

サーバにアクセスすると「証明書は失効しています」と表示される

問題

サーバにアクセスすると「証明書は失効しています」と表示されるようになった。

解決方法

エラー詳細：

Windows Vista / Windows 7 上の Internet Explorerの場合：

このWebサイトのセキュリティ証明書には問題があります。

この組織の証明書は失効しています。

セキュリティ証明書の問題によって、詐欺や、お使いのコンピュータからサーバーに送信される情報を盗み取る意図が示唆されている場合があります。

Windows Vista / Windows 7 上の Google Chromeの場合：

このサーバーのセキュリティ証明書は取り消されています

～にアクセスしようとしたますが、サーバーにより提示された証明書は発行元により取り消されています。これは、サーバーにより提示されたセキュリティ認証が信頼できないことを示しており、悪意のあるユーザーと通信を行っている可能性があります。処理を続行しないでください。

Windows 上の Safariの場合：

SafariはWebサイト～の識別情報を検証できません。

このWebサイトの証明書は無効です。～に偽装したWebサイトに接続している可能性があり、機密情報が漏えいするおそれがあります。

Operaの場合：

セキュア処理を完了することができません

アクセス先のアドレス～は現在使用できません。

保護された接続: 致命的なエラー(44)

証明書が発行人により無効にされています

Windows XP 上の Internet Explorerの場合：

このWebサイトのセキュリティ証明書には問題があります。

この組織の証明書は失効しています。

セキュリティ証明書の問題によって、詐欺や、お使いのコンピュータからサーバーに送信される情報を盗み取る意図が示唆されている場合があります。

Firefoxの場合：

安全な接続ができませんでした

～への接続中にエラーが発生しました。

Peer's Certificate has been revoked.

(エラーコード: sec_error_revoked_certificate)

Mac OS X 上の Safariの場合：

SafariはWebサイト～の識別情報を検証できません。

このWebサイトの証明書は無効です。～に偽装したWebサイトに接続している可能性があり、機密情報が漏えいするおそれがあります。

Windows XP 上の Google Chromeの場合：

このサーバーのセキュリティ証明書は取り消されています。

～にアクセスしようとしたますが、サーバーにより提示された証明書は発行元により取り消されています。これは、サーバーにより提示されたセキュリティ認証が信頼できないことを示しており、悪意のあるユーザーと通信を行っている可能性があります。処理を続行しないでください。

サーバにインストールされているサーバ証明書が何らかの理由により失効されていることが原因です。

この場合、上に挙げたブラウザでは場合によってエラーメッセージが表示されることがあります(*1)。

Safariを除いてこの画面から続行することはできませんし、文面にもある通り偽装・なりすましのおそれがありますので、そのサーバの管理者にお問い合わせください。

特に旧プロジェクトで発行された証明書は、認証局閉局に伴い2009年11月より全て失効されています。

サーバ管理者の方はすみやかに新しいサーバ証明書をインストールしてください。

(*1) - 各ブラウザがデフォルト設定のままであればエラーメッセージは表示されません(*2)。

エラーメッセージが表示されるのは下記設定が変更されている場合に限られます。

- Windows XPおよびそれ以前の上のInternet Explorerの場合（同OS上のGoogle Chromeも同じ設定を参照）
[ツール]→[インターネットオプション]→[詳細設定]→「サーバ証明書の取り消しを確認する」
- Firefoxの場合
[ツール]→[オプション]→[詳細]→[暗号化]→[失効リスト]
ここで表示されているCRLのみ失効確認されます。

- Mac OS X上のSafariの場合
"アプリケーション / ユーティリティ / キーチェーンアクセス"を起動
[キーチェーンアクセス]→[環境設定]→[証明書]→「証明書失効リスト(CRL)」

(*2) - 2009年11月の調査に基づくものです。

ここではCRL (Certificate Revocation List, 証明書失効リスト) を用いた失効確認のみを対象として調査しております。
本プロジェクトで発行された証明書はOCSPによる失効確認をサポートしていませんのでOCSPは調査対象外です。

関連記事

- [サーバ証明書の発行申請時にエラーコード 371:1「主体者DN,主体者DNのOUが許可リストとして登録された値と一致しません。」が表示される](#)
- [サーバ証明書の新規発行申請時にエラーコード 212「主体者DN,指定したDNはすでに存在しています。」が表示される](#)
- [電子証明書自動発行支援システムやUPKI申請システムにログインできなくなった](#)
- [ブラウザでのクライアント証明書認証時、エラーが表示される \(2021年8月31日以降\)](#)
- [登録担当者が支援システムにアクセスすると、エラーが表示されます](#)