2017 年 3 月 2 日
一般財団法人日本データ通信協会
タイムビジネス認定センター

「SHA-1 衝突の実現」による
時刻認証業務認定事業者が発行するタイムスタンプへの影響について

2 月 23 日に米 Google Inc.より「SHA-1 衝突の実現」に関する発表がありました。これを受け、一般財団法人日本データ通信協会が「タイムビジネス信頼・安心認定制度」に基づき認定する時刻認証業務認定事業者の認定に係る業務により発行されるタイムスタンプへの影響についてお知らせします。
2007 年以降に発行されたタイムスタンプは、すべて SHA-256 以上の文書ハッシュが用いられており、本件への影響は無いことを確認しました。また、2006 年以前に発行されたタイムスタンプは、その一部で SHA-1 の文書ハッシュが用いられており、有効期間を経過していないタイムスタンプが存在する可能性があります。しかしながら、本件では、予め与えられたハッシュ値となるような文書を新たに生成することはできませんので、影響が出ることはないと考えます。

（参考）

米 Google Inc.の発表
https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html
概要：初めての SHA-1 の衝突
米 Google が 2 月 23 日に発表した通り、Google はオランダの CWI Institute との共同研究により SHA-1 の衝突を初めて実現しました。発表に合わせて同じハッシュ値となる異なる 2 つの PDF コンテンツも提示されており、90 日後には、同じハッシュ値を持つ異なる 2 つの PDF を生成するためのコードを公開するともアナウンスされています。

米 Google Inc.の発表に対する我が国 CRYPTREC 暗号技術評価委員会の見解
https://www.cryptrec.go.jp/topics/cryptrec_20170301_sha1_cryptanalysis.html
概要：SHA-1 の安全性低下について
現在、CRYPTREC では、SHA-1 を「CRYPTREC 暗号リスト」の「運用監視暗号リスト」に掲載し、互換性維持以外の目的での利用を推奨していません。また、情報セキュリティ政策会議からも 2008 年に移行指針が発表されています。このように SHA-1 の安全性低下が進んでいることから、SHA-256 等のより安全なハッシュ関数への移行を推奨いたします。

以上