サイバー攻撃により生じる損害の分担に関わる法的判断枠組み

Legal Framework for Sharing Damages Caused by Cyber-Attacks

町田 力・マネジメント分科会・情報セキュリティ大学院大学

Abstract: The party that should, in principle, bear legal responsibility for damages caused by cyberattacks is the attacker. However, in practice, it is extremely difficult to hold attackers legally accountable. Consequently, situations often arise in which the victimized company and related parties must share the resulting losses. This study divides the elements of liability for damages into three phases—breach of obligation/negligence, damage and causation, and contributory negligence—and examines a framework for determining how such losses can be fairly allocated among the parties involved in the event of a cyberattack. Furthermore, the paper applies the proposed analytical framework to potential future cases and presents the outcomes of this application.

サイバー攻撃によって生じた損害について、攻撃者への責任追及は現実的ではなく、被害企業と関係当事者との間で損害を分担せざるを得ない状況のなかで、、、

- サイバーセキュリティって、どこまでやれば法的責任を問われないの? ⇒ 債務不履行・過失
- サプライチェーンで波及する損害って、どこまで責任を負わないといけないの? ⇒ 損害・因果関係
- 当事者の双方に過失がある場合の責任割合ってどのくらい? ⇒ 過失相殺

損害賠償責任を構成する「**債務不履行・過失**」「**損害・因果関係**」「**過失相殺**」の3フェーズで、基準（責任分界点）の明確化を検討する。

債務不履行・過失

Tschiderモデル

:「合理的な」サイバーセキュリティ義務（“reasonable” cybersecurity duty）を分析する2部構成のモデル

1. **静的義務**(static duty)
   …**業界水準**に基づく客観的な義務
2. **動的義務**(dynamic duty)
   …**状況や文脈に応じた**主観的な義務

日本法への適用可能性

Yahoo!BB事件
→危険性の高い手段を用いている場合は一般的に採られている対策よりもさらに高度な対策が求められる。

政府関係機関が注意喚起や公表等で推奨するセキュリティ対策

過失相殺

過失割合を、リスク寄与度の定量的分析(※)として再構成する試み（ビジネスメール詐欺（BEC）をモデルケースとする）

1. 実例から過失相殺において考慮すべき要素を抽出
2. 各要素を以下の3軸(暫定)で評価(1～5点)
   ① 予見可能性
   ② 回避容易性
   ③ 防止効果
3. 3軸の重要度を重みづけ
4. 各要素のスコアを算出

(※)本研究は、個別の数値を算出することが目的ではなく、評価プロセスの客観化（経験的蓄積が形成される前段階での理論的基礎づけ）が目的である。

1つの法的判断枠組みを確立し、それがサプライチェーンのような複雑な事案にも適用可能かどうかを検証する。