

平成27年度

監査結果報告書

行政監査

(外部記憶媒体(USBメモリ)の管理状況について)

大分市監査委員



監査第1080号

平成28年3月14日

大分市長 佐藤樹一郎 殿
大分市議会議長 永松弘基 殿

大分市監査委員 佐藤 浩

大分市監査委員 古庄 研二

大分市監査委員 安東 房吉

大分市監査委員 仲家 孝治

監査の結果について（報告）

行政監査を実施したので、地方自治法第199条第9項の規定によりその結果に関する報告を次のとおり提出します。

目 次

第1	監査の種類	1
第2	監査のテーマ	1
第3	監査の目的	1
第4	監査の対象	1
第5	監査の期間	1
第6	監査の方法	1
第7	監査の着眼点	2
第8	監査の結果	2
	(1) USBメモリの取扱い基準等について	2
	(2) USBメモリの管理状況等について	2
	(3) まとめ	5
別表1	USBメモリ登録状況	6
別表2	USBメモリ保管状況	7
別表3	暗号化機能付きUSBメモリの使用状況	9
資料		11

(注)

1. 「大分市情報セキュリティ対策基準」や「情報セキュリティ実施手順」、
「大分市USBメモリ取扱いルール」等では、「記憶媒体」と「記録媒体」の
表記が混在して用いられているため、文中の表記は、「記憶媒体」に統一した。
2. 統括情報セキュリティ責任者・・・「情報政策課長」
情報セキュリティ責任者・・・「課等の長」

第1 監査の種類

行政監査（地方自治法第199条第2項）

第2 監査のテーマ

外部記憶媒体（USBメモリ）の管理状況について

第3 監査の目的

市が取り扱う情報には、市民の個人情報や行政運営上重要な情報等、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を適切に保護し、管理する責任がある。

今回、各課等が管理保有する情報を処理する際に使用している外部記憶媒体（USBメモリ）について、管理状況及び活用状況等の実態を監査することにより、今後の適正な事務の執行に資することを目的とする。

第4 監査の対象

（1）対象部局

市長事務部局

（2）対象範囲

大分市情報セキュリティ対策基準に規定する外部記憶媒体（USBメモリ）のうち、平成27年9月30日現在、全庁ネットワークシステム（以下「全庁システム」という。）で使用するため保有しているもの

第5 監査の期間

平成27年9月30日から平成28年2月29日まで

第6 監査の方法

各課等から提出された「USBメモリ管理状況調査表」（以下「調査表」という。）と全庁システムで管理しているUSBメモリ登録データを突合し、その内容を検証するとともに関係職員から説明を求めた。

第7 監査の着眼点

- (1) 外部記憶媒体（USBメモリ）について適正な管理が行われているか
- (2) 外部記憶媒体（USBメモリ）の使用制限は守られているか
- (3) 外部記憶媒体（USBメモリ）の外部への持ち出し方法は適切か

第8 監査の結果

- (1) USBメモリの取扱い基準等について

本市のUSBメモリ等の外部記憶媒体の適正な管理については、「大分市情報セキュリティ対策基準」（以下「基準」という。）及び「情報セキュリティ実施手順」に規定されており、なかでもUSBメモリについては、情報セキュリティ事故の発生を防止することを目的に、「大分市USBメモリ取扱いルール」（以下「取扱いルール」という。）が平成25年1月に定められている。

また、平成26年4月4日付「全庁ネットワークにおける外部記憶媒体の管理について」（以下「通知」という。）により、所属長が管理・保管しているUSBメモリ等の外部記憶媒体について、平成26年5月以降、登録された媒体のみ全庁ネットワークシステム端末（以下「システム端末」という。）で使用可能としており、情報セキュリティの向上を図っている。

この通知により、システム端末でUSBメモリ等外部記憶媒体を使用する場合、情報セキュリティ責任者である所属長は外部記憶媒体等使用報告書を統括情報セキュリティ責任者に提出し、全庁システムに登録する必要がある、使用する媒体を追加する場合においても順次報告書を提出しなければならない、仮に報告書を未提出のままシステム端末にUSBメモリ等を接続してもシステム上使用することができないよう制限がかけられている。

- (2) USBメモリの管理状況等について

①所有形態について

監査対象課で使用しているUSBメモリ2,407個のうち1,079個が個人で所有しているUSBメモリであった。

また、個人所有のUSBメモリ使用に関する明確な基準等はなかった。

[意見]

個人所有のUSBメモリについては、職員個人が保管していることから所属長の管理が徹底されず、業務上のデータだけではなく、業務以外の職員個人のデータも保存している可能性があり、自宅等での使用も考えられる。その際、紛失やウイルス感染による情報漏えいなどのリスクが懸念される場所である。

USBメモリは情報セキュリティ責任者である所属長が管理することとなっており、所属長はUSBメモリの業務上の必要性について、今一度確認するとともに、個人所有も含めてUSBメモリの管理状況を的確に把握しておく必要がある。

②登録状況について

各課等から提出のあった調査表によると、所属課で保有するUSBメモリの数は2,407個であり、全庁システムに登録されたUSBメモリの数は2,931個で524個の相違があった。

[意見]

通知では、各課等で使用しなくなったUSBメモリの登録廃止について届出が義務化されておらず、全庁システムに一度登録されたUSBメモリは、登録廃止の報告をしない限り使用が可能となっている。

そのため、個人所有のUSBメモリについては、人事異動により所属が変更となった職員が、業務上使用しなくなった場合でも、登録廃止の報告をしていなかったことなどから相違が生じたものと考えられる。

全庁システムで使用するUSBメモリは業務上必要な場合に限られており、人事異動等により業務上使用しなくなったUSBメモリについては、登録廃止の報告をするとともに、異動先の業務上の必要性に応じ再登録する必要があると考えられる。

③保管状況について

重要情報を保存したUSBメモリについては、基準によれば耐火・耐熱等の対策を講じ、なおかつ施錠可能な場所へ保管する必要があるが、重要情報を保存しているUSBメモリ643個のうち233個が個人の机に保管されており、

そのうち 138 個が未施錠のまま保管されていた。

[意見]

本市においては、平成 27 年 7 月に USB メモリを紛失するという事件が発生し、個人情報の外部流出が危惧されるなど、市政への信頼が損なわれる事態が生じている。

所属長はもとより、職員一人ひとりには情報を取り扱う際に潜在するリスクについて再認識し、重要な情報を保存した USB メモリは必ず施錠して保管する必要がある。

また、基準に示されている、耐火・耐熱等の対策を個人の机やキャビネットで講じることは可能なのか、施錠可能な場所であっても個人の机に重要な情報を保存した USB メモリを保管することが適切なのかを、今一度検討し、明確なルール作りをすることが望ましい。

④暗号化機能等について

重要情報を保存している USB メモリ 643 個のうち 580 個に暗号化機能等（以下「機能」という。）がついておらず、機能がついている USB メモリ 63 個のうち、39 個で暗号化等がされていなかった。

また、重要情報を保存している USB メモリの外部への持ち出しは 23 個で、そのうち 8 個に機能がついておらず、機能がついている USB メモリ 15 個のうち 1 個について暗号化等がされていなかった。

[意見]

重要情報の USB メモリへの保存は、取扱いルールでは原則禁止されており、例外的に所属部署以外へ情報を持ち出す必要がある場合や外部機関との情報交換が必要な場合、その他特に必要と認められる場合のみ認められているが、その際には、機能付き USB メモリを使用することとされている。

外部に持ち出す必要がある重要情報については、常に紛失又は盗難のリスクが伴うことから、暗号化等が可能な USB メモリを使用することはもとより、その機能は必ず利用する必要がある。

(3) まとめ

現在、本市の全庁システムにおいては、全庁ネットワークサーバ内の「所属フォルダ」で所属ごとのデータ管理が可能であり、取扱いルールに示されている外部機関との情報交換が必要な場合以外にUSBメモリを使用する必要性は乏しいものになっていると考えられる。

今回調査した2,407個のUSBメモリのうち2,286個のUSBメモリが情報を外部へ持ち出しをするためのものではないことや、1,079個が業務以外のデータも保存する可能性のある個人所有のUSBメモリであるという状況から判断すると、所属長がシステム端末でのUSBメモリ使用を認める業務上の必要性について疑念を抱かざるを得ない。

さらに、人事異動等によりUSBメモリを使用しなくなった場合でも登録廃止報告を行っていないものや、重要情報を保存するUSBメモリについて機能等がついているにもかかわらず、その機能を利用していないもの、重要情報を保存したUSBメモリを未施錠で机に保管していたものが見受けられたことなどから、情報セキュリティ責任者としての所属長の危機管理意識の不足が懸念されるところである。

とりわけ、自宅等での使用も考えられる個人所有のUSBメモリは、常に、紛失やウイルス感染等による情報漏えいなどのリスクが潜在していることを再認識するとともに、利便性のみで安易にUSBメモリを使用することなく、必要最低限のものに限定するなど、リスクの軽減を図ることが肝要である。

今回の監査結果が、情報セキュリティの確保は勿論のこと、潜在する様々なリスクに対する職員の危機管理意識の向上につながることを期待するものである。

別表1 USBメモリ登録状況

部 等	全庁システム の登録数	管理状況調査表 による登録数			重 要 性 分 類 ^{※1}				
		課等 所有	個人 所有	計	A	B	C	その他 ^{※2}	計
総務部	479	337	106	443	324	111	7	1	443
企画部	195	57	77	134	5	99	30	0	134
財務部	151	77	37	114	26	69	19	0	114
市民部	292	137	97	234	52	152	27	3	234
福祉保健部	617	410	109	519	116	334	42	27	519
環境部	287	112	145	257	4	247	6	0	257
商工農政部	228	50	111	161	41	111	9	0	161
土木建築部	224	96	72	168	4	162	2	0	168
都市計画部	268	26	192	218	2	212	4	0	218
下水道部	183	19	133	152	67	64	21	0	152
会計課	7	7	0	7	2	5	0	0	7
合 計	2,931	1,328	1,079	2,407	643	1,566	167	31	2,407

※1 重要性分類…基準第13条に基づく(P11資料参照)

※2 その他…情報が保存されていないもの

別表2 USBメモリ保管状況

部 等	重要性分類	保管場所	施錠	未施錠	計
総務部	A	机	15	0	15
		キャビネット	16	0	16
		その他	293	0	293
	A以外	机	85	17	102
		キャビネット	12	0	12
		その他	5	0	5
	計	426	17	443	
企画部	A	机	1	1	2
		キャビネット	1	0	1
		その他	2	0	2
	A以外	机	4	41	45
		キャビネット	57	0	57
		その他	27	0	27
	計	92	42	134	
財務部	A	机	9	0	9
		キャビネット	0	0	0
		その他	17	0	17
	A以外	机	28	40	68
		キャビネット	4	2	6
		その他	14	0	14
	計	72	42	114	
市民部	A	机	4	10	14
		キャビネット	17	0	17
		その他	21	0	21
	A以外	机	48	59	107
		キャビネット	17	0	17
		その他	49	9	58
	計	156	78	234	
福祉保健部	A	机	49	29	78
		キャビネット	34	0	34
		その他	4	0	4
	A以外	机	173	124	297
		キャビネット	72	0	72
		その他	34	0	34
	計	366	153	519	
環境部	A	机	2	0	2
		キャビネット	0	0	0
		その他	2	0	2
	A以外	机	64	152	216
		キャビネット	0	0	0
		その他	9	28	37
	計	77	180	257	
商工農政部	A	机	3	37	40
		キャビネット	1	0	1
		その他	0	0	0
	A以外	机	15	98	113
		キャビネット	1	0	1
		その他	6	0	6
	計	26	135	161	
土木建築部	A	机	0	4	4
		キャビネット	0	0	0
		その他	0	0	0
	A以外	机	5	153	158
		キャビネット	0	2	2
		その他	1	3	4
	計	6	162	168	

部 等	重要性分類	保管場所	施錠	未施錠	計
都市計画部	A	机	0	2	2
		キャビネット	0	0	0
		その他	0	0	0
	A以外	机	14	99	113
		キャビネット	76	0	76
		その他	24	3	27
	計	114	104	218	
下水道部	A	机	12	55	67
		キャビネット	0	0	0
		その他	0	0	0
	A以外	机	81	0	81
		キャビネット	0	0	0
		その他	4	0	4
	計	97	55	152	
会計課	A	机	0	0	0
		キャビネット	0	0	0
		その他	2	0	2
	A以外	机	0	0	0
		キャビネット	0	0	0
		その他	5	0	5
	計	7	0	7	
総計	A	机	95	138	233
		キャビネット	69	0	69
		その他	341	0	341
		小計	505	138	643
	A以外	机	517	783	1,300
		キャビネット	239	4	243
		その他	178	43	221
		小計	934	830	1,764
		合 計	1,439	968	2,407

別表3 暗号化機能等付きUSBメモリの使用状況

部 等	重要性分類	外部への持ち出し		暗号化機能等		
				有・使用	有・未使用	無
総務部	A	有	3	0	0	3
		無	321	0	1	320
	A以外	有	0	0	0	0
		無	119	3	18	98
	計		443	3	19	421
企画部	A	有	0	0	0	0
		無	5	1	3	1
	A以外	有	6	0	2	4
		無	123	7	51	65
	計		134	8	56	70
財務部	A	有	1	0	0	1
		無	25	0	1	24
	A以外	有	3	0	2	1
		無	85	2	15	68
	計		114	2	18	94
市民部	A	有	14	13	0	1
		無	38	4	0	34
	A以外	有	13	0	1	12
		無	169	11	18	140
	計		234	28	19	187
福祉保健部	A	有	4	1	1	2
		無	112	4	29	79
	A以外	有	35	0	7	28
		無	368	6	66	296
	計		519	11	103	405
環境部	A	有	0	0	0	0
		無	4	0	2	2
	A以外	有	26	0	1	25
		無	227	0	14	213
	計		257	0	17	240
商工農政部	A	有	1	0	0	1
		無	40	1	2	37
	A以外	有	8	0	0	8
		無	112	7	25	80
	計		161	8	27	126

部 等	重要性分類	外部への持ち出し		暗号化機能等		
				有・使用	有・未使用	無
土木建築部	A	有	0	0	0	0
		無	4	0	0	4
	A以外	有	0	0	0	0
		無	164	4	0	160
	計		168	4	0	164
都市計画部	A	有	0	0	0	0
		無	2	0	0	2
	A以外	有	7	0	0	7
		無	209	3	8	198
	計		218	3	8	207
下水道部	A	有	0	0	0	0
		無	67	0	0	67
	A以外	有	0	0	0	0
		無	85	1	27	57
	計		152	1	27	124
会計課	A	有	0	0	0	0
		無	2	0	0	2
	A以外	有	0	0	0	0
		無	5	0	0	5
	計		7	0	0	7
総計	A	有	23	14	1	8
		無	620	10	38	572
	小計	643	24	39	580	
	A以外	有	98	0	13	85
		無	1,666	44	242	1,380
	小計	1,764	44	255	1,465	
	合計	有	121	14	14	93
		無	2,286	54	280	1,952
計		2,407	68	294	2,045	

資料

【大分市情報セキュリティ対策基準】（抜粋）

（情報の分類）

第 13 条 本市のすべての情報は、その重要性を踏まえた管理を行わなければならない。

2 情報の重要性分類は、次の表に示す 3 段階とする。

情報の重要性分類	
重要性分類 A	(1) 個人情報 (2) 法令等により守秘義務が課されている情報 (3) 漏えい、滅失、き損等により個人又は法人の利益に重大な損害を与えるおそれのある情報 (4) 漏えい、滅失、き損等により公平かつ円滑な行政の執行を著しく妨げるおそれのある情報 (5) 事故等が発生したときに、その復元が著しく困難となる情報
重要性分類 B	重要性分類 A 及び C 以外の情報
重要性分類 C	公表を前提としている情報

（記録媒体の管理）

第 16 条 情報セキュリティ責任者は、取り外しが可能な記録媒体について、次のとおり適切な管理を行わなければならない。

(1) 記録媒体の特性を踏まえた管理

(2) 耐火、耐熱、耐水及び耐湿対策を講じた場所への保管

(3) 重要情報（情報の重要性分類 A に該当する情報をいう。以下同じ。）を記録した記録媒体の施錠可能な場所への保管

(4) 記録媒体の利用及び保管時の整理整頓

(5) 最終的に確定した情報を記録した記録媒体に対する書込み禁止措置を行った上での保管

2 情報セキュリティ責任者は、情報の滅失防止のため、情報システムが運用する業務及び保有する情報の重要度を勘案して、記録媒体を別の記録媒体に複製し、可能な限り当該記録媒体を自然災害を被る可能性の低い場所に別途保管しなければならない。

【大分市USBメモリ取扱いルール】

1. 目的

(1)このルールは、大分市情報セキュリティポリシー(「大分市における情報セキュリティの基本的な考え方(平成15年4月1日施行)」及び「大分市情報セキュリティ対策基準(平成19年4月1日施行)」から構成されるもの)に基づく行動のうちUSBメモリの取扱いについて必要な事項を定め、USBメモリによる情報セキュリティ事故の発生を防止することを目的とする。

2. 定義

(1)このルールにおいて、次の各号に掲げる用語の意義は、大分市情報セキュリティ対策基準に定めるもののほか、当該各号に定めるところによる。

(ア)USBメモリ コンピュータに周辺機器を接続するための規格であるUSB規格に準拠したものであって、USBコネクタに接続して使用する持ち歩き可能な記録媒体をいう。

(イ)重要情報 大分市情報セキュリティ対策基準第13条に規定する情報の重要性分類Aに該当する情報をいう。

(ウ)所属長 大分市情報セキュリティ対策基準第2条第3号に規定する課等の長をいう。

3. 使用制限

(1)市の管理保有する情報を保存する際には、重要情報をUSBメモリに保存することを禁止する。ただし、次に掲げる場合に限りUSBメモリの使用を認める。

(ア)所属部署以外に情報を持ち出す必要がある場合

(イ)国、県及び委託業者等の外部機関との情報交換が必要な場合

(ウ)その他特に必要と認められる場合

(2)前項ただし書きの場合に使用するUSBメモリについては、パスワード機能及び暗号化機能付きUSBメモリを使用するものとし、外部持ち出し等の必要がある場合については所定の手続きを経るものとする。

4. 適正な管理

(1)所属長は、USBメモリを施錠可能な場所に保管するとともに、パスワード機能及び暗号化機能付のUSBメモリについては、類推されにくいパスワードの設定等適正な管理を行い、紛失又は盗難対策に必要な措置を講じなければならない。

5. 外部への持ち出し等

(1)職員等は、重要情報を保存した USB メモリを所属部署以外に持ち出す必要がある場合には、所属長に持出管理簿(情報セキュリティ実施手順 様式第 3 号)を提示し、許可を得なければならない。

(2)所属長は、職員等から持出管理簿の提示を受けた場合、必要と認めるときは、外部持ち出しについて情報漏えい事故対策の指示を出し許可を与えることができる。

(3)職員等は、所属長の指示に従い、USB メモリを所属部署以外に持ち出すことができる。その場合、盗難・紛失・コンピュータウィルス等による情報漏えい事故がないように必要な措置を講じなければならない。

(4)職員等は、USB メモリを所属部署以外に持ち出す目的が達せられたときには、速やかに USB メモリ内のデータを削除しなければならない。

6. 盗難・紛失

(1)重要情報を保存した USB メモリを紛失し、又は盗難にあった場合は、職員等は直ちに所属長に報告するものとする。

(2)前項の報告を受けた所属長は、情報政策課長に報告しなければならない。

7. 適用

このルールは、平成 25 年 1 月 1 日から適用する。ただし、同日より適用することが困難な場合は可能な時期より順次実施していくものとする。

【平成 26 年 4 月 4 日付情報政策課長通知】(抜粋)

全庁ネットワークにおける外部記憶媒体の管理について

今回、全庁ネットワークの更新にあたり、本ネットワークのセキュリティ向上を図るため、現在、所属長が管理・保管している USB メモリ等の外部記憶媒体について、システムへの機器登録を行い、その管理を明確にすることといたしました。このことにより、システムに登録された媒体のみが全庁ネットワークで利用可能となります。

つきましては、今後、業務上必要な USB メモリ等の外部記憶媒体を使用する場合は、情報セキュリティ責任者(所属長)からの報告が必要となりますので、使用媒体の確認及び報告書の提出をお願いいたします。