

eviDaemon for XAdES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

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お願いいたします。

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。
電子署名については対象外となります。今後認証局から別途案内がある場合は、その案内に従いご対応ください。

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)					

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

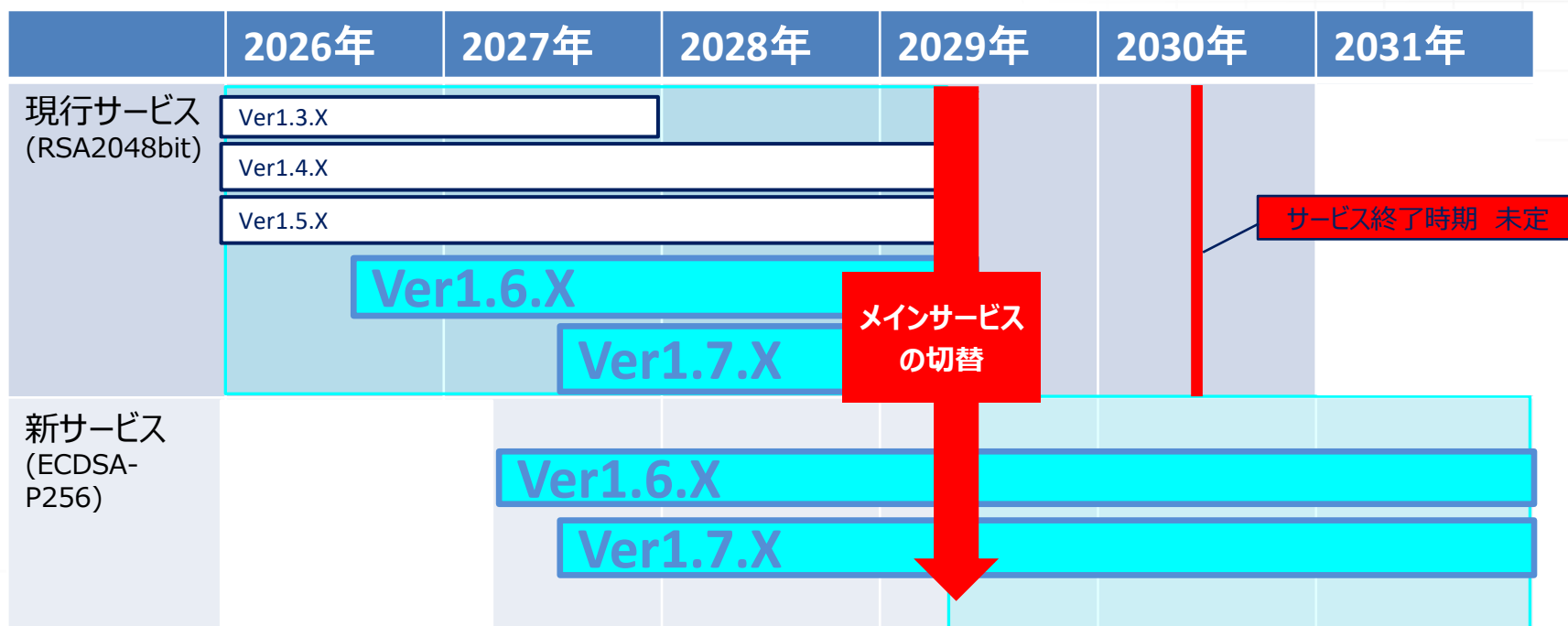


- 1) 2027年上期より128ビット相当暗号方式(ECDSA-P256)の新サービスをご提供開始予定
- 2) **2029年度、メインサービスを128ビット相当暗号方式(ECDSA-P256)に切替**予定
(2030年末までの移行完了に向けた措置)
- 3) **メインサービス切替から一定期間後、112ビット相当暗号方式のサービスはサービス提供を終了**予定

※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。

SEIKO タイムスタンプの暗号移行計画にあわせ、eviDaemon for XAdES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 XAdESバージョンアップ計画



- ・2026年8月上旬リリース予定のeviDaemon for XAdES Ver1.6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」時点までに、
Ver1.6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。

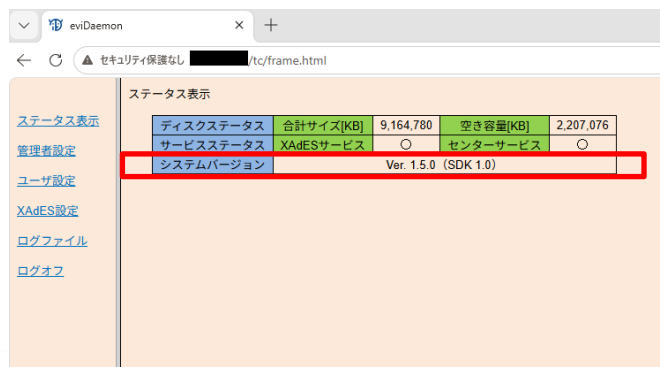
eviDaemon for XAdESをご利用頂いているお客様には以下のご対応をお願い致します。

- 2029年度に予定されている弊社タイムスタンプのメインサービス切替までに、
eviDaemon for XAdES Ver1.6以降へのバージョンアップをご計画ください。

ご利用中のバージョン	お客様側の対応	補足
Ver1.6.X以降	本件に関する対応は不要	新サービスへの対応済
Ver1.5.X Ver1.4.X	Ver1.6以降へのバージョンアップが必要	・2029年度メインサービスの切替までに対応が必要 ・メインサービス切替後、新規タイムスタンプ取得ができなくなる
Ver1.3以前	Ver1.6以降へのバージョンアップが必要	・2029年度メインサービスの切替までに対応が必要 ・メインサービス切替後、新規タイムスタンプ取得ができなくなる ・通信環境等の観点からでもバージョンアップをご案内済

eviDaemon for XAdESバージョンの確認方法

eviDaemon for XAdESの管理画面のステータス表示より、「システムバージョン」をご確認ください。



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、Ver1.6以降で継続して検証可能です。

Q2. 電子署名も今回の対象ですか？

A2. 本資料はタイムスタンプに関するご案内です。

電子署名については、ご利用中の認証局や証明書の種類により対応が異なりますので、認証局からのご案内にもとづき対応をご検討いただく必要がございます。

SEIKO

セイコーソリューションズ株式会社