Keidanren
Policy & Action

Cybersecurity by All

# 全員参加による
# サイバーセキュリティの実現に向けて
# 【概要】

2021年7月13日

一般社団法人
日本経済団体連合会

# 目次

# Ⅰ．はじめに

Keidanren
Policy & Action

## サイバーセキュリティをめぐる主な環境変化

① 業種を問わないDX（デジタル・トランスフォーメーション）が浸透
② 新型コロナウイルス感染拡大に伴う急激なテレワークへの移行
③ サプライチェーンを経由したサイバー攻撃の増加
④ 国家間における地政学的緊張の高まり

こうした状況を踏まえ…

「次期サイバーセキュリティ戦略」骨子においては、
「Cybersecurity for All～誰も取り残さないサイバーセキュリティ」
というコンセプトを提示

Cybersecurity for Allに加えて、
**誰もが主体的に危機意識を持って取り組む**
**（Cybersecurity by All）が重要**

# ２．全員参加によるサイバーセキュリティの実現に向けた３つの視点

Keidanren
Policy & Action

□ Cybersecurity by Allの実現に向けては、各主体の役割発揮、人材育成・研究開発力強化、社会の変化への対応といった視点から、取組みの推進が必要

**視点１　各主体の果たすべき役割**

① 国による率先垂範
② サイバーセキュリティ経営のさらなる推進
③ サプライチェーン全体での取組み強化
④ 官民一体での社会風土醸成

**視点２　人材育成・研究開発力強化**

① 全員参加の人材教育
② 産業・国際競争力の強化
③ サイバー空間の信頼性確保への貢献

**視点３　社会の変化に対応した取組みの推進**

① 連携の強化
② 重要インフラの分野の相互依存関係の分析および新規分野の追加
③ 既存制度の検証

# （１）各主体の果たすべき役割
## ①　国による率先垂範

Keidanren
Policy & Action

- わが国全体のサイバーセキュリティの強化にあたっては、**国が率先垂範してサイバーセキュリティに取り組む**ことが重要
- 国際動向を踏まえた国の取組みを示すことで、**企業や地方公共団体が国を参考としつつ対策を講じ**、国全体のサイバーセキュリティが強化されるよう期待

**国際動向も踏まえた取組みの提示**


**国を参考にセキュリティ対策を実施**


**わが国全体のサイバーセキュリティが強化**

# （１）各主体の果たすべき役割
# ②　サイバーセキュリティ経営のさらなる推進

Keidanren
Policy & Action

- サイバーセキュリティは経営課題であり、**各企業の自主的な取組み**が重要
- 経団連としても、自主的な取組み推進を期待するとともに、サイバーセキュリティ対策の取組みレベル可視化、情報発信の重要性等について**引き続き周知活動を実施**


DECLARATION OF CYBER SECURITY MANAGEMENT
経団連サイバーセキュリティ経営宣言

2018年3月

一般社団法人 日本経済団体連合会

最新テクノロジーとデータを活用して社会全体の生産性向上と課題解決を図る「Society 5.0」に向け、あらゆる場面でITとの融合が進む一方、サイバー空間の秩序や安全に脅威を与える、著しい悪意を持った行為も多発している。いまやすべての企業にとって価値創造とリスクマネジメントの両面からサイバーセキュリティ対策に努めることが経営の重要課題となっている。

重要インフラの多くを担い、さまざまな製品やサービスを提供する経済界は、主体的に対策を講じる必要性を強く自覚する。

経済界は、全員参加でサイバーセキュリティ対策を推進し、安心・安全なサイバー空間の構築に貢献する。サイバー攻撃が激化する2020年の東京オリンピック・パラリンピック競技大会までを重点取り組み期間として、以下の事項の実践に努めることを宣言する。

1 経営課題としての認識
- 経営者自らが最新情勢への理解を深めることを怠らず、サイバーセキュリティを投資と位置づけて積極的な経営に取り組む。
- 経営者自らが現実を直視してリスクと向き合い、経営の重要課題として認識し、経営者としてのリーダーシップを発揮しつつ、自らの責任で対策に取り組む。

2 経営方針の策定と意思表明
- 特定・防御だけでなく、検知・対応・復旧も重視したうえで、経営方針やインシデントからの早期回復に向けたBCP(事業継続計画)の策定を行う。
- 経営者が率先して社内外のステークホルダーに意思表明を行うとともに、認識するリスクとそれに応じた取り組みを各種報告書に自主的に記載するなど開示に努める。

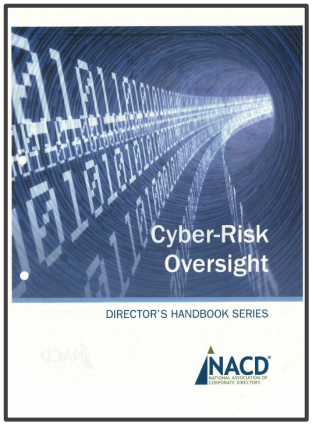
3 社内外体制の構築・対策の実施
- 予算・人員等のリソースを十分に確保するとともに、社内体制を整え、人的・技術的・物理的等の必要な対策を講じる。
- 経営・企画管理・技術者・従業員の各層における人材育成と必要な教育を行う。
- 取引先や委託先、海外も含めたサプライチェーン対策に努める。

4 対策を講じた製品・システムやサービスの社会への普及
- 製品・システムやサービスの開発・設計・製造・提供をはじめとするさまざまな事業活動において、サイバーセキュリティ対策に努める。

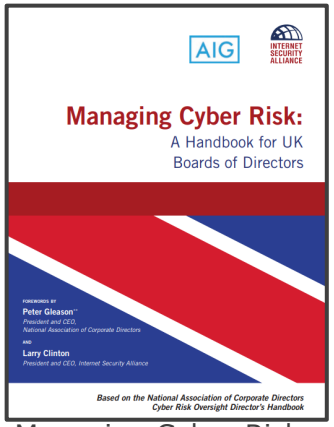
5 安心・安全なエコシステムの構築への貢献
- 関係官庁・組織・団体等との連携のもと、各自の積極的な情報提供による情報共有や国内外における対話、人的ネットワーク構築を図る。
- 各種情報を踏まえた対策に関して注意喚起することによって、社会全体のサイバーセキュリティ強化に寄与する。

DECLARATION OF CYBER SECURITY MANAGEMENT

経団連サイバーセキュリティ経営宣言
（2018年3月）




Cyber Risk Oversight Director's Handbook



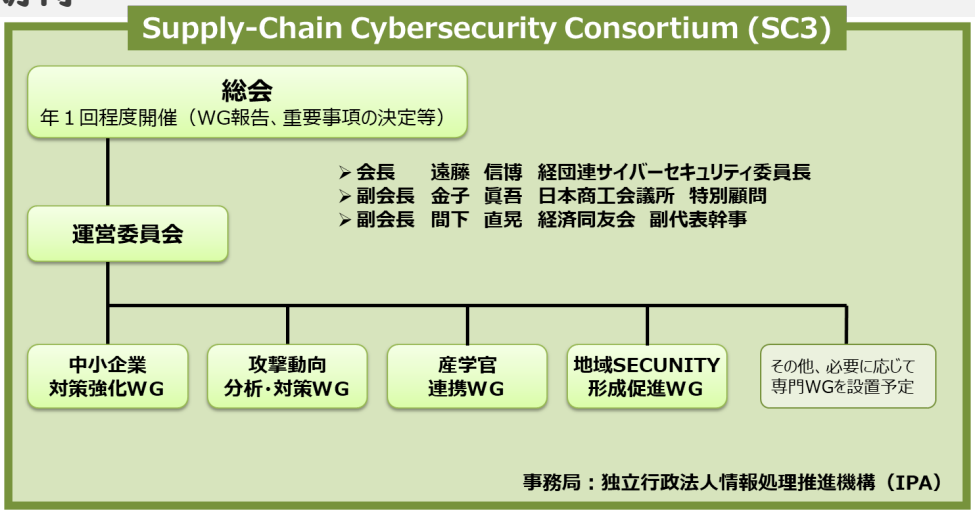

Managing Cyber Risk:
A Handbook for
UK Boards of Directors


経団連サイバーリスクハンドブック
（2019年10月）

# （１）各主体の果たすべき役割
## ③　サプライチェーン全体での取組み強化

Keidanren
Policy & Action

□ サプライチェーン・サイバーセキュリティ・コンソーシアム(SC3)を通じて、企業規模・業界の枠を超えた活動、地域単位でのセキュリティ・コミュニティが形成されるとともに、企業の規模・業種に応じた具体的取組みが示され、中小企業を中心としたサプライチェーン・サイバーセキュリティが強化されることを期待




［出典］情報処理推進機構 ホームページの情報を一部加工

## ④　官民一体での社会風土醸成

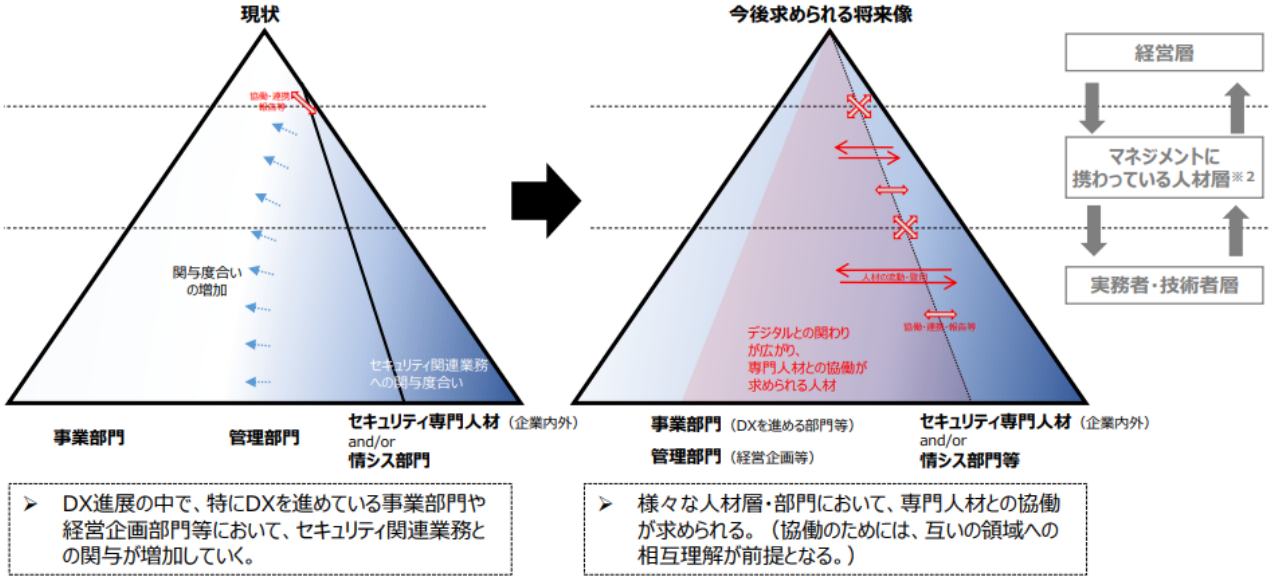
□ 被害者を過度に批判することは、適切な情報公開や迅速な行動を妨げる要因
□ 被害者を過度に責めない社会風土醸成に向け、一般市民を含む関係者への広報活動に官民一体で、取り組むことが重要

# （２）人材育成・研究開発力強化
## ①　全員参加の人材教育

Keidanren
Policy & Action

- わが国全体のサイバーセキュリティを高めるには、社会の全構成員に向けた、**セキュリティリテラシー教育**が重要
- DXの推進に際しては、IT・セキュリティ専門人材と協働するうえで必要な**「プラス・セキュリティ知識」**を役職・部門に関わらず習得するとともに、人材のエコシステム形成に向けて、産学官の連携が重要


＋




**リテラシー教育**

**「プラス・セキュリティ知識」の習得**

［出典］内閣サイバーセキュリティセンター
インターネットの安全・安心ハンドブック

［出典］内閣サイバーセキュリティセンター　普及啓発・人材育成専門調査会　資料より抜粋

# （２）人材育成・研究開発力強化
# ②　産業・国際競争力の強化

Keidanren
Policy & Action

- サイバーセキュリティの研究開発推進にあたっては、「Beyond 5G」をはじめとする新たな社会基盤を安全に構築することへの貢献、新たな価値を生み出すと同時にサイバー空間上の脅威になり得る技術（例：AI、量子技術）への対応が必要
- 上記領域は市場のポテンシャルが高いだけでなく、安全保障にも関わる重要な領域
- わが国が研究開発・事業化を推進し、国際的にリードする立場となるため、国際標準化の対応も重要

中長期トレンドを見据えた
研究開発

＋

国際標準化の対応を推進

研究開発・事業化において
わが国が国際的にリードする立場へ

# （２）人材育成・研究開発力強化
# ③　サイバー空間の信頼性確保への貢献

Keidanren
Policy & Action

- サイバー空間の信頼性確保にあたっては、使用する製品・サービスの信頼性が確保されていることが前提
- IoT製品の一般家庭への普及も進んでいることから、「セキュリティ・バイ・デザイン」の考えのもと、製品の設計・製造段階からセキュリティを意識し、製品のライフサイクルを通じて信頼性を高め続けることが不可欠
- 政府は企業等の迅速なセキュリティ対策の実行を促すため、わが国の技術を用いた信頼性の高い製品・サービスに関する情報を明らかにするとともに適切な使用に関するガイドライン等を整備すべき

信頼性が確保された製品・
サービスの製造・保守

導入・展開支援により
サイバー空間の信頼性を確保

# （３）社会の変化に対応した取組みの推進
## ①　連携の強化

Keidanren
Policy & Action

- サイバー攻撃が高度化、深刻化し、地政学的緊張がサイバー空間にも波及しつつあるなか、**被害発生時に迅速に情報共有・対処が可能となる体制を構築**することが重要
- 関係府省庁および関係組織のさらなる連携ならび**サイバー攻撃の予測・特定・対処能力の強化**を図るとともに、サイバー攻撃を受けた際の報告先・相談窓口の一元化、物理的セキュリティとの連携（出入国管理、捜査、監視等）を促進すべき
- 情報共有等の前提となる、**関係者の信頼性を担保する仕組みの検討**が必要

# （３）社会の変化に対応した取組みの推進

## ②　重要インフラ分野の相互依存関係の分析および新規分野の追加

- 重要インフラ分野は生活インフラを中心に１４分野が対象
- サイバー空間とフィジカル空間の融合が進み、分野を超えて事業者間の相互依存関係が深まっている現代、サイバー攻撃に備え、**各分野の相互依存関係を分析**するとともに、**新たな重要インフラ分野の追加を検討**すべき


＋


［出典］内閣サイバーセキュリティセンター重要インフラの情報セキュリティ対策に係る第４次行動計画（概要）

## ③　既存制度の検証

- 全員参加によるサイバーセキュリティを実現するためには、対策を実施する側に必要以上の負担をかけず、効果的な対策を可能とする態勢を整えておくことが重要
- 既存の**施策・枠組み・法制度について、不要なもの、改めるべきものがないか不断に検証**すべき

# 3．おわりに

Keidanren
Policy & Action

サイバー空間とフィジカル空間の垣根が低くなり、
サイバー空間にも地政学的緊張が波及している昨今、
サイバーセキュリティの重要性はますます増大

サイバーセキュリティはDXを推進し、
Society 5.0を実現するための根幹

サイバー空間の信頼性確保に向け、
経団連としては、引き続き取組みを強化