資料４

Keidanren
Policy & Action

JCIC
Japan Cybersecurity Innovation Committee

経営視点と人材育成・活用

2020年 1月 15日

経団連　サイバーセキュリティ強化ＷＧ　主査
日本サイバーセキュリティ・イノベーション委員会　代表理事　　梶浦敏範

経団連　サイバーセキュリティ委員会

▼ 2019年5月30日に発足
▼ 約170社が加盟（2019年11月時点）

サイバーセキュリティ委員会

委員長：　遠藤　信博　日本電気会長

委員長：　金子　眞吾　凸版印刷会長

サイバーセキュリティ強化WG

※旧「情報通信委員会 サイバーセキュリティに関する懇親会」の後継

主査：　梶浦　敏範　日立製作所上席研究員

経団連サイバーセキュリティ委員会　近年の提言等

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

Society 5.0実現に向け、2017年12月に
改めて**サイバーセキュリティ対策の強化を提言**

経営層の覚悟表明と理解促進に向けたアクションプラン
として**「経団連サイバーセキュリティ経営宣言」を策定**

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 ＋

基盤となる体制整備

政府体制　企業体制　法制度・規範

経団連サイバーセキュリティ宣言のポイント

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・復旧も重視した上で、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

- 2020年の**東京オリンピックまでを重点取組み期間**として、サイバーセキュリティ経営を宣言。
- 経済界が一丸となり、**全員参加**で対策を推進することを明記。
- **「Society 5.0」での価値創造**に向けた前向きな投資としてサイバーセキュリティ対策に取り組む重要性を指摘。
- サプライチェーンの対策や積極的な情報共有、国際連携などを通じて、社会全体のサイバーセキュリティ強化に貢献する点を強調。

サイバーセキュリティ委員会での検討事項 ①成熟度の可視化

セキュリティ対策の可視化

サイバーセキュリティは経営課題である

- 自社対策は十分か？
- ｻﾌﾟﾗｲﾁｪｰﾝ上の他社の対策は？
- セキュリティ人材の採用
- 株式市場へのアピール

サイバーセキュリティ **成熟度の可視化**

成熟度の開示

サイバーセキュリティ委員会での検討事項 ②人材の可視化

人材の可視化

セキュリティ人材の不足

そもそも、どこにどれだけの人材が不足しているか明らかになっていない

↓

人材定義を使用したサイバーセキュリティ人材の可視化

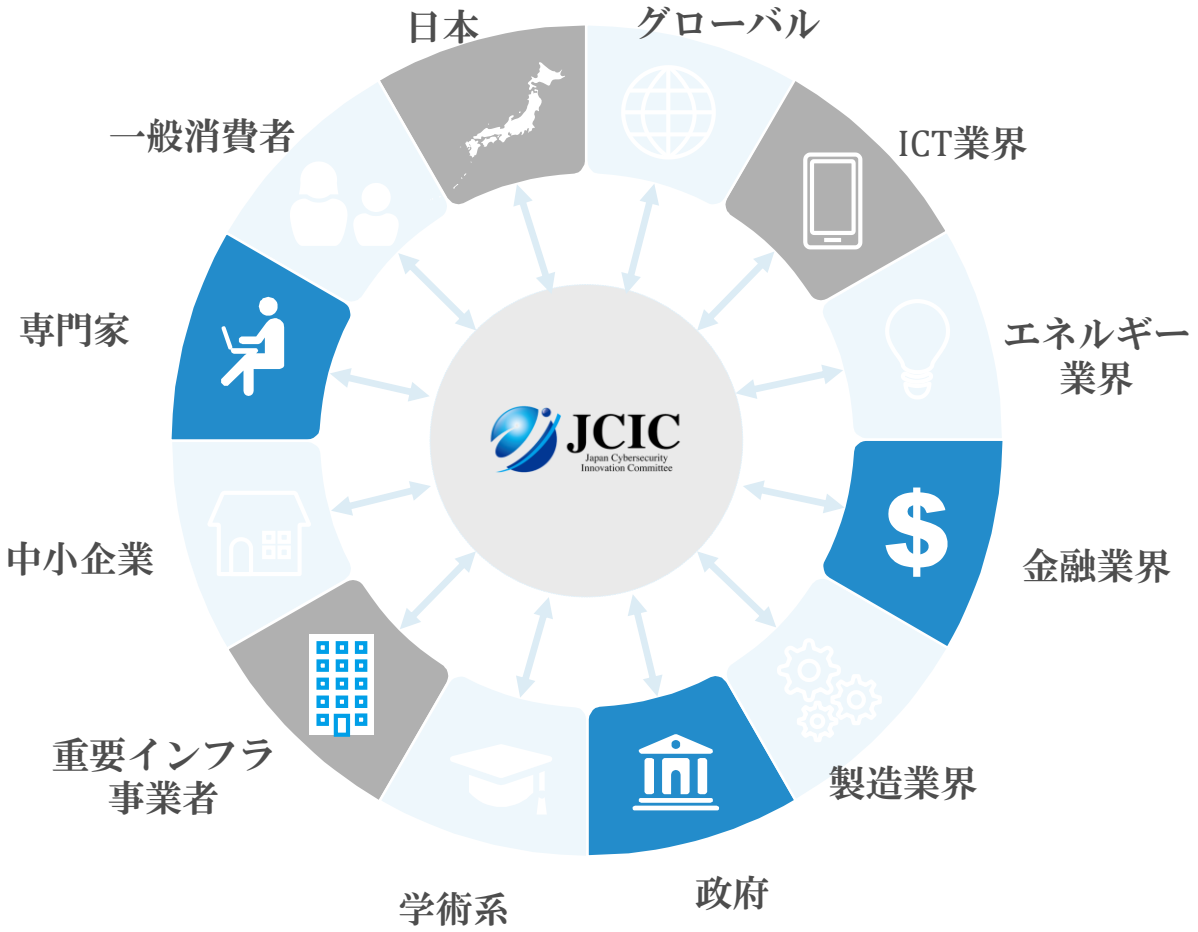
CRIC-CSF「IT人材/OT人材の定義」、ISEPA「JTAG」等

↓

・企業は、適材適所へ人材配置・採用が可能に
・個人は、キャリアパス開発に利用
・人材の質×量から企業のセキュリティ耐力を推量

日本サイバーセキュリティ・イノベーション委員会

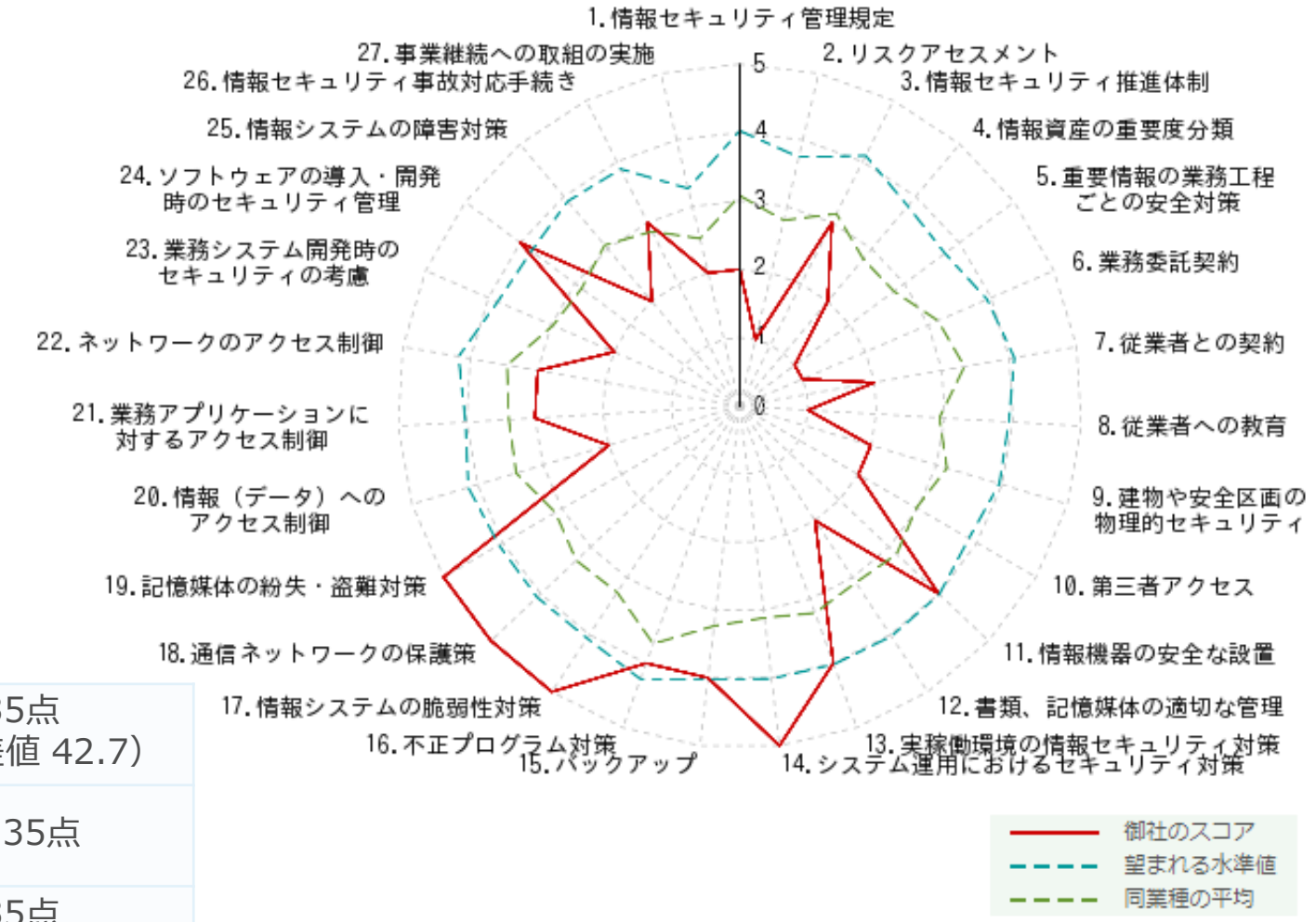
日本唯一の専門シンクタンク



事務所所在地	〒107-0062 東京都港区南青山2-2-8DFビル 6F
設立年月日	2017年11月
代表理事	梶浦 敏範 (株式会社日立製作所上席研究員(ICT政策)；日本経済団体連合会サイバーセキュリティに関する懇談会座長)
会員企業	26社＋オブザーバー3団体
URL	https://www.j-cic.com/

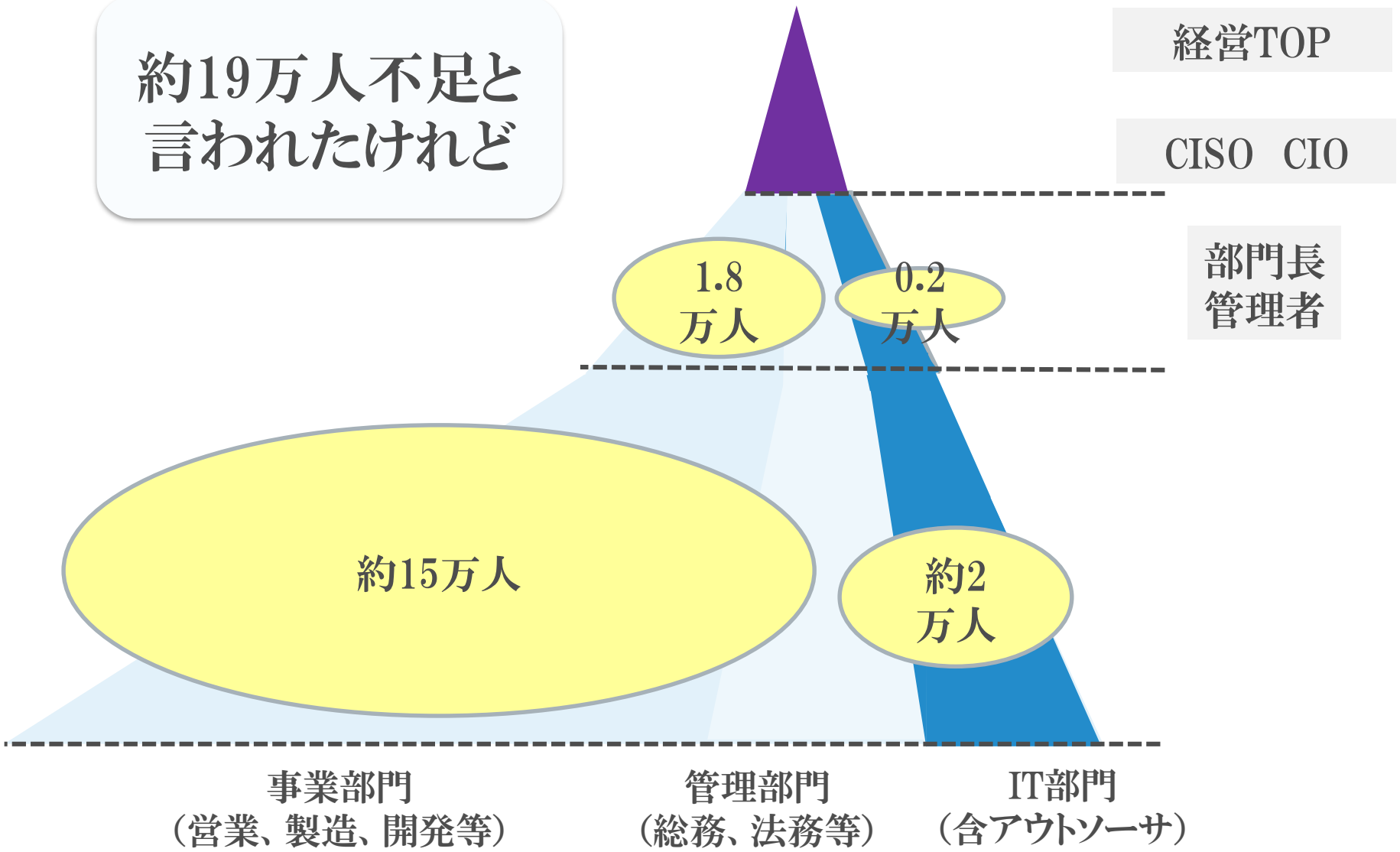
経営者からの見える化

ベンチマークで自社の位置を確認



当社のスコア	76/135点 （偏差値 42.7）
同業種に望まれる水準値	107/135点
同業種の平均	84/135点

人材の見える化


約19万人不足と
言われたけれど
経営TOP
CISO　CIO
部門長
管理者
1.8
万人
0.2
万人
約15万人
約2
万人
事業部門
（営業、製造、開発等）
管理部門
（総務、法務等）
IT部門
（含アウトソーサ）

人材育成・活用のための検討

行政

③’行政における人材キャリアパスを示す。

④　評価機関の立ち上げを（公式・非公式に）支援する。

⑤‘ 教育機関からのインターンを受け入れる。

⑧　企業・団体の規模や特性に応じて、雇用する人材の質×量（例：ポイント数）の推奨値を示す。

産業界

①　勉強会を立ち上げ、人材に求められる要件を示す。

③’企業における人材キャリアパスを示す。

④　評価機関の立ち上げを、資金面含め支援する。

⑤　教育機関に必要な資源（講師・実験の場等）を提供する仕組みを導入する。

⑤‘ 教育機関からのインターンを受け入れる。

推進コア機関

評価機関

③　評価機関（例：NPO）を立ち上げ、人材の見える化制度を検討する。例えばスキルをある数値（ポイント）で示す。（現行制度の整理を含め）

⑦　人材評価・登録制度を整備し、人材情報を提供する。

教育機関

②　情報セキュリティ全般に関わる研究会を立ち上げ、要件を満たすためのカリキュラム等を検討する。

⑥　カリキュラムを大学間共有する仕組みを導入し、教育課程を実施する。