AMT/NEWSLETTER
Cyber & AI Security

2026 年 8 月 7 日

G7 におけるデジタル空間・サイバーセキュリティ政策の動向
―ポスト量子暗号移行、サイバーセキュリティ WG 宣言、青少年保護―

弁護士 清水 亘 / 弁護士 石川 雅人

Contents

Ⅰ. はじめに

2026 年 5 月から 6 月にかけて、G7 の首脳会合やデジタル・技術相会合、サイバーセキュリティ・ワーキンググループ会合等がフランスで開催され、G7 からデジタル空間の安全性及びサイバーセキュリティに関する文書が相次いで公表された。具体的には、①「ポスト量子暗号移行の準備に関する G7 サイバーセキュリティ WG 声明」(G7 Cybersecurity Working Group Statement on preparing for a post-quantum cryptography migration)[1]、②G7 サイバーセキュリティ・ワーキンググループ宣言(以下「G7 サイバーセキュリティ WG 宣言」という。)[2]、③「青少年のためのより安全なデジタル空間に関す

1 CCCS(カナダサイバーセキュリティセンター)「G7 Cybersecurity Working Group Statement on preparing for a post-quantum cryptography migration」(CCCS、2026 年 6 月 1 日)https://www.cyber.gc.ca/en/news-events/g7-cybersecurity-working-group-statement-preparing-post-quantum-cryptography-migration

2 ANSSI(フランス国家情報システムセキュリティ庁)「Declaration of the G7 cybersecurity working group - 27 may 2026」(ANSSI、

る首脳による呼びかけ」(Leaders' call on a safer digital space for minors)[3]、の 3 文書である。以下では、各文書の内容を概観する。

II. ポスト量子暗号移行の準備に関する G7 サイバーセキュリティ WG 声明

1. 概要

量子計算機が現在広く使用されている公開鍵暗号を破る(解読する)可能性があることを前提として、米国国立標準技術研究所(NIST)は、量子攻撃に耐性のある新しいアルゴリズムを選定しており、この新しい暗号はポスト量子暗号(Post-Quantum Cryptography。以下「PQC」という。)と呼ばれている。PQC 移行の準備に関する G7 サイバーセキュリティ WG 声明は、中堅・大企業の技術管理層に向けて、PQC 移行準備のための実務的助言を整理したものである。

2. 主な内容

同声明は、PQC への移行準備について、主として次の点を挙げている。

① PQC 移行は組織全体の課題であること

同声明は、PQC への移行を、単なる技術更新ではなく、経営判断、予算措置、調達、社内体制整備及びサプライチェーン対応を含む組織全体の課題として捉えるべきだとしている。そのため、経営層の関与、推進体制の整備、組織内での周知、必要に応じた外部専門家の活用が重要であるとしている。

② 将来の量子計算機による情報漏えいリスク

同声明は、現時点では暗号化されている情報であっても、将来、量子計算機の性能向上により、保存されていたデータが後に解読されるおそれがあることを指摘する。このため、政府情報、機微な個人情報、営業秘密その他長期間保護を要する情報については、特に留意が必要であるとしている。

③ 暗号利用状況の棚卸しの必要性

準備の出発点として、同声明は、自組織のシステムやサービスのどこで暗号が利用されているかを把握することを重視している。対象は、社内システム、ネットワーク機器、認証基盤、クラウドサービス、ソフトウェア、組込み機器等、広範に及ぶ。

④ 優先順位付けの必要性

同声明は、すべての対象を一度に移行することは困難であることを前提に、情報が漏えいした場合の影響、どの程度

2026 年 6 月 8 日)https://cyber.gouv.fr/en/publications/jointly-led-international-publications/declaration-of-the-g7-cybersecurity-working-group/

3 「Leaders' call on a safer digital space for minors」(2026 年 6 月 17 日)https://www.elysee.fr/en/G7evian/2026/06/17/leaders-call-on-a-safer-digital-space-for-minors。外務省による仮訳「青少年のためのより安全なデジタル空間に関する首脳による呼びかけ」https://www.mofa.go.jp/mofaj/files/101046859.pdf

長期間保護する必要があるか、外部からの攻撃にさらされやすいか、移行にどの程度の時間を要するかといった要素を踏まえ、優先順位を付して対応を進めるべきであるとしている。特に、長期間秘匿を要する情報や、更新に長期間を要する仕組みは、優先度が高い例として示されている。

⑤　移行時の検証及び関連文書の更新

同声明は、移行作業自体に加え、事前の計画確認、移行後の動作確認、関連文書の更新も重要であるとする。また、将来の暗号変更にも対応しやすい設計、既存方式との併用、更新が困難な環境への対応、クラウド事業者の移行計画の確認や調達条件の見直しにも言及している。

III. G7 サイバーセキュリティ WG 宣言

1. 概要

G7 サイバーセキュリティ WG 宣言は、サイバー攻撃の脅威の高度化、新興技術、及びそれらが国家安全保障や経済レジリエンスに与える影響を踏まえ、G7 各国のサイバー当局が連携と調整を継続・強化していくことを確認する文書である。

2. 主な内容

G7 サイバーセキュリティ WG 宣言は、G7 サイバーセキュリティ WG を、重要インフラ及びデジタル・サプライチェーンの保護、情報共有、基準やベストプラクティスに関する対話、AI や量子計算のような新興技術を踏まえたレジリエンス強化を進めるための場として位置付けている。

また、同宣言は、2025 年の G7 の議長国のカナダの下で策定された 2 つの文書、すなわち透明性・セキュリティ・信頼を促進するための AI システムに関する最小要素を示した「AI のためのソフトウェア部品表に関する最小要素」（Minimum Elements on a SBOM for AI）[4]及び上記 1 の「ポスト量子暗号移行の準備に関する G7 サイバーセキュリティ WG 声明」を高く評価したうえで、2026 年の議長国であるフランスの下において G7 サイバーセキュリティ WG が取り組むべき優先事項として以下 4 つの取組を挙げている。

①　PQC への移行

計算能力の向上に伴う量子の脅威や遡及的な攻撃（retroactive attacks）のリスクを踏まえ、官民の組織にとって、PQC への移行はもはや先送りできない喫緊の課題であるとしている。

②　高度 AI がもたらすサイバーセキュリティリスクに対する共通理解

生成 AI や大規模言語モデルは現代のデジタル・イノベーションの要であり、組織に柔軟性と効率性をもたらす一方、攻撃者によって武器化され得ること、また AI システム自体も、モデル汚染（model poisoning）、ソフトウェア・サプライチェーン侵害、機微データ流出等の標的になることを指摘する。さらに、AI の支援による脆弱性の発見やコード生成の進展により、ソフトウェア・セキュリティと効率的なパッチ運用の重要性が高まるとしている。

③　通信分野のサイバーセキュリティの強化

4 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/SBOM-for-AI_minimum-elements.pdf?__blob=publicationFile&v=4

通信分野のサイバーセキュリティはきわめて重要な世界的な課題であり、ネットワークの複雑性と相互依存性の増大により、システミック・リスクが生じているとしている。

④　中小企業のサイバーセキュリティの強化

中小企業は世界経済の基盤であることから、これを標的とするサイバー攻撃もシステミック・リスクとなり得ると指摘する。そのうえで、技術ベンダーに対し、中小企業が利用する製品を設計段階から安全性を組み込んだもの（secure by design）として提供することを求めている。

Ⅳ. 青少年のためのより安全なデジタル空間に関する首脳による呼びかけ

1. 概要

2026 年 6 月 17 日に公表された、青少年のためのより安全なデジタル空間に関する首脳による呼びかけは、18 歳未満の子供・若者を含む青少年のオンライン体験は、安全であり、豊かなものであり、発達を重視したものであるべきであることを確認するものである。

2. 主な内容

①　サービス設計に関する要請

青少年に対してデジタルサービスを提供する者は、安全性を設計段階から組み込む考え方（safe-by-design）、安全性（secure）、プライバシー保護（privacy-preserving）、年齢に応じた適切性（age-appropriate）を備えた設計や、保護的なデフォルト設定（protective and by default settings）を採用すべきであるとされている。

②　保護者による関与の支援

保護者が青少年のオンライン体験を導くことができるよう、保護者によるペアレンタルコントロールツールの利用が支援されるべきであるとされている。

③　年齢確認・年齢推定への対応

年齢確認・年齢推定を含む年齢保証（age assurance）については、各国法制や適用法令に従いつつ、利用者のプライバシーを保護しながら有効に機能する仕組みの開発・導入が求められている。

④　レコメンデーションシステム及び対話型 AI への対応

レコメンデーションシステム（recommendation systems）については、年齢に適したコンテンツを優先し、リスクへの露出を減らすよう設計されるべきであるとする。また、対話型 AI ツール（conversational artificial intelligence tools）についても、教育等への有用性が認められる一方で、児童と若者の福祉と安全に対するリスクがあるとして、デフォルトの安全設定、保護者向け利用管理機能、年齢確認手段の整備が重要であるとされている。

⑤　コンテンツの透明性と違法・有害情報への対応

真正なコンテンツと合成コンテンツを見分けやすくし、コンテンツの出所（content provenance）を識別できるように支援すること、デジタル・リテラシーを向上させることにも言及がある。

また、児童に対する性的虐待の資料、本人の同意のない親密画像、ディープフェイク、オンライン・グルーミング、性的搾取及び性的恐喝については、生成・操作・流通の禁止と、効果的な検知・削除措置の必要性が明記されている。

⑥　研究及びエビデンスに基づく政策形成

研究者、教育制度、デジタルサービス提供者等が関与する研究や、データ共有、評価手法の共通化を通じたエビデンスに基づく政策形成にも触れられている。

Ⅴ. おわりに

以上の 3 文書は、未成年者保護、G7 サイバー当局間の連携、PQC 移行準備という異なるテーマを扱うものであるが、いずれも、デジタルサービス、AI、通信及び暗号基盤をめぐる論点について、G7 がどのような事項を重視しているかを示している。今後の各国の政策や国際的な議論の方向性を把握するうえでも、これらの文書は重要な参照資料となるものと考える。

以上

■ 本ニュースレターの内容は、一般的な情報提供であり、具体的な法的アドバイスではありません。お問い合わせ等ございましたら、下記弁護士までご遠慮なくご連絡下さいますよう、お願いいたします。

■ 本ニュースレターの執筆者は、以下のとおりです。

弁護士 清水 亘 wataru.shimizu[at]amt-law.com
弁護士 石川 雅人 masato.ishikawa[at]amt-law.com
※メールを送信する際には、[at]を@に変更してお送りください。

■ ニュースレターの配信停止をご希望の場合には、お手数ですが、お問い合わせにてお手続き下さいますようお願いいたします。