第２段階調査報告書（公表版）

県保有情報漏えいの指摘に係る調査に関する
第三者調査委員会

委員長　　弁護士　工　藤　　涼　二

委員　　弁護士　中　村　　真

委員　　弁護士　李　　延　壮

補助委員　　弁護士　辻　　のぼる

はじめに

インターネットでの動画配信及びＳＮＳ並びに報道において、兵庫県（以下「県」という。）が保有していたと思われる情報であって外部へ漏えいした可能性が指摘されるもの（以下「ネット情報」という。）が複数存在するとともに、動画配信者が、ネット情報の外部への持出は公益通報者保護法（平成１６年法律第１２２号）において不利益な取扱が禁止される公益通報に該当するとの主張を行っていること（以下「本件事案」という。）から、兵庫県及びその組織・職員から独立した中立・公正な弁護士及び委員長によって選任された１名の補助委員から構成される当委員会は、令和７年１月７日、兵庫県より依頼を受け、「県保有情報漏えいの指摘に係る調査に関する第三者による調査実施要綱」（以下「本件要綱」という。）に基づき、本件要綱別表に掲げるネット情報に関して、調査にあたってきた。

第１段階調査報告書のとおり、本件要綱第２条１項１号に定める「第１段階調査」のアについては情報の同一性が認められ、同イについては公益通報に該当するとは認められなかったことから、当委員会は、同条２項に従い、同条１項２号の「第２段階調査」にあたることとなった。

本調査報告書は、同号の、

ア　ネット情報の外部への漏えいが、県職員によるものであるか、又は外部の者によるものであるかの調査、

イ　ネット情報の外部への漏えいの原因、背景及び方法並びに県における情報管理の現状等の調査

について、その調査結果をまとめたものである。

目　　次

（本調査報告書の目次であり、公表版のものではない。）

調　査　の　結　論

1　ネット情報の外部への漏えいが、県職員によるものであるか、又は外部の者によるものであるか。

県人事課の情報管理にかかるセキュリティシステム上及び同システムの運用上、いくつかの重大な脆弱性があり、漏えい者、漏えい経路ともに複数の可能性が存在することが判明したことから、現時点では究明には至らなかった。

2　ネット情報の外部への漏えいの原因、背景及び方法並びに県における情報管理の現状等の調査

セキュリティシステム運用上の脆弱性に加えて、USB メモリの利用方法等に初歩的な誤りが見受けられ、これが外部漏えいの原因ないし背景となっている。

これらは、一定のセキュリティシステムを構築したことでセキュリティ対策が万全であるという慢心により起こったものと推測されるところ、早急に適正かつ有効な改善策を講じるとともに職員の一層の意識改革が必要である。

結論に至る理由

第１　県庁のネットワーク・ＰＣ端末の概要

１　県庁のネットワークは、インターネットからの接続をファイアウォール及びプロキシサーバによって保護された構成となっており、外部からの不正アクセスを遮断し、内部ネットワークのセキュリティを確保している。ファイアウォール及びプロキシサーバを経由し、各部署で使用される公用ＰＣなどが接続されている。

２　職員のメールは、プロキシサーバを経由する際に、ログが取得され、履歴が残るようになっており、職員が公用ＰＣ上でメールを削除しても、ログは削除されないようになっている。また、プロキシサーバには、あるフィルタリングアプリが導入されており、外部のＷＥＢメールを使用できない設定にしているほか、外部にファイルをアップロードする際には、上長の許可が必要となっている。

３　公用ＰＣの大部分を占める端末はセキュリティ強化等を目的としたソフトウェアによる監視がなされ、操作の履歴がそこに残るようになっている。

４　人事課では、人事課で共有するデータファイルを、特定のファイルサーバに保存している。本件に関するデータファイルは、同ファイルサーバ内の【副課長のフォルダ】以下のフォルダ及びもう一つのフォルダ（フォルダ名省略）に保存されていた。また、年度替わりの時期に、同ファイルサーバ内の【処分関係】以下のフォルダにコピーされている。さらに、本件に関するデータは、アクセス権限を細かく設定するために、ある時期に、別のファイルサーバ内の【テスト】以下のフォルダに移動されている。

※以下の報告については、現時点で公表するのは相当ではないので割愛する。

第２　調査対象について

第一段階調査において、ネット情報と県保有情報の同一性が認められており、ネット情報の外部への漏えいの調査は、下記の県保有情報のデータ（一部は未特定）の漏えいの調査である。

記

１　令和６年８月２３日付け週刊文春電子版で報道された令和６年３月２５日の片山元副知事による元西播磨県民局長事情聴取の音声データ

ファイル名：「240325　事情聴取①（省略）.mp3」

２　令和６年８月２８日付け週刊文春電子版で報道された令和６年３月２５日の調査実施手順書（３班体制）の内容

ファイル名：「240325 調査実施手順（3 班体制）.docx」

３　令和６年８月３０日付け週刊文春電子版で報道された令和６年２月１２日付け及び同月１３日付けある職員の転出先候補資料

ファイル名：「240212 転出先候補.docx」「240213 転出先候補.docx」

４　令和６年９月１日付け週刊文春電子版で報道された①令和６年３月２６日付け元西播磨県民局長処遇と今後の調査方針案，②（ア）同月２７日の記者レク結果、（イ）知事定例記者会見想定ＱＡ，（ウ）斎藤知事が自ら作成したメモ

① ファイル名：「240326　今後の調査方針.docx」

②（ア）ファイル名：「240327　事前の記者レク結果.docx」

（イ）ファイル名：「240327　知事会見：想定ＱＡ（西播磨県民局長交代）.docx」

（ウ）ファイル名：「240327　知事会見：知事コメント（事前に知事作成）.pdf」

５　令和６年９月２日付け週刊文春電子版で報道された①３月 27 日の元西播磨県民局長辞令交付時の音声データ並びに当時の様子及び発言に関するメモ，②３月 28 日の元西播磨県民局長が職員局長に送ったメール（写真），③３月 27 日のさわやか提案箱投書

① ファイル名：「240327　辞令交付（省略）.MP3」「240327　辞令交付（省略）.docx」

② ファイル名：「240328　メール（省略）.jpg」

③ ファイル名：「240327（21 時 54 分）さわやか提案箱-不明様-.pdf」

６　令和６年９月４日付け週刊文春電子版で報道された令和６年４月２日

付けアイアン経緯報告書

ファイル名：「240402　省略：調査結果.docx」

７　令和６年１１月２９日Ａ氏のYouTube及びＸに投稿された元西播磨県民局長の公用ＰＣ内の私的情報（フォルダ名及びファイル名が表示されたもの）

ファイル名：未特定

８　令和６年１１月３０日Ｂ氏のYouTube及びＸに投稿された元西播磨県民局長の公用ＰＣ内の私的情報（フォルダ名及びファイル名が表示されたもの）

ファイル名：未特定

９　令和６年１２月１日Ａ氏のＸに投稿された元西播磨県民局長の公用ＰＣ内の私的情報（ファイルの内容が表示されたもの）

ファイル名：「201122715180000.jpg」

10　令和６年１２月１１日Ｂ氏のYouTubeに投稿された元西播磨県民局長の公用ＰＣ内の私的情報（ファイル名及びフォルダ名並びにファイルのプロパティが表示されたもの）

ファイル名：未特定

第３　調査方法について

１　すでに述べたとおり、県においては、公用ＰＣの監視のためのソフトウェアを導入しており、公用ＰＣのうちの多くのＰＣにおけるファイル操作の履歴が保存される仕組みになっている。そこで、当委員会としては、上記３の調査対象のデータファイルのうち、ファイル名が特定しているものについては、ファイル名をもとに、ＵＳＢメモリなどの履歴、人事課共有フォルダへのアクセス、並びに、データにアクセス可能であった人事課職員、片山元副知事、Ｃ氏、Ｄ氏、及び、元西播磨県民局長の公用ＰＣにおける操作の履歴を調査する[1]とともに、これらの者のメールの履歴を調査す

[1]　調査対象者を４７名、調査対象期間を令和６年３月２５日から同年１１月２９日までとしたが、一人当たりのログが、１行５４列の数十万行から１３０万行程度と膨大

ることとした。

2⑴　もっとも、上記３の調査対象のデータファイルのうち、文書データ（ファイル拡張子が docx 及び pdf のもの）については、印刷物がコピーされて漏えいした可能性及び上記ソフトウェアの監視の及ばない方法で取得した可能性があり、これらの方法については、上記の調査方法では確認できないことから、これらの方法による情報漏えいの可能性を指摘するにとどめる。

⑵　また、上記３の調査対象のデータファイルのうち、音声データについては、マイク端子から別のレコーダーに録音した可能性があり、この方法については、上記の調査方法では確認できないことから、この方法による情報漏えいの可能性を指摘するにとどめる。

⑶　さらに、上記３の調査対象のうちの⑺から⑽までの元西播磨県民局長の公用ＰＣ内の私的情報については、上記ソフトウェアの監視の及ばない方法で取得した可能性があるが、この方法については、上記の調査方法では確認できないことから、この方法による情報漏洩の可能性を指摘するにとどめる。

⑷　これらに加えて、現時点では、上記ソフトウェアの監視がないＰＣを利用した方法による情報漏洩の可能性を指摘するにとどめる。

⑸　以上のほかにも、データ全般において、ＵＳＢメモリから公用ＰＣにデータをコピーした後もＵＳＢメモリにデータが残ったままの場合があり、録音データについては、ＵＳＢメモリだけでなく、ＩＣレコーダー上にもデータが残ったままの場合があることが判明していることから、これらが私的なＰＣに接続されて情報漏えいした場合もログが残らないため、この方法による情報漏洩の可能性を指摘するにとどめる。

３　以上のとおり、本件調査方法では確認できない様々な情報漏えいの可能性が存在することが判明したが、次に記載のとおり、調査を進めたので、調査結果を説明する。

であったことから完全目視ではなく、キーワード検索を行ったうえで関連部分を目視で詳細に確認する方法をとっている。

第４　各データファイルの調査結果

前項に記載した調査を行った結果について、県においてシステム上の対処が十分にできていない現時点においてその詳細を公表することは相当ではないと思われるので、差し控える。

第５　問題点の整理と改善策

１　問題点

以上で述べてきた情報セキュリティ上の問題点についても、県においてシステム上の対処が十分にできていない現時点においてその詳細を公表することは相当ではないと思われるので、差し控える。

２　改善策

上記の問題点についての改善策についても、県においてシステム上の対処が十分にできていない現時点においてその詳細を公表することは相当ではないと思われるので、差し控える。

第６　本報告書の公表方法 及び 時期について

１　以上で述べた県庁ネットワークの情報セキュリティ上の問題点と改善策については、情報漏えいの原因を公表することにより、当該脆弱性を利用したさらなる情報漏えいを誘発する危険性があり、また、改善策には限界があり、必ずしも完全なものではないことから、改善策を明らかにすることにより、改善策の脆弱性を研究される危険性があることから、本報告書の公表方法、及び、時期については、慎重に検討する必要がある。

２　そこで、下記のように２段階で報告書を公表することを提案する。

記

第１段階：改善策の実施前は、脆弱性や改善策は伏せた限定的な公開を行う。

※今回の公表は、この段階として行われたものである。

第２段階：改善策の実施完了後は、脆弱性や改善策を抽象化したうえで公開を行う。

３　なお、改善策を実施したとしても、完全に安全になるわけではなく、「継続的にセキュリティ対策を強化していく」という姿勢が重要である。

本件においては、セキュリティ上の初歩的な誤りが見受けられるが、これらは、上記ソフトウェアの導入など、一定のセキュリティシステムを構築したことでセキュリティ対策が万全であるという慢心により起こったものと推測できる。

したがって、上記の改善策の実施が完了した後も、定期的な点検、及び、さらなるセキュリティ強化の検討が必要である。

以上

※資料については、セキュリティ上の観点から添付を見合わせる。