資料４

SA環境への二要素認証の導入について

目次

１．DX推進を踏まえた現状

２．情報セキュリティ対策の方針

３．技術的セキュリティ対策

Ⅰ．DX推進を踏まえた現状

外部環境・内部環境ともに急激に変化しており、利便性の向上と安全性の確保の両立が求められている

	利便性の向上	安全性の確保
外部環境	✓ DX進展（手続電子化、キャッシュレス化等）	✓ 攻撃者の手法の巧妙化 ✓ 情報セキュリティの在り方の変化 ✓ セキュリティ事故の増加
内部環境	✓ ペーパレス、手続電子化、テレワーク等の増加	✓ 職員の情報リテラシーが追いついていない ✓ 電子的に個人情報等を取扱う機会が急増

2．情報セキュリティ対策の方針

情報セキュリティ対策の分類毎の方針については以下のとおり。
当資料では技術的セキュリティにフォーカス。

情報セキュリティ対策の分類	方針
物理的セキュリティ	■ クラウド・バイ・デフォルトの原則によるクラウド化で、サーバや管理区域の管理について、セキュリティを強化 ■ 引続き、通信回線・端末・電磁的記録媒体の適正な管理を実施
人的セキュリティ	■ 職員の情報セキュリティリテラシーの向上 ✓ 情報セキュリティ研修の全員受講 ✓ セキュリティ基礎としての研修コンテンツの追加配布
技術的セキュリティ	■ 上記では補えない対策を検討 ✓ 通信やファイルの暗号化 ✓ なりすましができない仕組の導入により、権限のない者による不正な情報持ち出しを防ぐ。

3．技術的セキュリティ対策

導入する仕組の方向性

＜対策対象・範囲＞

■ SAネットワークを対象とする
  ✓ 手続電子化の推進や文書管理システム更新により、SAネットワークで個人情報を管理する必要があることへ対処する。

＜セキュリティ対策を導入する際の留意点＞

■ 現状の利便性を著しく損なわない方法を採用する
  （テレワークの実施を阻害しないことも含む）
■ 向こう数年間で陳腐化しない方法を採用する
■ 導入や運用に過剰な負荷が掛からない製品を採用する

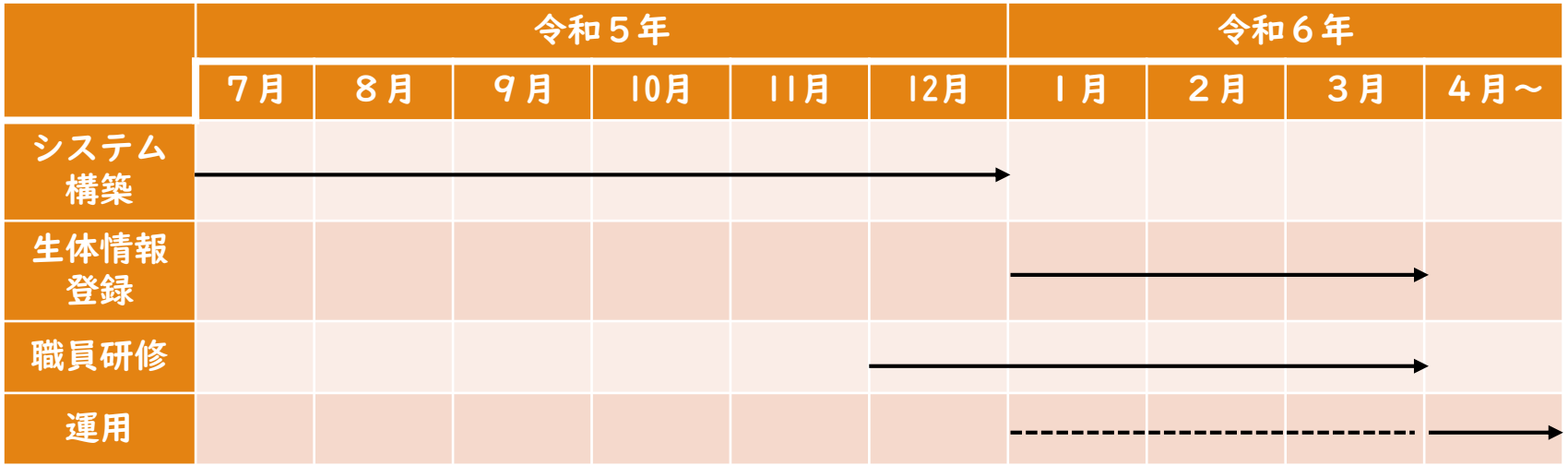
3．技術的セキュリティ対策

導入する仕組

二要素認証

概要	■ 従来のID/PWの認証に加えて、生体情報(例：顔、指紋)の認証を導入
効果	■ 確実に本人であることの担保 ■ なりすましの防止

スケジュール



製品導入によって100%安全になることはなく、物理的セキュリティ対策・人的セキュリティ対策と併せて実施していくことで、効果は最大化する。

End of the documents.