尼崎市長　稲村　和美　殿

尼崎市 USB メモリ―紛失事案に関する調査報告書

令和 4 年 11 月 28 日

尼崎市 USB メモリ―紛失事案調査委員会

第 1　調査委員会の設置と構成

BIPROGY 株式会社(旧商号は日本ユニシス株式会社。以下、現旧商号を区別せずに「B社」という。)の無断再々委託先従業員が住民税非課税世帯等への臨時特別給付金対応業務における全尼崎市民の個人データを含む USB メモリを紛失する事案(以下「本件紛失事案」または「本件事案」という。）が発生したことを踏まえ、その事実関係や原因および対処等を検証して今後の再発防止策等を調査審議するために、地方自治法 138 条の 4 第 3 項の付属機関として、本年（令和 4 年）7 月 1 日付けで、下記 3 名の委員からなる尼崎市 USB メモリー紛失事案調査委員会（以下「当委員会」という。）が設置された。下記委員は、いずれも当委員会が設置されるより以前に本件事案との利害関係を含む関わりを一切持ったことはなく、客観的かつ公正な立場から調査に当たった。

小林 孝史（当委員会委員長）	関西大学総合情報学部准教授
櫻庭 信之（当委員会委員・同委員長職務代理）	弁護士
大高 利夫（当委員会委員）	藤沢市総務部情報システム課

第 2　諮問調査事項

尼崎市長は、本年 7 月 4 日、調査審議事項として当委員会に下記事項を諮問した。

(1) 本件事案への対処について
(2) 原因の検証について
(3) 再発防止策に関する事項について

本調査報告書では、下記第 4 および第 5 で本件事案に関して認められた事実関係を摘示するとともに原因を検証し(上記(2))、下記第 5 および第 7 で再発防止策(上記(3))を述べる。最後に、調査の過程で判明した諸問題も併せ本件事案を踏まえた対処（上記(1)）として第 7 で尼崎市に対し提言する。

第 3　調査の概要

当調査委員会は下記 1 の調査補助者等を調査のため補強し下記 2 以下の方法で調査を遂行した。本調査報告書は、調査の目的に必要な範囲に限定して報告するものであり、機密情報やプライバシーの保護その他の観点から一部の開示を差し控えている。

1　調査補助者

当委員会は、小坂谷聡（弁護士)、クオリティネット株式会社、上町和生(尼崎市職員)に調査の補助をさせた。このうちクオリティネット株式会社(以下「補助調査機関」という。)

は、デジタルフォレンジック調査を実施した。紛失・発見にかかる後述の「012」「013」のUSB メモリ 2 本に関しては、同 USB メモリを製造したメーカーである株式会社アイ・オー・データ機器(以下「アイ・オー・データ」という。)が下記第 5-8 の解析・検証を行った。同社による解析・検証には浦口康也(株式会社くまなんピーシーネット)が立ち会った。

2　調査方法

当委員会委員および調査補助者は、本件紛失事案および周辺ないし背景事実を確認するため、尼崎市職員ら、B 社役員・従業員、尼崎市臨時特別給付金対応業務に関する B 社の再委託先・同再々委託先の各役員・従業員、コールセンター関係者等をヒアリングし、必要に応じて関連資料の提供を受けた。

補助調査機関は、関連する重要証拠が散逸・改変されず効率的に調査を遂行する見地から、当委員会設置直後に速やかに調査準備に着手し、実地でのフォレンジック調査に先行して関係する市職員らに予備ヒアリングを行ったうえで実地調査を実行した。実地のフォレンジック調査では、当委員会委員、調査補助者、市職員の立ち会いのもと、尼崎市から関連機器の提供を任意に受け、市の給付金サーバに関しては同サーバ稼働の状態のまま、外観、使用態様、区画の状況、施錠の有無、監視カメラの設置、バックアップ等々の諸状況を調べた。B 社の所有または管理にかかる機器や USB メモリに関しては、尼崎市が B 社の同意を得て、尼崎市を通じて任意に当委員会に提供を受けたうえで、庁舎内のネットワークに一切接続されない、尼崎市による物理的管理下の隔離空間に機器等を集約し、証拠の収集・保全を実施した。コールセンターでも、同管理者の協力を得て同意を得た範囲内で同様に現地で稼働中のまま、外観、使用態様、区画の状況、施錠有無、監視カメラの設置、バックアップ等の状況を調査し、併せて証拠の保全を実施した。以上の対象機器はいずれもパスワードその他の認証情報の入力を要するアクセス制御がかかっていたため、使用者本人ないし管理者に入力させたり、状況によりこれらの者から必要情報の提供を任意に受けて、市職員、委員もしくは調査補助者が代わって入力操作を行い、同意が得られた範囲で証拠の保全を実施した。

補助調査機関が実施したデジタルフォレンジック調査の概要は以下のとおりである。

(1)　調査対象機器

①　市政情報センター3 階サーバルーム内設置の給付金サーバ

②　本件紛失・発見にかかる USB メモリ「012」「013」。(「012」「013」は管理のため B 社が 2 本の USB メモリにそれぞれ貼付したラベル表示の番号)

③　市政情報センター3 階 B 社執務室内で本件事案発生直前まで使用されていた開発用デスクトップ PC、同じく同室内で使用されていたとされる開発用ノート PC

④　「012」「013」の USB メモリ 2 本を本年(令和 4 年)6 月 22 日未明に紛失した B 社再々委託先従業員(以下「A」という。)が上記 B 社執務室内で日常的に業務に使用していたとされるノート PC

⑤ 本年 6 月 21 日夕方上記 USB メモリに格納された尼崎市民個人データを移行・保存したコールセンターサーバ

⑥ 尼崎市の関係職員 6 名使用のメールデータ

⑦ 尼崎市が B 社に本件事案発生以前に貸与していた 12 本の USB メモリ(「001」～「010」、「177」、「179」のラベル表示があるもの。臨時特別給付金対応業務が開始する以前、「176」の USB メモリも B 社に貸与されていたが破損したため同業務では使用されていない。)および「011」の USB メモリ 1 本

(2) 調査項目

USB 接続履歴、外部デバイスのドライバーインストール履歴、メール通信履歴、イベントログ、各種レジストリ設定、プログラム実行履歴(Prefetch、AmCache、Shim Cache、UserAssist)、ファイル操作履歴(UsnJrnl、LNK ファイル、RecentDocs、JumpList、Shellbags)、ネットワーク接続履歴（有線・無線種別、インターネット利用有無、IP アドレス割当て等)、ブラウザ履歴、クラウドストレージ(Box)、暗号化(BitLocker)、ウイルス対策状況、ネットワーク関連情報(Remote Desktop Protocol、SRUM)、ごみ箱(Recycle Bin)、その他関連諸事項

(3) 使用ツール

EnCase Forensic、FTK (Forensic Tool Kit)、Magnet AXIOM、Forensic Falcon-NEO、Tableau TK8u、その他フォレンジックツール。「012」「013」の USB メモリ解析にはアイ・オー・データの開発用ツールを使用。

第 4　USB メモリ紛失・発見等の事実経緯

A 等に対するヒアリング結果その他関係証拠に基づき、以下の事実経過が認められた。

(1)　本年 6 月 22 日未明に USB メモリ 2 本を後に紛失した A が尼崎市の非課税世帯への臨時特別給付金対応の業務委託事業の会合に最初に出席したのは、今年 2 月頃であった。この会合の冒頭で、市職員 2 名と B 社従業員 2 名は自己紹介と名刺交換をした。B 社側で出席した A は、自分が B 社の再々委託先従業員であることを市側に明かすことができず、今日は名刺を持ってきていない、と述べて、市職員との名刺交換をしなかった。A は、市から B 社の従業員かと質問されても、再委託先・再々委託先の従業員であるとは言うなと上司から長年指導を受けてきたため、このときも言わなかった。この会合に出席した市職員 2 名は、A が初めて会う人であった。A は、B 社と別会社の従業員であるとは自己紹介せず、会合に一緒に出席した B 社職員 2 名も、A を別会社の従業員であると紹介しなかった。そのため、A は、この会合に出席した市職員 2 名は、自分を B 社従業員と誤解したと感じた。A はこのとき以降もこれ以前も、自身が B 社とは別会社（再々委託先）の従業員であると尼崎市職員に打ち明けたことは一度もなかった。

(2)　USB メモリを紛失する直前の市職員と B 社従業員の会合は今年 6 月 16 日に開かれ

た。この会合では、同月 22 日から臨時特別給付金の支給対象者に郵便の発送を開始し、その前日（21 日）データ更新を行う予定とし、ステータス状況、公用請求関連、現金書留、印刷関連・発送関連、ランディングページ・動画シナリオなどを話し合った。ただ、B 社側の出席者からも市職員からも、21 日の USB メモリの使用やデータの運搬方法の話は出なかった。データの複写・複製の話も 16 日の会合では出ず、B 社がその許可を市に申請をする話もなかった。この会合終了後の帰りがけ、一緒に会合に出席していた B 社従業員（本データ移行作業の主任）は A に、来週よろしく、と言って、同月 21 日に、市政情報センター3 階サーバルームの給付金サーバに格納された個人データを USB メモリにコピーしてコールセンターまで持って行くことを A に頼んだ。上記 B 社従業員は、同日、営業で本件の委託契約締結の担当部署の B 社従業員に宛てて、「今回も手伝って頂けますか?よろしくお願いします。」と 21 日 18 時からのコールセンターでのシステム導入作業への参加を依頼した。

(3)　6 月 21 日、A は市政情報センター3 階 B 社執務室に出勤して間もなくの午前 9 時過ぎ、B 社執務室に入って右手奥の隅にあるプラスチックの引出しの中から「008」の USB メモリを取り出し、同じく市政情報センター 3 階の廊下 1 本を隔てたサーバルームに管理カードを使って入り、同ルーム内にある給付金サーバに、管理番号「008」のラベルが貼られた USB メモリを挿して、尼崎市民の個人データ（ファイル名 ESB.bak（460,517 人分）とファイル名 ESBR4.bak（459,582 人分））を「008」の USB メモリにコピーした。サーバルーム内には普段オペレーターか誰かがいるが、このとき A がコピーした際は、サーバルーム内に人がいたかは A に記憶がない。A はサーバルームに入退室の際も、個人データを USB メモリにコピーする際も、誰にも声を掛けていない。A は市職員に USB メモリに給付金サーバの個人データをコピーすることを知らせることもしていない。A が 6 月 21 日に USB メモリを使って個人データのコピーをとったことを市職員が知ったのは、USB メモリの紛失が市に連絡が行って初めて知ったのではないかと A は想像しており、この点を当委員会が市職員に確認すると同様の回答があった。A はサーバルームで個人データを「008」の USB メモリにコピーし、その USB メモリを持って廊下を隔てた B 社執務室に移動し、同室内にある開発用デスクトップ PC に挿して上記 ESB.bak のファイルと ESBR4.bak のファイルを同 PC 内蔵の記憶装置に保存した。B 社執務室にある開発用 PC にはサーバルームの給付金サーバに格納された尼崎市民の個人データが保存されていたが、給付金サーバ保存の市民の個人データを B 社が開発用 PC に保存していることを B 社執務室で稼働する従業員らは知っているが、B 社は開発用 PC に上記個人データを保存することについて尼崎市から許可をとっていない。

(4)　6 月 21 日午前 9 時 30 分前後頃、A は、上記引出しから「012」「013」の USB メモリを取り出し、開発用デスクトップ PC に挿して ESB.bak のファイルと ESBR4.bak のファイルをこれら 2 本の USB メモリにコピーした。「012」「013」の 2 本の USB メモリに個人データをコピーしたのは、そのうち 1 本を副本とするためであった。A は、「012」「013」の 2

本の USB メモリだけでなく「008」の USB メモリも個人データを消去しないまま引出しに戻し、夕方まで別の仕事に従事した。これらの USB メモリは、6 月 21 日午前 9 時過ぎに給付金サーバから個人データをコピーする際、B 社執務室内の上記引出しから取り出して使用されたが、USB メモリには従前誰かが使用した際のデータが残ったままであったため、A は給付金サーバの個人データのコピーに USB メモリを使う直前にそれらのデータを消去した。「012」「013」の 2 本の USB メモリに A はパスワードを設定した。このパスワードは、本件の臨時特別給付金の委託業務に限らず、それよりだいぶ前から同じパスワードが尼崎市と B 社に使われていた。したがって、過去に市の委託業務に携わった B 社、B 社から再委託・再々委託を受けていた別会社の従業員らも知っているパスワードであった。

(5) 6 月 21 日正午前になって、16 日に B 社従業員がコールセンターでのシステム導入作業への参加を依頼した上記メールに対し、メールを受信していた B 社従業員から、「返信が遅くなりましたが、今日 17:50 に現地に行きます。手順書をご準備いただければ、現地で作業します。」との返信メールがあった。それに対し十数分後、データ移行作業の主任である上記 B 社従業員はお礼を述べたうえで、「帰りに軽く行きましょう!」と、コールセンターでの作業終了後飲みに行くことを誘うメールを送信した。

(6) A は、6 月 21 日市政情報センター内での作業が終わった後の夕方、上記引出しから「012」「013」の USB メモリを取り出し、それぞれ別々に透明のプラスチックケースに入れた状態で、カバンの内側にあるファスナーの付いたポケットに入れた。カバンは上部が大きく開いた革製の手提げカバンであったが、鍵のかかるカバンではなかった。USB メモリは封筒に入れて封印するなどもしなかった。USB メモリを入れた上記透明のプラスチックケースも両方とも鍵はかからなかった。A はこれら 2 本の USB メモリをカバンに入れ、市職員には何も告げずに 1 人で市政情報センターを出た。立花駅まで徒歩で行き、そこから JR で大阪駅に電車で移動し、地下鉄に乗り換え、17 時 40 分頃目的の駅に着いた。このように市政情報センターからコールセンターまでの間、A は USB メモリの入ったカバンを持って一人で移動した。17 時 50 分頃、A は、メールのやり取りがあった上記 B 社従業員 2 名のほか別の再委託先従業員 1 名と待合せ場所で合流し、4 人が揃った時点でコールセンターの担当者に連絡しコールセンターに入った。コールセンターに入ってすぐ、A ないしもう一人の再委託先従業員が 2 本のうちの 1 本の USB メモリを同所のサーバに挿して ESB.bak と ESBR4.bak の 2 つのファイルを同サーバにコピーした。データの SQL データベースへの展開は A ではない再委託先従業員が行った。その後 4 人は、コールセンターの各デスクに置かれた 25 台の端末に給付金のプログラムをインストールするなどの作業を行った。

(7) コールセンターでの作業は 19 時前後に終了するとそのまま 4 人は同所近くの飲食店に入って会食した。会食中、A ではない再委託先従業員が途中で帰り、A と B 社従業員 2 名は閉店の 23 時前まで会食した。このとき A はアルコールを大量に飲んでいた。店を出て 3 人は分かれたが、A は電車に乗らなかった。その後翌 22 日午前 3 時頃、目が覚め、A は知らない場所で寝ていて、USB メモリを入れたカバンがないことに気が付いた。カバンに財

布や携帯が入っていたため、A はタクシーに乗ることができず、歩いて午前 8 時半頃自宅に帰ったが、A は帰路の記憶が定かでなかった。A は、帰宅後、市政情報センター3 階 B 社執務室の責任者に同日（6 月 22 日）は有給休暇をとる旨連絡した。その後すぐコールセンター近くの駅まで電車で行き、交番で、カバンが遺失物で届いていないかを尋ねたが届出はなく、USB メモリには触れずにカバンの遺失物届を交番に出した。A は 1 人でカバンを探し回ったが見つからず、22 日 14 時頃、B 社執務室の責任者に再度電話して USB メモリの紛失を伝えた。その後いったん自宅に戻り、20 時頃、市政情報センターへ行き、尼崎市職員らに USB メモリ紛失の経緯を説明した。23 日午前中、市政情報センターで引き続き事情を説明した。A は、同日午後 B 社に行き、B 社の担当者から事情を聞かれた。23 日 20 時過ぎの帰宅途中、警察から A に電話があり、遺失物届を出したのが、報道されている USB 紛失の件かと尋ねられ、そうです、と答えると、翌 24 日警察が A と一緒に探すことになった。翌 24 日、朝から、警察の車両に乗せてもらって一緒に探した。A の当初の認識に従って車で往復して探しても違和感があったことから、警察から A は他の場所の可能性を問われ、21 日夜店から出て 2 人と分かれたあたりから自宅方面へ向かうと当日通った記憶のある場所を通りかかり、車を降りて警察と一緒に近くを探していると見覚えのある建物があった。寝ていた場所を思い出し、その場所の様子を記憶に基づいて警察に具体的に話すと、知っている警察官がいて A が言った場所を教えた。その場所に行ってみると A の記憶とおりで、その一角にカバンが逆さまになって半分くらい刺さった形で見つかった。発見したのは 6 月 24 日午前 11 時半頃である。

(8)　A は警察とともに、発見されたカバンを持って同日 13 時過ぎに警察へ行き、カバンの中身を確認したところ、「012」「013」の 2 本の USB メモリが入っていて、A の財布も携帯もカバンに入ったままであった。B 社から従業員が警察に駆けつけたきたので、警察は、USB メモリの中身を確かめるようその従業員に指示した。B 社従業員が持参したノート PC に 2 本の USB メモリを挿し込み、A がパスワードを入力し、ファイルを調べると、ESB.bak と ESBR4.bak の 2 つファイルがあった。SQL データベースのサーバがなかったためファイルの中身はこのとき見ることができなかったが、エクスプローラーで表示された作成日は、21 日のコピー時に A が目視した 6 月 21 日午前 1 時のままであった。午前 1 時とは、毎日 1 回給付金サーバのバックアップがとられる時刻である。発見された USB メモリ 2 本は、その後、尼崎市職員に渡された。

第 5　問題の所在と対策

1　市政情報センター3 階のサーバルーム内の給付金サーバからの個人データ移行の問題

(1) サーバルームの入退室

市政情報センターの入退館には、尼崎市長宛てに入退室管理カード貸与依頼書を提出して、市から入退館カードを借り受け、同カードを使用することが必要となる。本件で問題の

尼崎市民の個人データは、市政情報センター3 階の電子計算機室（以下「サーバルーム」という。）内に設置されている給付金サーバ内に格納され管理されている。サーバルームへの入退室にも同じカードを使用するが、市政情報センターへの入退館許可だけでなく、サーバルームへの入退室も登録された登録情報との照合により許可されたカードを使用する場合に限りサーバルームへの入退室が可能となる。今回の USB メモリの紛失に関連しては、B 社関西支社業務執行役員支社長名義（同社社印の印影がある）で尼崎市長宛てに本年 4 月 1 日付け入退室管理カード貸与依頼書が提出されている。同貸与依頼書には「BIPROGY 株式会社カード使用者一覧表（令和 4 年度継続申請）」の標題の下、23 人の氏名が被貸与者として記載されており、うち、サーバルームへの入退室のために管理カード貸与申請がなされたのは 19 名であった（「許可区分」が 6 および 10 の申請者）。しかし、上記管理カード使用者一覧表に記載された 19 名中 10 名は B 社以外の者の氏名であり、無断再委託先・再々委託先の従業員であった。A と同じ所属会社（無断再々委託先）の従業員も、同管理カード使用者一覧表には A を含め少なくとも 2 名が含まれていた。尼崎市は B 社関西支社長からの上記申請を信頼し、真実は無断の再委託先、無断の再々委託先の従業員であったにもかかわらず、カード使用者はいずれも B 社従業員であると誤認し、サーバルームへの入退室の可能な管理カードを B 社に貸与した。3 階 B 社執務室内で稼働する者は、再委託先や再々委託先の従業員に限らず全員サーバルームに入室可能な管理カードを所持していた。

本件事案発生前、3 階 B 社執務室内で稼働する B 社の従業員全員が、同室内で稼働する無断再委託先および無断再々委託先の従業員らが B 社従業員ではないことを認識していた。一方、B 社の役員が無断の再委託・再々委託を知っていたことを示す証拠は、当委員会は現時点までの調査では入手していない。したがって、B 社関西支社長が自身の名義の入退室管理カード貸与依頼書添付「BIPROGY 株式会社カード使用者一覧表」記載の従業員に B 社以外の者が含まれていることを認識しながら市長に対し管理カードの貸与依頼書を提出していたとまでは認められない。一方、無断再委託先および無断再々委託先の従業員でありながら、入退室管理カードを取得してしまうことについて B 社内のいずれかの者は知りながら、関西支社長名義の入退室管理カード貸与依頼書の作成ないし市への同提出の作業を進めていた、あるいはこれらの作業に関与していたことが推認される。

(2) 給付金サーバ格納の個人データへのアクセス

サーバルームに入室した者が、市民の個人データが格納された給付金サーバにアクセスするには同サーバの管理者 ID とパスワードの入力で足りた。接続する USB メモリには特に制限がなく、登録もなく、どのような USB メモリでも差し込めばサーバ側に接続が認識され、特に技術的に解放の措置をとる必要もなかった。

(3) 監視カメラ

サーバルーム内に監視カメラは 2 台設置されているがカメラの死角ができており、十分

な台数がサーバルーム内に設置されていなかった。

(4) ログ管理

給付金サーバにログ保存機能が装備されていたがデフォルトの 20MB であり、そのうえ後発で接続された USB メモリ等の媒体の接続ログによって先行の古い接続ログが上書きされて証跡が残らない場合があった。ログのバックアップも取得されていない。ログの保存期間は保存容量次第であり、たとえば 1 年などのように保存期間が一定しているわけではなかった。

(5) 給付金サーバの作業記録

誰が、いつ、何の目的で、どの記録媒体を給付金サーバに接続し、何を行ったか等について、作業記録等はつけられていない。

以上を踏まえた問題と対策は次のとおりである。

(a) サーバルームへの入退室管理カードの貸与

サーバルーム入室の管理カードは、尼崎市民の個人データという極めて重要な情報資産へのアクセスにつながるものであり、管理カード貸与の可否は厳格に審査されるべきであった。ところが、B 社関西支社長名義の貸与依頼書のカード使用者一覧表に氏名が記載されるだけで、再委託・再々委託が承諾されていない B 社ではない外部者もサーバルームへの入退室管理カードを尼崎市から手に入れることができた。加えて、令和 3 年 2 月にはサーバルーム内にそれまで設置されていたホストコンピュータが完全撤去されたことから、必ずしもサーバルームへの入室が必要ではない B 社従業員までも上記カード使用者一覧表への氏名記載によってサーバルームへの入退室管理カードを取得でき、最小特権の原則を逸脱していた。このように管理カード貸与依頼書ないしカード使用者一覧表には尼崎市民の重要な個人データを危険にさらしうる脆弱性を孕んでいた。貸与依頼書は B 社関西支社長名義で作成され、B 社社印が押されていながら、無断再委託・再々委託先の従業員がチェックされずに記載されており、これをチェックするだけの十分な体制が B 社内にあったとは思われない。今後市政情報センターに出入りする外部業者には、特にサーバルームへの入退室資格に関してチェックを厳密にして入退室管理カード貸与依頼書に氏名を記載させることが求められる。他方、尼崎市も、サーバルームは全尼崎市民の個人データを管理している厳格な管理を必要とするエリアであり、管理カードはそのエリアへの入室を認めるものなのであるから、貸与依頼があっても依頼書の記載をそのまま信用することなく、確実な裏付けがない貸与依頼は不許可とする方針を採るべきである。本件の B 社の場合、後述するように意図的組織的に他社の者を自社の従業員に見せかけて尼崎市と接することをさせており、顔写真付き社員証原本を提示させるだけではなく、本人の運転免許証、パスポート、マイナンバーカードなど顔写真付き身分証明書も併せて提示させ、かつ、それらのコピーを市側は

保管し参照する。また、入退室管理カードを一旦交付してしまうと、繰り返し使用されることから、最初の貸与時は審査を特に厳格にするのが適当である。本人面談の実施を検討すべきで、連日大量に貸与するような性質のものでもないから、本人面談を行うことの市側の負担よりも、無資格の者がサーバルームを出入りするリスクの方が重視されるべきである。市が面談する際も、無資格者に事前準備がなされてしまわないよう、承諾事業者に所属する真の適格者のみが答えられる質問を考案して行う。ただ、個人情報管理の重要性に鑑み、他に、入退室管理カード貸与の適否を厳格に判断しうる手法があれば適宜検討し実践する。

(b) サーバルームへの入室および給付金サーバ格納の個人データへのアクセス方法

本件事案直後から尼崎市はサーバルームに業者が単独で入室することを禁じ、市職員が帯同しなければ入室できない措置を執っている。併せて、サーバルームに入室する際には業者および帯同する市職員がそれぞれ入退室管理カードを使用することに加え、市職員の生体認証（静脈）を導入済みである。サーバルームに入室した後、給付金サーバ格納のデータにアクセスするには、現在 ID とパスワードを入力して登録情報との照合によりログインして行っている。この場合、サーバルームに帯同した市職員は、サーバルーム内には入るものの、給付金サーバに対する安全確保への寄与は直接的ではない。全尼崎市民 46 万人余りの個人データを格納する給付金サーバはいわば尼崎市の情報管理の心臓部ともいうべき部分であり、万全の安全措置を講じる観点から二人制御を図るのが適当である。すなわち、給付金サーバにログインして個人データに直接アクセスするには、業者による給付金サーバに対する認証だけではなく、帯同した市職員も同人の生体認証による給付金サーバに対する認証を重ねて実施し、これによって給付金サーバ管理者側からのチェック機能を効かせることで外部業者の濫用を抑止すると同時に、市職員および作業者に安全性を確保すべき十分な自覚を持たせる。また USB メモリ等記録媒体をサーバに接続する場合も接続を当然に認識するシステムの使用は止め、管理権者が解除の手続をとった場合に限り、記録媒体がサーバに認識されるシステムに切り替え、管理権者の事前許可なく記録媒体の接続が技術的に不可能なものに今後はすべきである。

(c) スマートフォン等の持込み禁止

本件事案発生後尼崎市はサーバルームには業者がスマートフォン等を持ち込めないよう、入室前に市職員がスマートフォン等の私物を取り上げ、サーバルーム外のロッカーに施錠して保管したうえで、業者を入室させるようにしている。市職員がスマートフォン等を持ち込む場合も個人情報は危険に晒されるため、市職員も同様にサーバルームには持ち込ませないようにし、持ち込む必要のある特段の事情がある場合には情報政策課にその理由を付して事前に申請し、許可を得た場合に限り、持ち込みが可能とする。情報政策課の職員がスマートフォンを持ち込まなければならない場合には、情報政策課課長に対し上記事前申請をし、情報政策課課長が同申請をする必要がある場合には行政法務部長に事前申請する。スマートフォンに限らず、現在、メガネ型カメラなどのウェアラブル端末なども個人情報に対する脅威となっており、帯同する市職員や情報政策課はこれらの脅威にも常時注意すべき

である。後述のセキュリティ情報のミーティング研修などの機会を含め、随時情報交換ないし情報共有し、対策を継続的にアップデートする。

(d) 監視カメラ

現状のサーバルームの監視カメラは不十分であり、早急に適切な位置・角度で必要な台数の監視カメラを設置すべきである。録画データは上書きによってインシデントの録画再生ができない事態が起こることがないよう、デフォルト装備の録画容量だけでなく、できるだけ長期の録画データを保存できる措置をとる。

(e) ログ管理

後行のログによっても先行ログが上書きされないようログ保存機能の全面刷新を行う。給付金サーバのログ保存容量はデフォルトで運用されてきており、このままではインシデントが発生した際ログが十分保存できるか不確実である。今回の件を踏まえ、ログの十分な保存容量を確保し、イベントの上書きもされず、アーカイブや外部保存などによって、ログ保存期間を可能な限り長期とすべきである。ログは意図的な消去も可能であるため、ログの冗長化を図るなど、不正対策も行う。

(f) 給付金サーバの作業記録

USB メモリ等の記録媒体による給付金サーバへのデータ移行や給付金サーバからのデータ移行の際、これらの作業記録は義務付けられていなかったが、今後は誰が、いつ（入室時刻)、何の目的で、いつまで（退室予定時刻)、どの記録媒体を使って何を行うか等を作業者自身に記録を付けさせ、担当部署に確認させることが必要である。これらをタイムリーに毎回記録させることにより証拠を残し、担当部署にチェックさせ、同時に作業者にも市民の大切なデータを扱っていることをその都度自覚させる。タイムリーにその都度記録しない場合（例：後日まとめて記録するなど）には、受託者および当該作業者に相当なペナルティを科すなどしてルールを厳守させる。この手続の履践が困難な例外的な状況下ではその状況でなしうる範囲で入室情報を記録し、あるいは担当部署に連絡し、その後可及的速やかに記録の補充を追完する。

2　市政情報センター施設内における USB メモリ等の管理状況

(1) 市側の管理状況

情報資産分類は、尼崎市情報セキュリティ対策基準（令和２年４月改定。以下「セキュリティ対策基準」という。)第３章１には情報資産の分類として下記のとおり定められている。

記

情報資産分類１：特定個人情報を含む情報資産

情報資産分類２：個人情報ならびに、漏洩または破壊等の脅威にさらされることにより行政事務に重大な影響を及ぼす情報を含む情報資産

情報資産分類３：それ以外の情報資産

情報資産は上記のように分類され、必要に応じ取扱い制限を行うべきものとされていたが、本件事案発生以前は市職員が建物内で USB メモリによりデータを物理移動させる場合、情報資産分類 1 ～3 は区分されることなく情報資産が扱われていた。情報資産分類 3 のデータの物理移動でもパスワード認証や暗号化などのセキュリティ機能を装備した USB メモリを平時より使用していたこと、情報政策課が USB メモリ全本を管理し、同課からの USB メモリの持出し日時および実返却日時、使用 USB メモリの特定、当該 USB メモリの使用者名をその都度記録して管理していたことが認められる。しかし他方、USB メモリの使用目的、データの移動元および移動先、データの物理移動終了直後の USB メモリの保存データ消去確認等は記録されていなかった。直線距離にして約 250m の市政情報センターと本庁舎との間も USB メモリに保存してデータ移動する際は、市政情報センター施設内での上記のデータ物理移動と同じやり方をしていた。

(2) B 社の管理状況

B 社が市政情報センター施設内で使用する USB メモリは、B 社が同センター3 階 B 社執務室内窓側の入口から見て右手奥の隅のプラスチックケースの鍵のかからない引出しの中に保管されていた。本件事案発生直前は同引出しの中に、市が購入して B 社に貸与した USB メモリが 12 本（うち「001」～「010」のラベル表示のある USB メモリ 10 本はセキュリティ機能付きであり、「177」「179」のラベル表示のある 2 本の USB メモリはセキュリティ機能が付いていないもの）、B 社が独自に調達した USB メモリが 3 本、その他に管理番号のラベルが貼られていない USB メモリが数本保管され、B 社執務室内で稼働する者たちは、これらの USB メモリを共同で使用していた（「177」「179」の USB メモリは、上記第 3-2(1)①・③～⑤の機器からは接続履歴は認められなかった。）。B 社が調達した 3 本の USB メモリにも管理番号「011」「012」「013」のラベルが貼られていて、本件事案で A が紛失した USB メモリはそのうちの「012」「013」の 2 本である。B 社執務室内で稼働する者が USB メモリを使用する際は引出しの中から自由に持ち出し、持ち出しの記録をつけることは一切なかった。そのため、誰が何のために持ち出したために引出しの中から USB メモリがなくなっているのかは、特にその旨の情報を共有していない限り実際に当該 USB メモリを使用している者以外は知り得なかった。持ち出した USB メモリの使用を終えた後、使用者本人は引出しの中に USB メモリを返却するが、返却したことの記録もつけることはなかった。B 社にはこれら USB メモリ使用の管理簿はなく、誰が、いつ、何の目的で、どのサーバからどのサーバに何のデータを物理移動させるのか、いつ戻したか、データ消去を行ったか等々を記録するものもなく、B 社従業員はもとより、無断再委託先、無断再々委託先の各従業員もこれら USB メモリの使用・借出しの事前または事後に届出や報告等をしておらず、チェックされることも一切なかった。そのため、保管場所の引出しの中の USB メモリの数が足りないとき、使用者以外の者は、誰かが USB メモリを持ち出していることはわかるものの、誰が何の用途で持ち出しているか、いつ戻されるのか、など特段の情報共有がなされ

ない限り知り得なかった。なお、当委員会が本年 7 月 21 日に 3 階 B 社執務室内を B 社の承諾を得て立ち入った際、上記の引出し内に、氏名表示のある複数のキーホルダーを入れたボックスと爪楊枝を 10 数本立てたホルダー掛けがあった。この点に関し、翌 22 日当委員会からの質問に対し、B 社従業員は、氏名表示のあるキーホルダーと上記ホルダー掛けは、本件事案発生当時を含めその前から引出しの中にあり使用していたとの趣旨を当委員会に説明したが、その後 B 社執務室内で稼働している他の従業員らに確認すると、これら氏名表示のあるキーホルダーも爪楊枝を使ったホルダー掛けも、少なくとも令和 2 年の特別定額給付金業務が始まって以降、本件事案発生までの間引出し内には存在しておらず、当委員会に対する上記説明は虚偽であることが判明した。B 社は尼崎市に対し、委託者尼崎市代表者尼崎市長と受託者 B 社関西支社執行役員支社長との間の令和 4 年 2 月 3 日付け業務委託契約（以下「委託契約」という。）5 条、同個人情報取扱特記事項 14 条およびデータ取扱特記事項 13 条に基づき、B 社の業務の処理状況につき必要な調査を受け、尼崎市からの求めに応じて報告し、調査または報告に協力すべき義務を負っていた。さらに、B 社関西支社長は、尼崎市長宛てに本年 4 月 1 日付けで誓約書を提出しており、誓約書では、「尼崎市が行う業務管理に係る立入検査に協力することとともに、誠実に契約を履行することを誓います」とあるほか、「①データを適正に取り扱うこと②データが漏えい、滅失又はき損される等の事故（略）を防止すること③データを（略）第三者に提供しないこと④データを複写又は複製しないこと⑤（略）⑥個人情報の保護及び情報セキュリティの重要性を従事者に教育すること」などを誓約していた。この誓約書には、「個人情報の保護及び情報セキュリティの重要性を深く認識し、誠実に職務を遂行することをここに確認します。」等々が記載された確認書が添付されており、上記説明をした者や A など B 社執務室内で稼動する者らの記名捺印がある。これらの義務、誓約、確認は、尼崎市に対し事実を報告し協力することを前提とするものであり、B 社従業員の上記の虚偽説明は協力等の義務に反する。

また、B 社執務室内の上記引出しの中に置かれていた各 USB メモリは、必ずしも保存された個人データが消去された状態で保管されていたわけではなかった。直前の作業で保存されたデータは USB メモリ内に残されたままの状態で、B 社執務室内で稼働する者が USB メモリを使用する際に初めて先行保存のデータを消去することがしばしばあった。事実、A が本年 6 月 21 日午前 9 時過ぎに給付金サーバから個人データを USB メモリにコピーする際も、USB メモリに残っていた従前の別データを消去したうえで、個人データの保存を行っている。B 社執務室内で稼働する者らがデータのやり取り終了の都度 USB メモリの保存データを消去する運用は確立しておらず、鍵のかからない引出しの中にデータが保存されたままの USB メモリが置かれていた。このような運用は、本件事案発生前 B 社の誰も注意したり、運用を改めるよう促すことはなかった。USB メモリの管理や消去等について B 社は点検することもなく、USB メモリのデータ消去や廃棄等について、事前・事後を問わず、届出や許可申請などを執務室内で稼働する者に促すこともなく、B 社執務室の責任者も、再委託先や再々委託先も、B 社執務室内で稼働する者に対し、注意や指示等をすることはなか

った。

USB メモリ保存データを直ちに消去することなく事後対応等の必要から一定期間データを消去しないままにする場合は一般にはある。しかしながら、今回問題なのは、全市民 46 万人分という尼崎市民にとって極めて重要な個人データである。これは分類 3 の扱いとは到底一緒くたにはできない情報資産である。USB メモリにセキュリティ機能が装備されていたとはいえ後述のとおりパスワードルールに不備もあり、特段の安全確保措置を講じる必要があったが、B 社はそうした措置をとっていない。個人データ消去の問題は更に下記 6 で論じる。

3　3 階 B 社執務室内の開発用 PC

市政情報センター3 階にはサーバルームと廊下を隔てて B 社執務室があり、同室内には、臨時特別給付金対応業務のためのいわゆる開発用 PC として、デスクトップ型 PC とノート PC があった。これらの PC がインターネットに接続されたことは確認されなかったが、USB メモリが頻繁に接続された形跡があった。執務室内で稼働する受託者（再委託先・再々委託先の従業員を含む）の従業員らは、USB メモリを使ってサーバルーム内の給付金サーバ格納の個人情報の実データをこれら開発用 PC 内蔵記憶装置に保存し、尼崎市民の個人情報実データを用いて開発を行っていた。開発用PC ではツール開発や動作検証などにある程度のボリュームのあるテスト用データが必要となることがあるとはいえ、たとえば疑似個人情報ジェネレータを用いれば、テスト目的を達しうるテスト用データを簡単に調達できた。開発環境で用いるテスト用データは実データである必然性は全くない。（必要上どうしても実データを用いらざるを得ない場合―疑似個人情報ジェネレータ生成のデータを用いてテスト目的を達し得ない状況は通常想定できないが－が万一仮にあったとしても、明示的に市の事前許可を得たうえで、安全性が十分確認された諸条件下、必要最小限の時間内かつ範囲内に限って行う例外的な場合に限るよう配慮すべきである。）また、B 社執務室内では、市民の個人情報を含む実データがシステム開発に用いられていただけでなく、下記のとおり複数のバージョンの大量の個人データが長期に同 PC 内に保持された状態のままであった。これら開発用 PC への USB メモリ等の外部記憶媒体の接続には、同執務室内で稼働している者たちが知っている ID とパスワードが求められているだけであり、他の技術的制約は特に実装されていなかった。本来サーバルーム内の給付金サーバのみで厳格に管理されるべき尼崎市民の個人データが、その隣の 3 階 B 社執務室内の PC 内に移され、同室で稼働する者であれば自由にアクセスできた状態に置かれ、他者が不在などの機会に乗じて私物 USB メモリにデータを複製して外部に持ち出すことも可能な状況にあった。開発用 PC はインターネットに接続されていない状態にあったとはいえ、物理的に情報漏えいが生じうる危険な環境が B 社執務室内に作られていたといわざるを得ない。テスト環境で実データを使用する問題については、本年 1 月 26 日、3 階 B 社執務室内で稼働する B 社従業員（同人はコールセンターにデータ移行をする当日、データ移行の主任で、同行する他の B 社

従業員に作業終了後飲みに行こうと誘った者）に宛てて、A は、「研修（注：ママ）用端末ですが、本番データを使用していいものなのでしょうか? NG なような気がします。。」と書いたメールを送って、個人データを使用するのを控えるよう進言している。それに対し、宛先の B 社従業員は、「本番データ大丈夫です。本番も本番データやし。」と返信した。このやりとりの CC には、B 社執務室内で稼働する他の従業員が入っているが、少なくともこのメール上では何も異議を唱えていない。A は、上記返信があったものの、実データの使用をやはり躊躇し、再度メールで、「とりあえず氏名の頭 1 文字だけ「尼」に変えておきましょうか。。」と再度進言した。宛先の B 社従業員は、「めんどうやなかったらそうしといて!」と再返信しただけであった。

(1) 開発用デスクトップ PC 内の個人情報データの残存状況(本年 1 月 27 日以降の例示)

ファイル名	個人情報件数	作成日時	ファイルパス
ESB.bak	460,481	2022/1/27 12:37	D:¥○○個人資料¥01_WORK¥02_開発¥03_2021 年度_非課税世帯給付金¥_temp¥ESB.bak
ESB.bak	460,481	2022/1/28 8:35	C:¥backup¥○○個人資料¥01_WORK¥02_開発¥03_2021 年度_非課税世帯給付金¥_temp¥ESB.bak
ESB.bak	460,488	2022/2/14 17:42	D:¥○○個人資料¥01_WORK¥02_開発¥03_2021 年度_非課税世帯給付金¥対応作業¥_temp¥ESB.bak
ESB.bak	460,488	2022/2/15 8:00	C:¥backup¥○○個人資料¥01_WORK¥02_開発¥03_2021 年度_非課税世帯給付金¥対応作業¥ESB.bak
ESB.bak	データ破損	2022/2/17 17:58	D:¥$RECYCLE.BIN¥S-1-5-21-3408464457-2532685637-1098198028-500¥ESB.bak
ESB.bak	460,488	2022/2/18 8:01	C:¥backup¥○○個人資料¥01_WORK¥02_開発¥03_2021 年度_非課税世帯給付金¥対応作業¥20220217¥_temp¥ESB.bak
ESB.bak	460,488	2022/2/18 18:02	D:¥○○個人資料¥01_WORK¥02_開発¥03_2021 年度_非課税世帯給付金¥対応作業¥_temp¥20220218¥log¥ESB.bak
ESB.bak	460,488	2022/2/21 8:56	C:¥backup¥○○個人資料¥01_WORK¥02_開発¥03_2021 年度_非課税世帯給付金¥対応作業¥20220218¥log¥ESB.bak
ESB.bak	460,488	2022/3/1 8:55	C:¥backup¥○○個人資料¥01_WORK¥02_開発¥03_2021 年度_非課税世帯給付金¥対応作業¥_temp¥ESB.bak
ESB.bak	460,488	2022/4/13 9:18	D:¥○○個人資料¥01_WORK¥02_開発¥03_2021 年度_非課税世帯給付金¥対応作業¥20220218¥log¥ESB.bak
ESB.bak	460,488	2022/4/14 9:03	C:¥backup¥○○個人資料¥01_WORK¥02_開発¥03_2021 年度_非課税世帯給付金¥対応作業¥_temp¥20220218¥log¥ESB.bak
ESB.bak	460,517	2022/6/21 9:26	D:¥○○個人資料¥01_WORK¥02_開発¥05_2022 年度_非課税世帯給付金¥20220621¥ESB.bak
ESBR4.bak	459,582	2022/6/21 9:27	D:¥○○個人資料¥01_WORK¥02_開発¥05_2022 年度_非課税世帯給付金¥20220621¥ESBR4.bak
ESB.bak	460,517	2022/6/23 8:35	C:¥backup¥○○個人資料¥01_WORK¥02_開発¥05_2022 年度_非課税世帯給付金¥20220621¥ESB.bak
ESBR4.bak	459,582	2022/6/23 8:35	C:¥backup¥○○個人資料¥01_WORK¥02_開発¥05_2022 年度_非課税世帯給付金¥20220621¥ESBR4.bak

(2) 開発用ノート PC 内の個人情報データの残存状況（本年 2 月 1 日以降の例示。）

ファイル名	個人情報件数	作成日時	ファイルパス
ESB.bak	データ破損	2022/2/1 9:01	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak
ESB.bak	データ破損	2022/2/17 1:00	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak
ESB.bak	460,488	2022/2/18 1:00	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak

ESB.bak	データ破損	2022/2/21 1:00	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak
ESB.bak	460,488	2022/2/24 1:00	C:¥Users¥CPAdministrator¥Desktop¥temp¥ESB¥ESB.bak
ESB.bak	460,489	2022/3/1 8:52	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak
ESB.bak	460,489	2022/3/2 15:27	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak
ESB.bak	460,489	2022/3/3 13:35	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak
ESB.bak	460,489	2022/3/3 13:57	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak
ESB.bak	データ破損	2022/3/4 9:36	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak
ESB.bak	460,493	2022/3/4 9:36	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak
ESB.bak	460,494	2022/3/4 9:36	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak
ESB.bak	460,497	2022/3/4 9:36	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak
ESB.bak	460,498	2022/3/17 9:30	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak
ESB.bak	データ破損	2022/3/22 9:26	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak
ESB.bak	460,499	2022/3/22 9:26	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak
ESB.bak	460,500	2022/3/22 9:26	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak
ESB.bak	460,500	2022/3/30 9:18	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak
ESB.bak	460,500	2022/3/31 9:20	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak
ESB.bak	データ破損	2022/4/1 9:22	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak
ESB.bak	460,501	2022/4/1 9:22	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak
ESB.bak	460,501	2022/4/7 9:16	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak
ESB.bak	460,501	2022/4/8 9:16	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak
ESB.bak	460,501	2022/4/12 9:18	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak
ESB.bak	460,501	2022/4/13 9:21	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak
ESB.bak	460,502	2022/4/14 9:19	C:¥$RECYCLE.BIN¥S-1-5-21-4182482647-1544586502-4135119168-1001¥ESB.bak
ESB.bak	460,517	2022/6/27 13:17	C:¥Unisys¥work¥_temp¥ESB¥ESB.bak

4　パスワード

尼崎市と B 社との間で機密情報をやり取りする際、「amagasaki」「Amagasaki」「AMAGASAKI」や、これらに単に日付を追加するだけの、いわば辞書攻撃をするまでもなく誰でも簡単に思いついてクラックできるパスワード設定が複数みられた。当委員会は調査の過程でこれを認知し直ちにそのことを注意した。尼崎市と B 社との間でパスワードを共有してもパスワード共有の時間的範囲や対象範囲に明確な限定がなく、パスワードの情報管理に不十分さがみられた。具体的には市側や外部業者の人事異動や離退職にかかわらず固定され、案件から離れたり、別会社に転職した者でもパスワードを知ったままの状態が続いた。B 社従業員からは受託者側（再委託先・再々委託先を含む。）でパスワードを知る者は十数名にとどまるとの発言もあったが、口述によってパスワードを伝播させており、パ

スワードの変更もなされていないために、パスワードを知る者がどこまで拡散しているか確認が困難になっていた。パスワードを知る対象プロジェクトの単位もチームの単位も限定されずに同一パスワードが使われていた。今回、紛失事案が発生しパスワードに危殆化が生じたことから、当委員会は、従来のパスワードを直ちに変更すべきこと、パスワードの共有範囲を必要最小に限定すべきことを情報政策課に直ちに指示した。なお、「012」「013」のUSB メモリに設定されていた実際のパスワードは本報告書で詳らかにすることはできないが、本件事案発生直後に SNS 等で噂されていたような容易に想像がつくパスワードではなく、文字種が多彩でブルートフォース攻撃に対し耐性の高いパスワードが設定されていた。

調査対象機器はいずれもパスワードや PIN を入力しなければ、機器にログインできないアクセス制御がかかっていたが、一部端末では一般ユーザ権限アカウントがなく管理者権限アカウントのみを業務に用いる過剰な権限を付与する運用が認められた。A が使用する PC の ID とパスワードが他の従業員らにも共有されており、A が PC を使用できなくなった後でありながら他の従業員らが依然として当該 PC にログインでき、別アカウントを作成したり、データを整理するなどしていた。そのため ID を見ただけでは実際の PC のユーザを特定できないなどの問題が生じていた。

5　USB メモリのコールセンターへの外部運搬状況

本年 6 月 21 日夕方、A は市政情報センターから、吹田市所在のコールセンターに「012」「013」の USB メモリをカバンに入れて、電車・地下鉄を利用し一人で運搬した。カバンは革製で、鍵がかからず、USB メモリ 2 本をファスナーのついたカバンの内ポケットに入れた状態で運んでいる。A が市政情報センターを出発する際、特に誰にも告げずに出発している。コールセンターで一緒に作業する他の従業員 3 名とは、現地のコールセンター入口に別々に移動して集合した。

尼崎市と B 社の間で締結した委託契約の臨時特別給付金対応業務委託仕様書（以下「仕様書」「委託契約仕様書」等ともいう。）には、同業務実施にあたり、仕様書によるほか（委託契約１条１項)、尼崎市財務規則、個人情報保護法等その他関連法令および条例、尼崎市情報セキュリティ基本方針および尼崎市情報セキュリティ対策基準や、情報セキュリティに関する関係法令等に準拠して行うことが定められており（仕様書第 1 章 3)、セキュリティ対策基準の定めを遵守する義務が B 社には課されていた。したがって、B 社が情報資産を市政情報センター施設外に運搬する場合、セキュリティ対策基準等に従って運搬しなければならなかった。セキュリティ対策基準は、「職員は、車両等により情報資産分類１又は２の情報資産を運搬する場合は、必要に応じ鍵付きのケース等に格納し、当該情報資産がデータの場合は暗号化又はパスワードの設定を行う、当該情報資産が文書の場合は、封かんする等の情報資産の不正利用や漏洩を防止するための措置を講じなければならない。」（セキュリティ対策基準第 3 章 2 項 9 号ア)、「職員は、情報資産分類１又は２の情報資産を運搬する場合は、情報セキュリティ管理者に事前に許可を得なければならない。」（同号イ）と定

めており、上記「職員」はB社ないしB社従業員と読み替えることになる。Aが当日USBメモリ2本に保存して運搬した個人データは情報資産分類2に該当するが、具体的な個人データの内容は下記のとおりである。

記

① 全市民の住民基本台帳の情報（46万517人分）
　統一コード、氏名、郵便番号、住所、生年月日、性別、住民となった年月日等
② 住民税に係る税情報（36万573件）
　統一コード、住民税の均等割額
③ 非課税世帯等臨時特別給付金の対象世帯情報
（R3年度分7万4,767世帯分、R4年度分7,949世帯分）
　世帯主の統一コード、申請書番号、申請受付日、申請書不達理由、振込済処理日時等
④ 生活保護受給世帯と児童手当受給世帯の口座情報
（生保1万6,765件、児手6万9,261件）
　統一コード、金融機関コード、支店コード、口座区分、口座番号、口座名義

上記①～④は情報資産の中でも極めて重要な情報であり、ESB.bak（460,517人分）とESBR4.bak（459,582人分）という2つのファイルに入れられ、いずれも上記USBメモリにそれぞれ保存されていた。全市民46万人という膨大な個人データであり、万一これらの個人データが漏えいした場合には、尼崎市の全市民の平穏な日常生活が長期にわたって脅かされ不安にする事態となる。

セキュリティ対策基準は運搬には必要に応じ鍵付きのケース等を用いることを義務付けている。また、委託契約仕様書別紙1の7は、データ入力作業実施の際の入力帳票の運搬に関する規定ではあるものの、USBメモリ等の運搬・受取にあたっては、「整理表には、送付責任者、運搬責任者が押印又はサインをすること」（同⑴イ）、「入力帳票は、送付責任者が鍵付きの金属ケースに収納し、施錠すること」（同⑴ウ）、「運搬責任者は、施錠された金属ケースを運搬車両で入力作業場所まで運搬すること」（同⑴エ）、「運搬責任者は、運搬中に盗難、逸失がないよう責任をもって管理すること」（同⑴オ）、「運搬車両は、セキュリティに配慮された車両であること」（同⑴カ）、さらには仕様書6条には委託者の許可がある場合を除き個人情報が記録された資料等の複写・複製ができないこと、後述のとおり申出・届出・承認等は書面により行わなければならない旨も定められている（尼崎市業務委託契約約款1条5項）。記録媒体がUSBメモリの場合、その見た目の小ささや手軽さから利便性のみが重視されがちであるが、USBメモリが保存可能なデータ量は現在膨大なものとなっており、保存情報の漏えいによる被害発生の規模や深刻さは甚大となりうる。また、格段とサイズが小さく、紛失時には追跡・発見は一般に困難となる（本件USBメモリ発見直後のB社の会見ではGPSの位置情報をもとにUSBメモリを発見した旨説明していたが、当委員会の調査の結果本件USBメモリの発見にGPSは利用されていない。）。USBメモリの特質に鑑みると、見た目の小ささで判断するのではなく、格納さ

れた情報資産の性質（機密性を含む）・情報資産分類・重要性の度合い、漏えい時の被害の深刻さの度合い等を基礎にし、それぞれの USB メモリの取扱いを判断するのが適当である。上記 USB メモリの運搬・受取に関する上記規定は市政情報センター施設と別の外部運搬先においてパンチ入力を行う場合を前提とした文言になっているものの、運搬先との間の物理移動に伴うセキュリティリスクは本件の場合と実質的に変わらない。「012」「013」の USB メモリには全尼崎市民の個人データが格納されているのであるから、その運搬にあたっては最高レベルでのセキュリティが確保されるべきであり、鍵付きの金属ケースに入れ、複数人が運搬を担当し、目的地までセキュリティに配慮した車両で場所的に移動し、これらの手続きについて責任の所在を明確にする押印・サインをさせるなどの安全措置を講ずる USB メモリ等の運搬・受取に関する上記規定に準じて運搬するのが適当であったと考えられる。ところが、本件の場合、コールセンターで作業した B 社従業員らは A が本件 USB メモリを所持し直前までその場で使用していたことを熟知していたにもかかわらず、作業が終わるや否や、何らためらいを感じることなく、本件 USB メモリを所持する A を飲みに連れて行った。この時もし、カバンに仕舞えるコンパクトな USB メモリではなく、金属製の大型ケースに重要な情報資産を入れて運搬していたのなら寄り道などしないはずである。

USB メモリの社会的有用性に関し当委員会は全く否定するものではなく、今後も引き続き社会において私用でも業務上でも広く活用されるべきものと思料している。ただ、記録媒体による物理移動には必然的に紛失、窃盗（ひったくりを含む。）その他の漏えいリスクがあるため、本件のような漏えいによって被害が甚大となりうる情報資産を USB メモリに格納して移動させる局面では格別の考慮が必要である。重要な情報資産に関しては記録媒体の物理移動を必要としない別途の安全なデータ移行の方法を検討すべきであり、記録媒体による物理移動をやむなく行わなければならない場合であっても、各個別状況下で最も安全な環境や方法を見つけ出し、物理移動の距離や時間もできるだけ短縮する考慮が必要である。データ送信元からデータ送信先の間を安全な通信によってデータを移した場合でも、データ送信先からさらに先の最終目的のサーバ間はどうしても USB メモリ等の記録媒体によるデータ移動を行わなければならないことがある。この場合も、情報資産分類 2 に関しては、上述のサーバルーム内の給付金サーバへの USB 接続に関する取扱いと同様、厳格な安全確保を実行すべきであり、かつ、尼崎市側もデータ送信先の説明を鵜呑みにはせず、その説明に確たる安全性の裏付けがあるかを十分に確認し、もし少しでも不安要素があればその不安の解消を徹底すべく最善の手を尽くさせ、市はその裏付けを確認すべきである。

6　個人データの消去確認

個人データが USB メモリ内に保存されている状態が継続する限り漏えいのリスクがなくならないため、USB メモリによるデータ移行後、特に一定期間保存しておくべき特段の必

要性もない場合には、速やかにUSBメモリから消去すべきである。仮に保存しておくべき必要があったとしても、必要性があるという一事だけで保存を継続するのは適当ではない。保存継続の必要性の度合いと、消去後に再保存を行う手間ないし負担を考え、何より保存データの性質・規模、漏えい可能性、発生被害の深刻さ等の諸リスクを衡量し、本件のような場合には移転作業後速やかに消去することを原則とすべきである。

6月21日夕方コールセンターでのデータ移行作業が終了した後、同行者の誰も、データ消去すべきであるとか、直ちにUSBメモリを返却すべきである、などの発言をする者はいなかった。もとより、飲みに行くのを止めようと制止する者もいなかった。本件のような事態が再発しないようにするためには、作業終了後にデータ消去をする自覚を単に促すだけでなく、データ消去を実際に行ったことをダブルチェックする仕組みが必要である。最も簡易な方法は、作業終了者に、USB メモリの保存データを消去したことをその場から何らかの方法で委託者に報告させることが考えられるが、不適切な行為が意図的に行われている場合、委託者への単なる報告だけで受託者は信用してよいか疑わしく、データ消去を実際に行ったとの十分は裏付けを委託者は得られない。本件事案では同行した年長者が率先して飲みに連れて行っており、受託作業者から委託者への報告が機能するか疑問がある。運搬対象が本件のような重要データの場合は、市職員も実際に運搬者に同行し、運搬先において、取扱い終了後に受託作業者がUSBメモリ保存データを実際に消去したことを市職員がその場で現認することによってデータ消去を直接確認する方法をとることもやむを得ないと思われる。委託契約仕様書の個人情報取扱特記事項10条は、「受託者は、委託者の許可がある場合を除き、委託契約による業務に関して知り得た個人情報について、保有する必要がなくなったときは、確実かつ速やかに廃棄し、又は消去しなければならない。その際、受託者は廃棄又は消去が完了したことを証明する書面を委託者に提出しなければならない。」と定め、また、同データ取扱特記事項9条(1)(2)も同趣旨を定めているが、当該文言では、単に保有する必要性があれば消去しなくともよいとの解釈が可能となるが、全尼崎市民の個人データといった極めて重要な情報資産の場合、必要性のみを消去の可否に関する唯一の考慮要素としたのでは、安全性確保の観点からは不十分である。もっとも、本件事案では、個人情報取扱特記事項およびデータ取扱特記事項の上記文言によったとしても、B社は、保有継続の必要がないにもかかわらず、「012」「013」のUSBメモリ格納の個人データを確実かつ速やかに消去することを怠り、かつ、消去完了証明書の提出も怠ったことが認められる。

仕様書やセキュリティ対策基準に「廃棄」の文言があるが、これはデータ消去ではなく、電磁的記録媒体自体の廃棄を示しており、本件事案では市がB社に貸与したすべてのUSBメモリも、「011」「012」「013」のB社調達のUSBメモリも、いずれも市が返却を受けて管理するに至っており、現時点では廃棄は問題になっていない。

7　複製データの管理

本件事案では、紛失した2本のUSBメモリからの情報漏えい問題に関心が集まっている

が、給付金サーバからコピーされた個人データは上記2本のUSBメモリだけでなく、他の諸記憶装置（内蔵、外付け、可搬式を問わない）にも複製して記録されている。複製記録された個人データは、給付金サーバ、2本のUSBメモリ、その他の諸記憶装置を問わず、いずれも同じ尼崎市民46万人分の個人データであり、その生成、保存、移動・運搬、複製・複写、消去・廃棄の情報ライフサイクルすべてに対し安全管理措置が必要となる。Aは、本年6月21日午前9時30分前後に、「012」「013」とは別のUSBメモリ（尼崎市が購入してB社に貸与していた管理番号「008」のUSBメモリ）を使用して、給付金サーバから46万人分の個人データをコピーし、サーバルームからB社執務室に当該USBメモリを持ち込んで開発用デスクトップにその全個人データをコピーして保存したうえで、「012」「013」のUSBメモリにそれぞれコピーし、さらにB社執務室内の別のPCにも接続した。「008」USBメモリは、開発用デスクトップにデータをコピーした後、「008」USBメモリ自体に格納された尼崎市民の個人データは消去されずデータが残ったまま、鍵のかからない前述の引き出しの中に戻された。「012」「013」USBメモリの内部に格納されたログ情報の解析結果は下記8のとおりである。また、6月21日午前9時過ぎに尼崎市民個人データが給付金サーバから「012」「013」USBメモリへデータ移行され紛失後発見されるまでの流れを経時的に解析した結果は下記9のとおりである。

本件では、6月21日夕方「012」「013」のUSBメモリがコールセンターまで持参・運搬され、同所のサーバにコピーされた。これら一連のデータ移行によって、この時の給付金サーバ格納の個人データは、「008」USBメモリ、「012」USBメモリ、「013」USBメモリ、開発用デスクトップ内記憶装置、(同室内のさらに別PCへの保存は不明)、コールセンターのサーバといった、5～6か所に複製・保存されている。これらコピーされた個人データの内容はいずれも同一であるため、紛失した「012」「013」のUSBメモリの2本の記録媒体に限らず、そのいずれであっても情報が漏えいすると尼崎市民にとって深刻な不安をもたらしうるリスクを内包していた。この点、委託契約仕様書も、上述のとおり「データ等の全部又は一部を当市の許可なく複写し、又は複製しないこと。」をB社に義務付けており（第2章2（1）①システム構築業務エ）a))、同個人情報取扱特記事項6条・データ取扱特記事項5条も同趣旨を定めていたが、こうした定めに対し関係者には意識が及んでいない。諸記憶装置に複製・保存されたすべての個人データは、その情報ライフサイクルの安全性確保に留意されなければならない。なお、コールセンターでは、入退室が厳重に管理されており、オペレーター室にも死角なく監視カメラが十分に設置されるなど、セキュリティの確保に不備は認められなかった。また、尼崎市がB社より本件事案発生後、「012」「013」USBメモリ以外の尼崎市貸与の全USBメモリの返却を受け、当委員会も調査の過程で、その内容を確認したが、B社が（どの時点か不明であるが）個人データ等のデータを消去したうえでUSBメモリが尼崎市に返却されていた。

8　USBメモリメーカーによる「012」「013」USBメモリの解析検証

6 月 24 日午前に発見された、A が同月 22 日未明に紛失したと見られる、「012」「013」のラベルが貼られた USB メモリ 2 本をこれら USB メモリの製造元であるアイ・オー・データが解析した結果、紛失前日（6 月 21 日）から発見（6 月 24 日）までの間（以下「調査対象期間」という。）にこれら 2 本の USB メモリに記録されていたログの内容は以下のとおりである。

(1) 発見された USB メモリと紛失した USB メモリとの同一性

発見された 2 本の USB メモリの製品型番は USB メモリの外観から確認可能であった。一方、製品内部シリアルナンバーは USB メモリの外観から確認できず、書込み防止装置・PC 等のデバイスに接続して初めて確認できる仕様になっている。本件では製品内部シリアルナンバーは USB メモリの解析により確認される過去の使用履歴等と照合して同一性を検証した。その結果、6 月 24 日に発見された「012」「013」のラベルが貼られた 2 本の USB メモリの各製品型番および各製品内部シリアルナンバーは、それぞれ紛失直前の使用歴と一致した。

(2) 製品仕様・解析方法

「012」「013」の USB メモリには、いずれもコントローラに AES256bit でユーザデータを自動暗号化する機能が搭載されており、USB メモリ内部のデータ保存領域に書き込まれる全データがパスワードで保護される。ユーザがデータ保存領域にアクセスするには搭載ソフトウェアを起動して制限回数内にパスワード入力に成功しログインする必要があり、USB メモリ内部のフラッシュメモリをチップオフして直接解析を試みてもデータの閲覧は困難となっている。パスワードを連続して制限回数まで間違えた場合、ロックの解除には初期化しなければならず、初期化した場合、全保存データが消去される仕様となっている。USB メモリに行われたログインの成否は、搭載ソフトウェアにより内部の秘匿領域に自動的にログとして記録保存され、仕様上ユーザはログの記録なくデータへのアクセスはできない。秘匿領域に保存されているログの閲覧機能はユーザには提供されていないが、本件 USB メモリの場合、メーカーの開発用ツールを使うことによってのみ閲覧が可能となる。本解析では、アイ・オー・データは、USB メモリ紛失中の調査対象期間のデータアクセスの有無を調査する目的に限定して開発用ツールを使い、対象 USB メモリの秘匿領域に格納されているログを確認した。

(3) 記録されるログ情報

開発用ツールによって確認されるログの情報は、①操作内容・結果、②操作を行った日時、③操作を行った PC のコンピュータ名、④操作を行った PC のユーザアカウント名、⑤操作を行った PC のネットワークアダプタの MAC アドレス、⑥操作を行ったアプリケーションである。上記②の日時は操作 PC の時刻によるが、その日時と関係なく、操作された順にロ

グが保存される。上記①のログインおよびパスワード変更に関して、ログインの成功、ログインの失敗、パスワード変更の成功、パスワード変更の失敗が記録される。

(4) 開発用ツールによる出力結果

「012」「013」の USB メモリ内に保存されていた調査対象期間のログを出力した結果は以下のとおりである。

（a)「012」の USB メモリに格納されていた調査対象期間のログ

Success - ○○_△△Log [wIndex = 425]
Date = 2022/06/21
Time = 09:30:01
PCName = 開発用デスクトップ PC
UserName = "Administrator"
Mac = ○○:○○:○○:○○:○○:○○
LogFunc = 1
App = 0

Success - ○○_△△Log [wIndex = 426]
Date = 2022/06/21
Time = 09:30:59
PCName = 開発用ノート PC
UserName = "○○Administrator"
Mac = ○○:○○:○○:○○:○○:○○
LogFunc = 2
App = 0

Success - ○○_△△Log [wIndex = 427]
Date = 2022/06/21
Time = 09:31:06
PCName = 開発用ノート PC
UserName = "○○Administrator"
Mac = ○○:○○:○○:○○:○○:○○
LogFunc = 1
App = 0

Success - ○○_△△Log [wIndex = 428]

Date　　= 2022/06/21
Time　　= 17:39:20
PCName　= コールセンターサーバ
UserName = "〇〇"
Mac　　= 〇〇:〇〇:〇〇:〇〇:〇〇:〇〇
LogFunc　= 1
App　　= 0

Success - 〇〇_△△Log　[wIndex = 429]
Date　　= 2022/06/21
Time　　= 18:18:39
PCName　= コールセンターサーバ
UserName = "〇〇"
Mac　　= 〇〇:〇〇:〇〇:〇〇:〇〇:〇〇
LogFunc　= 2
App　　= 0

Success - 〇〇_△△Log　[wIndex = 430]
Date　　= 2022/06/21
Time　　= 18:18:47
PCName　= コールセンターサーバ
UserName = "〇〇"
Mac　　= 〇〇:〇〇:〇〇:〇〇:〇〇:〇〇
LogFunc　= 1
App　　= 0

Success - 〇〇_△△Log　[wIndex = 431]
Date　　= 2022/06/24
Time　　= 13:23:21
PCName　= B 社従業員〇PC
UserName = B 社従業員〇
Mac　　= 〇〇:〇〇:〇〇:〇〇:〇〇:〇〇
LogFunc　= 1
App　　= 0

Success - 〇〇_△△Log　[wIndex = 432]

Date　　= 2022/06/24
Time　　= 13:26:45
PCName　= B 社従業員○PC
UserName = B 社従業員○
Mac　　= ○○:○○:○○:○○:○○:○○
LogFunc　= 1
App　　= 0

(b) 「013」の USB メモリに格納されていた調査対象期間のログ
Success - ○○_△△Log　[wIndex = 321]
Date　　= 2022/06/21
Time　　= 09:28:00
PCName　= 開発用デスクトップ PC
UserName = "Administrator"
Mac　　= ○○:○○:○○:○○:○○:○○
LogFunc　= 2
App　　= 0

Success - ○○_△△Log　[wIndex = 322]
Date　　= 2022/06/21
Time　　= 09:28:08
PCName　= 開発用デスクトップ PC
UserName = "Administrator"
Mac　　= ○○:○○:○○:○○:○○:○○
LogFunc　= 1
App　　= 0

Success - ○○_△△Log　[wIndex = 323]
Date　　= 2022/06/24
Time　　= 13:25:01
PCName　= B 社従業員○PC
UserName = B 社従業員○
Mac　　= ○○:○○:○○:○○:○○:○○
LogFunc　= 2
App　　= 0

Success - ○○_△△Log　[wIndex = 324]
Date　　= 2022/06/24
Time　　= 13:25:14
PCName　= B 社従業員○PC
UserName = B 社従業員○
Mac　　= ○○:○○:○○:○○:○○:○○
LogFunc　= 1
App　　= 0

上記の「Success - ○○_△△Log [wIndex = xxx]」(xxx はログの経時的な通し番号を示す)は、開発用ツールによるログの取得に成功したことを示し、「Date」から「App」までの 7 行が 1 つの操作のログ情報である。また、「LogFunc」の値は「操作内容・結果」を示し、LogFunc = 1：ログイン成功、LogFunc = 2 ：ログイン失敗を意味する。「App」の値は「操作を行ったアプリケーション」を示し、App = 0 ：USB メモリ搭載ソフトウェアである。

(5) 操作の日時・コンピュータ名・操作内容結果

ログの情報から、調査対象期間である 2022 年 6 月 21 日から同月 24 日までの間で「012」「013」の USB メモリに対する操作を行った日時、コンピュータ名、操作の内容・結果を整理すると以下のとおりである。

(i)「012」USB メモリ

操作を行った日時	コンピュータ名	操作内容・結果
2022/06/21 09:30:01	開発用デスクトップ PC	ログイン成功
2022/06/21 09:30:59	開発用ノート PC	ログイン失敗
2022/06/21 09:31:06	開発用ノート PC	ログイン成功
2022/06/21 17:39:20	コールセンターサーバ	ログイン成功
2022/06/21 18:18:39	コールセンターサーバ	ログイン失敗
2022/06/21 18:18:47	コールセンターサーバ	ログイン成功
2022/06/24 13:23:21	B 社従業員○PC	ログイン成功
2022/06/24 13:26:45	B 社従業員○PC	ログイン成功

(ii)「013」USB メモリ

操作を行った日時	コンピュータ名	操作内容・結果
2022/06/21 09:28:00	開発用デスクトップ PC	ログイン失敗

2022/06/21 09:28:08	開発用デスクトップ PC	ログイン成功
2022/06/24 13:25:01	B 社従業員〇PC	ログイン失敗
2022/06/24 13:25:14	B 社従業員〇PC	ログイン成功

9　尼崎市民個人データが給付金サーバから「012」「013」USB メモリへデータ移行され紛失後発見されるまでの流れを示す証跡

日時	接続機器	「012」USB メモリ （B 社所有）	「013」USB メモリ （B 社所有）	「008」　USB メモリ （市所有・貸与）
2022/6/21	給付金サーバ　※1	-	-	9:12:39 ※8
	開発用デスクトップ PC ※2	9:29:19 接続 ※5 09:30:01 認証成功　※6 09:31:00 取外し ※5	9:27:45 接続　※5 9:28:00 認証失敗 ※6 9:28:08 認証成功 ※6 9:29:13 取外し　※5	9:24:43 ※8 （上記直後、本件尼崎市民の個人データを含むファイルが開発用デスクトップ PC 上に作成されている。）
	開発用ノート PC ※3	接続履歴なし　※ 09:30:59 認証失敗　※6 09:31:06 認証成功 ※6 取外し履歴なし　※	-	
	コールセンターサーバ ※4	17:39:03 初回接続 ※7 17:39:20 認証成功 ※6 18:18:39 認証失敗 ※6 18:18:47 認証成功 ※6 18:23:07 取外し ※5	-	
2022/6/22 ｜ 2022/6/23	全	-	-	以後、開発用デスクトップ PC および開発用ノート PC で複数回使用　※5,8
2022/6/24	給付金サーバ	-	-	
	開発用デスクトップ PC	-	-	
	開発用ノート PC	-	-	
	コールセンターサーバ	-	-	
	B 社従業員〇PC	13:23:21 認証成功 ※6 13:26:45 認証成功 ※6	13:25:01 認証失敗 ※6 13:25:14 認証成功 ※6	

※ B 社より A が本件紛失事案発生前に B 社執務室内で開発用に使っていたノート PC として当調査委員会が提供を受けたが、
6 月 21 日に「012」USB メモリの接続および取外し履歴は同ノート PC のレジストリにはなかった。
※1 給付金サーバの時刻は、7/7 時点で約-10 分（時間が早い）。ネット不接続のため同期ができないことによる。
※2 開発用デスクトップ PC の時刻には時差がほぼなかった。
※3 開発用ノート PC の時刻は、7/7 時点で約+4 分（時間が遅い）。
※4 コールセンターサーバの時刻は、7/21 時点で約-19 分。
以下の ※5-8 の各日時の取得元は下記各記録情報による。
※5 Windows レジストリ
※6 上記 8　〇〇_△△Log
※7 Windows レジストリおよび USB ドライバーインストールログ
※8 Windows イベントログ

10　「012」「013」USB メモリとこれらが接続された機器の証跡に基づく結論

本年 6 月 22 日未明に紛失し、同月 24 日正午前に発見されるまでの間に、「012」「013」USB メモリに格納された尼崎市民の個人データが何者かによって正しいパスワードが入力されてログインされた形跡はなく、この間に上記個人データのこれら 2 本の USB メモリからの漏えいがあったとは認められない。

11　B 社による本件各契約条項の認識

受託者日本ユニシス株式会社関西支社執行役員支社長は、委託者尼崎市代表者尼崎市長との間で、令和 4 年 2 月 3 日付けで、業務委託名「臨時特別給付金対応業務委託」、「契約金額」320，870，000 円、「契約の期間」令和 4 年 2 月 4 日から同年 12 月 31 日等とする内容の委託契約を締結しているが、同日付けはバックデートによるものである。委託契約の仕様書案は、本年 2 月 16 日に尼崎市臨時特別給付金担当から、B 社公共第一事業部ビジネス三部の B 社従業員に送信したメールに添付して B 社に内容の確認を求めている。同仕様書案では、(ⅰ)「3　準拠する法令等」に、準拠すべきものとして、「(3)尼崎市情報セキュリティ基本方針及び尼崎市情報セキュリティ対策基準のほか、情報セキュリティに関する関係法令等」を追加し、セキュリティ対策基準が B 社との委託契約にも適用されることを明示して尼崎市職員を B 社従業員らに読み替える措置を執ったほか、(ⅱ)「2　業務内容」「(3)バックヤード体制（申請書の受付・審査)」の「②　申請書の受付、データ入力、審査、総合振込データ作成業務等」の「ウ　データ入力」に、申請管理、審査を目的として申請書情報のパンチ入力を行う詳細を「別紙 1 のとおり」として別紙に下記の約定事項を、修正履歴付きで追加した。

記

6　入力作業場所

(1)　受託者が指定し、委託者が認めた施設（東京都○○　・・・・）

(2)　委託者が指定する施設（尼崎市東七松町１－５－２０市政情報センター１Ｆ）

7　入力作業場所が 6(1)の場合

(1)　入力帳票の運搬

ア　(略)

イ　整理表には、送付責任者、運搬責任者が押印又はサインをすること

ウ　入力帳票は、送付責任者が鍵付きの金属ケースに収納し、施錠すること

エ　運搬責任者は、施錠された金属ケースを運搬車両で入力作業場所まで運搬すること

オ　運搬責任者は、運搬中に盗難、逸失がないよう責任をもって管理すること

カ　運搬車両は、セキュリティに配慮された車両であること

(2)　入力帳票の入力

ア　入力責任者は、運搬責任者から金属ケースを受け取り、開錠し、整理表に押印又はサインをすること

イ～エ・カ・キ　(略)

オ　入力作業場所は、関係者以外が立ち入ることができないようにセキュリティを確保すること

ク　セキュリティは、AES256bit ハードウェア暗号化を推奨する。(略)

ケ　入力帳票、USB、入力するパソコン等は他へ持ち出せないよう厳重に管理すること

(3)　USB 等の運搬

ア　(略)

イ　整理表には、入力責任者、運搬責任者が押印又はサインをすること

ウ　USB と入力済みの入力帳票は、入力責任者が鍵付きの金属ケースに収納し、施錠すること

エ　運搬責任者は、施錠された金属ケースを運搬車両で委託者が指定する場所まで運搬すること

オ　運搬責任者は、運搬中に盗難、逸失がないよう責任をもって管理すること

カ　運搬車両は、セキュリティに配慮された車両であること

(4)　USB 等の受取

ア　送付責任者は、運搬責任者から金属ケースを受け取り、開錠し、整理表に押印又はサインをすること

イ・ウ　(略)

尼崎市からの以上の仕様書案の提案に対し、B 社従業員は、翌 17 日、市職員 3 名と B 社の他の従業員 3 名を CC に入れて再修正案を尼崎市の上記担当者に返信する形で送付したが、情報セキュリティに関する上記（ⅰ）（ⅱ）は再修正案の中ではほぼそのまま維持し、何ら変更を加えなかった。同年 3 月 9 日には、尼崎市の上記担当者が B 社従業員に、「契約書（案）のご確認につきまして」の件名で、業務委託契約書、仕様書、個人情報取扱特記事項、データ取扱特記事項等を添付して契約書案等の確認を求めた。これに対し、同日中に B 社従業員は「内容確認させていただきました。問題はございません。よろしくお願いします。」とメールで返信し、委託契約等上記各書面の内容を了承した。それから間もなくして上記委託契約が双方により捺印され、締結に至っている。

以上のとおりであり、無断再委託等を禁じ、また、セキュリティ対策基準や USB メモリの運搬等に関する規定を特に盛り込む内容の契約締結のやり取りを、B 社の従業員らは尼崎市との間で直接担当し、ないしはこれら契約交渉のメールの CC に委託契約の締結所管部署の従業員として入っていて、個人情報取扱特記事項を含む仕様書、約款、セキュリティ対策基準を含む委託契約の内容を熟知すべき立場にあった。これら契約締結担当の B 社の従業員のうち 1 名は、6 月 21 日昼前に、データ移転作業の主任である別の B 社従業員からコールセンターでの作業後飲みに行くことをメールで誘われ、コールセンターに実際に行って本件 USB メモリを帯同する A を伴ってその後飲みに行った。コールセンターでの作業後の飲みを誘う 6 月 21 日昼前の上記メールの CC には、市との間で直接契約交渉を担当した B 社従業員も入っていた。委任契約締結に先立ち、B 社は、令和 2 年からの特別定額給付金業務から尼崎市から書面の承諾を得ることなく無断で再委託・再々委託を行っていた

ようであるが、令和 4 年の臨時特別給付金対応業務委託対応の委託契約の締結を担当した B 社従業員の中に、無断の再委託・再々委託を禁じることを明示する条項が同契約中に明記されながら、当該条項の違反になることを回避する行動をとったり、承諾の有無を確認するなどの行動をとっていたとは認められない。むしろ再委託・再々委託を承知のうえで市との間で委託契約の締結を進め、かつ契約締結後も A らが B 社の従業員ではないことを承知して A らの業務従事を認めており、元々尼崎市との間の約定を遵守する意思がなかったのではないかとすら推認されてもやむを得ない。

12　B 社による無断の再委託・再々委託

尼崎市と B 社との間の委託契約は、「受託者は、委託業務の一部を第三者に委託し、又は請け負わせようとするときは、あらかじめ委託者の承認を得なければならない」と定め（6 条 2 項）、同仕様書第 1 章 5、同個人情報取扱特記事項 11 条 1 項・3 項(1)およびデータ取扱特記事項 10 条 1 項・3 項(1)も同趣旨の規定を定めている。尼崎市業務委託契約約款は、「この約款又は仕様書等に定める委託者又は受託者による催告、請求、通知、報告、申出、届出、承認及び解除は、書面により行わなければならない。」（1 条 5 項）と規定し、承諾や届出等を「書面」で行うべきことを義務付けている。また、委託契約仕様書個人情報取扱特記事項は、委託者が再委託や再々委託を認める場合であっても、「再委託する業務内容に個人情報の取扱いが含まれる場合は、再委託先となる予定の者において、この特記事項に規定する安全管理措置が講じられることを再委託契約の締結前にあらかじめ確認し、書面により委託者に提出しなければならない。」（11 条 2 項）、「再々委託等の契約の締結前に、再々委託先となる予定の者において、この特記事項に規定する安全管理措置が講じられることをあらかじめ確認し、書面により委託者に提出すること」(11 条 3 項(2))としていずれも「書面」を義務付けている（委託契約書仕様書データ取扱特記事項 10 条 2 項・同 3 項(2)も同趣旨）。これは、再委託、再々委託の承認等の事実の確たる証拠化を図り、当事者間で後日承諾等の有無に疑義が生じないよう確定的な意思表示とすべく承諾等を書面によることを義務付けたものである。承諾の申出や承諾書面を得ることは、B 社には、市への定期報告義務、セキュリティ研修義実施務（委託契約仕様書第 2 章 2 (1)①システム構築業務エ）c)、同個人情報取扱特記事項 8 条 2 項・データ取扱特記事項 7 条 2 項）、同等以上の規定を再委託・再々委託の各契約に規定し、再委託先・再々委託先に一切の義務を遵守させ、かつ履行状況を監督すべき義務（個人情報取扱特記事項 12 条およびデータ取扱特記事項 11 条）、再々委託契約の通知義務（個人情報取扱特記事項 11 条 3 項⑶およびデータ取扱特記事項 10 条 3 項⑶）等々、再委託先・再々委託先に対する諸義務を負うことの B 社の組織的な自覚となる。尼崎市にとっても、承諾の申し出があれば再委託先・再々委託先の存在を知り、これらに対する受託者の監督等の履行状況を確認する契機が与えられる。ところが、B 社は本件臨時特別給付金対応業務委託（の一部）を再委託・再々委託を行うにあたり、あらかじめ尼崎市から承諾を得ることなく、本件事案発生前に事後にも承諾を得ることを怠って委託

契約 6 条 2 項に違反し、書面による承諾も得ていない。B 社の一部従業員は、A を含む複数の者が所属する別事業者への再々委託を知っていたが、同じく事前にも事後にも尼崎市から承諾を得るための申し出をするすることはなかった。市職員の一部が再委託・再々委託の事実を知っていたかのような報道が一部にあるが、何よりこうした疑義を生じさせないためにこそ承諾等は書面によるべきことを規定しているのである。B 社は再委託・再々委託について「書面」によって尼崎市から承諾を得るべきだったにもかかわらず B 社はその義務を怠った。尼崎市が B 社の臨時特別給付金対応業務委託（の一部）の再委託・再々委託を明示的に承諾した事実はなく、また、書面承諾に相当するような黙示の承諾を推認させる確たる証拠もない。なお念のため、当委員会は、尼崎市職員が上記業務委託に関し再委託ないし再々委託の事実を知っていたかを尼崎市職員らに確認したが、再委託や再々委託の事実は知らなかったとの回答を得、その裏付けを得るため、A 本人や B 社執務室内で稼働していた再委託先・再々委託先の従業員らにも直接確認を行った。それに対し、再委託先・再々委託先の従業員らは、自分は B 社従業員であるかのように市職員と接するようにとの指示を長年受けてきており、自身が B 社以外の会社に所属することは尼崎市には秘密にするよう口止めされていた、と説明した。市職員と初めて接する場合も、一緒にいる B 社従業員らは市職員との間で名刺交換はするが、自身らは名刺交換をせず、B 社従業員であるかのように市職員と接し、その場に一緒にいる B 社従業員らもそうした接し方を否定せず、再委託先ないし再々委託先の従業員であると市職員に紹介することは一切なかった。B 社執務室の管理責任者である B 社従業員は当委員会に対して、再委託先・再々委託先の従業員らには、自身らが B 社従業員であるかのように市職員と接するよう指示したことも認めている。再委託先・再々委託先の従業員らは、市職員と飲食を共にすることは過去十数年来なく、そのため市職員との間で打ち解けて素性を明かす機会もなかったと当委員会に説明している。

B 社執務室内で稼働する無断再委託先従業員や無断再々委託先従業員が使用するメールアドレスも B 社のメールアドレスであった。B 社はこれらの者に対し、B 社のメールアカウントを付与し、当該メールアカウントを使うように無断再委託先・再々委託先従業員らに指示し、尼崎市職員との間でメールをやり取りさせていたため、市職員からは、無断再委託先従業員のメールも、無断再々委託先従業員のメールも、B 社従業員からのメールに見える内容となっていた。B 社執務室の管理責任者である B 社従業員も、同執務室内で稼働する再委託先ないし再々委託先の従業員らに対し、B 社のメールアカウント（@の右側が B 社ドメイン名で、@の左側が英語表記した本人の名前）を使用させていたことを認めている。この点について上記 B 社従業員は、自分が責任者になる以前から B 社のメールアカウントを使うよう長年指示してきたことを自分も続けただけである、以前は再委託先従業員や再々委託先従業員にはメールアカウントがなかった、再委託先・再々委託先にはメールを使う環境がなかった、B 社の同じ Outlook を使えばメールをすることができると当委員会に説明した。その一方で、こうしたメール環境の話は 15 年前のことであり、現在のことでは

ないとも述べ、その説明には合理性は認められなかった。また、当委員会からは、B 社のメールアカウントを使うよう指示しただけでなく、尼崎市職員宛てに送信するメールの本文に「ユニシスの○○です」「日本ユニシスの○○です」「BIPROGY の○○です」とまで無断再委託先従業員、無断再々委託先従業員らに名乗らせていた理由を尋ねると、上記 B 社従業員は、同社の名前で仕事を市から請け負ったから市には B 社従業員と名乗らせたとか、B 社の名前で市から仕事を請け負って真実の所属社名を市に伝えると市が混乱するからと説明した。再委託や再々委託を B 社が尼崎市に隠して無断で行っている行動の一環とみれば上記説明は辻褄が合っていた。無断再委託先従業員や無断再々委託先従業員が尼崎市職員に対し B 社従業員と名乗って送信したメールは何通もあるが、A が本件紛失前に業務上使用していたインターネット接続用 PC の Outlook メールを調査した結果、たとえば、以下のようなメールがあった。

① A が「ユニシス」従業員を名乗って、市職員宛にメールを送信。
② A が「日本ユニシス」従業員を名乗って、市職員宛にメールを送信。
③ A が「BIPROGY」従業員を名乗って、市職員宛にメールを送信。
④ A が、「ユニシス　様」宛に送信したメールに対し、A が、ユニシスを代表して返信し、また、同メールの CC に他の B 社従業員らが含まれているにもかかわらず、A が B 社を代表してメールを返信したことに対して、CC に入っている B 社従業員らから訂正や異議等出されず、A が B 社従業員を名乗ることを認めていた。
⑤ 市職員が、B 社の他の従業員宛に送信したメールに対して、A が、B 社を代表して返信し、また、同メールの CC に他の B 社従業員らが含まれているにもかかわらず、A が B 社を代表してメールを返信したことに対して、これら B 社従業員らから訂正や異議等出されず、A が B 社従業員を名乗ることを認めていた。
⑥ 市職員が、「BIPROGY　A」と記載して B 社の他の従業員宛に送信したメールに対し、A が「B 社　A」と BIPROGY 従業員を名乗って返信し、同メールを受信した他の B 社従業員らは訂正や異議等出さず、A が B 社従業員を名乗ることを認めていた。
⑦ 無断再委託先従業員も、自身を「BIPROGY/ユニシス　○○」と名乗り、市職員も同人を「BIPROGY/ユニシス」の従業員として認識するメールを送信。

13　監査・研修

B 社執務室を管理する B 社責任者によると、B 社はこれまで再委託先や再々委託先に対し、セキュリティ監査を実施したことがない。B 社によるセキュリティ監査の実施については、再委託先も再々委託先も B 社は監査したことがないと同様に述べている。本件事案では、市政情報センターからコールセンターに個人データを移動運搬する当日の 6 月 21 日の昼前、この日のデータ移転作業の責任者的立場にある年長の B 社従業員が、率先して作業後の夜の飲み会を発案して誘い、また、セキュリティ対策基準など情報資産の安全管理等を詳細に盛り込む委任契約の締結に実際に関わった B 社従業員は、全尼崎市民 46 万人余りの

個人データを格納したUSBメモリを一緒の作業者が帯同しているにもかかわらず自身が担当した契約に定められた諸義務を顧慮せずためらいなく飲み会に行き、これらB社従業員２名は紛失者を飲み会に同席させている。上記B社従業員が作業後の飲み会を誘ったメールのCCには、セキュリティ対策基準など情報資産の安全管理等を詳細に盛り込む委任契約の締結を尼崎市側と直接やりとりしたB社従業員も含まれていたが、作業後の飲み会の誘いをするメールに対し異議や注意喚起等することもなかった。全尼崎市民の個人データを含むUSBメモリを所持していることに対するセキュリティ意識が完全に欠落しており、セキュリティ研修は実効性のある内容とやり方を工夫する必要がある。また、B社は、委託契約による業務に係る個人情報の取り扱い状況について、尼崎市に対し、定期的な報告義務があるにもかかわらず行っていない（委託契約個人情報取扱特記事項16条およびデータ取扱特記事項15条)。

コロナが流行する以前はB社が再委託先や再々委託先の従業員に対し、セキュリティ研修を年1回実施していたようであるが、コロナの流行によりセキュリティ環境が激変したにもかかわらず、コロナ流行以降B社は再委託先や再々委託先の従業員に対し、セキュリティ研修を実施していない。委託契約仕様書は、「委託業務従事者に対し、業務委託の実施に必要な知識及び技術を習得させるとともに、随時、セキュリティに関する研修、教育その他従事者の資質向上を図る研修を実施すること。」と定め、B社に対し、上記研修等の義務を課し（第２章２（１）①システム構築業務エ）c))、同個人情報取扱特記事項８条２項・データ取扱特記事項７条２項も同趣旨を定めている。

他方、尼崎市も、B社に対し、セキュリティ監査を直接実施したことがない。この点は改善が必要である。セキュリティ対策基準第27章に基づく監査の規定は尼崎市においては画餅（がべい）に過ぎず、最低でも規定どおりの実行はしなければならない。尼崎市はB社に対し、必要なセキュリティ対策の確保の定期的な確認等を求めることができ、個人情報の取り扱い状況についても定期的に報告を求めることができるが（委託契約個人情報取扱特記事項15条16条およびデータ取扱特記事項14条15条)、定期報告の性質上、尼崎市はB社からの報告を待つだけでなく、報告が長期にわたってない場合は市がB社に対し、積極的に報告を求めていくべきであるが、市はこれを行っていない。単にセキュリティ対策基準を策定して掲げるだけでなく、尼崎市民が不安に陥らないように、セキュリティガバナンスが実際に機能するよう仕組み自体を抜本的に見直す必要がある。

セキュリティ対策基準第10章には研修・訓練に関する規定があり、尼崎市は市職員に対し年1回これまで実施してきたものの、サーバルームの状況やB社に対するチェック等をみる限り、実効性のある研修・訓練が行われてきたとは思われず、尼崎市も研修を改善すべき必要がある。一方向的な研修の受講だけでなく、たとえば受発注者が同席し現場の実際を踏まえたセキュリティ情報を交換したり一緒に諸問題を議論するミーティングを実施するなど、セキュリティ意識向上に実のある研修を工夫し実行する。

本件事案の発生により、尼崎市職員および委託事業者のセキュリティ意識に対する市民

の不安は大きく、実効性のあるセキュリティ研修を実施し、セキュリティ意識および遵法精神（市職員が委託事業者にルールを厳格に守らせる意識を含む。）の向上を図る観点から、研修内容の充実化（習得されているかを確認するフィードバックの実施）、実施回数、模擬実践など研修効果を予想し十分検討して実施する。長期にわたって無断再委託、再々委託が行われていた事実を市が見抜けなかったが、従前からの継続・更新であるとして B 社に対する審査が緩んでいた。市民の重要な情報資産を預かる立場から、個人情報を扱うことの適否に関しゼロベースでセキュリティ監査を厳格に実施すべきであり、最低でもすでに具体的に定められている下記監査規定は今後実行すべきである。なお、下記に「必要に応じ」は現在の状況では必要であることは明白であり、下記をすべて実行するのが適当である。

記

第 27 章 監査

1　実施方法

最高情報セキュリティ責任者は、情報セキュリティ監査統括責任者を指名し、ネットワークおよび情報システム等の情報資産における情報セキュリティ対策状況について、必要に応じて監査を行わせなければならない。

2　監査を行う者の要件

情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

3　監査実施計画の立案および実施への協力

(1) 情報セキュリティ監査統括責任者は、監査を行うにあたって、監査実施計画を立案し、最高情報セキュリティ責任者の承認を得なければならない。

(2) 被監査部門は、監査の実施に協力しなければならない。

4　外部委託事業者および指定管理者に対する監査

情報セキュリティ監査統括責任者は、外部委託事業者に情報資産分類 1 または 2 の情報資産を扱う業務を委託している、あるいは指定管理者に委任している場合は、外部委託事業者および指定管理者から再委託として受託している事業者も含めて、情報セキュリティポリシーの遵守について監査を必要に応じて行わなければならない。

5　報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、最高情報セキュリティ責任者および情報セキュリティ監査確認者に報告する。

6　(略)

7　監査結果への対応

(1) 情報セキュリティ監査確認者は、監査結果を確認し、必要に応じて指摘事項等について最高情報セキュリティ責任者に意見を述べることができる。

(2) 最高情報セキュリティ責任者は、監査結果および情報セキュリティ確認者の意見を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指

示しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題および問題点がある可能性が高い場合には、当該課題および問題点の有無を確認させなければならない。

第 6　尼崎市の情報管理体制の問題

本件事案は、B 社従業員らが USB メモリを携帯する A を連れて飲みに行って発生した事案であるが、これを調査する過程で、上述のとおり B 社による複数の違反が認められた。A は、再々委託先従業員であることを市職員に打ち明けることをしないよう指導されたなどの B 社側の工作もあり、尼崎市の現場の幹部職員らが見抜けなかったことにはやむを得ないところがあるが、管理カード貸与を含めたサーバルームの入退室管理、B 社執務室内の業務に対する監査、USB メモリの取扱い、データ消去その他、尼崎市としていくつもの対策を講ずべき問題が認められた。主たる責任が B 社にあり意図的になされたものもあるとはいえ、尼崎市もセキュリティ事故を未然に防ぐセキュリティガバナンス体制の構築等は十分ではない。特に下記の者は尼崎市のセキュリティ組織体制のトップないしそれに次ぐ職務にあり、抜本的見直しを含め、より一層の職責を果たし得たのではないかと考えられる。

(1) セキュリティ対策基準第 2 章は組織体制のトップとして最高情報セキュリティ責任者を置いている。最高情報セキュリティ責任者は、「対策基準が適用される全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策を行わせ」、「対策基準が適用される全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する」責任を負うものであり、本件事案や既述の各種セキュリティ問題に対し一層の職責を果たすべきであった。

(2) セキュリティ対策基準第 2 章は組織体制の中で、最高情報セキュリティ責任者の次順位として、統括情報セキュリティ責任者を置いている。統括情報セキュリティ責任者の職責は、「最高情報セキュリティ責任者を補佐」し、「対策基準が適用される全てのネットワーク及び情報システムにおける、情報セキュリティ対策に関する」責任を負うとある。さらに本件の場合、統括情報セキュリティ責任者は情報セキュリティ責任者を兼任している。情報セキュリティ責任者は、「その所管する局等の情報セキュリティ対策に関する統括的な」責任を負い、「その所管する局等において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な」責任を負うものであり、本件事案や既述の各種セキュリティ問題に対し一層の職責を果たすべきであった。

(3) セキュリティ対策基準第 2 章は組織体制の中に情報セキュリティ監査確認者を置いている。情報セキュリティ監査確認者の職責は「情報セキュリティ監査の結果を確認させる」とあるが、B 社に関する情報セキュリティ監査の結果に対し一層の職責を果たすべきであった。

第７　再発防止策と提言

本件のような情報資産の取扱いに関する事故を再び起こさないために、短期的な方針として（すでに述べたところと重複するところもあるが)、再発防止策をまとめた。中長期的な防止策については提言としてまとめた。

1　個人情報保護・データ保護の確保

住民基本情報の取り扱いは、（業務委託契約の締結は当然として）所管課である市民課職員が立ち会いのもとで委託事業者での作業を行う。委託事業者のみでの作業となる場合、どの契約における作業で、どの範囲の情報が必要になっているのか、必要としている業務や情報システムの所管課と協議の上、書面での作業依頼を行い、その内容・件数等を所管課・情報政策課で確認して引き渡す。所得の情報や福祉の情報を取り扱う場合も同様で、必要となっている情報の所管課による作業の確認を確実なものとする。

USB メモリ等の外部電磁的記録媒体の使用は、特に情報資産分類１・２では、格納するデータファイルの種類・使用目的・使用場所・移動コスト等を総合的に判断し、上述のとおり必要最小限の使用に留める。それぞれの記録媒体の所管を明らかにし、使用記録簿により使用後に元の保管場所に戻ってくるまでの管理を行う。庁舎外への持ち出しについては、既に尼崎市で方針を決定しており、運搬する事業者に市職員が同行し、USB メモリ等の外部電磁的記録媒体等によってその情報を使用する場所まで搬送し、記録されたデータを移した後その場で事業者が直ちに削除し、市職員がこれをその場で現認して確認し、データ消去後の記録媒体等を庁舎に返却する。

同様に、既に検討しているオンラインストレージシステムの利用は、全業務で強制するのではなく、取り扱う情報の性質・分類・業務内容などに応じ、情報ライフサイクルのすべてのセキュリティをその都度確認したうえで利用を進める。

2　入退室の管理

住民基本情報を含む情報ファイルを管理している場所への入退室は、本人確認を伴う入室者登録を行う。サーバルームと作業場所の間の人の移動および作業場所からの遠隔接続・遠隔操作について記録をとる。個人・業務用いずれの外部電磁的記録媒体や PC 等の持ち込みを規制する。特に、サーバルームは、特定個人情報の管理区域に指定されており、物理的な安全管理措置を講じることが義務付けられている。

サーバルームおよび委託事業者の作業場所については、上述のとおり監視カメラ等による監視を拡充し、遠隔接続による住民情報に関するデータファイルへのアクセスは、端末・作業者を限定し、その利用記録をとる（委託事業内容に基づいた遠隔接続・遠隔操作に限る)。

3　情報セキュリティ施策の再構築

情報セキュリティに関する市全体の取組みは、計画的に実行することが求められる。情報セキュリティ施策を市職員全員に浸透させていくために、提言でも言及している情報セキュリティ研修等を含んだ、年間を通しての情報セキュリティ計画を毎年作成し、計画的に実行する。

4　契約関係

当該事業の所管課・室において、事務内容・業務フローを洗い出し、どの部分を職員で行い、職員で取り扱うことが不可能な事務処理等を委託事業として切り出す。委託事業者に委託したとしても、個人情報保護・データ保護は職員で行うのと同等あるいはそれ以上のレベルで取り扱い、「特記事項」を盛り込んだ委託仕様書を決める。

業務開始までの時間的な余裕がある場合は、それぞれの委託業務を個別に選定し、それぞれ実際に携わる事業者と契約を交わす。もしも、開始までの時間的に余裕がない場合、総合委託でも構わないが、再委託ではない、共同事業体として契約を交わす（それぞれの事業者がその受託内容を責任を持って担当する）ことを原則とするが、この問題は、本調査報告書提出後も引き続き当委員会は尼崎市と協議して検討を進め、令和５年３月末を目途に対策の具体化を目指す。

前例踏襲の契約書・業務委託仕様書の承認を最終的にどの部署が行うのか、所管課のみなのか、契約課なのか、情報政策課が関わるのか、それぞれの関わり方・体制づくりが必要である。特に、ホストコンピュータからオープン化が進んだ現在では、情報政策課の関わりが急激になくなりつつあり、原課任せになっている点を是正する必要がある。ホストコンピュータ時代に情報政策課がどのように情報を管理してきたか、その方法や仕組みは今後更に検討を継続する。

委託業務開始前後の打ち合わせ等、議事録を残し、後日双方で確認しておく。作業依頼については、当該業務での作業依頼であることを明示した書面での依頼を行い、作業報告を行う。本件業務に係る委託事業者の契約は、ほぼ１社への随意契約（地方自治法施行規則 167 条の２第５号　緊急の必要）として締結されたものである。この背景には、B 社との長期間にわたる契約継続に伴う経験値の高さもあり、それが他事業体の参入を難しくしているベンダーロックインの１つの要因となっている。再委託・再々委託の問題とともに、本報告書における提言だけでは本質的解決策の提示は困難であり、今後抜本的な検討を行い方針を打ち出す必要がある。

5　再発防止に向けた提言

尼崎市役所全体の個人情報の安全管理措置及び情報セキュリティ対策の向上へ向けた中長期的事項の提言は以下のとおりである。

(1) 情報セキュリティガバナンスの構築

情報セキュリティガバナンス、さらにはコンプライアンス違反やミスの防止など、地方公共団体の業務を確実に推進できる体制が機能していない。総務省が提示している情報セキュリティポリシーガイドラインをベースに作成された市の情報セキュリティポリシーや情報セキュリティ対策基準が実際に機能するように、情報セキュリティ制度や情報セキュリティを確保するための組織体制等の抜本的な見直しが必要である。対策基準が定めた各責任を意識するために、職員研修だけでなく、各責任者への研修の実施を進める。

情報セキュリティポリシーや個人情報保護制度に基づき、確実に運用されているか定期的な監査だけでなく、必要に応じて委託事業者の遵守状況も含めた監査を実施する。

改正個人情報保護法が令和 5 年 4 月に地方自治体に適用されることが決定している。尼崎市個人情報保護条例と改正個人情報保護法の過不足を解消するための見直しが令和 5 年 3 月末までに必要とされている。

(2) 規定を実際に遵守していることの裏付け取得を意識した契約事務の見直し

契約事務における仕様書には、業務内容のほか、個人情報の安全管理措置および情報セキュリティに関する事項が含まれている。これらが単なるひな形として扱われることなく、当該業務に適合しセキュリティ上漏れがなく契約文言上十分であることを契約締結前に事前検証できる仕組みを構築する必要がある。契約に当たり、個人情報に関する安全管理措置が十分備わっているか、契約の履行に際し、再委託、再々委託など業務の体制が実際に伴っているかの確認は必須であり、定期的にいつどのような作業を実施するか作業スケジュールを策定して確かめ、市職員の立ち会い、業務委託完了までの関与など、契約事務における発注者側の対応を企画する者の研修が必要である。また、情報システムに関係する契約の場合、業務主幹課と情報政策課との役割や連絡など、契約中の責任の所在を明確にする必要がある。

(3) 個人情報保護制度における安全管理措置研修の実施

尼崎市個人情報保護条例を理解し、個人情報に対する安全管理措置を適切に実行できるように、個人情報保護制度を理解するための研修の実施が必要である。令和 5 年 4 月から、個人情報保護法に基づく新しい個人情報保護条例に移行することが予定されている。新制度に対する安全管理措置に対するガイドラインが個人情報保護委員会から公表されている。同ガイドラインに沿った新しい尼崎市の規程に沿った対応が求められるので、市職員への周知が必要である。

(4) 個人番号制度研修の実施

今回の事故を起こした業務については、マイナンバー利用事務として、個人情報保護評価書を作成し公開されている。しかし、業務に携わる職員の意識の中にマイナンバー利用事務であるという意識が薄かったと考えられる。マイナンバー利用事務に携わる者に対しては、

番号制度の安全管理措置研修とサイバーセキュリティ研修の定期的な受講が義務づけられているため、改めて、番号制度に関する研修を実施し、番号制度に求められている安全管理措置を実施できるようにする。

(5) 情報セキュリティ研修

情報セキュリティ研修は毎年実施されているが、全職員に受講できる機会をあたえるとともに、受講状況を確認し必ず受講するように指導する。特に、人事異動などで新たに業務に携わる職員等に対し、個人情報保護制度及び番号制度並びに情報セキュリティに対する研修を経たうえで業務に携わるようにする必要がある。全国で発生している情報セキュリティの事件事故から、自分たちの組織で同じような事件事故を起こさないためにどうすべきか、職員自ら考える習慣を確立する。市の業務を受託した委託事業者も、市の業務を実施する上でのセキュリティ対策を遵守する。所属会社における一般的な情報セキュリティ研修だけではなく、市の業務における現場的なセキュリティ対策を理解してもらう必要があるので、市の研修に委託事業者を参加させ、今回のような事故が起こらないよう、現場の実際を踏まえたチームディスカッション等を行い、セキュリティ意識を確実に向上させ、研修の実が上がる工夫をする。情報セキュリティ対策においては、派遣・請負契約における指揮・命令系統は関係のないことであり、受講を促す方向で考えていただきたい。情報セキュリティに対する脅威や必要な対策は日々変化しており、情報セキュリティ対策の見直しが常に求められている。総務省の情報セキュリティポリシーガイドラインについても、この 3 年では毎年改訂されており、直近では令和 4 年 3 月に改訂されている。本年度も改訂が予定されており、各自治体における情報セキュリティポリシーの適時の見直しが求められている。情報セキュリティポリシーは、組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書であり、組織におけるルールブックである。この情報セキュリティポリシーを常に見直すとともに職員に確実に周知する体制を整えていただきたい。