



2016年6月

セイコーソリューションズ株式会社
サイバータイムセンター

時刻認証サービス利用に関わる注意事項

セイコータイムスタンプ サービスをご利用いただきましてありがとうございます。時刻認証サービスは暗号技術を基盤とした仕組みを使用しております。その仕組み上、使用にあたって下記注意を払う必要事項（1～10項）がございます。

また、サービスタイプが2種類の様態がございます。ご検討にあたって下記注意を払う必要事項（第6項）がございます。

1. タイムスタンプの有効期限と対象文書の保存期間

使用している暗号技術には有効期限があります。そのため有効期限を過ぎたタイムスタンプは有効ではありません。文書の証明にあたっては、その文書保存期間以上の有効期間を持ったタイムスタンプを取得する必要があります。

弊社時刻認証サービスで発行するタイムスタンプの有効期間は7～10年となっておりますので、その期間以上保存が必要な文書には有効期限延長等の対応が必要となります。

2. タイムスタンプ生成に用いる暗号技術

弊社時刻認証サービスで発行させていただくタイムスタンプには、暗号技術として総務省・経済産業省より発表された電子政府奨励暗号リストに掲載されているアルゴリズムを使用しており、十分な安全性を持っています。

弊社時刻認証サービスで発行するタイムスタンプは、タイムスタンプを押印した時刻から、TSA証明書の有効期限までがタイムスタンプの有効期間となります。

3. タイムビジネス信頼・安心制度認定

上述の有効期限を過ぎたタイムスタンプは有効ではありません。よって、『タイムビジネス信頼・安心認定制度』は有効期限を過ぎたタイムスタンプの信頼や安心を裏付けるものではありません。

4. タイムスタンプの有効期間の短縮

上述の通り、タイムスタンプには暗号技術を使用しております。暗号技術は日進月歩であり、安全であった暗号が突然危殆化することもあります。そういった場合、タイムスタンプの有効期限が短縮される可能性がございますのでご承知おきください。



5. 暗号アルゴリズム危殆化への対応

暗号アルゴリズムの危殆化が生じた場合や発行済みのタイムスタンプの有効期限内に危殆化が起こりうると予測される事態が発生した場合には以下の事項を実施します。

- ・事象が発生したこともしくは発生しうることを、できるだけ速やかに告知するか利用者様や関係各所へ通知します。
- ・発生した事象によるサービスの影響を考慮し、必要に応じて当該アルゴリズムを用いたタイムスタンプの発行の停止やシステムの改修を含めた対応計画を検討します。
- ・上記の対応計画を、できるだけ速やかに告知するか利用者様や関係各所へ通知します。

6. サービスタイプの様態

本サービスには、下記2種類のサービスがございます。

(1) 「Accredited サービス」

日本データ通信協会による「タイムビジネス信頼・安心認定制度」の認定を受けたタイムスタンプサービスであり、サービス内容により以下のタイプに細分されます。

「Accredited TypeG」

GMO グローバルサイン株式会社による「GlobalSign 認証業務」から認証された TSA 証明書を用いた認定タイムスタンプサービス

「Accredited TypeA」

GMO グローバルサイン株式会社による「DocumentSign Digital ID for Adobe CDS 認証業務」から認証された TSA 証明書を用いた認定タイムスタンプサービス

「Accredited TypeGT」

GMO グローバルサイン株式会社による「GlobalSign 認証業務」から認証された TSA 証明書を用い、かつ時刻監査証を参照情報としてタイムスタンプに添付する認定タイムスタンプサービス

「Accredited TypeGL」

GMO グローバルサイン株式会社による「GlobalSign 認証業務」から認証された TSA 証明書を用い、かつ、Accredited TypeG とは異なり、CA 証明書をタイムスタンプに添付しない認定タイムスタンプサービス

「Accredited TypeA2」

GMO グローバルサイン株式会社による「GlobalSign 認証業務」の内、AATL に登録された CA から認証された TSA 証明書を用いた認定タイムスタンプサービス

「Accredited TypeA2L」

GMO グローバルサイン株式会社による「GlobalSign 認証業務」の内、AATL に登録された CA から認証された TSA 証明書を用い、かつ、Accredited TypeA2 とは異なり CA 証明書をタイムスタンプに添付しない認定タイムスタンプサービス



(2) 「Advanced サービス」

汎用性を重視した一般向けセキュアタイムスタンプサービスであり、ハッシュアルゴリズムを除いて認定サービスと同一のセキュリティで運用されます。

日本データ通信協会による「タイムビジネス信頼・安心認定制度」の認定対象外のサービスです。認定を必要とする一部の政府関連文書へのタイムスタンプ用途に用いることはできません。

サービス内容により以下のタイプに細分されます。

「Advanced TypeG」

GMO グローバルサイン株式会社による「GlobalSign 認証業務」から認証された TSA 証明書を用いた汎用タイムスタンプサービス

「Advanced TypeA」

GMO グローバルサイン株式会社による「DocumentSign Digital ID for Adobe CDS 認証業務」から認証された TSA 証明書を用いた汎用タイムスタンプサービス

「Advanced TypeA2」

GMO グローバルサイン株式会社による「GlobalSign 認証業務」の内、AATL に登録された CA から認証された TSA 証明書を用いた汎用タイムスタンプサービス

詳細に関しましては、弊社時刻認証サービス運用規程をご参照ください。

7. TAA事業者の変更

本サービスは、日本データ通信協会認定のTAA事業者からの時刻配信監査を受けています。時刻配信監査を依頼しているTAA事業者は、変更されることがあります。変更の履歴については弊社時刻認証サービス運用規程第9章を参照ください。また、これらの変更に伴う本サービスの時刻精度、保証レベルは変更されません。

8. タイムスタンプ署名アルゴリズムについて

本サービスは、タイムスタンプ署名アルゴリズムとして下記を採用します。

「Accredited TypeG」	SHA512withRSA
「Accredited TypeA」	SHA512withRSA
「Accredited TypeGT」	SHA512withRSA
「Accredited TypeGL」	SHA512withRSA
「Accredited TypeA2」	SHA512withRSA
「Accredited TypeA2L」	SHA512withRSA
「Advanced TypeG」	SHA256withRSA
「Advanced TypeA」	SHA256withRSA
「Advanced TypeA2」	SHA256withRSA



9. TSA証明書暗号アルゴリズムの移行

本サービスは、「Accredited TypeG」・「Accredited TypeGT」・「Advanced TypeG」で使用しているTSA証明書および中間CA証明書およびRoot CA証明書の暗号アルゴリズムをSHA1からSHA256に変更いたしました。それに伴い、OIDを下記に変更いたしました。

「Accredited TypeG」 1.3.6.1.4.1.955.1.10.1.3.1→1.3.6.1.4.1.955.1.10.1.3.3

「Accredited TypeGT」 1.3.6.1.4.1.955.1.10.1.3.2→1.3.6.1.4.1.955.1.10.1.3.4

なお、従来サービス(1.3.6.1.4.1.955.1.10.1.3.1および1.3.6.1.4.1.955.1.10.1.3.2)については、2012/9/30に停止いたしました。

「Accredited TypeA」・「Advanced TypeA」・「Accredited TypeA2」・「Advanced TypeA2」で使用しているTSA証明書および中間CA証明書は、すでにSHA256に対応しております。

10. 認定事業者の承継

本サービスは、2013年4月1日より、セイコープレジジョン株式会社からセイコーソリューションズ株式会社に、事業譲渡されました。過去に本サービスによって発行されたタイムスタンプに対する全ての責任と義務は、セイコーソリューションズ株式会社が承継しています。承継に伴うタイムスタンプサービスの品質の変更はありません。

2013年4月1日にサービス承継に伴う旧事業者から新事業者への運用移行が実施されております。移行期間中は、新旧事業者のタイムスタンプが混在していますが、すべて新事業者が品質を保証し、日本データ通信協会の認定サービスの対象として扱われます(Advanced Typeを除く)。

以上