Keidanren
Policy & Action

資料１

サイバー安全保障分野での対応能力の向上に向けた有識者会議に対する経団連意見

2024年7月8日
（一社）日本経済団体連合会
サイバーセキュリティ委員会

総論（現状認識を踏まえた経団連としての取組み）

Keidanren
Policy & Action

- 取引先や海外子会社等のサプライチェーンを経由したサイバー攻撃は増加の一途。地政学的緊張の高まりがサイバー空間にも波及する中、サイバーセキュリティは**国家安全保障に関わる最重要領域の一つ**
- Society 5.0 for SDGsの実現に向けた価値創造やバリューチェーンの構築、さらにリスクマネジメントの観点から、実効あるサイバーセキュリティ対策を講じることは、今や全ての企業にとって、**経営のトッププライオリティ**
- 経団連としては、安心・安全なサイバー空間の構築に向けて、**「サイバーセキュリティ経営宣言2.0」**等を通じて、引き続き全員参加型の対策を推進していく所存

（参考）経団連サイバーセキュリティ経営宣言2.0（2022年10月）
https://www.keidanren.or.jp/policy/2022/087.html

各論

Keidanren
Policy & Action

1. 官民連携の枠組みの構築
2. 政府から民間事業者への情報共有の在り方
3. 民間事業者から政府への情報共有の在り方
4. サプライチェーン全体のサイバーセキュリティ強化
5. サイバーセキュリティ人材の育成・確保
6. 通信情報の活用に関する制度設計
7. 諸外国との連携強化

1．官民連携の枠組みの構築①

Keidanren
Policy & Action

(1) 民間事業者に対する過度な負担の回避

- 官民連携による情報共有は、**情報提供者が不幸にならない**こと、**事業者に過度な負担とならない**ことが大前提
- 「官民連携」の名の下に、情報共有における片務性が一層強まり、一方通行の報告に民間が疲弊することによって、わが国のサイバー・レジリエンスをかえって毀損する、という本末転倒な結果を招かないように留意すべき
- この観点から、**情報共有は官民双方向であることを明確に**しつつ、情報共有の目的や共有情報/共有者の範囲、情報共有の方法等を含む戦略を定めることが不可欠。実用的な情報を共有することが受信者による迅速な脅威認識・対応、ひいては情報共有の枠組みそのものへの信頼性を高めることに寄与

(2) 政府の役割の明確化

- 平時／有事の**インテリジェンス活動やインシデント発生時のアトリビューションに関しては、政府が責任を持って実行**し、**分析した情報を民間事業者と共有**すべき
- 今後発展的に改組されるNISCやサイバーセキュリティに関係するその他政府機関等、それぞれの役割と責任範囲を明確に整理すべき

(3) 既存の枠組みの有効活用

- サイバーセキュリティに関する情報共有の既存の枠組みの実効性も十分に検証した上で、屋上屋を架すような制度設計は避けるべき

1．官民連携の枠組みの構築②

Keidanren
Policy & Action

(4) 日英サイバー協力ミッションで得られた知見

① NCSC（国家サイバーセキュリティセンター）

- 英国でサイバーセキュリティを主導するのは、NCSC（National Cyber Security Centre）。主たる業務は、英国のサイバーセキュリティを強化し、サイバー脅威から国家を防護すること。事業所管官庁等に対しても政策のリーダーシップを発揮

② Active Cyber Defence

- 英国のActive Cyber Defence（≠能動的サイバー防御）においては、公共機関や国民向けに多様なサービスを無償で提供。能動的サイバー防御の在り方の検討にあたっては、英国の取組みも参考にしつつ、**現行法制度下でも実施可能な施策は躊躇なく取り入れる**べき

③ i100（アイ・ワンハンドレッド／ Industry 100）

- 年間100名を目安に、民間企業の専門家をNCSCに受け入れ。民が保有する知識・経験をサイバーセキュリティ政策に活かす仕組みの一つ。様々なレベルのセキュリティチェックをクリアし、必要な訓練も受けているi100のメンバーは、重要インフラ事業者とNCSCの間の橋渡し役として、NCSCが策定する政策（例：ガイドライン策定、人材育成等）をはじめ多岐に亘る分野で活躍
- わが国においても、情報や危機感の共有によるトラストの醸成を目的として、NISC等の政府機関との**官民人材交流に関する枠組みを導入**すべき

2．政府から民間事業者への情報共有の在り方①

Keidanren
Policy & Action

- 政府が受けた攻撃情報や政府が諸外国から受け取った情報を共有する際には、政府側でその重要性を精査し、必要な共有先には柔軟に情報共有すべき

【参考】共有すべき情報例

① 地政学的情報、攻撃者の属性（アトリビューション）等
② 攻撃の手口・手法（TTP：Tactics, Techniques, and Procedures）の観点（例：MITRE ATT＆CK（Adversarial Tactics, Techniques, and Common Knowledge）フレームワーク活用）
③ サイバー攻撃の侵害の痕跡IoC（Indicator of Compromise）情報（例：マルウェアのシグネチャ、ハッシュ値、IPアドレス等）

- このような仕組みの導入に当たっては、NCSCのCiSP（**C**yber Security **I**nformation **S**haring **P**artnership）も参考にすべき

2．政府から民間事業者への情報共有の在り方②

Keidanren
Policy & Action

※ 重要経済安保情報保護・活用法の下での情報共有

- 経済安全保障分野でのセキュリティ・クリアランス制度を規定する重要経済安保情報保護・活用法は、その文言に「活用」とある通り、政府が機微な情報を、安全保障の確保に資する活動を行う民間事業者に共有することが一つの狙い
- 一方で、同法はコンフィデンシャル級の情報が対象であり、トップ・シークレット／シークレット級の情報は特定秘密保護法の対象。特定秘密保護法でも同様の取組みを進めるには、政府内で両法をシームレスに運用することが必要
- 特定秘密保護法および重要経済安保情報保護・活用法は、民間事業者が政府と契約を結ぶことにより、政府が指定した重要情報の共有を受ける意思を示す仕組み
- 仮に民間事業者等が政府からの協力要請に応じて、秘密指定された重要情報に触れる場合には、経緯や実態を踏まえ、民間事業者等における保全の取組みに対する支援が必要

3．民間事業者から政府への情報共有の在り方①

Keidanren
Policy & Action

- 事業者は**複数の政府機関に対し、インシデント報告を実施している**のが現状。わが国のサイバー・レジリエンスを高める観点からは、**持続可能かつ実効的な制度設計が必須**（例：**報告の簡素化、窓口の一元化**等）
- **インシデント報告義務により事業者へ過度な負担を強いることのないよう留意すべき**。また、インシデント対応や報告等に割かれる人的リソース等、事業者の実態を踏まえた合理的な制度とすべき
- 今後、**仮に過度な報告義務が課されることになれば、事業者のインシデント対応能力を毀損**し、結果的に日本のサイバー・レジリエンスに負の影響を与えるおそれ
- インシデント情報に関する報道により、ブランドイメージの毀損や株価下落に直結するケースが散見されることから、情報共有のスピード感が損なわれる可能性も。**事業者から提供される情報は、センシティブ情報として慎重に取り扱う**べき（懲罰的な見せしめは避けるべき）
- 制度設計にあたっては、**経済界および事業者と双方向のコミュニケーション**をお願いしたい

3．民間事業者から政府への情報共有の在り方②

Keidanren
Policy & Action

- 経済安全保障推進法において、基幹インフラ事業者は所管省庁に対し、重要インフラの導入前に機器に関する事前届出を行う必要があり、義務・負担が増加しているのが実情
- こうした中、事業者に追加の情報提供を求めるばかりではなく、まずは政府自身のインテリジェンス力を高めることに注力すべき。その上で、公益の観点から民間事業者にもメリットが生じる形で官民連携の枠組みが構築されれば、事業者も当該枠組みに関与し、情報提供を行うインセンティブに
- 民から官への情報共有に際し、機微情報、個人情報・プライバシー情報の取扱いについて、GDPR等、他の法域に照らした法的リスクに対する考え方も整理すべき
- わが国のシステム開発の契約形態や運用形態に基づいたステークホルダー（システムインテグレーター、クラウド事業者等）を考慮のうえ、情報共有の仕組みおよび制度設計を検討すべき
- 米国ではCIRCIA（**C**yber **I**ncident **R**eporting for **C**ritical **I**nfrastructure **A**ct of 2022：重要インフラ向けサイバーインシデント報告法）を踏まえ、官民で情報共有。諸外国の取組みを参考に対応方針を検討すべき

4．サプライチェーン全体のサイバーセキュリティ強化

Keidanren Policy & Action

(1) サプライチェーン全体を俯瞰したサイバーセキュリティの在り方

- 総合的な国力という観点から、官民の明確な役割分担を含め、サプライチェーン全体を俯瞰したレジリエンス強化に向けて、実効的な仕組みを構築すべき。ガイドラインの策定のみならず、**実行に必要なリソース（費用・人材・技術）支援、政府調達要件への採用等も検討すべき**
- サプライチェーン・サイバーセキュリティ成熟度モデル（Cybersecurity Maturity Model Certification：米国防省が定めるサイバーセキュリティ調達基準）対応については、サプライチェーン全体の底上げに結実するように、中小企業を含む社会全体として検討すべき
- インシデント後の事業の復旧までを見据えレジリエンスを強化すべく、**サイバーのみならずオールハザードな事業継続計画（BCP）の策定**が必要
- 重要インフラ事業者のみではなく、重要インフラを顧客として抱える事業者等への影響や責任のあり方等も整理すべき

(2) プラットフォームの有効活用

- **業界横断で継続的に議論する場を確保し、政府関係部局とも双方向で連携可能なプラットフォームを構築**する必要。この点、民間を束ねるプラットフォームとして、既存のSC3の有効活用も一案

(3) 企業間連携・中小企業対策の強化

- **下請法や独占禁止法との関係や利益供与等について、明確な整理**が必要
- 中小企業を含むサプライチェーン全体の防護には、**国の支援が不可欠**

5．サイバーセキュリティ人材の育成・確保

Keidanren
Policy & Action

(1) 縦割りを排した政府横断的な取組み

- 経済産業省やIPAをはじめ政府の取組みを多としつつも、**省庁間や省内の縦割り等による弊害**も。中長期的なグランドデザインを描いた上で、**横串を刺した取組み**を進めるべき

(2) 参考とすべき英国の取組み事例

- 人材の育成・確保に関して、例えば英国では必要な国家予算を充当し、サイバースキルの階層に応じたトレーニングを無料で提供するなど、国民の意識を醸成、底上げ。日英サイバー協力ミッション（2024年1月）における面会先では、英国サイバーセキュリティ人材の多くが女性。わが国のサイバー人材不足は深刻で、**ダイバーシティの確保を含め、その育成・確保が喫緊の課題**

(3) 実践的な演習の継続的な実施等

- **地方におけるサイバーセキュリティ人材の育成・確保**の観点も踏まえ、**業界横断かつ中小企業を含むサプライチェーン全体で演習・訓練等の取組み**を官民一体となって強力に推進すべき
- NATO Locked Shields（※ NATOのCooperative Cyber Defence Centre of Excellenceが毎年実施しているサイバー防衛演習）のように、サイバー攻撃への対処能力の向上やサイバーセキュリティ動向の把握を目的とした実践的な演習を平時から継続的に実施すべき

６．通信情報の活用に関する制度設計

Keidanren
Policy & Action

- 通信を介した攻撃状況のモニターに関しては、**事業者の解釈に委ねることなく、法律での明文化**（事業者の法的義務とその要件が明示的に規定された法律）**と丁寧なルール作りが不可欠**
- 特に、プライバシーの尊重、国家安全保障の観点から真に必要な場合に限定した、制度的な保証を設けるべき
- また、海外からの通信については、モニター対象を明確化し、国の責任の下で対応すべき
- 法制度の運用開始に先立ち、**事業者に十分な準備期間を**設けるべき
- 通信情報の活用には通信事業者の協力が必須。協力にかかる費用補助等、適切な支援を実施すべき

７．諸外国との連携強化

Keidanren
Policy & Action

(1) 同盟国・同志国との連携強化

- ファイブアイズをはじめ同盟国・同志国は「セキュアバイデザイン・セキュアバイデフォルト」に向けた取組みを推進
- 安全・安心なサイバー空間を構築するためには、**トラストに立脚した相互運用性が不可欠**。このため、政府による制度設計においては（詳細な手続きを定めるのではなく）結果に着目すべきであり、また友好国との間での平仄と相互運用性に配慮すべき
- 具体的には、ISO/IEC基準や米国のNISTサイバーセキュリティ基準などの国際基準を参照に制度調和を推進し、また**SBOM（Software Bill of Materials）やセキュアバイデザイン・セキュアバイデフォルトを推進**すべき

(2) グローバルサウスへのトラストの輪の拡大

- グローバルサウスとの関係において、わが国が主体的かつ友好的にリーダーシップを果たすよう努めるべき

Keidanren

Policy & Action