

フロンティアAI時代のサイバー安全保障 日本企業に求められる経営的対応



藤井秀之

CONTENTS

- I フロンティアAIがもたらしたサイバー安全保障の質的变化
- II 「フロンティアAI×サイバー安全保障」の脅威構造
- III 日本の制度対応：サイバー法制とフロンティアAIへの即応
- IV 国際整合性：サイバー安保法制とAI規制
- V 「規制対応」から「安全保障投資」へ：両面性のある経営転換
- VI 経営者が今、着手すべき行動指針

要 約

- 1 フロンティアAIの登場により、サイバー安全保障を取り巻く状況は質的に変化した。攻撃側では、能力の段階的飛躍、攻撃の裾野の拡大、時間軸の圧縮、採算性のシフトという4つの構造変化が同時に進行し、対策の枠組み自体の見直しを企業に迫っている。
- 2 これらの変化は、国家関与型攻撃、サプライチェーン経由侵害、機微情報窃取という従来の脅威を増幅する。攻撃の担い手は専門知識を持たない層にまで広がり、標的も基幹インフラ・大手企業から中堅・中小企業へと拡大した。
- 3 こうした脅威に対し、日本では経済安全保障推進法、重要経済安保情報保護活用法、サイバー対処能力強化法の三法が整備され、政府対策パッケージ「Project YATA-Shield」が取りまとめられた。欧米でも規制・国際枠組みが整備されており、いずれも経営層の説明責任が直接問われる方向で規制強化が進んでいる。
- 4 フロンティアAI時代において経営者が着手すべきなのは、「規制対応」から「安全保障投資」への姿勢転換を前提に、①経営ガバナンスの確立、②機微情報・クリアランス体制の整備、③防御態勢の整備と高度化という3つの柱を、経営直轄で同時並行的に推進することである。

I フロンティアAIがもたらした サイバー安全保障の質的变化

1 Mythosが示した攻撃側の 構造変化

近年、日本企業を狙ったサイバー攻撃の様相は大きく変わった。かつてサイバーセキュリティは、機密情報の漏洩や業務妨害といった「事業リスク」の文脈で語られた。しかし現在、その実態は国家間競争の主戦場へと変容しつつある。2024年から2025年にかけては、宇宙関連研究機関や大手通信事業者、複数の金融機関に対する大規模な侵害事例が次々と公表されたが、いずれも国家関与が指摘される高度な攻撃と見られている。サイバー空間は、もはや有事に限定された「第5の戦場」ではなく、平時から継続する主要な戦場となっている。

この変化を決定的に推し進めたのが、フロンティアAIの登場である。フロンティアAIとは、業界最先端の大規模AIモデルを指す呼称である。2026年4月、米国のAI開発企業アンソロピックは、自社の最先端モデル「Claude Mythos」と、その限定パートナー向け配布プログラム「Project Glasswing」を発表した。

同社は発表に際し、Mythosが発表前数週間のうちに数千件のゼロデイ脆弱性を自律的に発見し、その99%以上が公表時点で未修正であった事実を公表した^{文献1}。中には1998年実装の「OpenBSD」の整数オーバーフロー脆弱性のように、28年間見逃されてきたものまで含まれる。また、先代モデル（Opus 4.6）との差としては、Firefoxで見つかった同じ弱点を「実際に突いて侵入する攻撃」に

仕立てられた成功割合はわずか0.8%（約250回中2回）だったが、Mythosはこれを約72%と約90倍引き上げた。

同種的能力獲得はOpenAI社の「GPT-5.5」や中国系研究機関による類似モデルにも観測されており、Mythos固有の現象ではない。英国AIセキュリティ・インスティテュート（AISI）が2026年5月に公表した評価では、GPT-5.5はMythos Previewを上回るスコアを記録した^{文献2}。AISIはまた、フロンティアAIのサイバー能力が約4.7カ月で進歩速度が倍増するトレンドにあると指摘している^{文献3}。フロンティアAI業界全体の進化トレンドとして広がっており、サイバー安全保障はこうしたフロンティアAI時代において新たな段階に入りつつある（表1）。

2 本稿の問いと 本特集における位置づけ

日本では、2022年から2025年にかけて、サイバー安全保障に関する法制整備が急速に進み、経済安全保障推進法（令和4年法律第43号）、重要経済安保情報保護活用法（令和6年法律第27号）、サイバー対処能力強化法（令和7年法律第42号、いわゆる能動的サイバー防御法）の三法が整備された。これらは企業に対し、これまでにない水準の対応を求めるものである。

本稿の問題意識は、フロンティアAI時代の到来を踏まえ、こうした制度整備が進む中で、日本企業はいかにして国家安全保障の「当事者」としての役割を果たすべきかという点にある。法制対応は経営課題の最低ラインにすぎない。求められるのは、規制対応の枠を超え、サイバーセキュリティを「コス

表1 フロンティアAIが変えたサイバー脅威の構造

	BEFORE フロンティアAI以前	フロンティアAIの登場	AFTER フロンティアAI以後
①攻撃能力	既知の脆弱性（CVE）や既存マルウェアを活用した攻撃		- 未知の脆弱性をAIが自律的に発見（ゼロデイ） - 特定標的に合わせたカスタム攻撃コードをゼロから生成
②攻撃者層	- 国家関与型攻撃グループ - 組織犯罪グループ （高度な専門知識・組織・資金が前提）		- 国家関与型攻撃グループ 継続 - 組織犯罪グループ 継続 ＋一般のエンジニア層 （フロンティアAIにより専門知識不要）
③攻撃速度	脆弱性公表から悪用まで 週～月単位		脆弱性公表から悪用まで 36時間以内 （AIによる高速解析・自動化が背景）
④標的範囲	- 防衛産業・基幹インフラ（電力・通信・金融など）・大手企業 * 散発的には中堅・中小企業なども対象に		- 防衛産業・基幹インフラ・大手企業 継続 - 中堅・中小企業 - サプライチェーン上の取引先・委託先 - 共同研究先・海外子会社 →日常的な攻撃対象へ

ト」ではなく「安全保障投資」として位置づける経営姿勢の根本的な転換である。

本稿では、経営層の視点から、フロンティアAI時代におけるサイバー安全保障の制度動向を考察したうえで、経営転換の考え方と進め方について論じる。なお、本特集の他論考において、ランサムウェア対応、サプライチェーンセキュリティ、2030年に向けたセキュリティの全体展望についてそれぞれ詳述しているため、本稿ではこれらの個別論点に深く立ち入らず、フロンティアAI時代における経営層の判断枠組みを示すことに焦点を絞る。

以下、第Ⅱ章では、フロンティアAIによる脅威構造の変化を整理し、第Ⅲ章では、日

本の制度対応（サイバー安全保障法制群とProject YATA-Shield）を整理する。第Ⅳ章でサイバー安保法制とAI規制の国際的な動向を、第Ⅴ章で「規制対応」から「安全保障投資」への経営転換の中身を提示する。第Ⅵ章で経営者が今、着手すべき行動指針をまとめる。

Ⅱ「フロンティアAI×サイバー安全保障」の脅威構造

1 フロンティアAIによる攻撃側の4つの構造変化

フロンティアAIの登場が攻撃側に与えた影響は、4つの構造変化として整理できる。

これらは個別の現象ではなく、同時かつ相互に作用しており、サイバー安全保障の対策枠組み自体の再設計を企業に迫っている。

第1の構造変化は、攻撃能力の段階的飛躍である。先代モデル比で量的にも質的にも段違いの能力向上が観測されている。FreeBSDにおける17年物のバグやOpenBSDにおける28年物のバグといった、長年見逃されてきた脆弱性をフロンティアAIが自律的に発見した事例は、人手による発見プロセスの限界を超えたことを意味する。

第2の構造変化は、攻撃の裾野の拡大である。従来、サイバー攻撃の高度化は、国家関与型攻撃グループや一部の高度な犯罪組織に限られていた。フロンティアAIは、専門的なセキュリティ訓練を受けていないエンジニアであっても、一晩で動作する攻撃コードを得る環境を実現しつつある。アンソロピック自身は、この点を発表時に明示的に警告している。

第3の構造変化は、時間軸の圧縮である。脆弱性の公表から実際の悪用までの時間（time-to-exploit）は、業界共通の認識としてすでに1日未満のオーダーに圧縮された。修正パッチの差分解析により、パッチ公開そのものが攻撃の設計図にもなり得る。米CISA（サイバーセキュリティ・インフラセキュリティ庁）も2026年6月、悪用が確認された脆弱性への一律の修正期限を、最高リスクは3日以内とするリスクベースの優先順位づけ（BOD 26-04）へと改めており、規制の枠組み自体がこの圧縮を織り込み始めている。

第4の構造変化は、攻撃採算性のシフトである。攻撃ツールを準備するコストの低下により、これまで採算が合わなかった規模の事

業者まで攻撃対象が広がり、中堅・中小企業まで標的とされるようになっていく。攻撃側のコストが低下する一方、防御側は監視対象の拡大と対応速度の引き上げによってコストが増大し、攻守のコスト非対称性が拡大している。

こうした攻守のコスト非対称性は、防御側のリスクを引き受けるサイバー保険の領域にも及んでいる。米国大手サイバー保険会社コアリション^{文献4}は、企業のリスク状態が短期間で大きく変動するため、年次のスナップショット評価では実態を捉えられず、継続的な脅威情報に基づく動的な引受モデルへの移行が必要と分析している。このため経営層は、サイバー保険の引受条件が厳格化することも前提に置く必要がある。

もっとも、フロンティアAIが攻撃の技術的なハードルを下げて、収益化（換金）や帰属（特定・報復を受けるリスク）といった制約は残り、脅威が際限なく拡大するわけではない。フロンティアAIの能力評価についても独立した検証の必要性が指摘されている。米国の脆弱性情報企業バルンチェック^{文献5}の分析（2026年4月時点）によれば、アンソロピックに帰属するCVE（Common Vulnerabilities and Exposures：共通脆弱性識別子）公表件数は実測で約40件、うちProject Glasswingからの明示帰属は1件にとどまっている。

一方、MozillaのCTO^{文献6}はMythosをFirefoxに適用した検証結果について、発見されたバグはいずれも熟練した研究者が発見可能な範囲にとどまる旨を公表しており、人間の能力を質的に超越する万能ツールではないとの慎重な見方を示している。

しかしいずれにせよ、上記のような4つの構造変化が同時に進行している事実認識は、業界として共有されている。経営判断として重要なのは、過大評価や過小評価をすることなく自社のリスクを可視化し、ステークホルダーと連携して対策の枠組みを再設計することである。

2 サイバー攻撃の3つの潮流

こうしたフロンティアAIの能力拡張により、想定されていた攻撃構造は大きく変わることになる。そうした状況下での日本企業を取り巻く脅威は、主に以下の3つの潮流として整理される。

第1の潮流は、国家が関与する攻撃グループによる組織的かつ持続的な活動の常態化である。日本企業を取り巻くサイバー脅威の中でも、この潮流は最も深刻な課題である。国家の関与が指摘される攻撃グループが、欧米の重要インフラに「Living off the Land 攻撃」（攻撃者が標的のシステムにあらかじめ備わっている正規のツールや機能を用いて攻撃活動を行う手法）で長期間侵入していた事例が、各国の当局により報告されている。標的は電力、通信、水道、運輸など、平時には目立たないが有事の際には致命的な意味を持つ基幹インフラである。日本の防衛産業、通信、エネルギー分野も同様の脅威にさらされている。

国家関与グループの狙いは重要インフラへの潜伏にとどまらない。暗号資産事業者や金融機関を標的に、外貨獲得を目的とした攻撃を継続的に実行している。情報技術従事者になりすまして海外企業に就労し、内部から情報窃取と資金詐取を行う手口も確認されてい

る。サイバー犯罪はもはや個人の犯行ではなく、国家事業として制度化されているといえよう。

この潮流は世界共通だが、日本は国家関与型攻撃の主要な担い手とされる国々と地理的に近接し、主要同盟国の一員として地域戦略上も標的となりやすい位置にある。とりわけ外貨獲得を目的とする一部の国家関与型攻撃は、暗号資産事業者が集積する日本を繰り返し標的としてきた。能動的サイバー防御の体制整備が主要同盟国に比べて遅れ、法制化も2025年となったことも攻撃者に対して「防御の空白（防御体制の隙間）」を相対的に残す結果となった。

第2の潮流は、サプライチェーン経由の間接侵害が常態化している点である。攻撃者は堅牢に守られた大企業の正面を直接突破するのではなく、相対的に防御の薄い取引先・委託先・子会社を突破口として本体へ横展開する手法を選ぶ。

複数の大手調査機関の集計によれば、2024年に発生した重大サイバー事案の約30%が第三者起因であり、その比率は前年の約15%から倍増した。このことは「自社さえ守ればよい」時代の終焉を意味しており、経営層は、自社の境界内のセキュリティ水準だけでなく、サプライチェーン全体での水準確保を経営課題として受け止める必要がある。

サプライチェーン経由侵害は世界的傾向だが、日本では多重下請けと系列を特徴とする産業構造により、被害が拡大する危険性が指摘されている。特に製造業では最終製品メーカーの下に多数の中小サプライヤーが連なり、その多くはセキュリティ投資余力に乏しい。たった1社の一次サプライヤーでのラン

サムウェア被害が、大手自動車メーカーの国内全工場の操業停止を招いた事例は、堅牢な本体であっても最も弱い結節点で攻撃を受ければ、いとも簡単に事業全体が止まるという厳しい現実を露呈させた。

第3の潮流は、半導体、量子、人工知能、宇宙、バイオ、先端材料などの分野で、機微技術情報の窃取が国家間競争の主要手段となっている点である。これらの分野で世界有数のコア技術や営業秘密を有する日本企業は、当然ながら攻撃者の標的となりやすい。

従来、日本企業の知的財産は不正競争防止法上の営業秘密として保護されてきた。しかし、サプライチェーン経由でアクセスされる情報、共同研究先や合弁会社で共有される情報、海外子会社で生成される情報など、自社の管理境界の外側での流出リスクが構造的に高まっている。経済安全保障の文脈では、こうした「機微情報」の保全が、個人情報や営業秘密の枠組みを超えた経営課題として位置づけられている。

機微技術の窃取が国家間競争の手段となる構図も世界共通だが、とりわけ素材、半導体製造装置、精密機械、ロボティクスといった分野で、競争関係を一転させ得る世界有数の技術を持つ日本は、その性格上、極めて魅力的な標的となる。産学連携や国際的な共同研究が拡大することにより、大学・研究機関を経由して流出するような経路も広がっている。日本では後述するセキュリティ・クリアランス制度の整備が諸外国と比較して遅れているため、保全水準が制度的に低い状態が長く続き、攻撃者にとって侵入しやすい環境を残してきた。

第Ⅱ章1節で述べた4つの構造変化は、攻

撃する側とされる側の双方の関係者の範囲を広げる。従来、攻撃の担い手は国家関与型・組織犯罪型に、標的は防衛産業・基幹インフラ・大手金融機関に限られていた。今や攻撃の専門性要件が大幅に低下していることから、その担い手はフロンティアAIを活用する一般のエンジニア層にまで広がっている。標的も中堅・中小企業、海外子会社、共同研究先、サプライチェーン上の小規模事業者へと拡大した。経営層には、自社単独の防御水準確保では完結せず、グループ全体・取引先・子会社・共同研究先を含む広い範囲での水準確保が求められる。

Ⅲ 日本の制度対応： サイバー法制とフロンティア AIへの即応

1 サイバー安全保障法制の 全体像と企業実務

2022年から2025年にかけて整備された日本のサイバー安全保障法制は、経済安全保障推進法、重要経済安保情報保護活用法、サイバー対処能力強化法に、従来の個人情報保護法、サイバーセキュリティ基本法を加えた複数の法律が重なり合う形で構成された法制として理解できる。

各法はそれぞれ異なる切り口で企業を規制する。すなわち、重要インフラの保護（経済安全保障推進法、サイバー対処能力強化法）、機微情報の保全（重要経済安保情報保護活用法）、個人データの保護（個人情報保護法）、サイバーセキュリティ全体の統治（サイバーセキュリティ基本法）である。

本章では、このうちサイバー安全保障の観

表2 日本のサイバー安全保障法制の概要

法律名	成立・施行	所管	主な規律対象	企業への主要義務	サイバー安全保障上の意義
経済安全保障推進法 令和4年法律第43号	2022年 成立・施行	内閣府	特定社会基盤事業者 先端技術育成協議会参加企業 電力・通信・金融など15分野の重要インフラ事業者、ならびに先端技術の官民協議会に参加する企業	・【基幹インフラ制度】 特定重要設備の導入・維持管理委託に際し、主務大臣への事前届出・審査が義務 ・【先端技術育成】 AI・量子・半導体など20分野を対象とした経済安全保障重要技術育成プログラムの協議会参加者に研究開発情報の守秘義務	・重要インフラの供給網（サプライチェーン）保護と、先端技術の官民共同育成基盤を整備。サイバー安全保障の前提となる経済基盤を法的に支える
重要経済安保情報保護活用法 通称：セキュリティ・クリアランス制度 令和6年法律第27号	2024年 成立／2025年 5月 全面施行	内閣府	適合事業者 適性評価対象者（個人） クリアランスを取得する企業（適合事業者）、および当該情報を取り扱う従業員個人	・情報管理体制の整備 ・従業員に対する適性評価の実施 ・目的外利用の禁止 クリアランス非保有を理由とした降格・解雇などの不利益取り扱い違法	・機微情報へのアクセス資格を制度化（米国Confidential級相当）。日本企業が国際的な機密情報共有に参画するための資格基盤を確立する
サイバー対処能力強化法 令和7年法律第42号	2025年 成立	内閣官房	特別社会基盤事業者 通信事業者 など 重要インフラ事業者および通信事業者など、能動的防御に協力する民間主体	・特別社会基盤事業者：特定重要電子計算機の導入時届出・重大インシデントの政府報告義務 ・電気通信事業者：攻撃関連通信情報の提供 監視委員会の事前承認を要件、原則6カ月以内 ・ITベンダー（海外事業者含む）：脆弱性措置申請への対応 ・協議会参加：政府保有の秘密性の高い脅威情報へのアクセスが可能	・攻撃者サーバへのアクセス・無害化措置を日本で初めて法的に整備（警察官職務執行法・自衛隊法改正により権限付与） ・攻撃関連通信情報の収集・分析を制度化（外外通信などに限定・監視委員会の事前承認制）し、平時からの早期脅威検知基盤を整備 ・供給者への脆弱性措置要請（42条）に域外適用規定を設け、国外のソフトウェア・AI供給者も規律の射程内に

出所）各法令・内閣府資料を基に作成

点で特に事業者側の対応強化が求められる経済安全保障推進法、重要経済安保情報保護活用法、サイバー対処能力強化法に関して、企業が押さえておくべきポイントについて概観する（表2）。そのうえで、フロンティアAIに対する政府の取り組み状況についても取り

上げる。

2 経済安全保障推進法

経済安全保障推進法は、①重要物資の安定供給確保、②基幹インフラ役務の安定的提供確保、③先端的な重要技術の開発支援、④特

許出願の非公開の4本柱で構成される。サイバー安全保障の観点で特に重要なのは、②および③である。

②の基幹インフラ制度では、電気、ガス、通信、金融など15分野の主要事業者が「特定社会基盤事業者」として指定され、特定重要設備の導入や重要維持管理などの委託に際し、主務大臣への事前届出と審査が義務づけられる。違反には罰則も用意されている。金融分野では2024年5月から運用が開始済みで、調達計画の見直しと期間の長期化が経営課題となっている。

③の先端技術育成では、人工知能、量子、半導体、宇宙、サイバーセキュリティ技術など20分野が指定され、約5000億円規模の「経済安全保障重要技術育成プログラム」による官民連携の研究開発が推進されている。協議会参加者には守秘義務が課され、違反時には刑事罰の対象となる。

なお、経済安全保障の経営向けガイドラインとして、2026年1月に経済産業省貿易経済安全保障局が「経済安全保障経営ガイドライン（第1版）」^{文献7}を策定している。本ガイドラインは法的義務づけではなく、一般的推奨事項であるが、経営者が認識すべき3原則として、①自社ビジネスを正確に把握し、リスクシナリオを策定する、②経済安保への対応を単なるコストではなく、投資と捉える、③マルチステークホルダーとの対話を欠かさない、を提示している点が重要である。

3 重要経済安保情報保護活用法 (セキュリティ・クリアランス制度)

重要経済安保情報保護活用法は、経済安全保障分野のセキュリティ・クリアランス制度

を創設する法律である。2024年5月に成立し、2025年5月16日に全面施行された^{文献8}。

従来の特定秘密保護法が「著しい支障」の機微情報（米国Top Secret／Secret級相当）を対象にしているのに対し、本法はその下位の「支障」の機微情報（米国Confidential級相当）を新たに保護対象としている。日本企業が、海外の合弁、共同研究、政府入札などで「クリアランス非保有を理由に参画できない」事例が多発していたことが、本法を整備する直接の契機となった。

制度は人と組織の両面で運用される。「適合事業者」の認定では、外国の所有・支配・影響の不存在、保護責任者・業務管理者の設置、施設設備の機能などが要件となる。対象者本人の同意の下で犯罪歴・信用状態などを調査する「適性評価」が課され、有効期間は最大10年に及ぶ。

民間企業の人事・労務上の留意点は多岐にわたる。新規採用時の雇用契約条項、外国籍従業員の取り扱い、適性評価不合格者の処遇、派遣労働者を含めた管理体制などが論点となる。たとえば「目的外利用禁止」（同法16条）に関しては、クリアランス非保有を理由として降格や解雇を行うことは違法となる恐れがあることから、あらかじめ社内規程を整備しておくことが不可欠である。

4 サイバー対処能力強化法 (能動的サイバー防御法)

サイバー対処能力強化法は、2025年5月に成立した日本のサイバー安全保障の新たな中核法制である。①官民連携の強化、②通信情報の利用、③脆弱性対応、④サイバー通信情報監理委員会の設置の4つの柱で構成され、

同時に整備された関連整備法では、警察や自衛隊などの国家機関に能動的サイバー防御の権限が付与された。

本法の施行は段階的に進む。サイバー通信情報監理委員会は2026年4月1日に発足済みであり、同年10月1日には官民連携（協議会）・脆弱性対応の中核規定、および関連整備法に基づくアクセス・無害化措置が施行されることが決まっている。通信情報の利用規定の全面施行は2027年11月までと見込まれている。

民間企業に対する直接の影響は、「特別社会基盤事業者」（経済安保推進法の特定社会基盤事業者を承継する概念）に集中する。具体的には、特定重要電子計算機の導入時の届出義務（同法4条）、特定侵害事象を認知した際の所管大臣および内閣総理大臣への報告義務（同法5条）、情報共有および対策のための協議会への参加（同法45条）である。協議会では、攻撃者の詳細な活動状況や設備の脆弱性など、政府が把握する秘密性の高い情報の共有を受けられる。

これらの義務は特別社会基盤事業者に限定して課されるものであり、すべての民間企業に一律に及ぶわけではない。一般の事業者は直接の義務対象ではなく、政府が整理した周知用の分析情報の提供を受ける立場にとどまる。ただし、自社がソフトウェアの供給者である場合には、同法の脆弱性措置要請（同法42条）の対象となり得る。

もう一つの重要な点は、電子計算機などの供給者（ITベンダー）に対する脆弱性措置要請の制度化（同法42条）である。内閣総理大臣などは、脆弱性対応のために必要な措置を供給者に要請できる。同条には域外適用規

定があり、国外の供給者にも適用される。ゼロデイ脆弱性やサプライチェーン攻撃の経路となる製品・サービスが対象となる。

通信情報の利用は、国家機関側の権限として制度化されたものであり、民間事業者に直接の義務は課されない。ただし、脅威把握能力が向上した国家機関を通じて、先述した協議会経由で情報提供が拡充されることも見込まれ、その場合には、守秘義務の範囲が広がることになる。

5 フロンティアAIへの政府対応と Project YATA-Shield

以上の三法整備の進展と並行して、フロンティアAIの急進展に対する検討も始まっている。

Mythos公表後の約1カ月、政府は対応を急速に進めており、自民党による日本版「Project Glasswing」構想^{※1}や、金融庁主催の官民連携会議、重要インフラ24社への緊急点検要請、3メガバンクのフロンティアAI先行アクセス確保、金融庁検討作業部会発足などを経て、2026年5月18日、これらを集約する政府全体の対策パッケージとして「Project YATA-Shield」が取りまとめられた^{文献9}。

この政策パッケージは大きく3つの特徴を有している。

第1に、これは松本尚サイバー安全保障担当大臣を議長とする「AI性能の高度化を踏まえたサイバーセキュリティ対策に関する関係省庁会議」が、内閣官房国家サイバー統括室を中心とする14省庁・関係機関の連名で取りまとめた政府横断の文書である。

第2に、その施策は「重要インフラ事業者

等及び政府機関等への対応」と「脆弱性の発見・修正等への対応」という2つの柱の下に、計9施策として整理されている。第3に、これと併せて、重要インフラ事業者等、ソフトウェア・ベンダー、政府機関等の3主体それぞれを対象とし、内容の異なる注意喚起が個別に発出されている。

YATA-Shieldの基本姿勢は、「高性能AIの悪用リスクを前提としつつ、同AIを積極的にサイバー防御に活用する」という方針である。重要インフラ事業者等への注意喚起は、サイバーセキュリティを経営層リーダーシップ下の「必要な投資」と位置づけ、英国AISIによるClaude Mythos Preview評価^{文献10}を参照基準として基本的対策の徹底と高性能AI活用の両立を求めた。

ソフトウェア・ベンダーへの注意喚起は、セキュア・バイ・デザイン原則（設計段階からセキュリティを組み込む考え方）に基づく開発ライフサイクル全体での高性能AI活用と脆弱性早期対応を要請した。これらと並行して、AISIによる技術支援、外国政府機関・AI開発者との連携（Project GlasswingおよびGPT-5.5-Cyberへのアクセス確保を含む）が柱に据えられた。

官民連携の場としてはサイバー対処能力強化法に基づく協議会の枠組みが用いられ、同協議会の下で情報処理推進機構（IPA）およびAISIとの情報共有が強化されることが示されている。同法第42条「特定電子計算機等の供給者に対する脆弱性措置要請」の域外適用規定により、フロンティアAIを供給する海外事業者も日本の規制の射程に入る。YATA-Shieldは、個別法令ではなく関係省庁が分担実施する施策群の一体化文書である

ことが特徴であり、機動的な実施状況確認と継続の見直しが規定される点で、フロンティアAI動向の急変に追随し得るガバナンス枠組みであると位置づけられる。

Ⅳ 国際整合性： サイバー安保法制とAI規制

1 欧米のサイバー安保法制とAI規制

欧米主要国もサイバー安全保障分野において、官民連携の強化、通信情報の利用、攻撃者サーバなどへの侵入・無害化、の各領域で先行的取り組みを整備している。本章では、企業実務に直接的に影響するであろう官民連携の領域を中心に、各国の法制度のポイントを整理する。

欧州では、NIS2指令^{文献11}（2024年10月加盟国国内法化）が広範な重要分野および重要産業を対象とし、リスク管理措置の網羅性、インシデント報告期限の厳格化、サプライチェーンセキュリティ義務、経営層の個人責任までを定めている。経営層はサイバーリスク管理措置の承認、実施監督、定期訓練を直接義務づけられ、違反時には全世界売上最大2%の制裁金と取締役個人責任が発生する構造である。サイバーセキュリティを取締役会の常設議題に押し上げる強い効力を持つことが特筆される。

EUサイバーレジリエンス法^{文献12}（2024年成立）は、デジタル要素を含む製品全般に脆弱性対応とソフトウェア透明性を義務づける、世界初の包括的な製品サイバーセキュリティ規制である。製品ライフタイム全期間にわたるパッチ提供義務とソフトウェア部品表

開示の要件は、製造業に「販売完了型」から「販売後長期サポート型」のビジネスモデルへの転換を迫り、製品ポートフォリオ全体の再設計と長期サポート原価による経営判断が求められることになった。

その他、金融機関にはデジタル・オペレーショナル・レジリエンス法^{文献13}が、第三者ICT提供者の継続監視や脅威ベース侵入テストを含む厳格な体制要求を課している。同法はクラウド・SaaSなどの第三者依存リスクの統制責任を「契約事項」から「経営事項」へと格上げし、取締役会レベルでのデジタル耐性枠組み承認を経営の常時業務として組み込ませた。これらEUの規制はEU域内にとどまらず、欧州に拠点を持ち、欧州市場で製品を販売し、欧州顧客にサービスを提供する日本企業はすべて対象となる。

米国は、国家サイバーセキュリティ戦略(2023年)の下、重要インフラサイバーインシデント報告法(CIRCI A、2022年)でインシデント報告を制度化し、大統領令14028^{文献14}(2021年)によりソフトウェア部品表(SBOM)を政府調達標準要件とした。

CIRCI Aは、重要インフラ事業者に重大インシデント認知から72時間以内、ランサム支払いから24時間以内の報告を義務づけており、インシデント検知から経営判断・公表に至る社内意思決定プロセスの抜本的短縮と、報告判断を担う経営層の常時即応体制の整備を迫る。

大統領令14028は、SBOM・ゼロトラスト(全アクセスを常時検証する設計)やサプライチェーン透明性を米国政府調達の標準条件とすることで、米国政府および政府契約企業の先の取引先(下流に当たる顧客)との取引

を継続するために、製品開発ライフサイクル全体への安全性組み込みを経営判断として実装することを求めている。

国防分野では、サイバーセキュリティ成熟度モデル認証(CMMC)を整備し、機微情報を扱う取引先に対して水準充足を求めている。そのため、防衛サプライチェーンに連なる日本企業は認証取得コストと運用体制の整備を事業継続条件として組み込まざるを得ない。CIRCI Aおよび大統領令14028は、政府調達やインシデント報告の経路を通じて事実上の域外効果を有するため、米国市場や米国政府調達と接点を持つ日本企業は同等の対応水準を求められる。

以上のサイバー安保法制に加え、欧米はAI規制も整備している。EU AI法^{文献15}(2024年成立)はハイリスクAI(人命や基本的人権への影響が大きい用途に用いられるAI)にリスク管理、データガバナンス、技術文書、人間による監督、サイバーセキュリティ要件、適合性評価、市販後監視などを義務づけ、禁止行為については最大全世界売上の7%、ハイリスクAI規定違反については同3%の制裁金を定める。

フロンティアAIに該当する汎用AIモデルには、別個の透明性義務が課せられるとともに、社会全体に連鎖的影響を及ぼす恐れ(システムック・リスク)には追加の義務が設けられた。

米国では2025年AI Action Plan^{文献16}が、基幹インフラのAI活用に対するサイバーセキュリティ要件、AI開発者の責任ある公開体制への協力要請、政府調達におけるAI評価基準の整備を盛り込み、連邦取引委員会・証券取引委員会も個別の規制を進めている。さら

に2026年3月にはトランプ政権下で新たな国家サイバーセキュリティ戦略^{文献17}が公表され、規制負担の合理化に加え、AI技術スタック全体の保護と自律型AIの防御活用を国家戦略レベルで明示しており、今後は同戦略を具体化する執行命令や標準の整備、AIサプライチェーンに対するベンダー要件、政府調達におけるAI駆動セキュリティの標準化などの制度化が進むといわれている。

現に2026年6月には、フロンティアAIモデルに特化した大統領令^{文献18}が署名され、先進AIモデルの政府・重要インフラへの最大30日間のリリース前アクセスを自主的枠組みとして確保し、財務省主導の脆弱性修正調整機能の新設、CISAによる民間向けAI防御ツール提供の指令、AI悪用犯罪への執行強化を定めた。米国市場や政府調達と接点を持つ日本企業もこうした動向を注視し、早期の対応に着手することが求められる段階に入っている。

2 国際的な対応動向と 日本企業への含意

このようにサイバー安保法制とAI規制への対応は、すでに国際的な政策アジェンダにもなっている。

2026年5月19日にパリで採択されたG7財務大臣・中央銀行総裁共同声明^{文献19}は、フロンティアAIモデルをめぐる最近の進展を踏まえ、G7サイバー専門家グループ（G7 CEG）がAI関連のサイバーセキュリティ上のリスクと機会の把握、情報共有強化、ベストプラクティスの特定にかかる追加的取り組みを進めていることを明記した。G7加盟国である日本の主要企業、具体的には金融機関や重要

インフラ事業者も、この国際合意の対象事業者に位置づけられる。

その他欧米以外の個別規制当局の注目すべき動きとしては、2026年4月にオーストラリア健全性規制庁（APRA）が全規制機関（銀行・保険・年金信託）宛に発出した「AIに関する業界書簡（APRA Letter to Industry on AI）」^{文献20}が挙げられる。

同書簡は、文中でフロンティアAIモデル Mythos（アンソロピック）に明示的に言及し、取締役会レベルではAI関連リスクの妥当性を実質的に問いただせる技術リテラシーと、リスク許容度に整合したAI戦略・監視トリガーを要求した。

執行役員層（最高リスク責任者、最高技術責任者、最高情報セキュリティ責任者）には、AI特有の脅威への統制策、AIライフサイクル全体（設計から廃止まで）の評価、AIサプライチェーン全依存関係の把握、モデル挙動の継続監視、統合的な保証体制の確保が求められた。フロンティアAI時代における取締役会や執行役員層の説明責任を、規制当局として最も具体的に明文化した事例である。

日本企業も、監督当局の運用基準が今後、APRA水準を参照する蓋然性を踏まえ、取締役会の議論枠組みと、リスク・技術・情報セキュリティ責任者の役割定義を、AIライフサイクル全体の継続監視を組み込んだ形に再設計する必要がある。同時に、G7合意形成プロセスへの追従が求められ、中でも金融機関・重要インフラ事業者においては、国際的説明責任の確保が経営アジェンダとして問われる段階に入っているといえるだろう。

V 「規制対応」から 「安全保障投資」へ： 両面性のある経営転換

1 法令遵守を超えた安全保障投資

第Ⅲ・Ⅳ章で見たとおり、日本国内の法制と国際的な規制はいずれも、企業に対しセキュリティ対応の強化を義務づける方向で整備が進んでいる。しかし、国家関与型攻撃の常態化、サプライチェーン経由侵害の深刻化、機微情報窃取の戦略化を踏まえれば、法令遵守自体は守りの起点でしかない。

日本企業がいま真に直面しているのは、サイバーセキュリティを「ITコスト」から「安全保障投資」へと位置づけ直す、根本的な認識転換である。法令対応の有無ではなく、何を、どこまで、どのように守るかという経営判断の質が問われる段階に入った。

経済安全保障経営ガイドラインが原則の第2に「経済安全保障対応を単なるコストではなく投資と捉える」を掲げているのは、まさにこの認識転換を企業経営の標準に組み込もうとする政策意図の表れである。

従来、サイバーセキュリティ予算は、IT予算の一部として情報システム部門の管掌下にあり、コスト削減の対象でもあった。しかしサイバー対応力は、事業継続、取引先からの信頼、国家安全保障への貢献の3点で経営の根幹に直結する。これらは投資判断の対象であって、削減対象ではない。「サイバー予算を減らせるか」という問いから、「どこに投資して競争優位を構築するか」という問いへ、経営の問題設定そのものを変える必要がある。

この認識転換は、政府が掲げる国家戦略の

方向性とも軌を一にする。2025年12月に改定されたサイバーセキュリティ戦略は、「世界最高水準のレジリエンスを持つ国家」を最終目標に掲げ、防御を完遂する発想から侵入・被害を前提とする「サイバーレジリエンス」への転換と、受動的対応から能動的対応（プロアクティブ）への転換という2つの軸を明示している。企業が行う「安全保障投資」も同様に、侵入や被害を完全に防ぎ切る発想から、侵入・被害を前提に被害を最小化し、早期復旧に資する能力を強化する方向へ、投資の重心を移すことを意味する。

投資としての位置づけを成立させるには、サイバーリスクを経営の言語で議論する共通基盤が必要である。情報リスク要因分析^{注2}などの定量化枠組みを用い、サイバーリスクを年間予想損失額として金銭表現し、リスク許容度と対比して投資判断することが望ましい。

取締役会では、情報システムの実装状況の詳細ではなく、損失額、許容度、進捗指標、規制対応の状況など、経営判断に直結する指標で議論することが求められる。最高情報セキュリティ責任者（CISO）についても、その役割を形式的に設置するのではなく、権限・予算・経営アクセス権を伴う「実質的CISO」として機能することが、この共通基盤を構築するうえで不可欠となるであろう。

2 フロンティアAIの 両面性と経営者責任

フロンティアAIがもたらす構造変化は、攻撃側の能力拡張だけでなく、防御側の能力拡張も同時に可能にする両面性を持つ。攻撃側で観測された4つの構造変化（①能力の段

階的飛躍、②攻撃の裾野の拡大、③時間軸の圧縮、④採算性のシフト）と同じ技術基盤は、防御側にも適用可能である。たとえば、フロンティアAIを脆弱性発見・パッチ優先順位づけ・インシデント解析・ログ相関分析に組み込み、人手では実現困難な速度と規模で防御運用を高度化できる。

業界横断的な整理として、Cloud Security Allianceが2026年に公表した「推奨アクション」では、第1に防御側にAIを取り込むこと、第2に運用サイクルを年次・四半期から日次・常時稼働へ転換すること、第3に攻撃成立を阻止する層への投資（ゼロトラスト、欺瞞技術と呼ばれる攻撃者を誘引・検知する仕組み）、第4に経営管理の再設計、の4つのアクションを提示している^{文献21}。

この点は、日本政府もProject YATA-Shieldにおいて触れている。この政策パッケージでは「高性能AIの悪用リスクを前提としつつ、同AIを積極的にサイバー防御に活用する」と明示しており、経営層が自社で同様の姿勢を取るうえでの政策的な裏づけともなる。また、本稿が論じる「規制対応」から「安全保障投資」への経営姿勢転換の根拠を強化することにもなる。フロンティアAIの脅威に受動的に対応するのではなく、同技術基盤を競争優位の源泉として位置づける経営判断の巧拙が、今後、企業価値の差を生むことになる。EU AI法のハイリスクAI規制のように、2027年以降の規制対応自体が、AI関連ビジネスの参入条件として機能する局面も視野に入ってくる。

フロンティアAIの防御活用は、新たな経営リスクを生むことを併せて留意する必要がある。高性能AIを供給できる事業者は世界

でも少数かつ偏在しており、防御運用をそのインフラに全面的に依存させれば、自社の脅威データや脆弱性情報が特定の海外ベンダーに集積する構造に陥りやすい。これは防御能力そのものを外部に握られる「グローバルなロックイン」とも呼ぶべき依存であり、安全保障上の問題に転じ得る。

この懸念は、2026年6月に現実のものとなった。米国政府は同月、安全保障上の理由（懸念国による軍事転用リスク）から輸出管理権限を用いて、最先端モデルへのアクセスを米国人に限定し、同盟国の利用者や供給元企業の外国籍従業員までを一律に制限する措置を発動した。供給元のアンソロピックは、コンプライアンス確保のため該当モデルを全世界で一時的に無効化し、複数の米系金融機関も海外拠点の従業員によるAI利用を自主的に停止した。措置は同月末に全面撤回され、提供も再開されたものの、フロンティアAIへのアクセスの可否が、一企業の判断にとどまらず供給国の政策によって左右され得ることが、ここで明確になった。

このような現実を踏まえれば、経営層がまず認識すべきは、フロンティアAIへのアクセス権の確保自体を目的としないという点である。本質は、複数のモデルを用途ごとに使い分ける運用能力と、自社データを意味づけ・整理したうえで、分析に供する基盤の整備にある。

したがって、経営判断としては単一ベンダーへの集中を避けるマルチモデル・分散調達、契約とデータガバナンスにおける主権の確保、そして国産技術やオープンソースを含む代替手段の選択肢確保を調達戦略に組み込むことが必要になる。これは経済安全保障経

営ガイドラインが掲げる自律性確保・不可欠性確保とも直結する。

第Ⅳ章で見たとおり、国際的な規制は経営層自身の責任に踏み込んでいる。EUのNIS2指令は経営層の個人責任を明文化し、米国証券取引委員会のサイバー開示規則は重要事案の4営業日開示を上場企業に義務づけている。EU AI法でも、ハイリスクAIの導入者には経営層が責任を負う体制構築が求められている。

欧州中央銀行（ECB）のフランク・エルダーソンECB監督委員会副議長は、ECBの公式Webサイト内のインタビューにおいて、「EUの銀行はフロンティアAIモデルへのアクセスがないことを行動しない言い訳とすべきではない」と公の場で警告している^{文献22}。フロンティアAIへのアクセス制約は、経営層がリスク管理を後ろ倒しにする正当な理由として認められないというメッセージである。

日本においても、会社法上の内部統制システム構築義務の対象に、サイバーリスクとAIリスクを明示的に位置づけることは避けられない。経営者がフロンティアAI時代のサイバーリスクおよびAIリスクの管理状況を取締役会で説明できないこと自体が、善管注意義務違反のリスクとなりつつある。

Ⅵ 経営者が今、 着手すべき行動指針

第Ⅴ章で論じた「規制対応」から「安全保障投資」への認識転換を実装するため、筆者は日本企業の経営層が今、着手すべき行動指針として、次の3つの柱を提示する。これら

は独立した取り組みではなく、経営直轄で同時並行的に推進すべき課題である。

1 経営ガバナンスの確立

1つ目の柱は「経営ガバナンスの確立」である。

第1に、サイバー安全保障対応を中期経営計画と予算プロセスに明示的に組み込むことである。これまでサイバー予算はIT部門の年度要求として個別に審議されがちであったが、その位置づけは事業継続、取引適格性、国家安全保障への対応などを含めた検討へと変わった。中期経営計画に独立項目として明示し、投資計画、人材計画、取引先評価、内部統制設計に反映することが望ましい。経済安全保障経営ガイドラインが示す自律性確保・不可欠性確保・ガバナンス強化の各領域に、自社の投資配分を紐づける作業が出発点となる。

第2に、取締役会へのサイバーリスク定期報告の制度化である。年1回の概況報告ではなく、四半期ごとの定期報告に加え、前述したMythosのような重大事象の発生時には随時、経営課題として対応を検討する機動的な体制を整える。定量的なリスク指標、重大インシデントの有無、規制対応の進捗、人材確保の状況を、平時は四半期ごとに、有事には随時、取締役会で確認する仕組みとする。CISOには取締役会への直接のアクセス権を付与し、独立した報告ラインを確保する。第Ⅴ章で論じた経営者責任の国際潮流を踏まえれば、これらはもはや先送りできない論点である。

2 機微情報・クリアランス体制の整備

2つ目の柱は「機微情報・クリアランス体制の整備」である。

第1に、セキュリティ・クリアランス取得体制を早期に整備する必要がある。クリアランス体制の整備はすべての企業が対象になるものではないが、特に防衛、宇宙、半導体、量子、人工知能、サイバーセキュリティ技術などの分野で、政府調達や国際共同研究への参画を視野に入れる企業、すなわち適合事業者認定を目指す企業にとっては優先課題となる。

これらの分野では、今後、クリアランス保有が取引参入の事実上の要件となる可能性が高い。取締役会レベルで戦略を決定し、保護責任者の指名、情報保全規程の策定、対象人材の選定、施設設備の整備を並行して進める必要がある。特に施設整備（執務室・保管容器・スタンドアロンの電子計算機など）には数カ月以上の準備期間を要するため、判断の遅延がそのまま機会損失に直結することに留意すべきである。クリアランスの認定を目指す企業も、まず機微情報・重要技術の棚卸し（後述）から着手し、自社が保全対象情報を扱うか否かを見極めることが出発点となる。

第2は、機微情報・重要技術情報の棚卸しである。経済安全保障推進法の特定重要設備・特定重要技術、重要経済安保情報保護活用法の重要経済基盤保護情報、不正競争防止法上の営業秘密の所在を、自社の事業地図と重ね合わせて可視化する。情報の所在は、自社サーバ、海外拠点、共同研究先、合弁会社、委託先と多岐にわたるため、機微情報・

重要技術情報を洗い出し、保護に向けた優先順位を決めるには、それらが有する情報を包括的に棚卸ししなくてはならない。この点については、サプライチェーン上での対策も必要になるが、その詳細については、本特集の第二論考「取引先のセキュリティは『自社のリスク』である」を参照されたい。

3 防御態勢の整備と高度化

3つ目の柱は「防御態勢の整備と高度化」である。

第1に、脅威インテリジェンスを活用した能動的防御態勢の整備を進める必要がある。攻撃の高度化と速さを踏まえれば、侵害される前に検知し、対処する発想への転換が必要である。継続的脅威エクスポージャー管理^{注3}を運用の骨格に据え、24時間の監視運用センター（SOC）、内部端末の挙動監視（EDR）、検知の自動相関（SIEM）への投資を進める。ただし、正規ツールを悪用する攻撃やEDRの無効化など、端末監視だけでは検知が困難な手口も確認されており、ネットワーク通信の挙動を監視するNDR（ネットワーク検知・対応）や、横展開を遮断するマイクロセグメンテーションを組み合わせた多層的な検知・封じ込めが求められる。

これらの具体的な技術動向については本特集の第一論考「企業価値を守るランサムウェア対策」を参照されたい。また、JPCERTコーディネーションセンター、金融分野の情報共有・分析センター、業界別の情報共有分析組織との連携を平時から維持することも欠かせない。この観点から、サイバー対処能力強化法の協議会への参加準備も、対象事業者にとっては喫緊の課題である。

第2に、フロンティアAI時代における防御側能力の獲得とSLAの再設計が必要となる。第Ⅱ章で見た4つの構造変化、特に時間軸の圧縮は、従来の脆弱性対応SLAの根本的な見直しを迫っている。公開から数時間～数日以内での対応を可能にする運用体制への移行が、特に基幹インフラ・金融・防衛産業の事業者には喫緊の課題となる。

この点について、金融セクター業界団体であるFS-ISACは、2026年4月のセクターリスクアドバイザリにおいて、パッチ適用速度を経営の業績指標として取締役会報告対象とすることを推奨している^{文献23}。また、前述の米CISAが2026年6月に発出した拘束的運用指令BOD 26-04は、全脆弱性に一律の期限を課す従来方式を廃し、①一般公開、②悪用の自動化可能性、③全面掌握の可否、④現に悪用が確認されている（KEV掲載）こと、の4要件をすべて満たす最高リスクの脆弱性のみ3日以内の修正とフォレンジック調査を義務づけ、リスクの低いものは14日・60日あるいは次回更新時への後ろ倒しする方針を示している。

このことは、深刻度（CVSS）を一律基準とする発想から実際の悪用リスクに資源を集中させる優先順位づけへの転換であり、限られた対応リソースをどこへ振り向けるかという経営判断の枠組みとして参照に値する。そのような運用体制を構築するうえでは、次の3つの方向で組織的な取り組みを並行して進めることがカギとなる。

- ①フロンティアAIを防御・活用する取り組みとして、自社コードへのAI駆動診断の組み込み、AIエージェント（自律

的にタスクを実行する形態のAI）導入の社内制度化、AIエージェント基盤自体の保護を進める。AIエージェントの本番環境への直接アクセスは原則として読み取り専用、隔離環境、人手承認を必須とする

- ②脅威対応の速度を組織として引き上げる。継続的なパッチ適用、攻撃面の常設監視、および自動対応能力の整備を通じ、脆弱性の発見から対応完了までのリードタイムを大幅に短縮する体制を確立する。この運用水準の目標値は、情報システム部門が独自に定める事項でなく、経営層がSLAとして設定・監視する経営指標と合致させる
- ③経営管理の再設計として、セキュリティ・法務・エンジニアリングを横断する例外承認・緊急対応の意思決定機構を取締役会直下に設ける。リスクモデルおよび経営報告は、年次・四半期報告から継続テレメトリ型（指標を常時計測し随時更新する形態）に転換する

これら3つの方向は、Project YATA-Shieldが、重要インフラ事業者等、ソフトウェア・ベンダー、政府機関等に対して発出した注意喚起の内容とも整合する。経営層は、自社がいずれの主体に位置づけられるかを確認し、Project YATA-Shieldが示した参照施策である、①英国AISIのClaude Mythos Preview評価が示す基本的対策の重要性、②米CISA「CI Fortify」^{文献24}が示す隔離・復旧の重要インフラレジリエンス枠組み、③セキュア・バイ・デザイン原則に基づくソフトウェア開発ライフサイクル（SDLC）全体での高性能AI

活用などに沿って具体的な実施計画を策定する必要がある。

もっとも、こうした体制整備やSLAの短縮だけで脆弱性の問題が解消するわけではない。フロンティアAIが噴出させる脆弱性は万単位に達し、修正版の開発と、とりわけ下流における適用判断・システムへの適用が処理能力を超えてしまっている。また、即時に対応できる組織は一部に限られるため、構造的に積み残しが発生する。とりわけ重要インフラのようにシステム更改サイクルが長期にわたる領域では、短期的な高速対応のみでは到底追いつかない。

経営層には、修正未完了や侵入を前提とした被害局限、早期復旧、縮退運転といったレジリエンス強化への投資を、対応速度の向上と並行して進める覚悟が求められる。加えて、同業他社はシステム特性が類似することから、脆弱性への対応要否の判断、検証、適用といった作業を業界の情報共有分析組織（ISAC）などで分担する集団的アプローチも、現実的な選択肢として検討に値する。

サイバー安全保障対応力は、フロンティアAI時代の日本企業にとって、調達適格性、信頼性、競争力を左右する経営の根幹となる。「守り」の姿勢を超え、安全保障への貢献と防御側能力獲得の両面を競争優位の源泉と捉える経営変革が、今、強く求められている。

注

- 1 米国では、財務省主導の下で金融機関等が参加する官民連携枠組みである「Project Glasswing」が始動している。日本版「Project Glasswing」は、これを踏まえ、自民党の国家サイバーセキ

ュリティ戦略本部・金融調査会の合同会議（2026/4/20）で、政府内に同様の枠組みを立ち上げ、Claude Mythosなどの高度AIを用いて脆弱性の発見・修正を行うこと、さらに基幹インフラ事業者の防衛も対象とする拡大版に取り組むことが提唱された構想を指す

- 2 情報リスク要因分析（FAIR：Factor Analysis of Information Risk）は、リスクを「損失イベントの発生頻度」と「発生時の損失規模」に分解し、脅威・脆弱性・資産価値などの下位要因をそれぞれ確率分布で表現したうえで、年間予想損失額として定量化する手法である。これにより、リスク許容度との対比に基づく投資判断や複数のリスクを横断的に比較した優先順位づけが可能となる
- 3 攻撃者目線で自社のエクスポージャを継続的に発見・優先づけ・検証する運用フレームワークである。米調査機関ガートナーが2022年に提唱した

参考文献

- 1 アンソロピック “System Card : Claude Mythos Preview” (2026/4/7)
<https://www-cdn.anthropic.com/8b8380204f74670be75e81c820ca8dda846ab289.pdf>
- 2 AI Security Institute (UK) “Our evaluation of OpenAI’s GPT-5.5 cyber capabilities” (2026/4/30)
<https://www.aisi.gov.uk/blog/our-evaluation-of-openais-gpt-5-5-cyber-capabilities>
- 3 AI Security Institute (UK) “How fast is autonomous AI cyber capability advancing?” (2026/5/13)
<https://www.aisi.gov.uk/blog/how-fast-is-autonomous-ai-cyber-capability-advancing>
- 4 コアリション “After Mythos: What Actually Changes for Cyber Risk” (2026/4/23)
<https://www.coalitioninc.com/blog/cyber-insurance/after-mythos-what-actually-changes-for-cyber-risk>
- 5 バルンチェック “Tracking CVEs Attributed to

- Anthropic Researchers and Project Glasswing” (2026/ 4 /15)
<https://www.vulncheck.com/blog/anthropic-glasswing-cves>
- 6 Mozilla “Behind the Scenes: Hardening Firefox with Claude Mythos Preview” (2026/ 5 / 7)
<https://hacks.mozilla.org/2026/05/behind-the-scenes-hardening-firefox/>
- 7 経済産業省 貿易経済安全保障局「経済安全保障経営ガイドライン (第1版)」(2026/ 1 /23)
https://www.meti.go.jp/policy/economy/economic_security/260123_guideline.pdf
- 8 内閣府「重要経済安保情報の指定及びその解除、適性評価の実施並びに適合事業者の認定に関し、統一的な運用を図るための基準」(2025/1 /31閣議決定)
https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/doc/kijun.pdf
- 9 内閣官房国家安全保障局ほか13機関「AI性能の高度化を踏まえたサイバーセキュリティ対策に関する関係省庁会議」(2026/ 5 /18)
https://www.cyber.go.jp/pdf/press/20260518_AI_CS_kankeishouchoukaigi.pdf
- 10 AI Security Institute (UK) “Our evaluation of Claude Mythos Preview’s cyber capabilities” (2026/ 4 /13)
<https://www.aisi.gov.uk/blog/our-evaluation-of-claude-mythos-previews-cyber-capabilities>
- 11 European Union “Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)” (2022/12/14)
- 12 European Union “Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)” (2024/10/23)
- 13 European Union “Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA)” (2022/12/14)
- 14 U.S. Executive Office of the President “Executive Order 14028 on Improving the Nation’s Cybersecurity” (2021/ 5 /12)
- 15 European Union “Regulation (EU) 2024/1689 on Artificial Intelligence (AI Act)” (2024/ 6 /13)
- 16 The White House “America’s AI Action Plan” (2025/ 7)
<https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>
- 17 The White House “President Trump’s CYBER STRATEGY for America” (2026/ 3)
<https://www.whitehouse.gov/wp-content/uploads/2026/03/President-Trump’s-Cyber-Strategy-for-America.pdf>
- 18 The White House “PROMOTING ADVANCED ARTIFICIAL INTELLIGENCE INNOVATION AND SECURITY” (2026/ 6 / 2)
<https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/>
- 19 財務省「G7財務大臣・中央銀行総裁共同声明 (仮訳)」(2026/ 5 /19)
https://www.mof.go.jp/policy/international_policy/convention/g7/g7_20260519_05.pdf
- 20 Australian Prudential Regulation Authority “APRA Letter to Industry on Artificial Intelligence (AI)” (2026/ 4 /30)
<https://www.apra.gov.au/apra-letter-to-industry-on-artificial-intelligence-ai>
- 21 Cloud Security Alliance “The ‘AI Vulnerability Storm’: Building a ‘Mythos-ready’ Security Program” (2026/ 4 /12)
<https://labs.cloudsecurityalliance.org/research/ai-vulnerability-storm-mythos-ready-security-program/>
- 22 European Central Bank “Market fragmentation is banks’ real constraint” (2026/ 5 /13)
<https://www.bankingsupervision.europa.eu/press/interviews/date/2026/html/ssm.in260513~cb8e1269c5.en.html>
- 23 FS-ISAC “Sector Risk Advisory: Preparing the Enterprise for AI-Enabled Vulnerability Discovery” (2026/ 4 /19)

<https://www.fsisac.com/knowledge/sector-risk-advisory-preparing-the-enterprise-for-ai-enabled-vulnerability-discovery>

- 24 Cybersecurity and Infrastructure Security Agency “CI Fortify: Strengthening Resilience Across Critical Infrastructure” (2026/5/5)
<https://www.cisa.gov/topics/industrial-control-systems/ci-fortify>

著 者

藤井秀之（ふじいひでゆき）

NRIセキュアテクノロジーズ インテリジェンスセンター統括部 部長

専門はサイバーセキュリティやデジタル政策に関するインテリジェンス分析