

ソフトウェア・セキュリティに関する日米豪印共同原則
(概要)

- ◆ 日米豪印上級サイバーグループは、政府のためのソフトウェアの開発、調達及び利用の指針となる最低限のサイバーセキュリティ・ガイドラインを構築することにより、ソフトウェア・セキュリティを共同で向上するとの我々のコミットメントを再確認する。
- ◆ 日米豪印は、以下のハイレベルの安全なソフトウェア開発慣行を追求し、既存の政府の政策にそれらを採用し、これらの慣行を満たすソフトウェアを取得し、ソフトウェア開発者/サプライヤにそれらの実施を奨励するとの意図を有する。
 - 組織の準備：人々が適切に訓練され、プロセスが定義され、安全なソフトウェア開発を実行するためのテクノロジー・ソリューションが導入されていることを確保する。
 - ソフトウェア及びソフトウェア開発環境の保護：ソフトウェアの全てのコンポーネントを改ざん及び不正アクセスから保護するための適切な管理を確保し、各ソフトウェアリリースをアーカイブ化し保護し、各リリースで使用される様々なコンポーネントの詳細（例：ソフトウェア部品表（SBOM））及びサプライチェーン関係の十分な記録を維持する。
 - 十分に安全が確保されたソフトウェアの作成：リリース時のセキュリティの脆弱性が最小限の、十分にセキュリティで保護され、テスト済みのソフトウェアを作成する。
 - 脆弱性への対応：継続的にそれらの脆弱性に対処し将来の同様の脆弱性の発生を防止するために、ソフトウェアリリースの脆弱性を特定し適切に対応する。
- ◆ 日米豪印各国は、ソフトウェア又はソフトウェアを含む製品の政府調達に関して、以下の最低限のガイドラインを追求する意図を有する。各国は、国際的義務、国内法、規制、及びそれぞれのサイバー空間の成熟度と整合的に、以下の慣行を奨励することにより、国内でガイドラインの実施を追求する意図を有する。
 - ソフトウェアの開発が安全なソフトウェア開発慣行に従っていることを示す第三者認証が提供されない限り、ソフトウェア開発者による自己申告を要求する。
 - ソフトウェア開発者に対し、報告と開示のプロセスを含む各国の脆弱性開示プログラムに報告するよう奨励する。
- ◆ 日米豪印は、政府によるソフトウェアの利用のために以下のセキュリティ対策を追求する意図を有する。
 - ソフトウェア及びソフトウェア・プラットフォームを不正なアクセス及び利用から保護するための十分な管理及びプロセスを確保する。
 - ソフトウェア及びソフトウェア・プラットフォームで使用されるデータの機密性、完全性、可用性を保護するための十分な管理及びプロセスを確保する。
 - ソフトウェアを不正利用から保護するため、ソフトウェア・プラットフォームと、それらのプラットフォームに展開されたソフトウェアを特定して維持する。
 - ソフトウェア及びソフトウェア・プラットフォームに関連するインシデントを迅速に検出、対応し、回復する。
 - ソフトウェア及びソフトウェア・プラットフォームのセキュリティを促進する人間の行動の理解及び遂行を強化する。