

セキュリティマインドを持った企業経営WG

Society 5.0 実現に向けた
サイバーセキュリティの強化

2018年 2月 9日

一般社団法人 日本経済団体連合会

Society 5.0の実現に向けた サイバーセキュリティの強化を求める (2017年12月12日公表)



ダウンロードはこちら

I はじめに

～経緯とねらい～

II 基本的な視点

1. 価値創造
2. 危機管理

III 具体的に 取り組むべき事項

1. 意識改革
2. リソース確保
 - (1) 人材育成
 - (2) 情報共有
 - (3) 技術対策
 - (4) 投資促進
3. 推進体制の整備
 - (1) 政府関連組織の整備・連携
 - (2) 企業内外の体制整備
4. 法制度・規範の整備
 - (1) 国内法制度
 - (2) 技術標準
 - (3) 国際規範

IV 経団連 アクションプラン

1. 経営層の理解促進
2. 広報・周知活動
3. 国際連携

V おわりに

～オリパラに向けて～

経緯とねらい

経団連は2015年・16年の二度にわたって
サイバーセキュリティ対策の強化を提言

2017年11月には企業行動憲章を改定
サイバー攻撃対策を社会的責任として行うと明言

サイバー攻撃の被害は世界中のあらゆる組織に
広がるなど新たな段階に突入



あらゆる企業や組織の具体的な取り組みと
関係者の連携を推し進めるため、改めて提言

Society 5.0時代のサイバーセキュリティ

あらゆるモノがつながり価値が生まれる反面、サイバー攻撃の対象が増加し、リスクも高まる。



二つの視点

価値創造

“Society 5.0”時代にサイバー空間で価値を創出する際の前提

- ◆サイバーセキュリティが競争力になる時代
- ◆グローバル市場でのビジネス環境確保

危機管理

サイバー攻撃対策を怠れば事業継続が困難となり、関係者・市民に大きな影響を与える可能性

- ◆自然災害と同様に避けられないものと認識
- ◆事業継続の観点が重要

サイバーセキュリティ対策の全体像

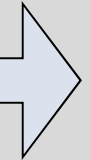
取り組む姿勢

自助

共助

公助

国際連携



意識改革とリソースの確保

意識改革



+

人材育成



情報共有



資源循環の
エコシステム

投資促進



技術対策



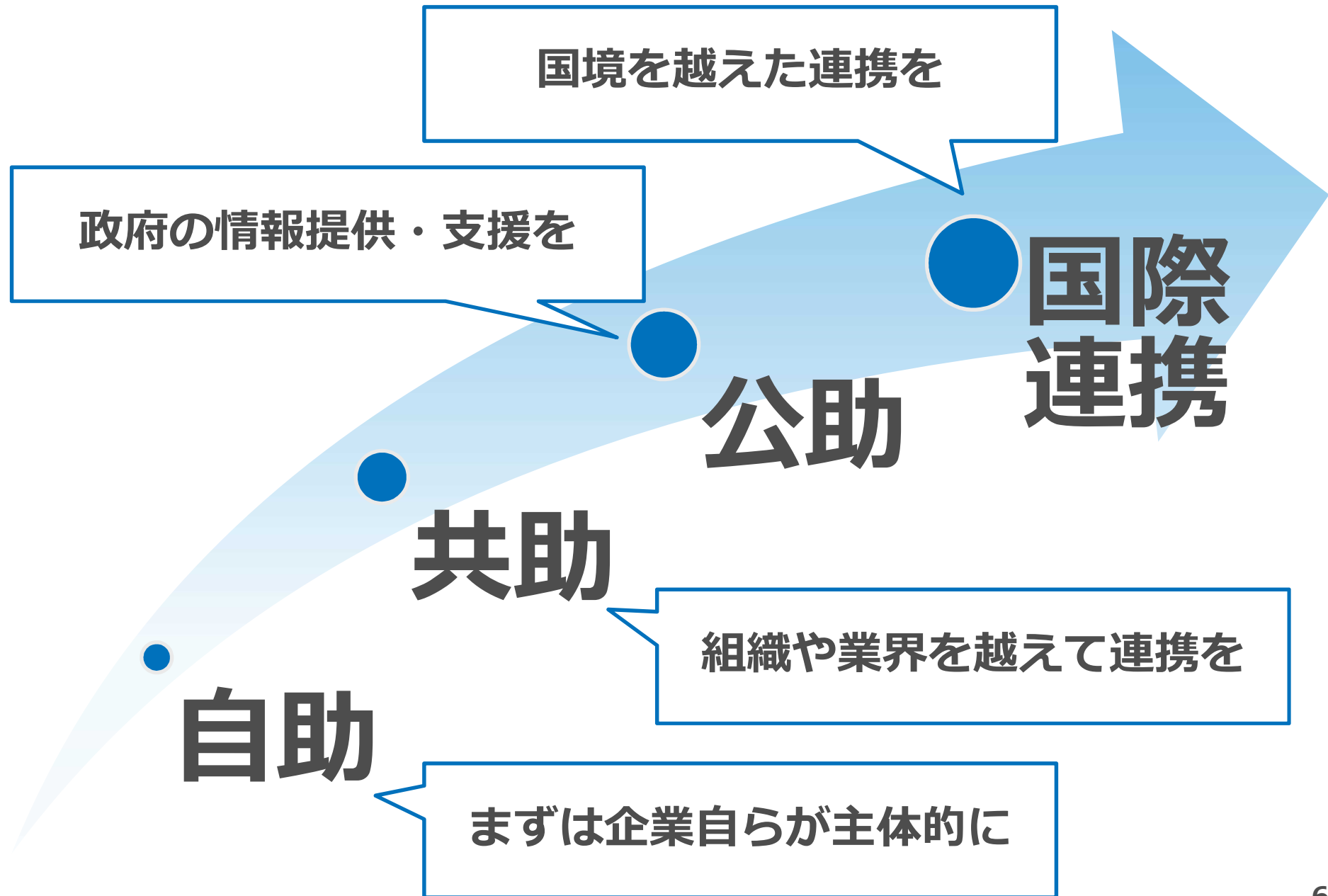
基盤となる体制整備

政府体制

企業体制

法制度・規範

サイバーセキュリティ対策に取り組む姿勢



具体的に行うべき事項

意識改革



- ✓ 国民全体の意識向上
- ✓ セキュリティ・バイ・デザイン
- ✓ 経営者の意識改革
- ✓ 被害を受けた企業を責めない社会風土

具体的に行うべき事項

- ✓ 全体のリテラシー向上
- ✓ 若年層の人材発掘
- ✓ 専門人材への教育、キャリアパス提供

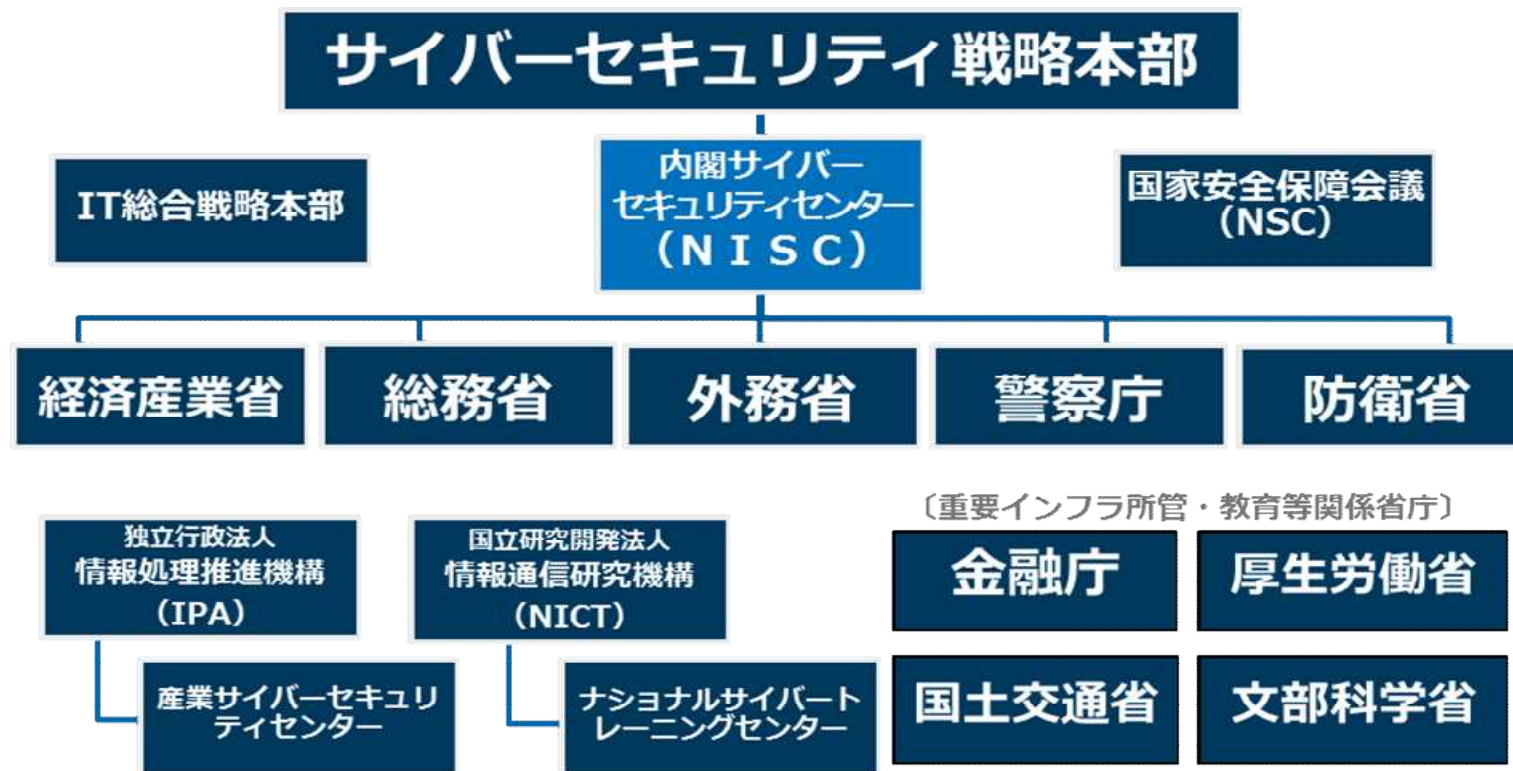
- ✓ 情報の類型整理
- ✓ 情報共有の枠組み
- ✓ 政府の情報提供
- ✓ 国際連携



- ✓ 官民で投資拡大
- ✓ 組織設立
- ✓ 税・補助金支援
- ✓ 政府予算拡大

- ✓ 各組織での対策
- ✓ 中小企業クラウド化
- ✓ 技術開発
- ✓ 国際標準化

政府の組織連携・施策の一体化



- ✓政策が各省でバラバラのため、一体化が必要
 - ✓司令塔組織として、NISCの機能強化を図るべき
- ↓
- ✓将来的には、各省に散在する情報関連政策を一元的に所管する機関の創設が必要

その他の体制整備

企業内外

- ✓セキュリティ担当役員や対応組織の設置
- ✓早期回復に向けたBCP(事業継続計画)等の策定
- ✓委託先や取引先も含めたサプライチェーン全体のサイバーセキュリティ管理

法制度

- ✓技術の進歩に合わせた法制度・規範の対応
- ✓不正アクセス禁止法等の必要十分な見直し
- ✓国際的に通用する技術標準等の策定
- ✓国際規範の策定に積極的に参加・主導

経団連アクションプラン

1 経営層の理解促進に向けたAction

- 🎯 『経団連サイバーセキュリティ経営宣言』の策定
- 🎯 経営者向けセミナー・研修・合宿の実施



2 周知・広報に関するAction

- 🎯 各社のサイバーセキュリティ対策の実態調査
- 🎯 機関誌や説明会・講師派遣等を通じた広報・周知
- 🎯 政府・各団体におけるイベントへの協力
- 🎯 国内外のステークホルダーへの情報発信



3 国際連携の推進に向けたAction

- 🎯 国際会合への参加
- 🎯 世界経済フォーラム（WEF）等との連携

