資料２

地方公共団体における情報セキュリティポリシーに関するガイドライン改定のポイントについて②
（情報セキュリティインシデント関係）

総務省

2023年１月12日

地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会

最近の地方公共団体における情報セキュリティインシデントについて

兵庫県尼崎市における個人情報流出事案の概要

○概要
　業務委託会社の再委託先の社員が個人情報を含むUSBメモリを紛失する情報流出事案が発生。

【流出した個人情報】
・全市民の住民基本台帳の情報（46万517人分）
・住民税に係る税情報（36万573件）
・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）
・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）

事案に対する対応の方向性

○尼崎市は、総務省のガイドラインに沿ってセキュリティポリシーを策定し、市のセキュリティポリシー上では、委託先管理の徹底等を求めていたが、運用面における管理が不十分であった。
○このため、①ガイドラインに運用面に関する記載を追記するほか、②委託先管理に関するチェックシートの提示やガイドラインの概要版の作成、研修の周知等を行い対策の徹底を求めていく。

（参考）地方公共団体における調達・運用時の情報セキュリティ対策の実施状況
○委託先管理について、調達時におけるセキュリティポリシーに基づいた要件の記載や契約等で情報漏えい防止策を義務付けている団体は多いが、運用時における管理が不十分な実態がある。

	都道府県	割合	市区町村	割合
情報資産の調達の際、仕様書等に情報セキュリティポリシーに基づいた要件を記載している	47団体	100%	1406	80.8%
委託事業者に対し、情報漏えい防止策を契約等により義務付けている	47団体	100%	1705	97.9%
情報システムの運用等の委託事業者に対する指導・監査を実施している	34団体	72.3%	1033	59.3%
機密性、完全性、可用性等についてサービス規約(SLA)に定め、委託業者に対し定期的に報告することを定めている	30団体	63.8%	868	49.9%

（参考：総務省「令和3年度 自治体DX・情報化推進概要」）

事案に対する対応ついて

（１）ガイドラインの運用面に関する記載の追記

○本事案にかかる再発防止策について、市第三者委員会報告書において示されたところであり、改めてガイドラインの外部委託先の管理について、特に運用面に関する必要なセキュリティ対策を記載する。

①機微なデータへのアクセス制御、情報の持ち出し管理、ログ管理など、個人情報の取扱いに関する管理の徹底不足（Ｐ３、４）
⇒業務委託を行う場合であっても、情報資産の分類に応じた情報のライフサイクル管理の徹底が必要であること。業務委託先が重要な情報資産を取り扱う場合においては、情報セキュリティの原則である「最小限の権限」、「複数人による確認」等を徹底する旨を記載する。また、USBメモリのような物理的なデータ移動ではなく、外部サービス等で委託事業者等へ重要な情報資産を運搬する場合の確認事項を記載する。

②サーバルームへの入退室管理や監視カメラ等による作業の記録など、物理的安全管理措置の徹底不足（Ｐ５）
⇒管理区域内に入室する際は、入室者に対して身分証の提示を求め、従事者名簿と突合することや職員の随行、監視カメラ等によって入室者を確認する。従事者の変更があった際は、委託事業者に対し、最新版の名簿の提出を求めるとともに、従事者名簿の提出時に身分証明書の確認や面談により本人確認を行う。委託事業者から名簿の提出がない場合であっても定期的（年１回程度）に従事者が変更されていないか確認する。

③職員、委託先の従業員の個人情報の取扱いに関する意識の欠如（Ｐ６）
⇒委託事業者の従業員が地方公共団体の情報セキュリティポリシー等を理解することが重要であり、業務委託先の従業員に地方公共団体が主催する研修等に参加させることや、研修を合同で行うことも有効である旨を記載する。

④作業報告書等の書面による委託業務管理の徹底不足（Ｐ７）
⇒委託事業者がセキュリティ要件を遵守していることを地方公共団体が確認するため、「外部委託先に関するセキュリティ要件のチェックシート」に基づいて、委託事業者がセキュリティ要件を遵守しているか確認する必要がある旨を記載する。

（２）セキュリティポリシーを運用する上での支援

○外部委託先の管理について、一定のセキュリティレベルを確保できるよう業務委託契約を締結する際のセキュリティ要件の確認事項について、委託先に提出を求めるチェックシートのひな型を作成し地方公共団体に提供する。（Ｐ８）

○セキュリティポリシーガイドラインの理解促進のため、ガイドラインの概要版の作成を行う。（Ｐ９）

○職員等に対する情報セキュリティ対策に関する研修の周知や説明会の実施等を行う。（Ｐ９）

ガイドライン改定案について①

原　因：機微なデータへのアクセス制御、情報の持ち出し管理など個人情報の取扱いに関する管理の徹底不足

対　応：業務委託を行う場合であっても、情報資産の分類に応じた情報のライフサイクル管理の徹底が必要であること。また、業務委託先が重要な情報資産を取り扱う場合においては、情報セキュリティの原則である「最小限の権限」、「複数人による確認」等を徹底する旨を記載する。

＜現行＞

対策基準８．１.業務委託
例文
（2）契約項目
契約項目を追記
・委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法
・委託事業者の従業員に対する教育の実施
解説
（2）契約項目
④委託事業者に許可する情報の種類とアクセス範囲、アクセス方法
委託に関わる情報の種類を定義し、種類ごとのアクセス許可、アクセス時の情報セキュリティ要求事項並びにアクセス方法の監視及び管理を行う。

＜改定案＞

対策基準８．１.業務委託
例文
（2）契約項目
契約項目を追記
・委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理の実施
・委託事業者の従業員に対する教育の実施
解説
（2）契約項目
④委託事業者に許可する情報の種類とアクセス範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理の実施
委託に関わる情報の種類を定義し、種類ごとのアクセス許可、アクセス時の情報セキュリティ要求事項並びにアクセス方法の監視及び管理を情報のライフサイクル全般で行う。また、委託事業者が重要な情報資産を取り扱う場合は、情報セキュリティの原則である「最小限の権限」、「複数人による確認」等を徹底する必要がある。情報資産の分類とライフサイクル全般の管理については、本ガイドラインの「2. 情報資産の分類と管理」も参照されたい。

ガイドライン改定案について①

原　因：機微なデータへのアクセス制御、情報の持ち出し管理など個人情報の取扱いに関する管理の徹底不足

対　応：庁外で情報資産を移動する際は、USBメモリのような物理的なデータ移動ではなく、外部サービス等で委託事業者等へ重要な情報資産を運搬する場合の確認事項を記載する。

＜現行＞

対策基準2.情報資産の分類と管理　解説
(２) 情報資産の管理
⑧情報資産の運搬

（注７）を新設

＜改定案＞

対策基準2.情報資産の分類と管理　解説
(２) 情報資産の管理
⑧情報資産の運搬

（注７）を新設
　委託事業者等の外部へ重要な情報資産を電磁的記録媒体で運搬する場合は、機密情報を運搬する専用のサービスを利用するなど安全な運搬措置を行うこと。インターネットを利用した外部サービス等で委託事業者等へ重要な情報資産を運搬する場合は、アクセス制御等のシステム設定が適切にされているか、重要な情報資産を暗号化して保存しているか、委託先と接続する通信が暗号化されているか等を確認する必要がある。また、委託事業者等に重要な情報資産が運搬された後の情報の管理を徹底することも重要となる。

ガイドライン改定案について②

原　因：サーバルームへの入退室管理や監視カメラ等による作業の記録など、物理的安全管理措置の徹底不足

対　応：管理区域内に入室する際は、入室者に対して身分証の提示を求め、従事者名簿と突合することや職員の随行、監視カメラ等によって入室者を確認する。従事者の変更があった際は、委託事業者に対し、最新版の名簿の提出を求めるとともに、従事者名簿の提出時に身分証明書の確認や面談により本人確認を行う。委託事業者から名簿の提出がない場合であっても定期的（年1回程度）に従事者が変更されていないか確認する。

＜現行＞

対策基準８．１.業務委託
解説
（2）契約項目
②委託事業者の責任者、委託内容、作業者、作業場所の特定
　委託事業者の責任者や作業者を明確にするとともに、これらの者が変更する場合の手続を定めておき、担当者の変更を常に把握できるようにする。また、作業場所を特定することにより、情報資産の紛失等を防止する。

＜改定案＞

対策基準８．１.業務委託
解説
（2）契約項目
②委託事業者の責任者、委託内容、作業者、作業場所の特定
　委託事業者の責任者や作業者を明確にするとともに、これらの者が変更する場合の手続を定めておき、担当者の変更を常に把握できるようにする。また、作業場所を特定することにより、情報資産の紛失等を防止する。
　なお、管理区域内に入室する際は、入室者に対して身分証の提示を求め、従事者名簿と突合することや職員の随行、監視カメラ等によって入室者を確認する。従事者の変更があった際は、委託事業者に対し、最新版の名簿の提出を求めるとともに、従事者名簿の提出時に身分証明書の確認や面談により本人確認を行う。委託事業者から名簿の提出がない場合であっても定期的（年1回程度）に従事者が変更されていないか確認する。管理区域の管理については、本ガイドラインの「4.2 管理区域（情報システム室等）の管理」も参照されたい。

ガイドライン改定案について③

原　因：職員、委託先の従業員の個人情報の取扱いに関する意識の欠如

対　応：委託事業者の従業員が地方公共団体の情報セキュリティポリシー等を理解することが重要であり、業務委託先の従業員に地方公共団体が主催する研修等に参加させることや、研修を合同で行うことも有効である旨を記載する。

＜現行＞

対策基準８．１.業務委託
解説
（2）契約項目
⑤従業員に対する教育の実施
　委託事業者において、情報セキュリティに対する意識の向上を図るために、従業員に対し教育を行うように規定しておく。

＜改定案＞

対策基準８．１.業務委託
解説
（2）契約項目
⑤従業員に対する教育の実施
　委託事業者において、情報セキュリティに対する意識の向上を図るために、従業員に対し教育を行うように規定しておく。**なお**、委託事業者が重要**な**情報資産を取り扱う場合は、委託事業者の従業員に委託元の地方公共団体の情報セキュリティポリシーや各規定を理解させるため、地方公共団体が主催する情報セキュリティに関する教育・研修・訓練等に参加させることや、研修を合同で行うことも有効である。教育・訓練については、本ガイドラインの「5.2 教育・訓練」も参照されたい。

ガイドライン改定案について④

原　因：作業報告書等の書面による委託業務管理の徹底不足

対　応：委託事業者がセキュリティ要件を遵守していることを地方公共団体が確認するため、「外部委託先に関するセキュリティ要件のチェックシート」に基づいて、委託事業者がセキュリティ要件を遵守しているか確認する必要がある旨を記載する。

＜現行＞

対策基準８．Ｉ.業務委託
解説
（3）確認・措置等
　情報セキュリティ管理者は、委託事業者において十分なセキュリティ対策が実施されているか、定期的に確認し、必要に応じ、改善要求等の措置を講じる必要がある。確認した内容は定期的に統括情報セキュリティ責任者に報告する。個人情報の漏えい等の重大なセキュリティ侵害行為が発見された場合には、速やかにCISOに報告を行う。また、情報セキュリティ管理者は、情報システムの運用・保守を業務委託する場合は、委託先が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、速やかに報告させる必要がある。
　なお、委託事業者に対する監査については、本ガイドラインの「9.1 監査 （4）委託事業者に対する監査」を参照されたい。

＜改定案＞

対策基準８．Ｉ.業務委託
解説
（3）確認・措置等
　情報セキュリティ管理者は、再委託先も含め、委託事業者に対し、十分なセキュリティ対策が実施されているか、定期的に確認し、必要に応じ、改善要求等の措置を講じる必要がある。
　また、契約を行う際に「外部委託先に関するセキュリティ要件のチェックシート」に基づいて、委託事業者のセキュリティ要件の遵守状況を確認する必要がある。確認した内容は、定期的に統括情報セキュリティ責任者に報告する。個人情報の漏えい等の重大なセキュリティ侵害行為が発見された場合には、速やかにCISOに報告を行う。また、情報セキュリティ管理者は、情報システムの運用・保守を業務委託する場合は、委託先が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、速やかに報告させる必要がある。
　なお、委託事業者に対する監査については、本ガイドラインの「9.1 監査 （4）委託事業者に対する監査」を参照されたい。

外部委託先に関するセキュリティ要件のチェックシート（サンプル）

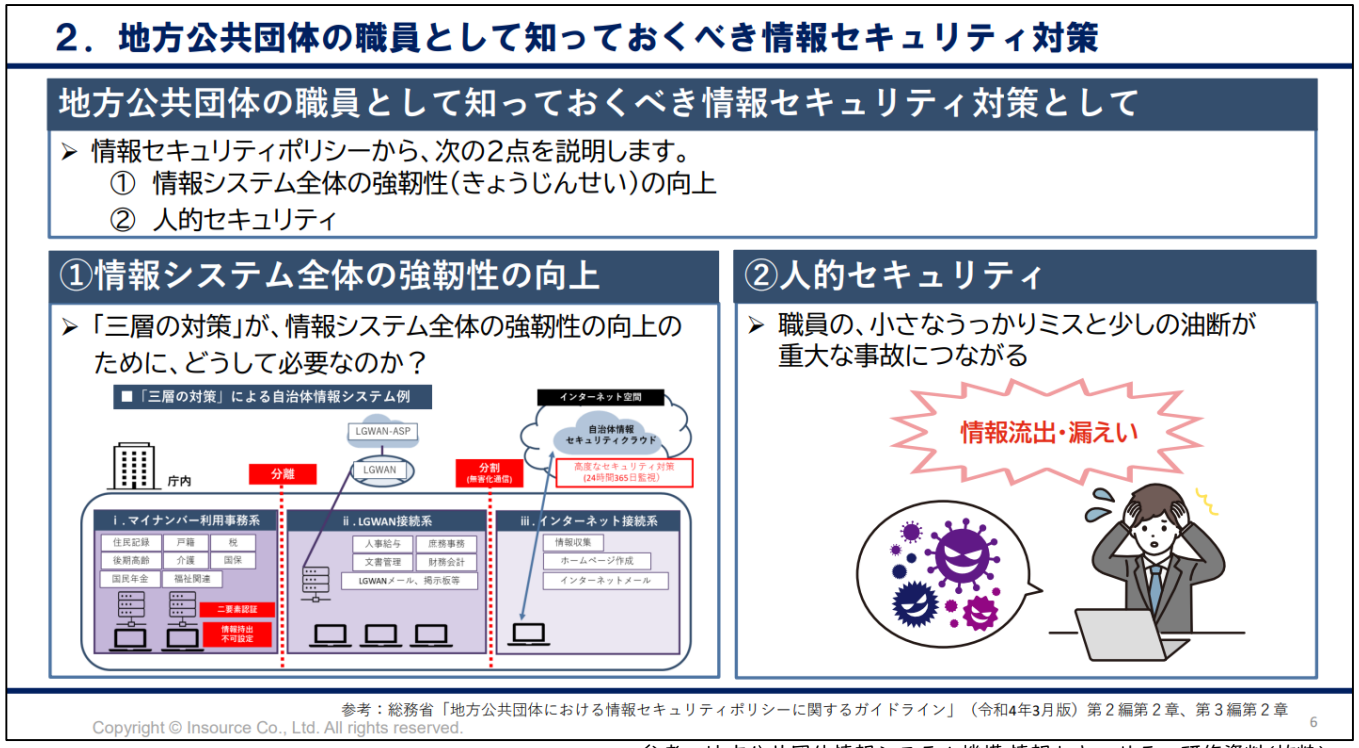
項目	確認事項	チェック欄
1.基本事項	契約に係るデータ及び知り得た秘密等の取扱いについて、その重要性を認識し、適切に取扱う。	☑
2.法令等遵守	個人情報の保護に関する法令等を遵守する。	☑
3.秘密の保持	契約の履行に際して知り得た秘密を他に漏らさない。	☑
	契約の終了後、解除後及び職を退いた場合においても同様とする。	☑
4.目的外使用及び第三者への提供禁止	契約に係るデータを委託者が指示する目的以外に使用し、第三者に提供しない。	☑
5.データの受領	委託者からデータ等の提供を受けた場合は、データ等の受領証を作成し、委託者に提出する。	☑
6.データの持ち出し	委託者の環境からデータを持出す場合は、書面で持出す目的、データの内容及び暗号化等の対策を記し、委託者から承認を受ける。	☑
	委託者の環境から業務システムで利用している本番データ（住民情報が含まれるデータ）を持出すことを禁止する。業務委託契約において本番データの持出しが認められている場合は、都度書面で申請し、委託者から承認を受ける。	☑
7.複写及び複製の禁止	本契約に係るデータを委託者の承認なく、用紙、記録媒体等に複写し、又は複製しない。	☑
8.パソコン及びデータの持込み	委託者の環境にパソコン及びデータを持込み、作業を行う場合は、書面で委託者からパソコン及びデータ持込みにかかる承認を受ける。	☑
9.安全管理義務	契約に係るデータの管理責任者を定め、業務の従事者を限定する。	☑
	契約に係るデータを取扱う場所を特定する。	☑
	データの無断持出し禁止を周知徹底し、やむを得ず、持ち出す場合は、委託者の承認を得たうえで、管理簿等の書面に記録する。	☑
	紛失、損傷、焼失等の事故が生じないよう安全かつ適切な管理体制を整備する。	☑
	パソコンやデータを持ち込む場合、最新のウイルス対策ソフト等の使用していることや不正なプログラムが書かれていないことを確認する。	☑
10.データの返却・消去	委託者から借用したデータは、速やかに返却する。借用したデータを複製・保存した場合は消去し、消去したことが分かる書類を委託者に提出する。	☑
11.記録媒体の廃棄	契約の履行上、委託者から廃棄指示がある場合の記録媒体等は、確実に物理的に破壊し、又はすべての記録を復元不可能な状態に消去した後に廃棄し、廃棄したことが分かる書類を委託者に提出する。	☑
12.監督及び監査	委託者が、契約の履行に関し必要があるときは、受託者及び再委託先に対して報告を求め、監査を行い、又は監査に立会うことができるように、体制等を整備する。	☑
13.教育	従業者に対して、データの保護及び秘密の保持等データの取扱いに関し履行すべき責務について充分な教育を行う。	☑
	教育の実施状況を記録する	☑
14.事故発生の報告義務	安全管理措置等が履行できない場合及び情報漏えい等の事故が発生した場合等に備え、直ちに委託者へ通知、報告できる体制を整備する。	☑
15.再委託の禁止	委託者の承諾なしに、業務を第三者に委託し又は請け負わせない。	☑
	委託者の承諾を受けて再委託した場合は、再委託者に本契約の規定を遵守させる。	☑

セキュリティポリシーを運用する上での支援

概　要

（１）情報セキュリティ対策に関する研修等の周知

（例）情報セキュリティ対策セミナー（地方公共団体情報システム機構）



参考：地方公共団体情報システム機構 情報セキュリティ研修資料(抜粋)

（２）セキュリティポリシーガイドライン概要版の作成

・ガイドラインの理解促進のため、ガイドラインのポイントを要約した概要版を作成し、自治体に周知

（３）セキュリティポリシーガイドラインの改定内容等について説明会の実施

・直近の改定内容や委託先管理のポイントについて説明会を実施

最近の動向を踏まえた改定について

改定のポイント

○ **昨今、感染被害が確認されているEmotet、ランサムウェア、フィッシング等の特徴と対策をガイドラインに記載。**

- **Emotet対策では、組織内への注意喚起、マクロの実行禁止、メールの監査ログの取得や定期的な確認等を記載**
- **ランサムウェア対策では、OSやソフトウェアのアップデート、パスワード設定の見直し、データ・システムのバックアップ等を記載。合わせて、自治体が採用している庁内ネットワーク構成に応じた留意点も記載。**
- **フィッシング対策では、あらかじめ登録しているURLからウェブサイトにアクセス、多要素認証設定の有効化等を記載**

6. 技術的セキュリティ解説の概要	
○不正プログラム対策	（１） **⑧Emotet（エモテット）** Emotetへの感染を予防し、被害を最小限にとどめるための対策として「組織内への注意喚起の実施」、「信頼できないWord文書やExcelファイルにおいてマクロの実行禁止」、「メールの監査ログの取得や定期的な確認」などが挙げられる。 **⑨ランサムウェア** 身代金を払ったとしても攻撃元が情報を正常な状態に戻す、又は外部に公表しないといった行為をとる確証は全くない。ランサムウェアに感染しないための事前対策として「導入しているOSやソフトウェアのアップデート」、「パスワード設定の見直し」、被害を受けた際の影響を低減するための対策として「データのバックアップ」などが挙げられる。なお、「データのバックアップ」については、バックアップの保存先が、ランサムウェアに感染した端末等からアクセスできる領域にある場合、バックアップを含め暗号化されてしまう可能性があるため、端末のOSからアクセスできないディスクや媒体へ保管する等の検討が必要となる。また、可用性を担保する対策としては、対象となるデータだけではなく、システムのバックアップを取ることでシステムの迅速な復旧につなげることができる。 **⑩フィッシング** 対策として、「メールやSMSに添付されているURLは安易にクリックせず、ウェブサイトにアクセスする際は、あらかじめ登録しているURLからアクセスする」、「Webサービスにログインする場合に、多要素認証等の設定が可能な場合、有効化する」などが挙げられる。