2005.12. Ver.1.0

タイムスタンプにおけるＳＨＡ－１問題に関連する対応策検討のための説明補足図

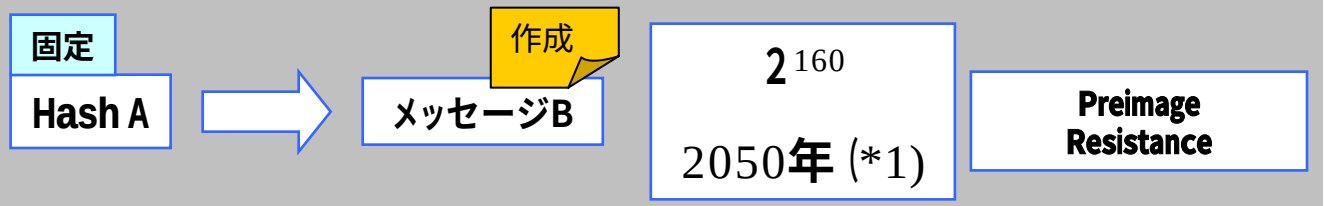
2005年12月

タイムビジネス推進協議会

SHA1の脆弱性

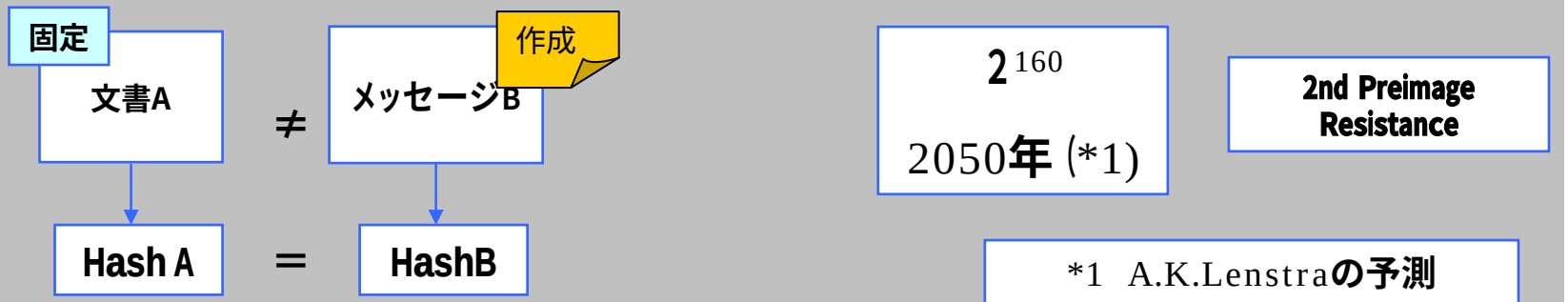
ケース1

固定のHash 値Aから同じHash値を持つメッセージBを作成　(ハッシュ値から原文作成)



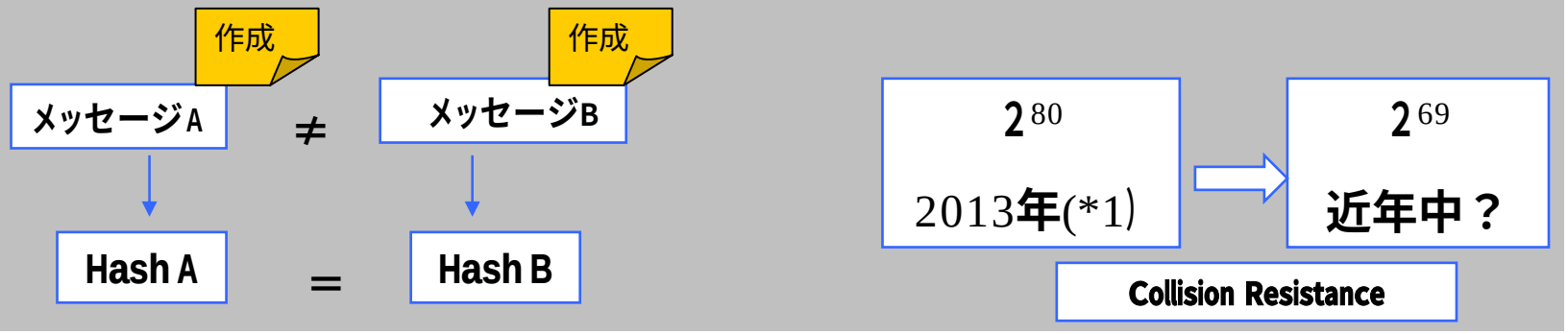
ケース2

固定の文書Aと、同じHash値を持つメッセージBの作成 (先に原文を2つ作成)



ケース3

同じHash値を持つ任意のメッセージA、Bの作成　：　今回の脆弱性指摘



TA-TSA-User間の通信環境におけるケース1～3の適用領域