




宮監公表第 18 号
令和 3 年 3 月 25 日

宮崎市監査委員	河	野	まつ	子
宮崎市監査委員	荒	木	敏	
宮崎市監査委員	上	野	悦	男
宮崎市監査委員	嶋	田	喜代	子



令和 2 年度行政監査結果の公表について

地方自治法第199条の規定に基づく行政監査の結果を次のとおり公表します。

令和 2 年度

行政監査報告書

外部記憶媒体（USBメモリ）の管理状況について

宮崎市監査委員

目 次

第1	種類	1
第2	対象	1
第3	着眼点	1
第4	主な実施内容	2
第5	日程	2
第6	意見	3
1	監査対象課の状況	3
2	情報政策課の状況	4
3	情報セキュリティの周知状況	5
4	まとめ	5
第7	結果	6
1	監査対象課の状況	6
2	情報政策課の状況	8
3	情報セキュリティの周知状況	8

参考資料

〔凡例〕

- 1 文中及び表中に記載した数値は、対象部局から提出された調査表の回答に基づき作成した。
- 2 文中の比率は、小数点第2位を四捨五入して小数点第1位まで表示した。従って、比率の合計と内訳が一致しない場合がある。
- 3 「ネットワーク機器に係るセキュリティ実施手順書」や「電算システム運用及び端末等の取り扱いについて」の通知、「USBメモリー接続申請書」等では「USBメモリ」と「USBメモリー」の表記が混在して用いられているため、文中の表記は、「USBメモリ」に統一した。
- 4 「室」「センター」「事務局」「署」は、「課」と読み替えた。
- 5 「室長」「センター長」「次長」「署長」は、「課長」と読み替えた。

第1 種類

地方自治法第199条第2項に基づく行政監査

第2 対象

1 テーマ

「外部記憶媒体（USBメモリ）の管理状況について」

2 目的

市が取り扱う情報には、個人情報や機密情報等、改ざんや外部への漏えいなどが発生した場合に極めて重大な影響を及ぼす情報が多数含まれており、市は、これら保有する情報の正確性や安全性の確保のため、適切に保護し、管理する責任がある。

USBメモリは利便性が高く容易に購入できることから、ネットワーク端末に接続できる周辺機器として全庁的に使用されているが、全国においては個人情報を含んだUSBメモリを紛失するなどの事件が起きている。

また、本市では今年度から内部統制制度が導入され、その方針に情報管理に関する事務が盛り込まれ、USBメモリに関するリスクの具体例として、ウイルス感染や紛失による個人情報の漏えい等が示されている。

このような中、各課が管理保有するUSBメモリについて管理状況の実態を監査することにより、重要な情報に関する不祥事を未然に防ぎ、今後の適正な事務の執行に資することを目的とする。

3 対象部局

市長部局、行政委員会事務局（教育委員会は学校を除く）、消防局、上下水道局

第3 着眼点

監査に当たっては、監査対象課及び情報政策課を対象に、次の着眼点に沿って実施した。

1 監査対象課の状況

(1) USBメモリの申請について

①課内で使用するUSBメモリについて、情報政策課へ申請を行っているか。

(2) USBメモリの管理について

①USBメモリの数・使用者について確認を行っているか。

②USBメモリの廃棄処理等は適正に行われているか。

(3) USBメモリの保管について

①USBメモリは適切に保管されているか。

(4) 情報セキュリティの周知について

①情報セキュリティについて職員への周知が図られているか。

2 情報政策課の状況

(1) 全庁的なUSBメモリの使用について

①定期的に各課のUSBメモリの使用状況について、実態を把握しているか。

(2) 研修・周知について

①情報セキュリティに関する研修において、USBメモリの取扱いや情報セキュリティに関して、最新情報の周知を行っているか。

第4 主な実施内容

USBメモリの管理状況等について、調査表を用いて調査を行い、必要に応じて関係職員の事情聴取を行った。

第5 日程

令和2年11月20日から令和3年3月23日まで

第6 意見

本市のUSBメモリを含む電磁的記録媒体の適正な管理については、「宮崎市情報セキュリティポリシー」（以下「セキュリティポリシー」という）及び「ネットワーク機器に係るセキュリティ実施手順書」（以下「実施手順書」という）に規定している。

また、USBメモリについて、「外部媒体（USBメモリ）の取り扱いについて」（平成27年5月20日 宮情第92号）及び「電算システム運用及び端末等の取り扱いについて」（令和元年5月30日 宮情第65号）の通知により、各課において購入や廃棄等があった際には情報政策課へ「USBメモリ接続申請書」（以下「申請書」という）を提出するとともに、適正な運用と管理の徹底を促している。

今回の行政監査では、重要な情報に関する不祥事を未然に防ぎ、今後の適正な事務の執行に資することを目的として、庁内のUSBメモリの管理状況について監査を行った。

調査の結果については後述するが、次のとおり検討を要する事項が見受けられたことから項目ごとに意見を述べる。

1 監査対象課の状況

(1) USBメモリの申請状況について

情報政策課は、各課において購入したUSBメモリについては、情報政策課へ申請するように周知しているが、上下水道局においては、情報政策課ではなく上下水道局総務課へ申請していた。このことについての意見は後述することとする。

調査の結果、各課が情報政策課又は上下水道局総務課へ申請していたUSBメモリの数は3,876個であった。そのうち実際に保有していたのは3,267個（84.3%）であり、609個（15.7%）は保有していなかった。申請したまま保有していなかった609個については、すでに廃棄したものが458個（75.2%）、他課への転出者が所有しているものが13個（2.1%）、その他138個（22.7%）であった。その他138個の中には、所在不明のものが58個（42.0%）、個人所有のものが2個（1.4%）含まれていた。

すでに廃棄したものについては、USBメモリの廃棄申請が疎かになっていたものであることから、廃棄後は速やかな事務処理を徹底されたい。

所在不明のものについては、人事異動等に伴う変更時の申請が疎かになっていたものであり、紛失及び盗難による情報漏えいにつながる極めて重大な事案であることを認識し、原因究明に努めるとともに、今後は、保有数の定期的な確認を徹底するよう努められたい。

個人所有のものについては、持ち帰りによる私物パソコンへの接続によるウイルス感染や紛失及び盗難による情報漏えいのリスクが懸念される。「実施手順書」においては、いかなる理由であっても個人所有の機器は、ネットワーク端末に接続してはならないとされており、早急に是正する必要がある。

また、申請せずに保有していたUSBメモリが122個であったが、本市のネットワーク端末は、一部の個人番号利用系の端末を除き、システム上の制限がかけられてい

ないため、申請の有無に関係なく接続が可能であることから、各課において購入したUSBメモリはすべて申請し、管理を徹底されたい。

(2) 申請しているUSBメモリの管理状況について

① USBメモリの保有数・使用者の確認、廃棄処理について

情報政策課は、USBメモリの管理について、申請番号を貼付し使用者を含め管理の徹底を行い、廃棄する際はデータを消去し復元不可能な状態にするように各課へ依頼している。

令和2年度にUSBメモリの保有数・使用者の確認を行っていた課は、全課101課のうち97課であったものの、実際には申請したまま保有していなかったUSBメモリが609個あったことから、確認の方法について検討されたい。

申請番号を貼付し管理することについては、申請し保有していたUSBメモリ3,267個のうち3,236個(99.1%)が適切に行われており、概ね良好であった。

また、USBメモリを廃棄する方法については、廃棄した実績のある43課のうち42課が復元不可能な状態にしており、概ね良好であった。

② USBメモリの保管場所について

申請し保有していたUSBメモリ3,267個のうち、使用者の机で保管されていたものが2,757個(84.4%)であった。

また、保管場所が施錠されていたものは278個(8.5%)であった。

USBメモリは小型軽量で利便性が高く保管場所を選ばないことから、多くが使用者の机で保管されていたが、使用者が外部へ持ち出すことも容易になり、私物パソコンへの接続によるウイルス感染や紛失及び盗難による情報漏えいのリスクが懸念されるため、保管場所が適切かを確認するとともに施錠の必要性について検討されたい。

2 情報政策課の状況

情報政策課によると、庁内のUSBメモリの使用状況を把握し、個人所有のUSBメモリの使用を抑止するため、「申請書」による運用を導入したとのことであった。

しかし、現状では、上下水道局各課の「申請書」については、上下水道局総務課が集約しており、情報政策課は、上下水道局の申請状況について全く関知していなかった。さらに、情報政策課においては、上下水道局総務課との連携や情報共有はなく、申請の集計や実態調査等も行っておらず、全庁的な使用状況を把握する体制を整えていなかった。

また、「実施手順書」においては、USBメモリ等の周辺機器をネットワーク端末に接続する際は、規定されている「周辺機器接続申請書」により、情報政策課長に申請し、許可を受けなければならないとされているが、「申請書」による運用は「実施手順書」の規定に則しておらず、経緯や運用開始時期が不明であり、目的や取扱い基準を明確に示す規程等が十分に整備されないまま導入され、現在まで慣例的に引き継がれてきたものである。

一方、廃棄の際は、「申請書」による申請を行うように周知しているものの、同様

式は廃棄に対応したものではないため、廃棄申請の方法が曖昧な状況となっていた。

情報政策課においては、このような状況を早急に見直し、USBメモリにおける情報セキュリティ対策を十分検討し、実効性のある体制や規程等を整備されたい。

3 情報セキュリティの周知状況

情報セキュリティに関する研修について、情報化推進員・情報化推進リーダー又は情報化推進担当者、新規採用職員を対象に毎年実施されていたものの、情報セキュリティ管理者である課長を対象とした研修は実施されていなかった。

「セキュリティポリシー」によると、情報セキュリティ管理者は、その所管する情報資産について管理責任を有し、適切に保管しなければならないとされていることから、管理者としての自覚をもって職務を遂行するため、研修を行う必要がある。

また、情報政策課が実施した情報セキュリティに関する研修内容の周知については、各課において研修資料の供覧や個別研修を概ね実施していたものの、研修内容に含まれているUSBメモリの申請や管理等は徹底されていなかった。

このことから、実効性の伴う研修の充実により、職員のセキュリティへの意識向上を図るとともに、「セキュリティポリシー」等の周知徹底に努められたい。

4 まとめ

本市では、今年度から内部統制制度が導入され、「宮崎市内部統制に関する方針」に、内部統制の対象とする事務として、財務に関する事務のほかに、市長が管理及び執行が法令に適合し、かつ、適正に行われることを特に確保する必要があると認める事務として「情報管理に関する事務」を加えている。その中で、情報セキュリティリスクのひとつとして、USBメモリ等の外部記憶媒体でデータを授受する際のウイルス感染を挙げ、重要性の高いリスクと位置づけ、対応策を整備している。

しかしながら、今回調査した結果、必要以上に多くのUSBメモリを保有しており、申請されていたUSBメモリの中には所在不明になっているものや個人所有のものが含まれていた。これは、USBメモリの利便性が優先され、紛失及び盗難による情報漏えいのリスクに対する危機管理意識が希薄になっていることが原因と考えられる。情報セキュリティに関する事故が発生する可能性が高まっていることを、職員一人ひとりが強く認識されたい。

なお、現在庁内では、全庁共有ファイルサーバ内で各課ごとのデータ管理が可能となっていることから、組織や業務内容に応じたUSBメモリの必要性について早急に検討されたい。

また、情報政策課においては、「セキュリティポリシー」の全庁的な遵守状況について定期的に自己点検を行い、USBメモリを含む情報セキュリティ対策のレベル向上に努められたい。

今回の監査結果が、情報管理リスクの低減を図り、情報セキュリティの確保と職員の危機管理意識の向上につながることを望むものである。

第7 結果

1 監査対象課の状況

(1) USBメモリの申請状況について

情報政策課は、各課で購入したUSBメモリについて、申請番号と型番を記載した「申請書」にて情報政策課へ申請するように各課へ周知しているが、上下水道局においては、情報政策課ではなく上下水道局総務課へ申請していた。

調査の結果、各課が情報政策課又は上下水道局総務課へ申請していたUSBメモリの数は3,876個であった。このうち実際に保有していた数は3,267個(84.3%)であり、申請したまま保有していなかった数が609個(15.7%)であった。

また、申請せずに保有していたUSBメモリは122個であった。

一方、情報政策課は、USBメモリを廃棄する際も「申請書」により申請するよう求めているが、同様式は廃棄申請に対応したものではなかった。

申請状況

(単位:個)

部局等	申請していた数			申請していなかった数	
	保有していた数 ①	保有していなかった数 ②	計 (①+②)		
企画財政部	6課	94	7	101	1
総務部	5課	162	78	240	0
危機管理部	2課	32	8	40	0
税務部	5課	97	11	108	0
地域振興部	10課	326	98	424	27
環境部	3課	146	10	156	0
福祉部	6課	272	135	407	12
子ども未来部	3課	223	15	238	1
健康管理部	4課	338	5	343	2
農政部	5課	136	17	153	0
観光商工部	4課	80	18	98	2
建設部	4課	150	8	158	41
都市整備部	7課	198	46	244	0
佐土原総合支所	2課	69	21	90	0
田野総合支所	2課	57	1	58	0
高岡総合支所	2課	74	0	74	0
清武総合支所	2課	73	1	74	0
会計管理者	1課	13	0	13	0
議会事務局	2課	23	1	24	0
選挙管理委員会事務局	1課	23	2	25	0
監査委員事務局	1課	23	0	23	0
農業委員会事務局	1課	29	3	32	0
教育委員会事務局	7課	243	11	254	36
上下水道局管理部	4課	62	17	79	0
上下水道局水道部	4課	154	6	160	0
上下水道局下水道部	2課	80	87	167	0
消防局	6課	90	3	93	0
合計(27部局)	101課	3,267	609	3,876	122

申請したまま保有していなかった 609 個のうち、すでに廃棄したものが 458 個 (75.2%)、他課への転出者が所有しているものが 13 個 (2.1%)、その他 138 個 (22.7%) であった。その他 138 個の中には、他課へ移管していたものが 77 個 (55.8%)、所在不明のものが 58 個 (42.0%)、個人所有のものが 2 個 (1.4%) 含まれていた。

申請したまま保有していなかった理由

(単位:個)

廃棄 ①	他課への 転出者が所有 ②	その他 ③	その他の内訳				計 (①+②+③)
			他課へ移管	所在不明	個人所有	申請誤り	

(2) 申請している USB メモリの管理状況について

情報政策課は、申請した USB メモリについて、申請番号を貼付し使用者を含め管理の徹底を行い、廃棄する際はデータを消去し、復元不可能な状態にするように各課へ依頼している。

申請し保有している USB メモリ 3,267 個の管理状況は次のとおりであった。

① USB メモリの保有数・使用者の確認について

令和 2 年度に保有数・使用者の確認を行っていた課は、全課 101 課のうち 97 課であった。

保有数・使用者の確認状況(令和2年度)

(単位:課の数)

確認を行っていた課	確認を行っていなかった課	計
97	4	101

また、申請番号を貼付し管理していたものは、3,236 個 (99.1%) であった。

申請番号の貼付状況

(単位:個)

申請番号を貼付していた	申請番号を貼付していなかった	計
3,236	31	3,267

USB メモリの廃棄については、廃棄実績があった 43 課のうち、データを消去のうえ復元不可能な処理を行っていた課は 42 課であった。

廃棄実績があった課の廃棄処理状況

(単位:課の数)

データを消去のうえ復元不可能な処理をしていた	データを消去のうえ復元不可能な処理をしていなかった	計
42	1	43

②USBメモリの保管場所について

USBメモリの保管場所については、使用者の机が2,757個(84.4%)、キャビネットが268個(8.2%)、その他の場所が242個(7.4%)であった。その他の場所には課長補佐の机や金庫等があった。

保管場所

(単位:個)

使用者の机	キャビネット	その他	計
2,757	268	242	3,267

施錠については、保管場所を施錠していたものは278個(8.5%)であった。

保管場所の施錠状況

(単位:個)

施錠していた	施錠していなかった	計
278	2,989	3,267

2 情報政策課の状況

情報政策課は、各課で購入したUSBメモリを「申請書」にて情報政策課へ申請するように各課へ周知しているが、上下水道局においては、情報政策課ではなく上下水道局総務課が申請を集約しており、このような体制になった経緯は不明であった。情報政策課においては、上下水道局総務課との連携や情報共有はなく、これまで全庁的な申請の集計や実態調査等は行っていなかった。

また、「実施手順書」においては、USBメモリ等の周辺機器をネットワーク端末に接続する際は、規定されている「周辺機器接続申請書」により情報政策課長に申請し、許可を受けなければならないとされているが、「申請書」による運用はこれに則したものではない。情報政策課によると、「申請書」による運用の導入の目的は、庁内のUSBメモリの使用を把握し、個人所有のUSBメモリの使用を抑止するためであるとのことであったが、それを明記した規程等はなく、経緯や運用開始時期は不明であった。

3 情報セキュリティの周知状況

情報政策課は、各課の情報化推進員・情報化推進リーダー又は情報化推進担当者の中で未受講者を優先し、各課1名を対象に年1回情報セキュリティに関する研修を実施していた。

各課においては、研修資料の供覧や個別研修により課員へ研修内容を周知していた。

そのほか、情報セキュリティに関する研修は新規採用職員を対象に実施していたものの、情報セキュリティ管理者である課長を対象に実施していなかった。

情報政策課による情報セキュリティに関する研修実績(全課対象)

実施年度	実施日	参加人数
平成27年度	7月8日	102名
平成28年度	6月24日	102名
平成29年度	5月24日	105名
平成30年度	5月25日	101名
令和元年度	5月30日	94名

情報セキュリティに関する研修の各課の周知状況(令和元年度)

(単位:課の数)

周知を行っていた課		周知を行っていなかった課
資料供覧	個別研修	
95	3	1

※令和2年度に新設された2課は除く

参 考 資 料

宮崎市情報セキュリティポリシー（抜粋）	1
外部媒体（USBメモリ）の取り扱いについて （平成27年5月20日通知）	5
電算システム運用及び端末等の取り扱いについて （令和元年5月30日依頼）	6
USBメモリ接続申請書	8

宮崎市情報セキュリティポリシー（抜粋）

第1章 情報セキュリティ基本方針

4. 適用範囲

（1）行政機関の範囲

本基本方針が適用される行政機関は、市長部局、行政委員会事務局、消防局、上下水道局、教育機関（事務室のみ）とする（以下、「部局等」という。）。

第2章 情報セキュリティ対策基準

2. 組織体制

（1）最高情報セキュリティ責任者（C I S O : Chief Information Security Officer、以下「C I S O」という。）

宮崎市の情報政策を担当する副市長を、C I S Oとする。C I S Oは、宮崎市におけ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最終決定権限及び責任を有する。

（2）統括情報セキュリティ責任者

- ①情報政策担当部長を、C I S O直属の統括情報セキュリティ責任者とする。統括情報セキュリティ責任者はC I S Oを補佐しなければならない。
- ②統括情報セキュリティ責任者は、宮崎市の全てのネットワークにおける開発、設定の変更、運用見直し等を行う権限及び責任を有する。
- ③統括情報セキュリティ責任者は、宮崎市の全てのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

（3）情報セキュリティ責任者

- ①市長部局の長、行政委員会事務局の長、消防局長、上下水道局長を情報セキュリティ責任者とする。
- ②情報セキュリティ責任者は、当該部局等の情報セキュリティ対策に関する統括的な権限及び責任を有する。
- ③情報セキュリティ責任者は、その所管する部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権限及び責任を有する。
- ④情報セキュリティ責任者は、その所管する部局等において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約及び職員等に対する教育、訓練、助言及び指示を行う。

（4）情報セキュリティ管理者

- ①課・室の長、地域センター長、行政委員会事務局の次長、消防局の課長、上下水道局の課長を、情報セキュリティ管理者とする。
- ②情報セキュリティ管理者はその所管する課室等の情報セキュリティ対策に関する

る権限及び責任を有する。

3. 情報資産の分類と管理方法

(2) 情報資産の管理

①管理責任

(ア) 情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。

⑥情報資産の保管

(ア) 情報セキュリティ管理者又は情報システム管理者は、情報資産の分類に従って、情報資産を適切に保管しなければならない。

4. 物理的セキュリティ

4. 4. 職員等のパソコン等の管理

①情報システム管理者は、執務時間外においては、執務室等の施錠管理やワイヤーによる固定等、パソコン等の盗難防止措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

5. 人的セキュリティ

5. 1. 職員等の遵守事項

(1) 職員等の遵守事項

②業務以外の目的での使用の禁止

職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

③モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

(イ) 職員等は、宮崎市のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。

(ウ) 職員等は、外部で情報処理作業を行う場合には、情報セキュリティ管理者の許可を得なければならない。

(エ) 職員等は、外部で情報処理作業を行う際は、情報セキュリティ管理者の許可を得た上で、安全管理措置を遵守しなければならない。

④支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

(ア) 職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、業務上必要な場合は、情報セキュリティ管理者の許可を得て利用することができる。

(イ) 職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、情報セキュリティ管理者の許可を得るものとし、外部で情報処理

作業を行う際には安全管理措置を遵守しなければならない。

⑤持ち出し及び持ち込みの記録

情報セキュリティ管理者は、端末等の外部への持ち出し及び外部からの持ち込みについて、記録を作成し、保管しなければならない。

⑦机上の端末等の管理

職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

⑧退職時等の遵守事項

職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

5. 2. 研修・訓練

(1) 情報セキュリティに関する研修・訓練

C I S Oは、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

(2) 研修計画の立案及び実施

①C I S Oは、幹部を含めすべての職員等に対する情報セキュリティに関する研修計画を定期的に立案しなければならない。

②研修計画において、職員等が情報セキュリティ研修を受講できるようにしなければならない。

③新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

④研修は、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者及びその他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

9. 評価・見直し

9. 2. 自己点検

(1) 実施方法

①統括情報セキュリティ責任者及び情報システム管理者は、所管するネットワーク及び情報システムについて、定期的又は必要に応じ自己点検を実施しなければならない。

②情報セキュリティ責任者は、情報セキュリティ管理者と連携して、所管する部局における情報セキュリティポリシーに沿った情報セキュリティ対策状況につい

て、毎年度又は必要に応じ自己点検を行わなければならない。

(2) 報告

統括情報セキュリティ責任者、情報システム管理者及び情報セキュリティ責任者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、宮崎市サンシャインネット推進委員会に報告しなければならない。

(3) 自己点検結果の活用

①職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

②宮崎市サンシャインネット推進委員会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

宮情第 92 号
平成27年5月20日

部 課 長
各 殿
委員会事務局長

総 務 部 長
(公 印 省 略)

外部媒体（USBメモリ）の取り扱いについて（通知）

平成25年4月25日付、宮情第23号におきまして、情報セキュリティ対策等の徹底について通知させていただき、適正な運用をお願いしているところです。

その中で、大容量の外部媒体については紛失・故障時のリスクが大きいことから容量を制限しておりましたが、業務の電算処理効率化のため、下記のとおり変更しましたのでご確認いただきますようお願いいたします。

記

USBメモリの容量について（8GB⇒16GBまで可）

- ・ 16GBを超えるUSBメモリは使用できません。
- ・ USBメモリを購入後は『USBメモリ接続申請書』の提出をお願いします。

【 注意事項 】

外部から持ち込まれたデータが主な感染経路となってウイルス感染事案が発生しています。パソコンや媒体の定期的なウイルスチェックを行ってください。

また、USBメモリの適切な管理を行うと共に、情報政策課に届出をしていない媒体の使用禁止を徹底してください。

【文書取扱】

総務部情報政策課
システム運用係
(内線2497)

部 課 長
各 殿
委員会事務局長

総 務 部 長
(情報政策課長)

電算システム運用及び端末等の取り扱いについて (依頼)

このことについて、所属職員に対し、下記内容の周知徹底をお願いいたします。

記

1. オンラインシステム等のパスワードの取り扱いについて

各業務システム (MICJET 住記・国保・年金、MICJET 税、THINKTAX、MCWEL 介護、MICJET 戸籍、福祉システム、住民基本台帳ネットワークシステム等) を利用するためのログイン ID とパスワードは、個人毎に貸与しています。

年度途中で取扱者の増減や変更が生じた場合は、メールで情報政策課代表あてに、業務システム端末取扱者登録依頼票を再提出してください。

貸与を受けた個人以外の者へ利用させたり、付箋等に記したログイン ID とパスワードを端末機やその周辺に貼り付ける等、不適切な利用のないようご注意ください。

2. ソフトウェアインストール・周辺機器接続・ネットワーク機器接続申請について

ネットワーク端末及びタブレット端末へのソフトウェアインストールやプリンタ等周辺機器の接続、NAS (ネットワークを通じ複数のユーザがアクセスできるハードディスク) のようなネットワーク接続機器等につきましては、事前に情報政策課へ許可申請書を提出してください。許可がおりましたら、端末設定作業 (タブレット端末を除く) は各課の情報推進担当者に行っていただきますようお願いいたします。

3. USB メモリーについて

USB メモリーについては、取り扱いに十分注意してください。使用する USB メモリーについて、容量は最大 16GBまでとします。

USB メモリーにテプラ等で番号を貼り、使用者を含め各課で、管理の徹底をお願いします。

また、各課で使用する USB メモリーの購入や廃棄等の変更があった際には、USB メモリー接続申請書の提出をお願いします。

なお、廃棄する際はデータを消去するだけでなく復元不可能な状態にして廃棄してください。

4. コンピュータウイルス対策について

外部媒体 (特に USB メモリー) によるコンピュータウイルスの感染が多発しています。

宮崎市情報セキュリティポリシー及びネットワーク機器に係るセキュリティ実施手順書を再度確認していただき、遵守していただきますようお願いいたします。

外部からの持ち込み、たとえば業者からの USB を持ち込まないといけない場合は、必ずインターネット端末において UTP ケーブル（青色のネットワーク線）を抜いた後に挿入し、ウイルススキャンを実施し、安全が確認できた後、作業を行ってください。

また、インターネットメールへ毎日新たな不審メールが多数送られて来ております。情報政策課にてフィルタリング等対策を講じていますが、防ぎきれずに各課端末で不審メールが受信されているのが現状です。

インターネットメールについてはこれまで以上に慎重に取り扱っていただき、送信者や本文の内容、添付ファイルの拡張子等不審点があれば開封せず、削除して下さい。

メール本文や添付データを庁内 LAN 端末へ移動させる場合、インターネット端末で USB メモリーをウイルススキャンする、メール本文をテキスト化する、添付ファイルを PDF 化する等、細心の注意をお願いします。

ウイルス感染が確認された際には、速やかに情報政策課までご連絡いただき、適正な処置をお願いします。なお、ウイルス検出後の対応及びウイルススキャンによってインターネットメールに文字化け等の不具合が発生した際の対応については、下記の部門フォルダ格納していますので、ご確認下さい。

【部門フォルダ>00.全庁>不審メール削除及び完全スキャンの実施手順】

5. インターネット端末での個人情報取り扱いについて

データ流出の可能性がありますので、インターネット端末でメール等を利用する際は、セキュリティポリシーに則り個人情報を取り扱わないようお願いします。

6. 端末機の取り扱いについて

不注意等により端末に飲み物等をこぼし端末の修繕や場合によっては、交換が必要となります。飲み物を端末の近くに置かないなど机上での飲食等にはご注意ください。

もし、不注意等により端末に飲み物等がこぼれた場合には、原課判断で対処することなく、電源を切り、速やかに情報政策課までご連絡いただき適正な処置を行ってください。

庁内 LAN 端末等をレイアウト変更や席替え等により、初期配布場所とは異なった場所で利用される場合は、設定変更・工事等が必要なこともありますので、お早めに情報政策課へご相談ください。

1. 2. 3. の申請書は、【部門フォルダ>00.全庁>情報政策課関係書式】を参照してください。

文書取扱：情報政策課 情報政策係

内線：(70)2491

直通：21-1712

令和 年 月 日

USB メモリー接続申請書

宮崎市行政情報ネットワークのネットワーク端末へのUSBメモリーの接続を下記のとおり申請します。

記

所属 _____ 課

No	型番	No	型番
1		26	
2		27	
3		28	
4		29	
5		30	
6		31	
7		32	
8		33	
9		34	
10		35	
11		36	
12		37	
13		38	
14		39	
15		40	
16		41	
17		42	
18		43	
19		44	
20		45	
21		46	
22		47	
23		48	
24		49	
25		50	

※USBメモリーには、テプラ等を貼るなど適正な管理をお願いします。