

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票 による点検結果（平成15年5月12日）

- 平成15年1・2月に、市区町村は標記調査票に基づいてセキュリティ対策の自己点検を実施。調査票を指定情報処理機関である（財）地方自治情報センターが回収、集計し、総務省ともに分析。
- 全体を通してみると、全国の9割程度の市区町村においては、体制・規定の整備や必要な管理がなされているが、1割程度の市区町村においては必ずしも十分な対応がなされていない面がある。

3 2 1 5 市区町村の点検結果の総平均値 2 . 4 8 点（3点満点）

- あわせて108市区町村において、監査法人によるシステム運営監査を実施
- 市区町村は、この点検結果を踏まえ、自主的にセキュリティ対策の強化を実施。
総務省としても、あらためて都道府県を通じて市区町村に対し技術指導を行い、7月上旬を目途にセキュリティ対策の実施状況について報告を求め、第2次稼働までに適切な管理運営の徹底を図る予定。

住基ネットのセキュリティ体制・規程等については概ね整いつつあるが、1割程度の団体が未整備。

- 住基ネットのセキュリティを確保するための責任体制の早期確立（特に、CIO＝セキュリティ統括責任者の早期任命）とセキュリティ関係規程・計画の早期作成を要請。
なお、本年5月・6月に改めて47都道府県でセキュリティ研修会を実施。

重要機能室を設置している団体（9割程度）については、概ねその適切な管理がなされているが、1割程度の団体で管理体制の強化が必要。

また、重要機能室を設置していない団体（1割程度）についても、概ねコミュニケーションサーバ等の適切な管理がなされているが、ごく一部の団体で管理体制の強化が必要。

- 重要機能室における入退室管理の徹底を要請（鍵等の管理状況の再点検等）。
また、重要機能室を設置できない市町村の場合、コミュニケーションサーバ等の盗難防止対策の徹底を要請（電子計算機等の厳重な固定、職員不在時の施錠、名札等を利用した不審者侵入時の早期発見等）。

OS管理については、1割程度から5割程度の団体で管理体制の強化が必要な項目（特に、パスワードの有効期限の設定や最低桁数の制限、ログオン失敗履歴の記録等）が存在。

- OSのユーザIDの適切な管理、パスワードが容易に推測されることのない措置等の実施を要請。

操作者識別カードについては、概ねその適切な管理がなされているが、一部の項目を除き、1割程度の団体で管理体制の強化が必要。

- 操作者識別カードの適切な管理の徹底を要請（パスワードの定期的な変更、個人ごとの貸与の徹底等）。

磁気ディスク、設計書等については、概ねその適切な管理がなされているが、一部の項目を除き、1割程度の

団体で管理体制の強化が必要。

- 磁気ディスク、設計書等の適切な管理、盗難防止対策等の実施の徹底を要請。
特に、バックアップ媒体については、保管場所の盗難防止対策、移送時の盗難防止措置等の実施について再度、徹底を要請

本人確認情報等（本人確認情報等が記載されている帳票を含む）については、概ねその適切な管理がなされているが、1割程度の団体で管理体制の強化が必要。

- 本人確認情報等の適切な管理の徹底を要請（市町村の実情に応じた本人確認情報等の取扱ルールの策定等）。

委託先については、概ねその適切な管理がなされているが、一部の項目を除き、1割程度の団体で管理体制の強化が必要。

- 委託先に対する適切な管理の徹底を要請（委託先からのセキュリティ報告の聴取、再委託制限の実施等）

既設ネットワークとコミュニケーションサーバ間のファイアウォール及び既設ネットワークとインターネットとの接続については、概ねその適切な管理がなされているが、2割程度の団体でアクセスログの管理体制の整備が必要。

- ファイアウォールの適切な管理の徹底を要請（アクセスログを適切に管理し、異常なアクセスの有無をチェックする等）
また、既設ネットワークからインターネットに接続する場合、外部からの不正アクセスを防止するための措置の徹底を要請。

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票 による点検結果集計表

集計団体数 3 2 1 5 団体

回答 3	運用している（定められた手続が関係する職員に周知され、適切に運用されている。）
回答 2	整備している（質問項目を実現する手続が文書等で定められている。）
回答 1	整備していない（規程等を常備していない。質問項目について文書等で定められていない。）

回答 3・2・1 以外に回答 0（関係するシステムが存在しない等、質問項目に該当しない。）とした団体もある。

	調 査 項 目	平均値	回答 3	回答 2	回答 1	備 考
1 体制・規程等の整備	1-1 セキュリティ統括責任者を任命している	2.527	57.1 %	37.6 %	4.7 %	
	1-2 システム管理者を任命している	2.538	57.8 %	37.3 %	4.3 %	
	1-3 本人確認情報管理責任者を任命している	2.346	49.3 %	33.2 %	15.4 %	
	1-4 セキュリティ責任者を任命している	2.498	56.2 %	36.0 %	6.9 %	
	1-5 セキュリティ会議を開催している	2.091	24.6%	55.9 %	15.8 %	
	2-1 セキュリティ組織規程を作成している	2.529	63.3 %	25.3 %	10.8 %	
	2-2 アクセス管理規程を作成している	2.451	59.5 %	24.2 %	15.0 %	
	2-3 情報資産管理規程を作成している	2.409	57.3 %	23.6 %	17.2 %	
	2-4 委託管理規程を作成している	2.299	49.9 %	23.4 %	21.6 %	
	3-1 配布された操作手引書を常時参照できるよう管理している	2.713	74.3 %	21.9 %	3.3 %	
	4-1 担当者に操作及びセキュリティ対策等の研修を受講させている	2.524	62.6 %	23.3 %	11.5 %	
	5-1 緊急時対応計画を整備している	2.406	57.7 %	23.4 %	17.7 %	
	5-2 庁内の緊急時連絡網を整備している	2.457	59.8 %	24.8 %	14.5 %	
	5-3 都道府県・市町村間の連絡網に登録している	2.636	70.5 %	20.4 %	7.8 %	

	調 査 項 目	平均値	回答 3	回答 2	回答 1	備 考
2 環境及び設備	6-1 電子計算機及び磁気ディスク等を専用の部屋（重要機能室）に設置している	2.799	76.1 %	7.8 %	5.1 %	重要機能室「有り」の場合に回答
	7-1 入退室管理規程を作成している	2.453	53.8 %	17.9 %	14.7 %	
	7-2 鍵又はカードの管理責任者を定めている	2.641	62.4 %	18.0 %	6.6 %	
	7-3 鍵又は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	2.558	58.1 %	18.8 %	9.8 %	
	7-4 物品の搬出入は職員が内容確認している	2.618	61.6 %	17.8 %	7.7 %	
	7-5 入退室者を記録している	2.340	48.1 %	18.2 %	19.1 %	
	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	2.732	7.8 %	1.4 %	0.6 %	重要機能室「無し」の場合に回答
	8-2 職員が不在となる時に施錠している	2.636	6.8 %	1.8 %	0.8 %	
	8-3 入室可能な者を限定している	2.444	5.1 %	2.6 %	1.2 %	
	9-1 端末機等を設置する事務室において、職員が不在となる時に施錠している	2.356	54.9 %	13.3 %	22.6 %	
	9-2 事務室への入退室管理を行っている	2.163	43.3 %	19.4 %	28.5 %	
3 システムの管理	10-1 OSのユーザIDの管理者を決めている	2.420	61.1 %	12.6 %	21.2 %	
	10-2 ユーザIDの所有者を明確にしている	2.395	60.5 %	12.2 %	22.8 %	
	10-3 ユーザIDに付与された権限が明確である	2.454	63.7 %	11.9 %	20.2 %	
	10-4 不要なユーザIDは登録していない	2.675	75.6 %	9.0 %	11.1 %	
	11-1 OSのパスワードに有効期限を設定している	1.602	17.4 %	16.4 %	51.4 %	
	11-2 OSのパスワードをマニュアルなどに記載していない	2.629	69.7 %	17.0 %	9.3 %	
	11-3 容易に推測されるパスワードを使用していない	2.486	57.5 %	27.4 %	10.9 %	
	11-4 OSのパスワードは利用者が設定している	2.206	46.8 %	19.0 %	27.6 %	
	11-5 OSのパスワードの最低桁数等の制限をしている	2.056	38.9 %	20.1 %	33.7 %	

	調 査 項 目	平均値	回答 3	回答 2	回答 1	備 考
3 シ ス テ ム の 管 理	12-1 OS に対するログオン失敗履歴を記録している	1.597	18.9 %	18.0 %	56.6 %	
	12-2 複数回パスワード入力を間違えた場合、ロックアウトするように設定している	1.785	28.7 %	4.9 %	45.8 %	
	12-3 フォルダの共有設定を行っていない	2.806	85.8 %	6.1 %	6.5 %	
	12-4 不要なプログラムを起動していない	2.856	88.3 %	6.0 %	4.0 %	
	13-1 標準的にインストールされるソフトを決めている	2.591	73.9 %	7.9 %	16.1 %	
	13-2 追加的なソフト導入ができない設定である	2.082	29.7 %	44.8 %	21.8 %	
	13-3 インストールされたソフトについて定期的に確認している	1.919	28.2 %	31.5 %	35.9 %	
	13-4 端末機でワープロ、表計算ソフトを使用していない	2.748	82.1 %	4.9 %	9.8 %	
	14-1 ウィルス発見時の対処手続を定めている	2.477	56.9 %	31.9 %	9.8 %	
	14-2 端末機からインターネットに接続できないよう制限している	2.880	87.9 %	7.0 %	2.3 %	
	15-1 担当職員がセキュリティ設定の内容を把握している	2.472	54.7 %	35.7 %	8.2 %	
	15-2 委託業者が行ったセキュリティに関する設定内容が適切か職員が確認している	2.434	52.5 %	35.4 %	10.0 %	
	15-3 住基ネットの市区町村整備部分の変更時にセキュリティの設定を見直している	2.376	47.3 %	31.9 %	12.8 %	
	15-4 セキュリティ対策に関する情報を収集し、分析を行い、必要な措置を講じている	2.339	48.4 %	33.4 %	15.4 %	
	16-1 操作者識別カードを個人ごとに貸与し、人事異動に際しては回収している	2.605	67.1 %	19.0 %	9.3 %	
	16-2 操作者識別カードの他者への貸与、目的以外の利用等を行っていない	2.720	76.9 %	16.0 %	5.8 %	
	16-3 操作者識別カードの紛失・盗難時は直ちに報告している	2.668	73.5 %	17.5 %	7.7 %	
	16-4 操作者識別カードの紛失・盗難時は速やかに失効手続をとっている	2.649	72.1 %	18.2 %	8.2 %	
	16-5 操作者識別カードが適正に利用されているか検査を行っている	2.297	50.9 %	23.5 %	22.2 %	
	17-1 操作者識別カードのパスワードに有効期限を設定している	1.791	24.4 %	20.4 %	42.8 %	
	17-2 操作者識別カードのパスワードをマニュアルなどに記載していない	2.709	75.1 %	17.4 %	5.5 %	

	調 査 項 目	平均値	回答 3	回答 2	回答 1	備 考
3 シ ス テ ム の 管 理	17-3 容易に推測されるパスワードを使用していない	2.577	62.7 %	29.4 %	6.1 %	
	17-4 操作者識別カードのパスワードは利用者が設定している	2.500	62.3 %	20.1 %	14.0 %	
	17-5 操作者識別カードのパスワードの最低桁数等の制限をしている	2.151	42.3 %	24.6 %	28.0 %	
	18-1 利用者の業務に必要な最低限の権限を付与している	2.730	77.7 %	13.4 %	6.4 %	
	18-2 担当業務の変更に伴い、利用者に付与された権限の見直しを定期的に行っている	2.566	65.4 %	16.3 %	12.3 %	
	19-1 アプリケーションの操作履歴をチェックしている	2.124	33.3 %	42.0 %	21.3 %	
	19-2 アプリケーションの操作履歴の保管期限を設定している	2.224	43.3 %	31.7 %	21.6 %	
	20-1 ネットワーク構成図を整備し、最新の状態に更新している	2.546	67.2 %	16.5 %	13.9 %	
	20-2 機器等を接続する場合、責任者に報告している	2.663	73.9 %	14.7 %	9.1 %	
	20-3 構成機器、ソフト等の台帳記録を作成している	2.199	49.1 %	17.3 %	29.9 %	
	20-4 台帳と現況が一致することを確認している	2.211	48.7 %	16.7 %	28.8 %	
	20-5 登録されていない機器等を使用していない	2.716	76.6 %	9.5 %	8.7 %	
	21-1 保守内容及び点検項目を明確にしている	2.720	78.3 %	13.5 %	7.1 %	
	21-2 保守実施内容の記録を保管している	2.717	77.5 %	14.4 %	6.7 %	
	22-1 重要機器の保守を行う場合、職員が立ち合っている	2.745	80.0 %	12.0 %	6.6 %	
	23-1 コミュニケーションサーバが存在する L A N の電気通信関係装置の物理的配線状況を管理している	2.724	77.4 %	13.5 %	6.7 %	
	23-2 余分なハブ等は設置していない	2.808	83.5 %	10.0 %	4.4 %	
	24-1 電気通信関係装置のユーザ名、パスワードを適切に管理している	2.626	71.4 %	17.2 %	9.8 %	
	24-2 電気通信関係装置をラック等に設置し施錠している	2.728	78.9 %	11.7 %	7.5 %	
	24-3 通信機器ラック等の鍵を適切に管理している	2.745	79.0 %	12.0 %	6.4 %	

	調 査 項 目	平均値	回答 3	回答 2	回答 1	備 考
3 シ ス テ ム の 管 理	25・1 磁気ディスクの保管場所は施錠している	2.781	80.7 %	10.5 %	5.3 %	
	25・2 定められた場所に保管し関係者に周知している	2.784	80.3 %	11.6 %	4.6 %	
	26・1 磁気ディスクの複写、廃棄等の記録を作成している	2.233	43.4 %	22.6 %	22.7 %	
	26・2 データの受渡しごとに保管状況を確認している	2.410	50.0 %	19.5 %	15.2 %	
	26・3 取扱担当者が決められている	2.590	64.3 %	16.3 %	10.5 %	
	26・4 記号等により他の磁気ディスクと識別している	2.551	62.6 %	13.9 %	13.2 %	
	27・1 磁気ディスクの廃棄時は専用ソフトによる物理的消去、媒体の破壊等を実施する	2.497	54.6 %	15.0 %	13.3 %	
	28・1 設計書等のドキュメントの保管場所を施錠している	2.463	58.5 %	20.3 %	15.1 %	
	28・2 設計書等のドキュメントを定められた場所に保管し関係者に周知している	2.592	64.9 %	20.8 %	8.9 %	
	29・1 ドキュメントの複写、廃棄等の記録を作成している	1.959	28.8 %	28.4 %	32.5 %	
	29・2 ドキュメントの取扱担当者が決められている	2.381	52.3 %	23.0 %	17.1 %	
	30・1 ドキュメントの廃棄時は裁断、溶解等を実施している	2.483	55.7 %	19.8 %	13.0 %	
	31・1 必要のない本人確認情報の検索を行っていない	2.519	64.4 %	20.3 %	13.5 %	
	31・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	2.576	71.6 %	10.0 %	15.6 %	
	31・3 ディスプレイを住民に見えない位置に設置している	2.828	86.0 %	7.3 %	4.8 %	
	31・4 画面のハードコピーをとっていない	2.454	60.2 %	20.6 %	16.1 %	
	31・5 本人確認情報の入力、訂正等の際に内容を確認している	2.501	53.6 %	24.3 %	9.7 %	
	31・6 大量データ出力の際に責任者の事前承認を得ている	2.631	47.3 %	11.2 %	6.4 %	
	32・1 帳票の管理対象を明確にしている	2.564	54.7 %	13.9 %	10.2 %	
	32・2 帳票を施錠のできる書庫等に保管している	2.599	55.7 %	12.6 %	9.2 %	
	32・3 帳票の廃棄時は焼却、溶解等を実施している	2.723	61.6 %	11.0 %	5.3 %	

	調 査 項 目	平均値	回答 3	回答 2	回答 1	備 考
3 シ ス テ ム の 管 理	33-1 帳票出力装置は、出力した帳票を第三者に盗取されないような場所に設置する	2.679	63.5 %	10.1 %	8.1 %	
	33-2 出力した帳票を出力装置に放置していない	2.761	65.5 %	9.0 %	5.0 %	
	34-1 障害発見時に責任者に報告を行っている	2.629	67.7 %	25.2 %	5.7 %	
	34-2 不正アクセス発見時に責任者に報告を行っている	2.638	68.5 %	24.0 %	5.8 %	
	35-1 バックアップを定期的に行っている	2.806	85.8 %	7.2 %	6.0 %	
	35-2 バックアップの実施記録簿を保管している	2.253	52.8 %	14.3 %	28.6 %	
	35-3 バックアップ媒体を別の場所に保管している	2.417	63.9 %	9.1 %	23.6 %	
	36-1 障害からの回復を行う責任者及び担当者が定められている	2.419	55.7 %	28.2 %	14.4 %	
	36-2 回復する手順が定められ、関係者に周知されている	2.319	49.9 %	29.2 %	18.7 %	
	37-1 委託先の社会的信用と能力を確認している	2.721	74.6 %	12.0 %	7.0 %	
	38-1 委託業務の範囲を明確に定めている	2.733	75.6 %	10.5 %	7.2 %	
	38-2 委託先にセキュリティ対策を実施させている	2.509	51.9 %	37.0 %	4.4 %	
	38-3 委託先から定期的にセキュリティ状況に関する報告を受けている	2.007	34.2 %	23.9 %	33.5 %	
	38-4 委託作業者の名簿を作成している	2.092	40.7 %	18.5 %	32.2 %	
	39-1 再委託を制限している	2.496	46.3 %	9.1 %	12.6 %	
	39-2 再委託時に事前申請及び承認を行っている	2.411	36.9 %	8.8 %	12.8 %	
	39-3 再委託先及び再委託業務を明確にしている	2.401	35.6 %	9.4 %	12.5 %	
	40-1 複数の事業者へ委託する場合、作業範囲及び責任範囲を文書化している	2.345	19.0 %	8.0 %	7.2 %	
	40-2 事業者間の情報交換を行っている	2.357	18.9 %	6.8 %	7.2 %	
	41-1 派遣要員、非常勤職員、臨時職員等に秘密保持の誓約を行わせている	2.468	22.0 %	9.5 %	4.9 %	
	41-2 セキュリティに関する指導・教育を行っている	2.414	20.2 %	10.5 %	5.3 %	

	調 査 項 目	平均値	回答 3	回答 2	回答 1	備 考
4 既設ネットワークとの接続	42-1 既設ネットワークとコミュニケーションサーバを物理的に分離している	2.443	28.4 %	3.1 %	10.0 %	
	42-2 ファイアウォールにより既設ネットワークとコミュニケーションサーバを分断	2.871	80.9 %	7.6 %	2.0 %	
	42-3 ファイアウォールの設定において既設ネットワークとコミュニケーションサーバの通信を必要最小限のサービスに制限している	2.853	80.5 %	5.4 %	3.9 %	
	42-4 ファイアウォールのアクセスログを保存している	2.374	52.8 %	22.3 %	18.0 %	
	42-5 ファイアウォールのアクセスログをチェックしている	2.122	35.5 %	32.9 %	24.2 %	
	43-1 既設ネットワーク運用に関する責任体制を明確にしている	2.605	71.0 %	10.9 %	13.3 %	
	43-2 既設ネットワークの管理者を定めている	2.601	70.4 %	11.8 %	13.1 %	
	43-3 セキュリティ管理者を任命している	2.465	63.6 %	11.4 %	19.6 %	
	44-1 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	2.584	58.8 %	7.5 %	12.7 %	
	45-1 インターネットへの接続を行っていない	2.565	60.7 %	13.2 %	12.1 %	
	45-2 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	2.634	29.7 %	7.6 %	3.7 %	
	45-3 庁内 LAN にインターネットからアクセス可能な公開サーバを設置していない	2.577	37.4 %	12.3 %	5.6 %	
	45-4 公開サーバ等に最新のパッチを当てている	2.495	23.8 %	10.4 %	4.6 %	
	45-5 内部ネットワークへの侵入検知の仕組みがある	2.166	21.4 %	16.3 %	13.0 %	
	45-6 遠隔保守等を行っていない	2.171	31.6 %	23.6 %	19.0 %	
	45-7 ダイヤルアップ接続は、コールバック、発信番号確認等を行っている	2.422	39.3 %	5.1 %	14.5 %	
	46-1 既設ネットワークに電子計算機等に接続するための手続、方法等を定めている	2.591	68.5 %	9.4 %	14.1 %	
	46-2 既設ネットワークの構成図を最新の状態に更新している	2.626	70.3 %	10.1 %	12.3 %	
	47-1 既設ネットワークに接続される端末の管理者を決めている	2.604	68.3 %	13.8 %	11.6 %	
	47-2 各端末の管理簿を整備している	2.175	46.6 %	14.5 %	30.5 %	

	調 査 項 目	平均値	回答 3	回答 2	回答 1	備 考
	47-3 標準的にインストールされるソフトを決めている	2.466	56.8 %	23.0 %	13.4 %	
	47-4 許可されていないソフトウェアの導入を禁止している	2.533	60.6 %	22.3 %	10.7 %	

	調 査 項 目	既存住基		住基ネット		備 考
		は い	いいえ	は い	いいえ	
(追加項目) バックアップデータの 取扱い	1-1 バックアップの作成者及び内容等を管理している	75.9 %	22.4 %	78.8 %	19.3 %	
	1-2 作成後速やかに保管庫に格納し、管理簿に記入している	57.7 %	40.4 %	62.0 %	35.9 %	
	1-3 他のバックアップメディアと容易に区別できるよう措置を行っている	91.6 %	6.8 %	94.3 %	3.9 %	
	2-1 バックアップデータの保管手続を定めている	47.7 %	50.0 %	52.0 %	44.9 %	
	2-2 保管手続を関係部課等に遵守させている	52.2 %	42.5 %	55.4 %	38.7 %	
	2-3 バックアップデータの盗難、破壊等が発生した場合の対処方法・連絡体制を整備	57.6 %	38.6 %	64.2 %	31.9 %	
	3-1 バックアップ対象と同一室内の保管庫に保管している	67.5 %	30.2 %	68.2 %	29.2 %	
	3-2 バックアップ対象と同一庁舎内の保管庫に保管している	61.0 %	32.8 %	63.7 %	30.1 %	
	3-3 バックアップ対象と別庁舎内の保管庫に保管している	6.2 %	87.5 %	2.8 %	90.6 %	
	3-4 委託事業者にて保管している	17.0 %	77.4 %	5.0 %	89.1 %	
	3-5 保管業者の倉庫に保管している	9.6 %	84.3 %	2.4 %	91.0 %	
	4-1 施錠のできる保管庫への保管等、盗難防止措置を実施している	86.7 %	11.6 %	90.8 %	7.1 %	
	4-2 自然災害の影響を受けない場所及び保管庫に保管している	71.0 %	26.3 %	70.1 %	26.5 %	
	5-1 バックアップデータの移送を行っている	26.0 %	74.0 %	6.1 %	93.9 %	
	5-2 移送に関する手続を定めている	15.6 %	8.4 %	2.4 %	2.2 %	5-1が「はい」の場合 に回答
	5-3 移送手続を関係部課等に遵守させている	16.6 %	7.0 %	2.6 %	2.0 %	

	調 査 項 目	既存住基		住基ネット		備 考
		は い	いいえ	は い	いいえ	
(追加項目)バックアップデータの取扱い	5-4 移送の際に盗難、紛失、破壊等が発生した場合の対処方法・連絡体制を整備	16.0 %	7.9 %	3.3 %	1.3 %	
	6-1 移送の際に移送日時やデータ内容を管理している	20.9 %	3.3 %	3.4 %	1.3 %	
	6-2 受渡管理簿を作成し、移送の際に記入している	16.0 %	8.1 %	2.4 %	2.2 %	
	6-3 移送責任者を任命し、移送手続に準拠しているか確認している	13.1 %	10.9 %	2.2 %	2.4 %	
	6-4 ラベルや梱包リスト等を確認し、内容物が正当なものであるか確認している	18.8 %	5.3 %	3.0 %	1.7 %	
	7-1 通信回線による伝送を行っている	6.6 %	18.7 %	1.3 %	4.0 %	
	8-1 専用回線を利用して接続している	4.8 %	1.4 %	1.0 %	0.2 %	7-1が「はい」の場合に回答
	8-2 発信者番号認証、コールバック等で接続者を限定している	5.1 %	0.9 %	0.5 %	0.3 %	
	8-3 インターネット経由での伝送を行っていない	5.1 %	0.9 %	0.6 %	0.3 %	
	8-4 ログを保存し不正アクセスがないか定期的に確認している	3.0 %	2.8 %	0.5 %	0.3 %	
	7-2 郵送又は運送業者による移送を行っている	4.9 %	19.8 %	1.0 %	4.0 %	
	9-1 盗難防止のための特別の移送方式を採用している	1.5 %	2.9 %	0.4 %	0.5 %	7-2が「はい」の場合に回答
	9-2 配達証明や電話連絡等で保管先への到着を確認している	2.1 %	2.3 %	0.7 %	0.3 %	
	9-3 内容物の取出しが容易にできないよう厳重に梱包している	3.5 %	0.9 %	0.8 %	0.2 %	
	9-4 未開封確認シールの利用等、未開封である事を確認している	1.2 %	3.2 %	0.4 %	0.6 %	
	7-3 職員による携行で移送を行っている	3.9 %	21.1 %	1.2 %	3.8 %	
	10-1 移送時には輸送物を外部から見えない場所に置いている	2.6 %	0.9 %	1.0 %	0.1 %	7-3が「はい」の場合に回答
	10-2 施錠できる専用の輸送鞆等を使用している	1.4 %	2.1 %	0.4 %	0.7 %	
	10-3 複数の移送担当で輸送を行っている	0.8 %	2.7 %	0.4 %	0.7 %	
	10-4 移送担当者が持ち場を離れないよう管理している	2.8 %	0.7 %	1.0 %	0.1 %	

	調 査 項 目	既存住基		住基ネット		備 考
		は い	いいえ	は い	いいえ	
(追加項目)バックアップデータの取扱い	7・4 委託業者による携行で移送を行っている	13.7 %	11.1 %	2.0 %	3.1 %	7・4が「はい」の場合に回答
	11・1 移送時には輸送物を外部から見えない場所に置いている	12.2 %	0.5 %	1.5 %	0.1 %	
	11・2 施錠できる専用の輸送鞆等を使用している	8.3 %	4.5 %	1.3 %	0.4 %	
	11・3 複数の移送担当で輸送を行っている	3.3 %	9.5 %	0.7 %	1.0 %	
	11・4 移送担当が持ち場を離れないよう管理している	10.8 %	2.0 %	1.4 %	0.3 %	
	13・1 バックアップデータの暗号化やそれに準じた措置を講じている	16.1 %	83.9 %	7.9 %	92.1 %	
	13・2 復号鍵等は内容を確認する権限が与えられた者が管理している	3.3 %	96.1 %	4.7 %	94.6 %	
	13・3 復号鍵等はバックアップメディアとは別の場所に保管している	2.7 %	96.8 %	4.2 %	95.0 %	