資料６－３

セキュリティ対策情報開示ガイドライン（仮称）に係る論点（案）

総務省　サイバーセキュリティ統括官室

情報開示分科会報告書（平成30年６月公表）概要①

■ 民間企業におけるセキュリティ対策の情報開示による「セキュリティ対策の見える化」を通じて、民間企業の経営層が自社のセキュリティ対策の現状を認識し、また、他社の状況と比較することにより、さらに必要な具体的な対策を検討し、導入する「セキュリティ対策の好循環」が起こる環境の実現が期待される。

■ 情報を開示するにあたっては、開示の対象者によってその考え方、取組が異なることから、報告書（案）においては、①社内の情報共有（第一者開示）、②契約者間等の情報開示（第二者開示）、③社会に対する情報開示（第三者開示）の３つの側面に分けて整理。

【これまでの開示の考え方】　情報開示　＝　社会に対する情報開示（第三者開示）

情報開示分科会において、セキュリティ対策の開示（共有）を**３つの側面に整理**

【類　型】		【意　義】
社内の情報共有（第一者開示）	＝ 自社のセキュリティ対策について、その必要性・重要性・緊急性をセキュリティ対策の担当部署だけでなく、社内全体で共有すること。	✓ 取締役会における検討等を通じて、経営層としても責任を自覚すること（気づき）となり、セキュリティ対策が経営課題として扱われる。 ✓ 経営層がセキュリティ面におけるリスク及びその対策の状況を適切に認識することにより、セキュリティ対策を強化するための経営判断に資する。
契約者間等の情報共有（第二者開示）	＝ 契約相手方やグループ企業、サプライチェーンを構成する企業、保険会社等、対象を限定して自社のセキュリティ対策を開示すること。	✓ 契約の相手方との間で信頼を醸成するとともに、サプライチェーン全体のセキュリティが向上する。 ✓ セキュリティインシデントやその対策等について情報を共有・開示することにより、共有範囲の中で信頼の醸成やセキュリティ対策の向上に資する。 ✓ サイバーセキュリティ保険について、保険会社に対して適切にセキュリティ対策を開示し、定期的に評価を受けることにより、追加的なセキュリティ対策を検討する機会となる。
社会に対する情報開示（第三者開示）	＝ 社会の幅広い対象に向けて自社のセキュリティ対策を開示すること。	✓ 経営層が自社のセキュリティ対策を認識するきっかけとなる。 ✓ 他社のセキュリティ対策の状況を知り、自社と比較することができる環境となり、さらに社会全体でセキュリティ対策が競争的に拡大する。 ✓ 開示した企業が、適切かつ優良な取引先として認識されることを通じて、サプライチェーン全体のセキュリティの確保に資する。

情報開示分科会報告書（平成30年６月公表）概要②

	【検討結果】	【今後の取組】
社内の情報共有（第一者開示）	✓ 経営層の理解を深め、気づきを与えるとともに、セキュリティ対策の担当部署の現場と経営層の間を繋ぐ、いわゆる「戦略マネジメント層」の育成に向け取組を進める必要がある。	（社内の情報共有に向けた戦略マネジメント層の育成） 1．人材のスキルの具体化、スキル取得のための教育コンテンツの開発・普及、スキル認定を行う仕組みを産学官により構築するための検討。 【平成30年度中を目途に方向性を整理】
契約者間等の情報共有（第二者開示）	✓ 契約者間等で確認すべき事項や必要な対策の整理、サプライチェーン全体またはグループ全体における情報共有体制の構築の促進が必要である。 ✓ サイバーセキュリティ保険について、対策の実施及び開示のインセンティブとなるような割引制度の普及や、グループ全体・サプライチェーン全体で一括して加入するような保険商品の展開が期待される。	（関係者間の情報共有促進のための仕組みづくりの検討） 2．米国等におけるISAO（※）等の動向等について調査するとともに、公的支援のあり方について検討。 【平成30年度中を目途に検討結果を取りまとめ】 （※）ISAO：Information Sharing and Analysis Organization 3．セキュリティベンダー、損害保険会社、その他の関連する企業によるサイバーセキュリティ保険を含む総合サービスの開発に向けたモデル事業を推進し、標準仕様化に向けて検討。また、企業のセキュリティ対策の強度を簡易に診断できるツールキットを評価する仕組みづくりを検討。 【モデル事業については平成30年度に検討】
社会に対する情報開示（第三者開示）	✓ 事業者の規模や取組状況に応じて、セキュリティ対策の自己宣言制度や主要５項目（※）の開示、「情報セキュリティ報告書」の作成など、段階的に対策を講じていくことが望ましい。 ※　①基本方針等の策定状況、②管理体制、③教育・人材育成、④社外との情報共有体制、⑤第三者評価・認証	（第三者開示の促進に向けたガイドラインの策定） 4．「セキュリティ対策情報開示ガイドライン」（仮称）を策定・公表。 【平成30年秋を目途にガイドラインを策定】 5．導入予定の「コネクティッド・インダストリー税制」の活用状況を分析するとともに、企業のニーズ等を反映した投資促進のための政策支援のあり方について検討。 【支援税制の運用にあわせて適宜実施】

サイバーセキュリティ戦略等における情報開示の位置づけ

○サイバーセキュリティ戦略（平成30年７月27日　閣議決定）

４．目的達成のための施策
４．１．経済社会の活力の向上及び持続的発展
４．１．１．新たな価値創出を支えるサイバーセキュリティの推進
（２）サイバーセキュリティに対する投資の推進

企業がサイバーセキュリティに関わる取組を継続的に実施するためには、それに対応する経営上のインセンティブがあることが重要である。すなわち、財務的な観点を含め、サイバーセキュリティに係るリスクとその対策が可視化され、経営層がその現状を認識し、更に必要な具体的な対策を検討・導入するとともに、市場がその取組を企業価値の向上につながるものとして評価し、サイバーセキュリティに対する投資へのインセンティブが継続的に生まれる、という好循環が形成されることが望ましい。

このため、投資家を意識して、企業が積極的にサイバーセキュリティに関する取組について情報発信・開示を行うことが重要であり、**国は、ベストプラクティスの共有やガイドラインを策定するとともに、情報発信・開示の状況についての継続的な把握・評価に取り組む。**加えて、投資家が企業経営層のサイバーセキュリティに関する取組を評価できるような仕組み作りを進めていくことも必要である。

○サイバーセキュリティ2018（平成30年７月25日　サイバーセキュリティ戦略本部決定）

１．経済社会の活力の向上及び持続的発展
１．１．新たな価値創出を支えるサイバーセキュリティの推進
（２）サイバーセキュリティに対する投資の推進

（イ）**総務省において、ベストプラクティスも盛り込んだ「セキュリティ対策情報開示ガイドライン」（仮称）を策定、公表**する。

情報開示の意義①

■ ICTの発展やサイバー空間と実空間の融合に伴い、経営でのサイバーセキュリティの重要性が増大。

■ その中で、セキュリティ対策に関する情報発信による社会的価値の向上の重要性が認識されている

企業経営のためのサイバーセキュリティの考え方（平成28年８月２日　内閣官房内閣サイバーセキュリティセンター）

企業が自発的に行うサイバーセキュリティの取組が促進されるよう、企業経営のためのサイバーセキュリティに係る基本的考え方とともに、経営層に期待される“認識”や経営戦略を企画する人材層に向けた実装のためのツールを示す。
※普及啓発・人材育成専門調査会の下に設置された、「セキュリティマインドを持った企業経営ワーキンググループ」（主査：林紘一郎 情報セキュリティ大学院大学教授）を通じ、検討を実施。

基本方針　　ーサイバーセキュリティは、より積極的な経営への「投資」へー

グローバルな競争環境の変化

- ITの発展によるビジネスの変革が、消費者向けのビジネスから企業間取引へと拡大
- サイバー空間と実空間の融合がさらに進み、チャンスもリスクも一層増大

サイバーセキュリティをやむを得ない「費用」でなく、積極的な経営への「投資」と位置づけ、企業としての「挑戦」と、それに付随する「責任」として取り組むことが期待される

I.基本的考え方

二つの基本的認識

＜①挑戦＞
サイバーセキュリティは、利益を生み出し、ビジネスモデルを革新するものであり、新しい製品やサービスを創造するための戦略の一環として考えていく必要がある。

＜②責任＞
全てがつながる社会において、サイバーセキュリティに取り組むことは社会的な要求・要請であり、自社のみならず社会全体の発展にも寄与することとなる。

三つの留意事項

＜①情報発信による社会的評価の向上＞
- 「セキュリティ品質」を高め、品質向上に有効な経営基盤の一つとしてセキュリティ対策を位置付けることで企業価値を高めることが必要。
- そのような取組に係る姿勢や方針を情報発信することが重要。

＜②リスクの一項目としてのサイバーセキュリティ＞
- 提供する機能やサービスを全うする（機能保証）という観点から、リスクの一項目としてのサイバーセキュリティの視点も踏まえ、リスクを分析し、総合的に判断。
- 経営層のリーダーシップが必要。

＜③サプライチェーン全体でのサイバーセキュリティの確保＞
- サプライチェーンの一部の対策が不十分な場合でも、自社の重要情報が流出するおそれあり。
- 一企業のみでの対策には限界があるため、関係者間での情報共有活動への参加等が必要。

情報開示の意義②

■ 政府全体の議論でもサイバーセキュリティに関する情報提供・開示は経営者に期待される認識として位置づけられている。

企業経営のためのサイバーセキュリティの考え方（平成28年８月２日　内閣官房内閣サイバーセキュリティセンター）

II.企業の視点別の取組

企業が投資すべき対象や経営リスクは様々であり、各企業の人的・金銭的資源にも限りがあることから、ITの利活用やサイバーセキュリティへの取組において、各企業の事業規模のみならず、その認識の違いなどを踏まえて取り組んでいく必要がある。

ITの利活用を事業戦略上に位置づけ、サイバーセキュリティを強く意識し、積極的に競争力強化に活用しようとしている企業

（積極的にITによる革新と高いレベルのセキュリティに挑戦するあらゆる企業）

【経営者に期待される認識】
- 積極的なITの利活用を推進する中で、製品やサービスの「セキュリティ品質」を一層高め、自社のブランド価値の向上につなげるべく、システムの基盤におけるセキュリティの向上、情報・データの保護、製品等の安全品質向上に取り組む。
- 様々な関係者との協働が重要であるため、情報提供に主体的に取り組む。
- 決して現存する標準や取り組みなどに満足することなく、実空間とサイバー空間の融合が高度に深化した明日の世界をリードし、変革していく存在となることが期待される。

【実装に向けたツール】
- IoTセキュリティに関するガイドライン（「IoTセキュリティのための一般的枠組」等）
- 自社のブランド価値としてのサイバーセキュリティに係る積極的な情報発信

IT・セキュリティをビジネスの基盤として捉えている企業

（IT・サイバーセキュリティの重要性は理解しているものの、積極的な事業戦略に組み込むところまでは位置づけていない企業）

【経営者に期待される認識】
- 経営者のリーダーシップによって、社会的責任としてのサイバーセキュリティ対策に取り組む。
- サプライチェーンやビジネスパートナー、委託先を含めた対策を行う。
- 平時・緊急時のいずれにおいても、情報開示などの適切なコミュニケーションを行う。

【実装に向けたツール】
- サイバーセキュリティ経営ガイドライン
- 企業等がセキュリティ対策に取り組む上での保険等のリスク管理手法の活用
- サイバーセキュリティを経営上の重要課題として取り組んでいることの情報発信

自らセキュリティ対策を行う上で、事業上のリソースの制約が大きい企業

（主に中小企業等でセキュリティの専門組織を保持することが困難な企業）

【経営者に期待される認識】
- サプライチェーンを通じて中小企業等の役割はますます重要となる中、消費者や取引先との信頼関係醸成の観点から経営者自らサイバーセキュリティ対策に関心を持ち、取り組む。
- 外部の能力や知見を活用しつつ、効率的に進める方策を検討する。

【実装に向けたツール】
- 効率的なセキュリティ対策のためのサービスの利用（中小企業向けクラウドサービス等）
- サイバーセキュリティに関する相談窓口やセミナー、地域の相談員等の活用

サイバーセキュリティに関する情報提供や情報開示は経営層に期待される認識。

各企業の事業規模やICT及びセキュリティに関する認識の違い等を踏まえ、**情報開示に関する具体的な手引きを作成**することにより、情報開示の促進に資する。

セキュリティ対策情報開示ガイドライン（仮称）の趣旨・目的（案）

■ 民間企業のセキュリティ対策の情報開示の促進により、社会的な企業価値の向上等を図ることを目的とし、民間企業にとって参考となり得る事例等をまとめたガイドライン（仮称）を策定する。

目的

- ✓ セキュリティ対策の情報開示が、企業にとっては自社の**社会的評価の向上**に、社会にとっては「セキュリティ対策の好循環（※）」を通じた社会全体の**セキュリティ対策の質の向上**につながることを踏まえ、企業が情報開示に当たって**How-Toを参照可能**なものとする。

（※）セキュリティ対策の情報開示の促進により、民間企業の経営層が自社のセキュリティ対策の現状を認識し、また、他社の状況と比較することを通じて、さらに必要な具体的な対策を検討し、導入をするような循環のこと。

ガイドラインの活用主体

- ✓ **社会的評価の向上のための自主的・能動的な情報開示**に一定の関心のある民間企業

対象とする情報開示

- ✓ **開示書類**を通じた情報開示を取り扱う。
- ✓ 開示書類の読み手は、**投資家、融資元、顧客・契約者・取引先、従業員、競合他社等を含む、社会全体の広範なステークホルダー**を想定。

内容

- ✓ 既に世の中に存在する**実例**を挙げた上で、各企業が自らの情報開示の実施に当たって**参考になる項目例や記載の粒度等**を記載する。

その他

- ✓ 情報開示のための**インセンティブ**の在り方については**ガイドライン（仮称）と並行して議論**の機会を設ける。
- ✓ 情報開示の前提となる**民間企業のセキュリティ対策の促進**については、本ガイドライン（仮称）や本分科会では直接取り扱わず、**政策的な措置を別途**とりながら引き続き実施。

情報開示の基本的な考え方（案）

■ セキュリティ対策に関する情報開示は、例えば以下の性質を満たすのが望ましいと考えられる。

■ その上で、開示されている要素が多いほど、情報開示が進展していると捉えることとする。

セキュリティ対策の情報開示において満たすのが望ましい要件の例

当該要件については事例の検討・選定と並行して随時見直しを行う。

①目的適合性

- ✓ 投資家や契約者、利用者等の意思決定に影響を与え得る情報を提供すること。
- ✓ 記載事項の決定にあたっては、開示の目的を踏まえること。

②表現真正性

- ✓ セキュリティ対策等について、真実を忠実に表現すること。
- ✓ 情報の完全性、中立性、合理性を確保すること。

③比較可能性

- ✓ 同業種間・同規模等の一定の範囲で比較可能とするための基礎となる情報を提供すること。

④理解容易性

- ✓ 読み手に特別な専門知識がなくても理解できるように、簡潔かつ明瞭な表現で十分な情報を記載すること。

⑤適時公表性

- ✓ 利用者の意思決定に間に合うタイミングで公表すること。

➢ 公開方法：インターネットで閲覧・認知可能なのが望ましい。

情報開示の手段

■ 情報開示の手段として使用される書類は、その性質や想定される閲覧者によって、セキュリティ対策に関する記載内容や記載の文量に違いがある。

【各開示書類の記載内容の比較（※１）】

制度開示 ←→ 任意開示

開示書類	有価証券報告書 コーポレートガバナンス報告書	CSR報告書 サステナビリティ報告書	情報セキュリティ基本方針 情報セキュリティ報告書
記載量	**少ない**	**多い**	**セキュリティに特化**
閲覧者（想定）	✓ **投資家**の投資判断を支援することを主目的とするため、閲覧対象者が限られている。	✓ 企業の取組、姿勢等をブランディングし、企業信頼度を高めることを目的とするため、**一般的な顧客**を幅広く対象。	✓ 内容がセキュリティに限られており、**セキュリティの専門家等**を閲覧者として想定。
記載内容	✓ **リスク**としてのセキュリティや**企業統治**に必要な防止対策等、限定された項目・内容	✓ **主要５項目（※２）を中心に簡易で幅広い**記載内容	✓ **セキュリティ対策に関する包括的かつ具体的**な内容

（※１）あくまで大まかな傾向を記したものであり、必ずしも全ての事例が上述に分類されるとは限らないことに留意。また、上記以外にも開示書類は存在する。
（※２）①基本方針等の策定状況、②管理体制、③教育・人材育成、④社外との情報共有体制、⑤第三者評価・認証の５項目

（出典）企業のセキュリティ対策に係る情報開示の実態等に関する調査報告書（平成30年３月）をベースに総務省作成

段階ごとの開示の在り方について（案）

- セキュリティ対策に関する情報開示は、各企業における対策の成熟度や開示のモメンタムの大きさにより、いくつかの段階が想定される。
- 典型的にはサステナビリティ報告書や情報セキュリティ報告書等の事例の紹介を行うとともに、開示内容の第三者コメントやセキュリティ対策の認証取得等と組み合わせることで、外部からの信頼性の向上を促すことが適当。

第０段階

↓

第１段階

（開示又は対策の初期段階）

↓

第２段階

（開示又は対策が一定程度進展

↓

第３段階

（開示又は対策が相当程度進展

【各開示手段や開示内容の現状（※１）】

Security Action（※２）
【基本的なセキュリティ対策に係る簡易的な自己宣言】

有価証券報告書
【主にリスクについて記載】

CG報告書
【主に管理体制について記載】

CSR報告書/サステナビリティ報告書
【主要５項目（※３）を中心に記載】

情報セキュリティ基本方針

情報セキュリティ報告書（※４）
【セキュリティに関する包括的な開示書類】

インシデントに係る情報開示

グループ全体・サプライチェーン全体の情報開示

情報開示と組み合わせることを推奨

開示内容の第三者意見

セキュリティ対策の認証

・・・

（※１）あくまで大まかな傾向を記したものであり、必ずしも全ての事例が上述に分類されるとは限らないことに留意。また、上記以外にも開示書類は存在する。
（※２）Security Actionの宣言数は平成31年１月時点で62,365。
（※３）①基本方針等の策定状況、②管理体制、③教育・人材育成、④社外との情報共有体制、⑤第三者評価・認証の５項目。
（※４）情報セキュリティ報告書については、日経225の内で公開している企業は電気機器、通信企業の5社のみ（平成30年３月時点）。

情報開示分科会での主な論点（案）

論点１ **セキュリティ対策の情報開示とガイドライン（仮称）の考え方の整理**

→ ①情報開示の意義と、それを踏まえた②望ましいセキュリティ対策の情報開示の基本的な考え方は何か？
→ 今回策定するガイドライン（仮称）の趣旨・目的はどうあるべきか？
→ 望ましい情報開示のレベルは企業のセキュリティ対策の成熟度や開示へのモメンタムによって段階的に設定すべきではないか？
→ 掲載する実例については優良事例にすべきか、ベースラインの事例とすべきか、又は両方か？ 若しくは単なる参考事例とすべきか？
→ 「ガイドライン」、「マニュアル」、「手引き」等名称について配慮すべきではないか？

論点２ **ガイドライン（仮称）のメンテナンスの在り方**

→ 記載内容の更なる深掘りに対応したメンテナンスのプロセスやタイミングについて検討しておくべきではないか？

論点３ **書面での情報開示の真正性の確保**

→ 開示書類での情報開示の信憑性を高めるため、例えば開示書類の第三者意見やセキュリティ対策に関する認証（ISO27001やＰマーク等）を紹介・奨励することは適当か？

ガイドライン（仮称）の中身を検討する過程で議論し、ガイドライン（仮称）に反映

論点４ **情報開示を促すようなインセンティブの整理**

→ 企業が情報開示を行うインセンティブについて、実際の開示の事例を踏まえて整理すべきではないか？

インセンティブの回で議論

論点５ **ガイドライン（仮称）や情報開示の周知・啓発手段の検討**

→ ガイドライン（仮称）や情報開示の周知・啓発手段を検討すべきではないか？

普及方策の回で議論