指針と向日市セキュリティポリシー及び向日市個人情報取扱事務委託基準との対比表
１．向日市セキュリティポリシーとの対比

行政機関等の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					向日市情報セキュリティポリシー	
番号	大項目	中項目		詳細	項目	詳細
4-8-6	情報システムにおける安全の確保等	アクセス制御	(1)	保護管理者は、保有個人情報の秘匿性等その内容に応じて、認証機能を設定する等のアクセス制御のために必要な措置を講ずる。	アクセス制御 ７．１(8)② ７．２(1)①	②統括情報セキュリティ管理者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。 ①統括情報セキュリティ管理者及び情報セキュリティ管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限しなければならない。
			(2)	保護管理者は、上記の措置を講ずる場合には、パスワード等の管理に関する定めを整備するとともに、パスワード等の読取防止等を行うために必要な措置を講ずる。	アクセス制御 ７．２(3)	３ 認証情報の管理 ①統括情報セキュリティ管理者及び情報セキュリティ管理者は、職員等の認証情報を厳重に管理しなければならない。 ②統括情報セキュリティ管理者及び情報セキュリティ管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、初回ログイン後直ちに仮のパスワードを変更させなければならない。 ③統括情報セキュリティ管理者及び 情報セキュリティ管理者は、認証情報の不正利用を防止するための措置を講じなければならない。
		アクセス記録	(3)	保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報へのアクセス状況を記録し、その記録（以下「アクセス記録」という。）を一定の期間保存し、及びアクセス記録を定期的に分析するために必要な措置を講ずる。	ログの取得等 ７．１(6)	①統括情報セキュリティ管理者及び情報セキュリティ管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存し、適正に管理しなければならない。 ②統括情報セキュリティ管理者及び情報セキュリティ管理者は、取得したログ等を定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。
			(4)	保護管理者は、アクセス記録の改ざん、窃取又は不正な消去の防止のために必要な措置を講ずる。	対象とする脅威 第２章3(1) コンピュータ及びネットワークの管理 第３章７．１(4) (6)	３ 情報資産に対する脅威として、次の脅威を想定し、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、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 ７．１ コンピュータ及びネットワークの管理 (4) システム管理記録及び作業の確認 ①情報セキュリティ管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。 ②統括情報セキュリティ管理者及び情報セキュリティ管理者は、所管する情報システムにおいてシステム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理しなければならない。 (6) ログの取得等 ①統括情報セキュリティ管理者及び情報セキュリティ管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存し、適正に管理しなければならない。 ②統括情報セキュリティ管理者及び情報セキュリティ管理者は、取得したログ等を定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。
		アクセス状況の監視	(5)	保護管理者は、保有個人情報の秘匿性等その内容及びその量に応じて、当該保有個人情報への不適切なアクセスの監視のため、保有個人情報を含む又は含むおそれがある一定量以上の情報が情報システムからダウンロードされた場合に警告表示がなされる機能の設定、当該設定の定期的確認等の必要な措置を講ずる。	不正アクセス対策 ７．５(4) 情報システムの監視 ８．１①	(4)内部からの攻撃 統括情報セキュリティ管理者及び情報セキュリティ管理者は、職員等及び委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃及び外部のサイトに対する攻撃を監視しなければならない。 ①統括情報セキュリティ管理者及び情報セキュリティ管理者は、情報セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。
		管理者権限の設定	(6)	保護管理者は、保有個人情報の秘匿性等その内容に応じて、情報システムの管理者権限の特権を不正に窃取された際の被害の最小化及び内部からの不正操作等の防止のため、当該特権を最小限とする等の必要な措置を講ずる。	③特権を付与されたＩＤの管理等 ７．２(1)③(7)	統括情報セキュリティ管理者及び情報セキュリティ管理者は、管理者権限等の特権を付与されたＩＤを利用する者を必要最小限にし、当該ＩＤに係るパスワードの漏えい等が発生しないよう、当該ＩＤ及びパスワードを厳重に管理しなければならない。
		外部からの不正アクセスの防止	(7)	保護管理者は、保有個人情報を取り扱う情報システムへの外部からの不正アクセスを防止するため、ファイアウォールの設定による経路制御等の必要な措置を講ずる。	外部ネットワークとの接続制限等 ７．１(10)③	統括情報セキュリティ管理者及び情報セキュリティ管理者は、ウェブサーバ等をインターネットに公開する場合、庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。
		不正プログラムによる漏えい等の防止	(8)	保護管理者は、不正プログラムによる保有個人情報の漏えい等の防止のため、ソフトウェアに関する公開された脆弱性の解消、把握された不正プログラムの感染防止等に必要な措置（導入したソフトウェアを常に最新の状態に保つことを含む。）を講ずる。	不正プログラム対策 ７．４(2)①, ②	①情報セキュリティ管理者は、その所管するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアをシステムに常駐させなければならない。 ②インターネットに接続していないシステムにおいて電磁的記録媒体を使用する場合、コンピュータウイルス等の感染を防止するために、本市が管理している電磁的記録媒体以外の媒体を職員等に利用させてはならない。また、不正プログラムの感染、侵入等が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

行政機関等の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					向日市情報セキュリティポリシー	
番号	大項目	中項目		詳細	項目	詳細
		情報システムにおける保有個人情報の処理	(9)	職員は、保有個人情報について、一時的に加工等の処理を行うため複製等を行う場合には、その対象を必要最小限に限り、処理終了後は不要となった情報を速やかに消去する。保護管理者は、当該保有個人情報の秘匿性等その内容に応じて、随時、消去等の実施状況を重点的に確認する。	取扱制限 ３．３(1) 情報資産の管理 ３．３.(2)③(ｳ) 職員等の利用する端末、電磁的記録媒体等の管理 ５．４①	(1)【「機密性による情報資産の分類」に関する「取扱制限」において、必要以上の複製及び配布を禁止】 (ｳ)情報を作成する者は、作成途上の情報についても、紛失、流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。 ①【前段略】電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。 **【後段部分は規程に直接規定】**
		暗号化	(10)	保護管理者は、保有個人情報の秘匿性等その内容に応じて、暗号化のために必要な措置を講ずる。職員は、これを踏まえ、その処理する保有個人情報について、当該保有個人情報の秘匿性等その内容に応じて、適切に暗号化を行う。	情報資産の分類と管理 ３．(1),(2)⑦ 職員等の利用する端末、電磁的記録媒体等の管理 ５．４⑤ その他の該当箇所 ７．１(13)(15)(16) ７．２(2) ９．２(5)	(1)　機密性による情報資産の分類において、機密性２及び機密性３の取扱い制限に「情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定、鍵付きケースへの格納」を規定 (2)⑦情報の送信 電子メール等により機密性２以上の情報を送信する者は、必要に応じ、パスワード等による暗号化を行わなければならない。 ⑤情報セキュリティ管理者は、パソコン、モバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。同様に、電磁的記録媒体についても利用できる場合にはデータ暗号化機能を備える媒体を使用しなければならない。
		記録機能を有する機器・媒体の接続制限	(11)	保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報の漏えい等の防止のため、スマートフォン、USB メモリ等の記録機能を有する機器・媒体の情報システム端末等への接続の制限（当該機器の更新への対応を含む。）等の必要な措置を講ずる。	情報の持ち出し不可設定 ３章４.(1)②(ｲ)	(ｲ)情報の持ち出し不可設定 原則として、ＵＳＢメモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。
		端末の限定	(12)	保護管理者は、保有個人情報の秘匿性等その内容に応じて、その処理を行う端末を限定するために必要な措置を講ずる。	情報のアクセス対策 ３章４.(1)②(ｱ)	(ｱ)情報のアクセス対策 情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を利用しなければならない。また、必要に応じて、業務ごとに専用端末を設置する。
		端末の盗難防止等	(13)	保護管理者は、端末の盗難又は紛失の防止のため、端末の固定、執務室の施錠等の必要な措置を講ずる。	職員等の利用する端末、電磁的記録媒体等の管理 ３章５．４①	①情報セキュリティ管理者は、盗難防止のため、執務室等で利用する端末については施錠管理された建物において、また電磁的記録媒体については施錠可能なキャビネット等において、使用時以外は適切に保管しなければならない。【後段略】
			(14)	職員は、保護管理者が必要であると認めるときを除き、端末を外部へ持ち出し、又は外部から持ち込んではならない。	職員等の遵守事項 ３章６．１(1)③、⑤	③モバイル端末、電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限 (ｲ)　職員等は、本市のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。 ⑤持ち出し及び持ち込みの記録 情報セキュリティ管理者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。
		第三者の閲覧防止	(15)	職員は、端末の使用に当たっては、保有個人情報が第三者に閲覧されることがないよう、使用状況に応じて情報システムからログオフを行うことを徹底する等の必要な措置を講ずる。	机上の端末等の管理 ３章６．１(1)⑦	職員等は、パソコン、モバイル端末、電磁的記録媒体、情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン及びモバイル端末のロック、電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じなければならない。
		入力情報の照合等	(16)	職員は、情報システムで取り扱う保有個人情報の重要度に応じて、入力原票と入力内容との照合、処理前後の当該保有個人情報の内容の確認、既存の保有個人情報との照合等を行う。		**【規程に直接規定】**
		バックアップ	(17)	保護管理者は、保有個人情報の重要度に応じて、バックアップを作成し、分散保管するために必要な措置を講ずる。	バックアップの実施 ３章７．１(2)	情報セキュリティ管理者は、情報システムのサーバ等に記録された情報について、サーバの冗長化対策にかかわらず、必要に応じて定期的にバックアップを実施しなければならない。
		情報システム設計書等の管理	(18)	保護管理者は、保有個人情報に係る情報システムの設計書、構成図等の文書について外部に知られることがないよう、その保管、複製、廃棄等について必要な措置を講ずる。	情報システム仕様書等の管理 ７．１(5)	統括情報セキュリティ管理者及び情報セキュリティ管理者は、ネットワーク構成図及び情報システム仕様書について、記録媒体にかかわらず、業務上必要とする者以外の者による閲覧、紛失等がないよう適正に管理しなければならない。

行政機関等の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					向日市情報セキュリティポリシー	
番号	大項目	中項目		詳細	項目	詳細
4-8-7	情報システム室等の安全管理	入退管理	(1)	保護管理者は、保有個人情報を取り扱う基幹的なサーバ等の機器を設置する室その他の区域（以下「情報システム室等」という。）に立ち入る権限を有する者を定めるとともに、用件の確認、入退の記録、部外者についての識別化、部外者が立ち入る場合の職員の立会い又は監視設備による監視、外部電磁的記録媒体等の持込み、利用及び持ち出しの制限又は検査等の措置を講ずる。また、保有個人情報を記録する媒体を保管するための施設を設けている場合においても、必要があると認めるときは、同様の措置を講ずる。	管理区域の入退室管理等 ３章５．２(2) ①,②,③	⑵管理区域の入退室管理等 ①情報セキュリティ管理者は、管理区域への入退室を許可された者のみに制限し、ＩＣカード、指紋認証等の生体認証及び入退室管理簿の記載による入退室管理を行わなければならない。 ②職員等及び外部委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。 ③情報セキュリティ管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。
			(2)	保護管理者は、必要があると認めるときは、情報システム室等の出入口の特定化による入退の管理の容易化、所在表示の制限等の措置を講ずる。	管理区域の構造等 ３章５．２(1)②	統括情報セキュリティ管理者及び情報セキュリティ管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。
			(3)	保護管理者は、情報システム室等及び保管施設の入退の管理について、必要があると認めるときは、立入りに係る認証機能を設定し、及びパスワード等の管理に関する定めの整備（その定期又は随時の見直しを含む。）、パスワード等の読取防止等を行うために必要な措置を講ずる。	管理区域の入退室管理等 ３章５．２(2)①	情報セキュリティ管理者は、管理区域への入退室を許可された者のみに制限し、ＩＣカード、指紋認証等の生体認証及び入退室管理簿の記載による入退室管理を行わなければならない。
		情報システム室等の管理	(4)	保護管理者は、外部からの不正な侵入に備え、情報システム室等に施錠装置、警報装置及び監視設備の設置等の措置を講ずる。	管理区域の構造等 ３章５．２(1)②	統括情報セキュリティ管理者及び情報セキュリティ管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。
			(5)	保護管理者は、災害等に備え、情報システム室等に、耐震、防火、防煙、防水等の必要な措置を講ずるとともに、サーバ等の機器の予備電源の確保、配線の損傷防止等の措置を講ずる。	機器の取付け ３章５．１(1) 機器の電源 ３章５．１(2)	⑴機器の取付け 情報セキュリティ管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適正に固定する等、必要な措置を講じなければならない。 ⑵機器の電源 ①情報セキュリティ管理者は、統括情報セキュリティ管理者及び施設管理部門と連携し、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適正に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

２．向日市個人情報取扱事務委託基準との対比

行政機関等の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					向日市個人情報取扱事務委託基準	
番号	大項目	中項目		詳細	項目	詳細
4-8-9	個人情報の取扱いの委託	業務の委託等	(1)	個人情報の取扱いに係る業務を外部に委託する場合には、個人情報の適切な管理を行う能力を有しない者を選定することがないよう、必要な措置を講ずる。また、契約書に、次の事項を明記するとともに、委託先における責任者及び業務従事者の管理体制及び実施体制、個人情報の管理の状況についての検査に関する事項等の必要な事項について書面で確認する。	委託に当たっての留意事項 第３(1) 個人情報取扱特記事項 第１～１２	第３ 実施機関は、委託に当たっては次の事項に留意するものとする。 (1)委託先の選定に当たっては、個人情報の適正な取扱いを確保する措置として別記「個人情報取扱特記事項」を遵守できるものを選ぶこと。
				① 個人情報に関する秘密保持、利用目的以外の目的のための利用の禁止等の義務 ② 再委託の制限又は事前承認等再委託に係る条件に関する事項 （※）委託先との契約書に、再委託に際して再委託先に求める事項は、再委託先が子会社である場合も、同様に求めるべきことを明記すること。 ③ 個人情報の複製等の制限に関する事項 ④ 個人情報の安全管理措置に関する事項 ⑤ 個人情報の漏えい等の事案の発生時における対応に関する事項 ⑥ 委託終了時における個人情報の消去及び媒体の返却に関する事項 ⑦ 法令及び契約に違反した場合における契約解除、損害賠償責任その他必要な事項 ⑧ 契約内容の遵守状況についての定期的報告に関する事項及び委託先における委託された個人情報の取扱状況を把握するための監査等に関する事項（再委託先の監査等に関する事項を含む。）	個人情報取扱特記事項 契約書本文	（秘密の保持） 第２ 受注者は、この契約による事務に関して知り得た個人情報を他人に知らせ、又は不当な目的に使用してはならない。この契約が終了し、又は解除された後においても同様とする。 （漏えい、滅失及びき損の防止） 第４ 受注者は、この契約による事務に関して知り得た個人情報について、漏えい、滅失及びき損の防止その他個人情報の適切な管理のために必要な措置を講じなければならない。 （事務従事者への通知） 第５ 受注者は、この契約による事務に従事している者に対し、在職中及び退職後においても当該契約による事務に関して知り得た個人情報を他人に知らせ、又は不当な目的に使用してはならないことなど、個人情報の保護に必要な事項を周知するものとする。 （複写又は複製の禁止） 第７ 受注者は、この契約による事務を処理するために発注者から引き渡された個人情報が記録された資料等を複写し、又は複製してはならない。ただし、発注者の指示に基づく場合は、この限りでない。 （再委託等の禁止） 第９ 受注者は、この契約による事務を処理するための個人情報を自ら取り扱うものとし、当該事務を他に委託し、又は請け負わせてはならない。 ただし、書面により発注者の承諾を得たときは、この限りでない。 （資料等の返還） 第１０ 受注者は、この契約による事務を処理するために、発注者から提供を受け、又は受注者自らが収集し、若しくは作成した個人情報を記録した資料等は、この契約の完了後直ちに発注者に返還し、又は引き渡すものとする。ただし、発注者が別に指示したときは当該方法によるものとする。 （調査） 第１１ 発注者は、受注者がこの契約による事務を行うにあたり取り扱っている個人情報の状況について、随時調査することができる。 （事故発生時における報告） 第１２ 受注者は、個人情報の漏えい、滅失、き損、改ざん等の事故が生じ、又は生じるおそれのあることを知ったときは、漏えい、滅失、き損、改ざん等のあった個人情報の項目、内容、数量、事故の発生場所、発生状況等を詳細に記載した書面をもって速やかに発注者に報告し、発注者の指示に従うものとする。 【契約書本文】 （発注者の解除権） 第８条　発注者は、受注者が次の各号のいずれかに該当するときは、この契約を解除することができる。 (3) 前２号に掲げる場合のほか、この契約に違反し、その違反によりこの契約の目的を達成することができないと認められるとき。
			(2)	保有個人情報の取扱いに係る業務を外部に委託する場合には、取扱いを委託する個人情報の範囲は、委託する業務内容に照らして必要最小限でなければならない。	委託に当たっての留意事項 第３（３）	委託先に提供する個人情報は、委託に係る事務の目的の範囲内で必要最小限のものとすること。
			(3)	保有個人情報の取扱いに係る業務を外部に委託する場合には、委託する業務に係る保有個人情報の秘匿性等その内容やその量等に応じて、作業の管理体制及び実施体制や個人情報の管理の状況について、少なくとも年1回以上、原則として実地検査により確認する。	規程に直接規定（第２１条第２項）	
			(4)	委託先において、保有個人情報の取扱いに係る業務が再委託される場合には、委託先に上記（1）の措置を講じさせるとともに、再委託される業務に係る保有個人情報の秘匿性等その内容に応じて、委託先を通じて又は委託元自らが上記（3）の措置を実施する。保有個人情報の取扱いに係る業務について再委託先が再々委託を行う場合以降も同様とする。	規程に直接規定（第２１条第３項）	
			(5)	保有個人情報の取扱いに係る業務を派遣労働者によって行わせる場合には、労働者派遣契約書に秘密保持義務等個人情報の取扱いに関する事項を明記する。	規程に直接規定（第２１条第４項）	
		その他	(6)	保有個人情報を提供し、又は業務委託する場合には、漏えい等による被害発生のリスクを低減する観点から、提供先の利用目的、委託する業務の内容、保有個人情報の秘匿性等その内容などを考慮し、必要に応じ、特定の個人を識別することができる記載の全部又は一部を削除し、又は別の記号等に置き換える等の措置を講ずる。	規程に直接規定（第２２条）	