

能動的サイバー防御における侵入・無害化の法的課題について

Legal Issues of Intrusion and Harmlessness in Active Cyber Defense

琴浦将貴・ネットワーク分科会・情報セキュリティ大学院大学

In December 2022, the Japanese government published its National Security Strategy, announcing the introduction of 'active cyber defense' to enhance its cybersecurity response capabilities to the level of major Western countries. The strategy explicitly states that, in the event of a serious cyber attack, it will penetrate and neutralize the attacker's servers in advance where possible. However, this approach goes beyond mere defense and may violate domestic laws such as the Act on Prohibition of Unauthorized Computer Access, as well as international laws concerning sovereignty and the use of force. This study examines legal challenges, discussions on avoiding illegal actions, and proposes a legal framework to justify active cyber defense under international law.

能動的サイバー防御の導入

2022年12月、国家安全保障戦略において能動的サイバー防御の導入が明記
「国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー
攻撃について、可能な限り未然に攻撃者のサーバ等への侵入・無害化」

(国家安全保障戦略Ⅵ 2 (4) ア P.21)



JP国内法上の課題

①「侵入・無害化」を実施する場合サイバーセキュリティに関する法に抵触の恐れ
(不正アクセス禁止法、刑法等)
→正当化していく必要あり

②正当化のアプローチ

- 構成要件から外す(適用除外にする)
侵入・無害化措置の実施内容は多岐に渡るため適用除外は非現実的
- 違法性を阻却する(正当防衛・緊急避難・正当行為のどれか)

正当防衛・緊急避難は未然に無害化する行為は非親和的

→正当行為により違法性を阻却すべき
そのため、新法を作り対応すべき
警察官職務執行法5条が特に参考になる
(犯罪の虞があるとき予防・制止できる)

③実施機関への権限の付与

実施行為を正当化するだけでなく、当該機関に法令により適切な権限を付与すべき
警職法、自衛隊法など

④第三者組織による適切性の確保

第三者組織の審査により、過剰・目的逸脱するような侵入・無害化の抑制をするべき

国際法上の課題

①国際法の考慮

侵入・無害化の対象が国外の場合、国際法の検討は必須

- 他国の主権に影響を与える可能性
主権侵害・干渉となる恐れ
- 他国に武力の行使となる可能性
武力攻撃・武力行使となる恐れ
(ただし、サイバー攻撃を武力行使と認定するハードルは高い)

②違法性阻却

「侵入・無害化」を正当化するため違法性を阻却する必要

- 対抗措置
先行する違法行為に対する措置
→未然に無害化する行為は非親和的
- 緊急避難
重大かつ差し迫った危険から守るためにやむを得ずとる措置
→先行する違反行為を立証する必要なく、無害化の違法性阻却としては有用

※2025年2月、能動的サイバー防御は「重要電子計算機に対する不正な行為による被害の防止に関する法律案」として国会に提出・審議中