インターネットガバナンス関連動向

～WSIS+20とエンドツーエンド暗号化をめぐる状況～

2024年から2025年にかけて、インターネットガバナンス界隈では大きな動きが起こっています。2025年の国連総会で「世界情報社会サミット（World Summit on the Information Society, WSIS）」の20年後の評価（WSIS+20）が予定されており、特集3では2025年3月中旬以降のWSIS+20評価の動きについてお伝えします。また、2025年4月1日に欧州委員会が発表した、欧州域内安全保障戦略（ProtectEU）についても説明します。この戦略は、変化する安全保障環境と地政学的状況に対応するための、今後数年間の野心的なビジョンと作業計画を定めています。

WSIS+20の検討状況

本項では2025年3月中旬以降のWSIS+20評価の動きについてお伝えします。WSISとはそもそも何か、および2025年3月中旬までの動きにつきましては、すでにお知らせしていますので以下ページをご参照ください。

- WSISとは（インターネット用語1分解説）
  https://www.nic.ad.jp/ja/basics/terms/wsis.html
- 世界情報社会サミットの20周年評価（WSIS+20 Review），JPNICニュースレター No.89
  https://www.nic.ad.jp/ja/newsletter/No89/0800.html

2025年3月中旬以降の動き

国連総会で、WSISの成果実施に関する包括的な評価の進め方決議（79/277）が採択（2025年3月25日）

この決議では、WSISの成果に関する国連総会による全体的レビューの具体的な様式（modalities）を定めています。総会議長が政府間交渉プロセスを主導する、2名の共同進行役を任命します。同プロセスには準備会合が含まれ、最終的に政府間合意の成果文書が総会のハイレベル会合で採択される予定です。その後5月21日に、ケニア政府国連常駐代表のEkitela Lokaale氏およびアルバニア政府国連常駐代表のSuela Janina氏が共同進行役に任命されました。準備プロセス中、すべての関係者（マルチステークホルダー）との非公式な対話型協議を開催し、政府間交渉プロセスへの意見を収集することになっています。

第28回国連科学技術開発委員会（CSTD）会合（2025年4月7日-11日）

WSIS+20については、4月9日に集中して情報共有および議論が行われました。WSIS+20共同進行役より、進め方についての国連総会決議が採択されマルチステークホルダーで進めることになったことが報告され、次いで、WSIS+20の成果文書の内容の協議に進み、各国連組織からの報告の後、背景文書として、国連貿易開発会議（UNCTAD）よりWSIS+20レビューに向けた、国連事務総長およびCSTD事務局による報告書が紹介されました。その後いくつかの国連加盟国より、主に以下の点について発言がありました。

- デジタル化の現状と課題：全世界で26億人がオフラインであるというデジタル格差は依然として深刻な問題として認識されました
- 新たな技術と倫理的課題：AIガバナンス、偽情報・誤情報、ヘイトスピーチといった新たなオンラインコンテンツの問題が共通の懸念事項です
- 人権と包摂性：米国は多様性・公平性・包括性（DEI）政策に慎重姿勢を示しつつも、WSIS成果の人権要素を擁護。ジェンダー間の不平等、特にインターネットアクセスやデジタルリテラシーにおける格差は多くの国が認識しています
- ガバナンスと国際協力：マルチステークホルダーアプローチの重要性は全参加者が一致して強調する点であり、IGFの恒久的な開催と持続可能な資金確保、および国内・地域IGF（NRI）との連携強化が提言されました。スイスはWSISとGDCの統合的実施ロードマップを提案し、他の多くの国やNGOも、デジタル協力に対する統一されたアプローチを確保し、重複を避け、資源効率を最大化するために、GDCのコミットメントをWSISの枠組みに統合することを強調しました

NGOや市民社会組織は、IGFの恒久化、草の根接続（コミュニティネットワーク）の支援、既存のアクションライン全体にわたりジェンダー主流化を体系的に推進するだけでなく専用のジェンダー・アクションラインの新設、マルチステークホルダー参加の制度化、GDC・SDGsとの整合性、地域間格差是正、市民社会の声の可視化を提言しました。また、気候変動・環境影響への対応、デジタル公共財の視点強化、エンドツーエンド暗号化の重要性、そして民間企業の利害を超えた公的価値への転換を訴えています。

第1回準備会合&現状把握セッション※1（2025年5月30日）

この会議は国連加盟国・オブザーバー向けのものですが、会議の内容がオンラインで中継されました。主な目的は、参加者からの期待

を聴取することと、政府間プロセスの次の段階への「要素文書」による情報提供のためとされています。

共同進行役より理念が再確認された後、今後の主なマイルストーンが共有されました。その後、各国および複数の国からなるグループによる意見表明が続きました。途上国側からはデジタル格差の是正、技術移転、能力開発支援などが主張され、先進国側からはマルチステークホルダーによるガバナンスやIGFの恒久化・強化などが提案されました。日本政府からは、WSISの枠組みを2025年以降も維持すべきこと、IGFを継続・強化し、恒久的なものとすべきこと、WSISとGDCの相互共働でグローバルな課題の解決とSDGs達成などの取り組みを効果的・効率的に進められると確信していること、12月の（国連総会でのWSIS）ハイレベル会合に向けたプロセスに積極的に参画していくこと、などが表明されました。

ユネスコ 公共セクターにおけるAIおよびデジタル転換（DX）に関する能力開発会議（2025年6月4日-5日）

6月5日（2日目）にWSIS+20に関するセッションが集中して開催されました。発表・議論された内容の要点は次の通りです。

デジタル化は著しく進展し、2005年には世界人口のわずか16%だったオンライン接続率は、現在では95%に達したものの、依然として26億人がオフライン状態にあり、なおもデジタル格差が存在しています。デジタル化進展の中で、AIガバナンス、偽情報・誤情報、ヘイトスピーチ、その他の有害なオンラインコンテンツといった新たな課題も浮上しています。また、インターネットアクセスやデジタルリテラシーにおけるジェンダー間の不平等も重要な課題として認識されています。これらの複雑な課題に対処するためには、マルチステークホルダーアプローチが不可欠であり、既存のメカニズムを最大限に活用していく必要があります。特に、デジタル協力に対する統一されたアプローチを確保し、重複を避け、資源効率を最大化するためには、GDCのコミットメントをWSISの枠組みに統合することが強く推奨されています。

WSIS+20ステークホルダーとのコンサルテーション（6月9日および10日）

今回は国連が開催するこの種の意見聴取では初めて、時差を考慮し2回開催されたので、アジア太平洋地域からも参加しやすくなりました。各ステークホルダーの意見をまとめると、WSIS+20レビューが、過去20年間のデジタル化の進展を評価しつつ、デジタル格差、人権侵害、環境影響、情報の集中といった新たな課題に対し、マルチステークホルダーによる協力と、人権を基盤とした、より包括的で一貫性のあるデジタルガバナンスの枠組みを構築する重要な機会である、と言えるでしょう。さらに、WSIS+20レビュープロセス自体の包摂性と透明性についても強く求められました。JPNICは、「マルチステークホルダー主義を支持する技術コミュニティ連合（TCCM）」の提出意見に賛同の署名を行いました。

今後の予定

主に国連経済社会局（UN DESA）が掲載している準備プロセスロードマップによれば、次のようになっています。

- 要素文書（Elements Paper）：6月20日公開予定で、7月15日まで意見募集予定
- IGF 2025（6月23日-27日）
  - ○ IGFのWebサイトにWSIS+20評価関連25セッションの一覧が掲載
- WSIS+20 High-Level Event 2025（7月7日-11日）
  - ○ WSISの次のフェーズへの針路を設定すること、ジュネーブ行動計画以来達成したこと、鍵となる動向、挑戦、機会について振り返ることが目的とされており、セッションは200以上。また、6種類の成果文書が発行される予定
- 成果文書第ゼロ版（zero draft）発行（8月予定）
- 第2回準備会合（10月中旬予定）
- ステークホルダーとのコンサルテーション（10月中旬予定）
- 国連本部における非公式交渉（10月-11月）
- 成果文書案（11月）
- 加盟国およびステークホルダーとのコンサルテーション（11月）
- 第80回国連総会でのハイレベル会議（12月16日-17日）

考察

WSIS+20レビューは国連が進めるプロジェクトのため、最終的には加盟国政府による取り決めが必要になります。一方、政府だけですべてが完結するわけではなく、他ステークホルダーに影響する、もしくは協力を求める部分も出てきます。その観点から、他のステークホルダーへの働きかけおよび意見聴取は重要です。当然、当センターは後者にのみ関わることができ、前者については日本政府およびTCCMなどを通じて間接的に他国政府に頼る必要があります。進め方に関する国連総会決議で（政府以外の）ステークホルダーの意見を聞くと明記されたこと、およびロードマップにステークホルダーとのコンサルテーションが明記されたことは大きな進歩であると考えます。日本政府および他ステークホルダーと協力して動向を注視したいと思います。

これまで表明された各国および各ステークホルダーの意見を総合すると、IGFを継続することはほぼ確実なのではないかという感触を得ていますが、それ以外がどのようになるかは今後少しずつ見えてくるのでしょう。

エンドツーエンド暗号化をめぐる状況

2025年4月1日に欧州委員会（以下、「委員会」）より、欧州域内安全保障戦略（ProtectEU）が発表されました。この戦略は、変化する安全保障環境と地政学的状況（敵対的な外国勢力や国家支援の行為者によるハイブリッド脅威の増加、組織犯罪ネットワークの拡大、

オンラインでの犯罪者やテロリストの活動の活発化）に対応するため、より明確な法的手段、情報共有の強化、協力の深化など、今後数年間の野心的なビジョンと作業計画を定めています※2。主な内容は次の通りです。

1.新たな欧州域内安全保障ガバナンス
2.諜報共有の新たな方法による安全保障上の脅威の予測
3.法執行機関向けの効果的なツールと司法・内務（JHA）機関の強化
4.ハイブリッド脅威に対する抵抗力の構築
5.重大な組織犯罪との闘い
6.テロリズムと暴力的過激主義との闘い
7.安全保障における強力なグローバルプレイヤーとしてのEU

この中で、3. の下に「暗号化に関する技術ロードマップおよび、EUのデータ保持規則の見直しを目的とした影響評価」という項目があり、ProtectEU本文※3の6-7ページには、次の記述があります（下線は筆者による）。

データへの合法的なアクセス
法執行機関と司法当局は、犯罪を調査し、適切な措置を講じる能力を有する必要がある。現在、重大かつ組織的な犯罪のほぼすべての形態にはデジタル足跡（フットプリント）が存在する。犯罪捜査の約85%は、法執行機関がデジタル情報にアクセスする能力に依存している。
（中略）
ハイレベルグループの勧告を踏まえ、委員会は2025年上半期に、データへの合法的かつ効果的なアクセスを確保するための法的・実務的な措置を定めるロードマップを提示する。このロードマップのフォローアップとして、委員会はEUレベルでのデータ保持規則の影響評価を優先し、暗号化に関する技術ロードマップの策定を進める。これにより、サイバーセキュリティと基本権を保護しつつ、法執行機関が暗号化されたデータに合法的にアクセスするための技術的解決策を特定し評価する。

さらに、同10ページでは、委員会は、以下の措置を講じるとなっています：

- 2025年までに、法執行機関によるデータへの合法的かつ効果的なアクセスに関する今後の道筋を定めるロードマップを提示する（中略）
- 2026年までに、法執行機関によるデータへの合法的アクセスを可能にするための技術的解決策を特定し評価する、暗号化に関する技術ロードマップを提示する

これ以上の詳細についての記載はありませんが、これらはすなわち、法執行機関が暗号化されたデータへアクセスできるようにするということで、そのためには暗号化メカニズムに裏口（バックドア）を設けることを意味すると解釈できます。

これに対して、Internet Societyが会員となっているGlobal Encryption Coalitionは、ProtectEUの、エンドツーエンド暗号化への潜在的影響に関する懸念を表明する内容の公開書簡※4を欧州委員会へ送り、それにはJPNICも署名しました。書簡に記載された懸念点の概要は、次の通りです。

- 「暗号化に関する技術ロードマップ」への懸念：ProtectEU戦略に含まれる「法執行機関が暗号化されたデータに合法的にアクセスできるようにする技術的ソリューションを特定・評価するための暗号化に関する技術ロードマップ」の枠組みに対し、深い懸念を表明
- 強力な暗号化の重要性：増加するセキュリティ脅威（サイバー攻撃、ハイブリッド脅威、スパイ活動、重要インフラへの攻撃）からサイバースペースの完全性を保護するためには、エンドツーエンド暗号化を含む強力な暗号化が不可欠であると主張。世界中の政府機関も、暗号化の使用を奨励していることを指摘
- EU自身の政策との矛盾：欧州委員会自身が、ネットワークおよび情報セキュリティ指令（NIS2）の改定でサイバースペースの完全性を保護するための投資の必要性を認識しており、暗号化を適切なサイバーセキュリティリスク管理措置の一つとして挙げている。また、欧州データ保護監督官も「暗号化への制限は経済と社会全体に重大なリスクをもたらす」と述べている
- 暗号化の弱体化/回避策への継続的な焦点への批判：これらの背景にもかかわらず、委員会が暗号化を弱体化または回避する方法を特定し続けることに深い懸念を持つ。これは、ProtectEU戦略が強調するレジリエンスと準備の重要性という、EU自身の安全保障目標を損なうものであると指摘
- クライアントサイドスキャンへの反対：特に、暗号化メカニズムが始まる前にユーザーデバイスをスキャンすることで暗号化を回避する「クライアントサイドスキャン」のような技術に過去および現在もEUが焦点を当てていることを批判。このようなスキャンは、エンドツーエンド暗号化の約束を破るだけでなく、犯罪者や敵対的な国家アクターに悪用される可能性のある脆弱性を生み出すと述べている。技術専門家の間では、暗号化回避ツールが国家安全保障を脅かす新たなリスクを生み出すという幅広い合意があることを強調

日本政府は2020年に同様の方向性を目指している「エンドツーエンド暗号化及び公共の安全に関する国際声明」に署名しているため※5、同様な動きが出てくる懸念はあります。例えば、2025年3月4日に自民党から石破首相に対して申し入れがなされた、「組織的な詐欺から国民の財産を守るための対策に関する緊急提言」※6には、「匿名性の高い通信アプリ等の通信内容や登録者情報等を把握するための措置の検討」という項目があり、通信内容を把握するためにはエンドツーエンド暗号化を回避する何らかの手段が必要と考えられることから、政府内でそのような手段について検討がなされている可能性はあり、今後の動向を注視したいと思います。

（JPNIC インターネット推進部 山崎信）

※1 https://publicadministration.desa.un.org/wsis20/1stPreparatoryMeetingStocktakingSession
※2 （プレスリリース）Commission unveils ProtectEU – a new European Internal Security Strategy https://ec.europa.eu/commission/presscorner/detail/en/ip_25_920
※3 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0148
※4 https://www.globalencryption.org/2025/05/joint-letter-on-the-european-internal-security-strategy-protecteu/
※5 エンドツーエンド暗号化と法規制、JPNIC Blog, https://blog.nic.ad.jp/2020/5545/
※6 https://www.jimin.jp/news/policy/210075.html