サイバー攻撃によるボトルネック資源の供給停止に起因する企業の事業継続リスクの考察

Consideration of business continuity risks for companies due to outages of bottleneck resources caused by cyber-attacks

山田祐也・法制倫理分科会・情報セキュリティ大学院大学

1. 研究背景

サイバー攻撃によって企業の事業継続が脅かされるリスクの増加

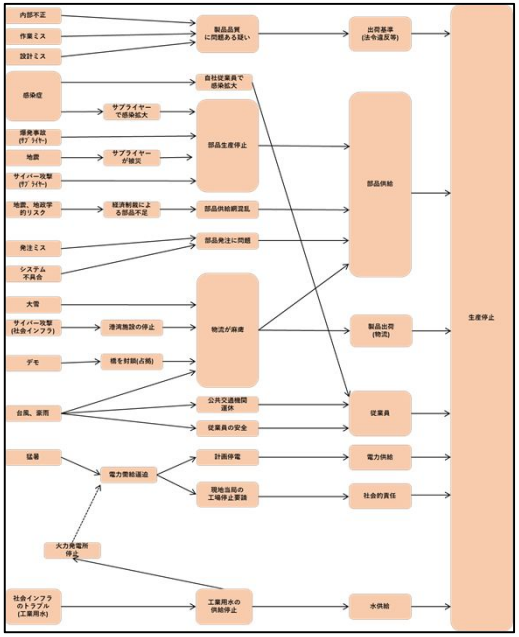
- 企業のIT/OT依存度が高まり、IT/OTシステムの停止が業務の停止や縮退に直結する（事例：大阪急性期総合医療センター、名古屋港）
- サプライチェーンを標的としたサイバー攻撃が増加し、他社へのサイバー攻撃が間接的に自社の事業停止を招く（事例：小島プレス）

2. 目的

サイバー攻撃を起点とした事業継続を脅かすリスクを網羅的に評価できるリスクアセスメント手法の提案

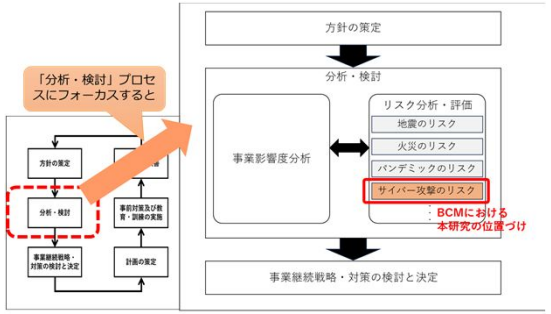
- 他社へのサイバー攻撃によって自社の事業が停止するリスクの定量的な評価を目指す
- 事業停止を防止または早期復旧するための具体的な対策を提案する
- 過少/過剰な対策を避けるため、合理的な対策の度合いを示す

3. 具体的な事業停止リスクの分析



- 企業のボトルネック資源を明らかにするため、新聞記事から企業の事業停止事例とその原因を調査した
- まず、トヨタについて調査し、左図にまとめた
- 他企業/業界についても同様の調査を実施し、業界による差分を明らかにする予定
- サプライチェーンだけでなく、重要インフラなどの様々な資源の供給停止によって、事業停止が実際に発生している事が明らかになった

4. 関連の取り組み調査　自然災害のBCM/サプライチェーン



- 企業の事業継続を脅かすリスクの内、間接的な被害のリスクは、自然災害と共通の場合が多い
- ⇒自然災害のBCM(事業継続マネジメント)の仕組みを応用できるのではないか？

5. 今後の予定

- 複数業界の事業停止事例を調査し、具体的な事業停止リスクを特定する
- 事業停止リスクについて先行する自然災害のBCMについて文献を調査する
- サイバー攻撃による事業停止リスクを評価する指標を考案する
- 経営、マネジメント、現場の各レベルに対して提言と対策検討のフレームワークをまとめる