

2024 年 6 月 19 日

能動的サイバー防御に関連する論点

土屋大洋

1. 能動的サイバー防御

- 2001 年の 9.11 テロ後、ブッシュ政権による大規模な令状なし傍受プログラム開始
- オバマ政権時にプログラム拡大。2010 年に米国サイバー軍設置、司令官が NSA 局長を兼任。コンテンツからメタデータの取得が中心に
- かつてのエシュロンがアナログの無線通信傍受が中心だったのに対し、現代ではデジタルの有線通信のモニタリングが中心に
- 諸外国の情報機関がデジタル技術に急速に対応

2. ビッグデータの取得と保存

- 2013 年のスノーデン事件で米国政府とプラットフォームの協力が発覚
 - 大量のデータを統合管理する技術
 - 蓄積したデータから必要なデータを探し出す検索技術
 - 探し出したデータを相関させる技術
- ヘッダーで振り分けるか。コンテンツまで見るか。誰が見るか
- Human Readable なデータと Machine Readable なデータ
- どの方向のデータを対象とするか
 - 国内で完結するデータ (domestic)
 - 国内から国外に出て行くデータ (outgoing)
 - 国内へ国外から入ってくるデータ (incoming)
 - 国外から国内を経由して国外へ出て行くデータ (transit)
- 非構造化データとの統合

3. 論点

- どんなデータをどこまで取得するか
- 平時と有事が切れ目なく続く中で平時からデータ取得ができるか
- 通信事業者やプラットフォームと合法的な協力関係を築き、企業の評判・信用を守るとともに、政府が企業に対価を支払うことができるか
- 膨大なデータを保存する設備と処理する能力を確保できるか