NISC National center of Incident readiness and Strategy for Cybersecurity

資料１－１

前回提示した論点及びこれまでの議論の整理について

平成３０年２月

内閣官房　内閣サイバーセキュリティセンター

１．論点（案）

１．ＩｏＴ、ＡＩ等の進展により、ビジネスにおいてＩＴの利活用が広がり、新しい価値を生み出していくことが求められる中、サイバーセキュリティに関連して**経営層が持つべき意識や、果たすべき役割**は何か？特に、**リスクマネジメントの一つとしてサイバーセキュリティを位置づけ**、組織全体で取組を進めていくにあたり、現時点の経営層の意識や役割はどのように評価すべきか。

２．経営層の意識改革や、経営層がリスクマネジメントの一つとしてサイバーセキュリティの取組を進めていく上で、**具体的な方策**として何をすべきか？特に、これまでの具体的な取組についてどのように評価し、**今後何に重点を置いて取り組むべきか**？

３．**中小企業をはじめとする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**について、今後どのような考え方で、具体的な取組を進めるべきか？特に、クラウドサービスの利用や、保険の活用によって、効率的な対策が進められないか？

４．セキュリティマインドを持った企業経営を推進するための**産学官連携による取組**が必要ではないか？

2. これまでの議論の整理（１）

１．経営層が持つべき意識や、果たすべき役割

- ＩＴを使ったビジネスイノベーションを進めていくと、新しいサイバーセキュリティリスクが出てくる。**経営の関心は、そのリスクを上回るリターンがあるかどうか**である。

- 経営層が、高いリターンを追求するためには、サイバー空間の不確実性という**リスクに積極的に向き合っていく意識が必要**である。具体的には、サイバー空間から得られる恩恵や利益（ベネフィット）と比較して、**リスク**（ネガティブなリスクだけでなく、ポジティブなリスクも含む）**を適切にコントロールしていく意識を持ち、ビジネスの判断することが必要**である。

- このため、**経営層には、リスクマネジメントのための最低限のＩＴやサイバーセキュリティに関する知識・能力が求められる**。例えば、**サイバー空間に関わるビジネスのベネフィットとリスクを説明できること**が求められる。

2. これまでの議論の整理（2）

2．経営層がリスクマネジメントの一つとしてサイバーセキュリティの取組を進めていく上での具体的な方策

a. 企業におけるサイバーセキュリティの位置づけ

- 企業におけるサイバーセキュリティの位置づけは、分野や業態によって大きく違う。これは、対象とするリスクそのものや、リスク基準・レベルが違うことが原因である。このため、それぞれの業態や組織形態に応じて、**ビジネス戦略におけるサイバーセキュリティの位置づけを明確にし、自然な形で会社のメカニズムに入っていくようにすることが重要**である。
- その際、分野や業態によっては、過去の事故事例をもとにした再発防止的な対応だけでなく、**ビジネス戦略の企画と一体となって**イメージを膨らませながら、**今後起こりうる事象を考えながら対応**することが必要となる可能性がある。
- サイバーセキュリティ事案は、企業グループの端で発生したものが全体に波及し、風評被害も含めて親会社が被るような問題になるので、**どのようにサプライチェーン全体を統制していくのかの検討が必要**である。

2. これまでの議論の整理（3）

b. 経営層への訴求に向けた具体的方策

- サイバーセキュリティの各項目について、**経営層、技術者それぞれの対応すべきことを明確にし、そのためのツールを整備することが必要**である。品質管理、環境、サイバーセキュリティなど個々のリスクへの対応が各分野の技術者によって実施される中で、経営者は、技術者の成果を参考に「判断」することが求められている。ここで、経営者と個々のリスクへの対応を行う技術者の間の刷り合わせが重要になってくる。
- このため、**他のリスク要因同様、サイバーセキュリティリスクを「想定内」のリスクにしていくための試行錯誤が必要**である。そのためには、経営層に対し、現実的な脅威の例示に留まらず、**確率的には低いが発生しうる事象も含めて、判断を迫ることが有効**である。
- 法規制の下でのコンプライアンスに訴える強制的なアプローチは、経営者には劇薬としてすぐに効くものの、副作用がある。具体的には、事業に不釣合いなサイバーセキュリティが強制された場合、経営資源の無駄遣いとなり、イノベーションの阻害要因にもなりうる。また、**特色あるリスクテイクによって、新しい価値・イノベーションが生み出せるよう、一定の自由度が必要**である。このため、サイバーセキュリティリスクに対する強制的なアプローチについては慎重に検討すべき。

2. これまでの議論の整理（４）

３．中小企業をはじめとする事業上のリソースの制約が大きい企業の対策

- 中小企業をカテゴライズした上での対応を考えるべき。例えば、
  ①グループ企業は、ホールディングスでガバナンスを効かせる
  ②大企業と取引のある中小企業は、大企業の方が取引先としての中小企業を指導する（サプライチェーン管理）
  ③規制業種（例えば観光業やタクシー業）は、どの中小企業も業務が似通っているので、数社でクラウドサービスつくり、そこに入ってもらう
  ④その他の中小企業は、社会全体に悪影響を与えないよう普及啓発を図る
  といった対応が挙げられる。

- 中小企業対策を個々の企業、社会全体のどちらが困るからやるのか、考え方の整理が必要。