# サイバー空間の規範

佐々木将宣

# 自己紹介

- 名前: 佐々木将宣
- 興味: サイバー国際情勢
- 近況: 直近の数年、日本政府でサイバー及び情報通信に関する国際関係を担当

# 本日の趣旨

- インターネット・ガバナンスコミュニティと、サイバー規範の概要を共有したい
- 国際的にも発展途上の分野であり、自分も勉強中なので、今日を機会に、自分自身の理解も深められることを期待
- 現在・過去の担当業務や関係政策を職務として紹介するものではなく、全て個人的見解です

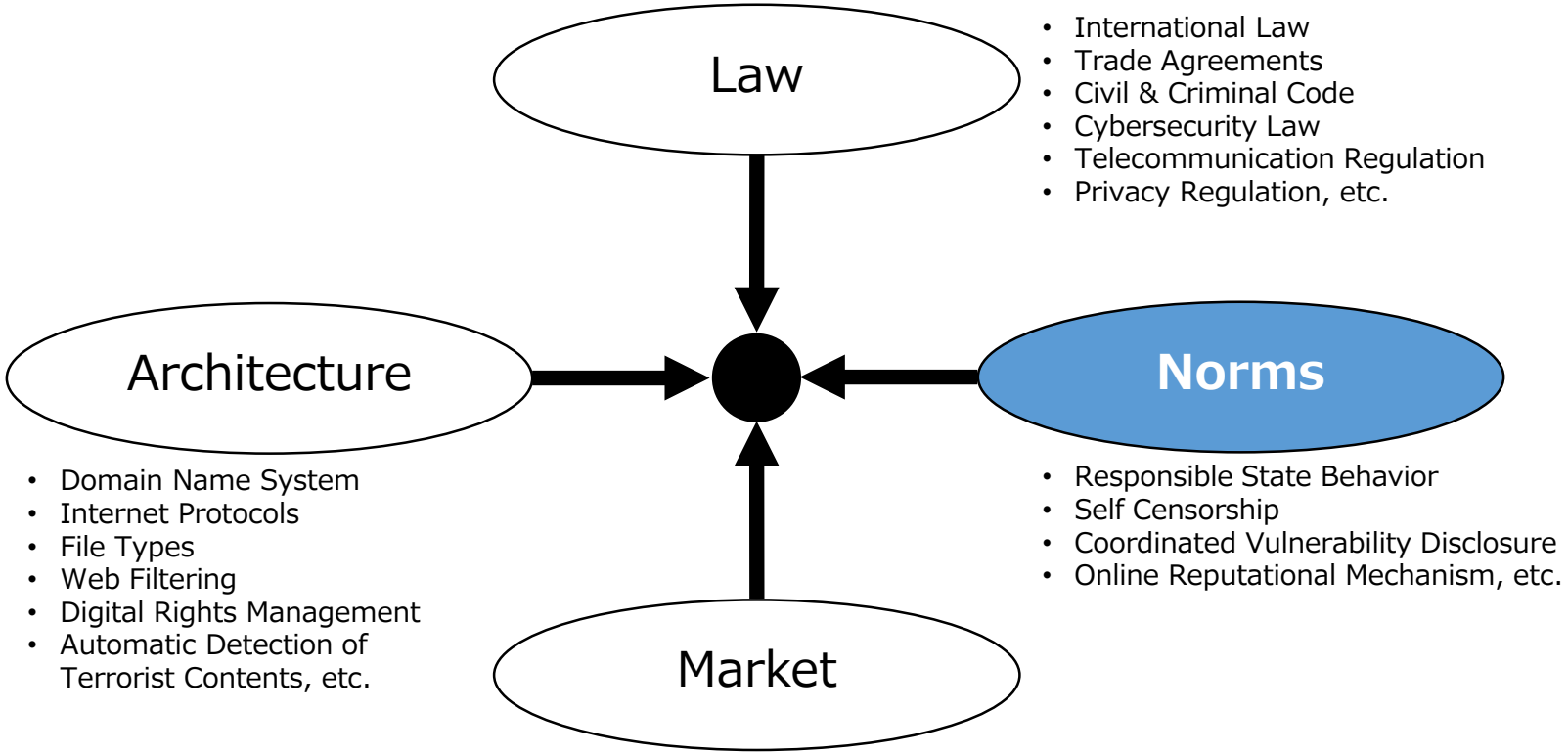
# 「規範」とは～辞書的意味の再確認～

- 社会や集団において個人が同調することを期待されている行動や判断の基準。「行動の望ましさ」も含む。法律などの顕現的なものから、個人や人間関係の中に暗黙のうちに成立しているものまで含まれる。

出典: はてなキーワード http://d.hatena.ne.jp/keyword/%B5%AC%C8%CF

# 規制と規範

- Pathetic Dot Theory by L. Lessig




Reference: Lessig, L. 2007, “Code v2.0”. http://codev2.cc/
※個別事項の例示は発表者

# 「国際規範」とは

- 国際社会における適切な行為の基準・共通了解

出典:西谷真規子,（2018）,「国際規範はどう実現されるか:複合化するグローバル・ガバナンスの動態」, ミネルヴァ書房

# サイバー規範

- サイバーセキュリティ確保のために同調することを期待されている行動や判断の基準
- 規範の主体（規範の名宛人）:
  - 国家 (states)
  - 非国家主体 (non-state actors)
    - 国際機関、産業界、重要インフラ事業者、開発者、セキュリティ研究者、市民 etc.
- 規範の客体（規律される行為）: サイバー規範の形成を目的とした文書の他、サイバーセキュリティ法、サイバーセキュリティ戦略、各種サイバー関連のガイドライン等に埋め込まれている

# サイバー国際規範

- サイバー規範のうち、国際安全保障の確保のために同調することを期待されている行動や判断の基準
- 規範の主体: (これまでは主として)国家。非国家主体に拡大中？
- 分類及び関係文書等:
  - 国際法（のサイバー空間への適用についての整理）
    - 第3回UNサイバーGGE報告書
    - タリン・マニュアル etc.
  - 政治的合意
    - 2015年米中合意 etc.
  - 非拘束的規範（「サイバー空間における責任ある国家の行動」）
    - 第4回UNサイバーGGE報告書
    - G7/G20 declarations & communiqué
    - SCO etc.

# 第3回国連サイバーGGE報告書(2013年)

- 以降のサイバー国際規範の議論の基礎の一つ
  - The application of norms derived from existing international law relevant to the use of ICTs by States is an essential measure to reduce risks to international peace, security and stability.
  - International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.

    抜粋元: 第3回国連サイバーGGE報告書（2013年6月24日）http://undocs.org/en/A/68/98

# 第4回国連サイバーGGE報告書(2015年)

- 具体的なサイバー国際規範を検討して報告
  - States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs
  - States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.
  - States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.
  - States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

    抜粋元: 第4回国連サイバーGGE報告書（2015年7月22日） http://undocs.org/A/70/174

# オバマ・習会談

- 米中首脳による政治的合意
  - The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.
  - Both sides are committed to making common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community.

    抜粋元: FACT SHEET: President Xi Jinping's State Visit to the United States （September 25, 2015）https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

# 2015年G20アンタルヤサミット

- サイバー空間に対する国家の責任について主要国首脳間で確認
  - ICT環境においては、その他の全ての場所と同様に、国家は、安全性、安定性及び他の国家との経済的なきずなを促進する特別な責任を有する。
  - その目的を支持するため、我々は、いずれの国も、企業又は商業部門に競争上の優位性を与えることを意図して、ICTにより可能となる、営業上の秘密その他の企業秘密に係る情報を含む知的財産の窃盗の実行又は幇助をすべきでないことを確認する。
  - 全ての国は、ICTsの安全な使用を確保するに当たり、デジタル通信の文脈におけるものを含め、違法で、かつ、恣意的なプライバシーの妨害からの自由の諸原則を尊重し、保護すべきである。

    抜粋元: G20アンタルヤ・サミット 首脳コミュニケ（仮訳）（2015年11月17日）
    https://www.mofa.go.jp/mofaj/ecm/ec/page4_001553.html

# 2016年G7伊勢志摩サミット

- 有志国首脳による原則と行動の宣言
  - 我々は、国家及びテロリストを含む非国家主体の双方によるサイバー空間の悪意のある利用に対し、密接に協力し、断固とした強固な措置をとることを約束する。
  - 我々は、国際連合憲章を含む国際法がサイバー空間において適用可能であることを確認する。
  - 我々は、一定の場合には、サイバー活動が国際連合憲章及び国際慣習法にいう武力の行使又は武力攻撃となり得ることを確認する。また、我々は、サイバー空間を通じた武力攻撃に対し、国家が、国際人道法を含む国際法に従い、国際連合憲章第51条において認められている個別的又は集団的自衛の固有の権利を行使し得ることを認識する。
  - 我々は、既存の国際法のサイバー空間における国家の行動への適用、平時における国家の責任ある行動に関する自発的な規範の促進並びにサイバーに関する国家間の実務的な信頼醸成措置の発展及び実施から構成される国際的なサイバー空間の安定に関する戦略的枠組みを促進することにコミットする。この文脈において、我々は、2015年の国連政府専門家会合（GGE）の報告書を歓迎するとともに、全ての国に対し、この報告書の評価及び勧告を指針とすることを要請する。
  - 我々は、いずれの国も、企業又は商業部門に競争上の優位性を与えることを意図して、ICTにより可能となる、営業上の秘密又はその他の企業秘密情報を含む知的財産の窃盗を実行し、又は支援すべきでないことを再確認する。

抜粋元: G7伊勢志摩首脳宣言 サイバーに関するG7の原則と行動（仮訳）（2016年5月27日）https://www.mofa.go.jp/mofaj/files/000160315.pdf

# その後の国家主導の動き

- 国連サイバーGGE
  - 第5回国連サイバーGGEは報告書の内容に合意せず2017年6月に終了
  - 2018年11月、国連第一委員会は、第6回国連サイバーGGEの開催及びマルチステークホルダーによるオープンエンド作業部会の開催を決議
- G7/G20
  - 定着に向け既存の合意内容を繰り返し確認

# 法的拘束力のないサイバー国際規範は、国家のサイバー活動を抑止できるか？

- パリ不戦条約（ケロッグ＝ブリアン協定）
  - 1928年
  - 63カ国が署名

# Tallinn Manual

- 国際法学者らによる既存国際法のサイバー空間への適用関係を具体化しようとする試み
- 有事に関するTallinn Manual 1.0（2013年）
- 平時に関するTallinn Manual 2.0（2017年）

# Global Commission on the Stability of Cyberspace (GCSC)

- サイバー分野の有識者中心の規範形成の取組
- 2017～2018にかけ3次に渡ってサイバー規範を公表
  - Non-interference with the public core of the Internet
  - Protecting electoral infrastructure
  - Norm Package Singapore
    - Norm to Avoid Tampering
    - Norm Against Commandeering of ICT Devices into Botnets
    - Norm for States to Create a Vulnerability Equities Process
    - Norm to Reduce and Mitigate Significant Vulnerabilities
    - Norm on Basic Cyber Hygiene as Foundational Defense
    - Norm Against Offensive Cyber Operations by Non-State Actors

    抜粋元:Global Commission on the Stability of Cyberspace https://cyberstability.org/
- インターネット・ガバナンス近縁分野や民主的プロセスもスコープに

# Cybersecurity Tech Accord

- デジタル/サイバー関連産業主導の規範形成の取組
- 2018年4月の規範を公表。合意企業は発足当初の32社から11月現在で69社に拡大
  - We will protect all of our users and customers everywhere.
  - We will oppose cyberattacks on innocent citizens and enterprises from anywhere.
    - We will not help governments launch cyberattacks against innocent citizens and enterprises from anywhere.
  - We will help empower users, customers and developers to strengthen cybersecurity protection.
  - We will partner with each other and with likeminded groups to enhance cybersecurity.

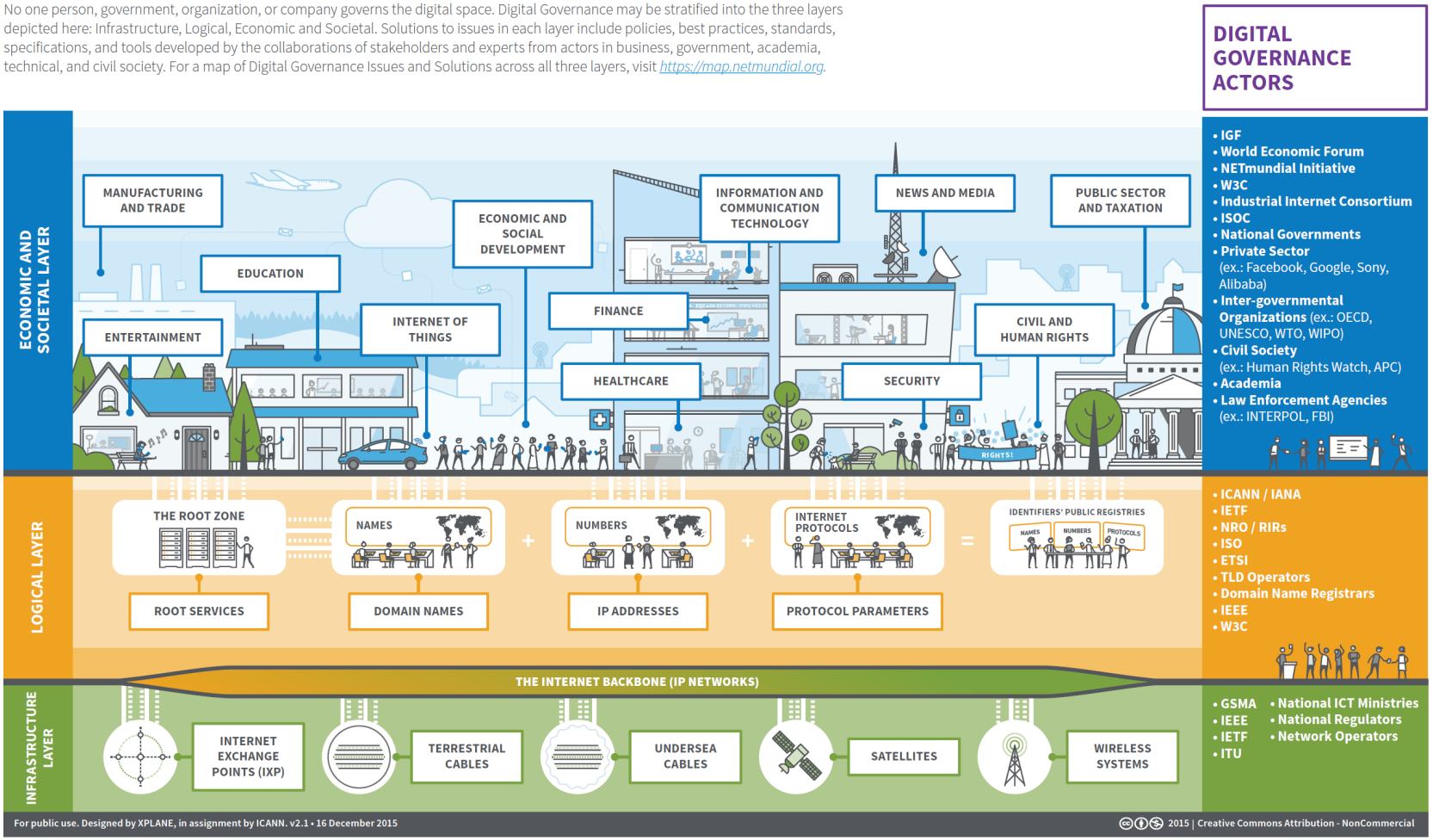
抜粋元: Cybersecurity Tech Accord: https://cybertechaccord.org/about/

# Paris Call

- IGF2018（2018年11月）にてフランス政府主導で提唱
  - 悪意あるオンライン活動の予防と強靭性を向上
  - インターネットのアクセシビリティと完全性を保護
  - 選挙プロセスへの干渉を防ぐために協力
  - サイバー空間を通した知的財産権侵害に協力して対抗
  - 悪意あるプログラムやオンライン技術の拡散を防止
  - デジタル製品やデジタルサービスの安全性ならびにすべての人の「サイバー衛生」を向上
  - サイバー傭兵や非国家主体の攻撃に対する対抗措置を実施
  - 適切な国際規範の強化に協力して取り組む

    抜粋元: サイバー空間の信頼性と安全性のためのパリ・コール （在京仏大による和訳）https://jp.ambafrance.org/article13835
- 我が国を含む51カ国と数百の民間企業・組織が賛同

# インターネットガバナンスとサイバー規範




Source: ICANN https://www.icann.org/news/multimedia/1563

# サイバー国際規範はどう確立されるか？

- 行動として実践？
- 国際場裡で同内容の声明・宣言を繰り返す？
- 逸脱した主体への公の場での非難？
- 逸脱した主体への対抗措置？
- サイバー条約？
- アーキテクチャとして具現化？

# 脆弱性ハンドリングに関するサイバー規範

- Coordinated Vulnerability Disclosure
- Vulnerability Equity Process

# コードとサイバー規範

- コードによる規制というこの仕組みが発達するにつれて、それは独自の規範を持つようになる。その規範は、コードが課す構造やルールの中で表現される。法と経済学の予言が正しければ、この規範は間違いなく高効率となり、公正なものにだってなれる。でも正義が必ずしも効率性に伴わない以上、それはその分だけ高効率で不公正なものとなってしまうだろう、すると問題はこのギャップにどう対応すべきか、ということだ。

出典: ローレンス・レッシグ, （2007）,「CODE 2.0」 pp. 408-409（日本語版）