

2304JuminhyoError.pdf

2023.4 ブログ：マイナカードで別人の住民票誤発行の原因、の詳細
(→ <http://www.1968start.com/M/blog/index3.html#2304>)

マイナカードで別人の住民票誤発行の原因

中所武司

■このブログのきっかけ

2023.3.29～3.31 の日経・朝日の記事：

- ・日経（3/29）「別人の住民票が誤って発行されるバグ」ほか
<https://xtech.nikkei.com/atcl/nxt/news/18/14913/>
- ・朝日（3/30）「マイナカードで別人の住民票」ほか
<https://www.asahi.com/articles/ASR3Z66DQR3ZUTIL02F.html>

■記事内容の要約とコメント（→★）

- ・27 日午前 11 時 40 分ごろ、コンビニで交付を受けようとした 2 人から、磯子、青葉の各区役所に「別人の住民票が出てきた」と連絡があった。東京都大田区も含め、計 4 人が 5 枚の別人の住民票を受け取っていた。
- ・同じ富士通 Japan のシステムを使っている全国約 30 団体の一部でシステムを一時停止。
＊横浜市、宮崎市、東京都（世田谷区、足立区）など
- ・横浜市はプログラム改修の報告を受け、3 月 29 日午前 6 時 30 分にサービスを再開。
- ・2017 年 1 月から同サービスを提供している富士通 Japan（広報）は、「今回初めて不具合が表面化した」、「リリース前にテストは実施していたものの、今回のような高い負荷を想定したテストが十分でなかったのが原因と考えている」とした。

→★直接の原因は、後述するような、タイムアウト処理のプログラムミスと思われる。
また、タイムアウトに関する基本的なテストが抜けていたと思われる。

- ・交付申請が同じ時間帯に集中してシステムに負荷がかかり、印刷処理の規定時間を超える「タイムアウト」が発生。
印刷イメージファイルが正しく取得されないまま印刷が解除され、次のファイルを取得してしまったという。

→★この説明が正しいとすると、以下の処理が実行されたと思われる：

ユーザAの入力操作に基づき、印刷イメージファイルが作成されたが、印刷操作による印刷コマンドがシステムに到着するのが遅れたため、システム側でタイムアウト処理が実行され、ユーザAの印刷イメージファイルが印刷不可の状態になった。

(多分、当該ファイルを削除したと思われる)

その後、印刷コマンドが到着したので、次の異なるユーザのファイルを印刷した。

・具体的な処理詳細：

- * コンビニで証明書交付を申請すると、コンビニ証明書交付サービス上で、住民票などの印刷イメージファイルが生成される。
- * 当該ファイルは申請者しか印刷できないようロックがかかるが、システムにはタイムアウトの上限が設定されていたため、アクセス集中で処理が遅れた際にタイムアウトとなってロックが解除された。
- * 同時期に申請した別の利用者が当該ファイルをつかめる状態にあったため、別人の住民票が印刷されるトラブルにつながったという。

→★この説明が正しいとすると、以下の処理が実行されたと思われる：

ユーザAの印刷イメージファイルに対して、タイムアウト処理が実行され、「当該ファイルは申請者しか印刷できないようロック」が解除され、誰でも印刷可能な状態になった。

(当該ファイルは削除されなかったと思われる)

その後、異なるユーザの印刷コマンドが到着したので、当該ファイルを印刷した。

- ・ 別の利用者がファイルをつかめてしまう仕様の詳細などについては回答を控えた。
富士通 Japan はタイムアウトでロックが解除されないようプログラムを改修。

→★プログラムミスの内容（推測）

記事の説明内容に曖昧さがあり、以下のいずれのケースかが不明：

ケースX：ユーザAの申請処理中にタイムアウトになり、当該住民票は削除され、ユーザAの印刷コマンドに対して、ユーザBの住民票が印刷された。

ケースY：ユーザAの申請処理中にタイムアウトになり、印刷不可となったが、当該住民票は残り、ユーザBの申請処理でユーザAの住民票が印刷された。

ケースZ：ロックやロック解除の処理や、タイムアウトの処理の有無には関係なく、印刷イメージファイルは作成順に保存され、印刷コマンドの到着順に、先頭の印刷イメージファイルが印刷された。
この場合、ケースXとケースYは両立する！

(ファイル作成順と印刷コマンド到着順が必ず同じと想定していた)

→★本来、以下のような処理になっていれば問題なかったのでは？

前提条件：

- *当該ファイルは申請者しか印刷できないようロックがかかる
- *システムにはタイムアウトの上限が設定されていた

問題のない処理内容：

- *タイムアウトになったファイルは、ロック解除ではなく、削除する。
- *印刷コマンドの到着後、申請者本人の確認をして、ロックを解除し、印刷する。
- *印刷コマンドの到着後、当該ファイルが削除されていれば、申請者にその旨のメッセージを伝える。

→★要するに

「当該ファイルは申請者しか印刷できないようロックがかかる」という仕様なのに、でたらめな実装になっていたと思われる。

→★また、通信回線経由なので、

複数のユーザの入力操作に基づき、印刷イメージファイルが作成される順番とその複数のユーザの印刷操作に基づく印刷コマンドの到着順が必ずしも一致しないという基本がわかっていない担当者が実装した。
さらに、テスト担当者も、到着順が前後するテストケースを作成しなかったと思われる。

以上