サイバーセキュリティに関する情報開示制度の改革による企業価値と市場信頼性の向上に関する報告書

2026 年 11 月

一般社団法人 IT 団体連盟（サイバーセキュリティ委員会）

一般社団法人スチュワードシップ研究会

要約

本報告書は、サイバー空間の脅威が企業経営と資本市場に与える影響の深刻化を踏まえ、日本の情報開示制度の改善を目的とするものである。現状、我が国の上場企業におけるサイバーセキュリティ情報の開示は、企業の裁量に委ねられている部分が多く、その内容や適時性に大きなばらつきが見られる。これは投資家が企業間の開示の比較等を通じて適切なリスク評価を行う上で重大な障害であり、結果として企業価値の毀損や市場全体の信頼性低下に繋がりかねない。

とりわけ、2023 年に米国証券取引委員会（SEC）が導入した新たなサイバーセキュリティ開示規則は、国際的な潮流の転換点であり、日本もこれに比肩する制度を早急に整備する必要がある。さもなければ、グローバルな投資家から「サイバー・ガバナンスに関する情報開示が不十分な市場」と評価されるリスクを看過できない。

そこで本報告書では、投資家保護と企業の持続的成長の両立を目的とし、以下の二本柱からなる制度改革を金融庁及び東京証券取引所に提案する。

1．**有価証券報告書におけるサイバーセキュリティ情報の体系的開示の義務化**

- 金融商品取引法に基づく『企業内容等の開示に関する内閣府令』（昭和 40 年大蔵省令第 5 号。以下「開示府令」という。）を改正し、有価証券報告書の「事業等のリスク」の項目においてサイバーセキュリティに関する「ガバナンス」と「リスク管理」の体系的な記載を義務付ける。
- 開示項目は、SEC 規則を参考に、取締役会の監督体制や経営陣の役割・知見、リスク評価・管理プロセスなど、投資家の判断に資する本質的な情報に絞り込む。これにより、経営層の意識改革を促し、企業全体のサイバーレジリエンス向上に繋げる。

2. **重大サイバーインシデントに関する迅速な情報開示の義務化**

- 企業内容等の開示に関する内閣府令第 19 条第 2 項を改正し、臨時報告書の提出事由として「重大なサイバーセキュリティ・インシデントの発生」を追加する。
- 開示期限は、SEC 規則に倣い「当該インシデントが投資者にとって重大（material）であると会社が判断することが合理的に可能となった時点から 4 営業日以内」とする。これにより、企業の初動対応と投資家への情報提供のバランスを図る。
- 併せて、東京証券取引所は、上記と同様に適時開示規則を変更することで、制度の実効性を担保する。
- また、国家安全保障に関わる場合に捜査当局等との連携のもと開示を一時的に遅延できる仕組みも導入し、制度の柔軟性を確保する。

これらの改革により、情報開示を通じて企業のサイバーセキュリティ対策を「コスト」から「投資」へと転換させ、経営の重要課題として位置づけることを促すことにつながる。本提案の実現は、日本企業の国際競争力を高め、資本市場の健全な発展に不可欠な基盤となると考える。

はじめに

サイバーセキュリティが企業の存続、ひいては資本市場全体の安定性を揺るがしかねない経営およびガバナンスの中核的課題であることは、疑いの余地がない。近年のランサムウェア事案等に見られるように、大規模なサイバーインシデントは事業活動を長期間停止させ、株価を大きく下落させるなど、投資家に甚大な損害を与え得る。

しかし、日本の現行開示制度は、こうしたリスクを投資家が事前に、あるいは適時に把握するには十分とは言えない。本報告書は、この現状を改善し、日本の資本市場をより強靭で信頼性の高いものへと進化させるための具体的な対策を示すものである。

（１）現状分析：国際潮流と日本の課題

1. 米国 SEC による開示改革の先進性 2023 年 7 月に最終化された SEC のサイバーセキュリティ開示規則は、世界中の規制当局にとってのベンチマークとなる画期的なものである。その本質は、以下の二つの情報開示を両輪として義務付けた点にある。

- **重大インシデントの適時開示（Form 8-K, Item 1.05）**：企業がサイバーインシデントを「material（投資家にとって重要）」であると判断することが合理的に可能となった時点から**4営業日以内**に、その性質、範囲、時期、および企業への重大な影響（実際または合理的に予見される影響）を開示することを求めたものである。重要なのは、起算日を「インシデント発生日」ではなく「当該インシデントが投資家にとって重要（material）であると判断することが合理的に可能となった時点」とした点である。これにより、企業はインシデント発生後の初期の事実確認や応急対応に必要な時間を確保しつつ、投資家への迅速な情報提供との両立を図ることが可能となる。また、攻撃手法や特定の脆弱性といった、攻撃者を利するおそれのある技術的詳細の開示は求めないことも明示されている。

- **ガバナンスとリスク管理の年次開示（Regulation S-K, Item 106）**：年次報告書（Form 10-K など）において、①サイバーセキュリティリスクを評価・管理するためのプロセス、②取締役会によるリスクの監督体制、③リスク管理における経営陣の役割と専門性の開示を求めている。当初案（2022 年 3 月提案）では取締役会メンバーのサイバーセキュリティ専門性の開示が提案されていたが、最終規則では取締役会レベルではなく「経営陣の専門知識」の開示に修正された。この変更は、形式的な専門家の配置よりも実質的なガバナンス機能を重視する姿勢の表れとして注目に値する。これは、特定の経歴を持つ人物を形式的に取締役に置くことよりも、組織として実質的な知見をどのように確保しているかを問う、原則主義的（principles-based）なアプローチの表れである。

これらの規則は、投資家保護を強化すると同時に、企業の経営層に対し、サイバーセキュリティを経営リスクとして真摯に向き合うことを強く促すインセンティブとして機能する。

2. 日本の開示制度の現状と限界　一方、日本の現状は米国の最新動向と比較すると、改善の余地があると言える。

- **有価証券報告書**：金融商品取引法に基づく「企業内容等の開示に関する内閣府令」では、「事業等のリスク」の項目でサイバーセキュリティについて言及する企業は増えている。しかし、記載内容は各社の任意であり、「当社の事業はシステムに依存しており、障害が発生した場合は影響を受ける可能性があります」といった定型的・抽象的な記述に留まる例も少なくない。実際の開示内容を分析すると、情報開示の質と量には企業間で大きな差が存在することが確認されている。日本 IT 団体連盟の調査によれば、日経 500 種平均構成企業のうち、総じて上位の 100 社程度の企業では開示情報が一定程度充実している一方、その他の企業ではまだ開示が進んでいない状況にある。2023 年 1 月に導入されたサステナビリティ情報の開示枠組みにおいても、サイバーセキュリティはリスク管理の一環として言及されうるが、具体的な記載項目は定められておらず、企業間での比較が十分にできるようになっていないため、実効性は限定的である。

- **適時開示**：東京証券取引所の適時開示規則では、「サイバー攻撃の発生」は独立した開示項目ではない。「災害に起因する損害」や「投資者の投資判断に著しい影響を及ぼす事実」（いわゆるバスケット条項）に該当する場合に開示が求められるが、その判断は企業に委ねられている。結果として、インシデントの公表が遅れたり、そもそも公表されなかったりするケースも発生し得る。

このように、サイバーセキュリティに関する情報開示について明確なルールや期待水準が必ずしも十分に共有されていない現状は、投資家の適切なリスク評価を妨げ、市場の非効率性につながりかねない。また、経営層にとっても、明示的な開示義務がないことが、サイバーセキュリティへの投資や体制整備を後回しにする誘因となるおそれがある。

（2）提案

以上の分析に基づき、実務上の実効性を重視しつつ、金融庁と東京証券取引所に対して以下の二つの政策を提案する。

提言 1：有価証券報告書におけるサイバーセキュリティ情報開示の体系的な義務化

有価証券報告書におけるサイバーセキュリティリスクの開示は、経営層の意識向上と投資家保護の観点から極めて重要である。これを実現するため、**「企業内容等の開示に関する内閣府令」を改正し、有価証券報告書の「事業等のリスク」の記載要領に、サイバーセキュリティに関する明確なセクションを設けるか、あるいは明確な記載事項を追加する**ことを提案する。

開示項目については、SEC 規則（Regulation S-K, Item 106）の原則主義的アプローチを参考としつつ、我が国の企業実務に適合する形で、以下のように定めることを提案する

- **A. サイバーセキュリティに関するガバナンス体制**
    - 取締役会によるサイバーセキュリティリスクの監督に関する説明（例：取締役会または特定の委員会が監督責任を負うか、経営陣からどのような頻度で報告を受けるか等）。
    - サイバーセキュリティの脅威を評価・管理する上での経営陣の役割、およびその責任を担う役員・部署の位置付けや関連する経験・知見の概要。
- **B. サイバーセキュリティに関するリスク管理**
    - サイバーセキュリティの脅威（サードパーティ・サービスプロバイダ等に起因するサプライチェーンリスクを含む）から生じる重大なリスクを特定、評価、管理するための企業のプロセスに

関する説明。その際には、重要な情報資産、教育・演習の実施状況、取引先・サプライチェーンリスクの対応状況を含むものとする。

- 過去に発生した重大なサイバーインシデント（報告対象期間中に発生したものを含む）が、企業の事業戦略、業績、財政状態に与えた影響、または今後与える可能性のある重大な影響についての説明。ただし、インシデントが発生していない場合はその旨を記載すれば足りるものとする。

これにより、投資家は企業のサイバーリスクへの向き合い方を比較可能な形で把握できるとともに、企業側も、開示の準備過程を通じて自らのリスク管理態勢を点検・強化するインセンティブを得る。

提言 2：重大サイバーインシデントに関する迅速な情報開示の義務化

インシデント発生時の迅速な情報開示は、市場の混乱を最小限に抑え、他社への連鎖的な被害を防ぐ上で不可欠である。そこで**二段階のアプローチ**を提案する。

- **アプローチ①：臨時報告書制度の活用**
  - **開示府令第 19 条第 2 項**（「投資者の投資判断に著しい影響を及ぼすものとして内閣府令で定める事実」を列挙する規定）について、**第 12 号**（その他の重要事実）の活用又は新たな号の追加により、「企業の事業運営、財政状態または業績に重大な影響を与える、又は与えるおそれのある**サイバーセキュリティ・インシデントの発生**（以下「重大サイバーインシデント」という。）」を**臨時報告書の提出事由**として明記することを提案する。
  - **開示期限**: SEC 規則に倣い、「**インシデントが重大であると会社が判断することが合理的に可能となった時点から 4 営業日以内**」とする。なお、この起算点は「インシデントの発生日」ではなく、「重要性判断が可能となった時点」であることを明確にし、企業が初動対応や事実確認に必要な時間を確保できるよう配慮する。
  - **開示内容**: インシデントの性質、範囲、発生時期または発生期間、並びに判明している範囲での事業、業務、財政状態への重大な影響。攻撃手法などの技術的詳細や、脆弱性に関する情報の開示は求めない。
- **アプローチ②：東京証券取引所適時開示規則改正**
  - 東京証券取引所は適時開示規則のガイドラインを改正し、「**サイバー攻撃による重大な損害の発生またはそのおそれ**」を明確な開示項目として例示する。開示基準やタイミングは、上記の臨時報告書制度との整合性を図ることが望ましい。

【開示遅延に関する特例措置の導入】さらに、SEC が司法長官の要請に基づき開示を遅延できる制度を設けたことを参考に、日本でも特例措置を検討すべきである。具体的には、「**国家安全保障または公共の安全に対する重大なリスクがあると主務大臣（又は国家サイバー統括室等）が判断した場合、一定期間、開示を延期できる**」という仕組みを導入する。これにより、犯罪捜査への支障や、国家の重要インフラに対する脅威の拡散を防ぐことが可能となる。

おわりに

本報告書は、サイバーセキュリティ情報の開示を巡るルールや期待水準が十分に明確でない現状を改め、投資家と企業の双方に対し、予見可能性の高い枠組みを提供することを目指すものである。その目的は、単に米国制度を形式的に模倣することではない。企業の過度な負担を避けつつ、実効性を最大化する原則主義的アプローチを取り入れ、日本の法制度と企業実務に適合した制度設計を行うことにある。

金融庁及び東京証券取引所が本提案に沿った制度改革を推進することは、企業のサイバーセキュリティ対策を「守りのコスト」から「攻めのガバナンス投資」へと転換させ、日本企業全体のレジリエンスと国際競争力を引き上げることに直結する。ひいては、それが我が国の資本市場の信頼性と魅力を高め、持続的な経済成長に資するものと考える。

以　上