総務省

ＩＣＴ政策を巡る世界の動き

平成２８年６月１６日

総務省情報通信国際戦略局

WSIS＋10 ／ G7 ／ G20

国連総会WSIS（世界情報サミット）＋10の成果

1　経緯

（1）WSISは、国連主催の会議として、2003年ジュネーブ、2005年チュニスの二回に分けて行われ、その際、デジタルデバイド解消等の取り組みについてアクションラインを定めるとともに、10年後（2015年）の国連総会におけるハイレベルのレビューを行うことを決定。

（2）今般、昨年12月15日・16日に国連総会WSIS+10ハイレベル会合がニューヨークの国連本部で行われ、2012年のITU世界国際電気通信会議（WCIT）（先進国と途上国の意見が対立したまま閉会）の再現の可能性もあったが、各国の努力により合意文書が採択。

2　主な会合内容

（1）情報社会サミットは、「人間中心の、包括的な開発志向の情報社会の構築」の観点から重要であり、10年間の取組みは、大きな成果を挙げていることにつき各国間で合意。一方、デジタルディバイドの解消などの課題が未だ残っていることも認識。

（2）インターネットガバナンス、サイバーセキュリティ分野等について、「政府によるマルチラテラルな管理・国連主導の新たな仕組み・政府主導の取組み」との考え方と、「マルチステークホルダー（政府、民間、学術、市民団体がそれぞれ役割を果す）・既存の枠組みの活用」との考え方が大きく対立。一部両論を併記する形や、マルチステークホルダーの取組を記載した形で合意。

（3）IGF(インターネット・ガバナンスフォーラム）は10年間延長で合意。

（4）次回ハイレベル会合は10年後の2025年に開催することで合意。

会議場風景（10日）

（参考）チュニスアジェンダ・アクションライン（2005年）

アクションライン	促進機関（ファシリテーター）
1. 開発のためのICT利活用における公的政府当局及び全ての関係者の役割	ECOSOC/国連地域委員会/ITU
2. 情報通信インフラ	ITU
3. 情報・知識へのアクセス	ITU/UNESCO
4. 人材開発	UNDP/UNESCO/ITU/UNCTAD
5. ICTの利用における信頼性とセキュリティの確立	ITU
6. 環境整備	ITU/UNDP/国連地域委員会/UNCTAD
7. ICTアプリケーション • 電子政府 • eビジネス • eラーニング • eヘルス • e雇用 • e環境 • e農業 • eサイエンス	 UNDP/ITU WTO/UNCTAD/ITU/UPU UNESCO/ITU/UNIDO WHO/ITU ILO/ITU WHO/WMO/UNEP/UN-Habitat/ITU/ICAO FAO/ITU UNESCO/ITU
8. 文化的多様性と独自性（アイデンティティ）、言語の多様性、ローカルコンテンツ	UNESCO
9. メディア	UNESCO
10. 情報社会の倫理的側面	UNESCO/ECOSOC
11. 国際的及び地域的協力	国連地域委員会/ UNDP/ITU/UNESCO/ECOSOC

G7香川・高松情報通信大臣会合　開催結果①

１．日時・場所

○　日時：2016年4月29日（金）15:00～17:30、4月30日（土）10:15～11:25
○　場所：香川県　高松市　かがわ国際会議場

２．参加者

【日本側】高市総務大臣（議長）、林経済産業大臣、松下総務副大臣、
　　輿水総務大臣政務官
【G7,EU,OECD,ITU】G7各国、EU、国際機関代表（ITU、OECD）が参加

３．主な開催結果

（１）会合における主な議論

①新たなICTがもたらすイノベーションや経済成長

・IoT、ビッグデータ、AIなどの次世代技術のイノベーションを促進することで一致した。
・AIの社会経済へのインパクトの分析と開発原則の検討を提案し、高い評価と賛同を得た。（スライド９参照）

②情報の自由な流通とサイバーセキュリティ

・情報の自由な流通とインターネット管理への産学の参画の原則を再確認し、同時に、ICTのテロや犯罪への悪用に対し、強く反対することで一致した。

③ICTによる地球規模課題の解決

・2020年までに世界中で新たに15億人をインターネットに接続可能とするなど、デジタルディバイドを解消することで一致した。
・高齢化社会や防災など、Ｇ７が先進的な知見を有する分野におけるICTの活用を推進し「持続可能な開発のための2030アジェンダ」の実現への寄与を確認した。

④国際連携と国際協力

・あらゆる人やモノがグローバルにつながる「デジタル連結世界」の実現に向けた基本理念や行動指針をとりまとめた「憲章」と「共同宣言」とを採択し、同時に「共同宣言」の附属書として「協調行動集」を策定した。

G7香川・高松情報通信大臣会合　開催結果②

３．主な開催結果（続き）

（２）G7 ICTマルチステークホルダー会議（4月29日（金）9：00～14：50）

○産学のICT分野のリーダー達が集まり、ダボス会議方式で、下記のテーマについて集中的に議論した。

（テーマ）①　ICTによるイノベーションと経済成長
②　インターネットガバナンス及びサイバーセキュリティの共通認識の確立
③　地球規模課題の解決とデジタル連結性

○松下総務副大臣の挨拶、G7各国等の代表による基調講演の後、各テーマについて議論が行われ、会議の結果は30日（土）の大臣会合にて報告された。

○会合には300人が参加するとともに、インターネットでライブ配信が行われた。

（３）ICT関連展示視察（4月30日（土）午前）

○「2020年に向けた社会全体のICT化」に関する展示を高市総務大臣が視察した。（ICT関連12社・団体が出展）

○同展示は、4月28日～30日の3日間、一般公開され、延べ3500人が来場した。

（４）高松市商店街視察（4月30日（土）午後）

○視察先の高松丸亀町商店街は商店街振興組合を中心に民間主導で再開発に成功した。

○同商店街は、「多言語音声翻訳システム」の実証実験や無料公衆無線LANの整備などを積極的に行っており、高市総務大臣がは最新のＩＣＴが地方創生、地域経済の活性化に貢献する現場を視察した。

（５）直島エクスカーション（4月30日（土）午後）

○大臣会合終了後、香川県・高松市が直島へのエクスカーションを主催した。

○浜田香川県知事がG7各国等の代表を瀬戸内の美しい景観を損なわないように建物の大半が地中に埋設された「地中美術館」に案内した。

G7情報通信大臣会合　デジタル連結世界憲章の概要
ー Charter for the Digitally Connected World ー

意義：ICTによるイノベーションを通じた経済成長の実現と地球規模課題の解決による持続的・包摂的成長を目指し、G7として中長期的に推進すべき戦略を共有する。

（デジタル連結世界憲章の構成）

【目標】

ICTによる社会の更なる繁栄
- ICTは社会の繁栄に貢献。テロ・犯罪への悪用に協力して対抗。

イノベーションによる経済成長
- 新たなビジネスモデルやイノベーションを通じて成長を促進し、雇用と富を創出。

持続的・包括的成長
- ICTにより医療、教育、農業、防災など、国連総会で採択された2030アジェンダの地球規模課題に対処。

【基本原則】

サイバー空間における人権の保護
- サイバー空間でも実空間と同じ人権を保護。

情報の自由な流通の確保
- イノベーションと成長の源泉となる情報の自由な流通を確保。

マルチステークホルダーアプローチの支持
- サイバー空間の政策策定には産学官やユーザなどすべての関係者の幅広い関与が必要。

連結性、包摂性の強化
- 人・モノのネットワークへの連結性強化が重要。

【戦略】(→共同宣言に具体的に記述)

アクセスの向上
- 全世界で質の高い情報通信インフラへのアクセスを協働して推進。

情報の自由な流通の確保
- プライバシーやセキュリティに配慮しつつ情報の自由な流通を確保。

イノベーションの推進
- ICTはデータの利活用を通じ生産性の向上と雇用を創出。標準化、人材育成、次世代技術の推進等により恩恵を最大化

地球規模課題への貢献
- ICTによる課題解決を促進。

包括的な国際協力
- デジタル連結世界の効用を最大化するため産学官のすべての関係者が協力。

G7情報通信大臣会合　共同宣言の概要
ー Joint Declaration by G7 ICT Ministersー

意義：憲章の戦略に基づき、短期的な観点から取り組むべき具体的な行動・措置に関する認識を共有する。

（憲章の構成）（再掲）

【戦略】

アクセスの向上

情報の自由な流通の確保

イノベーションの推進

地球規模課題への貢献

包括的な国際協力

（共同宣言の構成）

【アクション】（抜粋）

アクセスの向上

- 開発機関等あらゆる関係者の参画によるデジタルディバイドの解消推進
- 研究・教育ネットワークの発展と相互接続の拡大、及びその利用の促進
- 質の高いインフラ実現のための投資と競争促進的政策・制度
- 女性、高齢者、若者、障がい者や遠隔地のICTアクセスとリテラシーの向上

情報の自由な流通の確保

- オープンなインターネットの推進、データローカライゼーション要求等不当な制限への反対
- プライバシーバイデザインなど積極的なプライバシー保護の推進
- サイバーセキュリティの重要性の認識共有およびリスク分析に基づく取組の推進
- 人材育成の推進によるセキュリティの向上

イノベーションの推進

- IoT、ビッグデータ、AI、5Gなどの次世代技術の促進
- 相互接続性のための産業界主導による標準化の尊重
- 新たなニーズに対応する人材育成と中小企業支援
- 量販品のソースコード開示禁止を含む知的財産の保護

地球規模課題への貢献

- ICTによる健康、高齢化、教育、女性活躍等への貢献

包括的な国際協力

フォローアップ

- 2017年にG7情報通信大臣会合を開催してフォローアップ（議長国：イタリア）

G7情報通信大臣会合　協調行動集の概要
― G7 Opportunities for Collaboration―

意義：憲章および共同宣言の理念を実現するために、各国の具体的取組事例を共有した上で、メンバー国が協力して行動しうる取組とその方向性を明確にし、相互の参画や連携の強化を図る。
また、これらの分野の重要性についてOECD等の国際機関とも共有し、連携の推進に取り組む。

協調行動集のポイント

●ICTアクセスの向上

ブロードバンドへのアクセスの向上を図り、世界のデジタルディバイドの解消を推進するため、質の高いインフラ整備を促進。

（関連する事例）

・質の高いインフラ構築パートナーシップ（日本）
・Global Connect Initiative（米国）（注１）など

（注１）米国務省が2015年９月に立ち上げたイニシアティブ。2020年までに世界の15億人を新たにインターネットに接続しようとするもの。

●サイバーセキュリティの向上

サイバーセキュリティの向上に資するために、セキュリティに関する指標開発や情報共有を推進

（関連する事例）

・リスクベースの共通指標の検討（日本）
・NICTERへの参加（日本)
・ISACの連携（日本）
・Core Infrastructure Initiative （米国）(注２）

（注２）オープンソースソフトのセキュリティ監査、脆弱性補正

●イノベーションの推進

新たなICTの構築するデジタル連結世界の進展を促進するため、IoT社会に関する社会経済分析やIoT推進に関する民間団体の連携支援を推進

（関連する事例）

・AIネットワーク化の社会経済へのインパクト分析および開発原則に関する議論と情報共有（日独伊)
・IoT推進の官民イニシアティブの国際連携推進（日独仏）
・Human Brain Project（EU)　（注３）　など

（注３）EUが主導するオープンな研究データ共有の枠組み。人間の脳を研究し人工知能技術の開発に利用するもの。

●地球規模課題への貢献

地球規模課題に貢献する情報共有や協力を推進。

（関連する事例）

・ 高齢化に対応するコミュニケーションロボットの研究開発結果に関する情報共有（日EU)

（参考）AIの研究開発の原則の策定について

高市総務大臣より、会合において、AIの研究開発の原則について議論を行うべきとして、以下の提案を行った。

・OECDプライバシーガイドライン、同・セキュリティガイドライン等を参考に、関係ステークホルダーの参画を得つつ、**研究開発に関する原則を国際的に参照される枠組みとして策定**することに向け、検討に着手することが必要。

・研究開発に関する原則の策定に当たっては、少なくとも、次に掲げる事項をその内容に盛り込むべき。

① 透明性の原則

AIネットワークシステムの動作の説明可能性及び検証可能性を確保すること 。

② 利用者支援の原則

AIネットワークシステムが利用者を支援するとともに、利用者に選択の機会を適切に提供するよう配慮すること 。

③ 制御可能性の原則

人間によるAIネットワークシステムの制御可能性を確保すること 。

④ セキュリティ確保の原則

AIネットワークシステムの頑健性及び信頼性を確保すること 。

⑤ 安全保護の原則

AIネットワークシステムが利用者及び第三者の生命・身体の安全に危害を及ぼさないように配慮すること 。

⑥ プライバシー保護の原則

AIネットワークシステムが利用者及び第三者のプライバシーを侵害しないように配慮すること 。

⑦ 倫理の原則

ネットワーク化されるAIの研究開発において、人間の尊厳と個人の自律を尊重すること。

⑧ アカウンタビリティの原則

ネットワーク化されるAIの研究開発者が利用者等関係ステークホルダーへのアカウンタビリティを果たすこと。

Ｇ７サミット成果文書におけるサイバー（ICT）関連の記述

首脳宣言における記述

○ 経済成長の基盤としてのオープンで透明かつ自由なインターネットを強く支持。

○インターネットが自由、民主主義、人権というG7共通の価値の発展に貢献することを支持。

○テロリストを含むサイバー空間の悪用に協力して対抗。

○既存の法の適用と国際規範の構築を進め、信頼醸成を促進。

○情報の自由な流通とインターネットガバナンスに関するマルチステークホルダーアプローチを遵守。

○デジタル連結世界の潜在力を最大化し、デジタルディバイドの解消等、2030アジェンダに貢献。

○独立文書「サイバーに関するG7の原則と行動」を承認。

○サイバーに関するG7作業部会の設置に合意。

サイバーに関するＧ７の原則と行動（Annex）　における記述

【目指すべきサイバー空間】

○オープンで透明かつ自由なインターネットが成長と成功の鍵であることを確認。

○情報の自由な流通が経済社会及び開発を促進する基本原則であることを再確認。

○インターネットガバナンスに関するマルチステークホルダーアプローチの遵守を強調。

○サイバー空間における人権の尊重と法の支配を促進。

○ICTの地球規模課題への貢献と2030アジェンダの推進を強調。

【サイバー空間における安全及び安定の促進】

○テロリストを含むサイバー空間の悪用に協力して対抗。

○テロリストによるリクルート、資金調達、訓練などへの悪用の増加を懸念。

○相互の信頼を促進しリスクを軽減するための国家間のサイバー空間信頼醸成措置の開発・実施を支持。

【デジタル経済の促進】

○ 次世代技術によるイノベーションが成長、雇用や富の源泉であり、連結性の向上、標準化の推進、ビジネス阻害措置への対処などの政策を推進。

○情報の自由な流通を推進するとともに、個人データ保護などの公正な目的への対処にしかるべく配慮。

○適切なプライバシー保護、セキュリティの向上がビジネス上の信頼を確保し、イノベーションを推進することを認識。

○データローカライゼーションやソースコード移転の強制は、公共目的のために正当化されない限りは採用・維持されるべきでないことを確認。

○知的財産の保護の重要性を再確認。

○デジタル連結世界憲章の採択を歓迎。

【G7の一致した行動】

○デジタル連結世界が経済成長と持続的発展に持つ潜在力を最大化するよう協力。

○デジタルディバイドを解消し、ICTへのアクセスとリテラシーの向上を図ることでICTによる社会の繁栄を促進。

○金融、エネルギー、通信などの重要インフラに関するリスク情報の共有を進めサイバーセキュリティの向上を確保。

欧　　州

①欧州のデジタル単一市場（DSM）戦略の動向

- 2015年５月６日、欧州委員会は、28加盟国の障壁をなくし、欧州全体を一つのデジタル市場として統合することを目的に**デジタル単一市場(DSM: Digital Single Market)**に関する戦略文書を公表した。

- DSM戦略は、ユンカー欧州委員長が掲げる優先政策課題の１つであり、デジタル単一市場の実現に向け、３つの柱の下に**16の施策**を掲げている。

- 2016年6月現在、パブリックコンサルテーション等を経て、既にいくつかの施策については法案の提出等が行われたところであり、**2016年末までに全ての施策について欧州委員会から提案がなされる予定**。

- 欧州委員会は、デジタル単一市場の実現により**最大4,150億ユーロ**の経済成長に寄与すると予測している。

※欧州委員会デジタル単一市場戦略文書本文より

（参考）１６の施策項目

１．域内における消費者及び企業によるデジタル財・サービスへのアクセス向上

① 越境電子商取引を可能とするルール作り（契約ルールの調和化等）
② 消費者保護ルールの迅速・統一的な執行（加盟国当局の連携強化等）
③ 小包配送の効率化・低廉化を通じた電子商取引の活性化
④ 不公正な地理的ブロッキング（自国からのネット接続のみ許可する等の商慣行の廃止）
⑤ 電子商取引市場の潜在的な競争上の課題を特定するための反トラスト調査
⑥ 著作権法制の見直し（ＥＵ市民の越境コンテンツ利用の容認等）
⑦ 衛星・ケーブル指令の見直しを通じた放送事業者のサービス範囲の拡大等
⑧ 付加価値税（ＶＡＴ）法制の見直しを通じた越境物販の促進

２．デジタル・ネットワーク及び革新的サービスを促進するための環境づくり

⑨ 電気通信規制の見直し（ネット中立性の規定、域内ローミングの廃止）
⑩ 視聴覚メディア規制の見直し
⑪ オンライン・プラットフォーム事業者の見直し
⑫ 個人データ保護規則案の採択及びe-プライバシー指令の役割に関する包括的分析
⑬ 官民連携を通じたサイバーセキュリティの強化

３．デジタル経済の成長の最大化

⑭ 欧州域内のデータ流通の促進（欧州データの自由流通イニシアティブ、欧州クラウド）
⑮ 標準化及び相互運用性の促進
⑯ デジタル・スキルの向上、電子政府アクションプランの改定

（参考）欧州個人データ保護規則

- 2015年12月15日、欧州委員会、ＥＵ理事会及び欧州議会の三者において基本合意された。
- 2016年4月14日、欧州議会本会議で可決。2年後の2018年5月に施行。

合意された規則案の概要

（１）　ＥＵ域内における規制の単一化・簡素化

①ＥＵ法令が全加盟国に同一に直接適用されるよう、国内法制化の不要な「規則」に変更
②複数加盟国にまたがる事業者や事案を取り扱う場合、一つの監督機関が主管として対処する制度の導入

（２）　より強固な個人データ保護ルールの整備

①「忘れられる権利」に関する規定の導入
②「データ持ち運びの権利」を規定
③「プライバシー・バイ・デザイン」原則の導入
④　データ管理者のデータ漏えい時の通知義務（監督機関に対しては72時間以内に通知）
⑤　制裁金の引き上げ（最大2,000万ユーロまたは全世界年間売上高の４％の制裁金）

（３）　グローバルな課題への対応

①域外事業者への適用（原則として域外事業者はＥＵ域内に代理人を置くべき旨の規定（第25条）の導入等）
②十分性認定見直しメカニズムの導入（既存の十分性認定を最低４年ごとに見直す）

※上記情報はリーガルチェック前の条文に基づくもの

（参考）新たなデータ保護規則に基づく主な越境データ移転の手段

十分性認定（第41条）

- 欧州委員会が認定するに当たり、法の支配、司法的救済、独立したデータ保護機関の存在等を考慮要素とする
- 既存の十分性認定について最低４年ごとの見直し

国・地域全体の十分性認定

- スイス、アルゼンチン、イスラエル、アンドラ、ガーンジー、マン島、ジャージー、フェロー諸島、ウルグアイ、ニュージーランド

特定分野の十分性認定

- カナダ（民間部門）、米欧セーフハーバー（民間部門）、ＰＮＲ(乗客名簿)協定

十分性認定がない場合
↓
適切な安全管理措置（第42条）

拘束的企業準則（Biding Corporate Rule）

- 整合性メカニズムに基づき監督機関から承認された拘束的企業準則（ＢＣＲ）に基づくデータ移転

標準契約条項（Standard Contractual Clauses ）

- 欧州委員会が採択した標準契約条項（ＳＣＣ）に基づくデータ移転

行為規範（Code of Conduct）

- 拘束的かつ強制的なコミットメントが付与された、第３８条に基づき監督機関より承認された行為規範に基づくデータ移転

認証メカニズム

- 拘束的かつ強制的なコミットメントが付与された、第３９条に規定するＥＵ域内の認証機関によって運用されるデータ保護認証メカニズムに基づくデータ移転

適切な安全管理措置がない場合
↓
例外規定（第44条）

- データ主体からの同意取得
- データ主体との契約履行に必要な場合
- 公共の利益の重大な根拠
- データ主体の重大な利益の保護　等

（参考）規則案の議論の経緯

欧州議会案（2014）	欧州理事会案（2015）
１．域内統合	
● ＥＵ法を各国に直接適用	● ＥＵ法を直接適用。各国の上乗せ規制を許容。
２．個人の権利	
● 現行法上の権利を明確化。 ● 「忘れられる権利」を創設。削除要求を受けた事業者は、自ら削除することに加え、データが複製された先の第三者に対して通知し、当該第三者も削除を義務づけ ● 個人データの漏えい時の本人・当局への通知を義務づけ	● 現行法上の権利を明確化。 ● 「忘れられる権利」については、削除要求を受けた事業者は、費用対効果を勘案し、第三者に対して通知すればよい（第三者の削除義務は免除） ● 漏えい時の通知は、深刻なケースに限定。当局へは72時間以内で可。
３．事業者の義務	
● データ保護監督者の設置義務 ● 最大**1億ユーロ**又は**世界売上の5%相当**（高額な方）の課徴金。	● データ保護監督者の設置義務 ● **100万ユーロ**か**世界売上の2%相当**の課徴金。
４．グローバル対応	
● 域外事業者への法適用の明確化。 ● 既存の十分性認定は失効。 ● 第三国の判決等による情報開示を禁止。	● 域外事業者のうち、データを頻繁に取り扱わない者等に対する法適用を免除。 ● 既存の十分性認定は維持。

【三者合意の概要】

- ＥＵ法を直接適用するが、各国の上乗せ規制を一部許容

- 現行法上の権利を明確化。
- 「忘れられる権利」を創設。削除要求を受けた事業者は、費用対効果を勘案しつつ、第三者に対して通知義務を負う。
- 漏えい時の通知については、深刻なケースに限定し、当局への通知は72時間以内。

- データ保護監督者の設置義務
- 最大2,000万ユーロか世界売上の4%相当の課徴金（高額な方）

- 域外事業者のうち、データを頻繁に取り扱わない者等に対する法適用を免除。
- 既存の十分性認定は維持し、最低４年毎の見直しを行う。

③EU-US Privacy Shieldの動向

- 2016 年2月2 日、欧州委員会は、米政府との間で、データ流通に関する新たな枠組みについて合意した旨発表。同年2月29日、欧州委員会が文書全文を公表。
- 4月13日、第29条作業部会（各加盟国のデータ保護監督機関の代表者等で構成される機関）が、合意テキストに対する意見を公表。現在、意見を踏まえて、米ＥＵ間で改めて協議が行われており、６～７月頃に最終的なテキストを公表する予定。

欧州委員会-米商務省間の合意文書で定められた事項（欧州委員会報道発表より）

合意文書は、米国に、厳しく監視と執行を要求し、欧州データ保護機関との連携を強化する内容となった。

（１）商業セクター　－企業に対する強い規制と執行力

- 強い透明性の確保 *(企業へ年1回以上の自己申告書の提出、自社のプライバシーポリシーの宣言、該当リンク設置の義務づけ　等)*
- データ保護規則による監視メカニズムの遵守
- 原則に従わない場合の制裁及びプライバシーリストからの除外

（２）救済策

- 企業に対する義務：　企業は45日以内に個人からの苦情に対して回答する義務の規定
- 無料での代替的な紛争処理手続を提供
- データ保護機関は米国商務省と連邦取引委員会（FTC）が連携して、ＥＵ市民の苦情に対応する。
- 調停機能「プライバシーシールドパネル」の創設

（３）米国政府のアクセス　－明確なセーフガードと透明性の義務

- 国家安全当局によるデータへのアクセスは明確な制限、安全措置及び監視メカニズムに従う旨を初めて文書にて確認
- 米国の機関による無差別な大規模監視の禁止
- 国家情報当局によるアクセスに関する苦情に対して、新たにオンブズマン制度を創設。

（４）監視 -実施状況モニターのため、毎年の共同レビューの開催。

- プライバシーシールドと米国の書面の機能についてのデータへのアクセス等の監視
- 国家インテリジェンスの専門家と連携して、欧州委員会と米国商務省によって共同レビューの実施
- ＮＧＯや米国プライバシー法制のステークホルダーとの年一回のプライバシーサミットを開催
- 欧州委員会による毎年の共同レビュー及びその他の関連情報に基づいたレポートの発行

（参考）EU-US Privacy Shieldの動向

テキスト公表を受けての米欧政府関係者による声明概要

（1）プリツカー商務長官

- プライバシー・シールドは，何千もの欧米ビジネス及び何百万もの個人がオンライン上のサービスにアクセスし続けることができることを確保し、デジタル経済の成長に確実性をもたらす。

（2）ラミレス連邦取引委員会（FTC）委員長

- 今回の新たな合意”の下、連邦取引委員会は、消費者の情報・プライバシー保護に関する我々のより大きな取組の一部として位置づけられる本枠組みに基づく法執行を優先的に継続して行う。

（3）アンシップ欧州委員会副委員長

- 米欧は、市民の個人データがデジタル時代に適した形で完全に守られることを確保する。

（4）ヨウロバ欧州委員会委員

- プライバシー・シールドは、初めて、米国のパートナーに国家のセキュリティの公的機関によるデータアクセスに関する制限とセーフガードを約束させた。この強固なセーフガードは、米欧のデータフローを信頼のできるものにする。

※ 米国国家安全保障局（NSA）による個人データへのアクセスが発覚したことを受け（スノーデン事案）、従来からの米欧間の個人情報移転の枠組みであった「セーフハーバー協定」ではEU市民のプライバシーが十分に保証されないとして、2015年10月に欧州司法裁判所がセーフハーバー協定に無効判決を下した。
これを踏まえ、米国商務省と欧州委員会間でセーフハーバーに代わる新たな個人情報移転に関する新たな枠組み「プライバシー・シールド」が創設。プライバシー・シールドでは、EU市民の個人情報を保護するためのより強力な責任を求めるべく、米国商務省や連邦取引委員会(FTC)に対してより強力な監視・執行権限を求める等の内容が規定された。

④欧州ネットワーク・情報セキュリティ（ＮＩＳ）指令

- 13年2月7日、欧州委員会により、欧州連合外務・安全保障政策上級代表と共同で公表した「サイバーセキュリティ戦略」中の主要な立法措置として提案され、15年12月8日、欧州議会、理事会との３者協議において合意された。
- 最終的な合意文書は、リーガルチェックを経て議会及び理事会において７月上旬に最終採択予定。
- 指令案の承認後、加盟国は、指令内容を自国の法制度に反映するまで21ヶ月、主要なサービスに適用するまで更に6ヶ月間の期間を与えられる

合意された指令案の概要

（１）各加盟国におけるサイバーセキュリティへの対処能力の向上

- 法制度等を含む国レベルでのセキュリティ戦略の策定の義務付け
- 監督機関及び具体的事案に対処するコンピュータセキュリティ事案対応チーム（CSIRTs）の指定を義務付け

（２）加盟国間の協力強化

- 加盟国間における協力や情報交換を支援するため、協力グループを創設
- 特定の事案やリスクの迅速な対応を図るため、各加盟国のCSIRTで構成されるネットワークを構築

（３）デジタル・サービス提供事業者の義務

- 深刻な事案が発生した場合等の加盟国の監督機関への通知等の義務について、対象となる不可欠サービス事業者（※１）の範囲を拡大し、デジタル・サービス事業者（※２）の義務についても新たに規定された。
  - ※１　①エネルギー, ②運輸, ③銀行, ④金融, ⑤医療, ⑥水道, ⑦デジタルインフラ（IX等）（現制度では、通信事業者のみが対象）
  - ※２　①オンライン市場、②検索サービス、③クラウドサービス
- デジタル・サービス事業者に対し、ネットワークセキュリティリスク管理に関し、以下の要素に考慮し適切な措置を取ることを求める。
  - 考慮要素：システムと施設のセキュリティ、インシデント管理、事業継続マネージメント、監視・監査・監督、国際標準の順守
- ＥＵ域内にデジタルサービスを提供している事業者のうち域内に事業所を設置していない事業者は、セキュリティを担当する代表者を域内に設置することを義務付ける。

※上記情報はリーガルチェック前の条文に基づくもの。（出典：欧州委員会HP、ＥＵ理事会ＨＰ）

⑤ドイツ「デジタル戦略２０２５」

- 2016年3月14日、連邦経済エネルギー省がCebit（ハノーファーで毎年3月に開催される情報通信技術関連メッセ）に会わせて公表。
- **2025年の時点において、ドイツがデジタル化において世界をリードするために実施すべき10のステップを記載。**

1. ドイツのためのギガビット光ファイバー網を2025年までに構築
   - ・ドイツ全土にギガビットネットワークを整備するために100億ユーロ規模のファンドを設立
   - ・インフラ投資を促進するようなアクセス/料金規制を発展
2. スタートアップ企業の支援及び若者並びに既存企業との協働の促進
3. さらなる投資及びイノベーションの創造のための秩序枠組み
   - ・インターネット上に国際的なレベル・プレイングフィールドを発展させるための各種施策
   - ・経済だけではなく、技術的・法制的な欧州デジタル単一市場を形成
   - ・OTT事業者を規制の枠内へ取り込むための措置を実施
   - ・ドイツ国内のICT関連諸法を改正・統一し「デジタル法典」を編纂
4. 我々の社会の中心的インフラ領域における「インテリジェンスネットワーク化」
5. データ安全性の強化及びデータ主権の発展
   - ・EU/USプライバシーシールドの遵守及び他国への模範化
6. 中小企業、手工業者及びサービス業のための新しいビジネスモデル
7. 「Industrie4.0」による産業立国ドイツの近代化
8. デジタル技術をトップレベルにもっていくための研究、発展及びイノベーション
9. すべてのライフフェーズにおけるデジタル教育の実現
10. 近代的専門センターとしてのデジタル庁の創設

⑥フランス「デジタル共和国法案」（１）

● 仏がICT分野で優位に立ち続け、利用者や法人を含むすべてのデジタル関係者を念頭に置き、**仏における新たなICT政策の枠組み**として、「デジタル国家戦略」（2015年6月）に基づき起草された。

● **３部構成**（オープンデータ・ネット利用の公平・ネットアクセスの保障）で、**透明な手続きを確保**。

１ オープンデータにおける「自由」

イノベーションと経済成長をもたらすよう、オープンデータの原則を促進すべく、政府は以下の環境整備を図る。

✓ 公共部門でのオープンデータを促進するべく、**公共部門の文書やデータのオンライン上の公開を義務付け**

✓ 公共部門で公開されたデータや公開済みの**個人情報の再利用を促進する環境を整備**

２ デジタル利用における「平等」

インターネットにおける利用の公平性を図るべく、政府は以下の環境整備を図る。

✓ プラットフォームの透明性を図る観点から、「**インターネットの中立性**」を明確化し事業者はネット上のコンテンツを公平に扱わなければならないこととし、**利用者はコンテンツ間での個人データの持ち運び**を可能とする

✓ オンライン上のプライバシー保護の観点から、**未成年者におけるいわゆる「忘れられる権利」の適用**するとともに、利用者の**死後のオンライン上の個人データの取扱い**を事前の指定を可能とする

３ デジタル社会を通じた「博愛」

社会生活において不可欠となっているICTを誰もが利活用できるようにすべく、政府は以下の環境整備を図る。

✓ **公共サービスにおける電子登録やSMSの利用**の促進

✓ **障害者を含むインターネットへのアクセス**や**生活困窮者におけるインターネット接続**の維持を支援

⑥フランス「デジタル共和国法案」（２）

（参考1） 法案作成の経緯

2014.10～2015.2	「**全国デジタル評議会**」(CNN:ICT分野の政府諮問機関)における議論
2015.6	「**デジタル国家戦略**」の策定
2015.9.26～ 10.18	**インターネット上で法案公開**
2015. 12.9	**法案の議会提出**
2016.1.19～21	下院における審議(第一読会)(148の修正)。1.26に、**下院にて採択**
2016.4.26～ 5.3	上院にて審議・**修正可決**
今後	上院での修正点を踏まえ、両院協議会にかけられる。(2016年夏頃の成立を予定)

（参考2） 法案手続きの特徴

議会提出前に、法案を広くインターネット上に公開し、意見を募集。

修正案は「いいね」型のボード(右図参照)の対象となり、特に支持が多かった修正案の提案者は、ルメールデジタル担当大臣との協議に招待され、政府が直接の回答を約束するという形をとった。**21,330人の参加者から、約8,500の意見の提出があり、５項目の新規追加と90以上の修正**を行った。

このような**幅広い市民参加型の意見募集の実施は、フランスでは初めての試み**となった。

米　国

米国サイバーセキュリティ法２０１５

構成

サイバーセキュリティ法2015（2015年12月18日成立）は、①官民間のサイバー脅威及び防護情報の共有に関する規定（Title I Cybersecurity Information Sharingとして規定）及びその実施に向けて適用される国土安全保障法（Homeland Security act of 2002）の改正に関する規定（Title Ⅱ National Cybersecurity Advancementとして規定）によって構成される。前者を新たに規定することにより、民間とのサイバー脅威・防護策情報共有を促進するもの。

サイバーセキュリティ法2015の内容（主に官民サイバー情報共有に関する部分を記載）

1. 民間主体におけるサイバーセキュリティの向上及びサイバー脅威に関する情報共有の促進

（1）民間主体がサイバーセキュリティを目的として自身のネットワークを監視し、また明示的な許可及び同意を得て顧客または他の第三者ネットワークを監視するための権限及び免責について規定。
（2）民間主体がサイバーセキュリティを目的としてそのネットワークにおいて防御策を執ることを許容。（ただし、攻撃的な対抗措置を執ることや、他のネットワークに対して実質的な害を及ぼすような行動を企業が取ることは許容しないものと見られる。）
（3）民間主体がサイバー脅威及び防御策について他の企業や連邦政府と共有するための明確な権限及び免責について規定。

2. 政府におけるサイバー情報の共有及び利用

（1）連邦政府は、企業のシステム防護を支援するため、民間セクターに対してサイバー情報をより共有するように努める。
（2）本法案の下で連邦政府に共有された情報は、次の各事項を含む明確かつ透明な規則によって管理されなければならない。
①国土安全保障省による体制整備（ポータル等の設置が想定される ）
②連邦政府によるサイバー脅威情報の利用を、サイバーセキュリティ目的に制限
③司法長官及び国土安全保障長官が定めるプライバシー保護措置

3. その他

（1）アメリカ国民から盗んだ金融関連情報により利益を得た海外のサイバー犯罪者を連邦政府が起訴することを可能とする規定。
（2）本法によって生じる権限等を10年後に無効とする規定。（施行日から発効し、2025年9月30日に失効）

サイバーセキュリティ国家行動計画概要

サイバーセキュリティ国家行動計画(Cybersecurity National Action Plan: CNAP)の概要

■2016年2月9日にホワイトハウスが公表。7年以上にわたるオバマ政権の取組の集大成として、短期的取組から長期的な改善に向けた環境整備を図るための計画。
■連邦政府機関から国民全体や重要インフラに至るまでの対策強化、技術開発や国際的な規範作りなど、サイバーセキュリティに関する包括的な計画となっている。
■関連予算として、2017年度予算案に190億ドル(2016年度比:35%増)を計上。

CNAPのポイント(ホワイトハウス公表ファクトシートより)

①国家サイバーセキュリティ強化委員会(Commission on Enhancing National Cybersecurity)の設置
- 次の10年間で官民両方のサイバーセキュリティ強化のための取られ得る取組について、2016年末までに大統領へ勧告を提出

②連邦政府機関のサイバーセキュリティ強化
- 31億ドルの「IT近代化基金」を創設し、連邦政府のITシステム近代化及びサイバーセキュリティ管理方法の更新を実施。
- 新たに連邦CISO (Federal Chief Information Security Officer) を設置
- サイバーセキュリティ専門家の育成と政府機関への採用推進 (奨学金の拡充や学資ローンの免除等)

③国民の強化
- 複数認証の推進 (指紋認証やテキストメッセージによるコード送信を活用) 、中小企業向けにサイバーセキュリティ研修を実施

④重要インフラ防護
- 企業等がシステムについてのセキュリティテストを実施できる「国家サイバーセキュリティ強靭化センター」を創設
- IoT機器のテスト・認証を行う「サイバーセキュリティ・アシュアランス・プログラム」の開発
- 官民研究開発パートナーシップである「国際サイバーセキュリティセンター」を開所

⑤技術開発
- 国家としての戦略的な研究開発目標を定めた「2016年連邦サイバーセキュリティ研究開発計画」を発表

⑥サイバー空間における悪意ある活動の抑止
- 連邦捜査局 (FBI) や米軍サイバーコマンドの体制強化

⑦プライバシー保護
- 「連邦プライバシー評議会」を創設。政府横断的な戦略的・包括的なプライバシーガイドラインを実施。

中　国

中国のサイバーセキュリティ規制強化の動き

1. 銀行システムセキュリティ規制ガイドライン

- 2014年9月及び12月、中国政府（銀行業監督管理委員会、工業・情報化部等）は、銀行が調達するICT関連製品やサービスに関し、中国国内の知的所有権に基づく製品や中国独自の基準に基づく認証を得た製品の使用を要求するガイドラインを策定。
- 当該ガイドラインでは、上記要件を満たす製品・サービスの使用割合を2019年までに75%以上となるよう目標を定め、目標達成のための推進計画を2015年3月15日までに当局に提出するよう要求。
- 各国政府や産業界から懸念を表明する声もあり、同年4月、中国政府はガイドラインの見直しを決定。施行についても延期されている。

2. サイバーセキュリティ法案

- 2015年7月、全人代常務委員会は「サイバーセキュリティ法案」を公表、パブリックコメントを募集。
- 本法案では、ネットワーク製品等に対し中国の国家規格・業界規格への適合を求めるほか、ネットワーク基幹機器及びセキュリティ専用製品については中国の認証をクリアしなければ販売できない旨規定。また、個人情報等の重要データの中国国内保存義務や、当局による違法情報の処理・遮断権限等を規定。

3. 反テロ法

- 2015年12月、テロ対策を強化する「反テロ法」が全人代常務委員会で可決、成立。
- 本法では、通信事業者等に対し、公安機関、国家安全保障機関がテロ活動を防止・調査するために接続・復号等の技術的支援を提供することを義務付け。

4. 国家安全法

- 2015年7月、全人代常務委員会で可決、成立。従来の安保分野に加え、サイバー空間についても国家の主権が及ぶことを前提に、インターネット管理の強化を通じて国家の安全を確保する旨明記。

5. 中国インターネットドメイン名管理弁法改正案

- 2016年3月、工業・情報化部は2004年12月に施行された現行規定を改正する「インターネットドメイン名管理弁法改正案」を発表し、パブリックコメントを募集。
- 中国の登録機関で登録したドメイン名以外は中国国内でインターネットに接続できない旨を規定する等、海外のウェブサイトへのアクセス規制を強化する改正内容となっている。

ASEAN

サイバーセキュリティ関係のASEANとの国際連携

● 日・ＡＳＥＡＮサイバーセキュリティ協力に関する閣僚政策会議（2013年9月東京）
- セキュリティをテーマとする日・ASEANで初の閣僚レベルの会議
- 我が国からの提案に基づき、次のプロジェクトを連携して勧めることで合意

①JASPER（ジャスパー）(Japan-ASEAN Security Partnership)
- i）PRACTICE（プラクティス）：我が国及び連携国に設置したセンサーにて、サイバー攻撃発生の予兆を検知するためのプロジェクト
- ii）DAEDALUS（ダイダロス）：連携国内のPCからのウィルス感染が疑われるトラフィックが観測された場合に、連携国に警告を送付するプロジェクト

②ASEANサイバーセキュリティ人材育成イニシアティブ

● 日・ＡＳＥＡＮ情報セキュリティ政策会議
- 情報セキュリティを担当する局長級の会議。2009年に第１回を開催し、2015年10月14日・15日に第８回をインドネシアで開催。2016年10月20日・21日に第９回を東京で開催予定。
- 閣僚政策会議での議論の具体化を検討。

PRACTICE（プラクティス）連携国

・タイ	2013年2月～
・マレーシア	2013年3月～
・インドネシア	2013年5月～
・フィリピン	2014年1月～
・シンガポール	2014年3月～

DAEDALUS（ダイダロス）連携国

・ミャンマー	2013年10月～
・ラオス	2013年11月～
・インドネシア	2013年11月～
・フィリピン	2013年12月～
・マレーシア	2014年3月～
・タイ	2016年4月～

連携国拡大の働きかけ

ASEANにおけるサイバー脅威の認識共有、情報交換のための基盤として活用

ASEANサイバーセキュリティ人材育成イニシアティブ

①　（独）国際協力機構（JICA）専門家派遣
- 2014年7月から2年半、2名の専門家をインドネシアに派遣
- ニーズに合わせた研修を企画・立案

②　実践的サイバー防御演習（CYDER）の海外展開
- ASEAN域内でのCYDER演習実施の検討

政府職員のサイバー攻撃等への対応能力の強化