KEIZAI DOYUKAI

「Cyber Security Everywhere」時代

～経営者の８つのアクションと政府への６つの提言～

委員長：伊藤　穣一　（デジタルガレージ　取締役・千葉工業大学　学長）
上野山　勝也（PKSHA Technology 代表取締役）
鈴木　国正　（インテル　取締役会長）

2024年10月23日（水）
公益社団法人　経済同友会

Ⅰ．提言の検討の視点、ターゲット

検討の視点

・地政学の地殻変動の1つになるロシアのウクライナ侵攻において、武力攻撃の前に衛星通信システムや変電所にサイバー攻撃
・すでに中国や北朝鮮からの攻撃があり、特に北朝鮮の弾道ミサイル開発には日本国内へのサイバー攻撃により搾取された資金の一部流入

サイバー攻撃は一段と巧妙化、高度化、複雑化、組織化

・持続的な賃上げ、金利のある世界の回帰など長らく止まっていた経済成長のエンジンが、ようやく、動き出す兆し
・再び成長の果実を掴み取るための足かせになる、深刻な人手不足・人材不足の常態化

デジタル技術を活用したDXが不可欠

あらゆる場面でサイバー攻撃の脅威と対峙する

「Cyber Security Everywhere」時代へ

提言のターゲット（誰に向けた提言か）

・影響度が大きい大企業を中心とした企業経営者が行動すべき8つの提言、政府が進めるべき6つの提言の**2つの視点**で意見を述べる。

２．現状認識

- 外部要因として①アタックサーフェイスの増加②サイバー犯罪エコシステムの複雑化③IT及びAI発展による攻撃の高度化④地政学リスクが顕在化しており、サイバー攻撃リスクは高まり続けている。

現状認識

①　アタックサーフェイスの増加

情報システムやクラウドの利用が広がり、2024年には

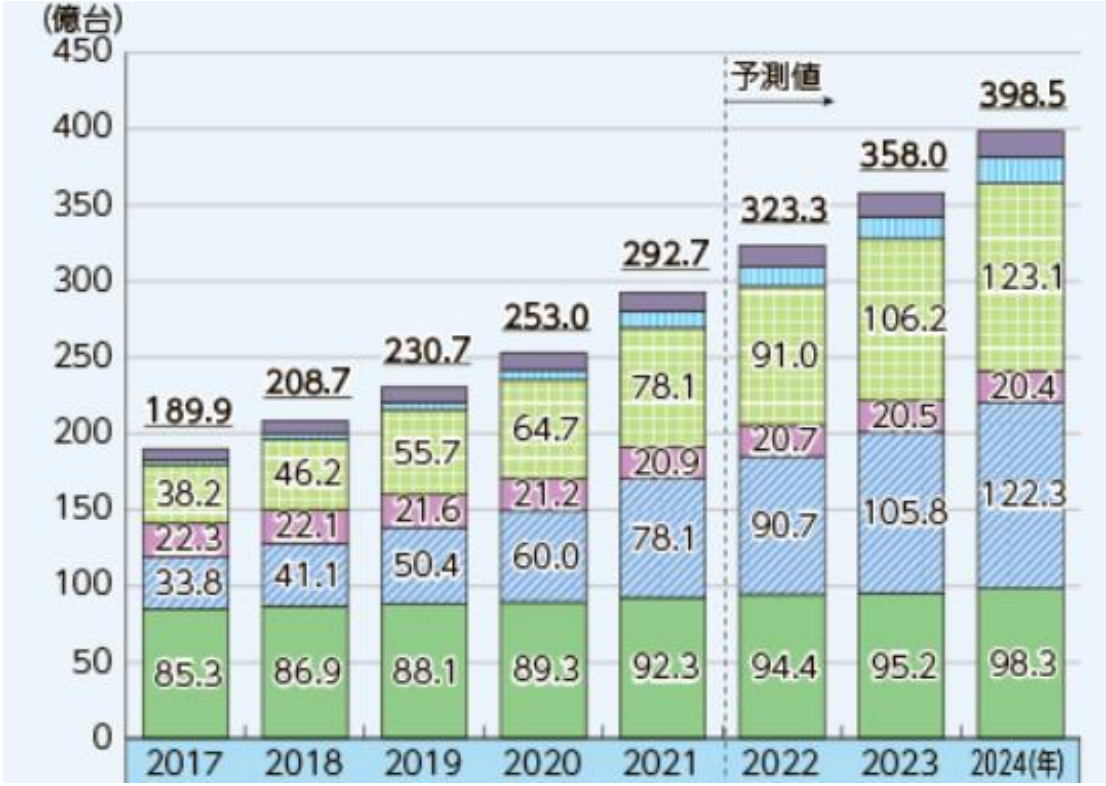
IoTデバイスが2019年の1.7倍に増加見込み

② サイバー犯罪エコシステムの成熟化・複雑化

③ IT及びAI発展による攻撃の高度化

④ 地政学リスクの高まり

【アタックサーフェイスの増加】



＜出所＞令和4年情報通信白書　世界のIoTデバイス数の推移と予測

２．現状認識

- サイバー攻撃の件数が増加、サービス停止・廃止、セキュリティ人材不足など経営者として経営課題の重要度は増しつづけている。

現状認識

＋

- 着実にDX が企業に浸透
- サイバーセキュリティ対策の関心高まり

－

- **サイバー攻撃の件数は年々増加傾向**

2023年のサイバー攻撃関連の通信数（パケット）の年間総数は約6,197億パケットと過去最高の通信数を記録

- **サービス停止・廃止の現実**

サイバーセキュリティ対策を怠ると、不正アクセス等による機密情報や流失だけでなく、本業のサービス停止、廃止の現実は起こっている。

- **サイバーセキュリティ人材不足**

【サイバー攻撃関連の通信数（パケット）】

＜出所＞令和6年情報通信白書　サイバー攻撃関連の通信数の推移

【サイバーセキュリティ等の具体的な被害】

企業種別	概要	結果
小売業	不十分な認証機能が原因で不正チャージや利用が発生	サービス廃止
エンタメ業	主力サービス群のサーバーを標的にしたサイバー攻撃	1カ月以上サービス停止

＜出所＞各種報道により事務局作成

３．現状認識からの３つの課題

- 「Cyber Security Everywhere」時代における現状認識から3つの課題に整理した。

現状認識

アタックサーフェイスの増加
サイバー犯罪エコシステムの成熟化
IT及びAI発展による攻撃の高度化
地政学リスクの高まり

【認識すべき世界】
「Cyber Security Everywhere」時代

＋ 着実にDX が企業に浸透
サイバーセキュリティ対策
の関心高まり
（大企業・中小企業含む）

－ サイバー攻撃の件数は年々増加
サービス停止・廃止の現実
サイバーセキュリティ人材不足

3つの課題

１．サイバーセキュリティは経営課題、常時有事対応

- 「Cyber Security Everywhere」の時代においては、サイバーセキュリティは**重要な経営課題と位置づける**ため、経営トップは**守りから攻めへの転換**を図る。
- **CISO等の体制づくり**を行い、経営トップは常に有事捉え、迅速かつ効果的に対応できる組織、リスク把握を行い、しなやかに推進する。

２．ガバナンス強化

- サイバーセキュリティのガバナンス強化ため、**専門性のある取締役における議論とモニタリング**が必要である。
- またそれを支えるために**リスクの見える化・数値化、インシデントを想定した計画策定**、さらに予算面では**ITとセキュリティ予算の独立**が重要である。
- 中長期的な議論と投資を図り、変化する脅威に柔軟に対応する。

３．人材育成・獲得

- サイバーセキュリティを支える人材強化を図るため、自社戦略に基づきサイバーセキュリティに必要な**人材を定義**することが重要である。
- 人材確保のための**制度や情報発信**とともに体系的なトレーニングを提供して強いセキュリティ体制を構築する。

４．経営者の８つのアクションポイント

3つの課題

１．サイバーセキュリティは経営課題、常時有事対応

- 「Cyber Security Everywhere」の時代においては、サイバーセキュリティは**重要な経営課題と位置づける**ため、経営トップは**守りから攻めへの転換**を図る。
- **CISO等の体制づくり**を行い、経営トップは常に有事捉え、迅速かつ効果的に対応できる組織、リスク把握を行い、しなやかに推進する。

２．ガバナンス強化

- 企業のガバナンス強化ため、**専門性のある取締役における議論とモニタリング**が必要である。
- またそれを支えるために**リスクの見える化・数値化、インシデントを想定した計画策定**、さらに予算面では**ITとセキュリティ予算の独立**が重要である。
- 中長期的な議論と投資を図り、変化する脅威に柔軟に対応する。

３．人材育成・獲得

- サイバーセキュリティを支える人材強化を図るため、自社戦略に基づきサイバーセキュリティに必要な**人材を定義**することが重要である。
- 人材確保のための**制度や情報発信**とともに体系的なトレーニングを提供して強いセキュリティ体制を構築する。

経営者が取り組むべき8つのアクション

①サイバーセキュリティを成長のドライバーへ

経営者はサイバーセキュリティを経営の重要課題とし、成長のドライバーと考える。

②体制強化

日本企業のCISO設置率は43%と低く、経営者はCISOの重要性を理解し、積極的な配置とともに、密なコミュニケーションが必要である。

③専門性のある取締役における議論・モニタリング

取締役会に知見ある人材を配置し、定期的に議論・モニタリングして意見を反映させる。

④リスクの見える化・数値化

自社のアセットを見える化し、被害リスクを数値化して影響度を把握する。

⑤リスク対応計画策定

自社の事業戦略や価値をもとに、優先順位とリスクの影響度を鑑みて、複数のリスク対応計画を策定する。

⑥予算の独立化

脅威は増えることがあっても減ることはないことを前提に、IT予算とセキュリティ予算の独立化を行う。

⑦人材の定義化

自社の戦略に基づき、サイバーセキュリティ人材定義を行う。

⑧人材の育成・獲得

「シン・日本型雇用システム」導入など、人材の制度・報酬体系を整えるとともに、海外人材の獲得や人材育成実践の場を検討

５．政府への６つの提言ポイント

- 経営者の取り組むべき8つのアクションやグローバルの動向を踏まえて、政府への６つの提言を示す。

テーマ	提言内容
①能動的サイバー防御・NISCの司令塔機能強化	• 「Cyber Security Everywhere」の時代となった現実がある中、安全保障や重大なサイバー攻撃の恐れのある場合、未然に排除、侵害拡大を防止する**能動的サイバー防御を早期に導入すべきである。** • そのために、官民連携の強化、情報通信の利用、アクセス・無害化について速やかに取り組むべきである。 • 内閣サイバーセキュリティセンター（NISC）は、**司令塔機能の強化が必須**である。 • NISCを中心に各府省庁と連携をこれまで以上にできるように、各府省庁のサイバーセキュリティ部門人材をNISCへ兼務することや各府省庁のサイバーセキュリティ部門が**物理的に同じ執務室で協働することも検討すべき**である。
②重要インフラ事業者への報告義務化・新たな官民連携組織の創設 **※参考資料**	• サイバーセキュリティにおいて情報は最も重要なファクターである。そのため**重要インフラ事業者への報告義務化を早期に導入するべきである。** **＜新たな官民連携の在り方＞** • 新たな官民連携の組織体は**「give and take」の概念**を念頭、情報収集・提供、インシデント対応支援等を行う。また**定期的な会合、ワークショップ、官民の人材交流など信頼関係の構築を図るべきである**。 • 組織設置にあたっては、米国の共同サイバー防衛連携（JCDC）、英国のインダストリー100（i100）、豪州のサイバー脅威情報共有 (CTIS)など諸外国の事例は大いに参考にするべきである。 **＜情報提供の内容・方法＞** • 民間へ提供する情報は経営層の意識決定に有用な情報提供を実施すべきである。例えば、**攻撃者の主体・目的・背景、攻撃の緊急度・重要度、攻撃の被害想定・波及効果、初期対応や中長期の対応方法**がある。 • セキュリティ・クリアランス制度を活用し、情報提供においても十分に活用すべきである。 • インデント報告は現状、各業法やガイドライン等に基づき、各事業者の監督省庁へ行われているが、リアルタイム性が欠けている。そのため**インシデント報告先の一元化**を行うべきである。 • また監督省庁等により、報告内容が異なり、自由記述の箇所が多く、さらにはWordやExcelでの形式である。そこで**報告フォーマットの統一に加えて、報告や集約が一元化できる仕組みを構築し、効率性を上げるべきである**。

５．政府への６つの提言ポイント

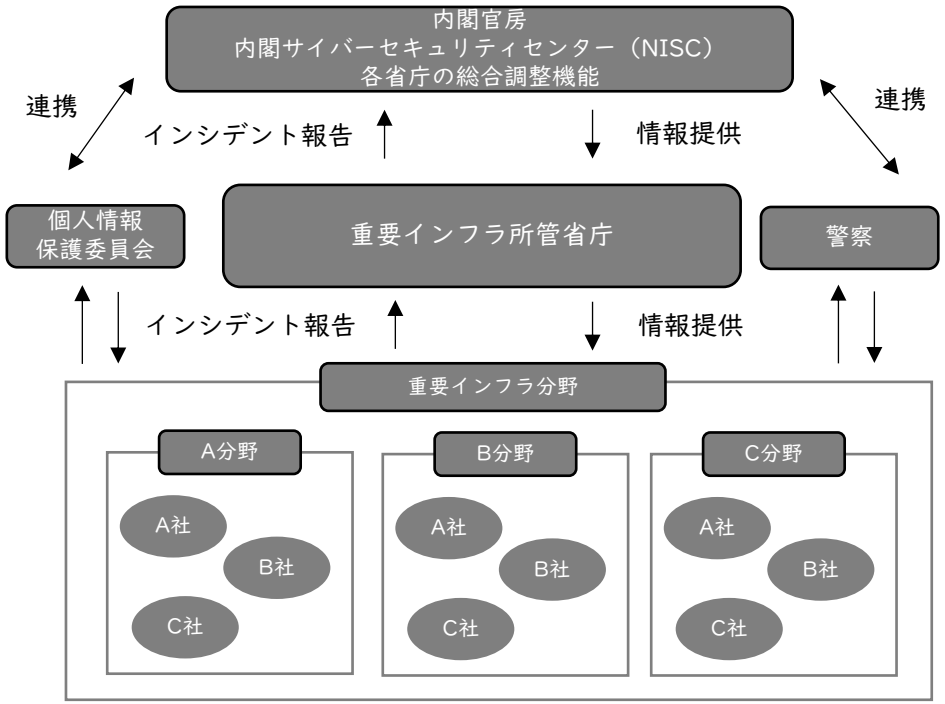
テーマ	提言内容
③人材育成	＜サイバーセキュリティ人材定義と可視化＞ • 人材定義の可視化が重要である。サイバーセキュリティの人材強化における産官学の共通認識をするためにも、諸外国の事例や国内の動きを参考に、**政府主導で人材定義の可視化を検討すべきである**。また人材定義の可視化とともに教育機関と連携する必要がある。米国や欧州等の諸外国の事例は多いに参考するべき。 ＜教育機関の質と量の拡充＞ • サイバーセキュリティのリテラシー向上や人材育成・確保の視点からも**初等教育段階から中等教育までセキュリティ教育をすべきである**。 • **民間人材を活用**し、生徒の指導と共に教員の研修など知識・スキル向上を行うべきである。 • セキュリティ人材の即戦力、さらにはCISOなどのトップ人材を増やすべく、**高専、大学、大学院の人材において質、量を広げる必要がある**。例えば、豪州で導入しているサイバーアカデミーを参考にサイバーセキュリティを専門に学べる仕組みを検討すべきである。
④情報開示	• サイバーセキュリティに関する重要情報の正確かつタイムリーな開示（適時開示）を行うことを念頭に、**有価証券報告書への記載義務を検討するべきである**。またコーポレートガバナンスコードにサイバーセキュリティに関する方針策定を記載するべきである。
⑤サイバーセキュリティ産業の振興	• **高品質な国産セキュリティ製品、サービス供給を強化すべきである。**さらに、それらを海外展開し、その利益を新たな研究開発や人材育成に充当するなどのエコシステムを構築する。 • 加えて耐量子計算機暗号への対応もする必要があるため、政府主導で民間ともに取り組みについてのロードマップを描くべきである。
⑥サイバー保険	• **政府主導でデータ集約、分析等、サイバー保険によるリスク評価の枠組みとしての選択肢を作るべきである**。

（参考）新たな官民連携組織のイメージ

- NISCがサイバーセキュリティの司令塔機能となり、**新たな官民連携の枠組みを構築**。新たな枠組みは会合、インシデント対応、人材交流等とともに、報告先の一元化、報告内容・形式の統一化、作業の効率化を実現

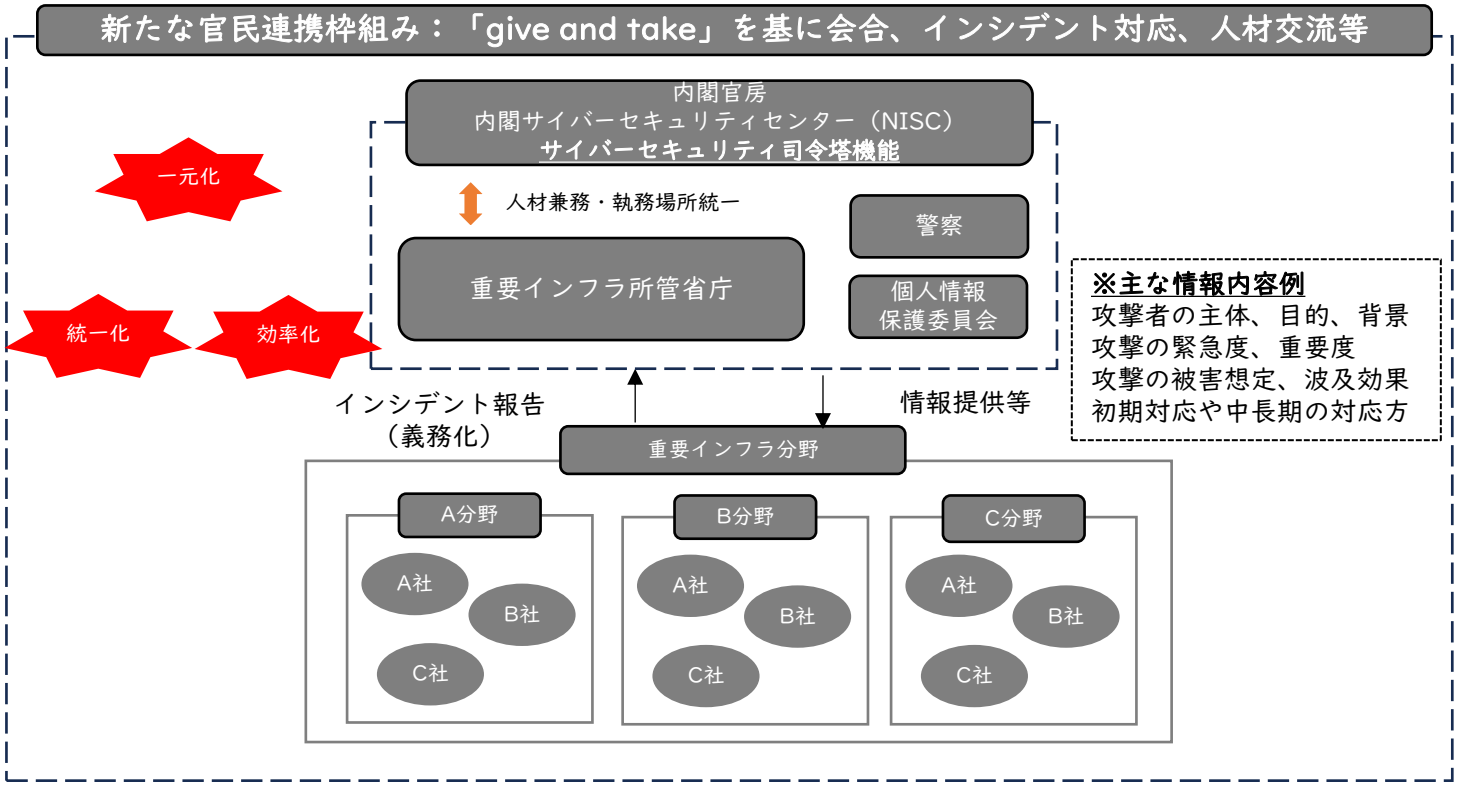
＜現状＞

重要インフラサービス・システムの不具合
（法令等報告対象の事象）



・サイバーセキュリティにおける司令塔機能の不在
・インシデント報告のリアルタイム性の不足
・報告内容や報告フォーマットのばらつき、手作業の存在

＜今後＞



・NISCがサイバーセキュリティ司令塔機能
・インシデント報告の**一元化**によるリアルタイム性の向上
・報告内容や報告形式の**統一化**、作業の**効率化**