ＤＸ・議会改革に関する特別委員会資料
令 和 ７ 年 １２ 月 ９ 日
政 策 経 営 部 情 報 管 理 課

サイバーセキュリティを確保するための方針の策定について

地方自治法の一部が改正され、令和８年４月１日から、同法第 244 条の６第１項の規定に基づき、特別区の議会及び長その他の執行機関は、それぞれサイバーセキュリティを確保するための方針（以下「方針」とする。）を定め、これに基づき必要な措置を講じなければならないものとされました。

令和７年４月１日付けで示された国の指針（令和７年４月１日付け総行サ第１号）では、「必要に応じて既存の情報セキュリティ基本方針の見直しを行ったものの策定をもって方針に位置付けることとして差し支えないこと」、「必要となる情報セキュリティ対策が概ね同様のものとなるなど別個の方針を定めることが非効率となるような場合は共同策定などの運用上の工夫を行うことも可能であること」が示されました。

これらのことを踏まえ、以下のとおり方針の策定に向けて検討を行い、このたび方針を策定したのでご報告します。

１　検討組織等

（１）検討組織

区政イノベーション本部で方針案を策定することとし、杉並区情報セキュリティ基本方針の策定等に関することを所掌事項としている「デジタル・セキュリティ部会」において具体的な検討を行った。

（２）区長部局と他の執行機関の方針案の共同策定

方針案の内容については、区長部局と他の執行機関（教育委員会、選挙管理委員会、監査委員及び農業委員会）で大きな相違がないものと想定し、方針案の策定に当たっては、区長部局と他の執行機関で共同で行った。

２　策定の方法

（１）総務省が定める「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」に従い、既存の杉並区情報セキュリティ基本方針に必要な修正を行うことで、サイバーセキュリティを確保するための方針を包含することとした。

（２）方針は各執行機関において自らの方針として決定する必要があることから、１つの方針を共有するのではなく、執行機関ごとに策定することとした。

３　確定した区長部局の方針案（既存の情報セキュリティ基本方針の見直し）の内容

別紙１－１及び別紙１－２のとおり

（１）目的
（２）定義
（３）対象とする脅威
（４）適用範囲
（５）職員等の遵守義務及び違反への対応
（６）情報セキュリティ対策
（７）情報セキュリティ監査及び自己点検の実施
（８）情報セキュリティポリシーの見直し
（９）情報セキュリティ対策基準の策定
（10）情報セキュリティ実施手順の策定

４　確定した区長部局の方針案と他の執行機関の方針案の比較表

別紙２～別紙５のとおり

５　今後の予定

令和８年３月まで　各執行機関で方針に基づく情報セキュリティ対策基準等の策定
　　４月　　方針施行

別紙 1-1

新旧対照表及び国ガイドラインとの比較表

○杉並区情報セキュリティ基本方針

新	旧	国ガイドライン	備考
杉並区情報セキュリティ基本方針 策定日　令和７年12月１日 目次 杉並区情報セキュリティ基本方針	杉並区情報セキュリティ基本方針 策定日　平成15年８月５日 目次 杉並区情報セキュリティ基本方針		○「情報セキュリティ」は、紙媒体や電子媒体など、あらゆる形式の情報とその関連資産を保護する広範な概念であり、「サイバーセキュリティ」は、主に電子化された情報、ネットワーク、システム、デバイスなど、デジタル空間における情報を守ることに重点を置いているとされ、**「情報セキュリティ」の方が「サイバーセキュリティ」より範囲が広い**こと、国ガイドライン（総務省の「**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**」。以下同じ。）でも「サイバーセキュリティ」を包含したものとして「情報セキュリティ基本方針」としていることから、従来どおり「杉並区情報セキュリティ基本方針」とする。
1　目的 2　定義 （1）　ネットワーク （2）　情報システム （3）　情報資産 （4）　機密性 （5）　完全性 （6）　可用性 （7）　情報セキュリティ （8）　情報セキュリティポリシー （9）　住民情報系 (10)　内部情報系 (11)　インターネット接続系 (12)　通信経路の分割 (13)　無害化通信 3　対象とする脅威 4　適用範囲 （1）　行政機関の範囲 （2）　情報資産の範囲 5　職員等の遵守義務及び違反への対応 6　情報セキュリティ対策 （1）　組織体制 （2）　情報資産の分類と管理 （3）　情報システム全体の強靭性の向上 （4）　物理的セキュリティ （5）　人的セキュリティ （6）　技術的セキュリティ （7）　運用 （8）　業務委託と外部サービス（クラウドサービス）の利用 7　情報セキュリティ監査及び自己点検の実施 8　情報セキュリティポリシーの見直し 9　情報セキュリティ対策基準の策定 10　情報セキュリティ実施手順の策定	1　策定の目的 2　定義 （1）　情報セキュリティマネジメントシステム （2）　機密性 （3）　完全性 （4）　可用性 （5）　リスク評価 （6）　リスクマネジメント （7）　情報システム （8）　情報資産 （9）　情報セキュリティ 3　情報セキュリティ管理体制 4　職員の遵守義務及び違反への対応 5　外部委託事業者等への対応 6　情報資産の評価等 7　情報資産に対する脅威 8　情報セキュリティの対策 （1）　人的セキュリティ （2）　物理的セキュリティ （3）　情報システムセキュリティ 9　情報セキュリティ実施手順の策定 10　情報セキュリティ監査の実施 11　評価及び見直し		
		情報セキュリティ基本方針（宣言書） 今日、インターネットをはじめとする情報通信ネットワークや情報システムの利用は生活、経済、社会のあらゆる面で拡大している。一方で、個人情報の漏えい、不正アクセスや新たな攻撃手法による情報資産の破壊・改ざん、操作ミス等によるシステム障害等が後を絶たない。また、自然災害によるシステム障害や疾病を起因とするシステム運用の機能不全にも備える必要がある。 本市は、市民の個人情報や行政運営上重要な情報などを多数取り扱っている。また、電子自治体の構築が進み、多くの業務が情報システムやネットワークに依存している。したがって、これらの情報資産を様々な脅威から	○改正前（旧）の「１　策定の目的」が前文のような規定になっていることを踏まえ、この「情報セキュリティ基本方針（宣言書）」の内容については改正後（新）の「１　目的」にその内容を規定する。

新	旧	国ガイドライン	備考
		防御することは、市民の権利、利益を守るためにも、また、行政の安定的、継続的な運営のためにも必要不可欠である。また、本市には、地域全体の情報セキュリティ基盤を強化していく役割も期待されている。 　これらの状況を鑑み、本市における情報資産に対する安全対策を推進し、市民からの信頼を確保し、さらに地域に貢献するため、以下に積極的に取り組むことを宣言する。 （１）　情報セキュリティ対策に取り組むための全庁的な体制を確立する。 （２）　情報セキュリティ対策の基準として情報セキュリティ対策基準を策定し、その実行のための手順等を盛り込んだ実施手順を策定する。 （３）　本市の保有する情報資産を適正に管理する。 （４）　情報セキュリティ対策の重要性を認識させ、当該対策を適正に実施するために、職員等に対して必要な教育を実施する。 （５）　情報セキュリティインシデントが発生した場合又はその予兆があった場合に速やかに対応するため、緊急時対応計画を定める。 （６）　情報セキュリティ対策の実施状況の監査及び自己点検等を通して、定期的に対策の見直しを実施する。 （７）　全ての職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティ基本方針、情報セキュリティ対策基準及び情報セキュリティ実施手順を遵守する。 （８）　地域全体の情報セキュリティの基盤を強化するため、地域における広報啓発や注意喚起、官民の連携・協力等に積極的に貢献する。 令和○○年○○月○○日 ○○市長（又は、最高情報セキュリティ責任者）	
1　　目的	1　策定の目的	1．目的	○国ガイドラインでは端的に「目的」となっていることや、区の他の例規等の規定に合わせて文言を修正する。
今日、インターネットをはじめとする情報通信ネットワークや情報システムの利用は生活、経済、社会のあらゆる面で拡大している。 一方で、個人情報の漏えい、不正アクセスや新たな攻撃手法による情報資産の破壊・改ざん、操作ミス等によるシステム障害等が後を絶たない。また、自然災害によるシステム障害や疾病を起因とするシステム運用の機能不全にも備える必要がある。 さらに、昨今、国・地方公共団体・民間企業・住民の間のネットワークを通じた相互接続がますます進展していることに伴い、一つの地方公共団体の情報セキュリティ対策の不備や不適切なシステム利用が、他の地方公共団体や国の機関等の情報セキュリティにも脅威となり、その安全性や信頼性に影響を与える蓋然性が高くなっている。 杉並区（以下「区」という。）においても、区民の個人情報や行政運営上重要な情報などを多数取り扱っている。また、電子自治体の構築が進み、多くの業務が情報システムやネットワークに依存している。このため、これらの情報資産を様々な脅威から防御することは、区民の権利、利益を守るためにも、また、行政の安定的、継続的な運営のためにも必要不可欠である。 これらのことを踏まえ、他に定めがあるものを除き、区が実施する情報セキュリティ対策についての基本的な事項を定めるた	杉並区（以下「区」という。）は、昭和61年に、区が管理する情報を原則として公開する杉並区情報公開条例（昭和61年杉並区条例第38号）並びに個人情報の厳格な取扱い及び自己情報のコントロール権を盛り込んだ個人情報保護条例（昭和61年杉並区条例第39号）を同時制定するなど、情報の適正な管理に努めてきた。今日、区にはＩＴを活用し、区民サービスの向上、区民との情報共有の拡充、協働（パートナーシップ）の充実及び行政の効率化を図り質の高い行政運営をめざすこと（電子区役所の構築）が求められている。 したがって、区の行政情報はＩＴ（情報技術）によって取り扱われる比重が飛躍的に大きくなってきている。 ネットワークによる高度な情報化は、区の全ての分野に大きな変革をもたらす可能性がある反面、ネットワークを介したシステムに対する不正アクセスや攻撃、情報の漏洩や改ざんといった脅威（リスク）が増大する。原因を問わず、個人情報漏洩や情報システムの障害が発生した場合の影響は甚大であり、区に対する信頼は喪失する。 このため、個人情報はもとより、区が管理する全ての情報を区の情報資産ととらえ、これらをさまざまな脅威から守る効果的で実効性のある情報セキュリティ対策を講ずることが必要である。そこで区は、情報セキュリティを運営していくためのシステム（情報マネジメントシステム）を構築	本基本方針は、本市が保有する情報資産の機密性、完全性及び可用性を維持するため、本市が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。	○改正前の目的は平成15年の方針策定時に規定したものであり、前文のような記載であるが、「（電子区役所の構築）が求められている」などの記載が現状と合わなくなっている（現状はITの更なる活用が当然の前提）。「個人情報保護条例（昭和61年杉並区条例第39号）」も既に廃止した条例である。これらのことを踏まえ、国ガイドラインの宣言書の記載内容も踏まえて現状に合った規定に修正する。 ○改正後の目的の「さらに…」の段落は国ガイドラインに規定はないが、サイバーセキュリティ基本方針策定の背景として、令和７年４月１日付け国指針（案）に記載されている内容を踏まえて記載する。 ○改正後の目的では、**区長と他の執行機関とでそれぞれ別個の方針を定める**こと、**他に定めがないものは包括的にこの方針の適用**

新	旧	国ガイドライン	備考
めの基本方針として、また、地方自治法（昭和22年法律第67号）第244条の６第１項に規定するサイバーセキュリティを確保するための方針として、区が保有する情報資産の機密性、完全性及び可用性を維持することを目的に杉並区情報セキュリティ基本方針（以下「基本方針」という。）を定める。	し、情報資産を厳格に保護することを目的に情報セキュリティ基本方針（以下「基本方針」という。）を定める。		**対象とすることを明確化**するため、「他に定めがあるものを除き」とする。 ○改正後の目的では、この方針は、**地方自治法第244条の６第１項に規定するサイバーセキュリティを確保するための方針」でもあることを明確化**する。
2　定義 基本方針において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。	2　定義 基本方針における用語の意義は、次に定めるところとする。	2．定義	○規定の書きぶりが古いため今回の改正を機に他の例規等の規定に合わせて文言を修正する。
~~（1）　情報セキュリティマネジメントシステム（information security management system）~~ ~~組織のマネジメントとしてリスクに対する保証すべきレベルを決め、プランを持ち資源を配分して、継続的なマネジメントシステム（ＰＤＣＡモデル）の運用を実現するためのフレームワーク（枠組み）。~~	（1）　情報セキュリティマネジメントシステム（information security management system） 組織のマネジメントとしてリスクに対する保証すべきレベルを決め、プランを持ち資源を配分して、継続的なマネジメントシステム（ＰＤＣＡモデル）の運用を実現するためのフレームワーク（枠組み）。		○基本方針中に「情報セキュリティマネジメントシステム」が出てこないこと、令和２年度でISMSの認証取得を終了している実情を踏まえて削除する。
（4）　機密性 情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。 （5）　完全性 情報が破壊、改ざん又は消去されていない状態を確保することをいう。 （6）　可用性 情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。	（2）　機密性（confidentiality） アクセスを認可された（authorized）者だけが情報にアクセスできることを確実にすること。 （3）　完全性（integrity） 情報及び処理方法が、正確であること及び完全であることを保護すること。 （4）　可用性（availability） 認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること。	（5）　機密性 情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。 （6）　完全性 情報が破壊、改ざん又は消去されていない状態を確保することをいう。 （7）　可用性 情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。	○規定の順序の考え方は以下のとおり。 ・国ガイドラインを踏まえつつ、「２　定義」の中で、ある定義が他の定義の中に含まれる場合はその他の定義より前に規定する。たとえば「（７）情報セキュリティ」は「情報資産の機密性、完全性及び可用性を維持することをいう。」としていることから、「（４）　機密性」「（５）　完全性」「（６）　可用性」は「（７）情報セキュリティ」より前に規定する。 ・「３　対象とする脅威」以降で定義が出てくるものは定義が出てくる順序で規定する。たとえば「（８）　情報セキュリティポリシー」は「５　職員等の遵守義務及び違反への対応」、「（９）　住民情報系」は「６　情報セキュリティ対策」で出てくることから「２　定義」でもその順序で規定する。 ・旧の定義で「（２）　機密性（confidentiality）」のように一部英単語が記載されているものがあるが、国ガイドラインでは記載していないこと、一部のみ英単語を記載する必要性が乏しいこと、現在も目次と合致していないことから削除する。
	（5）　リスク評価 リスクの重大さを決定するために、算定されたリスクを与えられたリスク基準と比較するプロセス。 （6）　リスクマネジメント リスクに関して組織を指揮し管理する調整された活動。		○改正前の「３　情報セキュリティ管理体制」を削除することに伴い、「（５）　リスク評価」及び「（６）　リスクマネジメント」の定義も不要となるため削除する。削除の理由は「３　情報セキュリティ管理体制」の備考欄に記載する。
（1）　ネットワーク コンピュータ等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。		（1）　ネットワーク コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。	
（2）　情報システム 区の組織運営に必要な情報の収集・蓄積・処理・伝達・利用に関わるコンピュータのハードウェア、ソフトウェア、データベース、ネットワーク、保管・蓄積装置、記録媒体等の仕組みをいう。	（7）　情報システム 中央電子計算組織及び小型電子計算組織におけるネットワーク、ハードウェア、ソフトウェア及び記録媒体で構成され、事務処理を行う仕組み。	（2）　情報システム コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。	○区の管理するすべての情報システムが対象となっていることを分かりやすくするため規定を修正する。 ○記録媒体等の「等」は記録された情報やその管理方法なども含意することがあり得るため規定する。
（3）　情報資産 情報システムで取り扱う全ての情報及び情報システムの開発と運用に係る情報並びに紙等の有体物としての情報をいう。	（8）　情報資産 情報システムで取り扱う全ての情報及び情報システムの開発と運用に係る情報並びに紙等の有体物としての情報をいう。		○国ガイドラインには定義がないが、「（７）情報セキュリティ」の定義の中で「情報資産」が出てくること、「情報資産」とは何か定義が必要であることから、「情報セキュリティ」の前に規定する。
（7）　情報セキュリティ 情報資産の機密性、完全性及び可用性を維持することをいう。 （8）　情報セキュリティポリシー	（9）　情報セキュリティ 情報資産の機密性、完全性及び可用性を維持すること。	（3）　情報セキュリティ 情報資産の機密性、完全性及び可用性を維持することをいう。 （4）　情報セキュリティポリシー	

新	旧	国ガイドライン	備考
基本方針及び情報セキュリティ対策基準をいう。		本基本方針及び情報セキュリティ対策基準をいう。	
（９） 住民情報系 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）第２条第11項に規定する個人番号利用事務等に係る情報システム及びその情報システムで取り扱うデータをいう。		（８） マイナンバー利用事務系（個人番号利用事務系） 個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。	○国ガイドラインでいう「マイナンバー利用事務系（個人番号利用事務系）」を、杉並区では従来から「住民情報系」と呼称していることを踏まえて規定する（杉並区情報セキュリティ対策基準第２条第２項第７号参照）。
(10) 内部情報系 総合行政ネットワーク（ＬＧＷＡＮ）に接続された情報システム及びその情報システムで取り扱うデータをいう。		（９） ＬＧＷＡＮ接続系 ＬＧＷＡＮに接続された情報システム及びその情報システムで取り扱うデータをいう（マイナンバー利用事務系を除く。）。	○国ガイドラインでいう「ＬＧＷＡＮ接続系」を、杉並区では従来から「内部情報系」と呼称していることを踏まえて規定する（杉並区情報セキュリティ対策基準第２条第２項第８号参照）。
(11) インターネット接続系 インターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。		(10) インターネット接続系 インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。	○国ガイドラインと「インターネット接続系」という名称自体は同じであるが、定義の内容は杉並区情報セキュリティ対策基準第２条第２項第９号の規定に合わせて規定する。
(12) 通信経路の分割 内部情報続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。 (13) 無害化通信 インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。		(11) 通信経路の分割 ＬＧＷＡＮ接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。 (12) 無害化通信 インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。	
	3 情報セキュリティ管理体制 基本方針の実効性を高め、情報セキュリティを適正に管理していくために、計画立案・運用・見直し及び改善のマネジメントサイクルに対する経営層の役割と責任を明確にした管理体制（杉並区デジタル・セキュリティ部会。以下「部会」という。）を整備する。部会はリスク評価の基準を確立するとともに、リスクマネジメントの環境を整備するために、情報セキュリティに関する全般的な方向性かつ目標の設定及び計画的な運営を図る。		○情報セキュリティ管理体制は改正後の「６ 情報セキュリティ対策－（１） 組織体制」と重なること、「リスク評価」や「リスクマネジメント」は平成15年度当時認証取得を目指していたISMSの名残であり、令和2年度を最後にISMSの認証取得は終了している実情等を踏まえて削除する。
5 職員等の遵守義務及び違反への対応 職員、臨時・非常勤職員等（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。また、基本方針の実効性を確保するために違反者に対しては、必要な処分等を行う。	4 職員の遵守義務及び違反への対応 区が管理する情報資産について、職員は、情報セキュリティの重要性を認識するとともに法令等を遵守する。また、基本方針の実効性を確保するために違反者に対しては、必要な処分を行う。	５．職員等の遵守義務 職員、臨時・非常勤職員等（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。	○国ガイドラインの「臨時・非常勤職員等」の「等」に何が含まれるかは明確でないが、区への派遣職員などが想定される。そうすると職員でない者もあり得るため、国ガイドラインに合わせて「職員等」と規定するとともに、必要な規定の整備を行う。
~~5 外部委託事業者等への対応~~ ~~脅威から情報資産を保護するため、外部委託事業者等（区の業務を受託する公益法人、民間事業者（ＮＰＯを含む））との間で適切な契約を締結し、その完全な履行を確保する。~~	5 外部委託事業者等への対応 脅威から情報資産を保護するため、外部委託事業者等（区の業務を受託する公益法人、民間事業者（ＮＰＯを含む））との間で適切な契約を締結し、その完全な履行を確保する。		○改正後の「７ 情報セキュリティ対策－（８） 業務委託と外部サービス（クラウドサービス）」の内容と重なること、「完全な履行を確保する」の意味合いが分かりづらいことから削除する。
~~6 情報資産の評価等~~ ~~区が管理する情報資産を機密性、完全性、可用性のそれぞれの視点から評価し、情報資産への脅威の発生度合いや発生した場合の影響を考慮するとともに、適切な情報セキュリティ対策を講ずるものとする。~~	6 情報資産の評価等 区が管理する情報資産を機密性、完全性、可用性のそれぞれの視点から評価し、情報資産への脅威の発生度合いや発生した場合の影響を考慮するとともに、適切な情報セキュリティ対策を講ずるものとする。		○改正後の「７ 情報セキュリティ対策－（２） 情報資産の分類と管理」の内容と重なることから削除する。
3 対象とする脅威 情報資産に対する脅威として、以下のものを想定し、情報セキュリティ対策を実施する。 （１） 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情	7 情報資産に対する脅威 特に認識すべき脅威を例示すれば、次のとおりである。 （１） 部外者の侵入による情報資産の破壊・盗難、故意の不正アクセス又は不正操作による情報資産の破壊・盗聴・改ざん・消去等の脅威	３．対象とする脅威 情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。 （１） 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、	

新	旧	国ガイドライン	備考
報の詐取、内部不正等 （２） 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等 （３） 地震、落雷、火災等の災害によるサービス及び業務の停止等 （４） 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等 （５） 電力供給の途絶、通信の断絶、水道供給の途絶等のインフラの障害からの波及等	（２） 職員又は外部委託事業者等による情報資産の持出、誤操作、パスワード等の不適切管理、故意の不正アクセス又は不正行為による破壊・盗聴・改ざん・消去等、規定外の端末接続による漏洩等の脅威 （３） コンピュータウィルス、地震、落雷、火災等の災害並びに事故、故障等による業務停止の脅威	重要情報の詐取、内部不正等 （２） 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等 （３） 地震、落雷、火災等の災害によるサービス及び業務の停止等 （４） 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等 （５） 電力供給の途絶、通信の断絶、水道供給の途絶等のインフラの障害からの波及等	
4 適用範囲 （１） 行政機関の範囲 基本方針が適用される範囲は、区長、杉並区組織規則（昭和50年杉並区規則第９号）第７条第１項に規定する本庁の部及び室、同条第２項に規定する室並びに同規則別表第３に規定する行政機関とする。		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、内部部局、行政委員会、議会事務局、消防本部及び地方公営企業とする。	○令和７年８月19日付け国Q＆Aによると、執行機関等の事務局職員はそれぞれの執行機関等で定める基本方針が適用されることから、区長の基本方針が適用対象となる行政機関の範囲を規定する。なお、杉並区立子供園は規則別表第３に規定する行政機関に含まれる。
（２） 情報資産の範囲 基本方針が対象とする情報資産は、次のとおりとする。		（２） 情報資産の範囲 本基本方針が対象とする情報資産は、次のとおりとする。	
①~~ネットワーク及び~~情報システム~~並びにこれらに関する設備及び電磁的記録媒体~~等		①ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体	○国ガイドラインでは規定しているが、「ネットワーク」は「情報システム」の定義に含まれるため削除する。②についても同様である。 ○「これらに関する設備及び電磁的記録媒体」も「情報システム」の定義に含まれるため削除する。
②~~ネットワーク及び~~情報システムで取り扱う情報（これらを印刷した文書を含む。） ③情報システムの仕様書及びネットワーク図等のシステム関連文書		②ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。） ③情報システムの仕様書及びネットワーク図等のシステム関連文書	
6 情報セキュリティ対策 上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。	8 情報セキュリティ対策 脅威から情報資産を保護するために、人的、物理的、技術的及び運用の面から情報セキュリティ対策を講ずるものとする。	6．情報セキュリティ対策 上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。	
（１） 組織体制 区の保有する情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。		（１） 組織体制 本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。	○改正前の「３ 情報セキュリティ管理体制」と同様に、区長は全庁横断的な組織体制を確立することとする。 ○各執行機関で個別に方針を定めるため、当該執行機関の方針に基づく組織体制は個々に定める必要がある。
（２） 情報資産の分類と管理 区の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。 （３） 情報システム全体の強靭性の向上 情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。 ①住民情報系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。 ②内部情報系においては、ＬＧＷＡＮと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を		（２） 情報資産の分類と管理 本市の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。 （３） 情報システム全体の強靭性の向上 情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。 ①マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。 ②ＬＧＷＡＮ接続系においては、ＬＧＷＡＮと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化	

新	旧	国ガイドライン	備考
実施する。 ③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。		通信を実施する。 ③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。	
（５） 人的セキュリティ 情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。 （８） 業務委託と外部サービス（クラウドサービス）の利用 業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。	（１） 人的セキュリティ 職員の故意又は過失による不正行為から情報資産を適切に保護するため、情報セキュリティに関する権限や責任を定め、基本方針の内容を周知徹底するなど、十分な教育及び啓発が実施できるよう必要な管理策を講じる。また、外部委託事業者等に対しては秘密保持の徹底等、必要な対策を講じる。	（５） 人的セキュリティ 情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。 （８） 業務委託と外部サービス（クラウドサービス）の利用 業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。	○改正前の「職員の故意又は過失による不正行為から情報資産を適切に保護するため」という文言は、「６　情報セキュリティ対策」冒頭の「上記３の脅威から情報資産を保護するため」と重なるため不要であると判断した。
外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。 ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。		外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。 ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。	
（４） 物理的セキュリティ サーバ、情報システム室を有する場合には、それらの管理について、また職員等のパソコン等の管理について、物理的な対策を講じる。	（２） 物理的セキュリティ 区の施設への不正な立入り、情報資産の破壊・盗難等を防止するため、入退室管理等、適切な管理策を講ずる。	（４） 物理的セキュリティ サーバ、情報システム室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。	○改正前の「区の施設への不正な立入り、情報資産の破壊・盗難等を防止するため」という文言は、「６　情報セキュリティ対策」冒頭の「上記３の脅威から情報資産を保護するため」と重なるため不要であると判断した。
（６） 技術的セキュリティ 情報システムへのアクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。	（３） 情報システムセキュリティ 情報資産を不正アクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等、適切な対策を講ずる。	（６） 技術的セキュリティ コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。	○改正前の「情報資産を不正アクセス等から適切に保護するため」という文言は、「６情報セキュリティ対策」冒頭の「上記３の脅威から情報資産を保護するため」と重なるため不要であると判断した。
（７） 運用 情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。	また、システム開発等委託業務の管理監督、ネットワークの監視、基本方針の遵守状況の確認等、運用面での対策を講ずる。	（７） 運用 情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。	
		（９） 評価・見直し 情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。	○改正後の「８　情報セキュリティポリシーの見直し」と同内容であるため規定は不要であると判断した。
９　情報セキュリティ対策基準の策定 上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。		９．情報セキュリティ対策基準の策定 上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。	
10　情報セキュリティ実施手順の策定 情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。 なお、情報セキュリティ実施手順は、公	９　情報セキュリティ実施手順の策定 情報資産に対するリスク分析結果への対応を評価したうえで、各所管で業務内容に応じた具体的な情報セキュリティ実施手順（以下「実施手順」という。）を策定するものとする。	10．情報セキュリティ実施手順の策定 情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。 なお、情報セキュリティ実施手順は、	

新	旧	国ガイドライン	備考
にすることにより区の組織運営に重大な支障を及ぼすおそれがあることから非公開とする。		公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。	
7　情報セキュリティ監査及び自己点検の実施 　情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。	10　情報セキュリティ監査の実施 　基本方針及び実施手順が遵守されていることを検証するため、定期的に監査を実施する。	7．情報セキュリティ監査及び自己点検の実施 　情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。	○現在情報管理課の職員が毎年度全課の情報セキュリティ監査の事務を担っているが、**令和８年度以降は各執行機関でそれぞれ定期監査**を行うこととなる。
8　情報セキュリティポリシーの見直し 　情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討した上で、情報セキュリティポリシーを見直す。	11　評価及び見直し 　情報セキュリティ監査の結果等により、基本方針に定める事項及び情報セキュリティ対策の評価を実施し、基本方針の見直しを行う。	8．情報セキュリティポリシーの見直し 　情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。	
附　則（令和７年12月１日杉並第45823号） この方針は、令和８年４月１日から施行する。	附　則 この方針は、平成15年８月５日から施行する。 附　則（令和５年４月１日杉並第62890号） この方針は、令和５年４月１日から施行する。		○旧の杉並区情報セキュリティ基本方針は要綱として制定しているが、このたび、地方自治法に基づくサイバーセキュリティを確保するため方針を包含するものとして改めて区長決裁により制定した。

別紙 1-2

杉並区情報セキュリティ基本方針

策定日　令和７年 12 月１日

目次

10　情報セキュリティ実施手順の策定

1　目的

今日、インターネットをはじめとする情報通信ネットワークや情報システムの利用は生活、経済、社会のあらゆる面で拡大している。

一方で、個人情報の漏えい、不正アクセスや新たな攻撃手法による情報資産の破壊・改ざん、操作ミス等によるシステム障害等が後を絶たない。また、自然災害によるシステム障害や疾病を起因とするシステム運用の機能不全にも備える必要がある。

さらに、昨今、国・地方公共団体・民間企業・住民の間のネットワークを通じた相互接続がますます進展していることに伴い、一つの地方公共団体の情報セキュリティ対策の不備や不適切なシステム利用が、他の地方公共団体や国の機関等の情報セキュリティにも脅威となり、その安全性や信頼性に影響を与える蓋然性が高くなっている。

杉並区（以下「区」という。）においても、区民の個人情報や行政運営上重要な情報などを多数取り扱っている。また、電子自治体の構築が進み、多くの業務が情報システムやネットワークに依存している。このため、これらの情報資産を様々な脅威から防御することは、区民の権利、利益を守るためにも、また、行政の安定的、継続的な運営のためにも必要不可欠である。

これらのことを踏まえ、他に定めがあるものを除き、区が実施する情報セキュリティ対策についての基本的な事項を定めるための基本方針として、また、地方自治法（昭和 22 年法律第 67 号）第 244 条の６第１項に規定するサイバーセキュリティを確保するための方針として、区が保有する情報資産の機密性、完全性及び可用性を維持することを目的に杉並区情報セキュリティ基本方針（以下「基本方針」という。）を定める。

2　定義

基本方針において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

（1）　ネットワーク

コンピュータ等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。

（2）　情報システム

区の組織運営に必要な情報の収集・蓄積・処理・伝達・利用に関わるコンピュータのハードウェア、ソフトウェア、データベース、ネットワーク、保管・蓄積装置、記録媒体等の仕組みをいう。

（3）　情報資産

情報システムで取り扱う全ての情報及び情報システムの開発と運用に係る情報並びに紙等の有体物としての情報をいう。

（4）　機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確

保することをいう。

（５） 完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（６） 可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

（７） 情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

（８） 情報セキュリティポリシー

基本方針及び情報セキュリティ対策基準をいう。

（９） 住民情報系

行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）第２条第11項に規定する個人番号利用事務等に係る情報システム及びその情報システムで取り扱うデータをいう。

(10) 内部情報系

総合行政ネットワーク（ＬＧＷＡＮ）に接続された情報システム及びその情報システムで取り扱うデータをいう。

(11) インターネット接続系

インターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

(12) 通信経路の分割

内部情報続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

(13) 無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

３　対象とする脅威

情報資産に対する脅威として、以下のものを想定し、情報セキュリティ対策を実施する。

（１） 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（２） 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（３） 地震、落雷、火災等の災害によるサービス及び業務の停止等

（４） 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（５） 電力供給の途絶、通信の断絶、水道供給の途絶等のインフラの障害からの波及等

４　適用範囲

（１） 行政機関の範囲

基本方針が適用される範囲は、区長、杉並区組織規則（昭和 50 年杉並区規則第９号）第７条第１項に規定する本庁の部及び室、同条第２項に規定する室並びに同規則別表第３に規定する行政機関とする。

（２） 情報資産の範囲

基本方針が対象とする情報資産は、次のとおりとする。

①情報システム等

②情報システムで取り扱う情報（これらを印刷した文書を含む。）

③情報システムの仕様書及びネットワーク図等のシステム関連文書

５　職員等の遵守義務及び違反への対応

職員、臨時・非常勤職員等（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。また、基本方針の実効性を確保するために違反者に対しては、必要な処分等を行う。

６　情報セキュリティ対策

上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

（１） 組織体制

区の保有する情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

（２） 情報資産の分類と管理

区の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

（３） 情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

①住民情報系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

②内部情報系においては、ＬＧＷＡＮと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市

区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（４） 物理的セキュリティ

サーバ、情報システム室を有する場合には、それらの管理について、また職員等のパソコン等の管理について、物理的な対策を講じる。

（５） 人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（６） 技術的セキュリティ

情報システムへのアクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（７） 運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

（８） 業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

７　情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

８　情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討した上で、情報セキュリティポリシーを見直す。

９　情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

10　情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。なお、情報セキュリティ実施手順は、公にすることにより区の組織運営に重大な支障を及ぼすおそれがあることから非公開とする。

附　則（令和７年 12 月１日杉並第 45823 号）

この方針は、令和８年４月１日から施行する。

別紙２

区長・教育委員会比較表

○杉並区情報セキュリティ基本方針・杉並区教育委員会情報セキュリティ基本方針

区長	教育委員会
杉並区情報セキュリティ基本方針	杉並区教育委員会情報セキュリティ基本方針
目次	目次
杉並区情報セキュリティ基本方針	杉並区教育委員会情報セキュリティ基本方針
1　目的	1　目的
2　定義	2　定義
（1）　ネットワーク	（1）　ネットワーク
（2）　情報システム	（2）　情報システム
（3）　情報資産	（3）　情報資産
（4）　機密性	（4）　機密性
（5）　完全性	（5）　完全性
（6）　可用性	（6）　可用性
（7）　情報セキュリティ	（7）　情報セキュリティ
（8）　情報セキュリティポリシー	（8）　情報セキュリティポリシー
（9）　住民情報系	（9）　住民情報系
（10）　内部情報系	（10）　内部情報系
（11）　インターネット接続系	（11）　インターネット接続系
（12）　通信経路の分割	（12）　通信経路の分割
（13）　無害化通信	（13）　無害化通信
3　対象とする脅威	3　対象とする脅威
4　適用範囲	4　適用範囲
（1）　行政機関の範囲	（1）　行政機関の範囲
（2）　情報資産の範囲	（2）　情報資産の範囲
5　職員等の遵守義務及び違反への対応	5　職員等の遵守義務及び違反への対応
6　情報セキュリティ対策	6　情報セキュリティ対策
（1）　組織体制	（1）　組織体制
（2）　情報資産の分類と管理	（2）　情報資産の分類と管理
（3）　情報システム全体の強靭性の向上	（3）　情報システム全体の強靭性の向上
（4）　物理的セキュリティ	（4）　物理的セキュリティ
（5）　人的セキュリティ	（5）　人的セキュリティ
（6）　技術的セキュリティ	（6）　技術的セキュリティ
（7）　運用	（7）　運用
（8）　業務委託と外部サービス（クラウドサービス）の利用	（8）　業務委託と外部サービス（クラウドサービス）の利用
7　情報セキュリティ監査及び自己点検の実施	7　情報セキュリティ監査及び自己点検の実施
8　情報セキュリティポリシーの見直し	8　情報セキュリティポリシーの見直し
9　情報セキュリティ対策基準の策定	9　情報セキュリティ対策基準の策定
10　情報セキュリティ実施手順の策定	10　情報セキュリティ実施手順の策定
1　目的 今日、インターネットをはじめとする情報通信ネットワークや情報システムの利用は生活、経済、社会のあらゆる面で拡大している。 一方で、個人情報の漏えい、不正アクセスや新たな攻撃手法による情報資産の破壊・改ざん、操作ミス等によるシステム障害等が後を絶たない。また、自然災害によるシステム障害や疾病を起因とするシステム運用の機能不全にも備える必要がある。 さらに、昨今、国・地方公共団体・民間企業・住民の間のネットワークを通じた相互接続がますます進展していることに伴い、一つの地方公共団体の情報セキュリティ対策の不備や不適切なシステム利用が、他の地方公共団体や国の機関等の情報セキュリティにも脅威となり、その安全性や信頼性に影響を与える蓋然性が高くなっている。 杉並区（以下「区」という。）においても、区民の個人情報や行政運営上重要な情報などを多数取り扱っている。また、電子自治体の構築が進み、多くの業務が情報システムやネットワークに依存している。このため、これらの情報資産を様々な脅威から防御することは、区民の権利、利益を守るためにも、また、行政の安定的、継続的な運営のためにも必要不可欠である。 これらのことを踏まえ、他に定めがあるものを除き、区が実施する情報セキュリティ対策についての基本的な事項を定めるための基本方針として、また、地方自治法（昭和22年法律第67号）第244条の６第１項に規定するサイバーセキュリティを確保するための方針として、区　　が保有する情報資産の機密性、完全性及び可用性を維持することを目的に杉並区情報セキュリティ基本方針　　（以下「基本方針」という。）を定める。	1　目的 杉並区教育委員会（以下「教育委員会」という。）　　が実施する情報セキュリティ対策についての基本的な事項を定めるための基本方針として、また、地方自治法（昭和22年法律第67号）第244条の６第１項に規定するサイバーセキュリティを確保するための方針として、教育委員会が保有する情報資産の機密性、完全性及び可用性を維持することを目的に杉並区教育委員会情報セキュリティ基本方針（以下「基本方針」という。）を定める。
2　定義 基本方針において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。 （1）　ネットワーク コンピュータ等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。 （2）　情報システム 区　　の組織運営に必要な情報の収集・蓄積・処理・伝達・利用に関わるコンピュータのハードウェア、ソフトウェア、データベース、ネットワーク、保管・蓄積装置、記録媒体等の仕組みをいう。 （3）　情報資産 情報システムで取り扱う全ての情報及び情報システムの開発と運用に	2　定義 基本方針において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。 （1）　ネットワーク コンピュータ等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。 （2）　情報システム 教育委員会の組織運営に必要な情報の収集・蓄積・処理・伝達・利用に関わるコンピュータのハードウェア、ソフトウェア、データベース、ネットワーク、保管・蓄積装置、記録媒体等の仕組みをいう。 （3）　情報資産 情報システムで取り扱う全ての情報及び情報システムの開発と運用に

区長	教育委員会
係る情報並びに紙等の有体物としての情報をいう。 （４） 機密性 情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。 （５） 完全性 情報が破壊、改ざん又は消去されていない状態を確保することをいう。 （６） 可用性 情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。 （７） 情報セキュリティ 情報資産の機密性、完全性及び可用性を維持することをいう。 （８） 情報セキュリティポリシー 基本方針及び情報セキュリティ対策基準をいう。 （９） 住民情報系 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）第２条第11項に規定する個人番号利用事務等に係る情報システム及びその情報システムで取り扱うデータをいう。 (10) 内部情報系 総合行政ネットワーク（ＬＧＷＡＮ）に接続された情報システム及びその情報システムで取り扱うデータをいう。 (11) インターネット接続系 インターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。 (12) 通信経路の分割 内部情報系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。 (13) 無害化通信 インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。 3 対象とする脅威 情報資産に対する脅威として、以下のものを想定し、情報セキュリティ対策を実施する。 （１） 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等 （２） 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等 （３） 地震、落雷、火災等の災害によるサービス及び業務の停止等 （４） 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等 （５） 電力供給の途絶、通信の断絶、水道供給の途絶等のインフラの障害からの波及等 4 適用範囲 （１） 行政機関の範囲 基本方針が適用される範囲は、区長、杉並区組織規則（昭和50年杉並区規則第９号）第７条第１項に規定する本庁の部及び室、同条第２項に規定する室並びに同規則別表第３に規定する行政機関とする。 （２） 情報資産の範囲 基本方針が対象とする情報資産は、次のとおりとする。 ①情報システム等 ②情報システムで取り扱う情報（これらを印刷した文書を含む。） ③情報システムの仕様書及びネットワーク図等のシステム関連文書 5 職員等の遵守義務及び違反への対応 職員、臨時・非常勤職員等（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。また、基本方針の実効性を確保するために違反者に対しては、必要な処分等を行う。 6 情報セキュリティ対策 上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。 （１） 組織体制 区の保有する情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。 （２） 情報資産の分類と管理 区の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。 （３） 情報システム全体の強靭性の向上 情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を	係る情報並びに紙等の有体物としての情報をいう。 （４） 機密性 情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。 （５） 完全性 情報が破壊、改ざん又は消去されていない状態を確保することをいう。 （６） 可用性 情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。 （７） 情報セキュリティ 情報資産の機密性、完全性及び可用性を維持することをいう。 （８） 情報セキュリティポリシー 基本方針及び情報セキュリティ対策基準をいう。 （９） 住民情報系 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）第２条第11項に規定する個人番号利用事務等に係る情報システム及びその情報システムで取り扱うデータをいう。 (10) 内部情報系 総合行政ネットワーク（ＬＧＷＡＮ）に接続された情報システム及びその情報システムで取り扱うデータをいう。 (11) インターネット接続系 インターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。 (12) 通信経路の分割 内部情報系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。 (13) 無害化通信 インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。 3 対象とする脅威 情報資産に対する脅威として、以下のものを想定し、情報セキュリティ対策を実施する。 （１） 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等 （２） 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等 （３） 地震、落雷、火災等の災害によるサービス及び業務の停止等 （４） 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等 （５） 電力供給の途絶、通信の断絶、水道供給の途絶等のインフラの障害からの波及等 4 適用範囲 （１） 行政機関の範囲 基本方針が適用される範囲は、教育委員会、教育委員会事務局、社会教育センター、郷土博物館、済美教育センター、就学前教育支援センター及び図書館とする。ただし、杉並区立学校情報セキュリティ基本方針（平成20年杉教第1888号）が適用される範囲を除く。 （２） 情報資産の範囲 基本方針が対象とする情報資産は、次のとおりとする。 ①情報システム等 ②情報システムで取り扱う情報（これらを印刷した文書を含む。） ③情報システムの仕様書及びネットワーク図等のシステム関連文書 5 職員等の遵守義務及び違反への対応 職員、臨時・非常勤職員等（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。また、基本方針の実効性を確保するために違反者に対しては、必要な処分等を行う。 6 情報セキュリティ対策 上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。 （１） 組織体制 教育委員会の保有する情報資産について、情報セキュリティ対策を推進する組織体制を確立する。 （２） 情報資産の分類と管理 教育委員会の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。 （３） 情報システム全体の強靭性の向上 情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を

区長	教育委員会
踏まえ、情報システム全体に対し、次の三段階の対策を講じる。 ①住民情報系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。 ②内部情報系においては、ＬＧＷＡＮと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。 ③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。	踏まえ、情報システム全体に対し、次の三段階の対策を講じる。 ①住民情報系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。 ②内部情報系においては、ＬＧＷＡＮと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。 ③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。
（４） 物理的セキュリティ サーバ、情報システム室を有する場合には、それらの管理について、また職員等のパソコン等の管理について、物理的な対策を講じる。	（４） 物理的セキュリティ サーバ、情報システム室を有する場合には、それらの管理について、また職員等のパソコン等の管理について、物理的な対策を講じる。
（５） 人的セキュリティ 情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。	（５） 人的セキュリティ 情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。
（６） 技術的セキュリティ 情報システムへのアクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。	（６） 技術的セキュリティ 情報システムへのアクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。
（７） 運用 情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。	（７） 運用 情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。
（８） 業務委託と外部サービス（クラウドサービス）の利用 業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。	（８） 業務委託と外部サービス（クラウドサービス）の利用 業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。
7　情報セキュリティ監査及び自己点検の実施 情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。	7　情報セキュリティ監査及び自己点検の実施 情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。
8　情報セキュリティポリシーの見直し 情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討した上で、情報セキュリティポリシーを見直す。	8　情報セキュリティポリシーの見直し 情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討した上で、情報セキュリティポリシーを見直す。
9　情報セキュリティ対策基準の策定 上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。	9　情報セキュリティ対策基準の策定 上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。
10　情報セキュリティ実施手順の策定 情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。なお、情報セキュリティ実施手順は、公にすることにより区　　の組織運営に重大な支障を及ぼすおそれがあることから非公開とする。	10　情報セキュリティ実施手順の策定 情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。なお、情報セキュリティ実施手順は、公にすることにより教育委員会の組織運営に重大な支障を及ぼすおそれがあることから非公開とする。

別紙３

区長・選挙管理委員会比較表

○杉並区情報セキュリティ基本方針・杉並区選挙管理委員会情報セキュリティ基本方針

区長	選挙管理委員会
杉並区情報セキュリティ基本方針	杉並区選挙管理委員会情報セキュリティ基本方針
目次	目次
杉並区情報セキュリティ基本方針	杉並区選挙管理委員会情報セキュリティ基本方針
1　目的	1　目的
2　定義	2　定義
（1）　ネットワーク	（1）　ネットワーク
（2）　情報システム	（2）　情報システム
（3）　情報資産	（3）　情報資産
（4）　機密性	（4）　機密性
（5）　完全性	（5）　完全性
（6）　可用性	（6）　可用性
（7）　情報セキュリティ	（7）　情報セキュリティ
（8）　情報セキュリティポリシー	（8）　情報セキュリティポリシー
（9）　住民情報系	（9）　住民情報系
(10)　内部情報系	(10)　内部情報系
(11)　インターネット接続系	(11)　インターネット接続系
(12)　通信経路の分割	(12)　通信経路の分割
(13)　無害化通信	(13)　無害化通信
3　対象とする脅威	3　対象とする脅威
4　適用範囲	4　適用範囲
（1）　行政機関の範囲	（1）　行政機関の範囲
（2）　情報資産の範囲	（2）　情報資産の範囲
5　職員等の遵守義務及び違反への対応	5　職員等の遵守義務及び違反への対応
6　情報セキュリティ対策	6　情報セキュリティ対策
（1）　組織体制	（1）　組織体制
（2）　情報資産の分類と管理	（2）　情報資産の分類と管理
（3）　情報システム全体の強靭性の向上	（3）　情報システム全体の強靭性の向上
（4）　物理的セキュリティ	（4）　物理的セキュリティ
（5）　人的セキュリティ	（5）　人的セキュリティ
（6）　技術的セキュリティ	（6）　技術的セキュリティ
（7）　運用	（7）　運用
（8）　業務委託と外部サービス（クラウドサービス）の利用	（8）　業務委託と外部サービス（クラウドサービス）の利用
7　情報セキュリティ監査及び自己点検の実施	7　情報セキュリティ監査及び自己点検の実施
8　情報セキュリティポリシーの見直し	8　情報セキュリティポリシーの見直し
9　情報セキュリティ対策基準の策定	9　情報セキュリティ対策基準の策定
10　情報セキュリティ実施手順の策定	10　情報セキュリティ実施手順の策定
1　目的	1　目的
今日、インターネットをはじめとする情報通信ネットワークや情報システムの利用は生活、経済、社会のあらゆる面で拡大している。 一方で、個人情報の漏えい、不正アクセスや新たな攻撃手法による情報資産の破壊・改ざん、操作ミス等によるシステム障害等が後を絶たない。また、自然災害によるシステム障害や疾病を起因とするシステム運用の機能不全にも備える必要がある。 さらに、昨今、国・地方公共団体・民間企業・住民の間のネットワークを通じた相互接続がますます進展していることに伴い、一つの地方公共団体の情報セキュリティ対策の不備や不適切なシステム利用が、他の地方公共団体や国の機関等の情報セキュリティにも脅威となり、その安全性や信頼性に影響を与える蓋然性が高くなっている。 杉並区（以下「区」という。）においても、区民の個人情報や行政運営上重要な情報などを多数取り扱っている。また、電子自治体の構築が進み、多くの業務が情報システムやネットワークに依存している。このため、これらの情報資産を様々な脅威から防御することは、区民の権利、利益を守るためにも、また、行政の安定的、継続的な運営のためにも必要不可欠である。 これらのことを踏まえ、他に定めがあるものを除き、区が実施する情報セキュリティ対策についての基本的な事項を定めるための基本方針として、また、地方自治法（昭和22年法律第67号）第244条の６第１項に規定するサイバーセキュリティを確保するための方針として、区が保有する情報資産の機密性、完全性及び可用性を維持することを目的に杉並区情報セキュリティ基本方針（以下「基本方針」という。）を定める。	杉並区選挙管理委員会（以下「選挙管理委員会」という。）が実施する情報セキュリティ対策についての基本的な事項を定めるための基本方針として、また、地方自治法（昭和22年法律第67号）第244条の６第１項に規定するサイバーセキュリティを確保するための方針として、選挙管理委員会が保有する情報資産の機密性、完全性及び可用性を維持することを目的に杉並区選挙管理委員会情報セキュリティ基本方針（以下「基本方針」という。）を定める。
2　定義	2　定義
基本方針において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。	基本方針において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。
（1）　ネットワーク コンピュータ等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。	（1）　ネットワーク コンピュータ等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。
（2）　情報システム 区の組織運営に必要な情報の収集・蓄積・処理・伝達・利用に関わるコンピュータのハードウェア、ソフトウェア、データベース、ネットワーク、保管・蓄積装置、記録媒体等の仕組みをいう。	（2）　情報システム 選挙管理委員会の組織運営に必要な情報の収集・蓄積・処理・伝達・利用に関わるコンピュータのハードウェア、ソフトウェア、データベース、ネットワーク、保管・蓄積装置、記録媒体等の仕組みをいう。
（3）　情報資産	（3）　情報資産

区長	選挙管理委員会
情報システムで取り扱う全ての情報及び情報システムの開発と運用に係る情報並びに紙等の有体物としての情報をいう。 （４） 機密性 情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。 （５） 完全性 情報が破壊、改ざん又は消去されていない状態を確保することをいう。 （６） 可用性 情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。 （７） 情報セキュリティ 情報資産の機密性、完全性及び可用性を維持することをいう。 （８） 情報セキュリティポリシー 基本方針及び情報セキュリティ対策基準をいう。 （９） 住民情報系 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）第２条第11項に規定する個人番号利用事務等に係る情報システム及びその情報システムで取り扱うデータをいう。 (10) 内部情報系 総合行政ネットワーク（ＬＧＷＡＮ）に接続された情報システム及びその情報システムで取り扱うデータをいう。 (11) インターネット接続系 インターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。 (12) 通信経路の分割 内部情報系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。 (13) 無害化通信 インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。 ３ 対象とする脅威 情報資産に対する脅威として、以下のものを想定し、情報セキュリティ対策を実施する。 （１） 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等 （２） 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等 （３） 地震、落雷、火災等の災害によるサービス及び業務の停止等 （４） 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等 （５） 電力供給の途絶、通信の断絶、水道供給の途絶等のインフラの障害からの波及等 ４ 適用範囲 （１） 行政機関の範囲 基本方針が適用される範囲は、区長、杉並区組織規則（昭和50年杉並区規則第９号）第７条第１項に規定する本庁の部及び室、同条第２項に規定する室並びに同規則別表第３に規定する行政機関とする。 （２） 情報資産の範囲 基本方針が対象とする情報資産は、次のとおりとする。 ①情報システム等 ②情報システムで取り扱う情報（これらを印刷した文書を含む。） ③情報システムの仕様書及びネットワーク図等のシステム関連文書 ５ 職員等の遵守義務及び違反への対応 職員、臨時・非常勤職員等（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。また、基本方針の実効性を確保するために違反者に対しては、必要な処分等を行う。 ６ 情報セキュリティ対策 上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。 （１） 組織体制 区の保有する情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。 （２） 情報資産の分類と管理 区の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。 （３） 情報システム全体の強靭性の向上 情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。	情報システムで取り扱う全ての情報及び情報システムの開発と運用に係る情報並びに紙等の有体物としての情報をいう。 （４） 機密性 情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。 （５） 完全性 情報が破壊、改ざん又は消去されていない状態を確保することをいう。 （６） 可用性 情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。 （７） 情報セキュリティ 情報資産の機密性、完全性及び可用性を維持することをいう。 （８） 情報セキュリティポリシー 基本方針及び情報セキュリティ対策基準をいう。 （９） 住民情報系 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）第２条第11項に規定する個人番号利用事務等に係る情報システム及びその情報システムで取り扱うデータをいう。 (10) 内部情報系 総合行政ネットワーク（ＬＧＷＡＮ）に接続された情報システム及びその情報システムで取り扱うデータをいう。 (11) インターネット接続系 インターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。 (12) 通信経路の分割 内部情報系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。 (13) 無害化通信 インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。 ３ 対象とする脅威 情報資産に対する脅威として、以下のものを想定し、情報セキュリティ対策を実施する。 （１） 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等 （２） 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等 （３） 地震、落雷、火災等の災害によるサービス及び業務の停止等 （４） 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等 （５） 電力供給の途絶、通信の断絶、水道供給の途絶等のインフラの障害からの波及等 ４ 適用範囲 （１） 行政機関の範囲 基本方針が適用される範囲は、選挙管理委員会及び選挙管理委員会事務局とする。 （２） 情報資産の範囲 基本方針が対象とする情報資産は、次のとおりとする。 ①情報システム等 ②情報システムで取り扱う情報（これらを印刷した文書を含む。） ③情報システムの仕様書及びネットワーク図等のシステム関連文書 ５ 職員等の遵守義務及び違反への対応 職員、臨時・非常勤職員等（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。また、基本方針の実効性を確保するために違反者に対しては、必要な処分等を行う。 ６ 情報セキュリティ対策 上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。 （１） 組織体制 選挙管理委員会の保有する情報資産について、情報セキュリティ対策を推進する組織体制を確立する。 （２） 情報資産の分類と管理 選挙管理委員会の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。 （３） 情報システム全体の強靭性の向上 情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

区長	選挙管理委員会
①住民情報系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。 ②内部情報系においては、ＬＧＷＡＮと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。 ③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。	①住民情報系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。 ②内部情報系においては、ＬＧＷＡＮと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。 ③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。
（４） 物理的セキュリティ サーバ、情報システム室を有する場合には、それらの管理について、また職員等のパソコン等の管理について、物理的な対策を講じる。	（４） 物理的セキュリティ サーバ、情報システム室を有する場合には、それらの管理について、また職員等のパソコン等の管理について、物理的な対策を講じる。
（５） 人的セキュリティ 情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。	（５） 人的セキュリティ 情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。
（６） 技術的セキュリティ 情報システムへのアクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。	（６） 技術的セキュリティ 情報システムへのアクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。
（７） 運用 情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。	（７） 運用 情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。
（８） 業務委託と外部サービス（クラウドサービス）の利用 業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。	（８） 業務委託と外部サービス（クラウドサービス）の利用 業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。
７　情報セキュリティ監査及び自己点検の実施 情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。	７　情報セキュリティ監査及び自己点検の実施 情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。
８　情報セキュリティポリシーの見直し 情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討した上で、情報セキュリティポリシーを見直す。	８　情報セキュリティポリシーの見直し 情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討した上で、情報セキュリティポリシーを見直す。
９　情報セキュリティ対策基準の策定 上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。	９　情報セキュリティ対策基準の策定 上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。
10　情報セキュリティ実施手順の策定 情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。なお、情報セキュリティ実施手順は、公にすることにより区の組織運営に重大な支障を及ぼすおそれがあることから非公開とする。	10　情報セキュリティ実施手順の策定 情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。なお、情報セキュリティ実施手順は、公にすることにより選挙管理委員会の組織運営に重大な支障を及ぼすおそれがあることから非公開とする。

別紙４

区長・監査委員比較表

○杉並区情報セキュリティ基本方針・杉並区監査委員情報セキュリティ基本方針

区長	監査委員
杉並区情報セキュリティ基本方針	杉並区監査委員情報セキュリティ基本方針
目次	目次
杉並区情報セキュリティ基本方針	杉並区監査委員情報セキュリティ基本方針
1　目的	1　目的
2　定義	2　定義
（1）　ネットワーク	（1）　ネットワーク
（2）　情報システム	（2）　情報システム
（3）　情報資産	（3）　情報資産
（4）　機密性	（4）　機密性
（5）　完全性	（5）　完全性
（6）　可用性	（6）　可用性
（7）　情報セキュリティ	（7）　情報セキュリティ
（8）　情報セキュリティポリシー	（8）　情報セキュリティポリシー
（9）　住民情報系	（9）　住民情報系
（10）　内部情報系	（10）　内部情報系
（11）　インターネット接続系	（11）　インターネット接続系
（12）　通信経路の分割	（12）　通信経路の分割
（13）　無害化通信	（13）　無害化通信
3　対象とする脅威	3　対象とする脅威
4　適用範囲	4　適用範囲
（1）　行政機関の範囲	（1）　行政機関の範囲
（2）　情報資産の範囲	（2）　情報資産の範囲
5　職員等の遵守義務及び違反への対応	5　職員等の遵守義務及び違反への対応
6　情報セキュリティ対策	6　情報セキュリティ対策
（1）　組織体制	（1）　組織体制
（2）　情報資産の分類と管理	（2）　情報資産の分類と管理
（3）　情報システム全体の強靭性の向上	（3）　情報システム全体の強靭性の向上
（4）　物理的セキュリティ	（4）　物理的セキュリティ
（5）　人的セキュリティ	（5）　人的セキュリティ
（6）　技術的セキュリティ	（6）　技術的セキュリティ
（7）　運用	（7）　運用
（8）　業務委託と外部サービス（クラウドサービス）の利用	（8）　業務委託と外部サービス（クラウドサービス）の利用
7　情報セキュリティ監査及び自己点検の実施	7　情報セキュリティ監査及び自己点検の実施
8　情報セキュリティポリシーの見直し	8　情報セキュリティポリシーの見直し
9　情報セキュリティ対策基準の策定	9　情報セキュリティ対策基準の策定
10　情報セキュリティ実施手順の策定	10　情報セキュリティ実施手順の策定
1　目的 今日、インターネットをはじめとする情報通信ネットワークや情報システムの利用は生活、経済、社会のあらゆる面で拡大している。 一方で、個人情報の漏えい、不正アクセスや新たな攻撃手法による情報資産の破壊・改ざん、操作ミス等によるシステム障害等が後を絶たない。また、自然災害によるシステム障害や疾病を起因とするシステム運用の機能不全にも備える必要がある。 さらに、昨今、国・地方公共団体・民間企業・住民の間のネットワークを通じた相互接続がますます進展していることに伴い、一つの地方公共団体の情報セキュリティ対策の不備や不適切なシステム利用が、他の地方公共団体や国の機関等の情報セキュリティにも脅威となり、その安全性や信頼性に影響を与える蓋然性が高くなっている。 杉並区（以下「区」という。）においても、区民の個人情報や行政運営上重要な情報などを多数取り扱っている。また、電子自治体の構築が進み、多くの業務が情報システムやネットワークに依存している。このため、これらの情報資産を様々な脅威から防御することは、区民の権利、利益を守るためにも、また、行政の安定的、継続的な運営のためにも必要不可欠である。 これらのことを踏まえ、他に定めがあるものを除き、区が実施する情報セキュリティ対策についての基本的な事項を定めるための基本方針として、また、地方自治法（昭和22年法律第67号）第244条の６第１項に規定するサイバーセキュリティを確保するための方針として、区　　が保有する情報資産の機密性、完全性及び可用性を維持することを目的に杉並区情報セキュリティ基本方針　　（以下「基本方針」という。）を定める。	1　目的 杉並区監査委員（以下「監査委員」という。）　　が実施する情報セキュリティ対策についての基本的な事項を定めるための基本方針として、また、地方自治法（昭和22年法律第67号）第244条の６第１項に規定するサイバーセキュリティを確保するための方針として、監査委員が保有する情報資産の機密性、完全性及び可用性を維持することを目的に杉並区監査委員情報セキュリティ基本方針（以下「基本方針」という。）を定める。
2　定義 基本方針において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。 （1）　ネットワーク コンピュータ等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。 （2）　情報システム 区　　の組織運営に必要な情報の収集・蓄積・処理・伝達・利用に関わるコンピュータのハードウェア、ソフトウェア、データベース、ネットワーク、保管・蓄積装置、記録媒体等の仕組みをいう。 （3）　情報資産 情報システムで取り扱う全ての情報及び情報システムの開発と運用に	2　定義 基本方針において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。 （1）　ネットワーク コンピュータ等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。 （2）　情報システム 監査委員の組織運営に必要な情報の収集・蓄積・処理・伝達・利用に関わるコンピュータのハードウェア、ソフトウェア、データベース、ネットワーク、保管・蓄積装置、記録媒体等の仕組みをいう。 （3）　情報資産 情報システムで取り扱う全ての情報及び情報システムの開発と運用に

区長	監査委員
係る情報並びに紙等の有体物としての情報をいう。 （４） 機密性 情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。 （５） 完全性 情報が破壊、改ざん又は消去されていない状態を確保することをいう。 （６） 可用性 情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。 （７） 情報セキュリティ 情報資産の機密性、完全性及び可用性を維持することをいう。 （８） 情報セキュリティポリシー 基本方針及び情報セキュリティ対策基準をいう。 （９） 住民情報系 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）第２条第11項に規定する個人番号利用事務等に係る情報システム及びその情報システムで取り扱うデータをいう。 (10) 内部情報系 総合行政ネットワーク（ＬＧＷＡＮ）に接続された情報システム及びその情報システムで取り扱うデータをいう。 (11) インターネット接続系 インターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。 (12) 通信経路の分割 内部情報系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。 (13) 無害化通信 インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。 3 対象とする脅威 情報資産に対する脅威として、以下のものを想定し、情報セキュリティ対策を実施する。 （１） 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等 （２） 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等 （３） 地震、落雷、火災等の災害によるサービス及び業務の停止等 （４） 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等 （５） 電力供給の途絶、通信の断絶、水道供給の途絶等のインフラの障害からの波及等 4 適用範囲 （１） 行政機関の範囲 基本方針が適用される範囲は、区長、杉並区組織規則（昭和50年杉並区規則第９号）第７条第１項に規定する本庁の部及び室、同条第２項に規定する室並びに同規則別表第３に規定する行政機関とする。 （２） 情報資産の範囲 基本方針が対象とする情報資産は、次のとおりとする。 ①情報システム等 ②情報システムで取り扱う情報（これらを印刷した文書を含む。） ③情報システムの仕様書及びネットワーク図等のシステム関連文書 5 職員等の遵守義務及び違反への対応 職員、臨時・非常勤職員等（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。また、基本方針の実効性を確保するために違反者に対しては、必要な処分等を行う。 6 情報セキュリティ対策 上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。 （１） 組織体制 区の保有する情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。 （２） 情報資産の分類と管理 区の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。 （３） 情報システム全体の強靭性の向上 情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。 ①住民情報系においては、原則として、他の領域との通信をできない	係る情報並びに紙等の有体物としての情報をいう。 （４） 機密性 情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。 （５） 完全性 情報が破壊、改ざん又は消去されていない状態を確保することをいう。 （６） 可用性 情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。 （７） 情報セキュリティ 情報資産の機密性、完全性及び可用性を維持することをいう。 （８） 情報セキュリティポリシー 基本方針及び情報セキュリティ対策基準をいう。 （９） 住民情報系 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）第２条第11項に規定する個人番号利用事務等に係る情報システム及びその情報システムで取り扱うデータをいう。 (10) 内部情報系 総合行政ネットワーク（ＬＧＷＡＮ）に接続された情報システム及びその情報システムで取り扱うデータをいう。 (11) インターネット接続系 インターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。 (12) 通信経路の分割 内部情報系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。 (13) 無害化通信 インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。 3 対象とする脅威 情報資産に対する脅威として、以下のものを想定し、情報セキュリティ対策を実施する。 （１） 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等 （２） 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等 （３） 地震、落雷、火災等の災害によるサービス及び業務の停止等 （４） 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等 （５） 電力供給の途絶、通信の断絶、水道供給の途絶等のインフラの障害からの波及等 4 適用範囲 （１） 行政機関の範囲 基本方針が適用される範囲は、監査委員及び監査委員事務局とする。 （２） 情報資産の範囲 基本方針が対象とする情報資産は、次のとおりとする。 ①情報システム等 ②情報システムで取り扱う情報（これらを印刷した文書を含む。） ③情報システムの仕様書及びネットワーク図等のシステム関連文書 5 職員等の遵守義務及び違反への対応 職員、臨時・非常勤職員等（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。また、基本方針の実効性を確保するために違反者に対しては、必要な処分等を行う。 6 情報セキュリティ対策 上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。 （１） 組織体制 監査委員の保有する情報資産について、情報セキュリティ対策を推進する組織体制を確立する。 （２） 情報資産の分類と管理 監査委員の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。 （３） 情報システム全体の強靭性の向上 情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。 ①住民情報系においては、原則として、他の領域との通信をできない

区長	監査委員
ようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。 ②内部情報系においては、ＬＧＷＡＮと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。 ③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。	ようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。 ②内部情報系においては、ＬＧＷＡＮと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。 ③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。
（４） 物理的セキュリティ サーバ、情報システム室を有する場合には、それらの管理について、また職員等のパソコン等の管理について、物理的な対策を講じる。	（４） 物理的セキュリティ サーバ、情報システム室を有する場合には、それらの管理について、また職員等のパソコン等の管理について、物理的な対策を講じる。
（５） 人的セキュリティ 情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。	（５） 人的セキュリティ 情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。
（６） 技術的セキュリティ 情報システムへのアクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。	（６） 技術的セキュリティ 情報システムへのアクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。
（７） 運用 情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。	（７） 運用 情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。
（８） 業務委託と外部サービス（クラウドサービス）の利用 業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。	（８） 業務委託と外部サービス（クラウドサービス）の利用 業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。
7　情報セキュリティ監査及び自己点検の実施 情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。	7　情報セキュリティ監査及び自己点検の実施 情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。
8　情報セキュリティポリシーの見直し 情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討した上で、情報セキュリティポリシーを見直す。	8　情報セキュリティポリシーの見直し 情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討した上で、情報セキュリティポリシーを見直す。
9　情報セキュリティ対策基準の策定 上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。	9　情報セキュリティ対策基準の策定 上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。
10　情報セキュリティ実施手順の策定 情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。なお、情報セキュリティ実施手順は、公にすることにより区　　の組織運営に重大な支障を及ぼすおそれがあることから非公開とする。	10　情報セキュリティ実施手順の策定 情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。なお、情報セキュリティ実施手順は、公にすることにより監査委員の組織運営に重大な支障を及ぼすおそれがあることから非公開とする。

別紙５

区長・農業委員会比較表

○杉並区情報セキュリティ基本方針・杉並区農業委員会情報セキュリティ基本方針

区長	農業委員会
杉並区情報セキュリティ基本方針	杉並区農業委員会情報セキュリティ基本方針
目次	目次
杉並区情報セキュリティ基本方針	杉並区農業委員会情報セキュリティ基本方針
1　目的	1　目的
2　定義	2　定義
（1）　ネットワーク	（1）　ネットワーク
（2）　情報システム	（2）　情報システム
（3）　情報資産	（3）　情報資産
（4）　機密性	（4）　機密性
（5）　完全性	（5）　完全性
（6）　可用性	（6）　可用性
（7）　情報セキュリティ	（7）　情報セキュリティ
（8）　情報セキュリティポリシー	（8）　情報セキュリティポリシー
（9）　住民情報系	（9）　住民情報系
（10）　内部情報系	（10）　内部情報系
（11）　インターネット接続系	（11）　インターネット接続系
（12）　通信経路の分割	（12）　通信経路の分割
（13）　無害化通信	（13）　無害化通信
3　対象とする脅威	3　対象とする脅威
4　適用範囲	4　適用範囲
（1）　行政機関の範囲	（1）　行政機関の範囲
（2）　情報資産の範囲	（2）　情報資産の範囲
5　職員等の遵守義務及び違反への対応	5　職員等の遵守義務及び違反への対応
6　情報セキュリティ対策	6　情報セキュリティ対策
（1）　組織体制	（1）　組織体制
（2）　情報資産の分類と管理	（2）　情報資産の分類と管理
（3）　情報システム全体の強靭性の向上	（3）　情報システム全体の強靭性の向上
（4）　物理的セキュリティ	（4）　物理的セキュリティ
（5）　人的セキュリティ	（5）　人的セキュリティ
（6）　技術的セキュリティ	（6）　技術的セキュリティ
（7）　運用	（7）　運用
（8）　業務委託と外部サービス（クラウドサービス）の利用	（8）　業務委託と外部サービス（クラウドサービス）の利用
7　情報セキュリティ監査及び自己点検の実施	7　情報セキュリティ監査及び自己点検の実施
8　情報セキュリティポリシーの見直し	8　情報セキュリティポリシーの見直し
9　情報セキュリティ対策基準の策定	9　情報セキュリティ対策基準の策定
10　情報セキュリティ実施手順の策定	10　情報セキュリティ実施手順の策定
1　目的	1　目的
今日、インターネットをはじめとする情報通信ネットワークや情報システムの利用は生活、経済、社会のあらゆる面で拡大している。 一方で、個人情報の漏えい、不正アクセスや新たな攻撃手法による情報資産の破壊・改ざん、操作ミス等によるシステム障害等が後を絶たない。また、自然災害によるシステム障害や疾病を起因とするシステム運用の機能不全にも備える必要がある。 さらに、昨今、国・地方公共団体・民間企業・住民の間のネットワークを通じた相互接続がますます進展していることに伴い、一つの地方公共団体の情報セキュリティ対策の不備や不適切なシステム利用が、他の地方公共団体や国の機関等の情報セキュリティにも脅威となり、その安全性や信頼性に影響を与える蓋然性が高くなっている。 杉並区（以下「区」という。）においても、区民の個人情報や行政運営上重要な情報などを多数取り扱っている。また、電子自治体の構築が進み、多くの業務が情報システムやネットワークに依存している。このため、これらの情報資産を様々な脅威から防御することは、区民の権利、利益を守るためにも、また、行政の安定的、継続的な運営のためにも必要不可欠である。 これらのことを踏まえ、他に定めがあるものを除き、区が実施する情報セキュリティ対策についての基本的な事項を定めるための基本方針として、また、地方自治法（昭和22年法律第67号）第244条の６第１項に規定するサイバーセキュリティを確保するための方針として、区　　が保有する情報資産の機密性、完全性及び可用性を維持することを目的に杉並区情報セキュリティ基本方針　　（以下「基本方針」という。）を定める。	杉並区農業委員会（以下「農業委員会」という。）　　が実施する情報セキュリティ対策についての基本的な事項を定めるための基本方針として、また、地方自治法（昭和22年法律第67号）第244条の６第１項に規定するサイバーセキュリティを確保するための方針として、農業委員会が保有する情報資産の機密性、完全性及び可用性を維持することを目的に杉並区農業委員会情報セキュリティ基本方針（以下「基本方針」という。）を定める。
2　定義 基本方針において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。 （1）　ネットワーク コンピュータ等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。 （2）　情報システム 区　　の組織運営に必要な情報の収集・蓄積・処理・伝達・利用に関わるコンピュータのハードウェア、ソフトウェア、データベース、ネットワーク、保管・蓄積装置、記録媒体等の仕組みをいう。 （3）　情報資産 情報システムで取り扱う全ての情報及び情報システムの開発と運用に	2　定義 基本方針において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。 （1）　ネットワーク コンピュータ等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。 （2）　情報システム 農業委員会の組織運営に必要な情報の収集・蓄積・処理・伝達・利用に関わるコンピュータのハードウェア、ソフトウェア、データベース、ネットワーク、保管・蓄積装置、記録媒体等の仕組みをいう。 （3）　情報資産 情報システムで取り扱う全ての情報及び情報システムの開発と運用に

区長	農業委員会
係る情報並びに紙等の有体物としての情報をいう。 （４） 機密性 情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。 （５） 完全性 情報が破壊、改ざん又は消去されていない状態を確保することをいう。 （６） 可用性 情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。 （７） 情報セキュリティ 情報資産の機密性、完全性及び可用性を維持することをいう。 （８） 情報セキュリティポリシー 基本方針及び情報セキュリティ対策基準をいう。 （９） 住民情報系 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）第２条第11項に規定する個人番号利用事務等に係る情報システム及びその情報システムで取り扱うデータをいう。 (10) 内部情報系 総合行政ネットワーク（ＬＧＷＡＮ）に接続された情報システム及びその情報システムで取り扱うデータをいう。 (11) インターネット接続系 インターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。 (12) 通信経路の分割 内部情報系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。 (13) 無害化通信 インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。 3 対象とする脅威 情報資産に対する脅威として、以下のものを想定し、情報セキュリティ対策を実施する。 （１） 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等 （２） 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等 （３） 地震、落雷、火災等の災害によるサービス及び業務の停止等 （４） 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等 （５） 電力供給の途絶、通信の断絶、水道供給の途絶等のインフラの障害からの波及等 4 適用範囲 （１） 行政機関の範囲 基本方針が適用される範囲は、区長、杉並区組織規則（昭和50年杉並区規則第９号）第７条第１項に規定する本庁の部及び室、同条第２項に規定する室並びに同規則別表第３に規定する行政機関とする。 （２） 情報資産の範囲 基本方針が対象とする情報資産は、次のとおりとする。 ①情報システム等 ②情報システムで取り扱う情報（これらを印刷した文書を含む。） ③情報システムの仕様書及びネットワーク図等のシステム関連文書 5 職員等の遵守義務及び違反への対応 職員、臨時・非常勤職員等（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。また、基本方針の実効性を確保するために違反者に対しては、必要な処分等を行う。 6 情報セキュリティ対策 上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。 （１） 組織体制 区の保有する情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。 （２） 情報資産の分類と管理 区の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。 （３） 情報システム全体の強靭性の向上 情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。 ①住民情報系においては、原則として、他の領域との通信をできない	係る情報並びに紙等の有体物としての情報をいう。 （４） 機密性 情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。 （５） 完全性 情報が破壊、改ざん又は消去されていない状態を確保することをいう。 （６） 可用性 情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。 （７） 情報セキュリティ 情報資産の機密性、完全性及び可用性を維持することをいう。 （８） 情報セキュリティポリシー 基本方針及び情報セキュリティ対策基準をいう。 （９） 住民情報系 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）第２条第11項に規定する個人番号利用事務等に係る情報システム及びその情報システムで取り扱うデータをいう。 (10) 内部情報系 総合行政ネットワーク（ＬＧＷＡＮ）に接続された情報システム及びその情報システムで取り扱うデータをいう。 (11) インターネット接続系 インターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。 (12) 通信経路の分割 内部情報系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。 (13) 無害化通信 インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。 3 対象とする脅威 情報資産に対する脅威として、以下のものを想定し、情報セキュリティ対策を実施する。 （１） 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等 （２） 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等 （３） 地震、落雷、火災等の災害によるサービス及び業務の停止等 （４） 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等 （５） 電力供給の途絶、通信の断絶、水道供給の途絶等のインフラの障害からの波及等 4 適用範囲 （１） 行政機関の範囲 基本方針が適用される範囲は、農業委員会及び農業委員会事務局とする。 （２） 情報資産の範囲 基本方針が対象とする情報資産は、次のとおりとする。 ①情報システム等 ②情報システムで取り扱う情報（これらを印刷した文書を含む。） ③情報システムの仕様書及びネットワーク図等のシステム関連文書 5 職員等の遵守義務及び違反への対応 職員、臨時・非常勤職員等（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。また、基本方針の実効性を確保するために違反者に対しては、必要な処分等を行う。 6 情報セキュリティ対策 上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。 （１） 組織体制 農業委員会の保有する情報資産について、情報セキュリティ対策を推進する組織体制を確立する。 （２） 情報資産の分類と管理 農業委員会の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。 （３） 情報システム全体の強靭性の向上 情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。 ①住民情報系においては、原則として、他の領域との通信をできない

区長	農業委員会
ようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。 ②内部情報系においては、ＬＧＷＡＮと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。 ③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。	ようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。 ②内部情報系においては、ＬＧＷＡＮと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。 ③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。
（４） 物理的セキュリティ サーバ、情報システム室を有する場合には、それらの管理について、また職員等のパソコン等の管理について、物理的な対策を講じる。	（４） 物理的セキュリティ サーバ、情報システム室を有する場合には、それらの管理について、また職員等のパソコン等の管理について、物理的な対策を講じる。
（５） 人的セキュリティ 情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。	（５） 人的セキュリティ 情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。
（６） 技術的セキュリティ 情報システムへのアクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。	（６） 技術的セキュリティ 情報システムへのアクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。
（７） 運用 情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。	（７） 運用 情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。
（８） 業務委託と外部サービス（クラウドサービス）の利用 業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。	（８） 業務委託と外部サービス（クラウドサービス）の利用 業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。
7　情報セキュリティ監査及び自己点検の実施 情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。	7　情報セキュリティ監査及び自己点検の実施 情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。
8　情報セキュリティポリシーの見直し 情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討した上で、情報セキュリティポリシーを見直す。	8　情報セキュリティポリシーの見直し 情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討した上で、情報セキュリティポリシーを見直す。
9　情報セキュリティ対策基準の策定 上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。	9　情報セキュリティ対策基準の策定 上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。
10　情報セキュリティ実施手順の策定 情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。なお、情報セキュリティ実施手順は、公にすることにより区　　の組織運営に重大な支障を及ぼすおそれがあることから非公開とする。	10　情報セキュリティ実施手順の策定 情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。なお、情報セキュリティ実施手順は、公にすることにより農業委員会の組織運営に重大な支障を及ぼすおそれがあることから非公開とする。