RightsCon参加報告：商用スパイウェア規制とサイバー空間における人権

JPCERTコーディネーションセンター
国際部 米澤 詩歩乃

目次

- RightsConとは
- 「RightsCon 2025」概要
- 商用スパイウェアの規制に関する動向
- サイバー空間における人権

RightsConとは

- **デジタル時代の人権について議論を行う国際会議**
- **主催者：**Access Now（米国の非営利団体）
  - 人権とテクノロジーが交わる幅広い問題に取り組む
    （AI、コンテンツガバナンス、データ保護、インターネット遮断、監視、サイバーセキュリティ、プライバシーなど）
- **参加者：**市民社会組織、政府関係者、民間企業、研究機関、技術者、ジャーナリストなど
- **過去の開催地：**サンノゼ、チュニス、トロント、ブリュッセル、リオデジャネイロ、マニラ、サンフランシスコなど
  - 2011年から継続して開催

参考：RightsCon 公式ページ https://www.rightscon.org

RightsConとは（参考：2023年・コスタリカの開催レポート）

- **2023年開催概要（現地＋オンラインのハイブリッド）**
- **参加者：**174カ国、689の組織

  現地参加 約2,871人、オンライン参加 5,466人

  — 女性 57.4%、男性 35.3%、ノンバイナリ・その他のジェンダー 7.1%

  — 市民社会 50.6%、学術 12.3%、メディア 5.6%、政府 5.1%、慈善団体 3.6%、民間 3.3%、政府間組織（IGO） 3.1%、クリエイティブ 3.1%、その他 7.9%

  — 北米 2,220人、欧州 2,023人、ラテンアメリカ・カリブ地域 1,863人、アフリカ 1,036人、アジア 856人、中東・北アフリカ 337人
- **セッション数：**638件

参考：RightsCon「RightsCon Costa Rica Outcomes Report」
https://www.rightscon.org/rc23-outcomes-report/

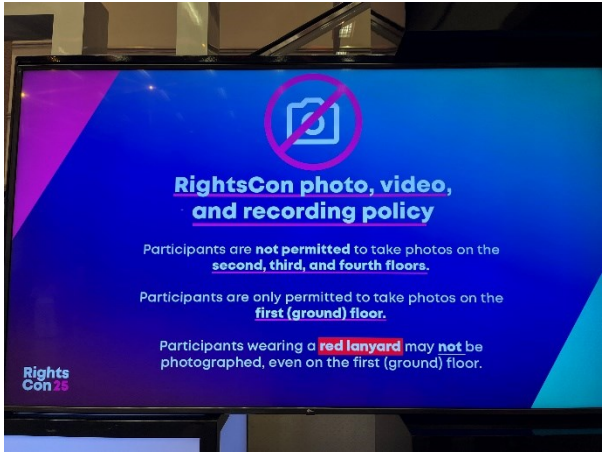
「RightsCon 2025」概要

- **会場：**Taipei International Convention Center（TICC、台北国際会議中心）
- **参加者数：**150カ国・地域から、およそ2,800人が参加
- **スポンサー：**カナダ政府、オランダ外務省、スウェーデン国際開発協力庁（SIDA）、Meta、Google、Microsoft、Netflix、Yahoo!、Cisco、Cloudflare、Surfshark、APNIC、TWNIC、Inernet Societyなど30組織
- **セッション数：**およそ550件
- **セッションフォーマット：**ラウンドテーブル、ワークショップ、ダイアログ形式、Lightningトーク、Tech Demo、Meet up、プライベートミーティング（非公開）など
- **18のカテゴリー：**

  - AIと新興技術
  - ビジネスと人権
  - 紛争と人道的活動
  - コンテンツガバナンス
  - データ保護
  - 組織の能力と資金
  - コミュニティーのためのデジタルセキュリティ
  - メディアの自由
  - 監視の時代における自由と主体性
  - 未来・フィクション・創造性
  - グローバルなサイバー規範と暗号化
  - アクティビストのための戦術と状況
  - ガバナンス・政治・選挙
  - 人権中心のデザイン
  - インターネットアクセスと包摂性
  - インターネット遮断と混乱
  - オンラインヘイトと暴力
  - 司法・訴訟・文書化

セキュリティとプライバシー

- 1階フロア以外での会場内の写真・動画撮影は禁止
- 入場用の参加パスのストラップは赤（撮影禁止）と青（ビデオや写真に写り込んでも問題ない）から選択
- チャタムハウスルールが適用されているセッションも



聴講したセッション

- スパイウェアの規制、被害者の救済
- インド太平洋地域におけるサイバー能力構築の取り組みと課題
- ランサムウェアの被害者が直面する問題について考えるワークショップ
- サイバーとデジタルガバナンスにおけるマルチステークホルダーモデルの未来
- 国連におけるサイバーおよびデジタル問題への取り組み
- 国連のAIガバナンスの取り組みは、権利を尊重するアプローチを確保しているか？
- その他

商用スパイウェア規制の動向

商用スパイウェアを巡る問題

- スパイウェア規制と被害者の救済に関するセッションを聴講
  - 欧州のPEGA委員会、米国の国内外の取り組み、ポール・モール・プロセスなどの規制の動向
  - 被害者の救済（訴訟の支援、被害者の心理的サポート）
- 商用スパイウェアとは
  - モバイル端末にひそかにインストールされ、位置情報の追跡、端末内の情報窃取、通話の傍受などを行うソフトウェア
  - 国家や政府がテロ対策などの安全保障の目的で使用
  - 例：Pegasus、Predatorなど
- 何が問題か？
  - ジャーナリストや活動家、敵対する国の政府関係者などの監視に濫用されている
  - 人権やプライバシーを侵害
  - 規制するにあたり、合法的使用と濫用の定義の難しさがある
  - 管轄権の問題：開発者が拠点を置く国、購入者の国、標的とする国がそれぞれ違う場合、どの国が違法行為を裁くことができるか？
  - ソフトウェアの脆弱性を悪用、攻撃の痕跡を残さないため攻撃の証明が困難

商用スパイウェアの規制の動向：比較

	米国主導の国際的取り組み	ポール・モール・プロセス	PEGA委員会
主導国／機関	米国政府	英国・フランス	欧州議会
目的	スパイウェアの濫用防止と人権保護を国際的に促進	商用スパイウェアの拡散防止と規制強化	EU加盟国の商用スパイウェアの使用実態調査と今後の規制に関する提言
特徴	• 国内の取り組み強化＋国際的取り組み強化（国内：米政府内でのスパイウェアの調達制限、スパイウェアを悪用した個人へのビザ制限）	• 民間企業・市民社会も参加 • 継続的対話 • ガイドラインの策定	• 実態調査に基づいた勧告と法制度の改善提案 • 今後のEUの立法や輸出管理政策に影響を与える可能性も
対象範囲	• 世界（21カ国が参加） • 日本も参加	• 世界（28カ国・連合、その他民間企業・市民社会も参加） • 日本も参加	EU加盟国
法的拘束力	なし	なし	なし
共通点	「スパイウェアの無責任な使用の規制」「人権保護」「国家・企業・市民社会の連携」「説明責任・透明性・スパイウェア使用に関する監視体制の強化」「輸出規制」「法的枠組みの国際的調和」などの課題意識は共通している		

商用スパイウェアの規制の動向（EU）

■ 欧州議会のPEGA委員会による調査

— 2022年3月10日に設置、2023年6月に最終報告書を公開

— **目的**：EU加盟国における商用スパイウェアの違法な使用の調査と報告書の作成

— **調査結果**：一部の加盟国での濫用（ポーランド、ハンガリー、ギリシャ、スペイン等）や、スパイウェアの使用に関する法的枠組みや適切な監視メカニズムの欠如が明らかに

— **提言**：EU共通の規制枠組みの構築や、セキュリティ強化以外の目的での脆弱性情報の販売の禁止、EU Tech Labの設立、輸出管理の強化、国際協力の促進などを求めた。また、下記の4つの条件を満たすまで、スパイウェアの使用を一時的に停止することを求めた

- スパイウェアの悪用事例の調査と解決
- 各国の法的枠組みを、適用される国際法の基準に適合させること
- 捜査に欧州警察機構（ユーロポール）を関与させるという明確な約束
- EU法に準拠しない輸出許可の撤廃

— **その後**：欧州議会の一部の議員が第2の調査委員会「PEGA2」の設立を提案。欧州委員会はPEGA委員会の勧告に対し、具体的な立法措置や規制の実施には至っていない

参考：PEGA Committee final report
https://www.rcmediafreedom.eu/Resources/Reports-and -papers/PEGA-Committee-final-report

商用スパイウェアの規制の動向（米国）

■ 米国政府内での使用を制限する大統領令

- 2023年3月、バイデン大統領が米国政府によるスパイウェアの使用を制限する大統領令を発令
- **目的**：商用スパイウェアの無責任な使用がもたらすリスクに対処し、米国および国際社会における人権と民主主義を守ること
- **使用禁止の条件**：
  - 米国政府に対する重大な防諜および安全保障上のリスクをもたらすもの（米国政府の情報を無許可で転送、使用、開示するなど）
  - 外国政府や外国人による不適切な使用のリスクがあるもの（米国政府のPCやデバイスへの不正アクセス、ジャーナリストや活動家などに対する人権侵害等）
- **除外対象**：テスト、研究、分析、サイバーセキュリティ、防諜もしくはセキュリティ上のリスクに対する対策の開発、スパイウェアの犯罪的な販売・使用に関する犯罪捜査の目的のための使用には適用されない

参考：The White House「FACT SHEET: President Biden Signs Executive Order to Prohibit U.S. Government Use of Commercial Spyware that Poses Risks to National Security」
https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/03/27/fact-sheet-president-biden-signs-executive-order-to-prohibit-u-s-government-use-of-commercial-spyware-that-poses-risks-to-national-security/

■ 商用スパイウェアの悪用に関与した個人への入国ビザ制限

- 2024年2月、商用スパイウェアを悪用した外国人に対し、入国ビザ制限を科す新たな政策を発表
- 対象：ジャーナリスト、活動家、人権擁護者、反体制派、少数派コミュニティーのメンバーなどを標的とした商用スパイウェアの悪用に関与した個人

参考：United States Department of State「Announcement of a Visa Restriction Policy to Promote Accountability for the Misuse of Commercial Spyware」
https://2021-2025.state.gov/announcement-of-a-visa-restriction-policy-to-promote-accountability-for-the-misuse-of-commercial-spyware

商用スパイウェアの規制の動向（米国）

■ 米国主導の国際的な取り組み

— 2023年3月の第2回民主主義サミットで、商用スパイウェアの拡散と悪用に対抗するための共同声明を公開

- 米国、英国、オーストラリア、カナダ、コスタリカ、デンマーク、フランス、ニュージーランド、ノルウェー、スウェーデン、スイス、フィンランド、ドイツ、アイルランド、日本、ポーランド、韓国、オーストリア、ラトビア、エストニア、リトアニア、スロベニア、オランダが賛同
  （賛同国は徐々に増え、2024年時点で計23カ国）

— 以下の取り組みを行うことに合意：

- 政府による商用スパイウェアの使用が、人権、法の支配、市民の権利と自由を尊重することを保証するための手続きとガイドラインの確立
- 悪意のあるサイバー活動に使用される可能性のあるソフトウェア、技術、機器の輸出を防止するための措置
- 商用スパイウェアの拡散と悪用に関する情報共有の強化
- 産業界や市民社会と緊密に協力し、意識向上を支援し、適切な基準設定を推進
- パートナー国や他の関係者と協力し、商用スパイウェアの悪用を抑制し、業界の改革を推進

参考：United States Department of State「Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware」
https://2021-2025.state.gov/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/

商用スパイウェアの規制の動向（ポール・モール・プロセス）

- **英仏主導の国際イニシアチブ「ポール・モール・プロセス」（2024年2月発足）**
  - **参加者**：2025年4月時点で、28の国・連合、14の民間企業、12の市民社会組織が参加
  - **目的**：商用スパイウェアの拡散と無責任な使用によってもたらされる課題について議論し、市販のスパイウェアの開発、購入、使用に関する国家、業界、市民社会の指針を確立する
  - 商用スパイウェアの開発、販売、移転、使用に関する各国の慣行を確立するための4つの指針を示した：
    - 説明責任：適用される既存の国際法および国内の法的枠組みに矛盾する無責任な活動に対し適切な措置をとる
    - 正確性：スパイウェアの開発、販売、移転、使用は、無責任な使用と結果を確実に回避・軽減できるようにする
    - 監視：合法的かつ責任ある使用であるか監視するための、評価と監査のメカニズムを設置する
    - 透明性：スパイウェアの商取引における各国政府の関与、輸出、政府調達、使用規制のために実施されるプロセスなどの透明性に関するメカニズムを確立する
  - 進捗：2025年4月に「行動規範」（拘束力のないガイドライン）を公開

参考：GOV.UK「The Pall Mall Process tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities」
https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities

サイバー空間における人権

- セキュリティと人権を両方守るための法制度や監督体制の確立
  - プライバシーの権利
  - 表現・結社の自由の権利（意見の発信）
  - 知る権利（調査報道や告発活動）
  - 安全にデジタル空間を使う権利
- 境界が曖昧なサイバー空間で起きる問題に対し、国際社会全体で対応していくための国際協力の必要性
- 防御や対策におけるサイバー能力の構築、さまざまな専門知識の統合と連携
- 政府、民間組織、市民社会それぞれが意識的・主体的に課題解決に取り組むことの重要性

RightsConはデジタル・サイバー空間における問題や課題を共有し、解決に向けたアクションにつなげていくための議論を行う市民社会主導のコミュニティーとして貴重な場になっている

Thank you!