

平成 28 年 4 月 27 日
地方公共団体情報システム機構

カード管理システムの中継サーバに生じた障害原因の特定と対応について

本年 1 月中旬以降に当機構のカード管理システムに障害が生じたことにより、各市区町村におけるマイナンバーカードの交付事務に影響を与える事象が発生しました。本事象により、住民の皆様及び地方公共団体の皆様に、多大なるご迷惑をおかけしましたことを、改めて深くお詫び申し上げます。

この度、発生以降調査を進めてきたカード管理システム内の中継サーバの障害の根本原因を特定し、その対応策を講じましたので下記のとおりお知らせいたします。

記

1 事象

中継サーバ内の障害により、市区町村の統合端末からカード管理システムに接続できない状態となった。

(障害発生日時)

- ・平成 28 年 1 月 13 日 (水) 11:40 頃 ~ 13:10 頃
- ・平成 28 年 1 月 18 日 (月) 15:40 頃 ~ 19:00 頃
- ・平成 28 年 1 月 19 日 (火) 8:30 頃 ~ 8:50 頃
- ・平成 28 年 1 月 21 日 (木) 18:40 頃 ~ 19:00 頃
- ・平成 28 年 1 月 22 日 (金) 9:40 頃 ~ 9:50 頃
- ・平成 28 年 1 月 25 日 (月) 10:45 頃 ~ 11:25 頃

2 原因

原因 1

(説明) CPU が耐タンパ装置からのデータを各コアで処理している最中に、ハードウェア監視ツールから CPU への状態確認が行われ、同一コアで処理されると、CPU ではハードウェア監視ツールへの対応のみが行われ、CPU での処理結果が耐タンパ装置へ返答されず、その結果、業務アプリケーション側から見て、耐タンパ装置が無応答になってしまう。

原因 2

(説明) 通常、業務アプリケーションがデータ処理を開始する際に、メモリ内に作業領域を確保してから処理を行う。ところが、業務アプリケーションがデータ処理を開始する前に Windows からタイムアウトの通知を受け取った場合、終了処理が実行され、メモリ内に作業領域を確保していないにも関わらず存在しない作業領域を解放しようとして、業務アプリケーションが異常終了する。

3 対応策

原因1への対応

- ・CPUがデータ処理中にハードウェア監視ツールからの状態確認が行われても、正しく処理(CPUでのデータ処理結果を耐タンパ装置へ返答)するように修正。
- ・中継サーバに対し4/15(1台)、4/22(残り3台)に修正を実施。

原因2への対応

- ・メモリの確保状況を確認した上で、終了処理が実行されるよう、中継サーバの業務アプリケーションを修正。
- ・中継サーバに対し4/15(1台)、4/22(残り3台)に修正を実施。

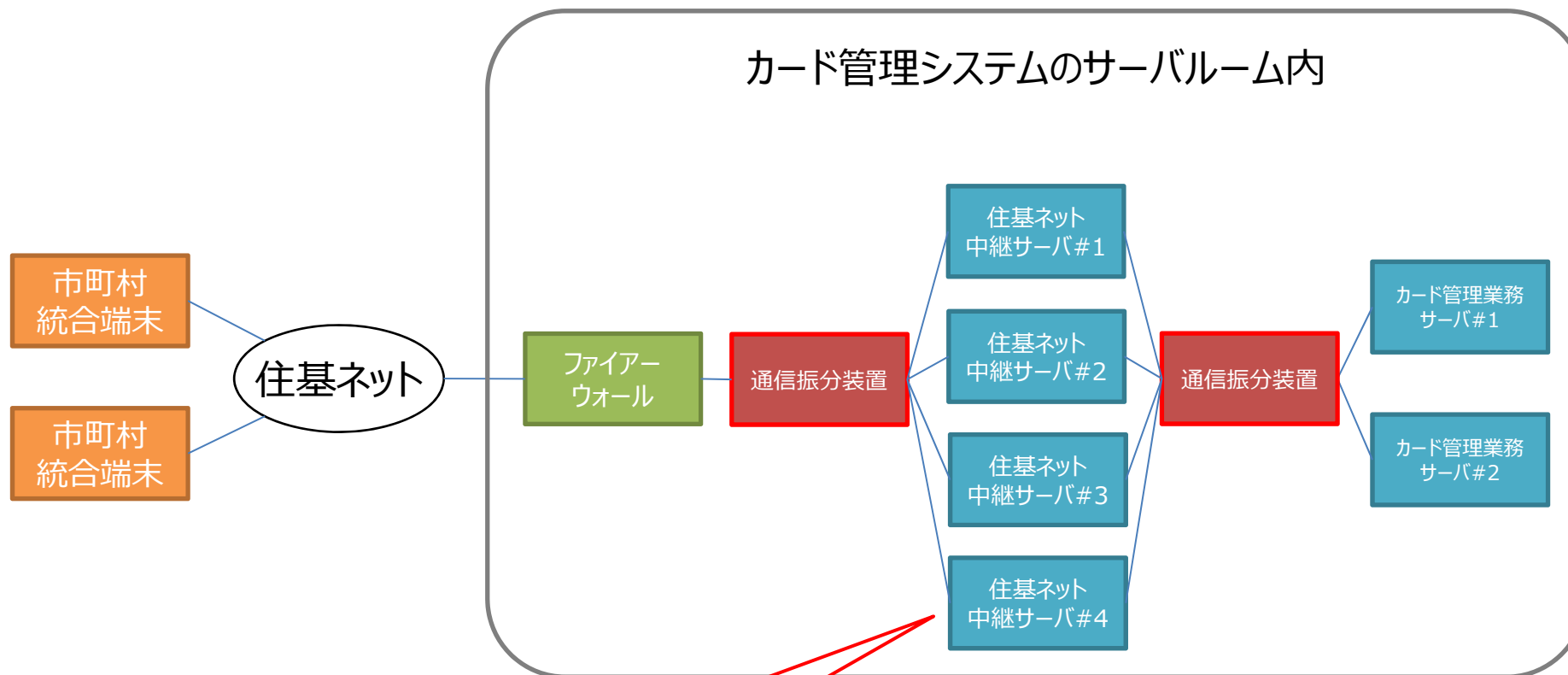
連絡先

地方公共団体情報システム機構

情報化支援戦略部 企画担当

電話：03-5214-3453

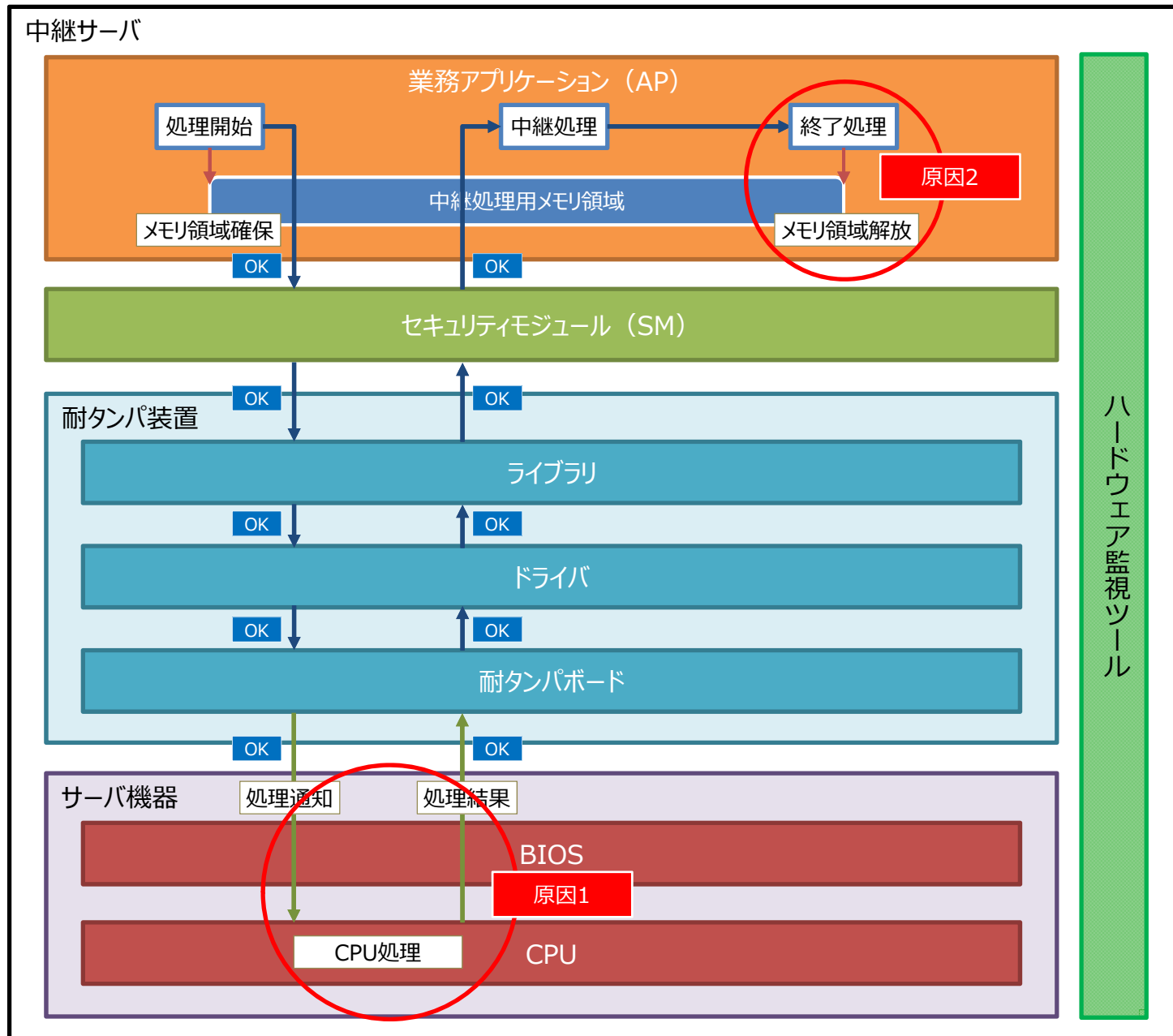
○全体図・障害発生日時



<中継サーバで障害が発生>

- ・平成28年1月13日(水) 11:40頃～13:10頃
- ・平成28年1月18日(月) 15:40頃～19:00頃
- ・平成28年1月19日(火) 8:30頃～8:50頃
- ・平成28年1月21日(木) 18:40頃～19:00頃
- ・平成28年1月22日(金) 9:40頃～9:50頃
- ・平成28年1月25日(月) 10:45頃～11:25頃

○中継サーバの処理の流れと原因箇所



○中継サーバ障害の原因 1 と対応策

説明

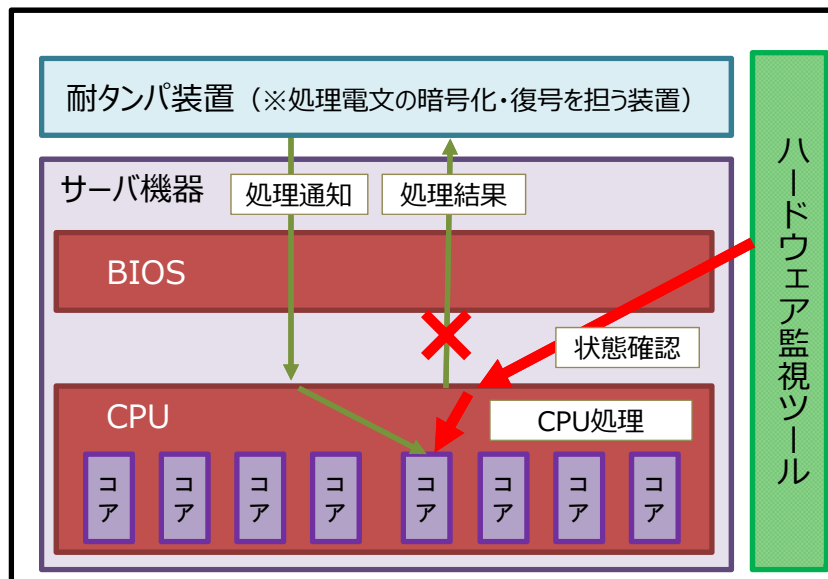
CPUが耐タンパ装置からのデータを各コアで処理している最中に、ハードウェア監視ツールからCPUへの状態確認が行われ、同一コアで処理されると、CPUではハードウェア監視ツールへの対応のみが行われ、CPUでの処理結果が耐タンパ装置へ返答されず、その結果、業務アプリケーション側から見て、耐タンパ装置が無応答になってしまう。



対応策

- CPUがデータ処理中にハードウェア監視ツールからの状態確認が行われても、正しく処理（CPUでのデータ処理結果を耐タンパ装置へ返答）するようにCPUの設定を修正。
- 中継サーバに対し4/15（1台）、4/22（残り3台）に修正を実施。

(中継サーバ内における原因 1 の発生のイメージ)



ハードウェア監視ツール :

対象の機器に定期的に通信を行い、機器の状態を監視するプログラム。

BIOS : (Basic Input/Output System)

接続されている機器や通信の管理を行うプログラム

CPU :

プログラムやデータの処理を行う機器

○中継サーバ障害の原因 2 と対応策

説明

・通常、業務アプリケーションがデータ処理を開始する際に、メモリ内に作業領域を確保してから処理を行う。ところが、業務アプリケーションがデータ処理を開始する前にWindowsからタイムアウトの通知を受け取った場合、終了処理が実行され、メモリ内に作業領域を確保していないにも関わらず存在しない作業領域を解放しようとして、業務アプリケーションが異常終了する。

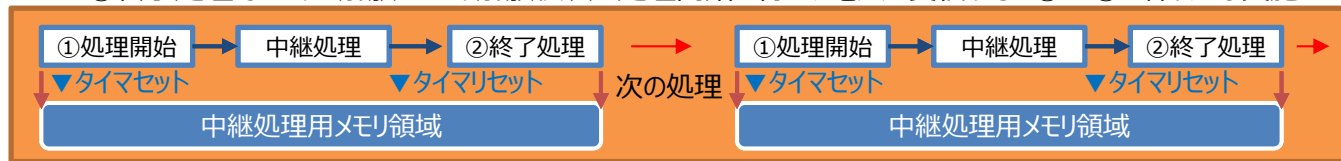


対応策

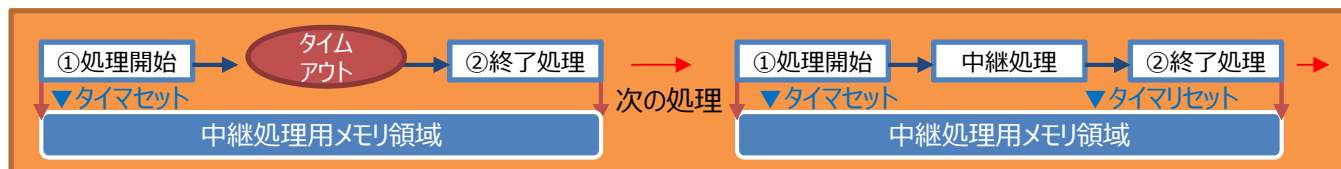
・メモリの確保状況を確認した上で、終了処理が実行されるよう、中継サーバの業務アプリケーションを修正。
 ・中継サーバに対し4/15（1台）、4/22（残り3台）に修正を実施。

（業務アプリケーションにおける通常の処理の流れと原因 2 の発生のイメージ）

通常の処理 ①処理開始時にメモリ領域を確保しタイマをセット。中継処理の完了時にタイマをリセット。
 ②終了処理でメモリを解放。メモリ解放後次の処理開始を待ち、電文を受信すると①～②を繰り返し実施。



タイムアウト処理 ①処理開始にタイマを設定。一定時間内に中継処理が完了しない場合、タイマに基づきWindowsからタイムアウトが通知
 ②終了処理が実行されメモリを解放する。



事象発生時処理 ①タイムアウト通知とタイマリセットが同時に発生した場合、Windowsの仕様上、タイマリセットが行われない場合がある。
 ②この場合、タイムアウト通知が保持されたままとなり、アプリケーションがデータ処理開始前にタイムアウト通知を受け取る。
 ※ タイマリセットが行われれば、タイムアウト通知が保持されることはない。

