資料２

企業経営で期待されるサイバーセキュリティの考え方（案）

平成 28 年６月２９日

内閣サイバーセキュリティセンター

○はじめに

IT（情報通信技術）の発展に伴って、経済・社会活動の大部分がインターネットに代表される、コンピュータ・ネットワークで処理されるようになった。電車に乗るにも、商品を買うにも、友人に連絡するにも、間違いなく IT の恩恵を受けている。企業が、これを有効に活用すれば、大幅なコストダウンとともに、顧客の行動パターンに合った新しいサービスの開発や、企業間取引など、ビジネスの革新が可能となる。逆に、この面で後れを取ると、競争優位を失うことにもなりかねないため、企業は IT にますます依存せざるを得なくなっている。

反面、こうしたビジネス・チャンスの陰では、サイバー攻撃などのリスクも増大するが、リスクをコントロールしつつ挑戦を続けることが重要となる。今後は、全てのモノがインターネットにつながる IoT（Internet of Things）システムが普及し、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するものと考えられる。

サイバーセキュリティリスクは目に見えないため、特別なものと見がちであるが、数あるリスク管理の一項目に過ぎない。また一般に、サイバーセキュリティを、やむを得ない「費用」と見る傾向があるが、より積極的な経営への「投資」と位置づけるべきである。言い換えれば、企業としての「挑戦」と、それに付随する「責任」として、サイバーセキュリティに取り組むことが期待される。

「責任」の面については、サイバーセキュリティリスクの管理も、会社法において取締役会の決議事項になっている「内部統制システム構築の基本方針」の中に含まれると考えられる。つまり、事業運営には IT の活用が不可欠になっていることから、サイバーセキュリティの確保は、企業が果たすべき社会的責任としての側面を併せ持つようになっている。

本文書は、企業がサイバーセキュリティの取り組む際に、昨年 9 月に閣議決定したサイバーセキュリティ戦略を踏まえ、昨年 12 月に経済産業省から発表された「サイバーセキュリティ経営ガイドライン」と併せて、経営層に期待される”認識“を示すとともに、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ことを目的にしている。

Ⅰ　基本的考え方

１．２つの基本的認識

サイバー空間における脅威の深刻化への対応として、事後追跡・再発防止及び今後生じ得る犯罪・脅威への対策を講じていく一方で、各企業においても、自ら進んで、意識・リテラシーを高め、主体的に取り組むことが必要である。特に、今後のビジネス環境の変化とサイバーセキュリティの関係を考慮すると、次のことを認識して、企業経営の中でサイバーセキュリティに取り組むことが重要である。

① 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、新しいものづくり戦略の一環として考えていく必要がある。
② 全てがつながる社会においては、サイバーセキュリティに取り組むことはいわば社会的なルールであり、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。

１―①　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、新しいものづくり戦略の一環として考えていく必要がある。

これまでも、IT の利活用により様々なビジネスの変革がもたらされたが、今後も企業は IoT システムを活用した新たなビジネスの創出や既存ビジネスの高度化を図る方向に向かうことが想定される。例えば、センサーを介し世界各地から集まるデータやノウハウを集約して、それを基にした製品・サービスの提供が進むことが考えられる。また、従来は交渉で決めていた企業間取引条件なども一定のルールの中でフレキシブルに、かつ自動運営されることも考えられる。

IT の利活用、IoT システムを積極的に取り入れる中で高いレベルのセキュリティ品質を実現していく取組は、企業価値や国際競争力の源泉となることが考えられる。

このため、経営者は、企業戦略において、サイバーセキュリティを、利益を生み出し、ビジネスモデルを革新する、新しいものづくり戦略の一環として考えていく必要がある。

１―② 全てがつながる社会においては、サイバーセキュリティに取り組むことはいわば社会的なルールであり、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。

IT が社会の基盤となり、既に企業は IT に依存しているが、今後は IoT の進展により、セキュリティ対策が十分されているか否かにかかわらず全てのものがつながる社会となることが予想される。

この場合、不十分なセキュリティ対策が原因で、個人情報等の流出をさせてしまった企業や、踏み台として狙われた企業は、意図せず、加害者側になってしまうリスクが発生し、管理責任を問われる場合がある。このようにシステムの一部の脆弱性が社会全体に重大な影響を及ぼすことがあるため、社会の一員として、サイバーセキュリティに取り組むことは、いわば社会的なルールであり、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ことを、各企業の経営者は認識すべきである。

２．３つの留意事項

IT が社会の基盤となる中、コーポレートガバナンスの一環としてセキュリティ対策を行うことは社会的な発展に寄与するとともに、自らの新しい企業戦略を担うものでもある。このため、社会の変化に合わせて、リスク分析、方針の策定、実施、評価、そして情報の開示という一連の仕組みを確立していくことが重要となる。その際、特に次のことに留意すべきである。

① リスクの一項目としてのサイバーセキュリティ
② 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
③ 情報発信による社会的評価の向上

２－①　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を分析し総合的に判断することが必要である。この際、これまでの判断基準に加えて、リスクの一項目としてのサイバーセキュリティの視点を忘れてはならない。これは経営の根幹にかかわることであるため、情報システム担当任せにするのでなく、新たな脅威への対処を先取りする真の「リスクマネジメント」として経営者がリーダーシップをもっ

て取り組む必要がある。

また、個人情報のみならず企業の営業秘密等の情報資産、企業ブランド、取引先との信頼関係、事業継続等の影響について検討し、総合的に判断していく必要がある。

２－②　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

より複雑に拡大していくサプライチェーンはビジネスの基盤となっていくが、これに参画しているビジネスパートナーやシステム管理の委託先などのほんの一部のセキュリティ対策が不十分であった場合でも、自社から提供した重要な情報が流出してしまうなどの問題が生じる。そのため、自社のみならず、ビジネスパートナーや委託先を含め、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が必要となる。その中で、海外も含めて一定レベルのセキュリティ対策が不可欠となる。また、サイバー攻撃が巧妙化する中、一企業のみで対策を行うには限界があることから、社会全体においてサイバー攻撃に対応した対策が可能になるよう、関係者間での情報共有活動への参加と、入手した情報を有効活用するための環境整備が必要となる。

２－③　情報発信による社会的評価の向上

新たなサービスを提供するに当たっては、市場における個人・企業が当該サービスに期待する品質の要素としての安全やセキュリティ、すなわち「セキュリティ品質」が保証されることが前提となる。セキュリティ対策を従来の問題解決策としてではなく、品質向上に有効な経営基盤の一つとして位置づけることで、こうした取組が企業価値の向上につながる。

また、関係者が各社のサイバーセキュリティへの対処状況を理解するために、企業からの情報発信も重要である。このため、例えば、一般に認知されている情報セキュリティ報告書、CSR 報告書、サステナビリティレポート、有価証券報告書やコーポレートガバナンス報告書等において、企業のサイバーセキュリティに係る取組等について積極的に示していくことは、企業価値を高める方法となると考えられる。

Ⅱ　企業の視点別の取組

社会全体が IT 化され、ネットワークでつながる中、各企業が「I.基本的な考え方」で示した認識や留意事項を踏まえて適切にセキュリティ対策を進めることが求められる。一方、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。

このため、本文書では、サイバーセキュリティに対する企業の視点別に次の３つに大別して、経営層に期待される認識や実装に向けたツールを示す。

① **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**
② **IT 化・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 化・サイバーセキュリティの重要性は理解しているものの、事業戦略に組み込むところまでは位置づけていない）
③ **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）

※①の企業は、②の企業が行うビジネスの基盤としてのセキュリティ対策に加えて、より高いレベルのセキュリティ品質を確保し、企業価値や国際競争力の向上につなげようとする企業を指す。なお、上述の分類は本文書において便宜的に分けたものであり、個別企業で見れば複数に該当する場合もあれば、どこにも分類することが困難な場合もある。

① 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

（経営層に期待される“認識”）

IT の利活用、IoT システムの積極的な取り入れなど新たなビジネスモデルの創出や既存ビジネスの高度化を目指す。この場合、データの積極的な活用に伴うリスクへの対応も含め、その製品・サービスの「セキュリティ品質」を一層高めるため、IoT システムの基盤におけるセキュリティの向上、データの保護、製品等の安全品質向上に取り組むことが必要である。その結果、高いレベルのセキュリティ品質の実現が、自社ブランド価値の向上につながることとなる。

さらに、企業活動において、株主をはじめとする様々な関係者との協働が重要となることから、法令に基づく開示を適切に行うことは勿論であるが、それ以外の情報提供にも主体的に取り組むことが期待される。その際、情報提供は、正確で、かつ利用者にとってわかりやすく有用性の高いものになることが期待される。

また、この分類となる企業群は、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日本、そして世界をリードし、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 社会に向けた環境整備の進展を踏まえて、安全な IoT システムの提供が期待される。このための一定の基準として、現在策定中の「IoT セキュリティのための一般的枠組」や「IoT セキュリティガイドライン」等を活用して、安全な IoT の実現に向けた製品・サービスへの取組が行われることが期待される。

●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

会社法においては、内部統制システム構築の基本方針を取締役会で決定することとなっているが、内部統制システムの構築・運用の一環として、自社のサイバーセキュリティに関する分掌と人材育成の現状を把握し、それを社外に向け情報発信していくことが期待される。また、上場会社は、コーポレートガバナンス・コードの考え方を踏まえ、取締役会全体の実効性について分析・評価することや、取締役・監査役に対する必要な知識の習得等の支援を行い、その結果を開示することとしているが、サイバーセキュリティに関しても、その中の 1 つとして実施していくことが期待される。

② **IT 化・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 化・サイバーセキュリティの重要性は理解しているものの、事業戦略に組み込むところまでは位置づけていない）

（経営層に期待される“認識”）

会社法において取締役会の決議事項になっている「内部統制システム構築の基本方針」の中にサイバーセキュリティリスクの管理も含まれると考えられる。つまり、事業運営には IT の活用が不可欠になっていることから、サイバーセキュリティの確保は、企業が果たすべき社会的責任としての側面を併せ持つようになっている。そのため、セキュリティ対策を担当者任せにするのでなく、経営者自らがリーダーシップをとって対策することが必要である。

また、取引データやシステムが企業や国境を越えて関係者と情報やデータを共有していくため、自社は勿論のこと、系列企業やサプライチェーンのビジネスパートナー、IT システム管理の委託先を含めたセキュリティ対策が必要である。

さらには、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リスクや対策、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要である。

（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」（平成 27 年 12 月経済産業省公表）

IT の利活用が企業の収益性向上に不可欠なものとなっている中で、経営者としての責任を果たしていくことが求められる。

こうした中で、「サイバーセキュリティ経営ガイドライン」では、体制の構築、攻撃を防ぐための事前対策、攻撃を受けた場合に備えた準備等について記載されており、これに基づきセキュリティ対策を実施することが期待される。

●企業等がセキュリティ対策に取り組む上でのリスク管理手法の活用

企業等がセキュリティ対策により積極的に取り組んでいくにあたり、そのためのインセンティブがあることが望まれる。このため、例えば、セキュリティ対策に取り組んでいることによって、サイバーセキュリティリスクに関する保険等での優遇が受けられる等の仕組みを活用していくことが考えられる。

●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開示

①のサイバーセキュリティを競争力強化に活用しようとしている企業に分類される企業と同様、コーポレートガバナンス・コードの考え方を踏まえ、サイバーセキュリティに関しても、取締役会全体の実効性について分析・評価することや、取締役・監査役に対する必要な知識の習得等の支援を行いその結果を開示することが期待される。

③ 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）

（経営層に期待される“認識”）

社会全体の IT 化が進む中、顧客に対する責任の観点から、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と考えられる。そうした中で、セキュリティ対策は不可欠であり、対策が不十分である場合には、顧客情報の流出等によって消費者や取引先との信頼関係を低下させ取引の機会損失につながるばかりでなく、踏み台になるなど、社会全体のセキュリティ低下にもつながる。そのため、経営層自らが積極的にサイバーセキュリティに関心を持ち取り組むべきである。

一方、中小企業等においては、様々な経営リスクがある中で使えるリソースには限界があることから、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べきである。

（実装に向けたツール）

●効率的なセキュリティ対策のサービスの利用

中小企業等においては、様々な経営リスクがある中で使えるリソースには限界があることから、基本的なウィルス対策ソフトの導入などに加えて、個別に高度なセキュリティ対策などを推進するのは困難であると考えられる。このため、関係者が連携して効率的なセキュリティ対策を行っていくことが期待される。そのためのツールの１つとして、中小企業向けクラウドサービスの利用が挙げられる。また、クラウドが千差万別であり、どのクラウドが適切であるかの判断をすることも難しいことから、例えば、公的な機関が一定の基準を満たしたクラウドを認定する等、適切なクラウドの選定に資する環境整備などを進めていく。また、意図せず残留するリスクや想定外のリスクに対する方策の１つとしてサイバーセキュリティリスクに関する保険等の活用も考えられる。

なお、効率的なサービスの利用を検討する際に、サイバーセキュリティは経営問題であり、現状を把握した上で、どのようなサービスを利用し対策を行っていくかの判断は経営者自らが行わなければならないとした原則を忘れてはならない。

●サイバーセキュリティに関する相談窓口やセミナー等の活用

セキュリティ対策は、身近な地域での活動や業種ごとのコミュニティなどを通じ、関係者が連携して取り組むことが重要である。このため、中小企業等が相談しやすい身近な相談窓口やサイバーセキュリティに関するセミナー等の活用、外部の専門家の有効活用等が期待される。

Ⅲ　今後の取組

経営層の認識を醸成していくためには、企業の規模、取り扱っている情報の性質やIT・セキュリティに対する認識も様々であることを踏まえるとともに、基礎的なところから段階的にそのレベルを向上させていく考え方が必要である。

このため、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においても、情報セキュリティ報告書、CSR 報告書、サステナビリティレポート、有価証券報告書やコーポレートガバナンス報告書等における情報発信の状況等、引き続き情勢の把握に努め、経営層の認識を高めるための推進方策等について引き続き検討する。