日米豪印サイバーセキュリティ・パートナーシップ：共同原則

1. 日米豪印上級サイバーグループは、自由で、開かれ、かつ強靭なインド太平洋に関する日米豪印首脳のビジョンを実現するため、パートナー間のサイバーセキュリティ協力の指針となり、インド太平洋地域におけるサイバーセキュリティの向上を支援することを目的とする、日米豪印サイバーセキュリティ・パートナーシップに基づく以下の原則を確認する。日米豪印各国は、デジタル化が一層進展し高度なサイバー脅威が存在する世界において、サイバーセキュリティを向上させる必要性を認識する。我々は、パートナーとして、重要インフラのサイバーセキュリティ、サプライチェーンリスクのマネジメント、ソフトウェアセキュリティ及び人材育成発展を強化するために、協力することを追求する。

2. 我々の市民が日々の基幹的なサービスのために依存している重要インフラは、サイバー脅威からのリスクに一層晒されている。相互に関連し相互依存している重要インフラの性質は、適切なサイバーセキュリティに関する保全措置がなければ、そのリスクを増大させ、意図的又は不注意に、国内及び国境を越えた形で混乱とその後の経済及び安全保障上の懸念を引き起こす可能性がある。例えば、エネルギー部門における長期にわたる広範な機能不全は、我々の経済、安全保障及び主権、並びに我々の生活様式に壊滅的な影響を及ぼす可能性がある。

3. 日米豪印各国は、重要インフラの継続的な防護において産業界及び政府が果たす重要な役割を認識し、サイバーセキュリティ及び重要インフラ防護政策の策定及び実施のため、関連する産業界及び非政府の利害関係者と共に協力する。日米豪印各国は、政策策定へのアプローチを共有してセキュリティを強化することにコミットし、また、政府間及び産業界のパートナーとの間で脅威情報を迅速かつ時宜を得た形で共有し、強靭なエコシステムを構築することにコミットする。我々は、重要インフラ提供事業者が依存する技術製品及びサービスのセキュリティを改善するために協働する。

4. 我々は、重要インフラ部門の資産、システム及びネットワークが極めて重要であり、その無能力化又は破壊は、国家安全保障、経済、公衆の健康及び安全を弱体化させる影響を及ぼすであろうことを理解する。安全で強靭な情報技術(IT)及び運用技術(OT)、並びにデジタル対応製品及びサービスのサプライチェーンは、我々の企業及び消費者がネットワーク及びシステムを保護するために必要な製品を入手することを確保するのに役立つ。透明性、情報共有、多様性、開放性、予見可能性及び持続可能性は、信頼されかつ強靭なサプライチェーンにとって不可欠な要素である。政府及び産業界は、日米豪印重要・新興技術作業部会における我々の作業と整合することを確保

しつつ、潜在的なリスクを特定し、サイバーセキュリティに関連するサプライチェーンリスクの依存関係を評価するための枠組みを開発するために協働することができる。我々は、ベスト・プラクティスの共有を確保するため、政府及び産業界による協議プロセス並びにその後の適切な管理及び保証メカニズムの定期的レビューを通じて、標準、ベースライン、ガイドライン及び手続に関する意見交換を継続する。

5. 日米豪印パートナーは、ベースラインのソフトウェアセキュリティ標準の国内及び国際的な実施を調整し、確保できる特異な立場にある。各政府の集積された購買力は、サイバーセキュリティの改善を推進し、基本的な設計上の考慮事項としてセキュリティを確保することができる。ベースラインのソフトウェア標準の実施を調整することは、国民、重要インフラ及び基幹的サービスのサイバーセキュリティに重大な影響を与える。

6. 我々は、政府調達のみならず、より広範なソフトウェア開発エコシステムの中で、マネージド・サービスプロバイダー及び技術製品・サービスの全体にわたって、ベースラインの標準を継続して整合していく。各パートナーの現在の活動及び産業状況に応じて、これらの標準には、脆弱性管理の改善及び最新のパッチの適用、ソフトウェア部品表の提供、多要素認証の使用、定期的なデータのバックアップ、データの暗号化及びセキュリティ管理システムの厳格な監査、並びに監査人の技能及び能力の検証のためのメカニズムが含まれ得る。

7. 日米豪印各国は、上記の標準を実施するための国内の努力に積極的に関与し、政府のソフトウェア調達のためのソフトウェアセキュリティに係る枠組みの開発を共に整合していくことにコミットする。我々は、このアプローチが、政府のサイバーセキュリティを強化するとともに、ソフトウェアセキュリティに関する市場の変化を促進すると信じている。国内産業の利害関係者との協力もまた、この取組にとって不可欠な要素である。なぜなら、民間部門が、最終的にこれらの要件を実施し、また、日米豪印政府と協力しながら深刻さを増す脅威環境にそれらの要件を継続的に適応させるべく取り組むことになるからである。我々は、政府が調達するソフトウェアに対して最低限のソフトウェアセキュリティ標準を実施するために、産業界とのオープンで協力的な関係を追求する。これらの協力は、いかにソフトウェア開発エコシステム全体にわたってこれらの最低限の基準を導入できるかについて、政府調達チャネル外のより広範な対話に繋がることが可能であるし、そうあるべきである。

8. 我々は、悪意のあるサイバーアクターに起因するかつてなく複雑かつ破壊的な脅威及びそれらが国家安全保障にもたらすリスクに対する深刻な懸念を共有し、日米豪印各

国及びインド太平洋地域におけるパートナーの能力構築を強化するためのそれぞれの取組の調整を加速させるとのコミットメントを確認する。日米豪印各国は、クアッド・サイバーセキュリティ・パートナーシップを通じて、インド太平洋地域における能力構築プログラムに協力し、その取組を更に強化する。

9. 我々は、サイバー攻撃が増加し、より複雑になっているという共通の認識に基づき、我々のサイバーセキュリティの人材を増やすための共同の取組を強化することの重要性を再確認するとともに、十分な専門知識を生み出すという課題も共有する。日米豪印各国は、能力構築に加え、我々の共同のサイバーセキュリティ人材及び有能なサイバー専門家の予備要員を強化するために協働する。

10. これらの原則は、共通の課題に対処するための日米豪印上級サイバーグループの協力を後押しし、急速に変化する脅威環境において我々がサイバーの強靭性を改善する機会を捉えることを可能にする。我々は、共通の目的と野心的、実用的及び行動指向の目標の下、ここに団結した。