

リンクコード変換処理性能について

2011年6月7日
情報連携基盤技術WG
構成員 鈴木

はじめに

本資料は、情報連携基盤技術WG骨格案にて提示されているリンクコード方式が、「情報連携処理においてどの程度の負荷をもたらすか（処理時間にどの程度影響を及ぼすか）」について試算・検討した内容を記載しています。

連携方式の検討材料の一部としていただくために、不確定要件においては仮定を置いて検討しており、結果等について確定的なご提案を行うものではありませんので、ご注意ください。

リンクコードの処理性能を試算する上での前提条件

1. 対象業務について

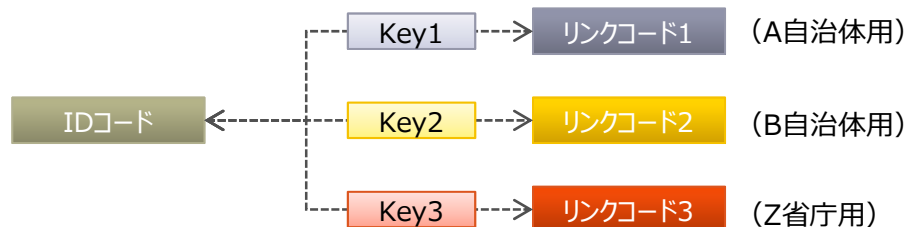
- ・処理件数の非常に大きなもので試算するという観点から、「公的年金の源泉徴収票を、日本年金機構から情報連携基盤を通じて国税庁へ送付する」という業務を想定しました。
- ・年間処理件数を35,800,000件と設定し、これを1トランザクションで処理する想定をしております。
※実際には、データ分割・複数トランザクション処理を行う設計をすべきですが、今回は敢えてもっとも負荷がかかるであろう処理形態を選択しています。

2. 試算範囲（情報連携処理フロー図参照）

- ・試算は、「日本年金機構からの送信～情報連携基盤での処理～国税庁での受信」部分のみとします。
- ・なお、データ転送においてはデータそのものの暗号化を行うことを想定し、試算に含めております。
※暗号方式はAES、リンクコード変換（次項）と異なり、ソフトウェアで処理するものとします。
- ・それぞれの前処理/後処理については、既存業務システムの内容と大きく関わることから、今回試算対象外としております。
※前処理/後処理に係る時間は、リンクコード方式以外でも同等と考えております。

3. リンクコード変換方式

- ・IDコードからリンクコード、リンクコードからIDコードへの変換には、国際標準であるAES暗号を用いるものとします。
- ・暗号鍵の生成・保管は、専用のハードウェア（HSM : Hardware Security Module）にて行うものとします。
- ・暗号鍵は、機関単位（リンクコード発行先単位）に変えるものとします。



リンクコードの処理性能を試算する上での前提条件

4. その他試算に用いる基礎値

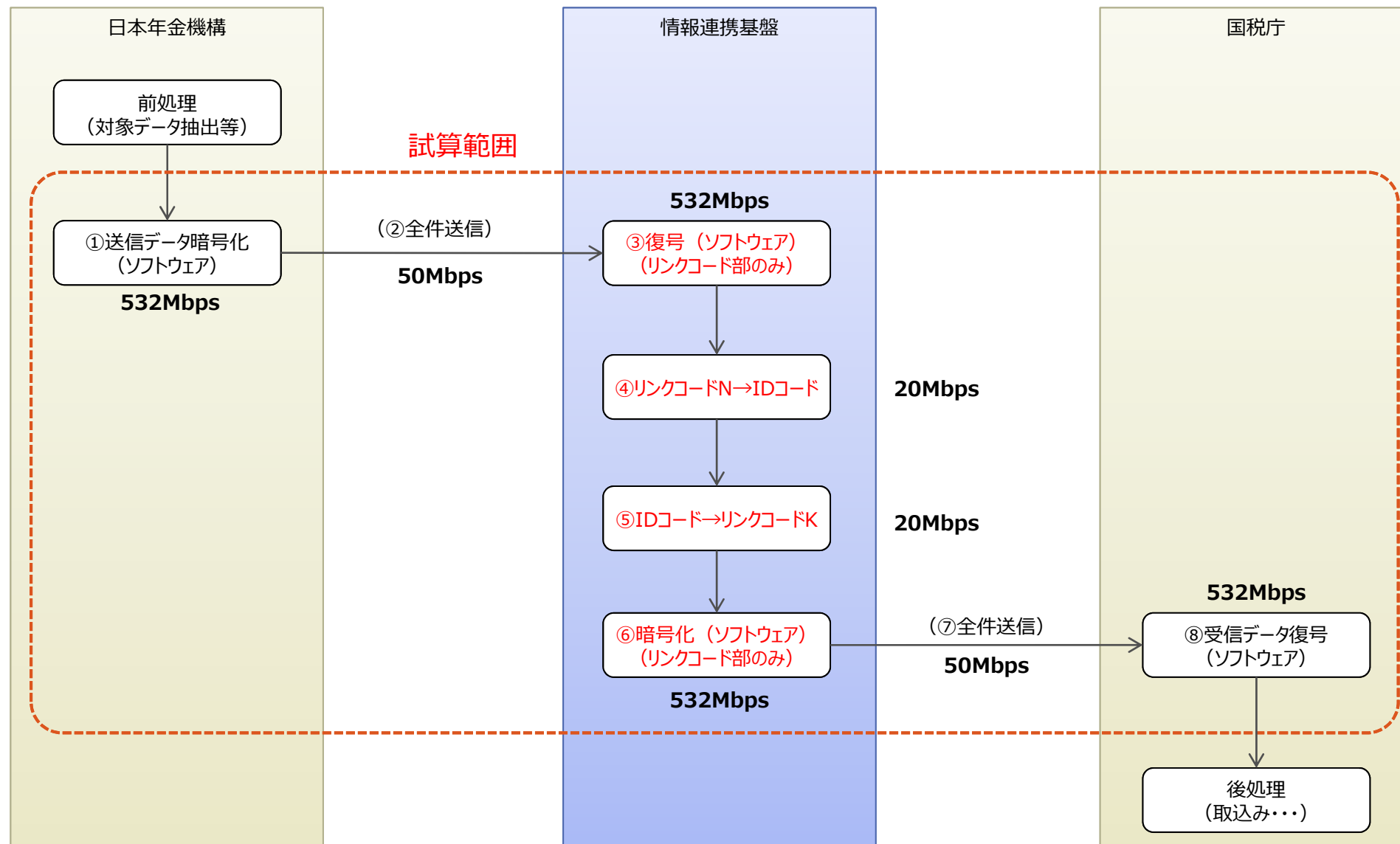
下表の数値は、全て当方にて想定した数値となります。

項目	数値	備考
1件あたり連携データ容量	2KB	源泉徴収票+ヘッダ情報で2KBと仮定しました（35,800,000件で、71.6GB）。
リンクコードサイズ	16B	
ハードウェアでの暗号演算性能 （HSMのスループット）（*1）	20Mbps	市販品を想定。単体性能4～60Mbps程度ですが、入出力のオーバーヘッドがあるため、実効性能を3分の1と仮定しました。 1秒間に156,250回の演算処理（リンクコード変換）が可能な数値です。
ソフトウェアでの暗号演算性能	532Mbps	「New AES software speed records」での測定値(*2)を基に算出しました。
回線速度	50Mbps	日本年金機構～情報連携基盤間、情報連携基盤～国税庁間。 50Mbpsの帯域保証型専用線と仮定しました。

（*1）ハードウェアでの処理においては、HSMがボトルネックになるため、HSMのスループットで試算をいたします。

（*2）New AES software speed recordsでの実際の測定値は1,064Mbps。ここでは実効性能として約2分の1と仮定しました。
測定環境：Intel Core2 Quad Q6600、OpenSSL

情報連携処理フロー



試算結果（どの程度の時間がかかるか）

項番	処理名称	処理時間（秒）	算定式
①	送信データ暗号化（ソフトウェア）	1,076	$35,800,000\text{件} \times 2\text{KB} \times 8\text{bit} \div 532\text{Mbps}$
②	（データ転送）	11,456	$35,800,000\text{件} \times 2\text{KB} \times 8\text{bit} \div 50\text{Mbps}$
③	復号（ソフトウェア）	9	$35,800,000\text{件} \times 16\text{B} \times 8\text{bit} \div 532\text{Mbps}$
④	リンクコードN→IDコード	229	$35,800,000\text{件} \times 16\text{B} \times 8\text{bit} \div 20\text{Mbps}$
⑤	IDコード→リンクコードK	229	$35,800,000\text{件} \times 16\text{B} \times 8\text{bit} \div 20\text{Mbps}$
⑥	暗号化（ソフトウェア）	9	$35,800,000\text{件} \times 16\text{B} \times 8\text{bit} \div 532\text{Mbps}$
⑦	（データ転送）	11,456	$35,800,000\text{件} \times 2\text{KB} \times 8\text{bit} \div 50\text{Mbps}$
⑧	送信データ復号（ソフトウェア）	1,076	$35,800,000\text{件} \times 2\text{KB} \times 8\text{bit} \div 532\text{Mbps}$

総処理時間**25,540秒（7時間5分40秒）**

そのうち、リンクコードの変換に係る時間（③～⑥）は**476秒（7分56秒）**

※上記数値（7分56秒）はCPU/HSMともに各1台での試算結果です。

CPU/HSMを複数台用意して並列処理を行うことにより、更に短縮が可能と想定されます。