資料３－２

平成２０年度住基ネット関連セキュリティ対策の方向性

Ⅰ－１　市町村（住基ネット）

（１）これまでの取組

〇チェックリストによる自己点検
- 全ての市区町村において、セキュリティ対策の自己点検及び必要な対策の見直し等を実施。
- 特に、毎年いくつかの項目を、重要点検項目として選定し、全ての市区町村において原則３点満点を達成すること、当該年度以前の重要点検項目についても、引き続き、３点満点を維持することを目標として、各都道府県、総務省及び指定情報処理機関において、技術的助言、指導を実施。
- チェックリストの自己点検の結果の状況について、住基ネット調査委員会に説明。

〇システム運営監査
- 監査法人によるシステム監査を毎年度100団体程度実施。
- 平成19年度においては、都道府県による立会等を実施。

〇セキュリティ研修
- 毎年度、全市区町村の住基ネット担当者を対象としたセキュリティ研修会（都道府県単位で開催）において、住民基本台帳ネットワークシステム等のセキュリティ対策について研修を実施。

（２）平成20年度の取組の方向性

〇平成20年度においても、チェックリストによる自己点検、システム運営監査、セキュリティ研修等の取組により、引き続き、セキュリティ水準の維持、向上に努めることとするが、セキュリティ対策が形式に流されないようにするため、外部監査等における都道府県の役割を強化した以下のような取組を行ってはどうか。

・監査対象市町村の選定にあたっては、希望する市区町村だけでなく、都道府県選定市区町村も対象とする。
・外部監査時には、都道府県は原則として立ち会い、監査の実施状況を把握。
・都道府県は、市区町村からの監査状況の報告を受けることとし、市区町村に対して必要な措置又は改善計画の作成等を行うよう指導。
・都道府県は、定期的に、上記の進捗をチェックし、改善状況を確認する。
・外部監査を行っていない市町村に対しても、都道府県による実地調査等の取組を行う。
・外部監査の立会や実地調査については、都道府県の情報担当課の協力も得ながら行う。
・以上のサイクルを回していくことにより実質的かつ継続的にセキュリティ水準の向上を促進する。
・チェックリストの自己点検の結果の状況だけでなく、システム運営監査の状況についても、住基ネット調査委員会に説明し、翌年度のセキュリティ対策に反映。

〇また、平成２０年度の重要点検項目については、近年、住基ネットに関わるものではないが、セキュリティ事故が発生している主な要因として、委託先からの情報流出が挙げられることから、住基ネットにおいても委託先の管理を徹底する必要があることから、「委託先の管理」に関する項目を重要点検項目に選定し、点検を実施することとしてはどうか。
（大分類　「3.システムの管理」　　中分類　「3.8外部委託」参照）

Ⅰ－２　市町村（既存住基）

（１）これまでの取組

○技術的基準の改正及び周知

・「住民基本台帳に係る電算処理の委託等に関する検討会」の報告書（平成１９年１２月）で提言された実効性のある対策（指定場所での処理、承認を受けないデータ持ち出しの禁止、データの暗号化処理、承認を受けないデータの複製・複写の禁止、処理作業後のデータの返還・廃棄、承認を受けない再委託の禁止、日々（一定期間ごと）の処理記録の提出）等を盛り込んだ「住民票に係る磁気ディスクへの記録、その利用並びに磁気ディスク及びこれに関連する施設又は設備の管理の方法に関する技術的基準の一部を改正する件（平成２０年総務省告示第５３号）」を本年２月６日に公布し、市町村に周知。

（２）平成20年度の取組の方向性

○改正された技術的基準の改正内容が遵守され、セキュリティの維持向上を図るため、以下のような取組を行うこととしてはどうか。

・技術的基準の改正内容への対応状況について、市町村に対するフォローアップ調査等を実施。

・住基ネットと同様に、セキュリティ対策の状況を市区町村が自ら点検し、必要な対策の見直し等を行い、セキュリティの維持向上を図るための自己点検表を市町村に提示することを検討。

・技術的基準の改正内容による対応のほか、市町村の個人情報保護条例等に基づく独自の対応など、市町村がセキュリティ対策のために講じている措置について、優良事例等を収集し、市町村に配布するなど、市町村のセキュリティ対策に資するような方策を検討。

Ⅱ　都道府県

（１）これまでの取組

○チェックリスト
・各道府県に対しても、チェックリスト（市区町村版）を参考に、都道府県の業務に合わせて、チェックリスト（都道府県版）を作成し、配布（都道府県によっては、独自のチェックリストによる自己点検を行っている団体もあることも踏まえ、点検結果の報告については求めていない）。

○セキュリティ研修
・毎年度、全都道府県の住基ネット担当者を対象とした全国住民基本台帳ネットワークシステム担当者説明会において、住民基本台帳ネットワークシステム等のセキュリティ対策について研修を実施。
・このほか、都道府県では、住基ネット事務関係職員を対象としたセキュリティ研修会を独自で実施。

（２）平成20年度の取組の方向性

○住基ネット全体の統一的なセキュリティ水準の確保のためには、都道府県においてもチェックリスト又はチェックリストと同等なものによる自己点検を行い、必要な対策を行う。

○市町村と同様に、セキュリティ確保のために重要な項目を選定し、総務省及び指定情報処理機関において、助言等を実施。重要点検項目については、人的側面から見た住基ネットのセキュリティ対策を確認するため、昨年度及び今年度の市町村の重要点検項目も踏まえ、「重要機能室及びそれに準ずる室の管理」、「操作者識別カード及び操作履歴の管理」、「磁気ディスクの管理」及び「委託先の管理」としてはどうか。

○市町村と同様のシステム運営監査の実施については、都道府県によってはすでに外部監査を独自に行っているところもあることから、都道府県の意見も聴きながら、今後の対応を検討。

Ⅲ　国の行政機関等

（１）これまでの取組

○チェックリスト（国の行政機関等版）による自己点検
　・国の行政機関等の担当者向け情報セキュリティ研修会において、チェックリスト（国の行政機関等版）を配付し、地方自治情報センターへの自己点検結果の報告を依頼。
○セキュリティ研修会
　・毎年度、国の行政機関等の住基ネット担当者を対象としたセキュリティ研修会において、住民基本台帳ネットワークシステム等のセキュリティ対策について研修を実施。

（２）平成20年度の取組の方向性

○今年度と同様、チェックリストによる国の行政機関等の自己点検を行い、その結果について地方自治情報センターに報告。地方自治情報センター等では、更に正確なセキュリティ対策の実施状況が把握できるように、国の行政機関等の中から数機関を選定し、個別ヒアリング又は訪問等を実施。
○地方自治情報センターでは、自己点検結果を確認し、点検結果に対する改善点を提示し、改善するよう国の行政機関等に依頼。
○国の行政機関等の情報提供を受けている原局だけでなく、省の情報セキュリティを統括している担当課にも、住基ネットのセキュリティ水準が保たれているかチェックするよう要請を検討。
○自己点検の結果の把握、個別ヒアリング等を通じて、総務省及び地方自治情報センターは、今後の自己点検の取組（チェックリストの改良等）に反映。

○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

大分類	中分類	小分類	管理目標			回答					
				小項目番号	管理状況	設問番号	回答番号				
1.体制、規程等の整備	1.1体制の整備	1.1.1セキュリティの責任体制の確立	1		住基ネットのセキュリティを確保するための責任体制及び連絡体制を確立している						
				1-1	セキュリティ統括責任者を任命している	6	－	1	2	3	
				1-2	システム管理者を任命している	7	－	1	2	3	
				1-3	アクセス管理責任者を任命している	8	－	1	2	3	
				1-4	本人確認情報管理責任者を任命している	9	－	1	2	3	
				1-5	セキュリティ責任者を任命している	10	－	1	2	3	
				1-6	セキュリティ会議を開催している	11	－	1	2	3	
	1.2規程等の整備	1.2.1規程の整備	2		住基ネットのセキュリティを確保するための規程を整備・運用している						
				2-1	セキュリティ組織規程を作成・運用している	12	－	1	2	3	
				2-2	アクセス管理規程を作成・運用している	13	－	1	2	3	
				2-3	情報資産管理規程を作成・運用している	14	－	1	2	3	
				2-4	委託管理規程を作成・運用している	15	－	1	2	3	
		1.2.2ドキュメントの整備	3		住基ネットのセキュリティを確保するための要領・手順書等を整備・運用している						
				3-1	要領・手順書等を整備・運用している	16	－	1	2	3	
	1.3教育、研修等	1.3.1教育及び研修	4		住基ネットの教育及び研修に関する計画を策定・実施している						
				4-1	住基ネットの教育及び研修に関する計画を策定・実施している	17	－	1	2	3	
	1.4緊急時体制	1.4.1緊急時における事務処理体制	5		緊急時の事務処理体制を確立している						
				5-1	緊急時対応計画書を策定している	18	－	1	2	3	
				5-2	庁内の緊急時連絡網を整備している	19	－	1	2	3	
				5-3	庁外の関係機関との緊急時連絡網を整備している	20	－	1	2	3	
2.環境及び設備	2.1重要機能室等の管理	2.1.1コンピュータ機器等の設置場所	6		重要機能室のセキュリティを確保している						
				6-1	重要機能室のセキュリティを確保している	21	0	1	2	3	
		2.1.2重要機能室の管理(設問番号21において「0」以外に回答した場合)	7		重要機能室の入退室管理を適切に行っている						
				7-1	入退室管理規程を作成・運用している	22	0	1	2	3	
				7-2	鍵又は入退室カードの管理責任者を定めている	23	0	1	2	3	
				7-3	鍵又は入退室カード等により、入室者が正当な権限を保有していることを確認している	24	0	1	2	3	
				7-4	物品の搬出入は職員が内容を確認している	25	0	1	2	3	
				7-5	訪問者について、入退室を適正に管理している	26	0	1	2	3	
		2.1.3電子計算機の設置された部屋の管理(設問番号21において「0」に回答した場合)	8		電子計算機の設置された部屋のセキュリティを確保している						
				8-1	電子計算機及び電気通信関係装置を厳重に固定し、磁気ディスク及びドキュメントを専用保管庫に施錠保管している	27	0	1	2	3	
				8-2	職員が不在となる時に施錠している	28	0	1	2	3	
				8-3	訪問者について、入退室を適正に管理している	29	0	1	2	3	

大分類	中分類	小分類	管理目標			回答				
				小項目番号	管理状況	設問番号	回答番号			
		2.1.4事務室(窓口業務等を行う室)の管理	9		CS端末の設置された部屋のセキュリティを確保している					
				9-1	職員が不在になる時に、ドキュメントを施錠保管する等の必要な手続きを行っている	30	－	1	2	3
				9-2	訪問者について、入退室を適正に管理している	31	－	1	2	3
3.システムの管理	3.1住基ネットの管理	3.1.1ユーザIDの管理	10		オペレーティングシステム（Windows)のユーザIDを適切に管理している					
				10-1	ユーザIDの所有者(利用者)を明確にしている	32	－	1	2	3
				10-2	ユーザIDに付与された権限を明確にしている	33	－	1	2	3
		3.1.2パスワードの管理	11		オペレーティングシステム（Windows)のパスワードが容易に推測されることのないような措置を講じている					
				11-1	パスワードを定期的に変更している	34	－	1	2	3
				11-2	パスワードをマニュアルなどに記載していない	35	－	1	2	3
				11-3	パスワードの最低桁数を定めている	36	－	1	2	3
				11-4	パスワードは利用者が設定している	37	－	1	2	3
				11-5	パスワードに英数字又は記号を組み合わせるよう制限している	38	－	1	2	3
		3.1.3オペレーティングシステムの不正使用防止	12		オペレーティングシステム（Windows)への不正なアクセスを予防している					
				12-1	オペレーティングシステムに対するログオン失敗履歴を記録している	39	－	1	2	3
				12-2	同じユーザIDで複数回パスワードの入力を間違えた場合、ロックアウト(無効化)するように設定している	40	－	1	2	3
				12-3	フォルダの共有を行っていない	41	－	1	2	3
				12-4	不要なプログラム(サービス)を起動していない	42	－	1	2	3
		3.1.4未許可ソフトウェアの稼働禁止	13		許可されていないソフトウェアの導入を禁止している					
				13-1	標準的にインストールされるソフトウェアを定めている	43	－	1	2	3
				13-2	追加的なソフトウェア導入ができないような設定としている	44	－	1	2	3
		3.1.5不正プログラムの混入防止	14		住基ネットに対しウィルス等の不正プログラムの混入防止等の対策を講じている					
				14-1	ウィルスが発見された場合の報告、対処手続を定めている	45	－	1	2	3
				14-2	CS端末からインターネットに接続できないように制限している	46	－	1	2	3
		3.1.6住民基本台帳ネットワークに関係する機器（市区町村整備部分）のセキュリティ設定の管理	15		住基ネットに関する機器について、そのネットワーク設定を管理している					
				15-1	システム担当職員がネットワーク設定の内容を把握している	47	－	1	2	3
				15-2	委託業者が実施したネットワーク設定内容が適切であるか職員が確認している	48	－	1	2	3
				15-3	セキュリティ情報を収集し、分析を行い、必要な措置を講じている	49	－	1	2	3
	3.2端末機操作の管理	3.2.1端末機の利用者管理	16		操作者識別カードを適切に管理している					
				16-1	個人ごとに貸与し、人事異動に際しては回収している	50	－	1	2	3
				16-2	他者への貸与、目的以外の利用等を禁止している	51	－	1	2	3
				16-3	紛失・盗難時は直ちに報告させることとしている	52	－	1	2	3
				16-4	紛失・盗難時は速やかに失効手続きをとることとしている	53	－	1	2	3
			17		操作者識別カードのパスワードが容易に推測されることのないような措置を講じている					
				17-1	パスワードを定期的に変更している	54	－	1	2	3
				17-2	パスワードをマニュアルなどに記載していない	55	－	1	2	3
				17-3	パスワードの最低桁数を定めている	56	－	1	2	3

大分類	中分類	小分類	管理目標		小項目番号	管理状況	回答 設問番号	回答番号			
					17-4	パスワードは利用者が設定している	57	－	1	2	3
					17-5	パスワードに、英数字を組み合わせるよう制限している	58	－	1	2	3
			18	不正アクセスを分析するために、CSにおいてアプリケーションの操作履歴の記録を取得、保管している							
					18-1	操作履歴をチェックしている	59	－	1	2	3
					18-2	操作履歴の保管期間を定めている	60	－	1	2	3
	3.3構成機器及び関連設備等の管理	3.3.1管理方法の明確化	19	住基ネットの構成機器の管理方法を明確にしている							
					19-1	ネットワーク構成図を整備し、変更があった際には最新の状態に更新している	61	－	1	2	3
					19-2	機器等を接続する場合、システム管理者の承認を得ている	62	－	1	2	3
					19-3	構成機器及びソフトウェアの管理台帳を作成している	63	－	1	2	3
		3.3.2保守	20	住基ネットの構成機器及び関連設備に対して、定期に又は臨時に保守を行っている							
					20-1	保守内容及び点検項目を明確にしている	64	－	1	2	3
					20-2	重要機器に対する保守を行う場合は職員が立ち合っている	65	－	1	2	3
		3.3.3ネットワークの管理	21	CSが設置されたセグメントへの電子計算機等の接続を制限している							
					21-1	電子計算機等の物理的配線状況を管理している	66	－	1	2	3
					21-2	不要なハブ等の電気通信関係装置は設置していない	67	－	1	2	3
			22	住基ネットに係る電気通信関係装置(ルータ、ハブ、ファイアウォール)に対して権限のある者以外による操作を防止するための措置を講じている							
					22-1	電気通信関係装置へログイン、操作するためのユーザID、パスワードを適切に管理している	68	－	1	2	3
					22-2	電気通信関係装置を通信機器ラック等に設置して施錠する等適切に管理している	69	－	1	2	3
					22-3	通信機器ラック等の鍵を適切に管理している	70	－	1	2	3
	3.4磁気ディスクの管理	3.4.1保管場所、持ち出しと返却の確認等	23	磁気ディスクを適切に管理している							
					23-1	盗難防止のため、専用保管庫により施錠保管している	71	－	1	2	3
					23-2	使用、複写、消去及び廃棄を適切に行っている	72	－	1	2	3
					23-3	磁気ディスクの受渡し毎に保管状況の確認を行っている	73	－	1	2	3
					23-4	取扱担当者を定めている	74	－	1	2	3
					23-5	記号等により他の磁気ディスクと識別している	75	－	1	2	3
		3.4.2廃棄	24	磁気ディスクを適切に廃棄している							
					24-1	廃棄する際には、専用のソフトウェアによる消去又は媒体の物理的破壊等を行っている	76	－	1	2	3
	3.5データ、プログラム、ドキュメントの管理	3.5.1保管場所、持ち出しと返却の確認、廃棄等	25	設計書等のドキュメントを適切に管理している							
					25-1	盗難防止のため、施錠保管している	77	－	1	2	3
					25-2	使用、複写、消去及び廃棄を適切に行っている	78	－	1	2	3
					25-3	取扱担当者が決められている	79	－	1	2	3
					25-4	廃棄する際には、裁断・溶解等を行っている	80	－	1	2	3
	3.6本人確認情報の管理	3.6.1本人確認情報の取り扱い	26	本人確認情報を適切に管理している							
					26-1	業務上必要のない検索、抽出を行わない	81	－	1	2	3
					26-2	スクリーンセーバ等を利用して、長時間にわたり本人確認情報を表示させない	82	－	1	2	3
					26-3	CS端末のディスプレイを、来庁者から見えない位置に置いている	83	－	1	2	3

大分類	中分類	小分類	管理目標				回答					
					小項目番号	管理状況	設問番号	回答番号				
					26-4	本人確認情報が表示された画面のハードコピーを必要以上に取らない	84	－	1	2	3	
					26-5	本人確認情報の入力、削除及び訂正を正確に行っている	85	－	1	2	3	
					26-6	大量のデータ出力に際しては、事前に管理責任者の承認を得ている	86	－	1	2	3	
		3.6.2本人確認情報が記載された帳票の管理	27	帳票の受渡し、在庫管理及び廃棄の方法を定めている								
					27-1	帳票の管理対象を明確にしている	87	－	1	2	3	
					27-2	盗難防止のため、専用保管庫により施錠保管している	88	－	1	2	3	
					27-3	廃棄する際には、裁断・溶解等を行っている	89	－	1	2	3	
			28	帳票の出力に関する管理を適切に行っている								
					28-1	帳票を出力する装置は、出力を第三者に盗取されないような場所に設置している	90	－	1	2	3	
					28-2	出力した帳票を出力装置に長時間放置していない	91	－	1	2	3	
	3.7障害時の対応	3.7.1早期回復のための代替機能	29	異常発見時の対応を適切に行うこととしている								
					29-1	障害を発見したときに、システム管理者に報告を行うこととしている	92	－	1	2	3	
					29-2	不正アクセスを発見したときに、システム管理者に報告を行う事としている	93	－	1	2	3	
			30	緊急時に備えてデータ及びシステムのバックアップを行っている								
					30-1	バックアップを定期的に行っている	94	－	1	2	3	
					30-2	バックアップ媒体を適切に保管している	95	－	1	2	3	
			31	障害から早期に回復するための体制、手順を整備している								
					31-1	障害からの回復をおこなう責任者及び担当者を定めている	96	－	1	2	3	
					31-2	回復する手続を定めている	97	－	1	2	3	
	3.8外部委託	3.8.1委託先の選定	32	委託先を適切に選定している								
					32-1	委託先の社会的信用と能力を確認している	98	0	1	2	3	
		3.8.2委託先の監督	33	委託先に対して作業不備及び不正行為を防止し、データを保護するための措置を講じさせている								
					33-1	委託業務の範囲を明確にしている	99	0	1	2	3	
					33-2	委託先にセキュリティ対策を実施させている	100	0	1	2	3	
					33-3	作業者を限定するために、委託作業者の名簿を提出させている	101	0	1	2	3	
		3.8.3再委託の制限	34	再委託の制限を行っている								
					34-1	再委託を制限している	102	0	1	2	3	
					34-2	再委託時には事前申請及び承認を行っている	103	0	1	2	3	
					34-3	再委託先及び再委託業務の範囲を明確にさせている	104	0	1	2	3	
		3.8.4委託先事業者等との分担範囲等の明確化	35	複数の事業者に委託する場合、作業範囲及び責任範囲を明確にしている								
					35-1	作業範囲及び責任範囲を明確にしている	105	0	1	2	3	
					35-2	事業者間の情報交換を行わせている	106	0	1	2	3	
		3.8.5要員派遣を受ける場合	36	派遣要員、非常勤職員、臨時職員等による情報漏えい対策を講じている								
					36-1	採用基準を定めている	107	0	1	2	3	
					36-2	セキュリティに関する教育及び研修を行っている	108	0	1	2	3	

大分類	中分類	小分類	管理目標			回答				
				小項目番号	管理状況	設問番号	回答番号			
4.既設ネットワークとの接続	4.1既設ネットワークとの接続条件	4.1.1ファイアウォールによる通信制御	37		既設ネットワークからCSへのアクセスを制限している					
				37-1	既設ネットワークとCSを直接接続しない	109	－	1	2	3
				37-2	市町村設置ファイアウォールを適切に運用保守している	110	0	1	2	3
				37-3	市町村設置ファイアウォールの設定において既設ネットワークとCSの通信を必要最小限のサービスに制限している	111	0	1	2	3
				37-4	市町村設置ファイアウォールのアクセスログを解析している	112	0	1	2	3
		4.1.2体制の整備	38		既設ネットワークのセキュリティを確保するための責任体制を確立している					
				38-1	既設ネットワークのセキュリティ統括責任者を任命している	113	0	1	2	3
				38-2	既設ネットワークのシステム管理者を任命している	114	0	1	2	3
				38-3	セキュリティ責任者を任命している	115	0	1	2	3
		4.1.3既設ネットワークと外部との接続	39		既設ネットワークから外部ネットワークへの接続及び運用に関する業務を総括的に管理している					
				39-1	外部ネットワークへ接続するための手続、方法等を定めている	116	0	1	2	3
			40		外部からの不正なアクセスを防止している					
				40-1	インターネットへの接続を行っていない	117	0	1	2	3
				40-2	インターネットに接続する場合は、ファイアウォールを設置して厳重な通信制御を行っている	118	0	1	2	3
				40-3	既設ネットワークに公開サーバを設置する場合は、DMZに設置している	119	0	1	2	3
				40-4	公開サーバ等には最新のパッチを当てている	120	0	1	2	3
				40-5	既設ネットワークに対する侵入検知の仕組みを有している	121	0	1	2	3
				40-6	遠隔保守を行う場合は、適切に行っている	122	0	1	2	3
				40-7	遠隔保守を行う際、ダイアルアップ接続は、コールバック、発信番号確認などを行っている	123	0	1	2	3
		4.1.4既設ネットワークにおける機器の接続	41		既設ネットワークへの機器の接続を適切に管理している					
				41-1	機器を接続する場合、システム管理者の承認を得ている	124	0	1	2	3
				41-2	ネットワーク構成図を整備し、変更があった際には最新の状態に更新している	125	0	1	2	3
			42		既設ネットワークに接続される端末の接続状況を適切に管理している					
				42-1	端末管理者を定めている	126	0	1	2	3
				42-2	各端末の管理台帳を整備している	127	0	1	2	3
				42-3	標準的にインストールされるソフトウェアを定めている	128	0	1	2	3
5.住民基本台帳カードの管理	5.1住民基本台帳カードの管理	5.1.1住民基本台帳カードの管理	43		住民基本台帳カードを適切に管理している					
				43-1	住民基本台帳カード（未使用、交付前を含む）を適切に保管している	129	－	1	2	3
				43-2	住民基本台帳カード（返却後、印刷ミス等）について適切に廃棄している	130	－	1	2	3
				43-3	住民から受領した顔写真について、適切に廃棄・管理している	131	－	1	2	3