

平成17年12月12日

総合行政ネットワーク運営協議会

LGPKIにおけるハッシュ関数MD5の廃止について

現在、LGPKIの各CAから発行された自己署名証明書のフィンガープリントについては、sha-1及びMD5の2種類のハッシュ関数にて公開しております。

しかし、このうちMD5については脆弱性が発見されていることから、LGPKIとしては、MD5による自己署名証明書のフィンガープリントの公開を、平成17年12月12日を以って廃止することとしました。

「地方公共団体における組織認証基盤(LGPKI)」のホームページに掲載しているフィンガープリント一覧より、MD5を削除いたしましたので、今後、LGPKIの各CAから発行された自己署名証明書のフィンガープリントを確認するに当たっては、sha-1にてご確認いただきますよう、お願いいたします。