資料３

令和５年度　第２回

杉並区情報公開・個人情報保護審議会

住民基本台帳ネットワークシステム・情報提供ネットワークシステム運用監視部会

報告事項

令和５年 11 月１日

次　　第

点検結果－１

住民基本台帳ネットワークシステムセキュリティ評価の実施内容等の点検結果について

杉並区情報公開・個人情報保護審議会

部会点検日
令和５年９月５日

点検内容
区が実施する住民基本台帳ネットワークシステム（以下「住基ネット」という。）セキュリティ評価の実施等にあたり、以下３点の内容について、妥当であるかの点検を行った。 （１）チェックリスト（注）の提出について （２）住民基本台帳ネットワークシステム緊急時対応訓練について （３）住民基本台帳ネットワークシステム安全措置実施状況等に関する職員自己点検について （注）総務省発出「住民基本台帳ネットワークシステム及びそれに接続している既設ネットワークに関する調査表 市区町村版」を指す。

点検結果
（１）チェックリストの提出について 各自己点検項目について、回答内容及び回答根拠となる規程類や資料等が妥当であることを確認した。チェックリストの自己点検項目に対応した対策がとられていることを確認した。 **（２）住民基本台帳ネットワークシステム緊急時対応訓練について** 職責や住基ネット端末の利用の実態で訓練を分けており、当該訓練は妥当であると考える。 **（３）住民基本台帳ネットワークシステム安全措置実施状況等に関する職員自己点検について** 点検内容については、職員の職責等に応じて設問が異なるようになっており、（１）のチェックリストの設問項目に沿って作成されていることを確認した。そのため、業務実態の把握に有効であり、当該点検は妥当であると考える。 また、「杉並区職員の逮捕に伴う再発防止対策検討委員会報告書」を踏まえた再発防止策等に合わせて、設問の修正を行ったことを確認した。

総　評
住基ネットセキュリティ評価の実施内容等について、妥当であることを確認した。

点検結果－２

情報提供ネットワークシステムセキュリティ評価の実施内容等の点検結果について

杉並区情報公開・個人情報保護審議会

部会点検日
令和５年９月５日

点検内容
区が実施する情報提供ネットワークシステムセキュリティ評価の実施等にあたり、以下２点の内容について、妥当であるかの点検を行った。 （１） 情報提供ネットワークシステム緊急時対応訓練について （２） 情報提供ネットワークシステム安全措置実施状況等に関する職員自己点検について ※なお、令和５年度第１回情報公開・個人情報保護審議会の諮問事項のうち、「デジタル庁発出情報提供ネットワークシステム接続運用規程に基づく安全管理措置の自己点検の回答内容等について」は、次回の運用監視部会で点検する。

点検結果
（１） 情報提供ネットワークシステム緊急時対応訓練について インシデント発生時の情報連絡体制を確認する訓練内容となっており、当該訓練は妥当であると考える。 **（２） 情報提供ネットワークシステム安全措置実施状況等に関する職員自己点検について** 自己点検の設問については、区の情報提供ネットワークシステム業務における情報セキュリティ対策の実施状況等を点検する内容となっており、各課の情報連携端末の設置状況に応じて設定されていることを確認した。そのため、業務実態の把握に有効であり、当該点検は妥当であると考える。 また、昨年度の運用監視部会の意見を踏まえて、設問の修正を行ったことを確認した。

総　評
情報提供ネットワークシステムセキュリティ評価の実施内容等について、妥当であることを確認した。

参考資料

令和５年度第１回運用監視部会配布資料

議題番号	資料名等	資料番号
―	次第	部会資料１
住民基本台帳ネットワークシステムに関する事項		
議題２－１	チェックリストの提出について	部会資料２
議題２－２	住民基本台帳ネットワークシステム 緊急時対応訓練について	部会資料３
議題２－３	住民基本台帳ネットワークシステム 安全措置実施状況等に関する職員自己点検について	部会資料４
情報提供ネットワークシステムに関する事項		
議題３－１	情報提供ネットワークシステム 緊急時対応訓練について	部会資料５
議題３－２	情報提供ネットワークシステム 安全措置実施状況等に関する職員自己点検について	部会資料６

部会資料１

令和５年９月５日（火）午後２時から
杉並区役所西棟６階第６会議室

令和５年度第１回住民基本台帳ネットワークシステム・情報提供ネットワークシステム運用監視部会　次第

○ 住民基本台帳ネットワークシステム及び情報提供ネットワークシステム運用状況等の視察実施（東棟１階　区民課）

１　視察に関する事項

○ 議題１
視察結果に対するご意見等について

２　住民基本台帳ネットワークシステムに関する事項

○ 議題
２－１　チェックリストの提出について
２－２　住民基本台帳ネットワークシステム緊急時対応訓練について
２－３　住民基本台帳ネットワークシステム安全措置実施状況等に関する職員自己点検について

３　情報提供ネットワークシステムに関する事項

○ 議題
３－１　情報提供ネットワークシステム緊急時対応訓練について
３－２　情報提供ネットワークシステム安全措置実施状況等に関する職員自己点検について

※　なお、令和５年度第１回情報公開・個人情報保護審議会の諮問事項のうち、『デジタル庁発出「情報提供ネットワークシステム接続運用規程」に基づく安全管理措置の自己点検の回答内容等について』の自己点検については、デジタル庁から通知があり次第実施し、次回の運用監視部会にご報告いたします。

担当：政策経営部情報管理課、区民生活部区民課

部会資料２

チェックリストの提出について

１　チェックリストの概要

総務省発出「住民基本台帳ネットワークシステム及びそれに接続している既設ネットワークに関する調査表　市区町村版」（以下「チェックリスト」という。）による自己点検は、住民基本台帳ネットワークシステム（以下「住基ネット」という。）に関する技術的基準や指針等に基づく市区町村におけるセキュリティ対策の状況を市区町村が自ら点検し、職員のセキュリティ意識を高めるとともに、必要に応じて対策の見直し等を行うことで、全国の住基ネット運用環境の継続的なセキュリティレベルの維持向上を図ることを目的としており、総務省からの依頼に基づき定期的に（年に１回）実施している。

点検する項目は設問形式になっており、チェックリストで示されたセキュリティ対策の基準と区の状況を照らし合わせ回答する必要がある。

なお、今年度の東京都への回答期限は令和５年８月 21 日だった。

２　チェックリストの主な変更点

管理目標の変更点

既設ネットワークに関する管理目標について、基幹系業務システムの例示として戸籍附票システムが追加された。（管理目標 37、38、39、40、41 及び 42）

＜補足＞　戸籍附票システムとは、戸籍附票に関する事務を処理するためのシステムである。戸籍附票とは、区に本籍を有する者の居住関係を記録・公証するものであり、住民基本台帳法に基づいて、戸籍が作られてから（または戸籍に入籍してから）現在に至るまで（または戸籍から除籍されるまで）の住所が記録されている。

※ 表記ゆれや軽微な誤記の修正等、回答に影響しないものは省略。

３　チェックリストの変更点への対応

基幹系業務システムの例示として追加された戸籍附票システムについては、従来より基幹系業務システムに含まれている認識でチェックリストの自己点検を実施していたため、回答の変更はない。（管理目標 37、38、39、40、41 及び 42）

部会資料３

住民基本台帳ネットワークシステム緊急時対応訓練について

１　目的

住民基本台帳ネットワークシステム（以下「住基ネット」という。）は現在安定した運用が維持されているが、システム障害やウイルス被害等の事件・事故が発生した場合、システムの安全性を確保するためには迅速かつ的確な対応が必要となる。そのため、当該訓練により緊急時の対応手順や連絡体制等を確認し、実際の緊急時に被害を最小限に抑えることを目的とする。

２　訓練内容

対　象	訓　練	
	概　要	備　考
緊急時対策会議構成員（注1）	・緊急時対応計画（注2）に基づき緊急時の対応手順とそれに係る連絡体制の確認 ・緊急時対策会議構成員の役割確認	・緊急時の対応手順については、緊急事態が発生してからの段階別の対応、脅威度による対応の違い及び緊急時に招集された際の流れについて確認する。 ・緊急時の連絡体制については、連絡経路だけでなく構成員が不在の際の代理者についても確認する。 ・各構成員の役割については、緊急時における各役職に応じた責務や規程に定められた取るべき行動について確認する。
区民課	・緊急時対応計画に基づき緊急時の対応手順とそれに係る連絡体制の確認 ・緊急事態を誘発しかねない事象に対する啓発	・緊急事態が発生した際の連絡体制と対応手順を確認する。 ・緊急事態の発生を想定し、緊急時連絡体制に基づく連絡訓練を実施する。 ・緊急事態を誘発しかねない事象に対する啓発として、離席時における住基ネット端末（以下「統合端末」という。）からのログオフや、不正利用を防止するための注意点等について周知徹底を行う。 ・訓練内容の理解度を確認するためにテストを行い、訓練効果の測定を行う。また、当該テストを通じて、訓練内容の定着を図る。
情報管理課及びその他住基ネットを利用する部署（注３）		

３　実施時期

令和5年 11～12 月を予定

＜ 注 釈 ＞

注1：緊急時対策会議構成員は「杉並区住民基本台帳ネットワークシステムセキュリティ対策規程」により定められており、統括責任者（副区長）、政策経営部デジタル戦略担当部長、総務部危機管理室長、区民生活部長、政策経営部情報管理課長、政策経営部情報システム担当課長、総務部危機管理室危機管理対策課長、区民生活部区民課長及びその他統括責任者が必要と認める者により構成される。

注2：杉並区において「緊急時対応計画」に位置づけられるものは以下の2つ。

・杉並区住民基本台帳ネットワークシステム緊急時対応計画に関する要綱

・杉並区住民基本台帳ネットワークシステム緊急時対応手順

注3：自課の執務室内に統合端末を設置せず、情報管理課の執務室内に設置してある統合端末をその都度利用する部署を指す。令和5年8月１日時点での該当部署は次のとおり。

課税課、国保年金課、障害者施策課、介護保険課、各福祉事務所、杉並保健所保健予防課、杉並保健所保健サービス課及び子ども家庭部管理課

以上

部会資料４

住民基本台帳ネットワークシステム
安全措置実施状況等に関する職員自己点検について

１　目的

住民基本台帳ネットワークシステム（以下「住基ネット」という。）における人的セキュリティ対策が、区において適正に実施されていることを確認するとともに、教育方法やセキュリティ対策実施上の問題点を把握する。

なお、集計した自己点検結果については各部署に対し振り返りを行うことで、職員の業務におけるセキュリティ意識の向上を図る。

２　調査内容の概要

自己点検の設問は、チェックリスト（注１）の設問から抽出し、次の２点を重点項目として作成する。

（１）離席時における住基ネット端末（以下「統合端末」という。）のログオフの徹底

（２）緊急事態が発生したときの緊急時連絡体制の確認

注１：正式名称は「住民基本台帳ネットワークシステム及びそれに接続している既設ネットワークに関する調査表　市区町村版」。総務省から年に１度提示され、市区町村が自ら点検し、職員のセキュリティ意識を高めるとともに、必要に応じて対策の見直し等を行うことで、セキュリティレベルを維持・向上させることを目的としている。

３　調査形式の概要

自己点検種別	対象者	対象者数(注２)	設問数
情報管理課管理担当用	情報管理課管理係の住基ネット担当	2	43
区民課住民記録係管理担当用	住民記録係の係長級、住基ネット担当	6	49
区民課管理担当用	各区民係及び個人番号カード交付担当の係長級、調整担当係長	26	36
区民課一般職員等用	住民記録係、各区民係、個人番号カード交付担当	130	20
その他住基ネットを利用する部署用	情報管理課、課税課、国保年金課、障害者施策課、介護保険課、各福祉事務所、杉並保健所保健予防課、杉並保健所保健サービス課、子ども家庭部管理課	97	7

注２：令和５年８月１日時点で統合端末の操作権限が付与されている職員の人数（休職中等の職員は除く）。

４　実施時期

令和５年 11 月下旬～12 月頃を予定

５　昨年度からの変更点

（１）統合端末のＯＳのパスワード管理について

統合端末を設置している課（情報管理課及び区民課）以外で住基ネットを利用する課を利用課としており、利用課が住基ネットを使用する際は、情報管理課の統合端末を使用している。

情報管理課に設置されている統合端末のＯＳのパスワード管理は、情報管理課が実施しているため、利用課が使用する際は、情報管理課が代わりに端末のログインを行ってから使用させている。

利用課は統合端末のＯＳのパスワード管理を行っていないため、情報管理課及び利用課を対象とした設問を追加・修正することで、より適切な設問内容とする。（設問連番 19、21）

＜参考＞設問連番 19、21 に係る変更内容

設問	設問連番	対象者	設問内容
9	19	情報管理課管理係の住基ネット担当	ＦＷ・統合端末のＯＳのパスワードを他人（情報管理課の住基ネット業務取扱者以外の者）に知られないように管理している。
9	20	住民記録係、各区民係、個人番号カード交付担当の職員	統合端末のＯＳ（ＪＵＫＩＮＵＳＥＲ）のパスワードを他人（住基ネット業務取扱者以外の者）に知られないように管理している。
9	21	上記以外で住基ネットを利用する部署の職員	統合端末のＯＳ（ＪＵＫＩＮＵＳＥＲ）のパスワードは情報管理課管理係の住基ネット担当が管理している。 ※統合端末のＯＳのログインが必要な時は、情報管理課管理係の住基ネット担当の職員にログインしてもらっている。

上表のとおり設問連番 19 の下線部を修正、設問連番 21 を追加する。

（２）その他

・不正行為を抑止し、住基ネットのセキュリティ対策について再認識できるようにするため、住基ネットの利用においては目的外利用が禁止されている旨を設問に追記する。（設問連番１、３）

・氏名等により本人確認情報検索を行う際、事前に「氏名等による住基ネット検索記録票」に記入し、他の職員の確認を受けた上で検索を行う運用に変更しているため、その旨を設問に追記する。（設問連番 44）

以上

部会資料５

情報提供ネットワークシステム緊急時対応訓練について

１　目的

現在、情報提供ネットワークシステムは安定した運用が維持されているが、情報提供ネットワークシステムで不正アクセス・不正プログラム被害やネットワーク機器の故障等の情報セキュリティインシデント（※１）が発生した場合、安全性確保のための対応が必要になる。迅速かつ適切に安全性を確保するため、平時からの備えとして、情報提供ネットワークシステム緊急時対応訓練を実施する。

２　訓練内容

情報提供ネットワークシステムにおいて、ネットワークを当面停止する必要がある障害が発生したことを想定し、下表のとおり、情報連携実施課への連絡確認を行う。より実態に沿った訓練にするため、情報提供ネットワークシステム接続運用規程に基づきデジタル庁が実施する「情報提供ネットワークシステム異常時対応訓練」の機会を利用する。

なお、障害の規模は、区民生活や行政運営への広範な被害が発生するインシデントレベル３を想定し、CSIRT 構成員等への役割・連絡確認をあわせて行う。

訓練対象	訓練内容
情報管理課	○デジタル庁から障害情報（訓練情報）を受信し、インシデント発生時の窓口の PoC 担当者（※２）へ報告する。 ○報告を受けた PoC 担当者は、CSIRT 情報連絡体制にそって CSIRT 管理者への報告等の対応を行う。 ○情報連携実施課へ障害情報を連絡する。
情報連携実施課	○情報管理課から障害情報を受信した職員は、課内の情報連携端末操作員に共有する。
CSIRT 構成員	○CSIRT 情報連絡体制にそって情報共有する。あわせて自身の役割確認を行う。 ○訓練終了後に自身の役割を確認できたかのアンケートを行い、訓練効果を測定する。

３　訓練実施時期

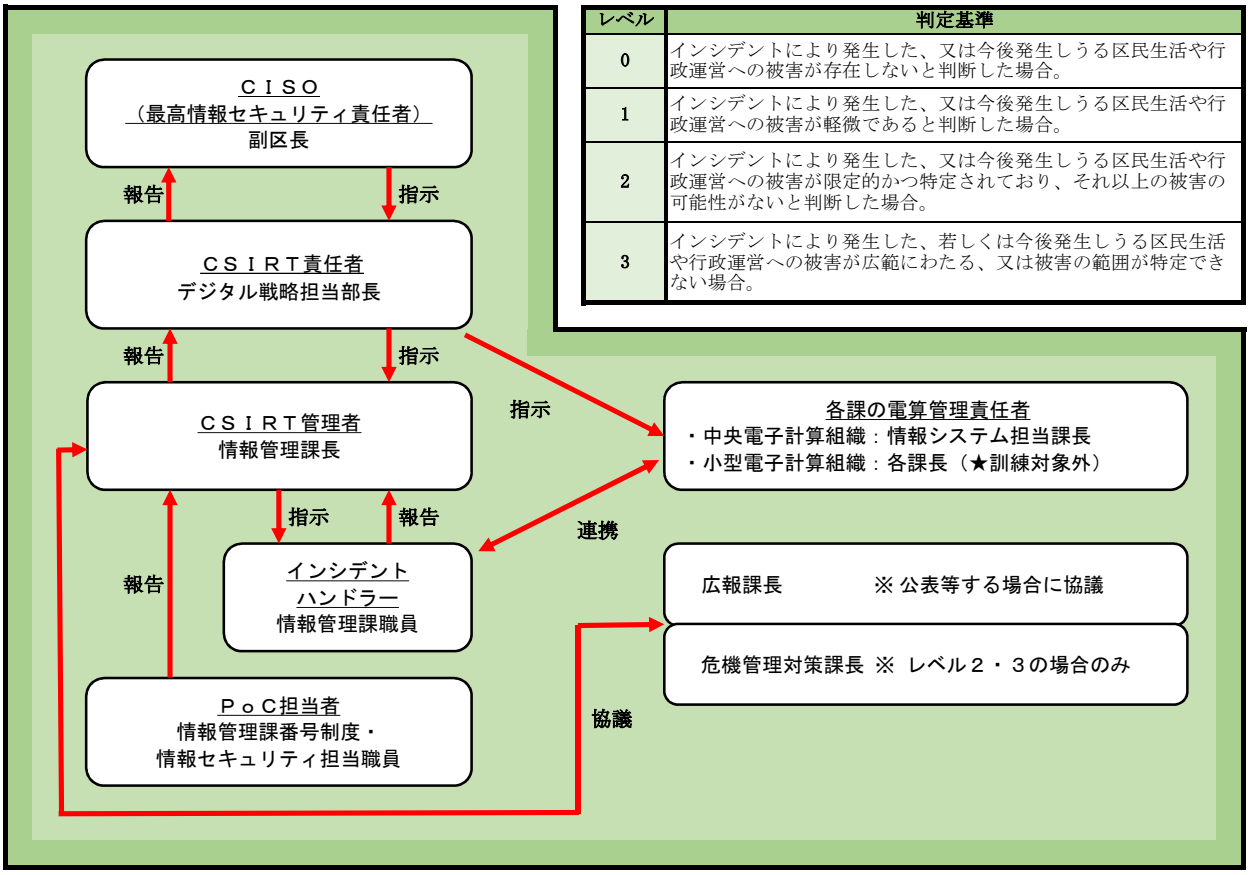
令和５年 10～12 月

※１　ウイルス感染や不正アクセス、機密情報の流出等のセキュリティ上の脅威となる事象を指す。

※２　情報セキュリティインシデントを発見した者からの通報を受ける、統一的な窓口担当者を指す。CSIRT 構成員及びその役割は、別紙のとおり。

杉並区ＣＳＩＲＴ情報連絡体制

部会資料５　別紙



レベル	判定基準
0	インシデントにより発生した、又は今後発生しうる区民生活や行政運営への被害が存在しないと判断した場合。
1	インシデントにより発生した、又は今後発生しうる区民生活や行政運営への被害が軽微であると判断した場合。
2	インシデントにより発生した、又は今後発生しうる区民生活や行政運営への被害が限定的かつ特定されており、それ以上の被害の可能性がないと判断した場合。
3	インシデントにより発生した、若しくは今後発生しうる区民生活や行政運営への被害が広範にわたる、又は被害の範囲が特定できない場合。

インシデント発生時の主な所掌事項一覧

名称	役職・課	インシデント発生時の主な所掌事項等
ＣＩＳＯ 最高情報セキュリティ責任者	副区長	・ＣＳＩＲＴ責任者への指示を行う。
ＣＳＩＲＴ責任者	デジタル戦略担当部長	・ＣＳＩＲＴの総括を行う。 ・ＣＩＳＯへの調整及び報告を行う。 ・電算管理責任者へのインシデント対応の指示を行う。
ＣＳＩＲＴ管理者	情報管理課長	・インシデントレベルを判定する。 ・インシデント対応の指示及び進行管理を行う。 ・ＣＳＩＲＴ責任者への報告を行う。 ・危機管理対策課、広報課と対応について協議する。
電算管理責任者	中央電算 情報システム担当課長 小型電算 各課長（★訓練対象外）	・インシデント対応について、ＣＳＩＲＴ責任者の指示に従う。
インシデントハンドラー	情報管理課職員	・ＣＳＩＲＴ管理者の補佐を行う。 ・インシデント対応を行う。 ・ＣＳＩＲＴ管理者にインシデント対応の進行状況等について報告し、指示を受ける。
ＰｏＣ担当者	情報管理課番号制度・情報セキュリティ担当職員	・インシデントの通報を受けた場合、速やかにＣＳＩＲＴ管理者に報告する。
協議先Ⅰ	危機管理対策課長	・レベル２・３の場合、危機管理対応についてＣＳＩＲＴ管理者と協議する。
協議先Ⅱ	広報課長	・公表を行う場合は、ＣＳＩＲＴ管理者と協議し、その結果をＣＳＩＲＴ責任者に報告し、承認を得る。

部会資料６

情報提供ネットワークシステム
安全措置実施状況等に関する職員自己点検について

１　目的及び概要

情報提供ネットワークシステム接続運用規程に基づく安全管理措置として、情報提供ネットワークシステムに係る事務に従事する職員へ適切な教育を実施する必要がある。各情報連携事務における教育の実施状況は、デジタル庁が実施する自己点検により確認できるが、当該教育内容に係る各職員の理解度の把握することは難しい。これを踏まえ、各職員の理解度を把握し、教育の有効性の評価を行うことで、教育内容の改善等につなげることを目的として自己点検を実施する。

２　自己点検実施方法

（１）調査形式

情報連携端末を所管課に設置している課と情報管理課に設置してある情報連携端末を使用する課に分け、設問ごとに「はい」又は「いいえ」で回答し、必要に応じて、その回答理由等を記載する。

自己点検種別	対象課	対象者数（※１）	設問数
情報連携端末設置課用（※２）	情報管理課、人事課、区民課、課税課、納税課、国保年金課、障害者施策課、介護保険課、各福祉事務所、杉並保健所保健予防課、杉並保健所保健サービス課、子ども家庭部管理課、地域子育て支援課	170	24
情報管理課設置の情報連携端末利用課用	保健福祉部管理課、高齢者在宅支援課、保育課、住宅課	12	21

※１：令和５年８月１日時点で情報連携端末の操作権限が付与されている職員の人数であり、休職中等の職員は除く。

※２：住民情報系端末から情報照会できる端末を含む。

（２）内容

別紙のとおり

３　実施時期

令和５年 11 月下旬～12 月頃を予定。

４　昨年度との変更点

設問№15には、２つの設問内容が含まれているため、設問を２つに分け、それぞれに対してそれぞれ回答が出来るように修正した。

＜参考＞変更内容

令和４年度		令和５年度	
設問	設問内容	設問	設問内容
15	DV・虐待等被害者等支援対象者の団体内統合宛名番号には、その支援措置を所管する課が、不開示フラグ・自動応答不可フラグを設定することを知っている。また、支援措置が解除された等により自動応答不可フラグを解除する時は、所属の自動応答制限等運用担当者が他の情報連携実施課に通知し、解除の可否について確認することを知っている。	15	DV・虐待等被害者等支援対象者の団体内統合宛名番号には、その支援措置を所管する課が、不開示フラグ・自動応答不可フラグを設定することを知っている。
―	―	16	支援措置が解除された等により自動応答不可フラグを解除する時は、所属の自動応答制限等運用担当者が他の情報連携実施課に通知し、解除の可否について確認することを知っている。

令和５年度情報提供ネットワークシステム安全措置実施状況等に関する職員自己点検

部会資料６別紙

設問No.	設問内容	回答欄	理由・具体的な内容記述欄 回答後、当該記述欄がグレーにならなかった場合、回答欄の答えとなった理由　又は　設問の具体的な内容を記述してください。		根拠規定	情報連携端末設置課	情報連携未設置課端末
1	番号利用事務に従事するにあたり、事前にセキュリティに関する研修(eラーニング含む)を受講した。			←「いいえ」の場合、未受講の理由	・杉並区特定個人情報取扱指針 ５（２）① ・各課セキュリティ実施手順	○	○
2	情報連携端末で障害、不正アクセス、特定個人情報の漏えい等が発生した場合は、情報管理課に報告することを知っている。				・情報セキュリティ対策基準「（情報セキュリティインシデントへの対応）第 52 条」 ・マイナンバー等事務に係る緊急事案の報告手順 ・杉並区情報セキュリティインシデントに関する緊急即応体制（ＣＳＩＲＴ）管理運営要綱 ・各課セキュリティ実施手順	○	○
3	退庁時等、執務室に職員が不在となる時には、情報連携端末の電源の切断や書庫・出入口の施錠状態について確認し、記録（例：退庁時のチェック表等）をしている。 ※課で実施している場合は「はい」と回答してください。			←「いいえ」の場合、未実施の理由	・セキュリティ対策基準「（管理区画の入退室管理等）第36条」 ・特定個人情報取扱指針５（６）情報システム室等の安全管理 ・各課セキュリティ実施手順	○	
4	執務室に外部の者を入室させる場合には、手順書で決められたルール（入退出記録等）を遵守している。 ※ルールはあるが、実際には外部の者が入室することがなかった場合は「はい」と回答してください。			←「いいえ」の場合、遵守していない理由	・セキュリティ対策基準「（管理区画の入退室管理等）第36条」 ・特定個人情報取扱指針５（６）情報システム室等の安全管理 ・各課セキュリティ実施手順	○	○
5	情報管理課の執務室内に設置している情報連携端末を使用する場合は、端末使用記録簿に記入し、情報管理課の職員から立入証を受け取った上で操作している。 ※情報管理課の執務室内に設置している情報連携端末を使用しない場合は「はい」と回答してください。				・セキュリティ対策基準「（管理区画の入退室管理等）第36条」 ・特定個人情報取扱指針５（６）情報システム室等の安全管理 ・各課セキュリティ実施手順	○	○
6	情報連携端末の操作員パスワードを、第三者に知られないように管理している。			←管理方法（記憶している、手帳に記載等）	・セキュリティ対策基準「（パスワードの取扱い）第54条」 ・各課セキュリティ実施手順（庁内ネットワーク利用要領「（パスワード管理）第13条」）	○	○
7	情報連携端末が、ログインされたまま放置されている状態を見かけたことがある。 （情報照会機能を持つ住民情報系システムにおいては、職員IDやパスワードを入力しなくても情報照会機能を操作できる状態を指すものとする）				・セキュリティ対策基準「（クリアデスク・クリアスクリーン）第45条」 ・特定個人情報取扱指針５（５）（サ）第三者の閲覧の防止 ・各課セキュリティ実施手順	○	○
7-1	（設問７で「はい」と回答した方） 何を処理する画面が表示されていたか覚えている場合は、その内容を「理由・具体的な内容記述欄」に記載する。					○	○
7-2	（設問７で「はい」と回答した方） このような状況を見つけた際、ログインしたままの職員に声をかけているか。					○	○
7-3	（設問７で「はい」と回答した方） このような状況を放置すると、どんなリスクがあると思うか、「理由・具体的な内容記述欄」に記入する。					○	○
8	情報連携端末で、業務上必要のない個人情報の検索、抽出は行っていない。			←「いいえ」の場合、その理由	・セキュリティ対策基準「（情報資産の利用）第 18条」 ・特定個人情報取扱指針５（４）（イ）アクセス制限 ・各課セキュリティ実施手順	○	○

設問No.	設問内容	回答欄	理由・具体的な内容記述欄 回答後、当該記述欄がグレーにならなかった場合、 回答欄の答えとなった理由　又は　設問の具体的な内容を記述してください。		根拠規定	情報連携端末設置課	情報連携端末未設置課
9	原則として、情報連携端末に可搬記録媒体（USBメモリ等）を接続してはいけないことを知っている。 ※統合端末との連携を行う時に、情報管理課保有の連携専用媒体（USBメモリ）を接続する場合を除く。				・セキュリティ対策基準「（職員等の業務端末等の管理）第33条 ・特定個人情報取扱指針５（５）（シ）記録機能を有する機器・媒体の接続制限 ・各課セキュリティ実施手順	○	○
10	自課に設置された情報連携端末には、盗難や盗み見等を防止するための対策（セキュリティワイヤー、パーテーション、のぞき見防止フィルター等）が施されている。 ※自課に情報連携端末が設置されていない場合は、「はい」と回答してください。			←「いいえ」の場合、行われていない理由	・セキュリティ対策基準「（クリアデスク・クリアスクリーン）第45条」 ・特定個人情報取扱指針５（５）（サ）第三者の閲覧の防止 ・各課セキュリティ実施手順	○	
11	退庁時等、執務室に職員が不在となる時、個人情報が含まれる書類を書庫等に保管し、施錠している。			←「いいえ」の場合、その理由	・セキュリティ対策基準「（情報資産の保管）第19条」 ・特定個人情報取扱指針５（４）（キ）媒体等の管理等 ・各課セキュリティ実施手順	○	○
12	情報連携端末から印刷した個人情報が含まれる書類を廃棄する際には、裁断・溶解等を行っている。			←「いいえ」の場合、具体的な廃棄方法、その理由	・セキュリティ対策基準「（情報資産の保管）第19条」 ・特定個人情報取扱指針５（４）（キ）媒体等の管理等 ・各課セキュリティ実施手順	○	○
13	個人情報が含まれる書類を出力するプリンタは、外部の者の手の届かない場所に設置されている。			←「いいえ」の場合、その理由	・セキュリティ対策基準「（プリンタ等のセキュリティ管理）第66条」 ・各課セキュリティ実施手順	○	
14	プリンターから出力した個人情報が含まれる書類を、プリンターに放置していない。 ※個人情報が含まれる書類をプリンターから出力していない場合は「はい」と回答してください。			←「いいえ」の場合、どんな時に放置、その理由	・セキュリティ対策基準「（クリアデスク・クリアスクリーン）第45条」 ・特定個人情報取扱指針５（５）（サ）第三者の閲覧の防止 ・各課セキュリティ実施手順	○	○
15	DV・虐待等被害者等支援対象者の団体内統合宛名番号には、その支援措置を所管する課が、不開示フラグ・自動応答不可フラグを設定することを知っている。					○	○
16	支援措置が解除された等により自動応答不可フラグを解除する時は、所属の自動応答制限等運用担当者が他の情報連携実施課に通知し、解除の可否について確認することを知っている。					○	○
17	DV・虐待等被害者に関して他団体へ情報照会を行う時は、不開示コードを設定している。 ※設定する事案が発生していない場合は「はい」と回答してください。			←「いいえ」の場合、その理由		○	○
18	情報提供ネットワークシステムでの異常事象発生時に、速やかに関係課が連携し対応が実施できる状況にあることを確認するため、訓練を毎年実施していることを知っている。					○	○
19	情報提供ネットワークシステムで障害等が発生し異常時運用に切り替えると連絡を受けた時、どのように対応すればよいか知っている。					○	○
20	情報連携端末等のセキュリティについて、「危ない」と感じたことはあるか。			←「はい」の場合、具体的な事例を記載		○	○
21	情報連携端末等のセキュリティについて、意見等はあるか。					○	○