

Java JCE関連例外逆引きメモ

Java JCE関連で出てくる例外メッセージから原因を探るための「逆引きメモ」を残しておこうと思います。

java.io.IOException: subject key, Unknown key spec: Invalid RSA modulus size.

CertificateFactory.generateCertificateなどで4096bitなど鍵長の大きい鍵の証明書等を読み込むと起きることがある。J2SE 1.4ではRSA4096はダメ。J2SE 6.0かBouncyなどの他のJCEプロバイダを使う。

java.io.IOException: Response is unreliable: its validity interval is out-of-date

ローカル時計が大幅にずれていて取得したOCSPレスポンスが時間範囲外の場合に起きることもある。sun.security.provider.certpath.OCSF.check