練馬区情報セキュリティに関する要綱

平成20年３月31日
19練企情第1686号

目次

第１章　総則

（目的）

第１条　この要綱は、練馬区情報化管理規程（平成16年11月練馬区訓令第24号。以下「管理規程」という。）第28条第１項の規定に基づき、練馬区（以下「区」という。）が保有する情報資産の機密性、完全性および可用性を確保ならびに維持するための基本的な事項を定めるとともに、区における情報セキュリティマネジメント、情報セキュリティマネジメントを推進するための体制（以下「セキュリティマネジメント体制」という。）および情報セキュリティマネジメント運用について必要な事項を定めるものとする。

（情報セキュリティマネジメント）

第２条　この要綱の定めるところにより、情報セキュリティマネジメント（情報資産の機密性、完全性および可用性を確保し、もって安全な区民生活に資するため、第９条に規定する情報セキュリティに関する対策（以下「セキュリティ対策」という。）を実施するための権限および責任を有する者を役割に応じ設置し、情報資産の重要度に応じたセキュリティ対策を実施し、維持しおよび向上させることをいう。以下同じ。）を実施する。

２　前項に規定する情報セキュリティマネジメント（以下「セキュリティマネジメント」という。）の実施に当たっては、セキュリティマネジメント体制を確立し、計画（Ｐｌａｎ）、実施（Ｄｏ）、評価（Ｃｈｅｃｋ）および見直し（Ａｃｔｉｏｎ）の各段階における活動を規定し、これらの活動について定期的に見直しを行い、繰り返し実施しなければならない。

３　第11条第１項に規定する最高情報セキュリティ責任者（以下「最高情報セキュリティ責任者」という。）は、セキュリティマネジメントを実施するに当たり、同条第５項に定めるところにより、マネジメントレビュー（計画に基づきセキュリティ対策が実施されているかおよび計画で定められた成果が得られているかをセキュリティ対策の有効性の観点から確認することをいう。以下同じ。）を実施する。

４　情報資産を適切に取り扱うため、第25条から第30条までに定めるところにより、情報セキュリティマネジメント運用（セキュリティに関する教育および啓発、自己点検、監査、リスクマネジメント、情報セキュリティ事故等の管理および委託事業者等の管理をいう。以下同じ。）を実施する。

（定義）

第３条　この要綱において使用する用語は、個人情報の保護に関する法律（平成15年法律第57号。以下「個人情報保護法」という。）および管理規程において使用する用語の例によるほか、つぎ

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。

⑴　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。

⑵　完全性　情報が破壊、改ざんまたは消去されていない状態を確保することをいう。

⑶　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、情報にアクセスすることができる状態を確保することをいう。

⑷　部　練馬区組織条例（昭和40年４月練馬区条例第４号）第１条に規定する室および部、練馬区会計管理室設置規則（平成19年６月規則第74号）第１条に規定する室、練馬区教育委員会事務局組織規則（平成４年３月練馬区教育委員会規則第１号）第２条に規定する部、練馬区選挙管理委員会規程（昭和39年７月練馬区選挙管理委員会訓令甲第１号）第14条に規定する事務局、練馬区監査委員条例（昭和39年４月練馬区条例第３号）第６条に規定する事務局、練馬区農業委員会事務局処務規則（昭和48年12月練馬区農業委員会議決）第２条に規定する事務局ならびに練馬区議会事務局条例（昭和48年３月練馬区条例第９号）第１条に規定する事務局をいう。

⑸　組織　前号に規定する部および管理規程第２条第１号に規定する課をいう。

⑹　部長　第４号に規定する部の長および練馬区組織規則（昭和48年12月規則第33号）第４条に規定する者をいう。

⑺　職員　第５号に規定する組織に所属する一般職および特別職の職員ならびに最高情報セキュリティ責任者が認める職員をいう。

⑻　委託事業者等　委託事業者、指定管理者または最高情報セキュリティ責任者が認めるもののうち、区の情報資産を取り扱う者をいう。

⑼　事務取扱担当者　職員および委託事業者等の従事者のうち、特定個人情報を取り扱う事務を担当する者をいう。

⑽　特定個人情報　保有個人情報のうち、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。以下「番号法」という。）第２条第８項に規定する特定個人情報をいう。

⑾　実施手順　課で所管する情報資産に係るセキュリティマネジメントの実施手順を示したもので、各情報セキュリティ責任者が作成するものをいう。

⑿　脅威　部外者の侵入、不正アクセス、ウィルス攻撃および情報資産の持ち出し等による情報資産の漏えい、破壊、改ざん、消去等をいう。

⒀　情報セキュリティ事故等　つぎに掲げる場合をいう。

ア　脅威が発生した場合またはそのおそれがある場合

イ　職員または委託事業者等が第８条に規定する法令もしくは練馬区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。）等に違反している事実またはこれらの兆候が認められる場合

⒁　緊急時対応計画　各課において情報セキュリティ事故等が発生した場合の個別具体的な対応方法を示した事故等発生時対応手順として各情報セキュリティ責任者が作成し、最高情報セキュリティ責任者が管理を行うものをいう。

⒂　個人情報の保護および管理ならびに情報セキュリティに関する特記事項　「情報の保護お

よび管理に関する特記事項」、「指定管理における情報の保護および管理に関する特記事項」、「労働者派遣契約における情報の保護および管理に関する特記事項」、「ファイナンスリースにおける情報の保護および管理に関する特記事項」、「メンテナンスリースにおける情報の保護および管理に関する特記事項」および「特定個人情報の保護および管理に関する特記事項」で、統括情報セキュリティ管理者が定めるものをいう。

⑯　一般教育　職員および委託事業者等に対して、第25条の定めるところにより、セキュリティマネジメントの実施に当たり求められる基本的な事項について、教育および啓発することをいう。

⑰　職場教育　職員および委託事業者等に対して、第25条の定めるところにより、各課における情報資産の取扱いに当たり求められる事項について、教育および啓発することをいう。

⑱　ガバメントクラウド　国の行政機関や地方公共団体が共同で行政システムを利用できるようにしたＩＴ基盤をいう。

（適用範囲）

第４条　セキュリティポリシーの適用範囲はつぎに掲げるものとする。

⑴　情報資産のうち、漏えい、破壊、改ざん、消去等またはそのおそれから保護するために管理を要するもの

⑵　組織

⑶　職員および委託事業者等

（職員の遵守義務）

第５条　職員は、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セキュリティポリシー、実施手順および緊急時対応計画を遵守しなければならない。

２　職員のうち事務取扱担当者等は、セキュリティポリシー、実施手順およびその他の関係規程ならびに情報セキュリティ責任者の指示事項等に基づき、特定個人情報を厳正に取り扱わなければならない。

３　職員は、一般教育を受講するとともに、必要があると認められた場合は、職場教育を受講しなければならない。

４　職員は、第26条に規定する情報セキュリティに関する自己点検（以下「自己点検」という。）を実施し、その結果に基づき、自己の権限の範囲内で改善を図らなければならない。

５　職員は、第27条に規定する情報セキュリティに関する監査（以下「監査」という。）および第28条に規定する情報セキュリティに関するリスクマネジメント（以下「リスクマネジメント」という。）の実施に協力しなければならない。

６　職員は、情報セキュリティ事故等（以下「セキュリティ事故等」という。）を把握した場合は、別に定める要領の規定および緊急時対応計画の記載に従い、対応しなければならない。

７　職員は、第30条に規定する委託事業者等の管理を実施しなければならない。

（業務の委託）

第６条　区が委託する場合（指定管理者制度における指定管理者に管理させる場合を含む。以下同じ。）は、セキュリティポリシー等のうち、委託事業者等が守るべき内容ならびに当該委託において取り扱う情報資産の種類および取扱い制限について説明することとし、別に定めるところにより、委託事業者等において区と同等以上の情報資産の安全管理措置が講じられることを

あらかじめ確認した上で、委託先を適切に選定しなければならない。

2　区が委託する場合においては、委託事業者等に対し、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たりセキュリティポリシーおよび実施手順ならびに「個人情報の保護および管理ならびに情報セキュリティに関する特記事項」（以下「特記事項」という。）を遵守することを契約・協定等で規定しなければならない。

3　区が委託する場合において、委託先が再委託を行う場合には、別に定めるところにより、再委託先において区と同等以上の安全管理措置が講じられることをあらかじめ確認しなければ、再委託を承認してはならない。再委託以降の委託行為についても同様とする。

4　前項により再委託または再委託以降の委託行為（以下「再委託等」という。）が行われる場合は、委託事業者等が再委託先および再委託以降の委託先（以下「再委託先等」という。）に対して、必要かつ適切な監督を行っているか監督しなければならない。

（東京都および国等からの業務の受託）

第７条　東京都および国等から受託する場合においては、東京都および国等に対して区のセキュリティポリシーと同等以上のセキュリティ対策が実施できるよう要請し、契約・協定等で規定するものとする。

（法令遵守）

第８条　職員は、職務において情報資産を取り扱うに当たり、つぎに掲げる法令および指針のほか関係法令を遵守し、これに従わなければならない。

⑴　地方公務員法(昭和25年法律第261号)
⑵　著作権法（昭和45年法律第48号）
⑶　不正アクセス行為の禁止等に関する法律（平成11年法律第128号）
⑷　個人情報保護法
⑸　番号法
⑹　サイバーセキュリティ基本法（平成26年法律第104号）
⑺　練馬区個人情報の保護に関する法律施行条例（令和４年12月練馬区条例第46号）
⑻　練馬区議会の個人情報の保護に関する条例（令和５年２月練馬区条例第１号）
⑼　練馬区の実施機関等が保有する個人情報の適切な管理のための措置に関する指針（令和５年３月27日４練総情第1261号）

2　区が東京都および国等からの業務を受託した場合、職員は、情報資産を取り扱うに当たり、つぎに掲げる法令のほか関係法令を遵守し、これに従わなければならない。

⑴　地方公務員法
⑵　著作権法
⑶　不正アクセス行為の禁止等に関する法律
⑷　個人情報保護法
⑸　番号法
⑹　サイバーセキュリティ基本法
⑺　その他東京都および国等が規定する個人情報保護に関する法令または条例等

3　職員がセキュリティポリシーおよびその他の関係規程に違反した場合は、その重大性、発生した事案の状況等に応じて、地方公務員法その他の関係法令に基づき、懲戒処分等の対象とす

る。

4　委託事業者等は、受託した業務において情報資産を取り扱うに当たり、つぎに掲げる法令および指針のほか関係法令を遵守し、これに従わなければならない。

⑴　著作権法

⑵　不正アクセス行為の禁止等に関する法律

⑶　個人情報保護法

⑷　番号法

⑸　サイバーセキュリティ基本法

⑹　練馬区個人情報の保護に関する法律施行条例

⑺　練馬区議会の個人情報の保護に関する条例

⑻　練馬区の実施機関等が保有する個人情報の適切な管理のための措置に関する指針

5　委託事業者等がセキュリティポリシーに違反した場合は、違反と過失の重大性に応じて、関係法令、契約等に基づき厳正な対応を求めるものとする。

（情報セキュリティ対策）

第９条　脅威から情報資産を保護するため、別に定めるところにより、つぎに掲げる情報セキュリティに関する対策を実施する。

⑴　物理的セキュリティ対策　情報システム機器の管理、管理区域の制限、特定個人情報を取り扱う事務を実施する区域（以下「取扱区域」という。）の明確化等による物理的な対策

⑵　人的セキュリティ対策　職員の遵守事項、利用者管理、委託管理等による人的な対策

⑶　技術的セキュリティ対策　コンピュータウィルス対策、不正アクセス対策等による技術的な対策

⑷　情報システムの運用対策　情報システムの開発段階から運用段階で求められる運用対策

2　前項に規定する情報セキュリティ対策を実施するに当たり、別に定めるところにより、情報資産について、機密性、完全性および可用性の観点から要求されるセキュリティの水準を定め、その重要度に応じて分類しなければならない。

（情報セキュリティに関する情報の収集等）

第10条　セキュリティ事故等を未然に防止し、セキュリティ対策の効果的かつ効率的な運用を実施するため、脅威等に関する情報を収集および共有しなければならない。

第２章　情報セキュリティマネジメント推進体制

（最高情報セキュリティ責任者）

第11条　セキュリティマネジメントを総合的に実施するため、最高情報セキュリティ責任者を置く。

2　最高情報セキュリティ責任者は、情報セキュリティに関する最終的な権限および責任を有する。

3　最高情報セキュリティ責任者は、企画部を担任する副区長とする。

4　最高情報セキュリティ責任者は、セキュリティマネジメントの実施に当たり、組織の総合調整を行う。

5　最高情報セキュリティ責任者は、つぎに掲げる事項についてマネジメントレビューを実施し、承認する。

⑴　セキュリティマネジメントに関する年度ごとの運営計画
⑵　一般教育に係る結果および効果の測定の報告
⑶　自己点検の結果および効果の測定の報告
⑷　監査の結果の報告
⑸　監査の結果により確認されたリスクに関するリスクマネジメントの実施状況
⑹　リスクマネジメントの結果
⑺　セキュリティ事故等に関する報告
⑻　委託事業者等の管理に関する報告
⑼　セキュリティマネジメントの実施状況

6　最高情報セキュリティ責任者は、別に定める要領の規定に従い、セキュリティ事故等に対応するとともに、区における緊急時対応計画の策定を管理する。

7　最高情報セキュリティ責任者は、第５項の規定によるマネジメントレビューの実施に当たり、指導および助言をする。

8　最高情報セキュリティ責任者は、本要綱に定める自らの担務を、本要綱に定める各責任者に担わせることができる。

（最高情報セキュリティアドバイザー）

第12条　最高情報セキュリティ責任者の職務を専門的な立場から補佐する者として、最高情報セキュリティアドバイザーを置くことができる。

2　最高情報セキュリティアドバイザーは、セキュリティマネジメントについて専門的な知識および経験を有する者のうちから、区長が委嘱する。

3　前項の規定にかかわらず、最高情報セキュリティアドバイザー業務を法人その他の団体（以下「法人等」という。）に委託する場合は、当該業務を受託した法人等がセキュリティマネジメントについて優れた見識を有する者として届け出た者を最高情報セキュリティアドバイザーとする。

4　最高情報セキュリティアドバイザーは、区のセキュリティマネジメントについて、専門的な立場から助言等をすることができる。

（情報セキュリティ監査責任者）

第13条　監査の実施に関する権限および責任を有する者として、情報セキュリティ監査責任者を置く。

2　情報セキュリティ監査責任者は、最高情報セキュリティ責任者が部長または課長のうち監査の公平性を確保できる者から任命する。

3　情報セキュリティ監査責任者は、監査について、つぎに掲げる事項を実施する。
⑴　監査に関する計画を策定すること。
⑵　監査の結果を承認すること。
⑶　監査の結果について最高情報セキュリティ責任者に報告すること。

（統括情報セキュリティ管理責任者）

第14条　最高情報セキュリティ責任者を補佐する者として、統括情報セキュリティ管理責任者を置く。

2　統括情報セキュリティ管理責任者は、企画部長とする。

3　統括情報セキュリティ管理責任者は、一般教育を実施する。

4　統括情報セキュリティ管理責任者は、つぎに掲げる事項を最高情報セキュリティ責任者に報告する。

⑴　一般教育の結果

⑵　自己点検の結果

⑶　リスクマネジメントの結果

⑷　委託事業者等の管理状況

5　統括情報セキュリティ管理責任者は、別に定める要領の規定および緊急時対応計画の記載に従い、セキュリティ事故等に対応する。

6　統括情報セキュリティ責任者は、セキュリティ事故等において最高情報セキュリティ責任者までの円滑な情報共有が図れるよう、緊急時の連絡体制を整備する。

7　統括情報セキュリティ管理責任者は、情報セキュリティ監査責任者に協力し、監査に関する職務を実施する。

8　統括情報セキュリティ管理責任者は、情報セキュリティ関連規程の運用に関して問題が生じた場合は、必要に応じて、最高情報セキュリティ責任者に報告する。

（統括情報システム管理者）

第15条　管理規程第10条第１項に規定する統括情報システム管理者（以下「統括情報システム管理者」という。）は、情報システムに関する専門的な観点から統括情報セキュリティ管理責任者を補佐する。

2　統括情報システム管理者は、管理規程第10条第３項第３号に規定する住民情報システム、庁内基盤システムおよびこれらの情報システムを取り扱うネットワークならびに共通基盤の情報セキュリティに関し、つぎに掲げる事項を実施する。

⑴　職場教育に関すること。

⑵　監査の結果により確認されたリスクに関するリスクマネジメント

⑶　別に定める要領の規定に従い、セキュリティ事故等に対応すること。

⑷　セキュリティポリシーの遵守状況について定期的に確認すること。

⑸　緊急時対応計画の策定および見直しに係る実務を担うこと。

⑹　実施手順の維持および管理を行うこと。

3　統括情報システム管理者は、情報セキュリティマネジメント運用（以下「セキュリティマネジメント運用」という。）に関し、指導および改善要求ならびに是正勧告された事項について、改善および是正するために必要な措置をとらなければならない。

（統括情報セキュリティ管理者）

第16条　情報セキュリティに関する専門的な観点で統括情報セキュリティ管理責任者を補佐するものとして、統括情報セキュリティ管理者を置く。

2　統括情報セキュリティ管理者は、情報政策課長とする。

3　統括情報セキュリティ管理者は、セキュリティマネジメント運用およびセキュリティ対策について指導および助言する。

4　統括情報セキュリティ管理者は、一般教育の結果および効果の測定の報告をとりまとめ、統括情報セキュリティ管理責任者に報告する。

5　統括情報セキュリティ管理者は、自己点検の結果をとりまとめ、統括情報セキュリティ管理責任者に報告する。

6　統括情報セキュリティ管理者は、別に定める要領の規定および緊急時対応計画の記載に従い、各課で発生したセキュリティ事故等に対応する。

7　統括情報セキュリティ管理者は、セキュリティ事故等に関する情報を収集し、必要に応じて関係する組織に周知しなければならない。

8　統括情報セキュリティ管理者は、委託事業者等の管理に関する状況をとりまとめ、統括情報セキュリティ管理責任者に報告する。

9　統括情報セキュリティ管理者は、監査に関する事務を担う。

（情報セキュリティ管理責任者）

第17条　各部におけるセキュリティマネジメントを実施するため、情報セキュリティ管理責任者を置く。

2　情報セキュリティ管理責任者は、部長とする。

3　情報セキュリティ管理責任者は、部のセキュリティ対策についての権限および責任を有する。

4　情報セキュリティ管理責任者は、情報セキュリティ責任者が適切に情報資産を管理するとともに、情報資産を取り扱うに当たり、適切なセキュリティ対策を実施するよう指揮監督しなければならない。

5　情報セキュリティ管理責任者は、部におけるセキュリティマネジメントについて、つぎに掲げる事項について指揮監督しなければならない。

⑴　所属する職員のセキュリティ対策に関すること。

⑵　所管する情報システムに関する開発、設定の変更、運用、更新等に関すること。

⑶　職員および委託事業者等のセキュリティポリシーの遵守状況について定期的に把握すること。

⑷　事務取扱担当者の特定個人情報の取扱い状況について定期的に把握すること。

6　情報セキュリティ管理責任者は、部におけるセキュリティマネジメント運用を適切に実施するに当たり、つぎに掲げる事項を実施するよう指揮監督しなければならない。

⑴　一般教育および職場教育の受講状況等を把握し、必要に応じて所管する情報資産の取扱いに関する職場教育を実施すること。

⑵　職員および委託事業者等に対して、一般教育を受講する機会を確保すること。

⑶　自己点検の実施状況等を把握すること。

⑷　監査の対象となった場合は、監査の実施に協力すること。

⑸　監査の結果により確認されたリスクに関するリスクマネジメントの実施状況を把握すること。

⑹　リスクマネジメントの結果について承認するとともに、定期的に統括情報セキュリティ管理責任者に報告すること。

⑺　別に定める要領の規定および緊急時対応計画の記載に従い、セキュリティ事故等に対応すること。

⑻　委託事業者等の管理状況を把握すること。

7　情報セキュリティ管理責任者は、セキュリティマネジメント運用に関する指導および改善要

求ならびに是正勧告等がされた事項について、改善および是正するために必要な措置をとらなければならない。

（情報セキュリティ責任者）

第18条　各課におけるセキュリティマネジメントを実施するため、情報セキュリティ責任者を置く。

2　情報セキュリティ責任者は、課長とする。ただし、担当課長を置く課にあっては、課長が定めるところにより、担当課長をその担任する事務に係る部分についての情報セキュリティ責任者とすることができる。

3　情報セキュリティ責任者は、課で所管する情報システムに関する開発、設定の変更、運用、更新等を行うに当たりセキュリティ対策を実施する権限および責任を有する。

4　情報セキュリティ責任者は、課における情報資産に関する管理責任を有するほか、情報資産を取り扱うに当たり、適切なセキュリティ対策を実施しなければならない。

5　情報セキュリティ責任者は、課におけるセキュリティマネジメントについて、つぎに掲げる事項を確認しなければならない。

⑴　課で所管する特定個人情報に係る実施手順の作成、維持および管理に関すること。

⑵　前号に規定する以外の情報資産に係る実施手順の作成、維持および管理を行うこと。

⑶　緊急時対応計画の作成、維持および管理を行うこと。

⑷　所属する職員のセキュリティ対策に関すること。

⑸　所管する情報システムに関する開発、設定の変更、運用、更新等に関すること。

⑹　職員および委託事業者等のセキュリティポリシーの遵守状況に関すること。

⑺　事務取扱担当者の特定個人情報の取扱い状況について定期的に把握すること。

6　情報セキュリティ責任者は、課におけるセキュリティマネジメント運用を適切に実施するに当たり、つぎに掲げる事項を実施しなければならない。

⑴　一般教育および職場教育の受講状況等を把握し、必要に応じて統括情報セキュリティ管理者に報告すること。

⑵　職員に対し、必要に応じて所管する情報資産の取扱いに関する職場教育を実施すること。

⑶　職員および委託事業者等に対して、一般教育を受講する機会を確保すること。

⑷　自己点検の実施状況を把握すること。

⑸　監査の対象となった場合は、監査の実施に協力すること。

⑹　監査の結果により、確認されたリスクに関するリスクマネジメントに関すること。

⑺　リスクマネジメントの実施状況について定期的に情報セキュリティ管理責任者に報告すること。

⑻　別に定める要領の規定および緊急時対応計画の記載に従い、セキュリティ事故等に対応すること。

⑼　委託事業者等の管理状況を把握すること。

7　情報セキュリティ責任者は、セキュリティマネジメント運用に関する指導および改善要求ならびに是正勧告等がされた事項について、改善および是正をするために必要な措置をとらなければならない。

8　情報セキュリティ責任者は、重要情報のうち特定個人情報を取り扱う場合は、つぎに掲げる

事項を実施しなければならない。

⑴　事務取扱担当者（委託事業者等を除く。）を明確にすること。

⑵　取り扱う特定個人情報の範囲を明確にした上で、適正に事務が執行されるよう、前号に規定する事務取扱担当者を指揮監督すること。

⑶　区が委託する場合および当該委託において再委託等が行われる場合は、委託事業者等および再委託先等が区と同等以上の情報資産の安全管理措置を講じることをあらかじめ確認すること。

⑷　区が委託する場合は、委託事業者等に事務取扱担当者となる者を明確にさせるとともに、適正な事務が行われるよう委託事業者等を監督すること。

⑸　前号の場合において、再委託等が行われるときは、再委託先等においても同号と同様に事務取扱担当者を明確にするとともに、適正な事務が行われるよう委託事業者等を監督すること。

⑹　取扱区域を明確にするとともに、適切に管理すること。

（情報セキュリティ担当者）

第19条　各課において、情報セキュリティ責任者の指示のもとセキュリティマネジメントの実施に関する実務を担う者として、各課に１名以上の情報セキュリティ担当者を置くものとし、当該情報セキュリティ担当者のうち１名は庶務担当係長とする。

２　前項の場合において、２名以上の情報セキュリティ担当者を置く場合は、同項の庶務担当係長に加え、つぎに掲げる者を置くものとする。

⑴　係長級職員を出先の施設等の長として配置する課にあっては、当該係長級職員。ただし、当該施設等に複数の係長級職員を配置しているときは、そのうちから情報セキュリティ責任者が指名する者とする。

⑵　前号に掲げる者のほか、情報セキュリティ責任者が指名する者

（情報システム担当者）

第20条　各課において、情報セキュリティ責任者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う者として、情報システム担当者を置く。

（ＩＴ推進本部）

第21条　ＩＴ推進本部は、管理規程第６条第６項の規定に基づき、同項第３号に規定する本部長が必要と認める事項として、つぎに掲げる事項について調査し、および審議する。

⑴　この要綱および対策基準の見直しならびに当該見直しの承認

⑵　セキュリティマネジメントの実施に当たり必要となる事項の見直しおよび当該見直しの承認

⑶　セキュリティ委員会からの発議に関すること。

（情報セキュリティ委員会）

第22条　セキュリティ対策に関する施策を立案し、推進するため、情報セキュリティ委員会を置く。

２　セキュリティ委員会は、委員長、副委員長および委員をもって構成する。

３　委員長は企画部長とし、副委員長は情報政策課長とする。

４　委員は別表に掲げる職にある者とする。

5　委員長は必要があると認められるときは、セキュリティ委員会に前項に掲げる委員以外の者の出席を求め、意見を聴き、または説明を求めることができる。

6　委員長は、セキュリティ委員会において調査および審議した結果について、速やかに最高情報セキュリティ責任者に報告するとともに、必要に応じ判断および指示を仰ぐ。

7　セキュリティ委員会は、つぎに掲げる事項を実施する。

⑴　この要綱および対策基準の見直しに関すること。

⑵　セキュリティマネジメントの実施に当たり必要となる事項の見直しに関すること。

⑶　セキュリティマネジメント運営計画（職員に対する情報セキュリティに関する研修計画を含む。）の原案の作成

⑷　ＩＴ推進本部への発議に関する検討

⑸　セキュリティ事故等に関する検討

⑹　ＣＳＩＲＴからの発議に関する審議

⑺　情報システムの分類に関する審議

⑻　前各号に掲げるもののほか、情報セキュリティに関すること。

8　前項第３号に規定する研修計画には、つぎに掲げる研修に関するものを含むものとする。

⑴　職員を対象とした研修

⑵　新規採用職員を対象とした研修

⑶　情報セキュリティ責任者およびその他の職員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研修

9　セキュリティ委員会の庶務は、企画部情報政策課において処理する。

（ＣＳＩＲＴ）

第23条　セキュリティ事故等が発生した際に、その状況を正確に把握・分析し、被害拡大防止、復旧等を迅速かつ的確に行うための緊急即応体制として、別に定めるところにより、CSIRT（Computer Security Incident Response Team）を設置する。

（ガバメントクラウドの利用における組織体制）

第24条　ガバメントクラウドの利用に関し、セキュリティ対策に取り組む十分な体制を整備しなければならない。

2　統括情報システム管理者および情報セキュリティ責任者は、ガバメントクラウドを利用する際は、関係する事業者の存在および責任の所在を確認し、複数の事業者が存在する場合は、必要な連絡体制を整備しなければならない。

第３章　情報セキュリティマネジメント運用

（情報セキュリティに関する教育および啓発）

第25条　セキュリティマネジメントを実施するための権限および責任を認識させるとともに、情報セキュリティに関する意識および理解度を高めるため、定期的にまたは必要に応じて、職員および委託事業者等に対して、情報セキュリティに関する教育および啓発を実施する。

（情報セキュリティに関する自己点検）

第26条　前条に規定する教育および啓発の効果を測定するとともに、自己のセキュリティ対策の状況把握および自己改善を推進することにより、セキュリティ対策の実効性を確保するため、定期的または必要に応じて、情報セキュリティに関する自己点検を実施する。

（情報セキュリティに関する監査）

第27条　セキュリティ対策の実施状況を評価し、是正を命ずることにより、セキュリティ対策の実効性を確保するため、各課におけるセキュリティ対策の実施状況について、定期的におよび必要に応じて、情報セキュリティに関する監査を実施する。

（情報セキュリティに関するリスクマネジメント）

第28条　監査の結果により、確認されたリスクについて、リスクに応じた適切なセキュリティ対策を実施するため、情報セキュリティに関するリスクマネジメントを実施する。

（情報セキュリティ事故等の管理）

第29条　セキュリティ事故等の発生時に迅速に対応し、被害の発生および拡大を防止するとともに、セキュリティ事故等の履歴等を記録および保存し、組織において共有することにより、その再発を未然に防止するため、セキュリティ事故等の管理を実施する。

２　セキュリティ事故等の管理に係る具体的事項は、別に要領で定めるとともに緊急時対応計画に記載する。

３　セキュリティ事故等が発生した場合は、事故等への対応、事故等の内容、責任の範囲等を斟酌し、必要に応じて情報資産の利用を制限することができる。

（委託事業者等の管理）

第30条　区の情報資産を取り扱う委託事業者等のセキュリティポリシーおよび実施手順ならびに特記事項の遵守状況を確認するため、委託事業者等の管理を実施する。

第４章　補則

（セキュリティマネジメント等の見直し）

第31条　セキュリティマネジメントおよびセキュリティマネジメント運営計画は、区の情報セキュリティを取り巻く状況の変化およびつぎに掲げる事項を反映し、効果的かつ効率的に実施できるよう見直しを行わなければならない。

⑴　セキュリティマネジメント運用の運用状況

⑵　セキュリティポリシーの遵守状況

⑶　新たな脅威の出現

２　前項の規定による見直しの場合において、必要に応じ、セキュリティポリシーおよび関係規程の見直しを行うものとする。

（委任）

第32条　この要綱に定めるもののほか、必要な事項は、別に定める。

付　則

この要綱は、平成20年４月１日から施行する。

付　則（平成21年３月31日　20練企情第1773号）

この要綱は、平成21年４月１日から施行する。

付　則（平成22年３月30日　21練企情第1440号）

この要綱は、平成22年４月１日から施行する。

付　則（平成24年３月28日　23練企情第1569号）

この要綱は、平成24年４月２日から施行する。

付　則（平成27年３月31日　26練企情第2097号）

この要綱は、平成27年４月１日から施行する。

付　則（平成27年10月１日　27練企情第1135号）

この要綱は、平成27年10月５日から施行する。

付　則（平成28年３月31日　27練企情第 2288号）

この要綱は、平成28年４月１日から施行する。

付　則（平成29年３月31日　28練企情第1961号）

この要綱は、平成29年４月１日から施行する。

付　則（平成31年３月15日　30練企情第1647号）

この要綱は、平成31年３月15日から施行する。

付　則（平成31年３月29日　30練企情第1718号）

この要綱は、平成31年４月１日から施行する。

付　則（令和５年３月31日　４練企情第2940号）

この要綱は、令和５年４月１日から施行する。

付　則（令和５年11月30日　５練企情第2198号）

この要綱は、令和５年12月１日から施行する。

別表（第22条関係）

区長室広聴広報課長
危機管理室危機管理課長
総務部総務課長
総務部文書法務課長
総務部情報公開課長
総務部経理用地課長
総務部職員課長
総務部人材育成課長
区民部戸籍住民課長
福祉部管理課長
健康部健康推進課長
教育振興部教育総務課長
こども家庭部子育て支援課長