2025 年 08 月 25 日

サーバー証明書発行サービスご利用者様各位

株式会社日本レジストリサービス（JPRS）

サーバー証明書の失効に関する留意事項

本書は、当社のサーバー証明書発行サービスをご利用いただく際に重要な「サーバー証明書の失効」に関する留意事項を記載しています。サーバー証明書の適切な運用を行うため内容をご理解いただき、以下 3 つの事項にご留意くださいますようお願い申し上げます。

A. サーバー証明書は有効期間中でも失効が必要になる可能性があります

1. サーバー証明書の失効とは

サーバー証明書の秘密鍵が危殆化した場合や、信頼性が失われた場合に、そのサーバー証明書の効力を停止させる手続きが「サーバー証明書の失効」です。

2. サーバー証明書の失効が必要となるケース

サーバー証明書の秘密鍵が安全ではなくなった場合、その効力をすみやかに停止することで、悪意ある攻撃者からの脅威を阻止し、サーバー証明書利用者およびインターネット全体の安全を守ることができます。

サーバー証明書の失効が必要となる主なケースは以下の通りです。

- 秘密鍵の漏洩：サーバー証明書の秘密鍵に盗難や漏洩があった場合
- 誤発行：誤って発行された、または発行時に適切な審査が行われなかった場合
- 情報の変更：ドメイン名や組織情報の変更に伴いサーバー証明書に含まれる情報が不正確となった場合

より具体的なケースと失効期間に関しては「参考」に記載しています。

3. 認証局の原則

当社を含めたインターネット上の Web サイトに利用されるパブリックなサーバー証明書を発行する認証局は、インターネットの通信や認証の信頼性を維持するため、業界団体である CA Browser Forum が定める Baseline Requirements(BR) [1]および、各ブラウザベンダーが定めるポリシーを遵守し、サーバー証明書の失効に関するポリシーを遵守する必要があります。

4. 業界の動向

「Mozilla Root Store Policy[2] Version 3.0」ではサーバー証明書の失効に対する遅延を許容しないと明記されており、他のブラウザベンダーも同様にサーバー証明書の失効とその期間に対して厳格な姿勢を見せています。

5. 当社の対応

当社は、証明書利用者のシステムに関する問題がある状況や、当社と証明書利用者との連絡が円滑でない状況であっても、失効が必要なサーバー証明書に対して、ポリシーで定められた期間内に失効させる義務を負っています。したがって、**緊急性が高いケース（例：秘密鍵の漏洩）では、サーバー証明書利用者様への事前連絡や個別の同意を得ることなく、当社がサーバー証明書の失効を行う場合があります。**これはインターネット全体の安全性、ならびにサーバー証明書利用者の Web サイトを訪問するユーザーの保護を目的とした措置です。サーバー証明書の失効に関するポリシーの遵守にご理解をお願い申し上げます。

B. 突発的なサーバー証明書の失効に対応できる運用方法の整備をお願いいたします

サーバー証明書の失効が必要となる事態に備え、迅速に対応できないシステムや環境の見直しをお願いいたします。

以下のようなシステムや運用方法では、サーバー証明書の失効について迅速に対応することが難しいため、認証局がサーバー証明書を失効することで予期せぬサービス停止やセキュリティリスクにつながる可能性があります。状況に応じて、**運用方法の改善や代替手段をご検討ください。**

[1]Baseline Requirements（BR）：サーバー証明書の認証局事業者やブラウザベンターで構成される業界団体が策定する証明書の発行ガイドライン
[2] Mozilla Root Store Policy：Mozilla が定めた証明書に関するルールや基準

・厳格な可用性が求められ、計画外のシステム停止が難しく、サーバー証明書の緊急交換や迅速な導入が困難なシステム
・複雑な組織プロセスや手動での作業に依存しており、サーバー証明書の失効、再発行などの手続きに時間がかかる運用体制
・サーバー証明書の再発行に必要な作業時間が認証局の定めるサーバー証明書の失効期間と合致しない原因となる、外部の規制や承認プロセスが必要な体制

このような環境では、ポリシーで定められた失効期間内にサーバー証明書を交換する対応ができない可能性が高まります。

運用方法にこのような制約がある場合、パブリックなサーバー証明書ではなく、プライベート PKI/認証局等による証明書の利用を推奨いたします。運用状況に応じてご検討くださいますようお願い申し上げます。

C. サーバー証明書の失効が必要な際はすみやかにご申請ください

サーバー証明書の失効が必要な事態が発生した場合や当社から要請があった際には、**ご利用の指定事業者へすみやかにサーバー証明書の失効および再発行をご申請ください。**当社は指定事業者からの失効申請を確認後、順次その処理を実施いたします。

サーバー証明書利用者様とインターネット全体の安全を守るため、サーバー証明書の適切な運用体制の整備および失効にご協力をお願い申し上げます。

以上

参考

「Baseline Requirements 4.9 項」が規定しているサーバー証明書が失効されるケースと期間

- 24 時間以内の失効が「必須」となるケース
  - a. サーバー証明書利用者が書面でサーバー証明書の失効を要求し、失効理由コードを特定しない場合
  - b. サーバー証明書利用者が認証局に対し、元のサーバー証明書証明書要求が承認されておらず、事後的に承認も与えられないことを通知した場合
  - c. 認証局が、サーバー証明書内の公開鍵に対応する秘密鍵が漏洩した証拠を得た場合
  - d. サーバー証明書内の公開鍵に対応する秘密鍵を容易に算出できる方法を認証局が認識した場合
  - e. 認証局が、サーバー証明書に含まれる任意の FQDN[3]または IP アドレスのドメイン認証または管理が信頼できないという証拠を得た場合
- 24 時間以内に失効が「原則、必要」、5 日以内に失効が「必須」となるケース
  - f. サーバー証明書が BR における要件に準拠しなくなった場合
  - g. 認証局がサーバー証明書の悪用された証拠を得た場合
  - h. サーバー証明書利用者が利用者契約または利用規約における重要な義務の一つ以上を違反したことが認証局に知らされた場合
  - i. サーバー証明書内の FQDN または IP アドレスの使用が法的に許可されなくなったことを示す状況が認証局に知らされた場合
  - j. ワイルドカード証明書が FQDN を認証するため不正に使用されたことが認証局に知らされた場合
  - k. サーバー証明書に含まれる情報に重要な変更があったことを認証局が認識した場合
  - l. サーバー証明書が BR または認証局の規則に従って発行されなかったことが認証局に知らされた場合
  - m. 認証局がサーバー証明書に表示されている情報のいずれかが不正確であると認識した場合
  - n. 認証局の BR に基づくサーバー証明書を発行する権利が取り消し、または終了し、認証局が失効情報を管理できなくなった場合
  - o. BR に記載の失効理由には該当しないが、認証局の規定により失効が要求される場合
  - p. サーバー証明書利用者の秘密鍵の漏洩を認証局が認識した場合、または秘密鍵の生成に使用された方法に明確な欠陥がある場合

[3]FQDN：DNS のホスト名やサブドメイン名などのラベルをすべて省略せずに書いた記述形式