資料５

2017 年 11 月 6 日

AI ネットワーク社会推進会議　第 1 回合同分科会

AI に関するセキュリティに対する法規制の可能性

湯淺　墾道
情報セキュリティ大学院大学学長補佐・情報セキュリティ研究科教授

1　法規制の必要性

・仮想空間　→　現実空間上での回復・賠償不可能な被害発生
　個人情報の漏洩被害の 3 段階：身体的・精神的・経済的
・軍事目的
　致死性無人兵器(Lethal Autonomous Robotics, LARs)の規制をめぐる動向
　2013 年国連ヘインズ報告
　2016 年ジュネーブ第 5 回レビュー会議[1]
　　人間のコントールによらず攻撃対象を決定する武器システムに関する検討開始を決定
・技術標準その他のソフト・ローの執行
　必ずしも市場原理が有効でない場面における執行力
・セーフハーバー
　禁止、制限事項を明示することにより、逆に開発者に予見可能性
・防止からレジリエンスへの転換
　一定のインシデント発生は不可避
　発生を前提とした原因解析と被害拡大防止
　被害防止及び損害賠償に関する責任分界
・AI ボット
　ネットワーク接続により AI へのマルウェア感染が伝播
　AI ボット化する恐れ、AI 開発時点で不正指令機能付加の恐れ

2　考慮すべき要素

・保安からセキュリティへの転換
　専用閉域回線網＋専用制御システムによる強固な保安体制　→　インタ

[1] https://www.un.org/disarmament/geneva/ccw/

ーネット＋AI による脆弱な管理体制

「安全」とセキュリティのずれ

Cf. 医療機器のセキュリティ

・解析の困難性

フォレンジックのツール依存

動作・判断ログ＋通信ログ

Cf. アメリカで発生した自動走行自動車の死亡事故調査[2]

ログ保存義務を課す場合

保存機能を実装する義務を負う者

保存義務を負う者

保存場所

執行する者とその手段

揮発性データのフォレンジック、アンチ・フォレンジック

プロプライエタリ(proprietary secrets)の主張

プロプライエタリに一定の制約を設けるべきか、その手法

・通信の秘密、所有権の制約

AI ネットワーク通信と通信の秘密

自然科学的事象を数値化して送受信しているにすぎない場合

個人情報、プライバシー等に係わる情報を送受信している場合

義務の範囲（電気通信事業者　→　拡大すべきか）

Cf. ボットネットのテイクダウン

Microsoft のみが裁判所により合法化

Citadel 決定が嚆矢

Microsoft Corp. v. John Does 1–82, No. 3:13-CV-00319 (W.D.N.C. Nov. 21, 2013)

Microsoft に対し、インジャンクション認容

Windows　OS の利用契約の文言に照らして許容されると判断[3]

ボットネット C&C サーバーに使用されているドメインを無効化することを許容

Citadel ボットネット・マルウェアに感染しているコンピューターの所有者に通知するため、20 分に 1 度の間隔で、コンピューターの所有者の同意なくマルウェアに関する通知を表示することを許容

・規制の段階と対象

[2] https://www.ntsb.gov/investigations/AccidentReports/Pages/HWY16FH018-preliminary.aspx

[3] “[C]onsistent with the terms of Microsoft’s license to its Windows operating system, Microsoft shall be permitted”, Microsoft Corp. v. John Does 1–82, No. 3:13-CV-00319 (W.D.N.C. Nov. 21, 2013), at 11.

コンピュータプログラムとしてのAIの開発自体
AIの製品への実装段階
AIを実装した製品の販売・提供段階
AIを実装した製品のネットワークへの接続段階

3　AI利用者に対して

・IoTセキュリティガイドライン（2016年）[4]
問合せ窓口やサポートがない機器やサービスの購入・利用を控える
初期設定に気をつける
使用しなくなった機器については電源を切る
機器を手放す時はデータを消す

・利用者自身の責任
製品保証（完成品を前提、利用者による改造禁止）　→　セキュリティ（常に未成､利用者は最新版アップデート義務 or アップデートしていない場合は製品保証なし）への転換は可能か
予見可能性と免責

・AIに関するインシデント情報の共有、通知義務
EU　GDPR
侵害発生前
仮名化・暗号化・システム復元力維持等の措置の実施、定期的な検査
侵害発生後
個人データ窃盗等の個人の権利・利益侵害の危険性が高い侵害に関する通知
オランダ
データ処理及びサイバーセキュリティ通知義務法義務法(Data processing and Cybersecurity Notification Act of 2016)
Data breach notificationから、cyber security notificationへ
必須事業者（第1条）　vital operator
製品またはサービスの事業者であって、その可用性及び信頼性がオランダ社会にとって必須の重要性を有しているもの
マルウェア感染その他のインシデントの発生時に治安・法務省の下にある国家サイバーセキュリティセンター(NCSC)に届け出ると共に、必要なデータを提供することを義務づけ

以上

[4] http://www.soumu.go.jp/main_content/000428393.pdf