報道資料

令和７年８月２６日
国家サイバー統括室

国際文書「暗号鍵及びシークレットの管理-実践者向けガイダンス」への共同署名について

令和７年８月２６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「文書暗号鍵及びシークレットの管理-実践者向けガイダンス（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。（日本語仮訳は追って公表予定です。）

本件文書は、暗号鍵及びシークレットを利用・管理等する組織において、セキュリティを担当する上級管理職が、脅威環境を把握し、鍵及びシークレットの管理を実施する必要性を理解するための指針を提供するものです。

本件文書の目的である、暗号鍵及びシークレットの適切な管理は、セキュア・バイ・デザインの基礎的要素の１つであり、その普及啓発は、サイバーセキュリティを確保する上で重要な要素であることから、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、日本の他、英国、カナダ、ニュージーランドの計５か国です。

１．本件文書の概要

(1) 背景・目的

本文書は、暗号鍵及びシークレットを利用・管理等する組織において、セキュリティを担当する上級管理職が、脅威環境を把握し、鍵及びシークレットの管理を実施する必要性を理解するためのガイダンスを提供する。

(2) ８点の留意事項

① ガバナンス：鍵及びシークレット管理を目的としたポリシーを作成し、標準や規制への準拠を確保する。

② 生成：鍵やシークレットを生成する際は、適切な暗号アルゴリズムを使用すべき。また、量子演算能力の向上による既存アルゴリズムの危殆化を踏まえ、鍵管理計画において耐量子アルゴリズム等への移行を考慮すべき。

③ 登録、保存、アクセス：鍵及びシークレットは、許可されたユーザまたはシステムのみがアクセスを許可される、安全な方法で登録及び保存されることが必要。そのために、定期的なアクセス監査及び検証を実施すべき。

④ 鍵の配布：鍵をやりとりする方法を可能な限り安全なものとし、データの完全性を維持することが必要。また、侵害等の兆候が検出された場合は鍵の置き換えが必要。

⑤ 鍵の置き換えと破棄：アルゴリズムの危殆化やデジタル証明書の有効期限切れ、攻撃者による侵害の確認等が発生した場合は鍵の置き換え

が必要。また、破棄する際はあらゆる痕跡を永久に削除する必要がある。

⑥　信頼の連鎖：利用者が、デジタル証明書の有効性を検証することができ、情報を使用する主体と利用者間の信頼を確立することが必要。

⑦　信頼される立場：システム管理者、特権ユーザ、高価値の鍵やシークレットへのアクセス権を持つ者等は、鍵や秘密情報を安全に保つために、実行しなければならない多くの追加の責任を負っている。

⑧　監督：組織は鍵及びシークレットの監査及び監視要件を作成し、侵害を検出、防止する必要がある。

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