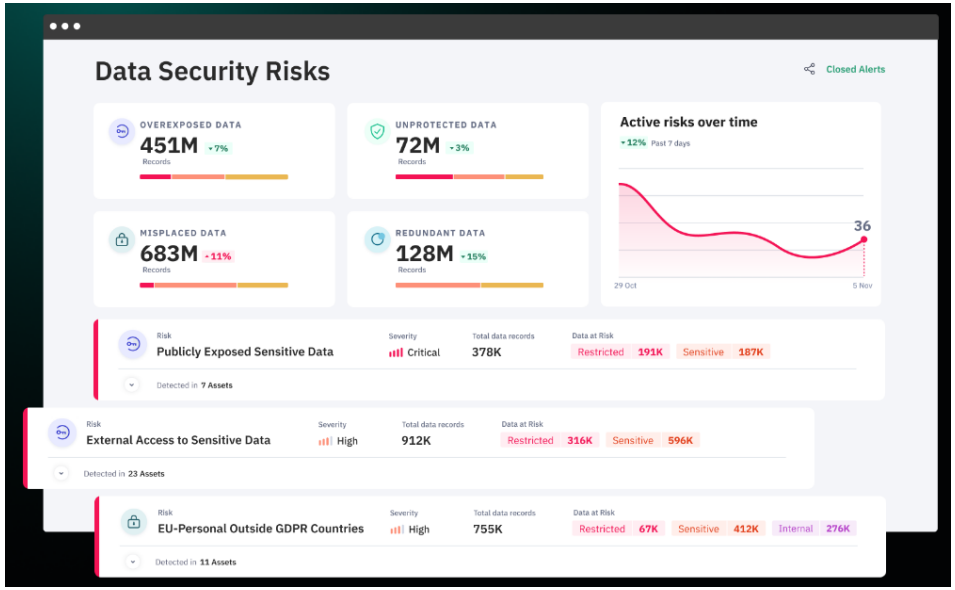
【BigIDのホームページより】



Laminar（Rubrik）

- https://laminarsecurity.com/
- 本社イスラエル、2020年設立。(*データセキュリティ企業大手のRubrikが2023年8月買収Laminarの買収を発表)
- データの機密性や企業のセキュリティ体制、利用状況などに基づいて、リスクベースでデータ保護対策を提示
- 企業が扱うデータの中でリスクが高い機密データを迅速に特定して保護対策を行うほか、データの管理状況をまとめた監査対応のコンプライアンス・レポートを作成することなどが可能。

【Laminarのホームページより】



第４章

１０．まとめ

- 様々な産業におけるサイバー攻撃が急増する一方、日本企業がサイバーセキュリティにかける予算は大幅に増加しておらず、多様化するサイバー攻撃への十分な対策が取られていない。背景として挙げられるのは、欧米企業と比較すると、日本企業の経営者がセキュリティ施策に関与する割合が低く、全社的に投資をする体制が十分に整備されていない点である。
- 経営者には、深刻化するサイバー攻撃や社内の対策の実態を正確に把握するとともに、サイバーセキュリティ経営ガイドラインなどを参考に、トップダウンで戦略の立案や対策の見直しを図ることが求められる。また、政府が果たす役割として、サイバーセキュリティ戦略とESG経営との関連性を明確に示し、経営者のセキュリティ施策への関与を強く促す仕組みを整備してくことが期待される。
- 近年、クラウドサービスやIoTの普及により、サイバー空間と物理空間の接点が急増し、ハードウェアやソフトウェアを含む全てのプロダクトが連携するシステム構成が一般的になる一方、サプライチェーンの脆弱性を突いたサイバー攻撃のリスクが一層高まっており、サイバーセキュリティ対策が複雑化している。多くの企業にとって、サプライチェーン環境の管理体制の強化や、サプライチェーン全体を対象にしたソフトウェアの脆弱性対策、データの保護対策などが急務となっている。
- 本章で紹介したSBOMやDSPMに関連するデジタルソリューションは、ソフトウェアの脆弱性対策やデータの保護対策を統合的かつ正確に行うという点において、日本企業にとっても有効活用が期待できる。特に米国等の法規制の状況を鑑みると、日本国内においても経済安保推進法の一連の施策の中で、サプライチェーンの管理体制について情報提示をすることが予想されるため、今の段階から、サードパーティも含めたサプライチェーン環境の整備や管理体制の強化に努めることが肝要であろう。

総括

1章から4章までのまとめ

➢グローバルにデジタル化の動きが加速するなか、企業にはDXの推進と併せてガバナンス関連施策の推進強化を図る必要性が指摘されている。特にサイバーセキュリティ戦略は、ESG経営の根幹をなす要素として大きく注目されており、企業はサイバー危機管理のプラクティスを立案し、セキュリティポリシーや対策に関する具体的な情報を投資家や顧客などのステークホルダーに提示することが求められている。

➢近年、ソフトウェアの脆弱性を突いた大規模なサイバー攻撃が急増しており、欧米ではサイバーセキュリティに関する様々な法律やガイドラインが施行され、企業におけるサイバーセキュリティの対策強化が義務付けられている。欧米のCISOにとってサイバーセキュリティへの投資は最優先事項であり、経営層のトップダウンによるセキュリティ戦略の立案が企業の評価や信頼を左右する要素となっている。サイバーセキュリティ対策はDXの推進と共に事業継続において不可欠な施策の一つとして位置づけられている。

➢日本国内でもサイバー攻撃は急増しているものの、日本企業がサイバーセキュリティにかける予算は大幅に増加しておらず、多様化するサイバー攻撃への十分な対策が講じられていない。ただし、経済安保推進法の関連施策によって、今後、産業横断的に対象の組織にセキュリティ施策の整備や強化が求められ、対策が不十分な企業にはサプライチェーンの見直しなど厳格な措置が取られることも予想される。

➢経営者には、グローバルに深刻化するサイバー攻撃の状況や、自社・サードパーティを含めたセキュリティ対策の実態を正確に把握するとともに、国内で公表されているセキュリティ経営ガイドラインなどを参考に、トップダウンでサイバーセキュリティ戦略の立案や対策の見直しを図ることが求められる。

筆者からの提言

➢近年、ESG経営においてシステムリスクマネジメントやサイバーセキュリティ対策など、ESGにおけるガバナンス施策が企業や投資家等から広く関心を集めている。デジタル化やDXを推進する日本企業にとっても、システムの安定的な運用やシステムレジリエンスなど、ビジネスを支える根幹のインフラとしてITが果たす役割を十分に理解し、サステナビリティ経営に対する本質的な理解を深めることが必要になるだろう。

➢サイバーセキュリティ対策において経営層が果たすべき役割は大きい。海外の先進グローバル企業では、CISOの設置などによって、経営層がサイバーセキュリティ戦略の立案に積極的に携わっているが、日本企業においても先進の事例を参考にして、経営層がセキュリティ戦略を主体的に立案する体制を構築・整備していくことが求められる。

➢様々な業界でDXが推進されるなか、サプライチェーンのデジタル化も急速に進んでいる。物理的なプロダクトで構成される従来のサプライチェーンとは大きく異なり、ソフトウェアやデータを活用するサプライチェーンはサービスの変更などに伴い、サプライチェーンを構成するプロダクトやサプライヤーも頻繁に変更される可能性があり、管理がより煩雑化することも予想される。本稿で紹介したSBOMやDSPMに関連する先進のデジタルソリューションは、企業が対策の自動化や運用の効率化を検討する上で参考になるだろう。

➢政府には、継続的なシステム運用やサイバーセキュリティ対策の重要性など、ESG経営の根幹として、企業がサイバーセキュリティ施策を十分に認識できるような要素をESGガイドラインなどで具体的に示していくことが求められる。経営層がサイバーセキュリティ戦略の立案を行う体制づくりを定着させることが政府が果たすべき重要な役割であり、それが日本企業のDXやESG経営の一層の発展に繋がるであろう。