情報ネットワーク法学会第23回研究大会講演1

サイバー法は終わったか？

明治大学法学部教授

夏　井　高　人

はじめに

- サイバー法とのかかわり（下記ブログ記事参照）

  SHPプロジェクト

  http://www.isc.meiji.ac.jp/~sumwel_h/legalinfo/doc/SHIP-proj.htm

  サイバー法とは何か?

  http://www.isc.meiji.ac.jp/~sumwel_h/cyberlaw/doc/doc001.htm

  Cyberlawブログ：Chris Reed

  http://cyberlaw.cocolog-nifty.com/blog/2023/12/post-0a62ec.html

  Cyberlawブログ：英国Bletchley AIサミット：Rishi Sunakの発言

  http://cyberlaw.cocolog-nifty.com/blog/2023/11/post-6db030.html

  Cyberlawブログ：「越境」

  http://cyberlaw.cocolog-nifty.com/blog/2023/12/post-8cfb17.html

  Cyberlawブログ：人生は1回だけ（Life is one time）

  http://cyberlaw.cocolog-nifty.com/blog/2012/11/life-is-one-tim.html

  Cyberlawブログ：情報ネットワーク法学会の講演を終えて

  http://cyberlaw.cocolog-nifty.com/blog/2016/11/post-d2dc.html

  情報社会の素描－EUの関連法令を中心として-（2・完）

  https://meiji.repo.nii.ac.jp/records/1331

- 「サイバー（cyber）」のとらえ方（下記参考訳解説部分1～8頁参照）

  指令(EU) 2022/2555（NIS2 指令）

  http://cyberlaw.la.coocan.jp/Documents/LawandInformationMag_No54.pdf

(ancient Greek)

Κυβερνήτης

cybernetics

(synonym)

automaton

(cool naming)

Cyberspace
(syn. Information network)
(e.g., the Internet)

(logical)

Artificial Intelligence (AI)

(academic area)

Cyberspace Law
(Law of the Horse?)
(e.g., Lawrence Lessig)

Internet Law
(e.g., Chris Reed)

(law enforcement area)

CoE Cybercrime Convention
1st Additional Protocol
2nd Additional Protocol

(practical applications)

Generative AI
(e.g. GPT applications)

Robots
(e.g., network agents, mutants, Cyber physical objects in EU legislation)

Robotics
(see, ISO/TC 299 standards)
(syn. Industrial Robots)

(a classification or nomenclature)

形式的な意味でのサイバー法の検討（日本法）

- サイバーセキュリティ基本法（平成26年法律第104号・最終改正令和4年法律第68号）
- デジタル庁設置法（令和3年法律第36号・最終改正令和5年法律第63号）
- 警察法（昭和29年法律第162号・最終改正令和4年法律第97号）

形式的な意味でのサイバー法の検討（米国連邦法）

- 6 U.S. Code Part A §651-§655: Cybersecurity and Infrastructure Security
- 6 U.S. Code §146: Cybersecurity workforce assessment and strategy
- 10 U.S. Code §391: Reporting on cyber incidents with respect to networks and information systems of operationally critical contractors and certain other contractors
- 6 U.S. Code §1503: Authorizations for preventing, detecting, analyzing, and mitigating cybersecurity threats
- 10 U.S. Code §394: Authorities concerning military cyber operations
- 10 U.S. Code §167b: Unified combatant command for cyber operations

形式的な意味でのサイバー法の検討（EU法）

- 理事会決定(EU) 2023/436[参考訳]

  http://cyberlaw.la.coocan.jp/Documents/LawandInformationMag_No54.pdf

- 指令(EU) 2022/2555（NIS2 指令）[参考訳]

  http://cyberlaw.la.coocan.jp/Documents/LawandInformationMag_No54.pdf

- 指令(EU) 2022/2557 [参考訳]

  http://cyberlaw.la.coocan.jp/Documents/LawandInformationMag_No54.pdf

- 規則(EU) 2019/881（Cybersecurity Act）[参考訳・改訂版]

  http://cyberlaw.la.coocan.jp/Documents/EU%20Regulation%202019%20881%20Translation%20ver%202.pdf

- 規則(EU)2022/2065（デジタルサービス法）[参考訳]

  http://cyberlaw.la.coocan.jp/Documents/LawandInformationMag_No52.pdf

- 規則(EU)2022/868（データ統治法）[参考訳]

  http://cyberlaw.la.coocan.jp/Documents/LawandInformationMag_No53.pdf

- 人工知能規則案（COM/2021/206 final）[参考訳]

  http://cyberlaw.la.coocan.jp/Documents/LawandInformationMag_No45_2.pdf

- AI 法的責任指令案[参考訳]

  http://cyberlaw.la.coocan.jp/Documents/LawandInformationMag_No51.pdf

- 製造物責任指令改正指令案[参考訳]

  http://cyberlaw.la.coocan.jp/Documents/LawandInformationMag_No51.pdf

関連EU法の検討から得られた示唆

- 特に「cybersecurity」,「cybercrime」及び「cyberattack」の分野において,「cyber」の用例に大規模な混乱がある（NIS2指令参考訳の解説参照）。

on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents

≠

on cyber (risk, threats, and incidents) as well as on non-cyber (risks, threats and incidents)

- 「cyber」の概念の再検討の必要性

思考作業用のテンプレート

risks		
	NIS	non-NIS
cyber		
non-cyber		

threats		
	NIS	non-NIS
cyber		
non-cyber		

incidents		
	NIS	non-NIS
cyber		
non-cyber		

NIS2指令の第6条第10号が参照している規則(EU) 2019/881の第2条第8号の定義

risks		
	NIS	non-NIS
cyber	—	—
non-cyber	—	—

cyber threats		
	NIS	non-NIS
cyber	○	×
non-cyber	×	×

incidents		
	NIS	non-NIS
cyber	—	—
non-cyber	—	—

（注）
この定義はENISAの所管事項を限定する目的で定められている。

NIS2指令にそのままあてはめると
（形容詞がない場合cyberとnon-cyberを包摂と仮定）

risks		
	NIS	non-NIS
cyber	○	○
non-cyber	○	○

cyber threats		
	NIS	non-NIS
cyber	○	×
non-cyber	×	×

incidents		
	NIS	non-NIS
cyber	○	○
non-cyber	○	○

as well as

non-cyber risks		
	NIS	non-NIS
cyber	×	×
non-cyber	○	○

threats		
	NIS	non-NIS
cyber	○	○
non-cyber	○	○

incidents		
	NIS	non-NIS
cyber	○	○
non-cyber	○	○

NIS2指令にそのままあてはめると
（形容詞がない場合non-cyberと仮定）

risks		
	NIS	non-NIS
cyber	×	×
non-cyber	○	○

cyber threats		
	NIS	non-NIS
cyber	○	×
non-cyber	×	×

incidents		
	NIS	non-NIS
cyber	×	×
non-cyber	○	○

as well as

non-cyber risks		
	NIS	non-NIS
cyber	×	×
non-cyber	○	○

threats		
	NIS	non-NIS
cyber	×	×
non-cyber	○	○

incidents		
	NIS	non-NIS
cyber	×	×
non-cyber	○	○

NIS2指令にそのままあてはめると
（as well as の前はcyber, as well as の後はnon-cyberと仮定）

risks		
	NIS	non-NIS
cyber	○	○
non-cyber	×	×

cyber threats		
	NIS	non-NIS
cyber	○	×
non-cyber	×	×

incidents		
	NIS	non-NIS
cyber	○	○
non-cyber	×	×

as well as

non-cyber risks		
	NIS	non-NIS
cyber	×	×
non-cyber	○	○

threats		
	NIS	non-NIS
cyber	×	×
non-cyber	○	○

incidents		
	NIS	non-NIS
cyber	×	×
non-cyber	○	○

NIS2指令における語彙の検討結果から得られるもの

- NIS2それ自体の検討に限定した場合，「cyber threats」という語を定義するのではなく，「cyber threats to be noticed to ENISA」という概念を新たに構築し，その定義として規則(EU) 2019/881の第2条の定義を参照すれば良かったのではないか？
- しかし，NIS2の法解釈上の検討から示唆されることはNIS2に限定されない。
- そもそも「cyber」を「cyberspace」に限定しなければならない理由は存在しない。
- 情報ネットワークによって接続されていなくても1つのエコシステムとして認識可能な空間は存在し得る。

考察において考慮に入れられるべき要素

- 指令(EU) 2022/2557からの示唆
- 重要なリスクと脅威を具体的に想定してみると・・・
  - 化学物質による海洋汚染による魚介類の大量死に起因する水路閉塞等の結果としての水冷式冷却システムの機能停止のようなトラブル，天候不順による農作物や山林の大量枯死に伴って飛散する砂礫・微粒子の増加による化学的腐食や物理的汚損・微細な破損等の結果としての各種電子機器の劣化，異常気象による特定の微生物の大繁殖に起因する生物学的腐食の結果としての各種電子機器や送電網の劣化，強度の酸性雨に起因する化学的腐食の結果としての各種電子機器や送電網の劣化，環境ホルモンを含め各種化学薬品による環境汚染の結果としての情報システム管理要員となる自然人の全体的な知的能力や身体状態の劣化のようなリスク
  - ハイブリッドな脅威

実質的な意味でのサイバー法の検討（EU法中心）

Examples of current and future Cyber legal issues

- Cyberspace law
  - NIS:
    - connected automatic vehicle;
    - cyber security of NIS;
    - liability of provider of online platform, etc.
- Cybernetics law (non-Cyberspace law)
  - non-NIS:
    - non-connected automatic driving vehicle;
    - cyber security of independent devices;
    - liability of non-human autonomous entity, etc.

Examples of common legal issues (Cyber or not)

- Processing of mixture of personal data and non-personal data; mixture of real data and virtual data;
- Autonomous M2M communication; Internal communication within a device or digital-chip implanted;
- Identification, authentication, especially of mixture of human and one or more non-human entities.

基本に戻って（NISを構成要素としないサイバーなエコシステムの存否）

- サイバー犯罪条約（CoE Cybercrime Convention）に定めるサイバー犯罪
  - NISを必須の構成要件要素とする犯罪
    - 違法傍受（illegal interception）－第3条
  - NISを必須の構成要件要素としない犯罪
    - 違法アクセス（illegal Access）－第2条
      - 原則：全てのタイプのコンピュータを対象とする。
      - 例外：締約国は，他のコンピュータと接続されたコンピュータに対象を限定できる。
    - データ妨害（data interference）－第4条
  - NISを必須の構成要素とする場合と必須の構成要素としない場合の両方を包摂
    - システム妨害（system interference）－第5条
    - コンピュータ関連偽造（computer-related forgery）－第7条
    - コンピュータ関連詐偽（computer-related fraud）－第8条
    - 児童ポルノ（Offences related to child pornography）－第9条
    - 著作権及び関連権の侵害（Offences related to infringements of copyright and related rights）－第10条

実質的な意味でのサイバー法の検討（総合的所見）

- 形式的な意味でのサイバー法と一致している実質的な意味でのサイバー法の領域
  - サイバーセキュリティ・サイバー回復力
  - サイバー防衛
  - サイバーテロ
  - サイバー犯罪とその捜査，国際協力
- 名称・名目に拘わらず，実質的に見てサイバーな領域
  - 民主主義の根幹にかかわる基本的な情報への一般市民の支障のないアクセスの確保
  - オンラインプラットフォームにおける個人及び法人の電子商取引（金融商品取引を含む。）
  - 偽情報，欺瞞的な情報，市場の競争を歪める情報のオンライン流通
  - 電子証拠，電子認証，電子的な秘匿化，法的に保護されるコンテンツの電子的な追跡，自動的な証拠収集
  - 官庁の事務処理のオンライン化・ネットワーク化（電子的な手段による調達，財務監査の公表を含む。）
  - 文化遺産の保護・関連知識の普及のための情報技術の応用，オープンアクセスの拡充
  - 社会的弱者支援業務のオンライン化・ネットワーク化・より適切な個別化
  - AI技術（GPTを含む。）の濫用による知的財産保護制度の世界規模での壊滅の阻止
  - AI技術の濫用または完全に自律的なAI entity（cybernetics (syn. automaton)）による人間の尊厳の破壊に抗する正当防衛・緊急避難
  - 人間疎外的な効果をもつAI技術の開発・運用を排除・処罰するための堅牢な法制の確立

結論

- **サイバー法は終わっていない**
- その理由は・・・
  - Cyberの本質に迫る学術上の研究と考察には更に時間がかかる
  - Cyberな要素を含む法令や判例の解釈学はこれからも必要
  - Cyberな要素を含む実務に関する調査・評価，情報共有及び訓練はこれからも必要
  - Cyberな問題と関連する消費者教育・消費者保護はますます必要
  - Cyberな攻撃が生死に直結する医療分野及び機械分野における法制上及び実務上の再検討が急務
  - Cyberな問題と関連する法学教育の重要性は今後も重要
  - Cyberな問題を認識・理解できる裁判官・検察官・弁護士の確保・充実が不可欠
  - Cyberな経済と社会に対応するための政府の政策判断の必要性は変わらない
- そして
  - Cyberの本質に関する法哲学上の探求はこれからも続く
  - 社会・経済・学術の進展に伴い，変化するCyberの集合へのあてはめ（包摂の有無）の認識も変化し，再評価と再検討が常に必要となる
  - 「サイバー法」という学術上の領域は，これらの要求事項を満たすための基本的な概念枠組みとしての有用性・実効性・効率性・比例性を維持している

ただし，

分野の別を問わず，

有名大学の権威ある先生の学説を支持し，「通説に与していれば安泰」という時代は

終わった