eviDaemon for PAdESにおける
タイムスタンプ暗号方式の移行について

2026年7月17日

セイコーソリューションズ株式会社

概要

2030年末に迎える暗号アルゴリズムの移行に際し、
弊社のSEIKOタイムスタンプも新たな暗号アルゴリズムでのサービス提供を計画しております。

eviDaemonサービスでは、eviDaemonのバージョンアップを行っていただく事により、
新たな暗号アルゴリズムのタイムスタンプをご利用いただく事が可能となります。
eviDaemonのバージョンアップをご計画いただき、
セキュアなタイムスタンプサービスのご利用をご継続くださいますようご案内いたします。

尚、本資料はタイムスタンプの暗号アルゴリズム移行に関するご案内となります。
電子署名（文書署名）についても同様の対応が必要となりますが、
認証局の移行状況にも依りますため、ご利用形態により別途のご案内となります。

背景

CRYPTRECから公開されている
『暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準』
（2022年3月　デジタル庁・総務省・経済産業省）等で示される移行方針では、2031年以降、
112ビット相当アルゴリズムによる新規のタイムスタンプ発行（新規生成）は原則想定されません。
https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022r1.pdf

この方針を踏まえ、当社タイムスタンプも112ビット→128ビット相当アルゴリズムへの移行を計画しています。
2031年以降、当社は112ビット相当アルゴリズムによる新規タイムスタンプ発行を原則として提供いたしません。
※既に付与済のタイムスタンプの検証は別途定める期間・手順により継続可能です。

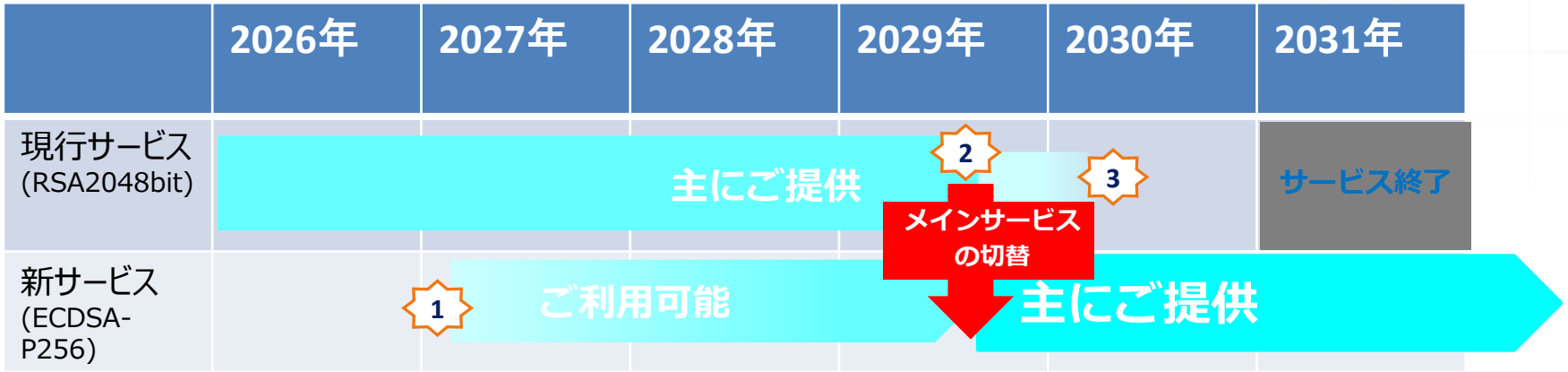
表 8　署名及びメッセージ認証におけるセキュリティ強度要件

想定運用終了・廃棄年／利用期間		2022～2030	2031～2040	2041～2050	2051～2060	2061～2070
112 ビット セキュリティ	新規生成（生成）	移行完遂期間	利用不可	利用不可	利用不可	利用不可
	処理（検証）		検証許容			
128 ビット セキュリティ	新規生成（生成）	利用可	利用可	移行完遂期間	利用不可	利用不可
	処理（検証）				検証許容	
192 ビット セキュリティ	新規生成（生成）	利用可	利用可	利用可	利用可	利用可
	処理（検証）					
256 ビット セキュリティ	新規生成（生成）	利用可	利用可	利用可	利用可	利用可
	処理（検証）					

SEIKOタイムスタンプの暗号切替

2026年現在、弊社のSEIKOタイムスタンプは、112ビット相当の暗号アルゴリズムである
RSA2048bitを採用しています。
2030年末までにセキュリティ強度を128ビット相当に引き上げる必要があり、
楕円曲線暗号（ECDSA-P256）を用いたタイムスタンプへの切替を計画しております。
2030年内の完全移行に向け、段階的に新サービスをご提供してまいります。

SEIKOタイムスタンプ　暗号切替計画



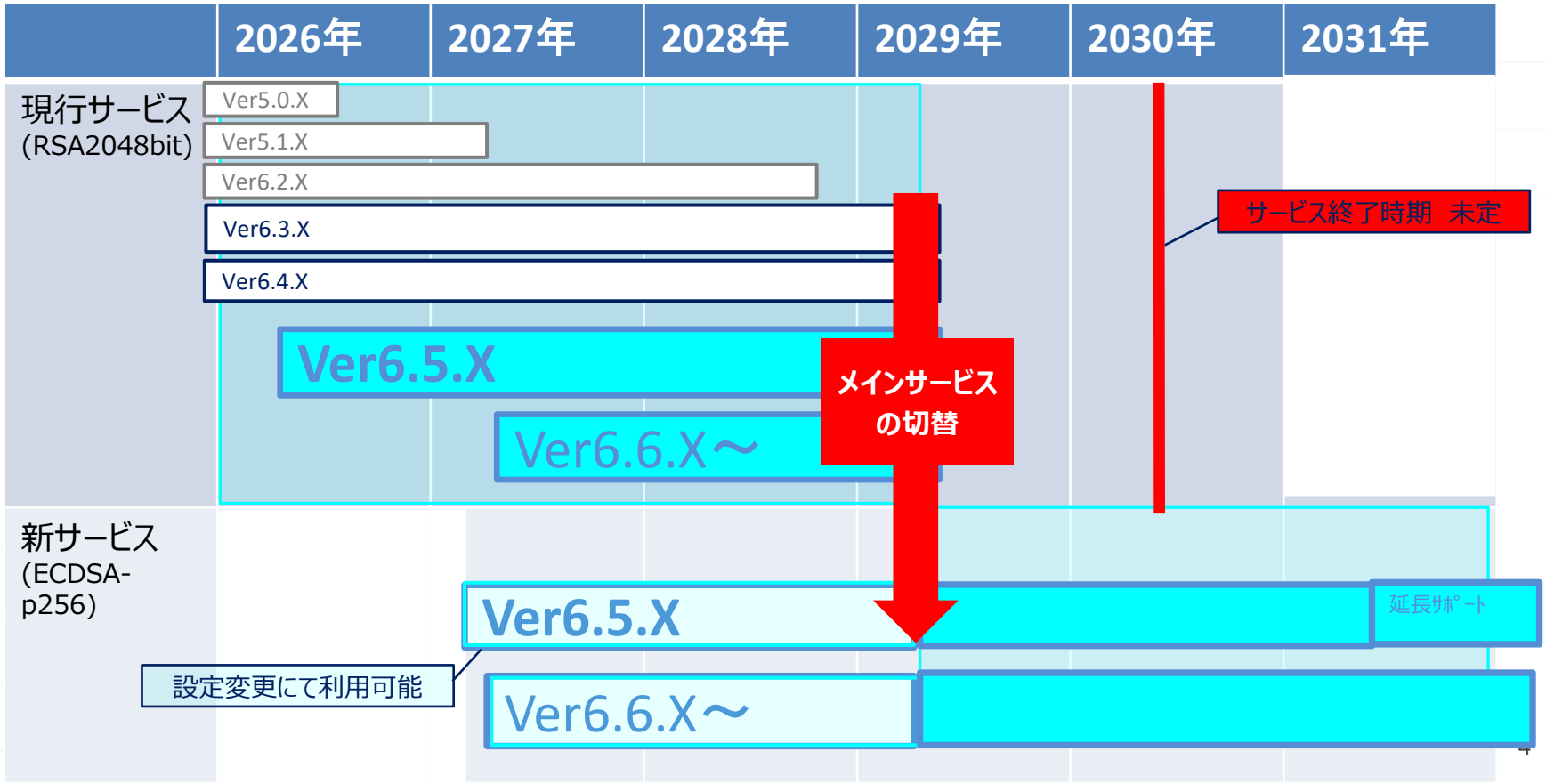
1) 2027年上期より128ビット相当暗号方式(ECDSA-P256)の新サービスをご提供開始予定
　明示的に設定いただければご使用いただく事が可能
2) **2029年度、メインサービスを128ビット相当暗号方式(ECDSA-P256)に切替**予定
(2030年末までの移行完了に向けた措置)
3) **メインサービス切替から一定期間後、112ビット相当暗号方式のサービスは**
サービス提供を終了予定

※本スケジュールは現時点での計画であり、関係機関の指針・認定要件・サービス運用上の判断により変更となる場合があります。確定情報は別途ご案内します。

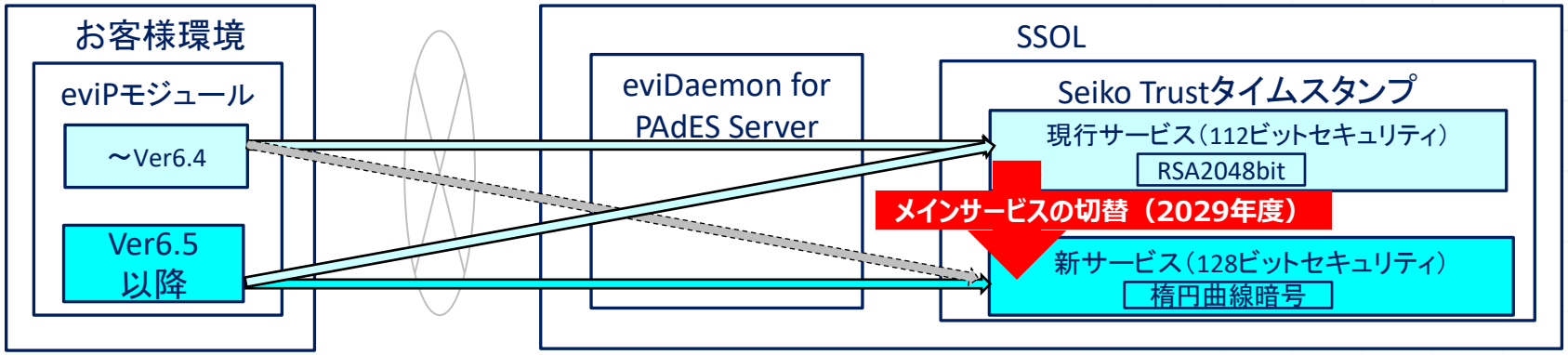
eviDaemon for PAdESの対応計画

SEIKO タイムスタンプの暗号移行計画にあわせ、eviDaemon for PAdESサービスも計画的にバージョンアップリリースをご提供し、
SEIKO タイムスタンプの新サービスをご利用いただけるよう計画しております。

eviDaemon for PAdESバージョンアップ計画



eviDaemon for PAdES　バージョンアップのお願い



2026年リリースの eviDaemon for PAdES Ver6.5以降は、
楕円曲線暗号（ECDSA-P256）のタイムスタンプ付与に対応済となります。

2029年度に予定している「メインサービスの切替」の時点で
Ver6.5以降をご利用の場合、当社側切替に追随可能です。
（ただし、接続先／ポリシーOIDを明示的に設定している場合は設定変更等が必要です。）

Ver6.4以前をご利用のお客様は、メインサービス切替後にタイムスタンプが取得できなくなります。 **Ver6.5以降のバージョンへのバージョンアップをご計画ください。**

よくあるご質問

よくあるご質問ご質問について

Q1. タイムスタンプサービスのメインサービス切替前に付与済のタイムスタンプは、
　　無効になりますか？
A1.いいえ、既に付与済のタイムスタンプについては、その有効期限までは有効です。
　　付与済のタイムスタンプの検証についても、Ver6.5以降で継続して検証可能です。

SEIKO

セイコーソリューションズ株式会社