資料３

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)

本取りまとめは、今後のビジネスとサイバーセキュリティとの関係を考えるに際し、セキュリティ対策は、やむを得ない「費用」ではなく、より積極的な経営への「投資」である、との認識を醸成することを目的として、経営層に対して、その考え方を示すとともに、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。

【ビジネス環境の変化】

1. 経済社会のサイバー空間への依存度が高まり、企業活動をする上でITの利活用は避けて通れない。
2. 今後、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。
3. 安全な IoT システムを創出するための高いセキュリティ品質は、企業価値や国際競争力の源泉となる。

【サイバーセキュリティに対する認識】

1. サイバーセキュリティは生かし方次第で、利益を生み出し、ビジネスモデルを革新する方向に使えるものである。
2. サイバーセキュリティといえば個人情報漏えい対策、との認識では不十分である。サイバーセキュリティは、ビジネス上の大切な資産を守るものであり、顧客に重要性を理解してもらうため、情報資産、企業ブランド、事業継続、サプライチェーン全体の影響などについて検討していくことが必要である。

【企業のタイプ別の取組】

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から、本取りまとめでは、次の3つに大別して必要な取組を示す。

I. IoTを(グローバル)事業戦略上に位置づけ、セキュリティを積極的に競争力に位置づけている企業
II. IT化・セキュリティについて基盤として捉えている企業(概念的に、IT化・セキュリティの必要性は理解しているものの、積極的な活用までは位置づけられていない企業)
III. 事業上のリソースの観点から自らセキュリティ対策を行うことが困難な企業

Ⅰ. IoTを事業戦略上に位置づけ、セキュリティを積極的に競争力に位置づけている企業

（経営層に期待される“認識”）

1．IoT システムを活用した新たなビジネスモデルの創出や既存ビジネスの高度化に向け、データの積極的な活用も含めて、その製品・サービスの「セキュリティ品質」を一層高めるべく、プラットフォームのセキュリティ向上、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。高いレベルのセキュリティ品質の実現がブランド価値につながる。

2．IoT システムの提供するサービスの効用と比較して、セキュリティリスクを許容し得る程度まで低減していくことが課題となる。

3．機能保証の観点からリスク分析し、再発防止ではなく、先取りしたセキュリティ対策を実施していく。また、事業活動のセキュリティを確保するためには、個々の企業だけでなく、サプライチェーン全体のセキュリティを確保する必要がある。

（実装に向けたツール）

1．IoT セキュリティガイドライン（現在策定中）

IoT社会に向けた環境整備の進展を踏まえて、それらを活用し、安全な IoT システムの提供が期待される。

2．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

法令に基づく開示を適切に行うとともに、それ以外の情報提供にも主体的に取り組むことや、開示・提供される情報が株主との間で建設的な対話を行う上での基盤となることも踏まえ、そうした情報が正確で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。

Ⅱ. IT化・セキュリティについて基盤として捉えている企業

（経営層に期待される“認識”）

1．IT の利活用を推進する中で、サイバーセキュリティに対する認識を持って情報セキュリティガバナンスに取り組むことは、企業価値につながるだけでなく、社会的な責任を果たすものである。リスク管理として担当者任せにするのでなく、リスクマネジメントとして経営者自らがリーダーシップをとって対策すべきである。

2．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。

3．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）

1．「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）

これを踏まえ、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を実施していくことが重要である。

2．具体的な事案を踏まえたケース、情報共有の枠組みの構築等

具体的な事案を踏まえたケースを活用して、意思決定の手順や方法を訓練することが重要。また、情報の入手と提供という双方向の情報共有を通じて、社会全体でサイバー攻撃の防御につなげるために、企業間での情報共有の枠組みの構築が重要である。なお、具体的な事案を踏まえたケースの作成等を行い、企業等に情報提供を行っていく。

3. 企業等がサイバーセキュリティ対策に取り組むインセンティブ

例えば、サイバーセキュリティ対策に取り組んでいることによって、サイバーリスクに関する保険等での優遇等も考えられる。

Ⅲ. 事業上のリソースの観点から自らセキュリティ対策を行うことが困難な企業

（経営層に期待される“認識”）

1. 社会全体のIT化が進む中、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。
2. ITを活用して事業を行う際には、セキュリティ対策は不可欠であり、対策を行わないことは、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。
3. 一方で、事業上使えるリソースには限界があることから、効率的にすすめる方策を検討すべきである。

（実装に向けたツール）

1. 中小企業向けクラウドサービスの利用

事業上のリソースの関係から、自らセキュリティ対策等を推進するのは困難であり、セキュリティが確保されたクラウドの活用等を期待する。なお、クラウドが千差万別なため、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など、適切なクラウドの選定に資する環境整備等を進めていく。

2. サイバーリスクに関する保険

セキュリティ対策にかけられるリソースは限られていることから、リスク移転の方策の1つとしてサイバーリスクに関する保険等の活用が考えられる。

3. 中小企業等が相談しやすい相談窓口や、サイバーセキュリティに関するセミナー等

こうした取組は身近な地域での活動や業種ごとのコミュニティー形成が重要となる。

【今後の取組】

1. 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。
2. このため、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や有価証券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、具体的な事案を踏まえたケースの作成、情報発信についての検討など、経営層の認識を高めるための取組を推進する。