報道資料

令和８年３月５日
国家サイバー統括室

国際文書「AI・機械学習のサプライチェーンリスクと緩和策」への共同署名について

令和８年３月５日、国家サイバー統括室は、豪州通信情報局（ASD）豪州サイバーセキュリティセンター（ACSC）が策定した「AI・機械学習のサプライチェーンリスクと緩和策（以下「本件文書」という。）」の共同署名に加わり、本件文書を公表しました。

本件文書は、AI・機械学習システム及びコンポーネントを導入または開発する組織及び担当者を対象に、AI・機械学習に関するサプライチェーンセキュリティの重要性を強調し、開発や調達の際に考慮すべき主要なリスクや緩和策を提供することを目的としています。

本件文書の普及啓発は、我が国のサイバーセキュリティ環境の向上にも資することから、共同署名に加わることとしました。

本件文書に共同署名した国は、豪州、日本のほか、カナダ、ニュージーランド、韓国、シンガポール、英国及び米国の計８か国です。

１．本件文書の概要

(1) 背景・目的

本件文書は、AI・機械学習のサプライチェーン（データ、モデル、ソフトウェア、インフラ、第三者サービス等）が複雑かつ独自のリスクをもたらすことを踏まえ、AI・機械学習システム及びコンポーネントを導入または開発する組織及び担当者を対象に、AI・機械学習に関するサプライチェーンセキュリティの重要性を強調し、開発や調達の際に考慮すべき主要なリスクや緩和策を提供することを目的としています。

(2) AI・機械学習におけるサプライチェーンリスク管理の概念

組織は、より広範なサイバーセキュリティリスク管理戦略の一環として自身の AI・機械学習サプライチェーンを評価するにあたり、製品・サービスのライフサイクル全体を検討する必要があります。以下に列挙されている事項は、各組織が実施するリスク評価に基づき、どれを優先して実施するかを各組織が判断することとされています。

- AI・機械学習に関する考慮事項は、包括的なサプライチェーン評価の一環として評価される必要がある。
- 効果的なリスク管理には、AI・機械学習システムとそのサプライチェーンの全体像を把握することが必要である（関係事業者の特定、AIBOM/SBOM の活用等）。
- AI・機械学習システムがもたらす新たなリスク等を考慮するため、リスク管理の見直しを行う必要がある（脆弱性マッピングの実施、インシデント対応計画の整備等）。
- AI・機械学習の関係事業者と協働する際には、サイバーセキュリティ上の考慮事項について早期に議論し、責任の所在を明確に理解することが重要である（ベンダに対するデュー・デリジェンスの実施、関係事業者に対する脆弱性・インシデント報

告の要求等)。
- AI・機械学習システムが組織のデータセキュリティにどのような影響を及ぼすか理解することが必要である（組織のデータに対する AI ベンダ含むアクセス権の確認等)。
- サプライチェーン管理及びスタッフトレーニングのための内部管理の強化が必要となる可能性がある。

(3) AI・機械学習サプライチェーンにおける主なリスクと緩和策

AI・機械学習のサプライチェーンは複雑であり、データ、モデル、ソフトウェア、ハードウェア、第三者サービス等の各コンポーネントにおいて、以下のように、悪意のあるアクターが利用し得る脆弱性やリスクが存在する可能性があります。

・AI データ
リスク：低品質または偏りのある学習データ、悪意ある学習データの改ざん、学習データの漏洩　等
緩和策：標準化された手法に基づくデータの収集・生成、外部データに対する検疫、偏り等を防止するデータの下処理、データの完全性の確認　等

・機械学習モデル
リスク：モデルパッケージへの悪意あるコードの混入、モデルに対する悪意ある変更、モデルへのマルウェアの埋め込み、モデルの入力制限の回避　等
緩和策：透明性のあるモデルを信頼できる提供元からの入手、性能検証の実施、マルウェア等を検出可能なセキュリティツールの利用　等

・AI ソフトウェア
リスク：AI システムは、多くのライブラリ及びツールに依存し複雑性を増しており、全てのコンポーネントの安全性を保証することが困難　等
緩和策：ソフトウェアの完全性検証、ソフトウェアコンポーネントの監査や SBOM の整備等により、既知の脆弱性が軽減されていることを確認　等

・AI インフラ・ハードウェア
リスク：AI 固有のアクセラレータデバイスの導入等に伴い、ドライバ、ファームウェア、関連コンポーネントを通じた攻撃面が拡大　等
緩和策：既存のセキュリティ慣行等に基づき、ハードウェアが悪意のある中身を含まず、ネットワーク内で適切に区分されていることを確認　等

・第三者サービス
リスク：AI・機械学習ツール、プラットフォーム、サービス等を提供する第三者事業者が、組織のサプライチェーンに脆弱性をもたらす可能性　等
緩和策：第三者事業者に対する徹底的な評価と継続的なモニタリング（セキュリティ慣行、脆弱性管理プロセス等）　等

２．関連リンク

【原文リンク】

【本報道発表に関する問い合わせ先】

国家サイバー統括室
国際ユニット国際戦略班
Tel：03-6277-7071