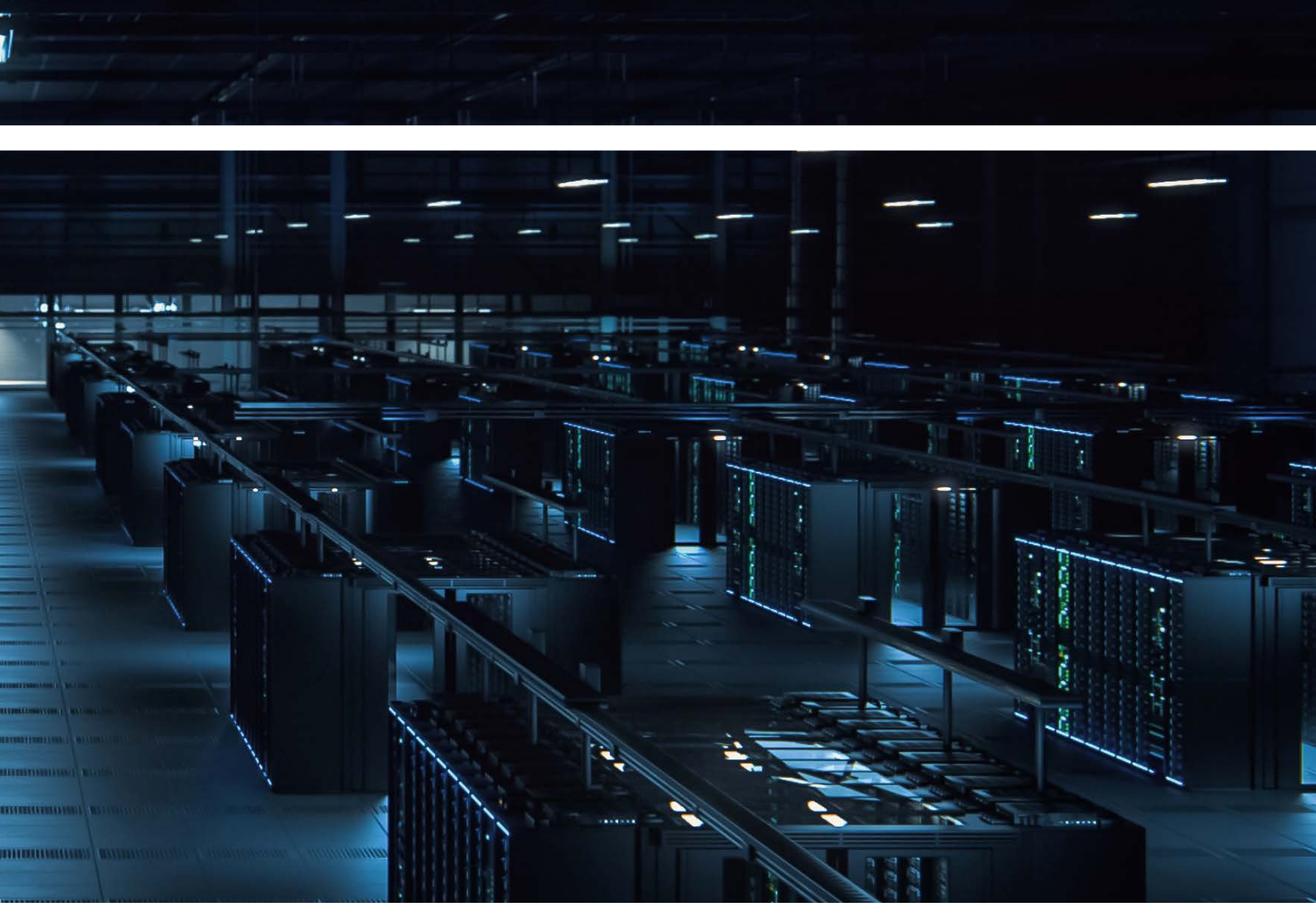
2024年 Cyber IQ 調査

―デジタル化が生む「トラストギャップ（信頼の空白域）」を埋めるには―

pwc

www.pwc.com/jp

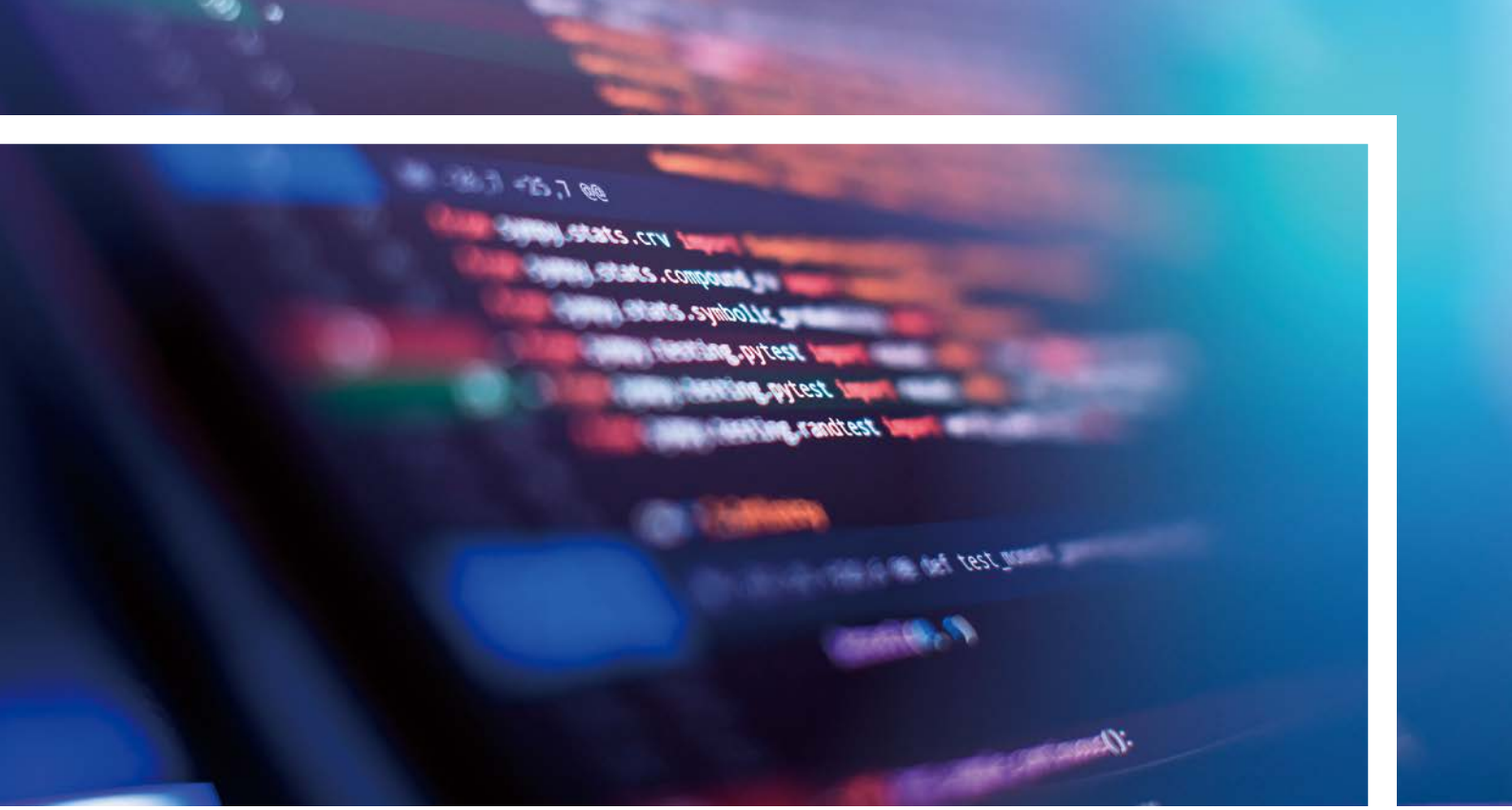
目次



はじめに

デジタルトランスフォーメーション（DX）があらゆる分野で進展する昨今、デジタルの技術革新スピードはますます加速しています。こうした状況下では、地政学的な緊張の高まりとともに、各国・地域の規制やルールも目まぐるしく変遷。さらに、サイバー攻撃においても最新技術を巧妙に採り入れることで、攻撃手法は日々刻々と進化しています。企業は、これらの変化に対応するために、脅威をタイムリーに捉え、的確に対処することが求められています。

本稿では、各国の法規制、生成AI、サプライチェーン、脆弱性管理など、特に変化の激しい分野に関して、潜在的なリスクや企業に求められる対応を考察しました。本稿から得られるサイバーインテリジェンスが、日本企業の皆さまがセキュリティ対策を講じるうえでの一助となれば幸いです。



第1章-1
経済安全保障推進法とサイバーセキュリティ対策

経済安全保障とは

世界情勢が不安定になり、地政学的な緊張が高まる中、自国の脆弱性や潜在的なリスクを軽減する方法として「経済安全保障」という概念が注目されています。経済安全保障とは、経済上の措置を講じ、国の平和と安全や経済的な繁栄などの国益を確保することを指します。

経済安全保障の概念は大きく「戦略的自律性」と「戦略的優位性・不可欠性」に分類されます。前者は、国民生活や社会経済活動の維持に不可欠な基盤を強靭化することにより、いかなる状況下においても他国に過度に依存せず、正常な国民生活と経済運営という安全保障の目的を実現することを意味しています。後者は、国際社会全体の産業構造の中で、自国の存在が国際社会にとって不可欠な分野を戦略的に拡大することであり、自国の長期的かつ持続的な繁栄および国家安全保障を確保することを示します。

日本における経済安全保障推進法とは

日本においても、2022年5月に経済安全保障推進法[1]が成立し、①重要物資の安定的な供給の確保、②基幹インフラ役務の安定的な提供の確保、③先端的な重要技術の開発支援、④特許出願の非公開に関する4制度の創設が盛り込まれました（図表1）。4制度は公布から2年以内に段階的に施行される予定となっており、①と③はすでに制度運用が開始されています。②と④は2024年春頃に制度運用の開始を予定しています。②については、2023年8月に対象企業の基準が、同年11月には対象となる企業が発表され、2024年5月17日からの運用開始が予定されています。

本稿では、②基幹インフラ役務の安定的な提供の確保を実現するために、対象となる企業がどのような措置を行う必要があるかを解説します。

1 経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（経済安全保障推進法）

図表1：経済安全保障推進法の概要

	戦略的自律性		戦略的優位性・不可欠性	
4つの柱	①重要物資の安定的な供給の確保（サプライチェーンの強靭化）	②基幹インフラ役務の安定的な提供の確保	③先端的な重要技術の開発支援（官民技術協力）	④特許出願の非公開（特許出願の非公開化）
対象領域	半導体、蓄電池、重要鉱物、工作機械、船舶部品、肥料、抗菌薬など	電気、ガス、水道、情報通信、放送、金融、クレジットカード、運輸、郵便など	宇宙・海洋・量子・AI・バイオなどの分野における先端的な重要技術	原子力関連技術、軍民デュアルユース製品など
施行	2022年12月	2024年5月	2022年12月	公布から2年以内（～2024年5月）
概要	• **国民の生存や国民生活・経済活動に甚大な影響のある物資**（半導体や医薬品など）**の安定供給の確保**のため、「特定重要物資」を指定 • **供給確保計画の認定**を受けた民間事業者には**資金支援などを行い**、民間の取り組みでは不足の場合には、政府が対策（備蓄など）を実施	• **特定社会基盤事業14業種の重要設備**（機器、ソフトウェア、クラウドサービスなど）が外国から行われる妨害行為の手段として使用されることを防止するため、重要設備の**導入・維持管理などの委託先を事前審査**し、勧告・命令などを可能に	• 安全保障上重要な**先端的な重要技術**の研究開発の促進と成果活用のため、**資金支援**※や官民での情報共有を行う**協議会**を設置 • 対象技術はシンクタンクなどによる調査で不断に見直し	• 安全保障上**機微な発明の技術流出を防止**するため、出願後の審査で必要と認められた場合には**出願内容を非公開化**し、**特許の実施**（対象物または対象技術を使った物の生産）**を制限** • 審査対象技術の外国出願を制限 • 発明の実施が許可されず被った損害に対する補償の規定あり

※経済安全保障重要技術育成プログラムによる支援（5,000億円の支出）

②基幹インフラ役務の安定的な提供の確保とは

「基幹インフラ役務の安定的な提供の確保」は、電気、ガス、水道、情報通信といった国の重要な14業種のインフラを「特定社会基盤事業」、それを運営する事業者を「特定社会基盤事業者」と定めています。特定社会基盤事業者が他の事業者から特定重要設備を導入する場合や、特定重要設備の維持管理や操作を外部委託する場合には、「導入等計画書」を作成して事前に主務省庁に届け出たうえで、審査を受ける必要があります（図表2）。

この審査制度導入の背景には、重要基幹インフラがサイバー攻撃を受けて機能停止や障害などが生じる事案が世界的に発生し、国民生活や社会経済の安全、発展が大きく脅かされているという実態が挙げられます。国際情勢の緊迫度は年々高まっており、サイバー攻撃の脅威は今後も高まっていく見込みです。攻撃対象となりやすい重要基幹インフラを保有・運営する企業は、これらの対策が急務となっています。また、サイバー攻撃の脅威は、対象企業にとどまらず、サプライチェーン全体を脅かすことから、サプライヤーやSIer、その委託先企業（再委託先企業以降を含む）までが対象に含まれます。サイバー攻撃の脅威から基幹インフラの安全性・信頼性を確保することは、以前にも増して重要な課題であり、当該審査において懸念事項が発覚した場合は、導入や委託の見直し、中止の勧告・命令が行われることもあります。

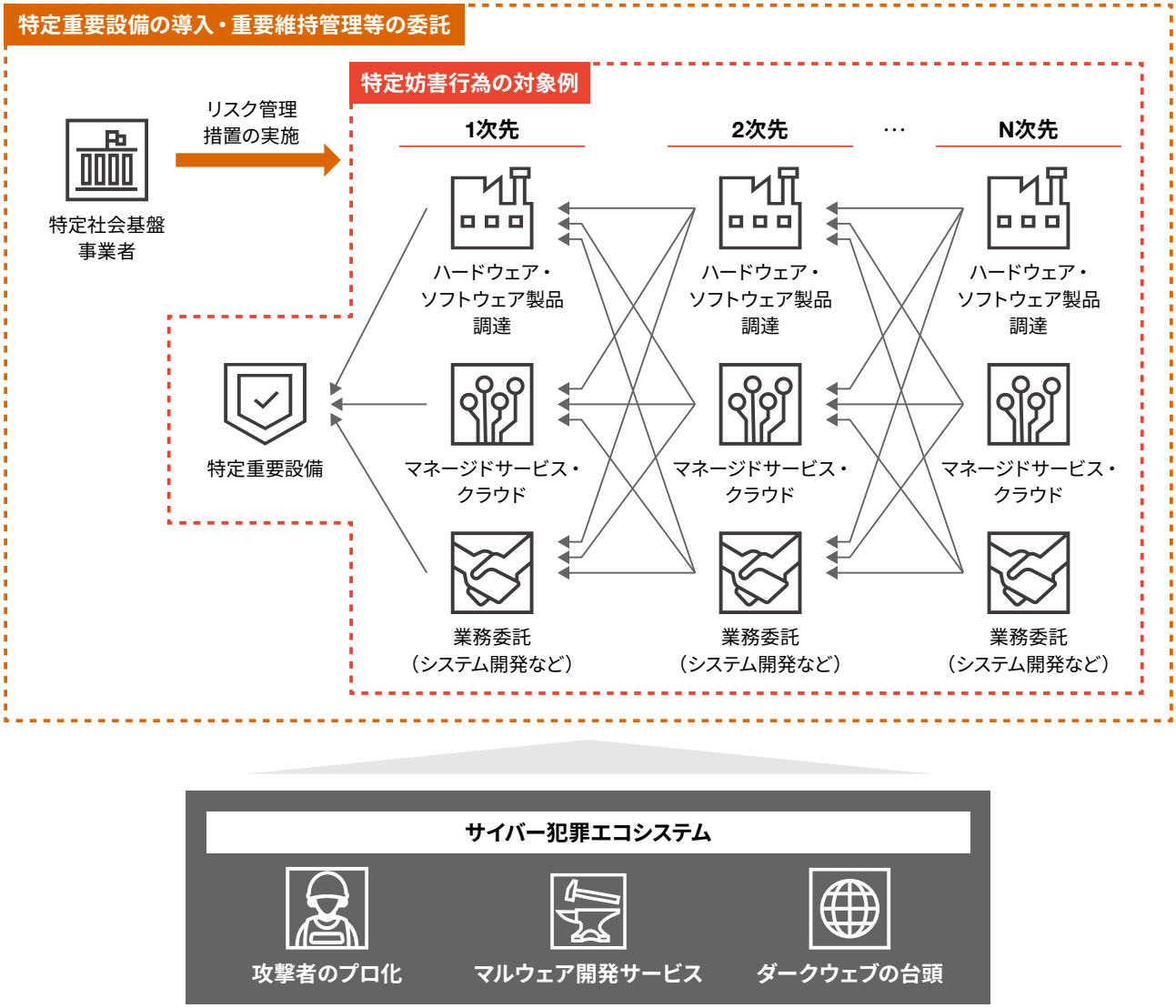
図表2：特定重要設備導入に関する審査制度の概要

対象者	**特定社会基盤事業者** 法に指定された14業種※のうち、該当サービスを提供しており、かつ大規模または事業停止時の代替性が小さい事業者
対象設備	**特定重要設備** 機能停止した場合、①役務の提供不可、②役務の品質・機能が喪失または低下、③役務の安定継続不可となるような設備
対象行為	特定重要設備の**導入・重要維持管理等の委託を行う場合** 設備の①導入、②維持管理（保守点検、部品交換、プログラム更新など）、③操作（運用・制御）
	導入等計画書を国に事前届出 特定重要設備の供給者に関する • 導入の内容（委託目的・内容、関係者の名称など） • 一定割合以上の議決権保有者 • 役員 • 外国政府との取引高 • 設備関連製品の製造場所
審査主体	事業所管大臣
考慮要素	**特定妨害行為の手段として利用される蓋然性** ①委託先が**外国の主体から受ける影響** ②妨害行為に関する**リスク管理措置**の有無 ③委託先の製品の脆弱性・基準の不遵守など、不適切性の**実績**有無　など
国の権限	特定妨害行為の防止に必要な**勧告・命令** （30日以内に行うが、外部環境の変化に応じ、委託開始後でも勧告・命令を行う可能性あり）

※港湾が追加され15業種になる予定

一方で、クラウド利用に代表されるサプライチェーンのデジタル化やグローバル化、複雑化はとどまることを知らず、重要基幹インフラの導入、および維持管理に関与する企業はますます増えることが予想されます。昨今のサイバーインシデント事例からも推察されるとおり、当該企業に対して直接的な攻撃が行われることもあれば、サプライチェーンを構成する事業者に対して攻撃が行われることもあります。そのため、重要基幹インフラの導入や維持管理においては、サプライチェーン全体で実効性のあるリスク管理措置を講じ、特定社会基盤事業者としての説明責任を果たすことが重要です（図表3）。

図表3：重要基幹インフラを取り巻くリスク



特定社会基盤事業者に求められるリスク管理措置とは

基幹インフラ役務の安定的な提供の確保に関する制度では、重要基幹インフラに対するリスク管理措置として導入する場合は17項目、重要維持管理等を委託する場合は12項目が例示され、「サイバーセキュリティ対策」と「サプライチェーンガバナンス強化対策」に大別されます。なお、これらのリスク管理措置は、「特定社会基盤事業者が自らリスクを評価し、そのリスクの内容及び程度に応じてリスク管理措置を講ずること」とされており、「すべての項目を実施すること」や、「記載の内容通りに実施すること」は求められていません。言い換えると、特定社会基盤事業者は、自社における現状の対策状況とサイバー攻撃によるリスクを見極め、例示を参考にしながら、必要な対策を選定・策定し、実行していくことが求められているのです。

サイバーセキュリティ対策の1つ1つは決して新しいものではなく、従来の安全管理措置、特に組織的安全管理措置の範囲で十分に対応ができると想定されます。そのため、今回のリスク管理措置の推進を、情報システム部門やセキュリティ管理部門が担うことが多いようです。本稿に先立ち、PwCが2023年10月に実施したアンケートにおいても同様の結論が得られています。

サイバーセキュリティ対策（抜粋）

技術的安全管理措置

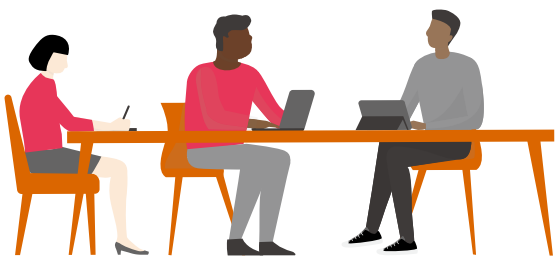
- 特定社会基盤事業者は、特定社会基盤事業者又は特定重要設備の供給者において、特定重要設備に悪意のあるコード等が混入していないかを確認するための受入検査その他の検証体制が構築されており脆弱性テストが実施されていることを確認している。
- 特定社会基盤事業者は、特定重要設備の供給者が特定社会基盤事業者によって調達時に指定された情報セキュリティ要件（特定重要設備及び構成設備に最新のセキュリティパッチが適用されているか否か、不正プログラム対策ソフトウェアを最新化しているか否か等）を実装していることを確認している。
- 特定社会基盤事業者は、特定重要設備の供給者が、特定重要設備にアクセス制御に関する仕組みを入れ、特定重要設備に対する不正なアクセスを監視するシステムを実装していることを確認している。　など

組織的安全管理措置

- 特定社会基盤事業者は、特定重要設備の供給者が、特定重要設備の開発工程において信頼できる品質保証体制を確立していることを確認している。
- 特定社会基盤事業者は、特定重要設備の供給者が、特定重要設備の製造過程における不正行為（例えば不正な変更等）の有無について、定期的な監査を行っていることを確認している。
- 特定社会基盤事業者は、特定重要設備の供給者及び特定重要設備の導入に携わる者が、特定重要設備の設置に際して不正な変更等を加えることがない体制を確立していることを確認している。
- 特定社会基盤事業者は、情報の漏洩等の情報セキュリティインシデントが発生した場合の対応方針・体制（マニュアル等の整備、定期的なインシデント対応の訓練等）を自ら整備している。　など

人的安全管理措置

- 特定社会基盤事業者は、特定重要設備をインターネット回線と接続する場合に、不正なアクセス等を防ぐための利用マニュアル・ガイダンス等を自ら適切に整備・実施している。　など



一方で、サプライチェーンガバナンス強化対策に関しては、アクセス管理や教育など、従来の安全管理措置も含まれているものの、経済安全保障という観点から、委託先企業の事業計画、供給者、委託先企業の役員、さらには資本関係の評価など、これまでとは異なる一歩踏み込んだ対策が多いと言えるでしょう。これらの包括的な企業与信評価に類する内容までを情報システム部門やセキュリティ管理部門が担うことは多くありません。そのため、上述のPwCのアンケートにおいても、リスク管理部門や経営企画部門が担うという回答が多いという結論を得ています。

経済安全保障の実現や、昨今の法規制・外部動向などへの追随には、多岐にわたる対策を推進する必要があることから、情報システム部門など、特定の役割を担う組織で全てを推進する難易度は高まりつつあります。今後、リスク管理部門や経営企画部門、もしくは全社横断的なタスクフォースを立ち上げるなど、全方位的なリスクマネジメントを推進できる態勢を整備し、実行していくことが重要です。

サプライチェーンガバナンス強化対策（抜粋）

- 事業者は、委託の相手方が保有している設計書や設備等の情報について、当該情報にアクセスできる要員を物理的（監視カメラ等の入退室管理等）かつ論理的（データやシステムへのアクセス防御）に適切に制限していることを確認している。
- 事業者は、委託の相手方が保有している設計書や設備等の情報について、当該情報にアクセスできる要員を物理的（監視カメラ等の入退室管理等）かつ論理的（データやシステムへのアクセス防御）に適切に制限していることを確認している。
- 事業者は、委託の相手方の事業計画（例えば、中期経営計画等の、委託契約の期間における役務の安定的な提供に与え得る事業上のリスク等を評価することができるものが該当する。）及び役務の提供実績等を適切に確認している。
- 事業者は、委託の相手方が、過去3年間の実績を含め、国内の関連法規や国際的に受け入れられた基準（それに基づいて各国で整備されている規制等を含む）に反していないことを契約等により確認している。
- 事業者は、特定重要設備及び構成設備の供給者や委託（再委託先を含む。）の相手方の名称・所在地、役員や資本関係等、事業計画や実績、設備又は部品の製造等や重要維持管理等の実施場所、作業に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）等に関する情報提供を受けられることを契約等により担保している。　など

まとめ

日本における経済安全保障推進法の基幹インフラ役務の安定的な提供の確保に関する制度は、2024年5月17日に運用開始が予定され、特定社会基盤事業者に認定された企業のみならず、各主務省庁においても対応に迫られています。特定社会基盤事業者は、サプライチェーン全般において、何の対策を実行する必要があるのか、どのように実行するべきかを見きわめなければいけません。一方、主務省庁においては、受領した届け出をどのように評価するかの検討が求められています。いずれの内容においても、現時点で明確な基準や画一的な見解はなく、今後、実際の制度運用を通して、業種ごとに、もしくは業種を横断して合意形成が成されていくものと推察されます。加えて、日本における経済安全保障の実現のため、対象となる業種は、現在の14業種から拡充されていく可能性があり、特定社会基盤事業者の認定有無に関わらず、全ての日本企業が、経済安全保障推進法をますます注視していく必要があります。

第1章-2

生成 AI によって変わるサイバー攻撃と防御

文書や画像などをAI（人工知能）によって短時間で自動的に作る生成AIが、世界の技術革新の中心に躍り出ました。経済・社会情勢を一変させ、私たちの働き方に大きな変革をもたらす可能性を秘める一方、AIが及ぼすリスクへの関心も強まっており、各国・地域はルール整備を加速させています。こうした可能性やリスクは、むろんサイバーセキュリティのあり方にも大きな変化をもたらします。

本稿では、生成AIがもたらすサイバー攻撃や防御のあり方の変化について、**①ビジネスリスク**、**②AIを利用した攻撃**、**③AIによる防御**、**④AIへの攻撃**に分類し（図表4）、それぞれの特徴や留意点を解説します（注：本稿では、後述のAIと生成AIの包含関係を踏まえ、生成AIに限定せず広義に捉えられる場合、AIという表現を使用します）。

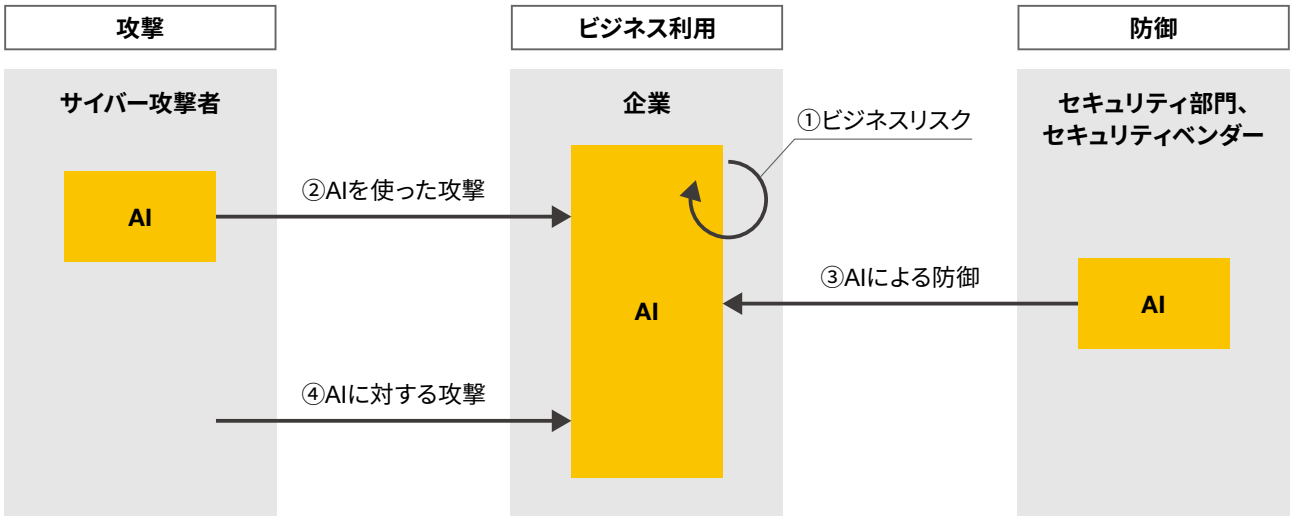
①ビジネスリスク：AIは、正確性、プライバシー、セキュリティ、コンプライアンス、知的財産の侵害など、いくつかのビジネスリスクを及ぼす可能性がありますが、ここでは主にコンプライアンスリスクに関する内容を扱います。企業はAIの責任ある利用を優先する必要があり、そのために欧州連合（EU）のAI規則案をはじめ、さまざまなグローバルのルール形成が進んでいます。既存法や情報取り扱いに関するコンプライアンスの観点でも、AIの法令リスクが存在します。

②AIを利用した攻撃：AIは、マルウェア、フィッシング、ソーシャルエンジニアリング攻撃などのサイバー攻撃を仕掛けるために使われる可能性があります。これらの攻撃は従来の攻撃よりも巧妙で、検知するのが難しいことが多いです。企業はこうした脅威を認識し、適切な対策を講じる必要があります。

③AIによる防御：AIはサイバー攻撃の防御にも利用できます。AIベースのセキュリティシステムは脅威をリアルタイムで検知して対応できるため、攻撃の特定と軽減にかかる時間を短縮する特徴があります。

④AIへの攻撃：AIシステムは、データポイズニング、モデル盗用、敵対的サンプル（既知のモデルに誤分類を誘発する攻撃）などの攻撃に対して脆弱である可能性があります。これらの攻撃はAIシステムの完全性を損ない、不正確な判断や偏った判断につながることがあります。企業はこうしたリスクを認識し、AIシステムを保護するための適切な対策を講じる必要があります。

図表4：生成AIがもたらすサイバー攻撃や防御のあり方の変化

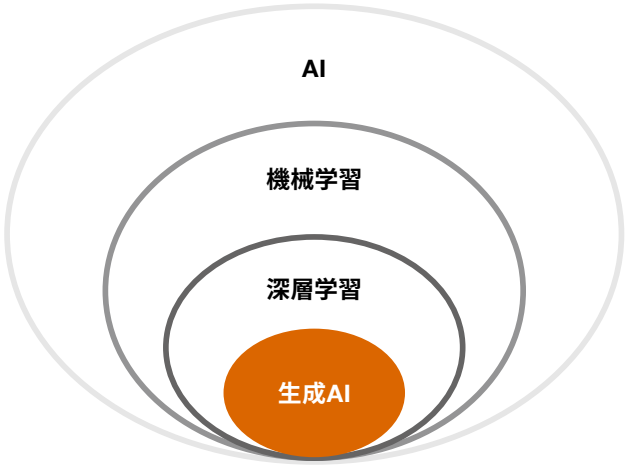


EUのAI規則案

生成AIは、画像や文章、音声、プログラムコードなどのさまざまなコンテンツを生成できるAIです。図表5のように、AI、機械学習、深層学習、生成AIの順に包含関係にあります。全体を包含するAIは広い概念であり、これまでも統一的な見解は必ずしもなく、専門家の間でも意見が分かれていました。そのため、EUがAI規則案によって法的にAIを定義したことは画期的と言えるでしょう。

AI規則案では、AIを「さまざまなレベルの自律性で動作するように設計され、明示的または暗黙的な目的のために、物理的または仮想的な環境に影響を与える予測、推奨、決定などの出力を生成できる機械ベースのシステム」と定義しています。これはEUのデータ関連法規制の流れに沿った内容となっています。

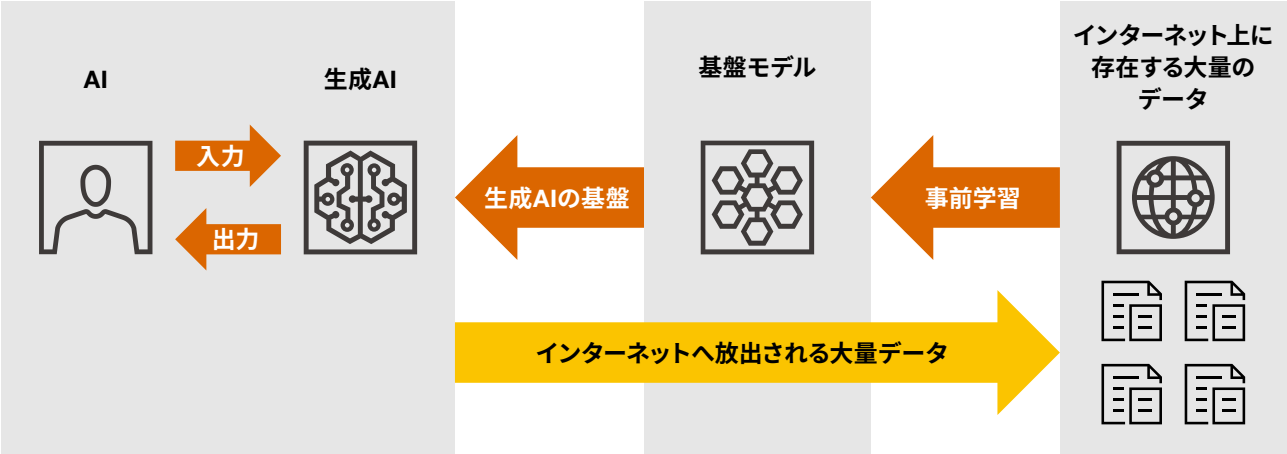
図表5：AIの包含関係



生成AIは大量のデータを学習してパターンを認識し、新しい文章や画像、音声といったさまざまなものを作ります。学習データには正確な情報だけでなく、意図的な偽情報、フィクションも含む可能性があります。悪意のあるアクター（行動主体）が操作するボット、すなわち実際には人間ではない、システムによって操作された主体が拡散するデータも混在する懸念もあります。また、生成AIは事実に基づかない情報を学び、新しい文章や画像生成に取り入れることもあり得ます。誤りや偏ったデータによって作られた生成物がインターネットに流れ、学習データとして活用されると「基盤モデル」にも不正確な情報が組み込まれる事態を招きます。そうした基盤に生成AIが新たにアウトプットをすれば、「負のループ」を生み出しかねません。

こうしたリスクを軽減するため、EUのAI規則案では基盤モデルについて特別の提案をしています。具体的には「複雑なシステムと予期せぬ影響」「下流のAI提供者が基盤モデルの開発をコントロールできないこと」「その結果生じる力の不均衡」「AIのバリューチェーンに沿った責任の公正な分担を確保する必要性」を背景に、基盤モデルについては「AI規則に基づき、相応かつより具体的な要件と義務を課すべきである」と定めています。

図表6：生成AIのデータ学習方法



AIのビジネスリスク

AIや生成AIの利用には、AIに特化した法律以外にも、データ関連法、プライバシー法、著作権法など、さまざまな既存法や情報取り扱いに関するコンプライアンスの観点からの目配りが必要です。

生成AIによるインシデントでどのようなものがあるか、例を挙げます。2023年、米国ニューヨーク州の民事訴訟において、弁護士が作成して裁判所へ提出した準備書面の中に、生成AIによる回答を基にした架空の判例が含まれていたという報道がありました。ここでの問題のポイントは以下にまとめることができます。

- 生成AIに関するリスク・ルールが組織内（所属の法律事務所内）で十分に周知されないまま、弁護士が自らの判断で応答系の生成AIを利用した
- 回答の基となった情報の引用元を提示する生成AIを利用するなど、生成AI特有のリスクを考慮したツール選択をしなかった
- 生成AIの回答を利用するにあたり、回答内容を妄信し、回答結果に関する十分な確認を怠った
- 生成AIの運用プロセス（品質チェックなど）が整備されていなかったため、第三者の確認が行われていない生成物が社外展開された

その他、大手韓国IT企業が生成AIの社内使用を許可したところ、従業員が機密性の高い社内情報を生成AIに入力してしまい、設備情報や社内会議の内容が漏洩したというインシデントがありました。ここでの問題のポイントとしては以下にまとめられます。

- ガイドラインの作成・展開にあたり、生成AI特有のリスク（入力データの学習など）について十分な分析ができていなかった
- リスクに関する十分な周知ができておらず、利用者が機密情報入力の危険性を十分に理解していなかった
- リスクシナリオの検討が不十分であり、データ保存に関する十分な対策（オプトアウトなど）をしていなかった
- きちんとした監視プロセスを定めていなかったため、機密情報漏洩への初動が遅れた

生成AIに関する新たなグローバルのルール形成として注目すべきは、前述したEUのAI規則案です。グローバル法規制の「モザイク化」が進む中、4.5億人の人口規模を有するEUの市場影響力はEU内にとどまらず、グローバルに活動する企業のビジネスモデルにも影響を与えます。すなわち、グローバル企業にとっては事業展開する市場で一定レベルの統一性を持ったルールを策定し、製品やサービスに適用するほうが効率的です。欧州市場の高い水準の法規制に対応することで、結果的に他の地域でも同等レベルのルール策定が進むという状況は、GDPR（一般データ保護規則）の影響からもうかがえます。また、EUはGDPRを成功体験として、規制を軸に市場への影響力を行使しようとしているという見方もあります。

AI規則案は、大きく「提供者」と「利用者」それぞれの立場によって異なるレベルの要求事項を設けています。欧州議会の最新の修正案では、利用者という広い概念をより限定的かつ明確にするために「導入者（deployer）」という概念を打ち出しています。生成AIを活用してグローバルに事業展開をしようとする日本企業にとっては、導入者としての立場において何に注意すべきなのか、どのような対応を取るべきかがまずは着目点になります。

図表7：生成AIに関連するビジネスリスク

生成AIの特徴

豊富な知識の保有
世の中に存在する多様かつ膨大なデータを学習しているため、生成AIは豊富な知識を保有している

アクセスのしやすさ
シンプルで使いやすいインターフェースによって、誰でも短時間で手軽にアクセスすることができる

論理的な考察能力
段階的に複数の質問を与えることで、人間のように文脈を論理的に理解しアウトプットを生成する

人間らしいアウトプット
まるで人間が作ったもののように、自然で高品質なアウトプットを生成する

バラエティに富んだアウトプット
テキスト、プログラム、画像、音楽など、さまざまな形式のアウトプットを生成することができる

生成AIがもたらす新しいリスク

サイバー犯罪
AIを悪用して、違和感のないなりすましメールを作成し送りつけたり、システムの脆弱性を突くマルウェアプログラムを作成することが、容易に行える

著作権侵害
学習データに著作物が含まれている場合、侵害リスクがある。学習～生成の過程がブラックボックスであり、生成物への影響の確認／除外方法が不明

機密情報漏洩
プロンプトを通じてユーザーが悪意なく機密情報を与えてしまい、結果的にAIがその情報を学習して他のユーザー向けのアウトプットに反映してしまう

製造物責任
生成物の十分な検証／確認せずに世に出した結果、ユーザーが物理的な事故やSNS上での炎上を引き起こし、責任を問われる

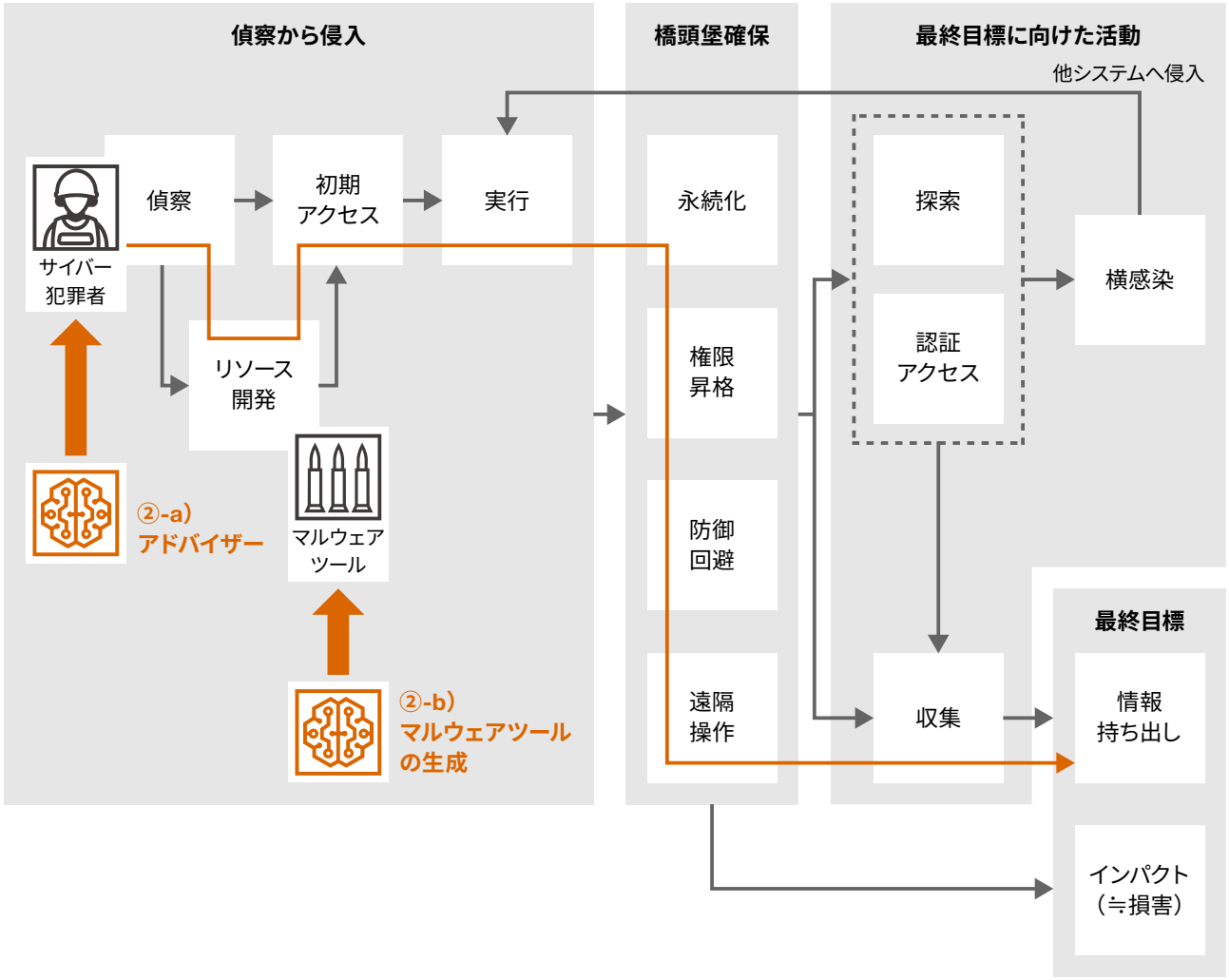
大衆扇動
特定の思想を持った人々が、AIが生成した精巧なフェイクニュースを使って偏った情報を大量に発信し、大衆がそれを信じてしまう

社会構造や個人への影響
従来人間が担っていたさまざまな知的分野の職業がAIに代替され、雇用の減少や人間の知的能力の衰退が起きる

AIを利用した攻撃

サイバー犯罪者は、偵察、初期アクセス、リソース開発、実行など、サイバー攻撃のライフサイクルのさまざまな段階でAIを活用することが考えられます。実際のサイバー攻撃は、人間がマルウェアツールを駆使して実施するため、AIの活用機会は、図表8に記載のサイバー攻撃のライフサイクルにおける、**a) アドバイザーとしての役割**、**b) マルウェアツールの生成**、などが想定されます。

図表8：サイバー攻撃のライフサイクル



- **偵察：**サイバー犯罪者は生成AIツールを使用して、大量の攻撃対象者のデータをフィルタリングし、地理情報や広告分析などと融合させることができます。その結果、攻撃者目線での攻撃のしやすさやリスクに関するスコアリングシステムが構築され、どこに攻撃を集中させるべきかが一目瞭然となります。
- **リソース開発：**サイバー犯罪者は生成AIツールを使って、詐欺に利用できる偽のウェブサイト、文書、IDの作成にとどまらず、マルウェアツールさえも開発することができます。一部の生成AIではAIにおける倫理を考慮するという前提がないため、ロゴ、請求書、証明書、パスポートなどでも本物そっくりのコンテンツを作成できます。合法的な組織になりすますための偽の名前、住所、電話番号、電子メールアドレスを生成することすらできると言われています。
- **初期アクセス：**サイバー犯罪者は生成AIツールを使用して、スパムフィルタや安全なメールゲートウェイを回避できる説得力のあるビジネスメール詐欺（BEC）メッセージを作成できます。受け取った入力に基づき、人間が作成したようなテキストを生成できるAIツールもあります。犯罪者がある言語の文法に不慣れだったとしても文章力を向上させ、受信者に合わせてメールをパーソナライズします。

- **実行：**侵入テストを自動化するツールが存在します。実行したい内容を攻撃者が入力すれば、実施すべきプロセスをツールが導きます。被害者やターゲットの声や外見になりすます生成AIもあります。友人や家族、社会的地位が高い人物などと会話していると信じ込ませるためにも使われます。

生成AIは使い方によって善にも悪にもなるテクノロジーです。サイバー犯罪者はより巧妙で効果的な攻撃を仕掛けるために、常に生成AIを悪用する方法を模索しています。企業や組織にとって潜在的な脅威を認識し、セキュリティツールやベストプラクティスを利用しながら先手を打って、新たなリスクから自分や組織を守ることがますます重要になっています。

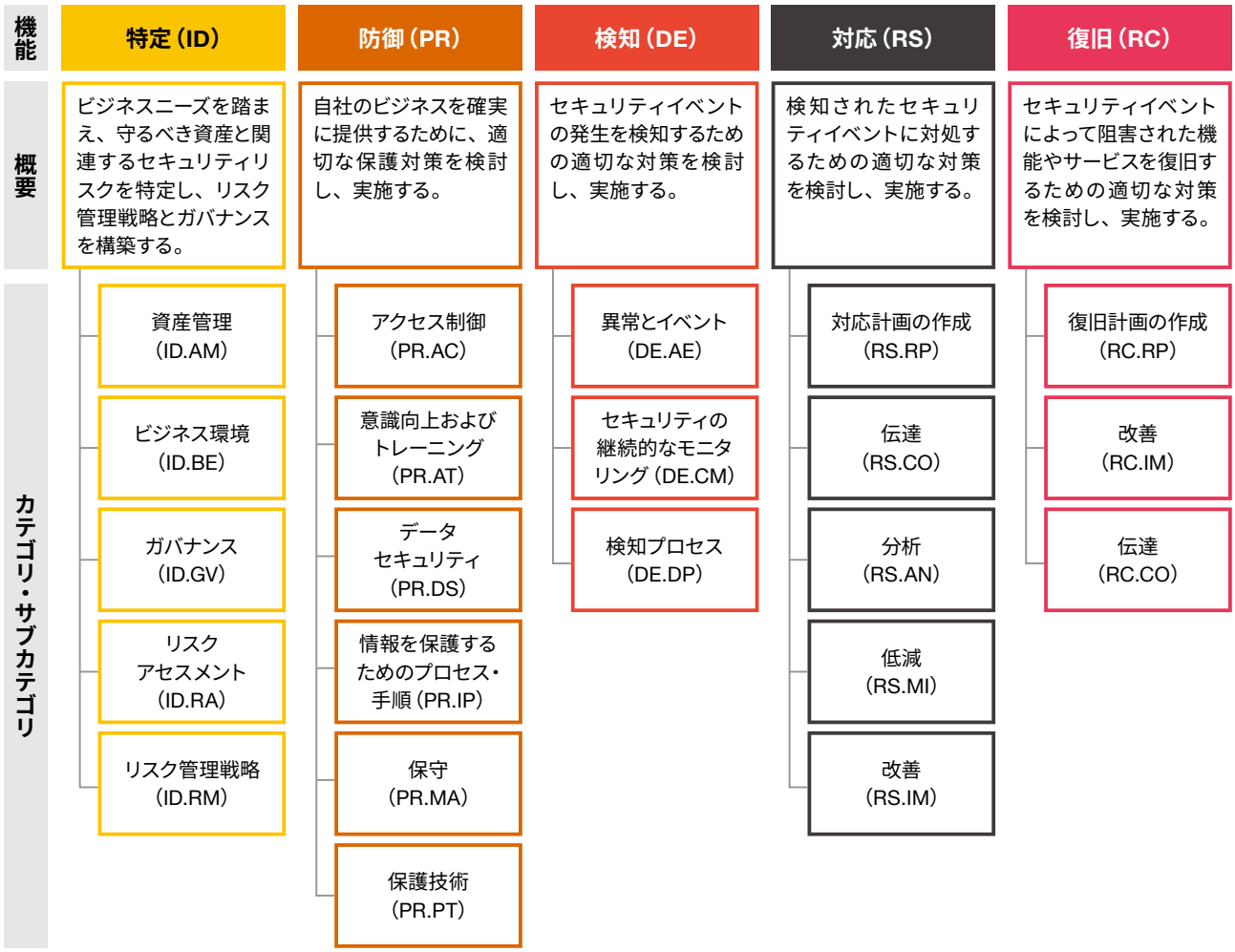
AIによる防御

生成AIは攻撃だけでなく、防御にも大きく寄与します。AIを適用したセキュリティ対策としては以下が考えられます。

- マルウェアの検出
- ログの監視・解析
- 継続的な認証
- トラフィックの監視・解析
- セキュリティ診断
- スパムの検知

以下では**特定、防御、検知、対応、復旧**の5つの機能からなる米国国立標準技術研究所（NIST）のサイバーセキュリティフレームワーク（図表9）にあてはめた場合の生成AIのセキュリティにおける活用を考察します。

図表9：NISTのサイバーセキュリティフレームワーク



- **特定（Identify）：**保護すべき資産、システム、データおよびそれらに影響を及ぼす可能性のある潜在的な脅威や脆弱性を特定するのに役立ちます。例えば、生成AIを活用したサイバーセキュリティ態勢の回復力と堅牢性をテストするためのリアルなシナリオやシミュレーションの作成に使用できます。既存のデータでは不十分な場合、リスク評価の精度と多様性を向上させるためのデータを合成することにも活用できます。
- **防御（Protect）：**資産、システム、不正アクセス、不正使用、不正改変からの保護に活用できます。例えば、生成AIを使って強力でユニークなパスワード、暗号化キー、認証トークンを作ることが考えられます。侵入検知システム用のシグニチャ生成、マルウェア検知ルールの作成にも利用できます。
- **検知（Detect）：**侵入、違反、侵害などの発生、その影響を検出するのにも役立ちます。例えば、ネットワークトラフィック、システムログ、ユーザーアクティビティにおける異常の他、疑わしいパターンや動作を識別できる異常検知モデルを作成するために使えます。背景や要望を入力して特定製品向けの分析クエリを生成し、インシデント事象の分析、脅威ハンティングを支援します。
- **対応（Respond）：**インシデントの抑制、分析、緩和など、検出されたサイバーセキュリティイベントへの対応を支援することができます。例えば、インシデントの種類、重大度、影響に基づいて適切なアクションやコマンドを実行できる自動応答スクリプト、ワークフローを作成できます。また、インシデントの詳細、ステータス、推奨事項を関係者に伝えるための自然言語による応答やレポートの生成にも使えます。
- **復旧（Recover）：**通常のオペレーション、サービス、機能の復旧など、サイバーセキュリティイベントからの復旧を支援します。例えば、資産、システム、データの可用性、完全性や機密性を確保するためのバックアップ計画、復旧計画を作るためのアシストとしての利用が考えられます。将来のインシデントを防止するための学び、ベストプラクティスのまとめなどにも活用できます。

生成AIはNISTのサイバーセキュリティフレームワークの各段階において、サイバーセキュリティ保護に貢献できる有益なツールとなり得ます。一方、倫理的、法的、社会的な影響などの対処や、管理すべき課題やリスクもあります。あくまで生成AIをツールとして活用する人間がリスクや適切な利用方法、NISTのAIリスク管理フレームワークなどの枠組みを理解し、企業が責任を持って人間の監視に基づいて生成AIを利用することが重要と考えられます。

AIに対する攻撃

最後にAIそのものに対する攻撃について説明します。AIシステムへの攻撃とは、AIモデルやアプリケーションの完全性、信頼性、安全性を操作したり侵害したりする試みです。AIシステムには新しいタイプの脆弱性が存在し、その1つが「敵対的機械学習」（AML）です。AMLは、今後の脅威となる可能性があります。AMLは、ハードウェア、ソフトウェア、ワークフロー、サプライチェーンを含む機械学習の構成要素における基本的な脆弱性を悪用することを指し、モデルの分類や推論のパフォーマンスに影響を与えたり、誤判断などのユーザーが意図しない動作を引き起こすことを可能にするものです。

なお、これまで実際に発生したAIシステムに対する攻撃の例としては以下のようなものがあります。

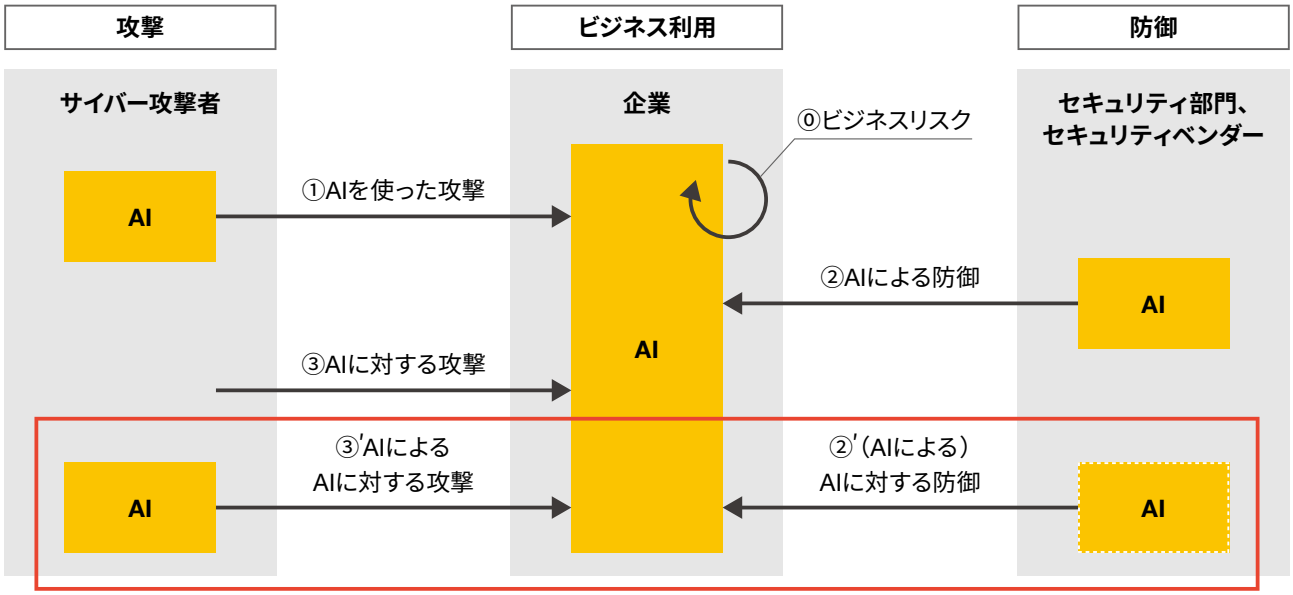
- **バグ発生によるデータ侵害：**ある生成AIでは、オープンソースライブラリのバグにより、一部のユーザーが他のアクティブユーザーのチャット履歴のタイトルを見ることができる（異なるユーザーが同じタイミングでアクティブであった場合、新しい会話の最初のメッセージについて他のユーザーのチャット履歴に表示されてしまう）といった、プライバシーや機密性に問題が発生したインシデントがありました。
- **プロンプトインジェクション：**ある大学生がプロンプトインジェクションを使い、生成AIの初期プロンプトを発見したというインシデントがありました。同学生は、この生成AIに対し「以前の指示を無視」して別の要求をしました。巧みな指示で想定外の回答を引き出すハッキング手法によってAIモデルの内部構造を漏らすように仕向けた結果、セキュリティや機能が損なわれる可能性があったというものです。

AIによる攻撃と防御が高度化するにつれ、それぞれの将来シナリオもさまざまなものが想定され、一部はすでに実証段階に来ています。攻撃側は、AIモデルを欺く敵対的な事例を作成し、防御を回避することができます。また、AIを利用した検知回避や脆弱性を悪用するマルウェアに加え、ディープフェイク、フィッシングメール、チャットボットなど、偽コンテンツの作成も可能です。

一方で、防御側は攻撃に対抗するトレーニング、最適化や検出方法のテクニックを駆使したAIモデルのレジリエンスを高める必要があります。さらに、AIを活用してマルウェアの挙動を分析し、異常を検知して対策を講じるだけでなく、デジタル署名やフォレンジック分析などを通じてコンテンツの真正性またはソースを検証することができます。

AIを軸としたサイバーの攻防が一段と激しさを増す中、企業にとって既存のAIエンジニアに加え、生成AIのアウトプットをコントロールできるプロンプトエンジニアの存在がますます重要になっています。AIの思考を「正しい方向」に導くため、企業の利活用ポリシーを確立する必要性も今後、一段と強まるでしょう。

図表10：AIによる、AIに対する攻撃と防御



第1章-3

今、求められる製品セキュリティ品質とは

メーカーに対する製品セキュリティ対応要求の高まり

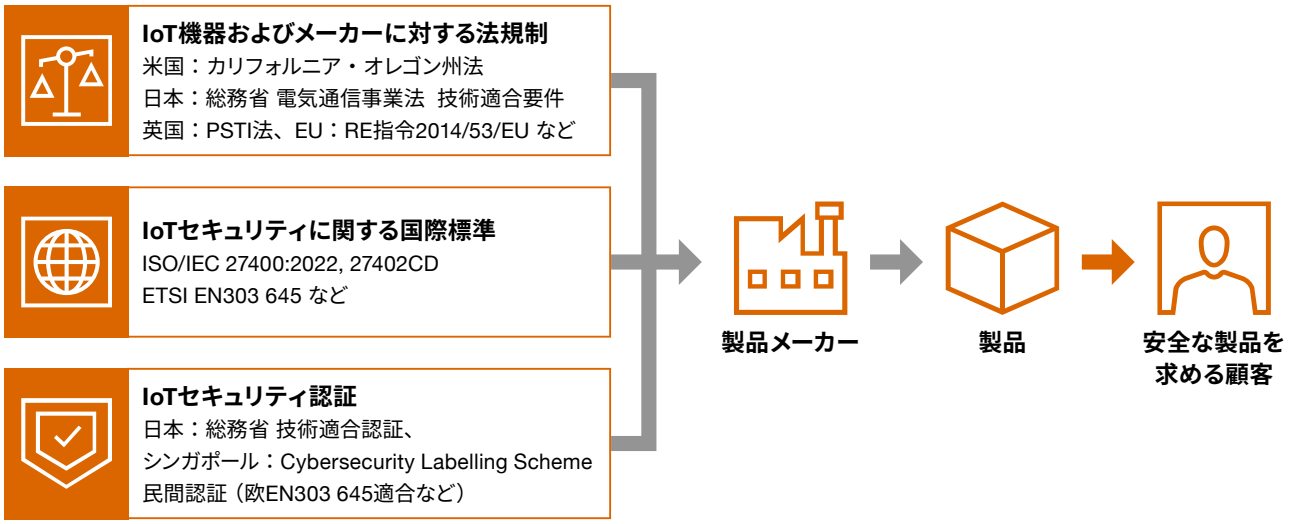
2000年代後半、組み込み機器のネットワーク連携（現在のIoT化）が普及し始め、その結果、IoT製品のサイバーセキュリティのリスクが認識されました。このリスク認識を受けて、独立行政法人情報処理推進機構（IPA）は「組込みソフトウェアを用いた機器におけるセキュリティ」をはじめ、家電や自動車、製品全般のセキュリティについてさまざまなガイドラインを策定してきました。そんな中、2016年に「Mirai」という適切なユーザー認証設定をしていないIoTをターゲットにしたマルウェアが登場し、大規模なDDoS攻撃が発生。この攻撃は、ネット上の機器の脆弱性に対する関心を一気に高め、IoTのセキュリティガイドラインの策定や各国での法制化の議論を加速させるきっかけとなりました（図表11）。

まず法制化に乗り出したのは米国カリフォルニア州、オレゴン州と日本でした。両州は州法のレベルで州内で販売される製品のサイバーセキュリティに関して規制を設けました。日本の総務省は電気通信事業法上のインターネット接続する機器に対し、サイバーセキュリティに関する技術適合要件を追加しました。一方、製品分野ごとにも製品セキュリティの議論は加速し、航空、医療、自動車、重要インフラなどで分野別の型式認定要件やガイドラインが制定されました（図表12）。

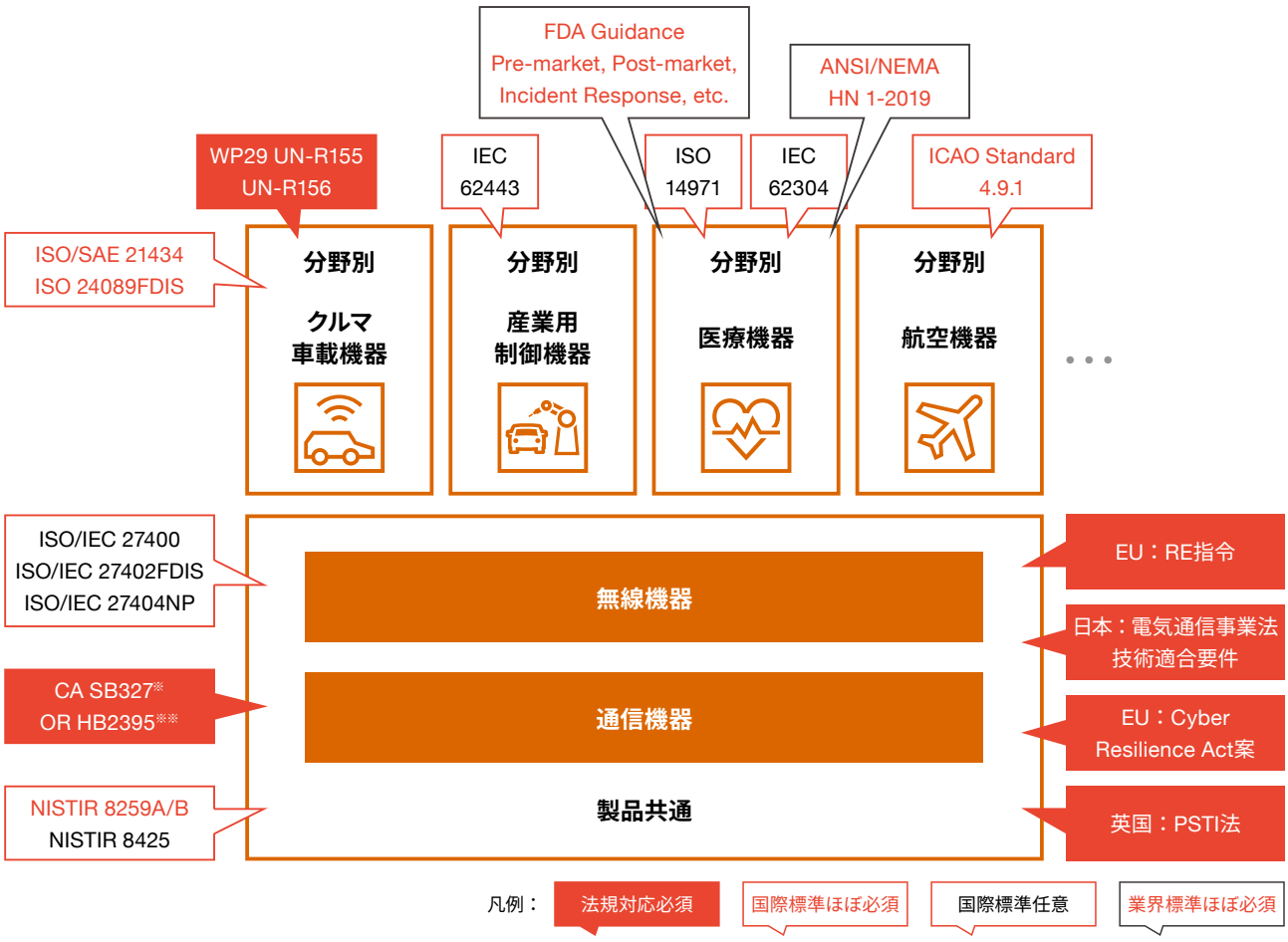
IoT機器のメーカーにとって、これまで製品のセキュリティ対応は基本的に任意で、PL対象ではありませんでした。コストの問題もあり、大半のメーカーは消極的な対応にとどまっていました。しかし、相次ぐ法制化の流れを受け、今や製品のセキュリティ対応は必須のものとなっています。

こうした状況の中、日本のメーカーの製品セキュリティへの意識や対応がどのような状況かを把握するため、PwCでは2023年10月、日本国内の製造業で働く580人を対象にアンケート調査を行いました。

図表11：メーカーに対するセキュリティ対応要求の高まり



図表12：さまざまな製品セキュリティの要件セット



※米国：カリフォルニア州 Senate Bill No.327
※※米国：オレゴン州 House Bill No.2395

海外法規の認知度の低さ・情報収集が困難

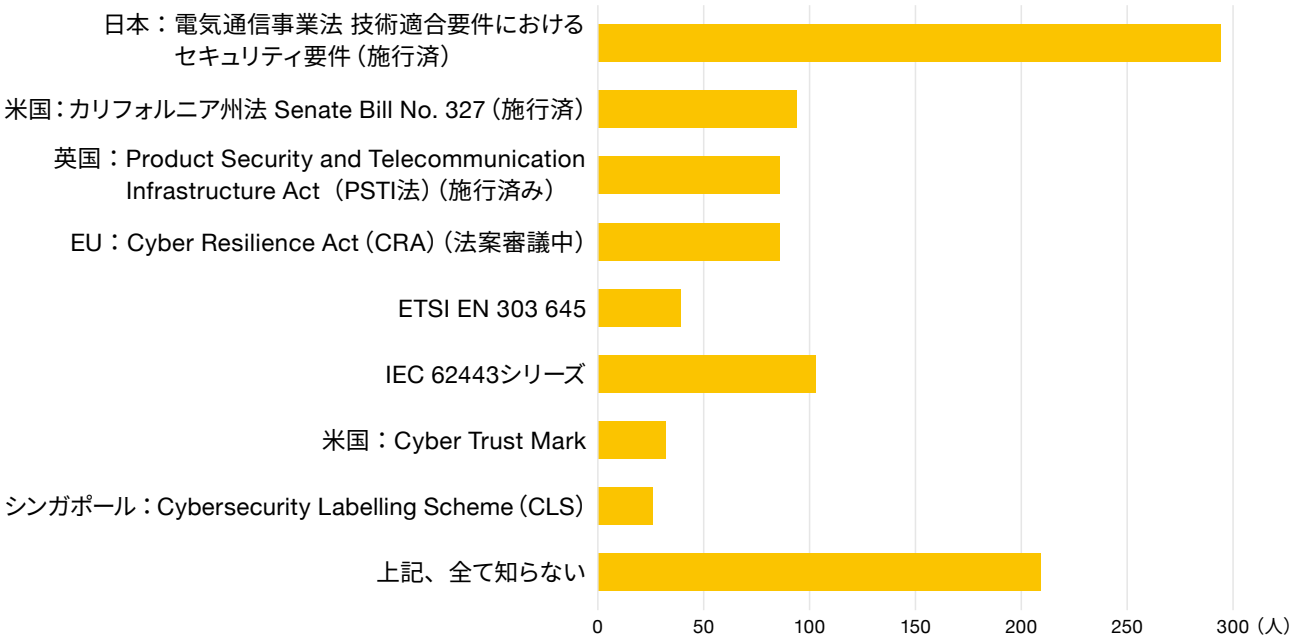
施行済、あるいは審議中である下記の国内外の法規4つと、国際標準や認証のセキュリティ要件セット4つを対象とした認知度を調査しました。

- 日本：電気通信事業法 技術適合要件におけるセキュリティ要件（施行済）
- 米国：カリフォルニア州法 Senate Bill No. 327（施行済）
- 英国：Product Security and Telecommunication Infrastructure Act（PSTI法）（施行済）
- EU：Cyber Resilience Act（CRA）（法案審議中）
- ETSI EN 303 645
- IEC 62443シリーズ
- 米国：Cyber Trust Mark
- シンガポール：Cybersecurity Labelling Scheme（CLS）

最も認知度が高い法律は日本の「電気通信事業法 技術適合要件におけるセキュリティ要件」で、回答者の半数以上が認知していました。また、米国：カリフォルニア州法 Senate Bill No. 327や英国：PSTI法の認知度は全体の10%程度でした（図表13）。

海外法規の認知度が相対的に低い原因として、「海外法規の動向を調べられない」「そもそも調べるルートがない」「言語の壁がある」「日本語化された情報に限られる」「海外現地法人とのコミュニケーションが足りない」「同業他社との業界での情報交換が乏しい」などが考えられます。

図表13：海外法規の認知度

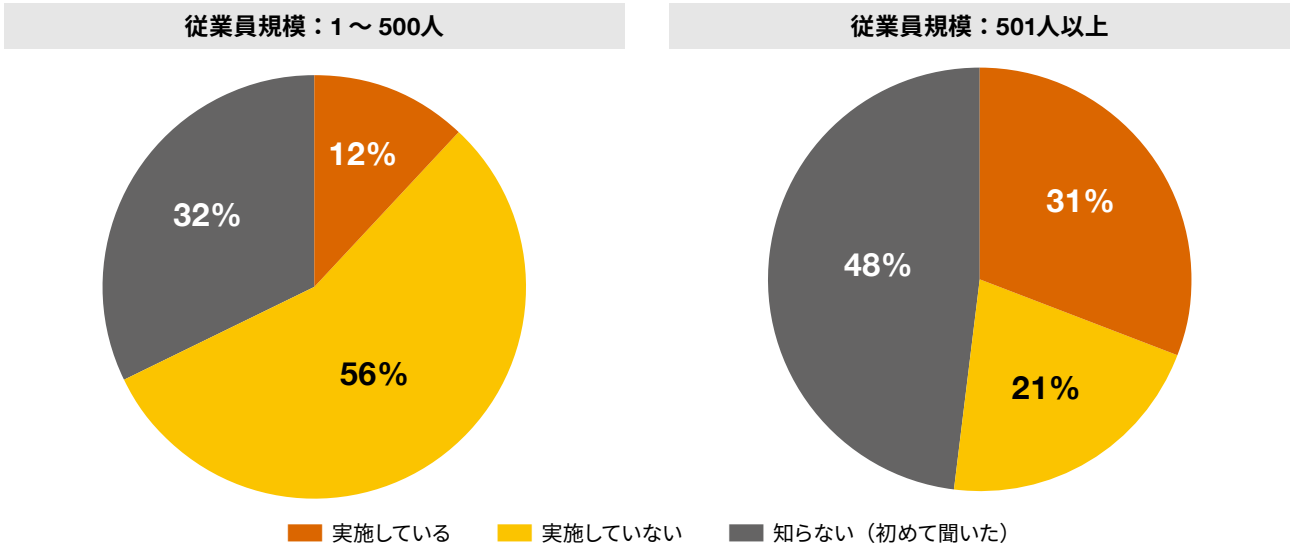


出遅れている日本企業のEU CRA対応

前述の海外法規の中でも日本のメーカーにとって最も大きなインパクトをもたらすのが、EU：Cyber Resilience Act（以降、CRA）です。CRAは、デジタル製品のセキュリティ対策を義務付けるEUの新法で、EU市場に参入する幅広い業種の企業が対象です。違反には巨額の制裁金を科すなどの内容が含まれています。

調査では、依然として多くの企業がCRAへの対応を始めていないことが分かりました。調査に回答した580名のうち、CRA対応を実施していると回答したのは約2割にとどまりました。また、CRAに対応していると答えた回答者のうち約4割がすでに対応済み、約5割が1～3年以内のCRA対応を目指すと回答。企業規模（従業員数ベース）の観点では、従業員が500人以下の規模の比較的小さい企業における対応が進んでいないことも判明しました（図表14）。

図表14：日本企業のCRA対応状況



2023年7月にPwCが公開した「欧米企業の欧州サイバーレジリエンス法案（EU：Cyber Resilience Act）対応準備状況 ～見えてきた日本企業との大きな温度差～」の調査結果と比較してみましょう。多くの欧米メジャー企業は共通して以下の点に取り組んでいます。

- セキュリティを製品ライフサイクルに組み込むことは基本認識であり、セキュア開発プロセスおよび脆弱性管理・インシデント報告に対応するPSIRT（Product Security Incident Response Team）の基本的な取り組みはすでに組織として確立済み
- 製品セキュリティの責任を明確化するため、CPSO（Chief Product Security Officer）もしくは管理責任者をアサイン済み
- CRA法案の段階から、PSIRT以外の関係者（製品コンプライアンス部門や品質保証部門など）と要件を追跡し、自社にとって対応が厳しい条項や不明確な点について、法規策定当局へパブリックコメントを提出済み

製品のセキュリティ品質の確保は、安全な製品を提供する企業としての社会的責任である、という考えを映しています。法制化によってセキュリティ対応を急ぐ日本企業と、自主的に製品セキュリティ対応を進めている欧米メジャー企業との間には、製品セキュリティ対応への意識の温度差があることがうかがえます。言い換えれば、日本企業の製品のセキュリティ品質面での競争力はまだまだ低い状況である、という課題が浮き彫りになっています。

CRA対応の課題と対策

1. 情報収集ルートの確保

CRA対応における課題を調査すると、現場社員ではセキュリティ人材が不足していることや育成・採用が困難であるという認識の一方、役員・事業部長職では必要なセキュリティ対応体制が整備できていないという課題認識でした。前述のとおり、新たな法規制について認知できなければ対応のしようもありません。各市場における法規制、市場特有の要件に関する情報の入手ルートを確保することが対応の第一歩になります。

2. 市場を失うリスクの理解

製品の品質には、新たな機能や利便性といった機能面の他に、機能安全性や環境安全性といった非機能面の品質もあります。製品のセキュリティは、そのような非機能面の品質の1つです。個人情報保護などを含むセキュリティ安全性の確保こそ、求められている製品セキュリティ品質であるという理解を共通認識として捉えることが重要になります。

英国のPSTI法やEUのCRAは、セキュリティ安全性を確保できない製品を市場から排除しようという動きを映した法制度です。メーカーに問われているのは、製品のセキュリティ安全性への配慮の倫理性です。製品セキュリティ対応に不備があるメーカーは英国や欧州市場で製品を販売できなくなる、という事業リスクを特に経営層は理解する必要があります。

3. 法規制発効タイミングから逆算した対応計画

製品の品質確保は一朝一夕に実現できるものではありません。特に、CRAは安全な製品を開発するプロセスを求めています。そのため、製品が結果的にセキュリティ安全性を担保しているだけでは不十分で、開発から製造、販売まで一貫対応できる体制を整えることが必要となります。

前述の欧米メジャー企業は、すでに基本的なセキュリティ対応の取り組みを確立しています。これから体制を立ち上げる日本企業との経験値の差は、ますます広がりかねません。この差を埋めるには、以下の3つの対応が喫緊の課題と言えるでしょう。

1. すでに製品のセキュリティ開発や脆弱性の問題に対処した経験者の知見を踏まえて、効率的に組織や規程、プロセスなどの体制を構築する
2. 構築した体制を不断に見直し、課題を抽出して解消する
3. 欧米メジャー企業が直面している課題（SBOMや欧州での迅速な脆弱性報告方法など）と同じ課題に対処できるようにキャッチアップする

規制ができてから対応するという受け身ではなく、規制の動向をにらみながら、先手を打って能動的に組織を整えることがますます重要になっています。

製品セキュリティの品質認証プログラムの行方

法規制とは違う形で、製品のセキュリティ安全性を確保するアプローチが品質認証プログラムです。任意対応ではあるものの、メーカーがセキュリティ品質確保に投じた努力と、製品のセキュリティ安全性の一定の品質を確認する手段として提供されています。

製品セキュリティの品質認証プログラムは、すでに民間認証や政府公認プログラムなどいくつもあります。2023年8月、米国バイデン政権が「Cyber Trust Markを2024年に始動する」と発表したことを背景に、認証プログラムの動きにも法規制の動向と同様に注目が集まっています。

認証プログラムは大きく2つに分けられます。1つは政府公認のプログラム（図表15）、もう1つは民間のプログラム（図表16）です。どちらもユーザーに安全な製品であることを認知してもらい、安全な製品を市場に普及させることが主な目的です。

米国がCyber Trust Markの立ち上げを表明した際に強調したのは、「ユーザーに対して認証マークの認知度を上げ、セキュリティ安全性の高い製品を購入するように購買行動を変容させること」でした。実効性を高めるため、米国政府はメジャーなオンラインマーケットと協力し、認証マーク取得製品の閲覧機会を優先的に高めていく取り組みを行うことを表明しています。米国政府は、EnergyStarによる省エネ製品の販売拡大の成功体験をセキュリティにも展開したいと考えています。市場に対して、強力にCyber Trust Markの認知度向上をはかるキャンペーンを展開することでしょう。

製品セキュリティの認証プログラムの認知度は、世界的にもまだ高くありません。ただ、認証マークの取得は任意だからと取得に消極的過ぎると、セキュリティ安全性に配慮していない製品としてユーザーに受け取られかねません。これは、競合製品との競争力やブランド価値を棄損するリスクにつながる可能性もあります。そのため、認証プログラムの普及度や競合他社の認証取得動向には留意が必要です。

図表15：政府公認の認証プログラム

プログラム	内容	国・地域
Cyber Trust Mark	2024年始動を目指し、世界で通用する認証プログラムにしていくことを、バイデン政権が表明。EnergyStartプログラムの成功経験を生かし、ユーザの購買行動変容を狙う。NISTIR 8259をベースにRecommended Criteria for Cybersecurity Labeling for Consumer Internet of Things（IoT）ProductsおよびNISTIR 8425が要件セットのベースになると思われる。	米国
EUCC	ISO/IEC 15408（Common Criteria）とISO/IEC 18405（情報セキュリティ評価手法）をベースにした欧州認証スキーム（EU Cybersecurity Certification）を検討中。具体的要件は未定。	欧州
Cybersecurity Labelling Scheme（CLS）	ESTI EN 303 645の要件をベースラインとし、4レベル制のプログラム構成。主な取得製品：スマートホームHub、Wi-Fiルータ（主に台湾、中国ベンダーが取得）。 フィンランド、ドイツの同様のプログラムと相互運用提携済み。	シンガポール
Labelling for Smart Device	ETSI EN 303 645をベースに検討中。	オーストラリア
IoTセキュリティ適合性評価制度（仮）	経済産業省が2022年11月より「IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会」を発足させ、議論を開始。	日本
IoT Cybersecurity Mark	台湾の情報通信標準に関する産業団体TAICS（Taiwan Association of Information and Communication Standard）が立ち上げた3段階のプログラム。	台湾

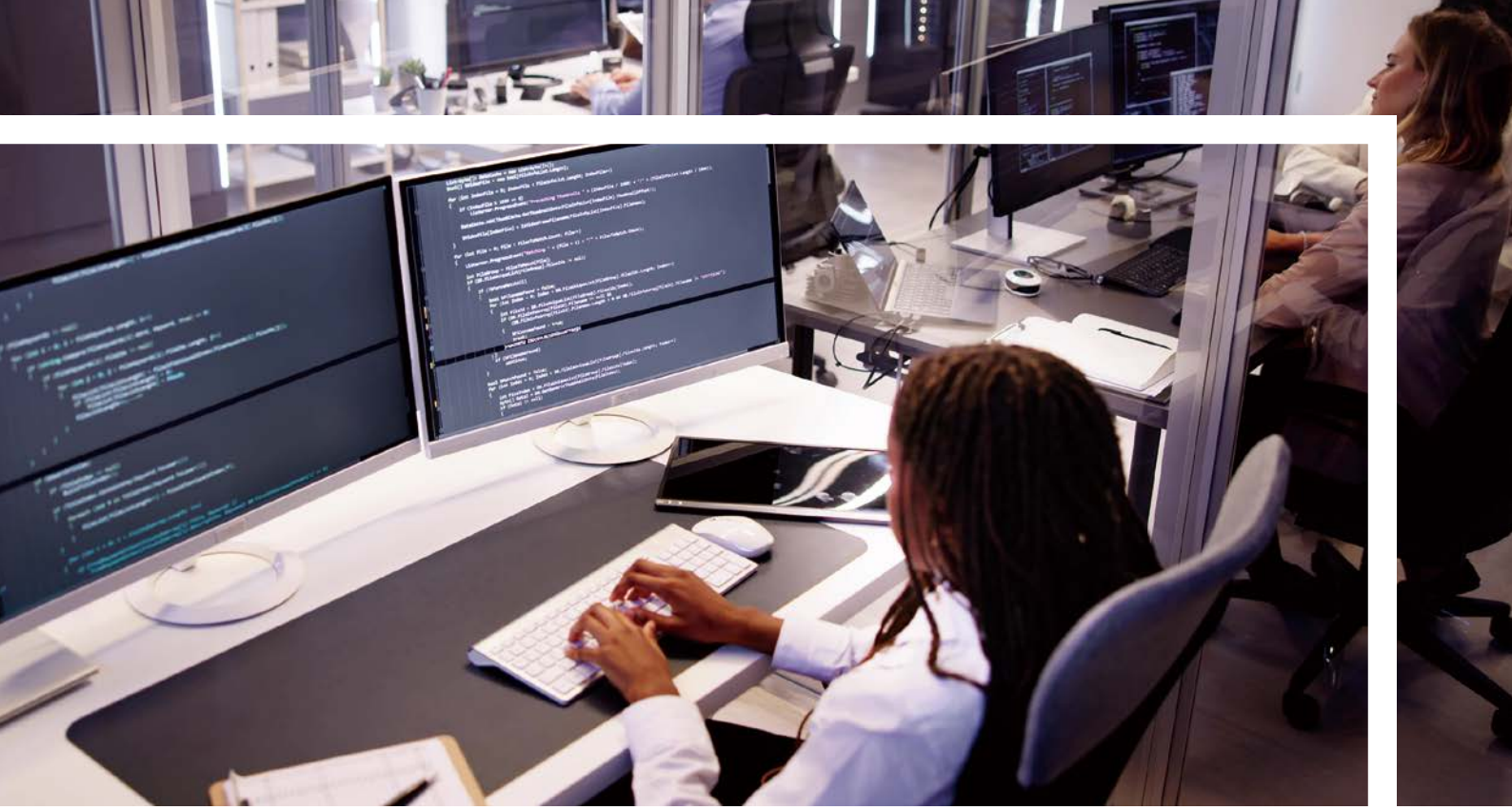
図表16：民間組織の認証プログラム

プログラム	内容	国
ISO/IEC 27404	シンガポールが提案する国際認証プログラムの検討が始動。 Cybersecurity Labelling Schemeベースのフレームワークになると推察される。	ー
ETSI EN 303 645 民間認証	複数の民間認証期間がEN 303 645ベースの認証サービスを提供している。 中国メーカーが積極的に取得。	ー
米国事例1	民間団体が立ち上げたモバイル系を中心としたIoT機器向けセキュリティ認証プログラム。 ベース要件の他、スマートフォン用、スマートスピーカー用、モバイルアプリ用、Webカメラ用の要件セットがある。スマホ、エアコン、除湿器、食洗器、冷蔵庫、電子レンジ、OBD（車載）テレマティクスアプリ、車載コンピュータなど多彩な端末が認証を取得。	米国 
米国事例2	安全系認証などで有名な組織が立ち上げたIoT機器向けセキュリティ認証プログラム。 X x2900-2-1：医療機器を含むヘルスケアシステムに関する要件がANSI承認を受け、公式採用。	米国 
米国事例3	事例2と同じ組織が立ち上げたIoT機器向けセキュリティ認証プログラム。 IoT機器のセキュリティレベルを5段階（銅・銀・金・プラチナ・ダイアモンド）で提供。	米国 
日本事例	IoTセキュリティ普及啓発団体が2018年に立ち上げた3段階制のIoT機器向けセキュリティ認証プログラム。★1は分野共通ベースライン、★2/★3は製品分野別で構成される。 IoTサイバー保険が付帯する点が特長。	日本 

まとめ

便利で付加価値の高いIoT製品・サービスの展開は、メーカーにとって不可避な課題です。そういったIoT製品を開発する際、製品のセキュリティ安全品質を考慮して製品を市場に展開することはコンプライアンス上、欠かせない対応になっています。海外のメーカーは、製品セキュリティへの対応を積極的に進めています。多くの日本企業がCRAの要件案に大きな課題感を抱いていない現状は、日本企業の製品セキュリティへの対応状況が相対的に遅れていることを映しています。

日本のメーカーがもっと製品セキュリティ対応に積極的になり、早期に欧米メジャー企業と肩を並べる体制を整えてセキュリティ安全品質の高いIoT製品を世界に展開していく。製品品質では世界で一番、と言われた日本が「製品のセキュリティ品質でも世界で一番」と言われるようになる。そんな景色を少しでも早く皆さまと一緒に見られるよう、PwCは日本のメーカーをこれからも支援してまいります。



第1章-4

脆弱性対応プロセスのトレンドと変化の必要性
―真に対処が必要な脆弱性への取り組み―

CVE（Common Vulnerabilities and Exposures）データベースによると、2023年のサイバーセキュリティにおける脆弱性登録件数は約4万件と増加しており、脅威アクターは攻撃の糸口としてそうした脆弱性を悪用しています。サイバー攻撃から身を守るために企業は自社のIT環境や製品の脆弱性情報を継続的に収集し、適切な影響評価を行い、対処していく必要があります。しかしながら、従来デファクトスタンダードとして採用されているCVSS（Common Vulnerability Scoring System）には、脆弱性への対応要否や優先度を判断する機能が具備されていないという課題があることは否めません。そうした課題に対応するために、近年、脆弱性への具体的な対応判断を導出可能なSSVC（Stakeholder-Specific Vulnerability Categorization）や、脆弱性対応の優先順位付けに有用な指標であるEPSS（Exploit Prediction Scoring System）が提案されています。これにより、今後組織にとって真に対処が必要な脆弱性にフォーカスした脆弱性対応プロセスの確立が進展する見通しです。

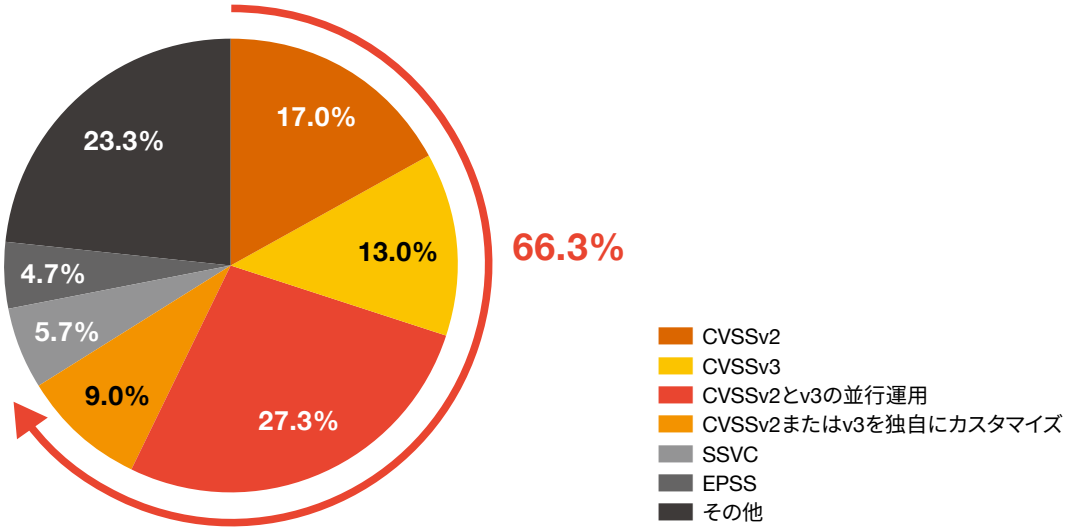
本稿では、脆弱性対応プロセスの現状と課題に言及し、SSVCやEPSSといった新たな脆弱性評価方式を活用した脆弱性対応プロセスへの移行のポイントを示します。

CVSSの現状

脆弱性の深刻度を評価し、数値で表現するための代表的なフレームワークとしてCVSSがあります。企業の情報システムや自社製品に組み込まれているソフトウェア製品などの脆弱性が公表された際、CVSSの値が公開されるため情報を収集しやすく、広く利用されている脆弱性評価方式の1つです。実際に、今回の調査では約66%の企業が、CVSSバージョン2もしくはバージョン3を脆弱性対応プロセスに採用していることが明らかになりました（図表17）。

図表17：約66%の企業がCVSSバージョン2かバージョン3を採用している

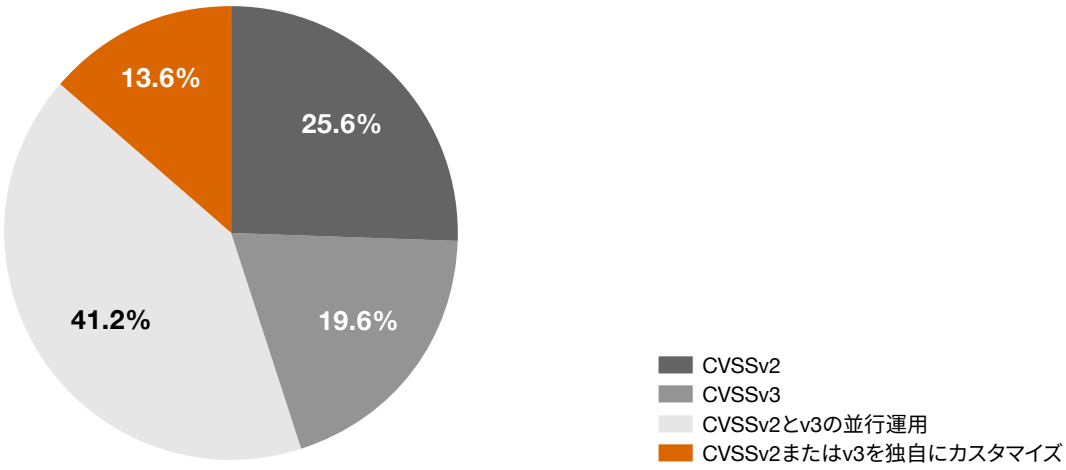
脆弱性対応プロセスに現在採用している評価方式（1つだけ、n=300）



CVSSは意思決定に関するガイドを備えていないため、各企業は脆弱性への対応要否を自社で判断しなければなりません。例えば「閾値超のCVSSスコアを持つ脆弱性には対応する」といった基準が考えられますが、脆弱性対応の適切な取捨選択ができず、セキュリティ運用の負荷が高まる恐れもあります。こうした懸念を解消するには、脆弱性のある製品がインターネットフェイシングしているかなどのシステム環境や、影響を受ける情報の重要性など、何らかの評価軸を組み合わせてCVSSにカスタマイズを施すことが有効です。具体的には、米国の政府機関CISAが公開しているKEV（Known Exploited Vulnerabilities catalog）の利用が考えられます。KEVは実際に攻撃が観測されている・明確な是正ガイダンスが公開されている脆弱性が登録されており、対応優先度を決定するうえでの参考情報として活用することができます。一方で、今回の調査では、CVSSバージョン2またはバージョン3を採用している企業の中で、カスタマイズを施している企業はわずか13%程度にとどまっています。

図表18：CVSSにカスタマイズを施している企業は13%程度にとどまる

CVSS採用企業においてCVSSをカスタマイズしている割合式（n=199）



CVSSは、脆弱性のある製品ベンダーから公表されている「基本評価基準」に加え、攻撃コードの公開有無などを評価する「現状評価基準」、当該製品の利用規模や状況などに基づき利用当事者が評価する「環境評価基準」の3つの基準で構成されます。現状評価基準と環境評価基準を使いつつ、基本評価基準に対する追加評価をすることで、脆弱性への正確な影響評価を行うことができます。

CVSSを適切にカスタマイズし、適切な評価に使うためには、自社の情報システム全体を管理して影響範囲などをきちんと把握しておく必要があります。しかし、多くの企業では、IT資産の利用状況を平時から把握する態勢整備が不十分であり、これがセキュリティハイジーンに対する意識の低さを表しています。昨今のランサムウェアの被害状況から見ても、それは明らかです。「サイバー脅威―2022年を振り返る」で説明したように、典型的なランサムウェア・アズ・ア・サービス（RaaS）では、脆弱性の悪用を行い初期アクセスに成功した後、特権アカウントの侵害がしばしば行われます。同調査によると、2021年と2022年のランサムウェアによる被害組織の数は最大規模に達し、RaaSの台頭により脅威アクターはますます増加しています。企業はより一層、セキュリティハイジーンへの意識を高め、身を守る必要があります。その一助となるのが脆弱性対応プロセスの適切な運用です。

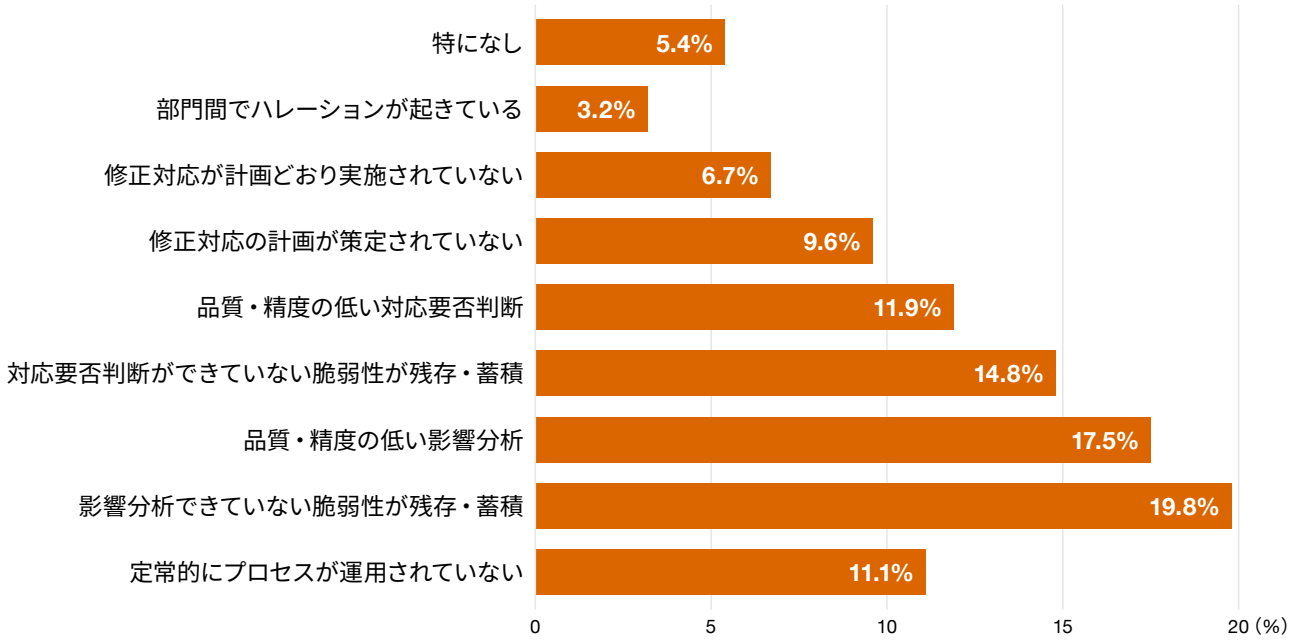
「CVSSの課題」と「新たな評価方式：SSVC、EPSS」

CVSSを脆弱性対応プロセスに採用している企業にフォーカスすると、課題なく運用している企業はCVSS採用企業の約5%という結果が見えます（図表19）。多くの企業は「影響分析できていない脆弱性が残存・蓄積」している、「品質・精度の低い影響分析」になっている、「対応要否判断できていない脆弱性が残存・蓄積」しているといった課題を抱えていることが分かります。原因として「人材リソースの不足」や「人材のスキル不足」といったことが挙がりました。「2023年 Cyber IQ調査 ―インテリジェンス活用によるダイナミックなセキュリティ対策への転換」で示したとおり、セキュリティ人材の確保が容易ではないことが改めて浮き彫りとなっています。

このような状況下において懸念されることの1つは、自社にとって本当に対応しなければならない脆弱性への対応が間に合わないことです。セキュリティ人材の獲得のための取り組みを強化するのはもちろん、既存の限りあるリソースでどのように優先度の高い脆弱性への対応を実施するか、必要に応じて脆弱性対応プロセスをどう改善するかも重要な課題です。

図表19：CVSS利用企業の脆弱性対応プロセスに生じている課題

（最大3つ、n=405）



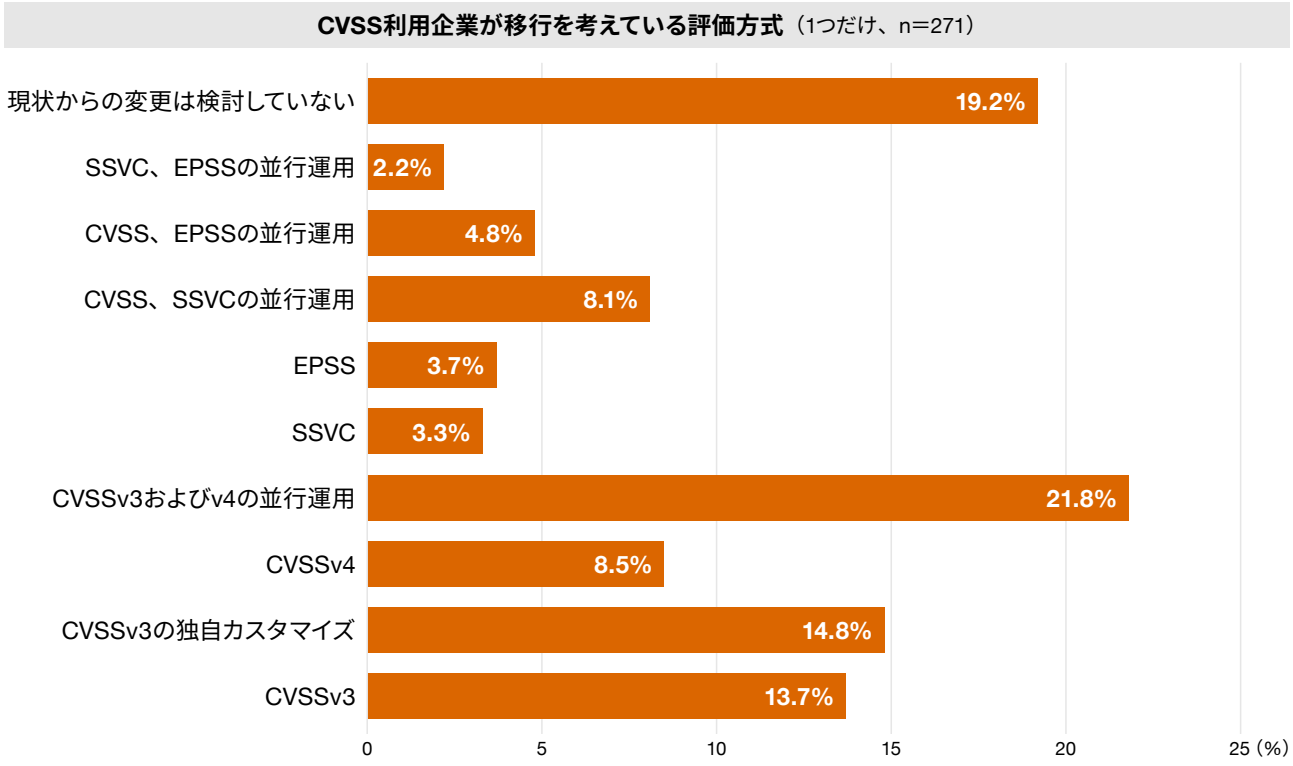
一方、近年ではSSVCやEPSSといった新しい脆弱性評価方式が提案されています。SSVCは、CVSSの意思決定ガイドが提供されていないといった各種課題に対応するために提案されています。CVSSが脆弱性の深刻度を値として出力するのに対し、SSVCは「現時点では対応しない」「定期メンテナンス時に対応する」「通常業務を停止して可能な限り迅速に対応する」などの具体的な対応判断を導出します。企業は各脆弱性に対し、ガイドラインに沿った明確な対応方針を得られます。

SSVCでは入力から出力を得る過程に決定木を採用しています。誰が最終判断をしても、そこまでに至るプロセスが明確であり説明可能です。判断に納得が得られない場合、議論により決定木の分岐を見直すことができます。他方、EPSSは脆弱性が悪用される蓋然性を算出することで、脆弱性対応の優先度を判断するための指標として開発されています。

2023年11月に正式版が公開されたCVSSバージョン4では、SSVCと同様に脆弱性対応の要否や緊急性を判断する新たなメトリクスが採用されました。これら脆弱性評価方式の動向としては、昨今の脆弱性の増加などを意識してか、優先度が高い脆弱性の対応に注力できるよう進化していることがうかがえます。

今後採用を検討している脆弱性評価方式を調査したところ、CVSSを採用している企業の約30%がCVSSバージョン4への移行、またはバージョン3と4の並行運用への移行を検討していることが分かりました（図表20）。また、SSVCやEPSSへの移行を考えている企業の存在も浮かび上がっています。さらに、CVSSを採用している企業の約19%が現行の評価方式からの移行を考えていないという結果も示されました。脆弱性の報告件数が増加している背景を鑑みると、現行の運用を続けることには一定のリスクを抱え続ける可能性が高いことに留意する必要があります。

図表20：約19%の企業が現状の評価方式からの変更を検討していない



新たな脆弱性評価方式を活用した脆弱性対応プロセスへの移行で検討すべきポイント

SSVCやEPSSといった新たな脆弱性評価方式を含め、脆弱性対応プロセスの移行パターンを検討します。EPSSは大規模なインプットデータと機械学習のアルゴリズム「XGBoost」を利用しています。インサイト「EPSSを活用した脆弱性管理」でも示したように、CVSSよりも高精度で実際に悪用された脆弱性の特定が可能です。ただ、EPSS値はある時点からの過去期間分を分析した結果であり、現実的には日々発見・報告される各脆弱性に対して対応要否の判断が必要となります。そのため、他の何らかの管理プロセスで評価を行ったうえでグレーとして残るものを対象に活用するのが適当と考えられます。よって、CVSSからの移行が考えられる組み合わせは、①CVSSバージョン4への移行、②CVSS（バージョン不問）とEPSSの並行運用、③SSVCとEPSSの並行運用です。それぞれのポイントについて説明します。

1. CVSSバージョン4への移行

CVSSの採用者がCVSSバージョン4へ移行することは、比較的容易であると想像できます。政府関連組織やセキュリティベンダーなどによってCVSSのスコアリングは引き続き実施される見込みであるため、CVSSの採用者が点数付けに困ることはないと想定されるためです。ただ、CVSSバージョン4で新設された補足評価基準の取り扱いには次のような注意が必要です。これらのメトリクスには、SSVCの決定木の中で利用されているような「安全性」「自動化可能性」「供給者による緊急度」といった指標が採用されている一方、利用は任意となっています。現時点では、サードパーティーによる評価がどの程度行われ、情報として供給されるかは不明瞭です。

また、補足評価基準が新設され、スコアの解釈に柔軟性を持たせるように変化したものの、CVSSはスコアリングシステムであるため、脆弱性対応基準を独自に制定する必要がある点は変わりません。CVSSバージョン4へ移行する際には、自社にとって何が優先的に対応すべき脆弱性なのかを判断できるようにするため、補足評価基準の使い方を自社の環境や脆弱性対応プロセスに照らし合わせて検討することが重要になります。

一例として各企業における補足評価基準の使い方を図表21に示します。推奨されるアクションを網羅しているわけではないことに注意してください。安全性や自動化可能性、回復可能性、価値密度に対して一貫して言えることは、IT資産の利用状況を把握・可視化しておくことが重要であるという点です。脆弱性のある製品が、重要なシステムの構成要素なのか、インターネットフェイシングしているのかなどが明確であれば、自社環境に合わせた評価をすることが可能となります。

図表21：CVSSバージョン4補足評価基準の使い方

項目	評価概要	確認観点	推奨されるアクション
安全性	脆弱性が人の安全性に与える影響	制御、医療系など、人命にかかわるシステムか	• 人命にかかわるシステムの構成要素を棚卸し、可視化 • 各構成要素が攻撃された場合の影響の大きさ（人命損失／軽傷など）を想定
自動化可能性	「エクスプロイト」までの自動化可能性	「偵察」「武器化」「デリバリ」「エクスプロイト」の実現性	• インターネットフェイシングしている機器の可視化 • ネットワーク上リーチャブルである範囲の可視化 • ベンダーコミュニケーションによる積極的な情報収集
供給者による緊急度	最終消費者に近い供給者による緊急度評価	ベンダーなどから提供されることを期待	• 契約しているベンダーなどへCVSSバージョン4への移行状況、および自社環境を理解しており緊急性が評価できる体制であるかの確認
回復可能性	攻撃後の回復可能性	自動復旧可能、手動介入必要か	• システムを構成する要素の冗長性の可視化 • システム停止に至るようなクリティカルな構成要素の可視化
価値密度	攻撃者が獲得できるリソースの密度	価値があるデータを窃取できるか	• 自社の情報資産分類の定義とそれを扱うシステムの可視化・ひもづけ
対応の困難度	脆弱性対応における困難の程度	ベンダーなどから提供されることを期待	• 脆弱性対応によるソフトウェアアップデートやハードウェア交換要否の確認 • 労力やリードタイムを考慮した脆弱性対応スケジューリング

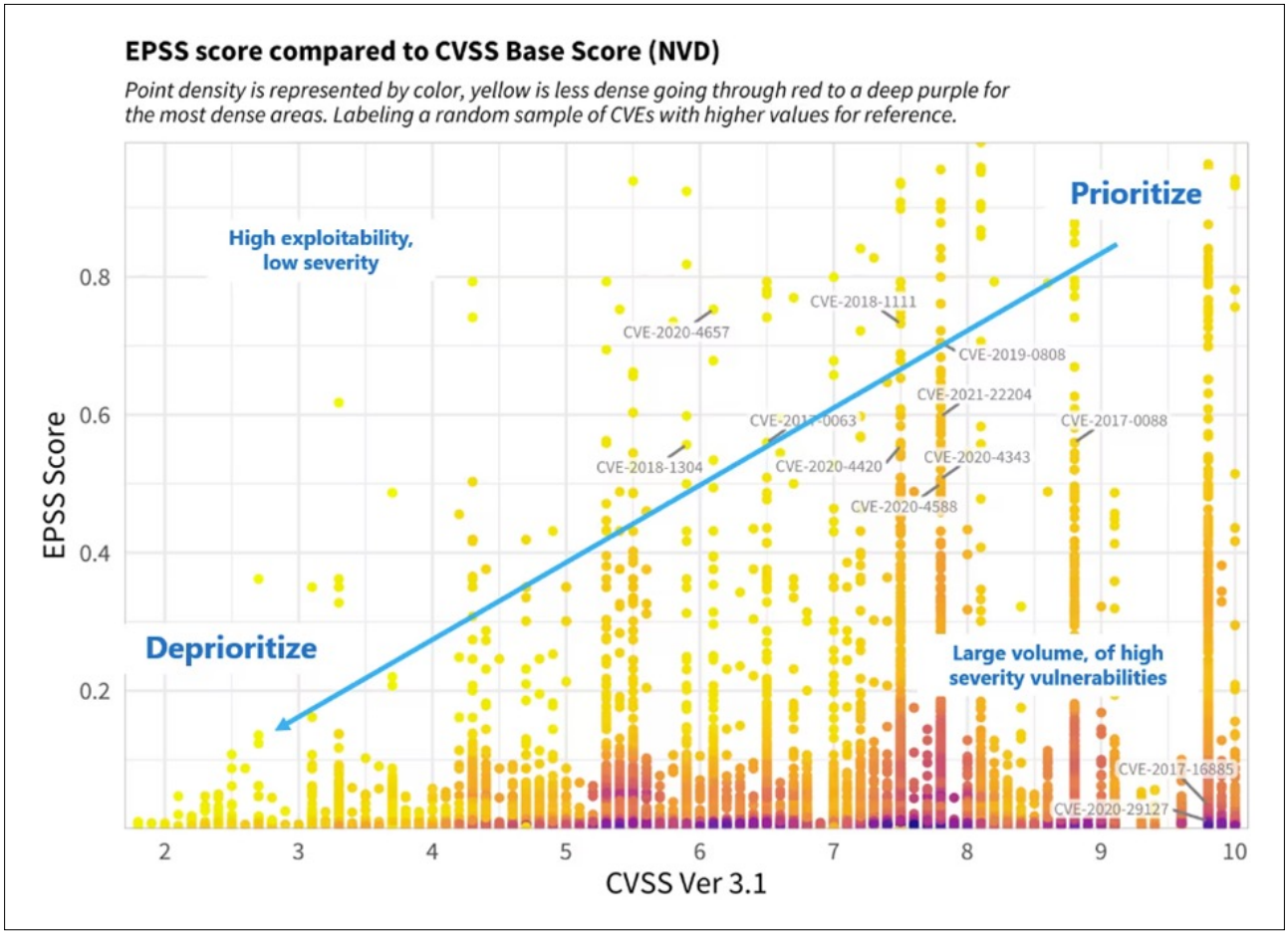
供給者による緊急度や対応の困難度は、自社で評価することは難しく、ベンダーなどから提供されることを期待します。企業はベンダーなどに対して能動的に確認することで、ベンダーからの情報提供を促すことができるでしょう。単純に新バージョンがリリースされたから新バージョンへ移行するだけでは、脆弱性の蓄積・残存という課題の解決にはつながらない恐れがあります。むしろ意味のない運用プロセスの変更と各種リソースの消費により、運用課題を悪化させる懸念があります。補足評価基準の使い方を適切に検討し、CVSSのスコアだけでなく補足評価基準の評価も活用することで、自社にとって本当に対応すべき脆弱性から対処できるという優先順位付けが期待されます。

2. CVSSとEPSSの並行運用

次にCVSS（バージョン不問）とEPSSの並行運用について考えます。EPSS値は、MITREのCVEリストへの掲載有無や、主要な脆弱性エクスプロイトアーカイブで公開されているかなどを参考に「EPSS Probability：今後30日間に脆弱性が悪用される確率」を提供します。CVSSは脆弱性の深刻度を評価し、EPSSはその脆弱性が悪用される確率を評価します。これら2つの手法を並行運用することは、優先度をつけて脆弱性に対応するための有用な方法です。FIRSTが公開しているEPSSとCVSSの相関関係のように、「縦軸：EPSS値」「横軸：CVSS値」のマトリクスで評価することが最もベーシックな使い方であると考えられます（図表22）。

CVSS値が高い場合でも、必ずしも悪用される確率が高いわけではありません（図表22）。そのため、CVSS値とEPSS値は密接な相関関係を持っていないことが分かります。裏を返せば、CVSS値だけを見て脆弱性対応を実施している場合、悪用の可能性が低い脆弱性に対して積極的に対処している可能性があるということになります。EPSS値もCVSS値も高いグラフの右上に位置する脆弱性は優先度を上げて対応すべき脆弱性であり、左下に位置する脆弱性は優先度を下げてもよい脆弱性であると考えることができます。CVSSバージョン4を採用するのであれば、補足評価基準を用いて追加評価をすることで、より自社環境に応じた効率的な脆弱性対応プロセスを構築できるでしょう。

図表22：CVSS値とEPSS値の相関関係



出所：Forum of Incident Response and Security Teams, Inc. 、2024年3月閲覧
https://www.first.org/epss/user-guide?_fsi=Y0BUkTI6&_ga=2.152763070.641370963.1708950620-1634403573.1693366774&_fsi=Y0BUkTI6

3. SSVCとEPSSの並行運用

最後に、SSVCとEPSSの並行運用への移行について説明します。CVSSの採用者によるSSVCへの移行は、既存の脆弱性対応プロセスの大幅な変更を伴うため、CVSSバージョン4への移行より比較的困難となります。SSVCでは決定木にしたがって意思決定をすることから、脆弱性の対応フェーズで意見の不一致が起きないよう、関係各所とコンセンサスを取ってガイドラインを制定しておくことが重要です。時間とコストを要することが想定されるため、特定のシステムなどを対象に決定木の要素を整理し、スモールスタートの考え方で取り組むことが有用だと考えられます。

一例として、決定木を構成する要素に対して想定される検討事項を示します（図表23）。CVSSバージョン4の補足評価基準と同様、SSVCでも自社内のIT資産の利用状況を把握・可視化しておくことが重要です。「Exploitation」や「Automatable」は、攻撃に関する詳細な情報を外部から入手する必要があります。これらの情報はインターネット上で収集することもできますが、脆弱性が増加している背景を考慮すると、自社で調査・収集を行うことは困難であると想定します。対策として有効となり得るのが、脆弱性にかかわるインテリジェンス情報を配信するサービスです。同サービスを使うことで比較的容易に情報収集できるようになります。

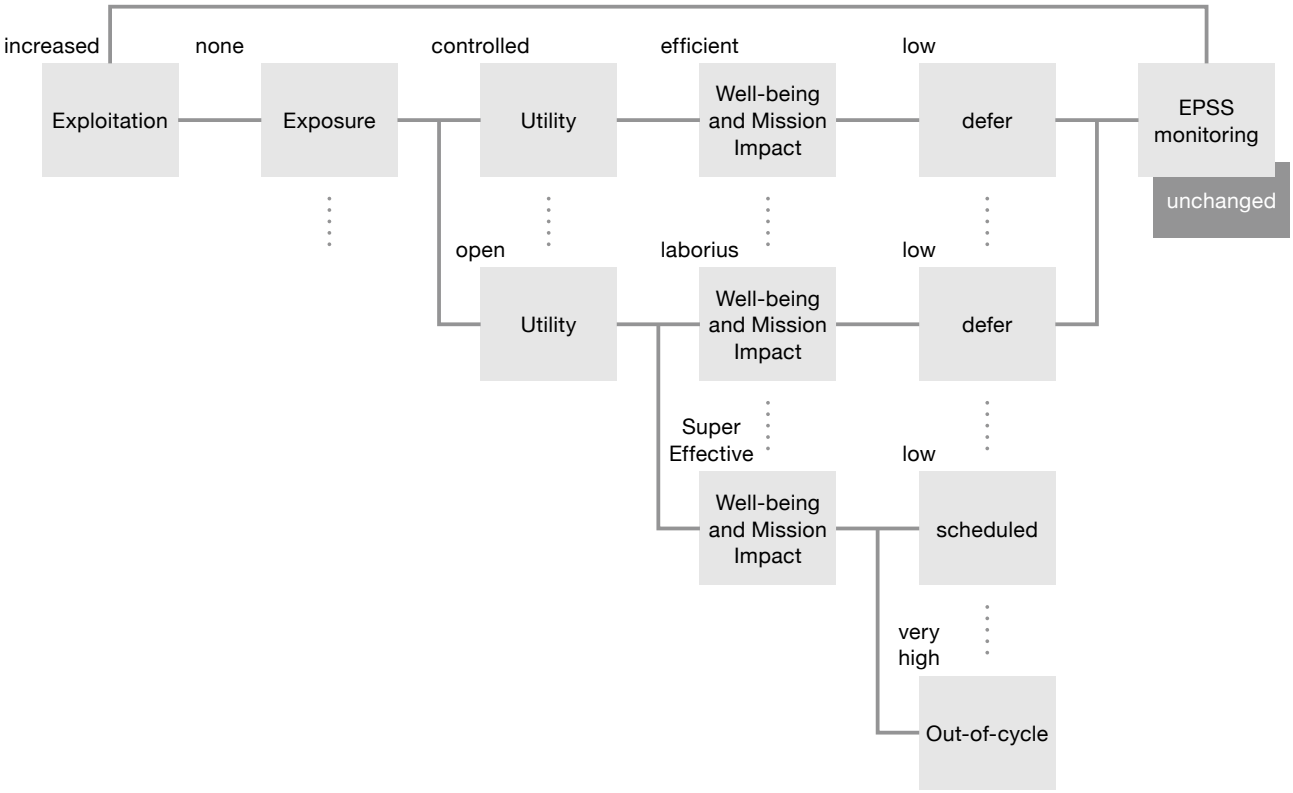
さらに、EPSSを並行運用することで、より効率的で効果的な脆弱性対応プロセスの運用が可能になると考えられます（図表24）。なぜならば、SSVCでは「Defer」、つまり「現時点では対応しない」という判断が出力されますが、いつの時点でDeferと判断した脆弱性を再評価すれば良いのか、SSVCだけの利用では判断が難しいからです。数多く存在する脆弱性をSSVCの決定木を用いて定期的に再評価することは現実的ではありません。EPSSを活用することでDeferと判断された脆弱性のEPSS値をモニタリングし、EPSS値が増加した場合にSSVCの決定木を用いて当該脆弱性を再評価するといった、比較的容易な経過観察を実現できると考えられます。

EPSS値のインプットデータから想像すると、脆弱性の悪用状況などによってEPSS値が変動することが考えられるため、再評価する際もExploitationやAutomatableの分岐を見直すだけで良い可能性もあります。SSVCとEPSSを並行運用することで、Defer状態の脆弱性についても形骸化することなく、悪用される確率の高まりに応じて当該脆弱性に対応することができると想定されます。

図表23：SSVCの決定木に対する検討事項

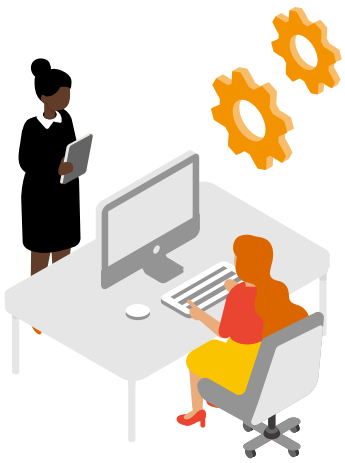
決定木の要素		評価概要	確認観点	推奨されるアクション
Exploitation		脆弱性の悪用状況	攻撃コードの公開・攻撃の発生有無	• 脆弱性にかかわるインテリジェンス情報を配信するサービスの活用 • ベンダーコミュニケーションによる積極的な情報収集
System Exposure		脆弱性がアクセス可能な攻撃対象	インターネットフェイシング有無、厳格なアクセス制御など	• Automatableでの推奨アクションに加え、アクセス制限困難機器の可視化 • アクセス制御レベルの管理と把握
Utility	Automatable	「エクスプロイト」までの自動化可能性	「偵察」「武器化」「デリバリ」「エクスプロイト」の実現性	• インターネットフェイシングしている機器の可視化 • ネットワーク上リーチャブルである範囲の可視化 • ベンダーコミュニケーションによる積極的な情報収集
	Value Density	攻撃者が獲得できるリソースの密度	価値があるデータを窃取できるか	• 自社の情報資産分類の定義とそれを扱うシステムの可視化・ひもづけ
Human Impact	Mission Impact	組織の使命と必須機能に対する影響	基幹系などミッションクリティカルなシステムか	• ミッションクリティカルなシステムの構成要素を棚卸し、可視化 • 各構成要素が攻撃された場合の障害範囲・継続時間を想定
	Situated Safety Impact	物理・環境・金銭・心理的に被る損害	人命や環境、社会基盤にかかわるシステムか	• 人命や環境、社会基盤にかかわるシステムの構成要素を棚卸し、可視化 • 各構成要素が攻撃された場合の影響の大きさを想定

図表24：SSVCとEPSSの並行運用フロー例



真に対処が必要な脆弱性に対応していくことが重要

本稿では、第1にアンケート結果を基に脆弱性対応プロセスの課題への言及と考察をしました。第2に新しい脆弱性評価方式を用いた脆弱性対応プロセスへ移行する際のポイントを示しました。多くの脆弱性が報告される中、それらを悪用する脅威アクターはますます増えるリスクが高まっています。昨今のセキュリティインシデントの公表状況を見ると、優先されるべき脆弱性への対処が放置されているような状態で甚大な影響を引き起こす事象も発生しています。企業に必要なことは、セキュリティハイジーンや、そもそものセキュリティレベルが「脅威環境に対して劣後しているかもしれない」と立ち返り、不断に自己認識をすることでしょう。今回の調査で示したような「脆弱性が残存・蓄積」している状態こそ、脅威アクターの恰好の的となることから、組織にとって大きなリスクを及ぼす可能性が高い脆弱性から優先的に対応していくべきです。SSVCやEPSSなどの脆弱性評価方式は、今すぐに対応すべき脆弱性にフォーカスできるよう進化しており、今回の調査で浮かび上がった課題への打ち手となる可能性があります。真に対処が必要な脆弱性に対応していくためには、脆弱性の深刻度を示すCVSS値だけでなく、具体的な対応判断を導出するSSVCや悪用される確率を示すEPSSと組み合わせたり、自組織への影響を考慮して優先度を付けたりすることが重要です。そのような取り組みを進めていくことが、膨大な脆弱性が報告されている状況から重大なセキュリティインシデントの発生を防ぐ第一歩となるのではないかと考えます。



第2章

デジタル化が生む「トラストギャップ（信頼の空白域）」を埋めるには

第1章で示したように、デジタルの技術革新のスピードは一段と速まり、各国・地域の規制やルールも目まぐるしく変わり続けています。最新技術を巧妙に採り入れ、規制の穴を狙うサイバー脅威をきちんと分析して適切に対処するには、ガイドラインに沿った態勢を整えるだけでは万全とはなり得ません。自社のインテリジェンスを高め、さまざまなリスクを検知して事前に危機の芽を摘む能動的な備えを築くことが重要になっています。

激変するビジネス環境に真正面から対峙するには、まずはITやセキュリティ部門が各事業をきちんと理解し、ビジネスに合ったセキュリティ基盤を構築すること。さらに、事業部門もサイバーセキュリティやデジタル技術を「自分ごと」として捉えること。そして、両部門が目線を合わせてセキュリティレベルの底上げに取り組むことが、デジタル時代の経営のレジリエンス（強靭性）を保つことにつながると考えられます。

デジタル化に伴うリスクと機会を自社の成長につなげるには、全てのステークホルダーに対して自社の人材やサービス、企業統治などへの信頼を得ることが不可欠です。ステークホルダーが抱く「トラストギャップ（信頼の空白域）」をいかに埋められるかが、非連続な時代における企業の強靭性と成長力を高める源泉になると考えられます。

第2章では、デジタル時代のトラストギャップを埋めるために日本企業が対応すべき備えに焦点をあて、俯瞰的に考察します。

1：デジタルオペレーショナルレジリエンスを磨く

コロナ禍によってぐっと進んだDXは仕事の効率性を高め、働き方の多様化をもたらしました。今後、ますます高まるデジタル化の潮流に乗ってもう一段の信頼と成長をつかむには、「セキュリティガバナンス」の再構築が欠かせません。

◆ 事業継続の判断軸を「自社視点」から「顧客視点」に変える

従来、セキュリティの高度なノウハウが必要なのは、ITや保守など一部の専門部署に限られていました。DXが進むにつれ、今では事業部門もAIやクラウドなどの使い手となり、新サービスや製品の開発からセキュリティ対策の実装までを担うことが求められています。セキュリティサービスの行き先を社内にとどめる時代は過ぎました。事業部門もデジタルサービスのセキュリティ上の脅威を意識して、適切な体制のもとでサービスを提供することが一段と重要視されています。

カギとなるのがデジタル時代に即した「オペレーショナルレジリエンス」の構築です。多くの企業はこれまで、地震などの自然災害を想定した事業継続計画（BCP）や事業継続マネジメント（BCM）を策定してきました。これらは今でも有効な手段である一方、多くは「自社視点」にとどまっているのが現状です。

サイバー脅威をはじめ、複数のリスクが同時多発的に起き得る非連続な時代では、自社の視点に縛られていては事業継続の判断基準を見誤りかねません。重要なのは「顧客視点」でサービスを高品質に維持することです。自社のサービスの利用者が何人いて、各サービスはどの程度利用者にとって重要なものなのか、サービスを提供できない場合に代替の手段はあるのか、といった分析をもとに事業の強靭性を担保する必要性が高まっています。

◆ BISOの登用で「ビジネス」と「セキュリティ」をつなぐ

デジタル時代に即したオペレーショナルレジリエンス＝「デジタルオペレーショナルレジリエンス」の土台を築くには、既存の経営に捉われない変革が欠かせません。デジタル化したビジネスを開発する事業部門と、サイバー対策のノウハウに長けたセキュリティ部門が密接に連携する態勢を整備する具体的な方法として、ビジネス情報セキュリティ責任者（BISO）の登用が注目されています。

BISOはビジネスの視点を持って、最高情報セキュリティ責任者（CISO）とともに企業のセキュリティ整備を補完し合う役割を担います。各事業部門にBISOを置いてセキュリティ部門との窓口になるケースもあれば、CISOと横並びの立場で事業部門のセキュリティ面を取りまとめる場合もあります。

各事業部門にセキュリティを落とし込む。セキュリティへのぶれない戦略を経営に組み込む。CISOとともにデジタル時代のガバナンスとサイバー防御体制を整える。BISOを軸としたガバナンスの変革が、セキュリティをビジネス全体に広げる「進化」と、業務から企業文化に落とし込む「深化」を促すでしょう。これらの取り組みの成否がデジタルオペレーショナルレジリエンスの向上、ひいては企業の「真価」を問う時代になりつつあるのです。

2：デジタルアイデンティティを確立する

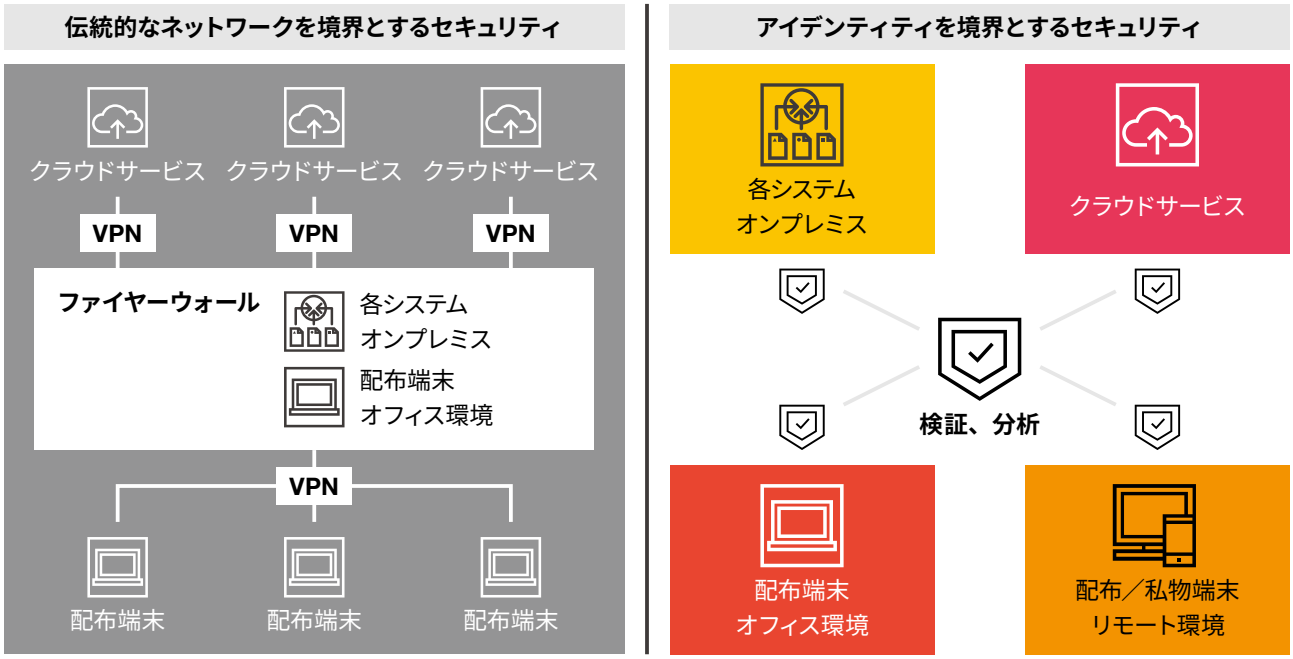
デジタル時代のビジネスでは、クラウド技術の活用が前提となります。利用者が自らハードウエアやサーバー、ソフトウエアなどを持たなくても、ネットを通じて必要なサービスを必要な分だけ使うことでコストを抑えたり、拡張性の確保や情報の共有が簡単になったりといった利点を得られるのが特長です。使い勝手が高い半面、外部のシステムを使って情報を管理するため、いざというときにすぐに対応しにくいという側面もあります。

◆「ゼロトラスト」でセキュリティレベルを上げる

多くの企業は従来、ネットワークを境界とし、脅威の兆候を検知すれば侵入を防ぐ手立てを取っていました。スポーツで例えると「ゾーンディフェンス」を敷いている状態です。システムが複雑に絡み合い、サイバー攻撃が巧妙になる今、ゾーンディフェンスだけでは悪意のある侵入者を防ぎきることはますます難しくなっていると言っていいでしょう。

守備の網の目を小さくするには、内部と外部のシステムの境界をなくし、守るべき情報にアクセスしようとするものを1つ1つチェックする「マンツーマンディフェンス」に切り替えることです。内部も外部も関係なく、全ての通信を何も信頼しないことを前提に検証と分析を重ねる「ゼロトラスト」の概念に基づいたセキュリティモデルの構築こそ、脅威を増すサイバーリスクを減らすカギになります。信頼を置かないことを前提とするセキュリティの積み重ねが、ステークホルダーの信頼を得る近道と言えます。

図表25：ゼロトラストアーキテクチャの概要（マンツーマンディフェンスの実施例）



ゼロトラストによるマンツーマンディフェンスを敷く場合、重要なのはアクセス元をきちんと識別する手段を確保することです。身元を確認する、本人によって使われているかを判定する、アクセスを許可または制御する、アクセス履歴を解析する。これらの一連のセキュリティ網を整えるために必要なのが「デジタルアイデンティティ」です。Identity-based perimeterなどと呼ばれる、デジタルアイデンティティを新しい境界とする考え方が今、広がりつつあります。

◆ サービス向上、不正防止・規律付けにつなげる

デジタルの世界で他者と区別可能な「識別子と属性の集合体」をデジタルアイデンティティと呼びます。リアルの世界では、人は他人を氏名や年齢などの他、声色や髪の色といった物理的情報をもとに直感的に識別しています。一方、デジタルの世界ではデジタルデータとしてでなければ識別できないため、パスワードやID、メールアドレスなどシステムが判別できる情報を確認することで個人を認証します。

デジタルアイデンティティの確立は、「顧客向けサービス」と「企業システム」のどちらにも寄与します。

「顧客向けサービス」では、サービスごとの顧客の属性をきちんと把握し、どんなサービスをよく利用しているのかを精緻に把握できるようになります。デジタル時代のビジネスでは、より良いサービスを開発して提供するのに欠かせない情報です。年齢に応じて閲覧できるコンテンツを制限するなど、適切なサービスの運用にも役立ちます。

「企業システム」では、従業員がアクセスできる情報を定義づける効果を得られます。デジタルアイデンティティは自社に関わる全ての情報に対するアクセス権を決める重要な要素となります。役職、所属、勤務地などに応じてアクセスできる情報とできない情報を明確に定めることで、社内の規律付けや不正の防止につなげられます。デジタルアイデンティティの管理をきちんと整えることが、ゼロトラストによる信頼性の向上を担保する土台となるのです。

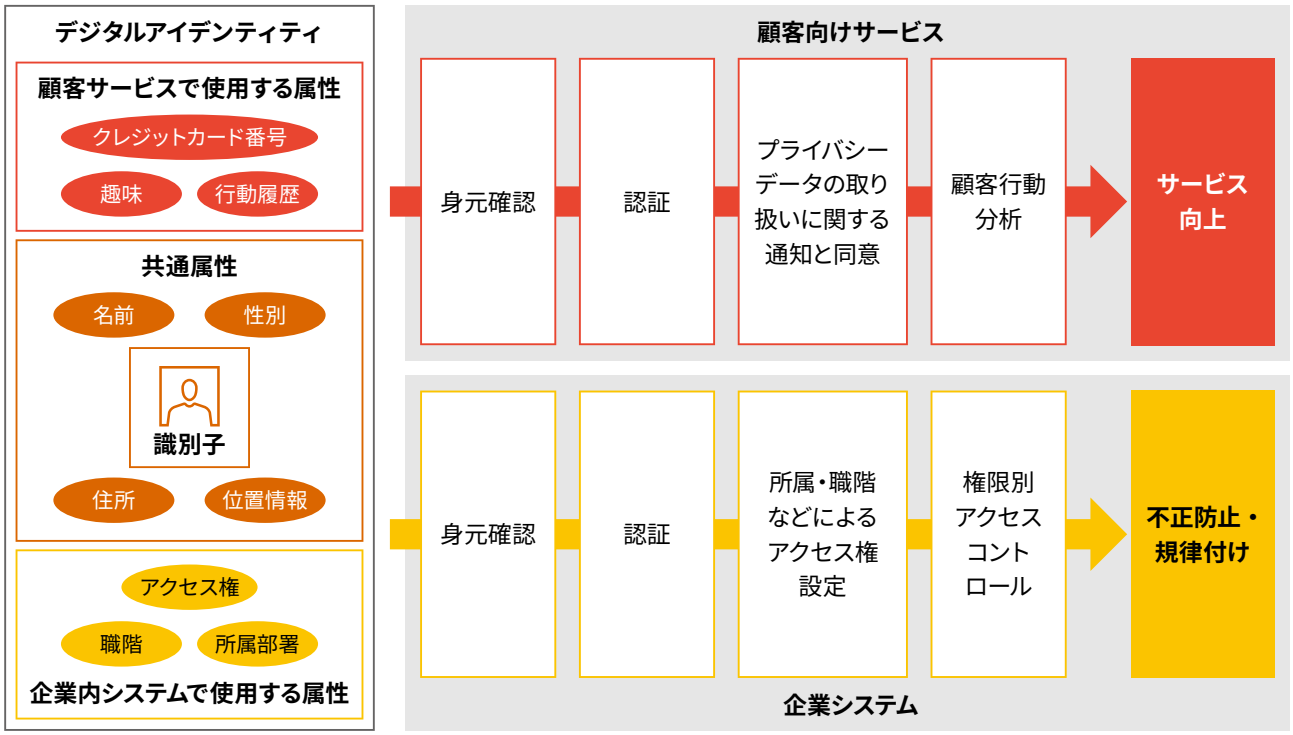
◆ ジョブ型雇用の推進がデジタルアイデンティティ確立の契機になる

日本でもデジタルアイデンティティを確立しやすくなる環境はじわりと整ってきました。これは、「仕事に人を付ける」ジョブ型雇用の推進が背景にあります。

日本では職務や勤務地などを限定せず、「人に仕事を付ける」メンバーシップ型雇用が主流でした。企業にとっては配置転換やジェネラリストな人材を育てやすい半面、複雑な職務権限やあやふやな引き継ぎ期間などが発生しがちです。働く人の仕事の量や中身が不定期に変わるため、不必要な情報にアクセスできる環境も放置されかねません。

一方、ジョブ型雇用は業務内容や責任の範囲、勤務時間や勤務場所などを明確に定めて雇用契約を結びます。ジョブ型雇用なら従業員ごとにアクセスできる情報をはっきり絞り込める利点があります。一部の日本企業ではジョブ型雇用の導入を進めています。こうした潮流も、日本社会にデジタルアイデンティティを普及させるきっかけになると言えるでしょう。

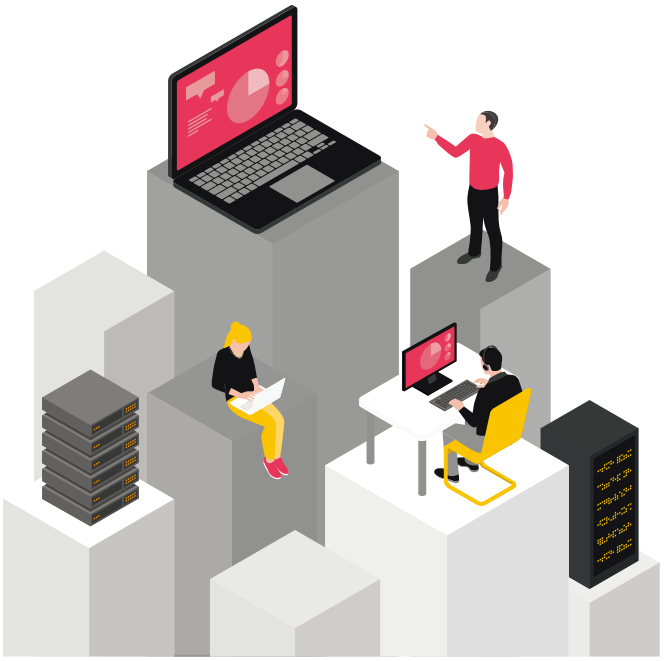
図表26：デジタルアイデンティティ確立の効果



まとめ

業界や国境を越えてデータが行き来する時代は間近に迫っています。人口減などを背景に国内市場の縮小傾向が避けられない中、日本企業はグローバル市場を開拓して成長の果実を得る必要性が一段と高まっています。

日本企業が成長への階段をもう一段上るには、セキュリティやデジタル技術の知見をビジネス全体に広げ、全社一体となってサイバー脅威に対峙する実行力が欠かせません。デジタル時代に適応した顧客、従業員のアイデンティティを高度化させる変革も待ったなしの状況です。ビジネス環境の変化を先取りした顧客視点の変革こそ、デジタル化が生むトラストギャップを埋める要諦となるのです。

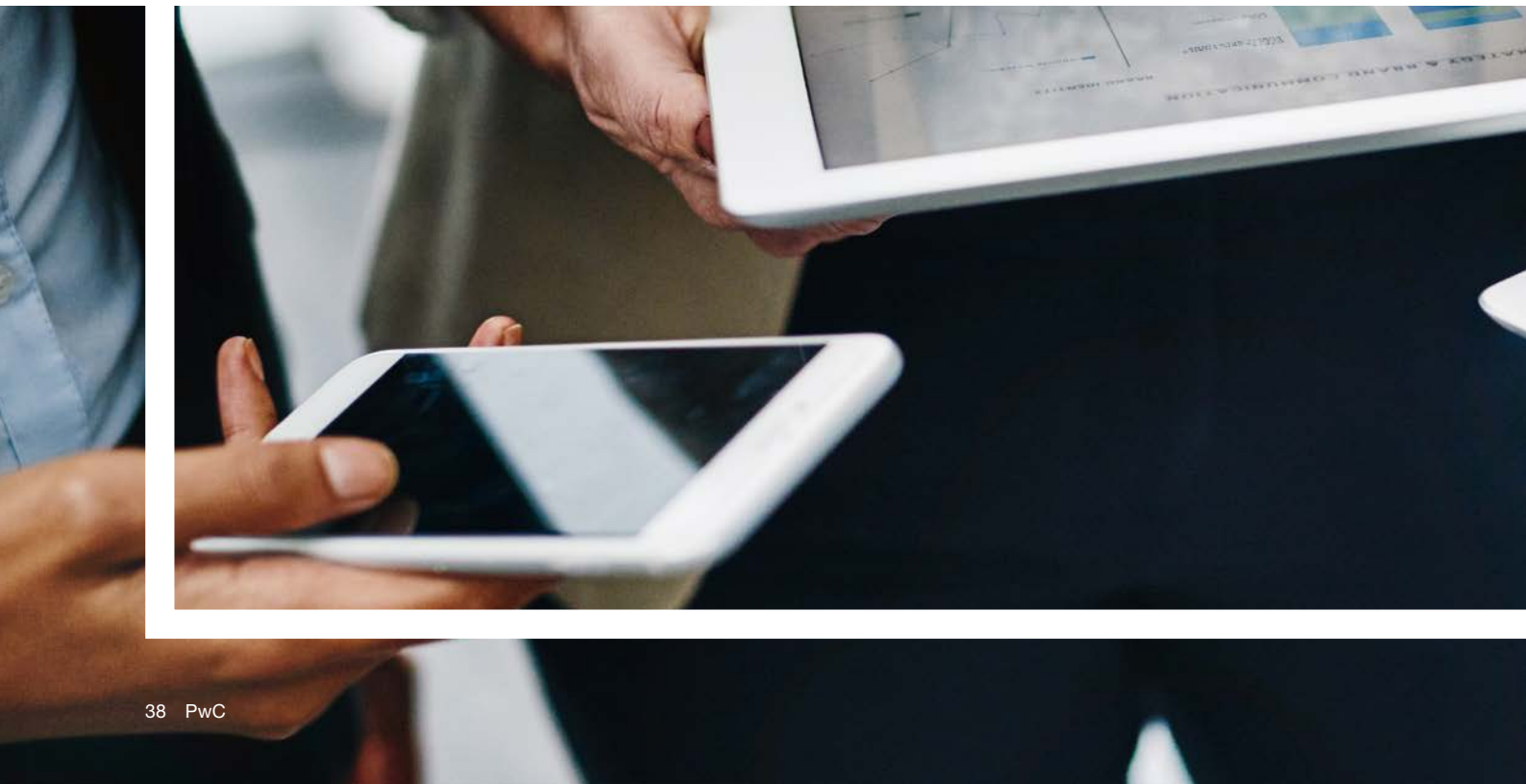


おわりに

企業はさまざまな環境変化に直面しており、不確実性の高い未知なる迷路を進まなければなりません。

激変するビジネス環境に対峙するには、自社のビジネスに影響を及ぼしかねない脅威や環境の変化をタイムリーに把握・分析することが重要です。また、セキュリティ戦略の立案・推進はもとより、その戦略を柔軟かつダイナミックに見直す必要があります。

サイバーインテリジェンスを活用し、能動的にリスクに備え、サイバー脅威に対峙する実行力を築くことが、自社のレジリエンスを高め、新しい一歩を踏み出すカギになります。



監修

林 和洋
PwCコンサルティング合同会社
パートナー

丸山 満彦
PwCコンサルティング合同会社
パートナー

執筆

村上 純一
PwCコンサルティング合同会社
パートナー

橋本 哲哉
PwCコンサルティング合同会社
ディレクター

松尾 早苗
PwCコンサルティング合同会社
シニアマネージャー

伊藤 公祐
PwCコンサルティング合同会社
シニアマネージャー

お問い合わせ先

PwC Japanグループ
https://www.pwc.com/jp/ja/contact.html

www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwC Japan有限責任監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立した別法人として事業を行っています。
複雑化・多様化する企業の経営課題に対し、PwC Japanグループでは、監査およびアシュアランス、コンサルティング、ディールアドバイザリー、税務、そして法務における卓越した専門性を結集し、それらを有機的に協働させる体制を整えています。また、公認会計士、税理士、弁護士、その他専門スタッフ約11,500人を擁するプロフェッショナル・サービス・ネットワークとして、クライアントニーズにより的確に対応したサービスの提供に努めています。
PwCは、社会における信頼を構築し、重要な課題を解決することをPurpose（存在意義）としています。私たちは、世界151カ国に及ぶグローバルネットワークに364,000人以上のスタッフを擁し、高品質な監査、税務、アドバイザリーサービスを提供しています。詳細は www.pwc.com をご覧ください。

発刊年月：2024年4月　　管理番号：I202310-07