資料1

個人情報保護管理運営会議　付議事項

件名	東京共同電子申請・届出サービスの利用に係る外部結合等について（手続の追加）

内容は別紙のとおり

要綱の根拠

◇第３条第１項第３号（外部結合、業務委託）

（担当部課：総合政策部行政管理課、情報システム課、
健康部四谷保健センター、
環境清掃部ごみ減量リサイクル課）

事業の概要

事業名	行政手続のオンライン化等の推進
担当課	行政管理課、情報システム課、四谷保健センター、ごみ減量リサイクル課
目　的	申請者が窓口に来庁することなく、２４時間申請手続を可能とするため、行政手続のオンライン化を推進し、区民の利便性向上を図るため。
対象者	資料１－１の手続の申請者
事業内容	１　概要 区では、平成１６年度から東京都及び都内区市町村で構成される東京電子自治体共同運営協議会（東京電子自治体共同運営センター）が提供する「東京共同電子申請・届出サービス」を活用し、子どもや健康、防災、景観などに関する申請やイベントの申込みなどの手続をオンラインで受け付けている（平成１６年度第７回情報公開･個人情報保護審議会承認・了承済。以降、手続の追加の都度、情報公開･個人情報保護審議会に諮問・報告又は個人情報保護管理運営会議に付議し、承認・了承済となっている。）。 この度、新たに資料１－１の手続を追加することで、さらなる区民の利便性の向上を図ることとする（各手続の事業概要は、参考１－１を参照)。 ２　個人情報保護管理運営会議への付議内容 （１）外部結合 既に外部結合を行っている「東京共同電子申請・届出サービス」において、手続の追加を行う。 （２）業務委託 「東京共同電子申請・届出サービス」の運用管理業務を委託する富士通株式会社が取扱う情報項目の追加を行う。 （３）その他 区では、これまで「東京共同電子申請・届出サービス」を活用し、行政手続きのオンライン化を進めてきたが、本サービスは令和６年度末で廃止となるほか、東京都及び都内区市町村で、新たな電子申請サービス（ＬｏＧｏフォーム）が導入され

	る。 　区においても、４月中旬以降、新たな電子申請の導入にあたり、当該サービスを利用することとなっているため、「東京共同電子申請・届出サービス」による電子申請の手続きの追加は、本件で最後となる。 　※個人情報の流れは、資料１－２のとおり

別紙（電子計算機の外部結合関係）

◇外部結合（第３条第１項第３号）

件名　東京共同電子申請・届出サービスの利用に係る外部結合について（情報項目の追加）

※太字ゴシック（下線）が、令和５年度第１２回新宿区個人情報保護管理運営会議承認済の内容からの変更箇所

保有課（担当課）	行政管理課、情報システム課、四谷保健センター、ごみ減量リサイクル課
登録業務の名称	**追加する手続（登録業務）は、資料１－１のとおり**
結合される情報項目（だれの、どのような項目か）	**追加する手続ごとの情報項目は、資料１－１のとおり**
結合の相手方	東京電子自治体共同運営協議会（東京電子自治体共同運営センター） ※東京都と都内区市町村で構成されている。
結合する理由	「東京共同電子申請・届出サービス」は、東京電子自治体共同運営協議会がシステムを構築し、構成団体で共同利用することで高品質なサービスの廉価な提供を実現している。 「東京共同電子申請・届出サービス」を活用することで、申請者は窓口に来庁することなく、２４時間申請手続が可能となり、区民の利便性向上を図ることができるため。
結合の形態	LGWAN 回線を利用して、東京電子自治体共同運営センターのサーバと区のイントラネット端末を接続する。
結合の開始時期と期間	**令和６年４月１５日から令和７年３月３１日まで** ※上記相手方との外部結合は、平成17年1月から行っている。
情報保護対策	別紙チェックリストのとおり

別紙（業務委託）

◇業務委託（第３条第１項第３号）

件名　東京共同電子申請・届出サービスの利用に係る運用管理業務の委託について（手続の追加）

※太字ゴシック（下線）が、令和５年度第１２回新宿区個人情報保護管理運営会議承認済の内容からの変更箇所

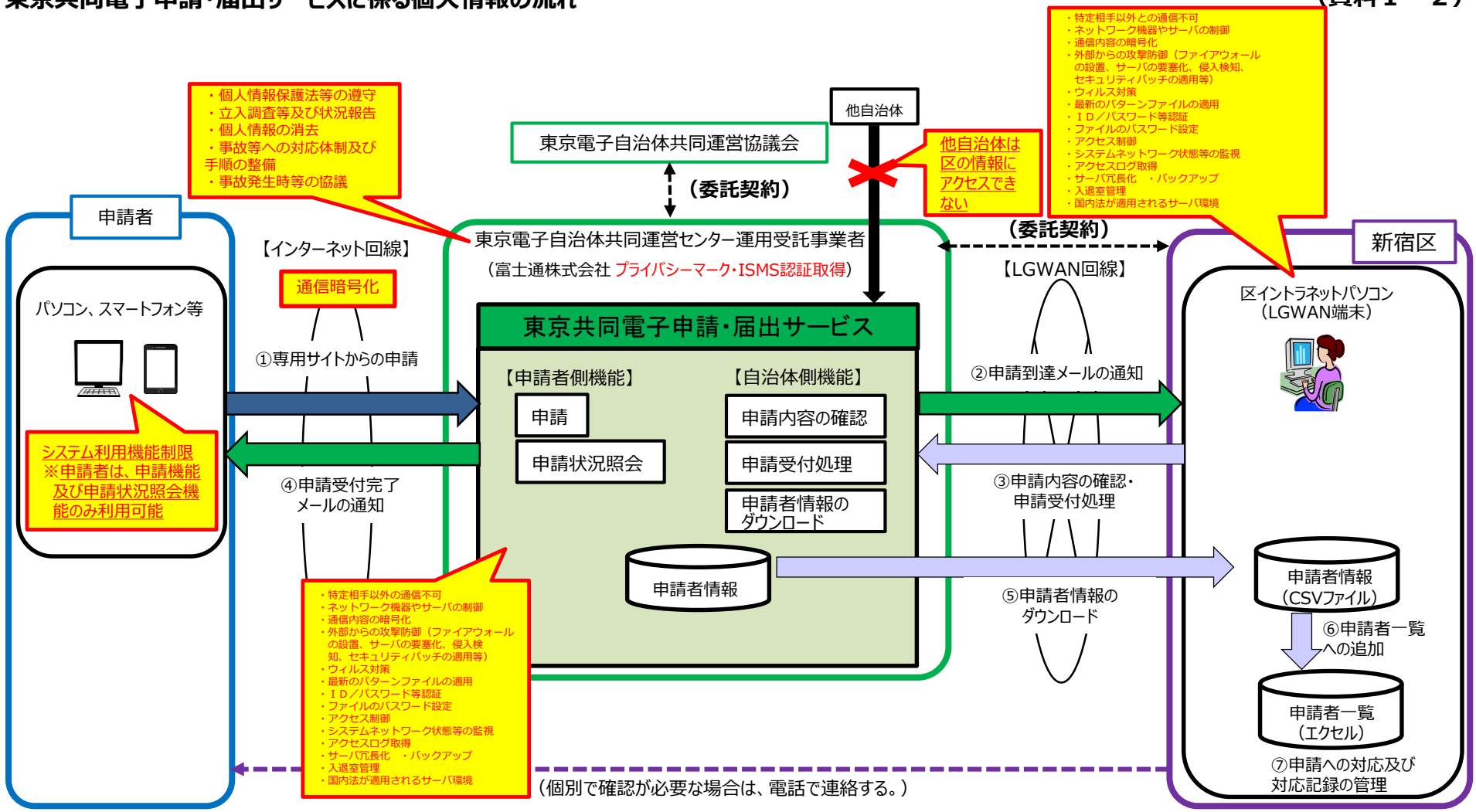
保有課（担当課）	行政管理課、情報システム課、四谷保健センター、ごみ減量リサイクル課
登録業務の名称	**追加する手続は、資料１－１のとおり**
委託先	富士通株式会社（プライバシーマーク、ＩＳＯ２７００１取得）
委託に伴い事業者に処理させる情報項目（だれの、どのような項目か）	**追加する手続ごとの情報項目は、資料１－１のとおり**
処理させる情報項目の記録媒体	東京電子自治体共同運営協議会（東京電子自治体共同運営センター）のサーバ
委託理由	「東京共同電子申請・届出サービス」は、東京電子自治体共同運営協議会がシステムを構築し、それを共用することで高品質なサービスの廉価な提供を実現している。 「東京共同電子申請・届出サービス」を活用することで、申請者は、窓口に来庁することなく、２４時間申請手続が可能となり、区民の利便性向上を図ることができる。 上記委託先については、東京電子自治体共同運営協議会に承認された事業者であり、セキュリティの安全確保に優れた事業者であるため。
委託の内容	東京電子自治体共同運営協議会が提供する「東京共同電子申請・届出サービス」の運用管理
委託の開始時期及び期限	**令和６年４月１５日から令和７年３月３１日まで**
委託にあたり区が行う情報保護対策	別紙チェックリストのとおり
受託事業者に行わせる情報保護対策	別紙チェックリストのとおり

【追加手続及び情報項目】

No	手続名（登録業務名）	担当課	取扱う個人情報項目	年間 申請件数 （予定）
1	女性の健康支援事業に関する申込み及びアンケート	四谷保健センター	氏名、性別、住所、電話番号、メールアドレス、在住・在勤・在学の別、年齢、診断日（乳がん体験者の会参加者のみ）	約 500 件
2	食品ロスダイアリーモニターへの参加申込み	ごみ減量リサイクル課	氏名、郵便番号、住所、電話番号、メールアドレス、年代、世帯人数	約 100 件
3	食品ロス削減協力店登録に関する届	ごみ減量リサイクル課	担当者名、送付先住所、電話番号、メールアドレス	約 20 件
4	フードドライブ物品借用申請に関する届	ごみ減量リサイクル課	担当者名、電話番号、メールアドレス	約 10 件
5	路上喫煙対策協力員活動計画書	ごみ減量リサイクル課	氏名、住所、電話番号、メールアドレス	約 10 件
6	路上喫煙対策協力員活動報告書	ごみ減量リサイクル課	氏名、住所、電話番号、メールアドレス	約 20 件
7	春のごみゼロデー参加申込み	ごみ減量リサイクル課	氏名、電話番号、メールアドレス	約 100 件

東京共同電子申請・届出サービスに係る個人情報の流れ

（資料１－２）



【各手続の概要】

No	手続名（登録業務名）	担当課	手続概要
1	女性の健康支援事業に関する申込み及びアンケート	四谷保健センター	女性の健康支援事業に関するセミナーやイベント、集まりの参加申し込みを受け付ける。また、事後アンケート等を収集する。
2	食品ロスダイアリーモニターへの参加申込み	ごみ減量リサイクル課	日々の食品ロスを記録する「食品ロスダイアリー」モニター調査を実施するため、モニターの参加申込の事前受付を行い、対象者に通知等を送付する。
3	新宿区食品ロス削減協力店登録に関する届	ごみ減量リサイクル課	区内事業者を対象に、食品ロス削減に積極的に取り組む事業者の登録や登録内容の変更等を受け付け、登録者に通知等を送付する。
4	フードドライブ物品借用申請に関する届	ごみ減量リサイクル課	企業等の団体がフードドライブを実施するための物品貸出について、事前受付等を行い、申請者に通知等を送付する。
5	路上喫煙対策協力員活動計画書	ごみ減量リサイクル課	路上喫煙対策協力員としての年間活動計画の提出を受け付ける。
6	路上喫煙対策協力員活動報告書	ごみ減量リサイクル課	路上喫煙対策協力員として活動した際の活動報告を受け付ける。
7	春のごみゼロデー参加申込み	ごみ減量リサイクル課	5月30日の新宿駅前イベント及びごみゼロ期間（5月30日を前後とした約1月間）の清掃活動の参加申込みを受け付ける。

4　外部結合にかかる個人情報保護対策チェックリスト

	・対策が可能であれば「○」 ・対策の必要がない場合は「ー」	情報保護対策
区が行う情報保護対策 【運用上の対策】	○	個人情報保護法及び新宿区情報セキュリティポリシーを遵守するよう指導する。また、クラウドサービスを利用する場合は、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」を準拠するよう指導する。
	○	必要に応じて、事業者への立入り調査等を実施するとともに、結合先に対し速やかに状況報告をするよう指導する。
	○	システム上で不要となった電子データを削除し、電子データの消去を行ったことの報告書を提出するよう指導する。
	○	業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備し、結合先と緊急時の連絡体制や対応手順を確認する。
	○	事故が発生した場合又は個人情報保護及び情報セキュリティ対策の変更があった場合は、直ちに結合先と今後の対応を協議する。
区が行う情報保護対策 【システム上の対策】	○	接続するネットワークについては、特定相手以外との通信を不可とする。
	○	ネットワーク機器やサーバを制御し、通信できるシステムを限定する。
	○	通信内容は暗号化し、通信途上の個人情報の盗用、改ざん、成りすましを防止する。
	○	ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じ、外部からの不正侵入やデータ破壊・漏えい等各種の攻撃から防御する。
	○	コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用する。
	○	ID・パスワードやアドレス情報による運用により、第三者による個人情報の盗用、改ざん、成りすましを防止する。
	○	個人情報を保存する場合は、保存先フォルダへアクセス権を設定するとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底する。
	○	システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得する。取得したログは、定期的に分析する。
	○	サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備する。
	○	入退室管理等により情報資産の危殆化を防止する。
	○	システムを提供するサーバは日本国内の法が適用される安全性が確保された環境にする。

4　外部結合にかかる個人情報保護対策チェックリスト

	・対策が可能であれば「○」 ・対策の必要がない場合は「ー」	情報保護対策
結合先に行わせる情報保護対策【運用上の対策】	○	個人情報保護法及び新宿区情報セキュリティポリシーを遵守させる。また、クラウドサービスを利用する場合は、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」を準拠させる。
	○	必要に応じて、事業者への立入り調査等を受けさせるとともに、結合先に対し速やかに状況報告をさせる。
	○	システム上で不要となった電子データを削除させ、電子データの消去を行ったことの報告書を提出させる。
	○	業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備させ、区と緊急時の連絡体制や対応手順を確認させる。
	○	事故が発生した場合又は個人情報保護及び情報セキュリティ対策の変更があった場合は、直ちに区と今後の対応を協議させる。
結合先に行わせる情報保護対策【システム上の対策】	○	接続するネットワークについては、特定相手以外との通信を不可とさせる。
	○	ネットワーク機器やサーバを制御し、通信できるシステムを限定させる。
	○	通信内容は暗号化させ、通信途上の個人情報の盗用、改ざん、成りすましを防止させる。
	○	ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じさせ、外部からの不正侵入やデータ破壊・漏えい等各種の攻撃から防御させる。
	○	コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用させる。
	○	ID・パスワードやアドレス情報による運用により、第三者による個人情報の盗用、改ざん、成りすましを防止させる。
	○	個人情報を保存する場合は、保存先フォルダへアクセス権を設定させるとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底させる。
	○	システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得させる。取得したログは、定期的に分析させる。
	○	サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備させる。
	○	入退室管理等により情報資産の危殆化を防止させる。
	○	システムを提供するサーバは日本国内の法が適用される安全性が確保された環境にさせる。

5　業務委託にかかる個人情報保護対策チェックリスト

（電磁的媒体・紙媒体の取扱い）

	・対策が可能であれば「○」 ・対策の必要がない場合は「ー」	情報保護対策
委託にあたり区が行う情報保護対策【運用上の対策】	○	契約にあたり、「特記事項」を付すとともに、個人情報保護法及び新宿区情報セキュリティポリシーを遵守するよう指導する。また、クラウドサービスを利用する場合は、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」を準拠するよう指導する。
	○	契約履行の間、特記事項に基づき立入り調査等を実施するとともに、委託先に対し速やかに状況報告をするよう指導する。
	○	取扱責任者及び取扱者をあらかじめ指定し、区に報告するよう指導する。
	○	全体の業務フローを作成し、委託先と共有する。
	○	個人情報を含むデータを作成する必要が生じた場合は、パスワードを付してデータを暗号化する。また、電磁的媒体（DVD-R等）とパスワード通知書の受渡しは、それぞれ別の機会を設定し、鍵付きカバン等を使用して、手渡しで行うよう指導する。
	ー（電子データのみの取扱いのため）	個人情報を手交する場合は、鍵付きカバン等を使用して運搬する。
	ー（電子データのみの取扱いのため）	個人情報の受渡しにあたっては、管理簿に記載する。管理簿には、日時、取扱者、情報の内容、数量を確認記録票に記録し、履歴を追跡できるようにする。
	ー（電子データのみの取扱いのため）	個人情報は、施錠できる金庫又はキャビネット等に保管する。
	○	業務履行後、個人情報が記録された電磁的媒体（DVD-R等）、紙媒体及びパスワード通知書は返却し、電子データは消去するよう指導する。また、区に電子データの消去を行ったことの報告書を提出するよう指導する。
	○	業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備し、委託先と緊急時の連絡体制や対応手順を確認する。
	○	事故が発生した場合又は個人情報保護及び情報セキュリティ対策の変更があった場合は、直ちに委託先と今後の対応を協議する。
委託にあたり区が行う情報保護対策【システム上の対策】	○	接続するネットワークについては、特定相手以外との通信を不可とする。
	○	ネットワーク機器やサーバを制御し、通信できるシステムを限定する。
	○	通信内容は暗号化し、通信途上の個人情報の盗用、改ざん、成りすましを防止する。
	○	ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じ、外部からの不正侵入やデータ破壊・漏えい等各種の攻撃から防御する。
	○	コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用する。
	○	ID・パスワードやアドレス情報による運用により、第三者による個人情報の盗用、改ざん、成りすましを防止する。
	○	個人情報を保存する場合は、保存先フォルダへアクセス権を設定するとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底する。
	○	システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得する。取得したログは、定期的に分析する。
	○	サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備する。
	○	入退室管理等により情報資産の危殆化を防止する。
	○	システムを提供するサーバは日本国内の法が適用される安全性が確保された環境にする。

5　業務委託にかかる個人情報保護対策チェックリスト

（電磁的媒体・紙媒体の取扱い）

	・対策が可能であれば「○」 ・対策の必要がない場合は「ー」	情報保護対策
委託事業者に行わせる情報保護対策【運用上の対策】	○	契約にあたり、「特記事項」を付すとともに、個人情報保護法及び新宿区情報セキュリティポリシーを遵守させる。また、クラウドサービスを利用する場合は、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」を準拠させる。
	○	契約履行の間、特記事項に基づき立入り調査等を受けさせるとともに、委託先に対し速やかに状況報告をさせる。
	○	取扱責任者及び取扱者をあらかじめ指定させ、区に報告させる。
	○	区が作成した業務フローに基づき、業務を行わせる。
	○	個人情報を含むデータを作成する必要が生じた場合は、パスワードを付してデータを暗号化させる。電磁的媒体（DVD-R等）とパスワード通知書の受渡しは、それぞれ別の機会を設定し、鍵付きカバン等を使用させ、手渡しで行わせる。
	ー（電子データのみの取扱いのため）	個人情報を手交する場合は、鍵付きカバン等を使用して運搬させる。
	ー（電子データのみの取扱いのため）	個人情報の受け渡しにあたっては、管理簿に記載させる。管理簿には、日時、取扱者、情報の内容、数量を確認記録票に記録し、履歴を追跡できるようにさせる。
	ー（電子データのみの取扱いのため）	個人情報は、施錠できる金庫又はキャビネット等に保管させる。
	○	業務履行後、個人情報が記録された電磁的媒体（DVD-R等）、紙媒体及びパスワード通知書は返却させ、電子データは消去させる。また、区に電子データの消去を行ったことの報告書を提出させる。
	○	業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備させ、区と緊急時の連絡体制や対応手順を確認させる。
	○	事故が発生した場合又は個人情報保護及び情報セキュリティ対策の変更があった場合は、直ちに区と今後の対応を協議させる。
委託事業者に行わせる情報保護対策【システム上の対策】	○	接続するネットワークについては、特定相手以外との通信を不可とする。
	○	ネットワーク機器やサーバを制御し、通信できるシステムを限定させる。
	○	通信内容は暗号化させ、通信途上の個人情報の盗用、改ざん、成りすましを防止させる。
	○	ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じさせ、外部からの不正侵入やデータ破壊・漏えい等各種の攻撃から防御させる。
	○	コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用させる。
	○	ID・パスワードやアドレス情報による運用により、第三者による個人情報の盗用、改ざん、成りすましを防止させる。
	○	個人情報を保存する場合は、保存先フォルダへアクセス権を設定させるとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底させる。
	○	システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得させる。取得したログは、定期的に分析させる。
	○	サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備させる。
	○	入退室管理等により情報資産の危殆化を防止させる。
	○	システムを提供するサーバは日本国内の法が適用される安全性が確保された環境にさせる。