報道資料

令和５年 10 月 17 日
内閣官房内閣サイバーセキュリティセンター（NISC）

セキュアバイデザイン・セキュアバイデフォルト原則について

１．概要

本日、内閣サイバーセキュリティセンター（NISC）は、米国サイバーセキュリティ・インフラ安全庁（CISA）等が策定した「セキュアバイデザイン・セキュアバイデフォルト原則に関する文書の改訂版（以下「本件文書」という。）の署名に加わり、本件文書を公表しました。

本件文書は、改訂に当たり、数百の個人、企業、非営利団体から受けたフィードバックを受け、特にソフトウェア作成業者に対する３つの原則、**①顧客のセキュリティの結果に責任を持つ**、**②徹底した透明性と説明責任を負う**、**③トップ主導での実施**、を具体的に説明し、ソフトウェア作成業者がこれらの原則を顧客や一般の人々に対し、どのように示すことができるかに焦点を当てて提言を行っています。

本件文書は我が国のサイバーセキュリティ戦略に盛り込まれている「セキュリティ・バイ・デザイン」の概念を具体化するものであり、サイバー空間上の脅威が高まる中で、国際的動向とも歩調を合わせることにより、我が国のサイバーセキュリティの強化に資するものであることから、サイバーセキュリティ戦略本部の意見に基づき、NISC として共同署名に加わりました。なお、本件文書の末尾の資料欄には、我が国のサイバーセキュリティ戦略も記載されています。

今後は、技術の進歩が早い分野であることも踏まえ、本件文書の具体化に当たり、産業界とも継続的に対話を重ねつつ、引き続き、サイバーセキュリティ分野での国際連携の強化に努めてまいります。

２．本件文書の内容

（１）定義

- セキュアバイデザイン：IT 製品（特にソフトウェア）が、設計段階から安全性を確保されていること。前提となるサイバー脅威の特定、リスク評価が不可欠。
- セキュアバイデフォルト：ユーザー（顧客）が、追加コストや手間をかけることなく、購入後すぐに IT 製品（特にソフトウェア）を安全に利用できること。

（２）ソフトウェア作成業者などテクノロジー企業への提言

- セキュアバイデザイン手法の導入：①メモリに安全なプログラミング言語の採用、②アプリケーションセキュリティのテスト実施、③コードレビューやソフトウェア部品表（SBOM）の採用、④脆弱性の報告を奨励する開示プログラムの導入、⑤侵害をシス

テム全体に広げないための多層防御の導入など。

- セキュアバイデフォルト手法の導入：①デフォルトパスワードを排除する、②多要素認証を導入する、③高品質の監査ログの追加料金なしでの提供、④シングルサインオン（SSO）を実装する、⑤古いシステムとの互換性よりもセキュリティを優先、⑥「セキュリティ強化ガイド」の簡素化など。
- ①顧客のセキュリティの結果の責任を持つ、②徹底した透明性と説明責任を負う、③トップ主導での実施、という３つの基本原則を遵守する。

（３）ユーザ組織（顧客）への提言

- セキュリティ結果の責任をソフトウェア作成業者に問うよう推奨する。
- セキュリティバイデザインやセキュリティバイデフォルトの製品の購入を優先する。
- ソフトウェア作成業者と戦略的な連携関係を構築。ソフトウェア作成業者への要望を調整し、セキュリティを優先させる。
- クラウド利用の場合、責任分担を明確し透明性の高い企業を優先する。

【本報道発表に関する問い合わせ先】
内閣官房内閣サイバーセキュリティセンター
基本戦略総括グループ
国際戦略グループ