参考資料４

企業経営のためのサイバーセキュリティの考え方の策定について

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

本文書は、企業の経営層を対象に、グローバルな競争環境の変化の中でサイバーセキュリティをより積極的な経営への「投資」と位置づけ、企業の自発的な取組を促進するため、「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」（主査：林紘一郎 情報セキュリティ大学院大学教授、別紙１及び２を参照）を通じた検討を経て、企業経営のためのサイバーセキュリティに係る基本的な考え方を示したものである。また、各企業の視点に合わせた取組方法についてのガイド（経営層に期待される“認識”及び実装のためのツール）も掲げ、来るべきサイバー社会に向けた準備に利用されることを想定している。

内閣官房　内閣サイバーセキュリティセンターでは、経済界・産業界と連携しつつ、より多くの経営層に本文書を読んでいただけるよう、普及に向けた取組を行うこととする。また、本文書に関するフォローアップとして、企業のサイバーセキュリティに係る取組について、経営層の認識、情報発信の状況や関連する制度面の課題等の把握に努め、適時、本文書の見直しを行うとともに、経営層の認識を高めていくための推進方策等について検討する。

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

〇はじめに～サイバーセキュリティは、より積極的な経営への「投資」へ～

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。このことにより、電車や飛行機に乗ったり、商品やサービスを買ったりする形態が大きく変化するなど、消費者向けのビジネスは一変した。今度は、企業間取引の世界が変革されようとしている。グローバルに競争環境が変化している中で勝ち抜いていくためには、ITを有効に活用し、大幅なコストダウンのみならず、顧客のライフスタイルに合った新しいサービスの開発や、企業間取引など、ビジネスの革新を進めていくことが重要である。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。

こうしたビジネス・チャンスが拡大する一方で、サイバー攻撃などのリスクも増大するため、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、あらゆるモノがインターネットにつながり、そこから得られるデータにより新たなサービスを実現する IoT（Internet of Things）システムの普及によって、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。

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、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、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、企業の経営層が果たすべき責任の一つである。

本文書は、企業が自発的に行うサイバーセキュリティに対する取組が促進されるよう、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

１．二つの基本的認識

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、サイバーセキュリティに対する意識やリテラシーを高め、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 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。

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。

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めたデータやノウハウを基にした製品や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柔軟に、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[1]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。

[1] ここでは、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を指す。

このため、経営層は、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。

1―② 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。

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 システムの普及により、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、個人情報や取引先等から預かった機密情報等を流出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おそれがある。また、社会インフラの一端を担う企業においては、サイバー攻撃により意図せず業務が停止した場合、自社の損失にとどまらず地域や社会全体にも支障を来しかねない。このようにシステムの一部の脆弱性により、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ことを、各企業の経営層は認識すべきである。つまり、自社のサイバーセキュリティの取組が社会全体の発展に寄与し、社会全体の発展がひいては自社の発展にもつながるという、共通化構造を理解することが重要である。

2．三つの留意事項

IT が社会の基盤となる中、コーポレートガバナンス（企業統治）の一環としてセキュリティ対策を行うことは、新しい価値を創造するとともに、社会的な発展に寄与するものである。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、情報の開示、そして不断の見直し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 情報発信による社会的評価の向上
② リスクの一項目としてのサイバーセキュリティ
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

2－①　情報発信による社会的評価の向上

競争力のある新たな製品やサービスを提供するに当たっては、高いレベルの「セキュリティ品質」を確保することが前提となる。このためには、セキュリティ対策を従来の問題解決策としてではなく、品質向上等に有効な経営基盤の一つとして位置づけて取り組むことが必要である。

そして、自社のこうした取組に係る姿勢や方針について情報発信していくことで、関係者の理解が深まり、社会的評価を高めることとなる。情報発信の方法として、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の活用が挙げられる。また、その過程を通じて自社のリスク認識を高めることにもつながるものと考えられる。

2－②　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を分析し、残存リスクへの対処も含め、総合的に判断することが必要である。この際、これまでの経営判断の基準に加えて、リスクの一項目として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と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の流出による企業ブランド、取引先との信頼関係、事業継続等へ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。

2－③　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

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おそれがある。そのため、国内外を問わず、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一定レベルのサイバーセキュリティの確保が不可欠となる。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への対策が可能になるよう、セキュリティ対策の関係者間での情報共有活動への参加や、入手した情報を有効活用するための環境整備等が必要となる。

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三つに大別して、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**　（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）

② **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）

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**（主に中小企業等のうち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　（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、情報・データの積極的な活用に伴うリスクへの対応も含め、その製品やサービスの「セキュリティ品質」を一層高めるため、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、自社の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、様々な関係者との協働が重要となることから、法令等に基づく開示を適切に行うことは勿論であるが、それ以外にも自社のセキュリティ品質を高めるための取組に係る姿勢や方針等について主体的に情報提供に取り組むことが重要である。その際の情報提供は、正確で、利用者にとってわかりやすく、かつ有用性が高く悪用されにく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 システムを提供することが不可欠である。このため、「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 システムの実現に向けた製品やサービスへの取組が行われることが必要である。

●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

ブランド価値の向上のため、セキュリティ対策を品質向上等に有効な経営基盤の一つとして位置づけて取り組む姿勢や方針に関わる情報を、積極的に発信していくことが重要である。例えば、自社のサービスや製品を訴求していく際、差別化戦略としてセキュリティ品質を分かりやすく説明していくことも有効と考えられる。

なお、②の「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」における実装に向けたツールのうち、会社法における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基本方針を発信することや、コーポレートガバナンス・コード[2]に基づく取締役会の情報開示の監督機能の中で、サイバーセキュリティについても実施していくことも必要である。

---

[2] 平成 27 年 6 月に東京証券取引所が策定。会社が、株主をはじめ顧客・従業員・地域社会等の立場を踏まえた上で、透明・公正かつ迅速・果断な意思決定を行うための実効的な仕組の実現に資する原則を取りまとめたもの。

② **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、企業の経営層が果たすべき責任の一つである。そのため、経営者自らが、担当者任せにすることなくリーダーシップをとって、セキュリティ対策を講じることが必要である。

また、情報やデータが企業や国境を越えて共有されるよう、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、委託先を含めてのセキュリティ対策が必要となる。

さらには、平時及び緊急時のいずれにおいても、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」

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保険等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。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、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議することとなっている。また、上場会社においては、コーポレートガバナンス・コード の考え方を踏まえ、取締役会が、適時かつ正確な情報開示が行われるよう監督を行うこと、取締役会全体としての実効性に関する分析・評価すること、取締役・監査役に対する必要な知識の習得等の支援が行われていることを確認すること等が求められている。このような内部統制システムの構築・運用の一環として、サイバーセキュリティに関しても、基本方針を策定し、適切に情報開示等に取り組んでいくことが重要である。

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（主に中小企業等のうち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、顧客情報や取引先等から預かった機密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。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ためのサービスの利用

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、ウィルス対策ソフトの導入など基本的な取組に加えて、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。そのツールの一つとして、中小企業向けのセキュリティ対策が行われているクラウドサービスの利用が挙げられる。この際、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、公的な機関により一定の基準を満たしたとの認証を受けたクラウドを利用する等、適切なクラウドの選定が必要である。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一つとして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いうこと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、地域のセキュリティ相談員など外部の専門家の有効活用等が期待される。

また、リソースが限られていることから同様の課題を持つ同業他社や取引先等との協力関係を築くことも重要である。

Ⅲ　今後に向けて

IT の発展に伴い、今後、経営を取り巻く環境は大きく変化することが考えられ、それに合わせたサイバーセキュリティの対応が求められる。企業の経営層はこうした時代の変化と対応について、新たな認識を醸成していく必要がある。その際、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、本文書で示した認識やツールを参照して PDCA（Plan, Do, Check, Act）を回しつつ、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ことが必要である。

別紙１

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の設置について

（平成２７年１２月１４日
普及啓発・人材育成専門調査会会長決定）

１　サイバーセキュリティを事業戦略の一つとした企業経営について検討するため、普及啓発・人材育成専門調査会の下に、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（以下「WG」という。）を置く。

２　WGは、サイバーセキュリティを事業戦略の一つとした企業経営推進方策等について、調査検討を行う。

３　WGの委員は、２に掲げる事項について優れた見識を有する者であって内閣サイバーセキュリティセンターのセンター長が委嘱した者とする。

４　WGに主査を置く。WGの主査は、その委員の互選により決する。

５　WGの主査は、必要があると認めるときは、WGの委員以外の者に対し、WGの会議に出席して意見を述べることを求めることができる。

６　WGの庶務は、関係省庁の協力を得て、内閣官房において処理する。

７　WGは、その設置に係る調査検討が終了したときは、廃止されるものとする。

８　前各項に掲げるもののほか、WGの運営に関する事項その他必要な事項は、WGの主査が定める。

別紙２

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　委員名簿

主査	林　紘一郎	情報セキュリティ大学院大学　教授
委員	引頭　麻実	株式会社大和総研　専務理事
委員	大杉　謙一	中央大学　法科大学院　教授
委員	岡村　久道	英知法律事務所　弁護士
委員	落合　正人	SOMPOリスケアマネジメント株式会社　ERM事業部　部長
委員	野口　和彦	横浜国立大学　大学院　環境情報研究院　教授
委員	橋本　伊知郎	野村ホールディングス株式会社　参事　Co-CIO兼IT統括部長 野村證券株式会社　経営役
委員	丸山　満彦	デロイト トーマツ リスクサービス株式会社　代表取締役社長

（平成28年4月現在、五十音順、敬称略）

開催実績

第1回
日時：平成28年4月28日（木）
議題：（1）セキュリティマインドを持った企業経営に係る検討
　　（2）その他

第2回
日時：平成28年6月1日（水）
議題：（1）セキュリティマインドを持った企業経営に係る発表
　　（2）セキュリティマインドを持った企業経営WG取りまとめ骨子（案）
　　（3）その他

第3回
日時：平成28年6月29日（水）
議題：（1）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取りまとめ（案）
　　（2）その他