ISS square　2023年度 ISS Square シンポジウム (2024/3/1)　No.102

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

Abstract: The increasing number of ransomware attacks and cyber attacks targeting supply chains have increased the risks that threaten the business continuity of companies. In order for companies to take effective countermeasures using their limited management resources, there is a need for a risk assessment method that can comprehensively evaluate risks related to business continuity stemming from cyber attacks. As a result of the study, it was found that risks that threaten business continuity triggered by cyber attacks exist in all resources that support corporate operations. It was also found that risks that threaten business continuity should be considered comprehensively within BCM, rather than considering countermeasures for each event that serves as a starting point. Therefore, this study aims to propose a risk assessment method to analyze and evaluate risks in BCM for supply chain risks that threaten corporate business continuity, starting from cyber attacks. As a result of a survey on current approaches, it was found that conventional risk assessment methods target information assets owned by the company and do not take business continuity and supply chain risks into consideration.

1. 研究背景

●事業継続を脅かすサイバー攻撃へ対処するには、自社のセキュリティ対策だけでは不十分

企業のIT/OTシステムを停止させるサイバー攻撃(例：ランサムウェア)
⇒被害は情報流出だけでなく、事業停止に繋がる

サプライチェーンを標的としたサイバー攻撃
⇒他社へのサイバー攻撃が自社の事業に影響

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が自社に波及するリスクはどの程度だろう？

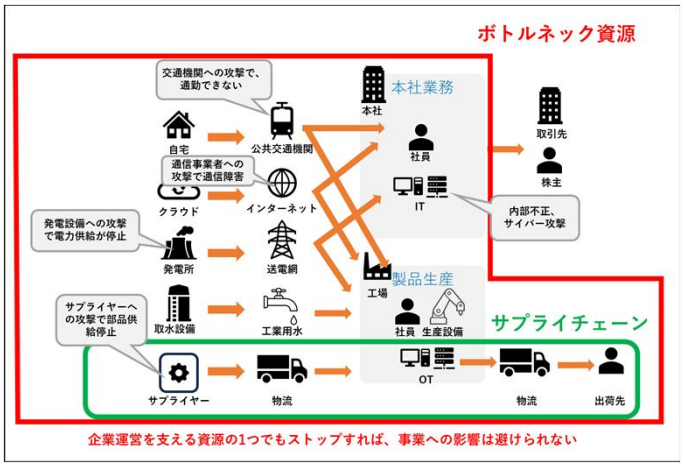
どのような対策が効果的だろう？

どこまで対策するのが妥当だろう？

3. 企業の事業継続を脅かすリスク

●事業継続を脅かすリスクは自社・サプライチェーンに限らない

- 通信障害でクラウド上の業務システムにアクセスできず、支払遅延
- 送電網への攻撃で電力供給が停止し、生産停止
- 公共交通機関が止まって社員が出社できず、生産停止



⇒ 事業継続に必須な資源 ＝ ボトルネック資源 で考える必要

4. サイバー攻撃と自然災害の被害の比較

●間接的な被害・対策は自然災害と共通点が多い

地震とサイバー攻撃の被害と対策の比較

比較項目		地震	サイバー攻撃
想定事例		東日本大震災(トヨタ、セブンイレブン)	小島プレス工業、名古屋港
脅威主体		自然	人間
自社への直接被害	被害の受けやすさ(発生確率)	地理的特性による	セキュリティが脆弱で、社会的・サプライチェーン上重要な企業が狙われやすい
	被害の性質	物理的、人的被害。工場設備全般が被災して、生産ができない。	工場設備に被害はないが、管理システム(IT/OT)が停止して生産ができない。
	被害の範囲	特定の地域に被害が集中	地理的な距離には無関係
	対策の変化	改善や事業の変化への対応を目的に定期的に見直す	攻撃の巧妙化や新たな脆弱性の発見に応じて、常に対策を見直す必要
	対策(識別)	ボトルネック資源の棚卸し、事業影響度分析など	情報資産の棚卸し、リスクアセスメントなど
	対策(防御)	建物の耐震化など	アクセス制御、脆弱性対応など
	対策(検知)	災害情報を見える化するシステムの導入など、被害報告の体制整備	脅威検知システムの導入、ログ監視など
	対策(対応)	避難訓練など	対応計画の作成、被害封じ込めの訓練など
	対策(復旧)	地理的に離れた場所にバックアップの設備を持つ。BCPの策定など	復旧計画の作成など
他社被害による間接被害	被害の性質	ボトルネック資源の供給停止(物流停止、部品生産停止など)	ボトルネック資源の供給停止(物流停止、部品生産停止など)
	被害の範囲	被災企業に依存している全ての企業に影響	被災企業に依存している全ての企業に影響
	対策の変化	改善や事業の変化への対応を目的に定期的に見直す	改善や事業の変化への対応を目的に定期的に見直す
	対策(識別)	ボトルネック資源の棚卸し	ボトルネック資源の棚卸し
	対策(防御)	-	-
	対策(検知)	連絡体制の整備	連絡体制の整備
	対策(対応)	復旧支援	インシデント対応支援
	対策(復旧)	サプライチェーンの冗長性確保、BCPの策定など	サプライチェーンの冗長性確保、BCPの策定など

⇒サイバー攻撃による間接的な被害＝ボトルネック資源の供給停止は自然災害のBCMに組み込めるのではないか

5. セキュリティフェーズ

●従来のセキュリティ対策 + 事業復旧では他社も考慮する

NISTサイバーセキュリティフレームワークを参考に、他社の概念を取り入れて拡張

6. 今後

- 具体的リスクの洗い出し(業界ごとの事業停止事例を調査)
- 自然災害のBCMの調査
- リスク評価手法の検討