NISC National center of Incident readiness and Strategy for Cybersecurity

資料２－１
(一部抜粋)

企業経営のための
サイバーセキュリティについて

平成２９年１０月

内閣官房　内閣サイバーセキュリティセンター

1．経緯（1）

- **「サイバーセキュリティ戦略」（平成27年9月）**を踏まえ、セキュリティ対策は「費用」ではなく「投資」であるとの認識の醸成等の経営層の意識改革や、経営能力を高めるサイバーセキュリティ人材の育成、経営層のリーダーシップの下での組織能力の向上など、**セキュリティマインドを持った企業経営**を推進。
- 同戦略を踏まえ、ＮＩＳＣでは、経営層に期待される認識等を示した**「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）**を策定。また、**「サイバーセキュリティ人材育成プログラム」（平成29年4月）**においては、本ワーキンググループを通じ、**産業界と連携しつつ、経営層のサイバーセキュリティに関する認識や課題の把握と、その解決に向けた取組の検討**を行うことが示された。
- さらに、サイバーセキュリティ戦略本部においても**「サイバーセキュリティ戦略中間レビュー」（平成29年7月）**を決定し、**経営層の意識改革を促すための取組や、中小企業のセキュリティを効率的に高めるための方策の検討・取組**を進めていくことが示された。

【サイバーセキュリティ戦略（平成27年9月）】(要約)

5.1.2 セキュリティマインドを持った企業経営の推進

セキュリティリスクの適切な把握・投資判断や、製品・サービスへのセキュリティ機能の実装、組織能力の向上が必要。

(1)経営層の意識改革

- セキュリティ対策は「費用」ではなく「投資」であるとの認識の醸成。
- サイバーセキュリティの取組が市場等から正当に評価される仕組みや財務面で有利となる仕組みの構築、認識醸成のための官民一体となった啓発活動。
- 経営層におけるCISOの機能の位置づけ推進。

(2)経営能力を高めるサイバーセキュリティ人材の育成

- 橋渡し人材層の育成の推進。
- キャリアパスを考慮した人材育成・人事評価、経営層への訴求。

(3)組織能力の向上

- セキュリティ・バイ・デザイン、リスク分析に基づく組織運営、サプライチェーン対策の推進。
- CSIRTの設置・運用、迅速な対応・復旧に向けた計画やツールの整備、演習の実施、対外説明機能の強化等。
- 経営層のリーダーシップの下での体制整備、有効な対策、情報開示等の在り方についてガイドライン等により企業に対して発信。第三者認証等により客観的に評価される仕組みを確立。
- 民民間・官民間における一層の情報共有網の拡充。

1．経緯（2）

【サイバーセキュリティ人材育成プログラム（平成29年4月）】

○ 企業の経営層におけるサイバーセキュリティに係る基本的な考え方の普及

NISCは、「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」（中略）を通じ、企業のサイバーセキュリティに係る取組について、産業界と連携しつつ、経営層の認識や有価証券報告書をはじめとした情報発信の状況や法律・税制を含めた関連する制度面の課題等の把握に努めるとともに、シンポジウムの開催等を通じ、経営層の認識を高めていくための普及啓発を含めた推進方策等課題の解決に資する取組について検討する。

【サイバーセキュリティ戦略中間レビュー（平成29年7月）】

○ 会社法等の企業経営に係る制度や訴訟・コンプライアンス対応におけるサイバーセキュリティの関わり方等について検討を進め、経営層の意識改革を促すための取組を行う。

○ 中小企業等においては、サイバーセキュリティ対策に使えるリソースに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の検討が必要である。特に、クラウドサービスの活用等、中小企業のセキュリティを実質的に高めるための取組を行う。

2．本WGの主な検討事項

次期「サイバーセキュリティ戦略」を念頭に、**企業経営とサイバーセキュリティに関する現状や関連する取組を把握**するとともに、**経営層の意識改革促進の方策や中小企業のセキュリティ対策、産学官の取組の方向性等について検討**を行い、**「企業経営のためのサイバーセキュリティの考え方」の内容を充実**することとしたい。

- 「企業経営のためのサイバーセキュリティの考え方」（28年８月）策定後の**企業経営に関するサイバーセキュリティを取り巻く動向**（経営者の意識、情報開示の状況、米国における動向等）やこれまでの**官民の取組を把握**する。

- **リスクマネジメント確保のための組織体制の在り方**について、各企業の事業規模・内容やＩＴ利活用の度合い、サイバーセキュリティに対する認識の違いなどを意識しつつ、検討する。（施策間ＷＧの議論と連携）

- **経営層の意識改革促進の方策**（例：会社法における内部統制システム、コーポレートガバナンス・コード等の考え方を踏まえた情報発信の在り方、情報セキュリティ格付制度などの「見える化」の取組）を検討する。

- **中小企業におけるセキュリティ確保の方策**（例：セキュアなクラウドの利用）を検討する。

- セキュリティマインドを持った企業経営を推進できるような**産学官連携による取組の方向性**について検討する。

→上記の内容を踏まえ、**「企業経営のためのサイバーセキュリティの考え方」の内容を充実**するとともに、その内容を、**次期「サイバーセキュリティ戦略」**に反映していく。

3．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？

今後のスケジュール(案)