資料５－８

番号連携に関するご参考資料

情報連携基盤技術WG構成員
中上昇一

目次

※なお、本資料では、IDコードおよび各リンクコードの対応関係を
セキュアに管理することを前提としています。

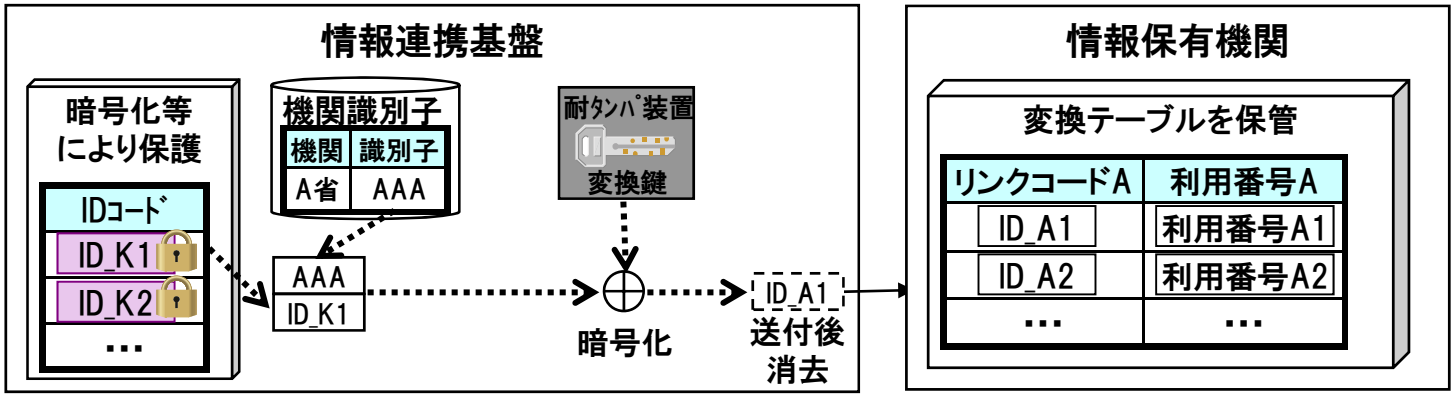
1. リンクコードの生成・変換方法の概要（一例）

1．1　暗号活用方式におけるリンクコードの生成・変換方法

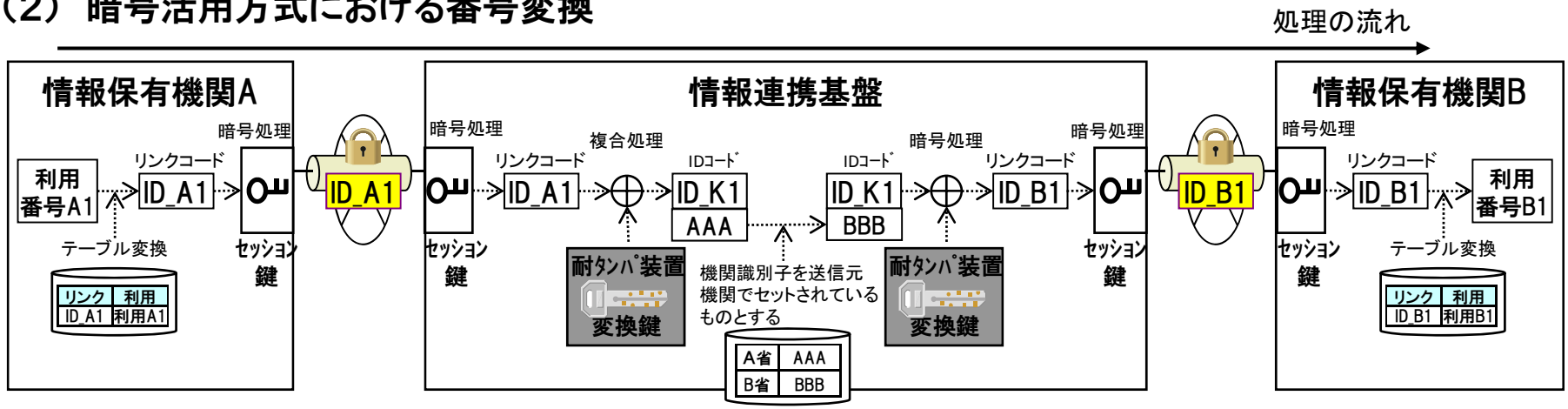
（1） 暗号活用方式におけるリンクコード生成

・変換鍵を使ってIDコードを暗号化し、リンクコードを生成する。
・生成したリンクコードは各情報保有機関へ送付した後は消去し、情報連携基盤では管理しない。
・IDコードは暗号化等により保護し、変換鍵は耐タンパ装置等で安全に管理する。

ポイント　番号のリンクは変換鍵を使って実現し、安全性は変換鍵を守る事で実現する



（2） 暗号活用方式における番号変換

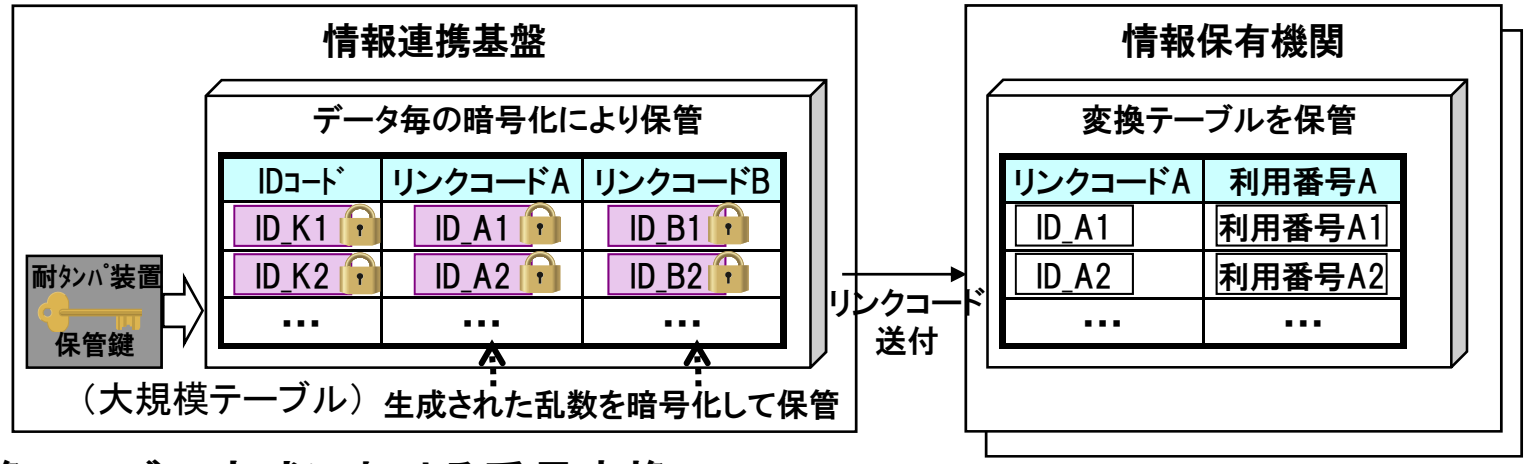


1．2　変換テーブル方式におけるリンクコードの生成・変換方法

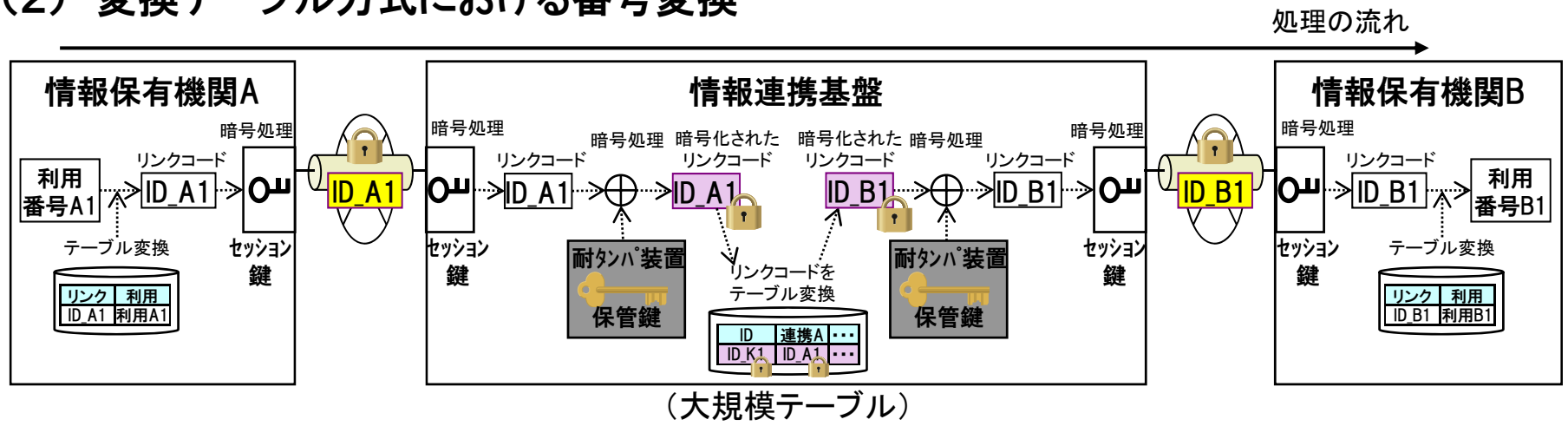
（1） 変換テーブル方式におけるリンクコード生成

・乱数等によりリンクコードを生成し、対応付けは変換テーブルにて管理する。
・変換テーブルでは、データ毎の暗号化等により保護し、その暗号化鍵は耐タンパ装置等で管理する。

ポイント　番号のリンクは変換テーブルで実現し、安全性は保管鍵を守る事で実現する



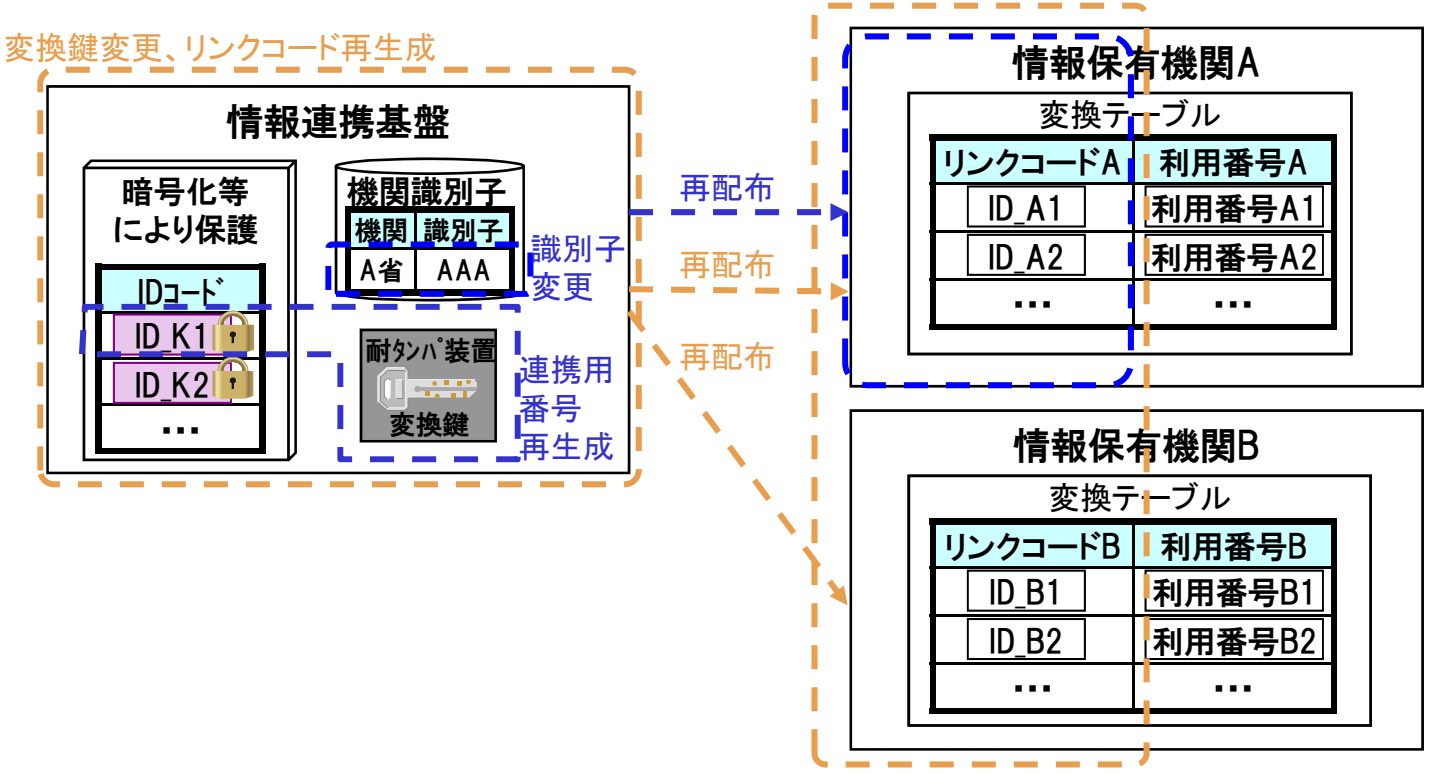
（2） 変換テーブル方式における番号変換



2. 1　暗号活用方式におけるリスクと影響範囲

（1）一部の情報保有機関でリンクコードを含む変換テーブルが漏洩した場合の対策
・機関識別子を変更するなどして、当該情報保有機関のリンクコードを再生成、再配布が必要である。

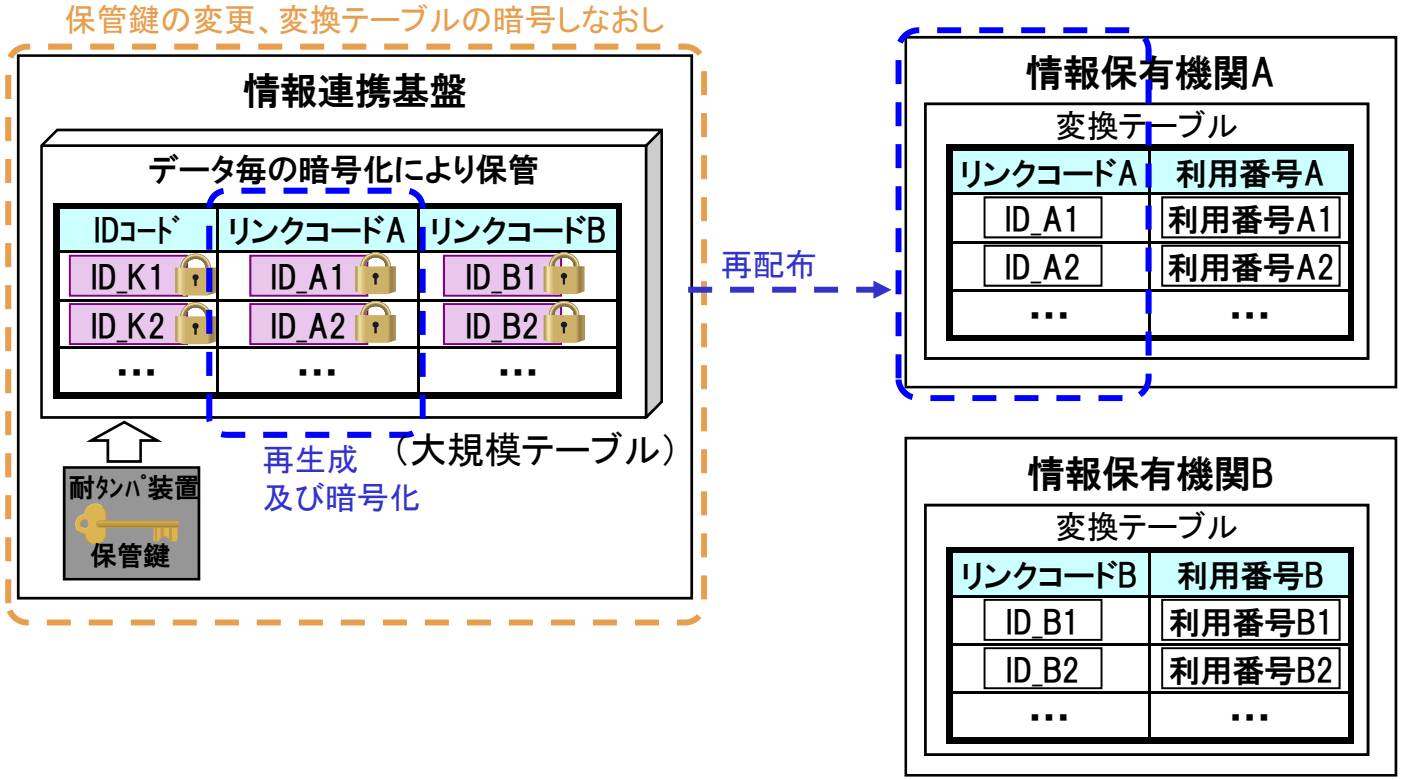
（2）暗号アルゴリズムの危殆化、変換鍵の更新への対策（数年毎に発生）
・IDコードの再付番、変換鍵の変更、全てのリンクコードの再生成、全ての情報保有機関への再配布が必要である。



2. 2　変換テーブル方式におけるリスクと影響範囲

（1）一部の情報保有機関でリンクコードを含む変換テーブルが漏洩した場合の対策
・当該情報保有機関のリンクコードを再生成、再配布する必要がある。

（2）暗号アルゴリズムの危殆化、変換鍵の更新への対策（数年毎に発生）
・保管鍵とアルゴリズムの移行（変換テーブル内情報の暗号しなおし）が必要になる。
ただし、情報連携基盤での処理となる。



3. リンクコードの変更処理例

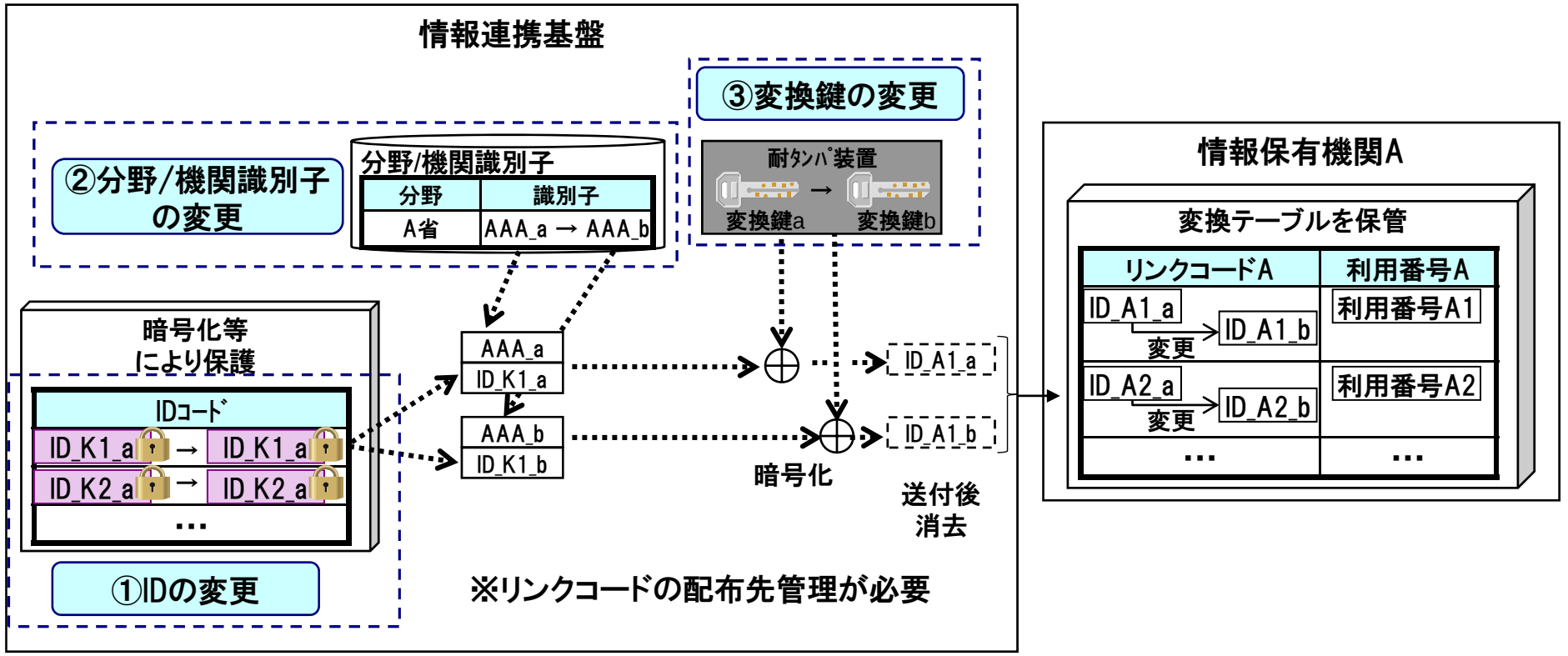
（1） リンクコード変更のケース

- リンクコードを変更するには、以下の3つのケースが考えられる。
  - ① IDコードの変更
  - ② 分野/機関識別子の変更
  - ③ 変換鍵の変更

（2） リンクコード変更の手順

- 上記いずれかの変更により、新・旧のリンクコードのセットを生成し、情報保有機関に送付する。
- 情報保有機関では、受け取った新・旧のリンクコードのセットをもとに、リンクコードの更新を行う。

※ 移行期間への対応が必要となる



4. まとめ

○：他の案に比べると影響が少ない、　△：他の案に比べると影響が大きい

比較項目	（1）暗号方式	（2）変換テーブル方式
処理性能	・運用上問題ない処理性能の実現が可能と想定される ○	・相対的に時間がかかる可能性がある △
一部の情報保有機関でのリンクコード漏洩時	・センタ処理と、対象機関へのリンクコード再配布を行う ○	・センタ処理と、対象機関へのリンクコード再配布を行う ○
暗号アルゴリズム危殆化、鍵更新時	・センタ処理と、全機関へのリンクコード再配布を行う ○ ※ただし、実施するのは数年に一度であり、影響範囲は限定される	・センタ処理を行う ○ ※ただし、実施するのは数年に一度であり、かつ影響範囲はセンタ内のみである

参考資料:リンクコード変換性能の計算例(理論値)

【暗号演算】

- 3.0G[Hz]のCPUを搭載したコンピュータが全ての帯域を暗号演算に用いた場合
  ※　純粋な暗号演算のみ、I/Oは含まない
- 方式:AES　鍵長:256[bit]　　ブロック長:128[bit]　＝　16[Byte]
- 1回の暗号化:350～700[cycle]　平文の長さ:16<x<33[Byte]　＝　2[ブロック]
  ※　1[cycle]＝CPUの処理単位(ex. 3.0G[Hz]のCPUは秒間3G[回]の処理が可能
- 1[ID]の処理にかかる時間
  (2[ブロック]＊700[cycle])／(3.0G[Hz])　＝　0.47μ[秒]

【リンクコードの変換】(リンクコードは最大32Byteと想定)

- IDコード→リンクコード　＝　0.47μ[秒]
- リンクコードA→IDコード→リンクコードB　＝　0.94μ[秒]

※　いずれもI/Oは含まない、機関IDは用意されているものとする

【4千万件のリンクコード変換】

- (リンクコードA→IDコード→リンクコードB)＊4千万件　＝　37.6[秒]

※　いずれもI/Oは含まない、分野IDは用意されているものとする