乙第41号証

住基ネットの個人情報保護対策

住民基本台帳ネットワークシステムでは、個人情報の保護を最も重要な課題としています。そのため、個人情報保護に関する国際的な基準を十分踏まえた上で、制度面、技術面及び運用面などあらゆる面で十分な対策を行っております。

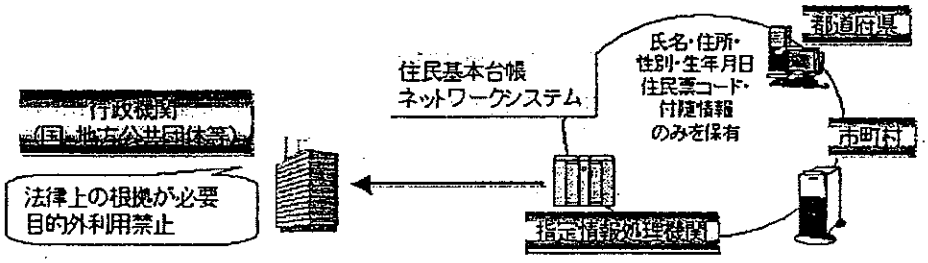
▼ 住民基本台帳ネットワークシステム　個人情報保護の取り組み（第4回住基ネット調査委員会資料）(PDF)

都道府県・指定情報処理機関で保有する情報を限定しています

1) 都道府県や指定情報処理機関が保有する情報は、4情報（氏名・住所・性別・生年月日）と住民票コード・これらの変更情報(*)に法律で限定されています。
(*)変更情報とは、氏名・住所・性別・生年月日・住民票コードについての変更年月日、理由などの必要最小限の関連情報です。

2) 都道府県や指定情報処理機関が情報提供を行う行政機関の範囲や利用目的を法律で具体的に限定しています。また、行政機関が提供された情報を目的外利用することを禁止しています。

3) 住民票の写しの広域交付、転入転出の特例等の際には、市町村から市町村へ、続柄、戸籍の表示等の情報も送信されますが、都道府県や指定情報処理機関のコンピュータに保有されることもありませんし、これらのコンピュータを通過することもありません。



▼ 住基ネット第2次稼働における住民票情報の通知について（第3回住基ネット調査委員会資料）(PDF)

住民票コードは、利用が限定されています

1) 民間部門が住民票コードを利用することは禁止されています。特に、民間部門が住民票コードの記録されたデータベースを作成したり、契約に際し住民票コードの告知を要求すると、刑罰（1年以下の懲役または50万円以下の罰金）が科せられます。

2) 行政機関が住民票コードを利用することも法律により具体的に限定しています。

3) 住民票コードは、無作為の番号で、住民の申請により、いつでも変更できます。

アメリカやカナダでは、Social Security Number等、北欧や韓国では、Personal Identity Number等が、行政や民間のさまざまな分野で使われ、共通番号となっています。
我が国の住民票コードは、市町村が住民票に記載する番号で、民間が利用できない、限られた行政分野で用いられる限定的な番号です。

▼ 住民票コード通知書関連の調査について(第4回住基ネット調査委員会資料)(PDF)

外部からの侵入と内部の不正利用を防止しています

【外部からの侵入の防止】

1) 専用回線の利用、ファイアウォール・IDS(侵入検知装置)の設置により、不正侵入を防止します。

2) 通信を行う際には、データを暗号化します。また、通信相手のコンピュータの正当性を確認してから通信を行うことにより、通信相手のなりすましを防止します。

3) 万が一の場合は、「緊急時対応計画」に基づき、ネットワークの運営を停止するなど、個人情報保護を最優先した運営を行います。

【内部の不正利用の防止】

1) 地方公共団体・指定情報処理機関・本人確認情報の受領者(行政機関)のシステム操作者に守秘義務を課し、刑罰を加重します。(通常は1年以下の懲役または3万円以下の罰金→2年以下の懲役または100万円以下の罰金)
また、委託業者が秘密を漏らした場合も、同じ刑罰が科せられます。

2) 地方公共団体・指定情報処理機関・本人確認情報の受領者(行政機関)において、操作者用ICカードやパスワードによる厳格な確認を行い、正当なシステム操作者だけがコンピュータを操作できるようにします。また、システム操作者ごとに住基ネットが保有するデータへ接続できる範囲を限定します。

3) コンピュータの使用記録を保存し、定期的な監査を行うことにより、いつ、だれが、コンピュータを使用したのか、追跡調査ができるようにします。

4) 全国で地方公共団体・指定情報処理機関・本人確認情報の受領者(行政機関)のシステム操作者のセキュリティ研修会を実施します。

▼ 電気通信回線を通じた送信又は磁気ディスクの送付の方法並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準(平成14年6月10日総務省告示第334号)概要・本文(PDF)
▼ 住基ネットのコンピュータウイルス対策について(第2回住基ネット調査委員会資料)(PDF)
▼ 2002年11月1日発生の全国センターサーバの障害について(第2回住基ネット調査委員会資料)(PDF)
▼ 住基ネットのセキュリティ研修等について(第5回住基ネット調査委員会資料)(PDF)

稼働に当たって、さらなる個人情報保護措置を講じています

▼ 住民基本台帳ネットワークシステムの稼働に当たっての新たな措置(2002年7月29日発表)

【総務省住民基本台帳ネットワークシステム緊急対策本部の設置】

セキュリティ面での緊急対応が必要な場合に、指定情報処理機関、都道府県及び市町村と連携を図りながら、迅速かつ的確に対応するため、「総務省住民基本台帳ネットワークシステム緊急対策本部」を2002年8月2日に設置

▼ 総務省における住民基本台帳ネットワークシステム緊急時の対応の概要(2002年8月2日発表)

【住民基本台帳ネットワークシステム調査委員会の新設】

住民基本台帳ネットワークシステムの運営、個人情報保護措置、セキュリティ対策、地方公共団体の体制などのあり方について幅広く調査審議を行い、総務大臣に意見を述べるため、学識経験者などの専門家や地方公共団体の代表者からなる「住民基本台帳ネットワークシステム調査員会」を8月30日に新設

- 詳しくは住民基本台帳ネットワークシステム調査委員会のページへ

【外部監査によるシステム運営調査】

全地方公共団体を対象とした「住民基本台帳ネットワークシステムセキュリティチェックリスト」による点検と一部の団体を対象とした監査法人等によるシステム運営監査をあわせて実施

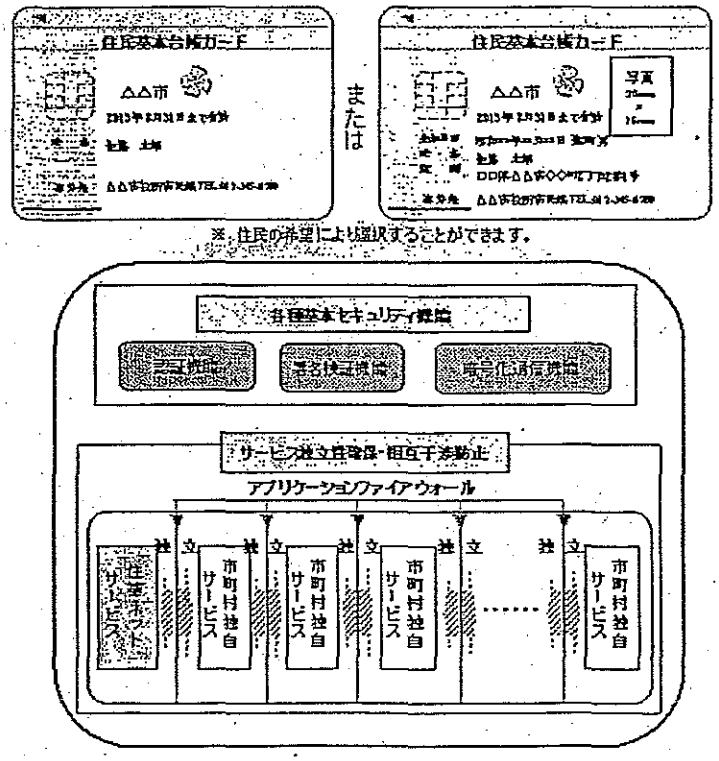
- チェックリスト、システム運営監査等について（第2回住基ネット調査委員会資料）(PDF)
- 住民基本台帳ネットワークシステムセキュリティチェックシート（第3回住基ネット調査委員会資料）(PDF)
- 住民基本台帳ネットワークシステム及びそれに接続している既設ネットワークに関する調査票による点検結果（平成15年5月12日）（第4回住基ネット調査委員会資料）(PDF)
- チェックリストの項目のうち特に重要な項目について（第5回住基ネット調査委員会資料）(PDF)
- 住民基本台帳ネットワークシステム及びそれに接続している既設ネットワークに関する調査票による点検状況（平成15年8月8日）（第6回住基ネット調査委員会資料）(PDF)

【さらに本人確認情報提供状況の開示を実施する予定】

住基ネットへのアクセスログを取得し、「開示用データ」を簡単に生成できる機能を実装し、住民からの請求に応じて、都道府県知事から自己の本人確認情報の提供状況を開示できるようなシステム開発等の準備をしています。

- 本人確認情報提供状況の開示について－検討状況－（第2回住基ネット調査委員会資料）(PDF)
- 本人確認情報提供状況の開示について住基ネット推進協議会決定（第3回住基ネット調査委員会資料）(PDF)
- 住基ネットにおける本人確認情報提供状況の開示について（平成15年9月12日）発表資料(PDF)

住民基本台帳カードは、個人情報を守るICカードです



1) 市町村がカードを発行・管理します。
→国家管理のカードではありません。

2) 住民の申請により交付します。
→携帯が義務づけられることはありません。

3) 市町村の独自サービスの範囲は条例で定める目的に限定されます。
→市町村が許可したアプリケーション以外のアプリケーションを搭載できないシステムとなっています。
→住基ネットサービス以外に、どのような市町村独自のサービスを受けるかどうかは住民が選択します。

4) 住基ネットサービス利用エリア、市町村独自サービスエリアはそれぞれ独立しています。
→住民基本台帳ネットワークシステムから市町村独自サービスエリアの情報へアクセスすることはできません。また、住民票コードは、市町村独自サービスエリアでは使用されません。

▼ 詳しくは住民基本台帳カードのページへ

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状況（平成１５年８月８日）

○　平成１５年１・２月に、市区町村は「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」に基づいてセキュリティ対策の自己点検を実施。
　その結果について、５月１２日の住民基本台帳ネットワークシステム調査委員会において報告し、公表。

○　総務省として、５月１３日に、都道府県・政令指定都市住民基本台帳ネットワークシステム担当課長会議を開催し、この点検結果を踏まえて、都道府県において、市区町村に対して必要な技術的指導を行うこと（政令指定都市にあっては、必要な対策を講じること）を要請。

○　以下の７項目については、セキュリティ確保のために特に重要な項目として、全ての市区町村において原則３点満点を達成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、徹底した技術的助言、指導を実施。

【重要点検項目】

① 重要機能室を設置できない場合、重要機器並びに磁気ディスク及びドキュメントについて、盗難されたり、権限のないものが容易にアクセスすることができないように、適切な管理を行う。

② ＣＳ端末について、ウィルスの侵入の脅威を最小限にとどめるとともに、外部への情報発信ができないようにするため、インターネットに接続できないよう制限を行う。

③ ＣＳと既設ネットワークの間にファイアウォールを設置し、適切な運用管理を行う。

④ ＣＳと既設ネットワークの間のファイアウォールについて、適切な設定を行う。

⑤ 住基ネットと接続する既設ネットワークがインターネットに接続する場合には、当該既設ネットワークとインターネットとの間にファイアウォールを設置し、厳重な通信制御を行う。

⑥ メールサーバ及びWWWサーバ等の公開サーバについて、ＤＭＺ上の設置など適切な対策を講じる。

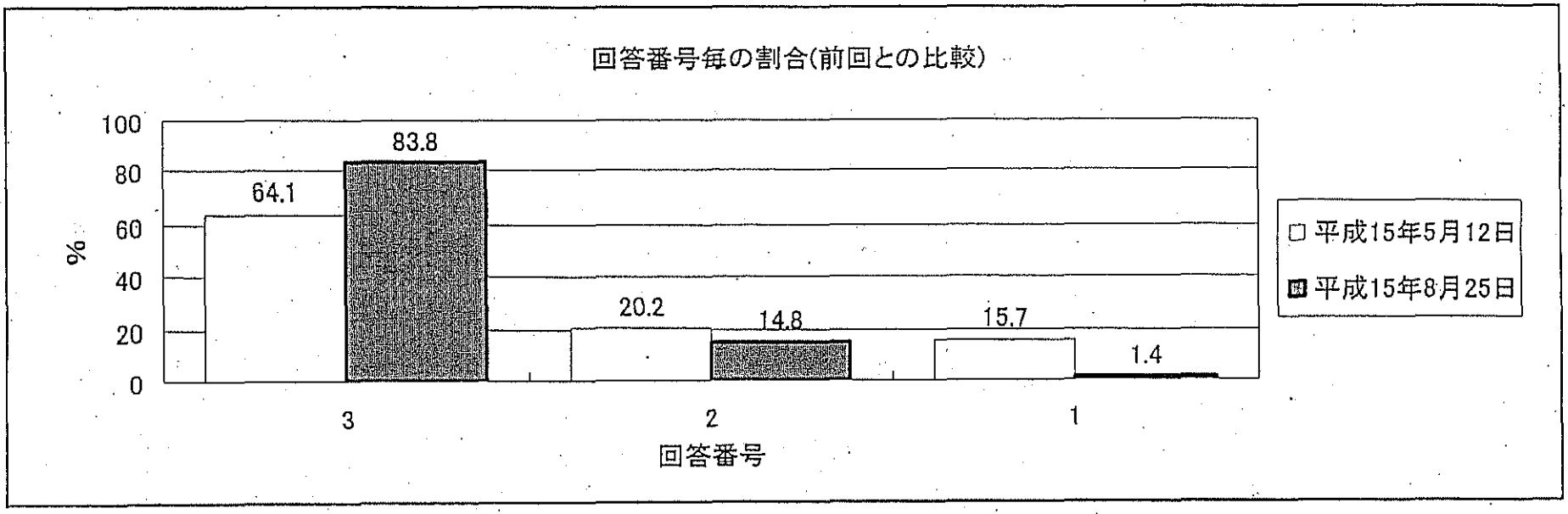
⑦ 公開サーバ等について、最新のパッチを当てる。

○ 対策状況について、自己点検結果を調査したところ、市区町村の積極的な取り組みにより、全ての市町村において、重要点検項目の７項目について３点満点を達成。

○　その他の項目についても、各都道府県、総務省及び指定情報処理機関における徹底した技術的助言、指導の実施、市区町村の積極的な取り組みにより、第２次稼働に向け、市区町村のセキュリティ対策の水準は大幅に向上。

３２０７市区町村の再点検結果の総平均点　２.８２点（３点満点）

（前回総平均点　２.４８点　＋　０.３４点）



○　なお、市区町村は今後とも、自主的にセキュリティ対策の継続的改善を実施。各都道府県、総務省及び指定情報処理機関は、引き続き技術的助言、指導に務める。

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　３２０７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	前回平均値	向上率	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	2.841	84.2 %	15.5 %	0.2 %	2.527	0.314	
	1-2 システム管理者を任命している	2.845	84.5 %	15.2 %	0.2 %	2.538	0.307	
	1-3 本人確認情報管理責任者を任命している	2.788	79.4 %	18.7 %	1.2 %	2.346	0.442	
	1-4 セキュリティ責任者を任命している	2.835	83.6 %	15.9 %	0.3 %	2.498	0.337	
	1-5 セキュリティ会議を開催している	2.542	54.7%	42.9 %	1.2 %	2.091	0.451	
	2-1 セキュリティ組織規程を作成している	2.871	87.6 %	11.9 %	0.5 %	2.529	0.342	
	2-2 アクセス管理規程を作成している	2.843	85.0 %	13.5 %	1.0 %	2.451	0.392	
	2-3 情報資産管理規程を作成している	2.834	84.1 %	14.0 %	1.2 %	2.409	0.425	
	2-4 委託管理規程を作成している	2.788	78.2 %	16.8 %	1.9 %	2.299	0.489	
	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	2.900	90.3 %	9.4 %	0.3 %	2.713	0.187	
	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	2.830	83.1 %	15.0 %	0.9 %	2.524	0.306	
	5-1 緊急時対応計画を整備している	2.830	84.0 %	14.1 %	1.4 %	2.406	0.424	
	5-2 庁内の緊急時連絡網を整備している	2.847	85.0 %	14.1 %	0.6 %	2.457	0.390	
	5-3 都道府県・市町村間の連絡網に登録している	2.888	88.7 %	10.2 %	0.4 %	2.636	0.252	

	調　査　項　目	平均値	回答３	回答２	回答１	前回平均値	向上率	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	2.946	85.6 %	3.8 %	0.5 %	2.799	0.147	
	7-1 入退室管理規程を作成している	2.836	75.6%	11.9 %	1.3 %	2.453	0.383	重要機能室有る場合に回答
	7-2 鍵又はカードの管理責任者を定めている	2.901	80.9 %	8.3 %	0.2 %	2.641	0.260	
	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	2.871	78.4 %	10.0 %	0.7 %	2.558	0.313	
	7-4 物品の搬出入は職員が内容確認している	2.891	80.2 %	8.7 %	0.5 %	2.618	0.273	
	7-5 入退室者を記録している	2.799	72.5 %	14.0 %	1.9 %	2.340	0.459	
	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【重要点検項目】	3.000	17.0 %	0.0 %	0.0 %	2.732	0.268	重要機能室無い場合に回答
	8-2 職員が不在となる時に施錠している	2.881	15.0 %	1.7 %	0.1 %	2.636	0.245	
	8-3 入室可能な者を限定している	2.792	13.4 %	2.8 %	0.3 %	2.444	0.348	
	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	2.764	73.6 %	14.6 %	3.5 %	2.356	0.408	
	9-2 事務室への入退室管理を行っている	2.680	68.6 %	21.8 %	4.2 %	2.163	0.517	
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	2.815	82.6 %	13.5 %	2.3 %	2.420	0.395	
	10-2 ユーザＩＤの所有者を明確にしている	2.811	82.2 %	13.9 %	2.3 %	2.395	0.416	
	10-3 ユーザＩＤに付与された権限が明確である	2.833	83.9 %	12.8 %	1.8 %	2.454	0.379	
	10-4 不要なユーザＩＤは登録していない	2.899	89.6 %	8.2 %	0.9 %	2.675	0.224	
	11-1 ＯＳのパスワードに有効期限を設定している	2.584	60.8 %	26.4 %	6.2 %	1.602	0.982	
	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	2.896	88.4 %	9.8 %	0.2 %	2.629	0.267	
	11-3 容易に推測されるパスワードを使用していない	2.817	81.3 %	16.4 %	0.8 %	2.486	0.331	
	11-4 ＯＳのパスワードは利用者が設定している	2.773	77.4 %	17.4 %	2.3 %	2.206	0.567	
	11-5 ＯＳのパスワードの最低桁数等の制限をしている	2.706	71.7 %	21.7 %	3.4 %	2.056	0.650	

	調　査　項　目	平均値	回答３	回答２	回答１	前回平均値	向上率	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	2.586	62.3 %	28.6 %	5.7 %	1.597	0.989	
	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	2.705	64.8 %	15.5 %	4.8 %	1.785	0.920	
	12-3 フォルダの共有設定を行っていない	2.934	93.4%	5.4 %	0.6 %	2.806	0.128	
	12-4 不要なプログラムを起動していない	2.951	95.1 %	3.8 %	0.5 %	2.856	0.095	
	13-1 標準的にインストールされるソフトを決めている	2.887	89.4 %	8.2 %	1.5 %	2.591	0.296	
	13-2 追加的なソフト導入ができない設定である	2.615	62.3 %	33.7 %	2.0 %	2.082	0.533	
	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	2.639	65.7 %	29.2 %	3.1 %	1.919	0.720	
	13-4 端末機でワープロ、表計算ソフトを使用していない	2.940	93.0 %	4.5 %	0.7 %	2.748	0.192	
	14-1 ウィルス発見時の対処手続を定めている	2.794	79.5 %	19.2 %	0.7 %	2.477	0.317	
	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【重要点検項目】	3.000	97.6 %	0.0 %	0.0 %	2.880	0.120	
	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	2.752	75.3 %	23.8 %	0.4 %	2.472	0.280	
	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	2.750	74.9 %	23.3 %	0.7 %	2.434	0.316	
	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	2.744	70.9 %	22.3 %	0.9 %	2.376	0.368	
	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	2.723	72.9 %	24.5 %	1.4 %	2.339	0.384	
	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	2.882	87.3 %	10.1 %	0.7 %	2.605	0.277	
	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	2.920	92.0 %	7.2 %	0.4 %	2.720	0.200	
	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	2.909	90.9 %	8.2 %	0.4 %	2.668	0.241	
	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	2.900	90.0 %	8.9 %	0.5 %	2.649	0.251	
	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	2.776	78.6 %	18.3 %	1.9%	2.297	0.479	
	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	2.615	62.3 %	27.5 %	4.4 %	1.791	0.824	
	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	2.903	89.9 %	9.3 %	0.2 %	2.709	0.194	

	調　査　項　目	平均値	回答３	回答２	回答１	前回平均値	向上率	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	2.838	83.6 %	15.6 %	0.3 %	2.577	0.261	
	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	2.843	84.1 %	13.4 %	1.0 %	2.500	0.343	
	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	2.725	73.2%	22.2 %	2.3 %	2.151	0.574	
	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	2.917	91.3 %	7.4 %	0.4 %	2.730	0.187	
	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	2.870	85.5 %	10.8 %	0.9 %	2.566	0.304	
	19-1 アプリケーションの操作履歴をチェックしている	2.623	63.4 %	33.8 %	1.7 %	2.124	0.499	
	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	2.730	73.9 %	23.2 %	1.7 %	2.224	0.506	
	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	2.845	84.9 %	13.2 %	1.1 %	2.546	0.299	
	20-2 機器等を接続する場合、責任者に報告している	2.897	89.6 %	8.7 %	0.7 %	2.663	0.234	
	20-3 構成機器、ソフト等の台帳記録を作成している	2.726	74.0 %	22.1 %	2.4 %	2.199	0.527	
	20-4 台帳と現況が一致することを確認している	2.729	73.5 %	21.7 %	2.3 %	2.211	0.518	
	20-5 登録されていない機器等を使用していない	2.912	89.6 %	7.4 %	0.6 %	2.716	0.196	
	21-1 保守内容及び点検項目を明確にしている	2.904	90.4 %	8.6 %	0.5 %	2.720	0.184	
	21-2 保守実施内容の記録を保管している	2.910	90.9 %	8.1 %	0.4 %	2.717	0.193	
	22-1 重要機器の保守を行う場合、職員が立ち合っている	2.908	90.6 %	8.6 %	0.3 %	2.745	0.163	
	23-1 コミュニケーションサーバが存在するＬＡＮの電気通信関係装置の物理的配線状況を管理している	2.877	87.2 %	11.1 %	0.5 %	2.724	0.153	
	23-2 余分なハブ等は設置していない	2.922	91.5 %	7.1 %	0.3 %	2.808	0.114	
	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	2.866	87.3 %	11.3 %	1.0 %	2.626	0.240	
	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	2.908	90.6 %	7.7 %	0.7 %	2.728	0.180	
	24-3 通信機器ラック等の鍵を適切に管理している	2.905	90.2 %	8.0 %	0.7 %	2.745	0.160	

	調　査　項　目	平均値	回答３	回答２	回答１	前回平均値	向上率	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	2.916	90.2 %	7.6 %	0.3 %	2.781	0.135	
	25-2 定められた場所に保管し関係者に周知している	2.934	91.6 %	6.1 %	0.2 %	2.784	0.150	
	26-1 磁気ディスクの複写、廃棄等の記録を作成している	2.703	67.2 %	23.9 %	1.9 %	2.233	0.470	
	26-2 データの受渡しごとに保管状況を確認している	2.777	71.6 %	17.5 %	1.3 %	2.410	0.367	
	26-3 取扱担当者が決められている	2.845	80.5 %	13.2 %	0.7 %	2.590	0.255	
	26-4 記号等により他の磁気ディスクと識別している	2.832	79.1 %	13.6 %	1.1 %	2.551	0.281	
	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	2.810	73.8 %	14.8 %	1.1 %	2.497	0.313	
	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	2.794	78.4 %	18.5 %	0.8 %	2.463	0.331	
	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	2.849	83.4 %	14.1 %	0.4 %	2.592	0.257	
	29-1 ドキュメントの複写、廃棄等の記録を作成している	2.588	59.1 %	32.6 %	3.2 %	1.959	0.629	
	29-2 ドキュメントの取扱担当者が決められている	2.767	75.0 %	20.5 %	1.0 %	2.381	0.386	
	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	2.798	75.5 %	17.1 %	0.9 %	2.483	0.315	
	31-1 必要のない本人確認情報の検索を行っていない	2.827	83.0 %	15.1 %	1.0 %	2.519	0.308	
	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	2.901	90.6 %	7.1 %	1.4 %	2.576	0.325	
	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	2.939	93.7 %	5.7 %	0.2 %	2.828	0.111	
	31-4 画面のハードコピーをとっていない	2.830	82.9 %	14.3 %	1.2 %	2.454	0.376	
	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	2.802	74.9 %	16.6 %	0.8 %	2.501	0.301	
	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	2.849	60.5 %	9.3 %	0.7 %	2.631	0.218	
	32-1 帳票の管理対象を明確にしている	2.824	69.8 %	12.9%	0.9 %	2.564	0.260	
	32-2 帳票を施錠のできる書庫等に保管している	2.839	70.3 %	11.6 %	0.9 %	2.599	0.240	
	32-3 帳票の廃棄時は焼却、溶解等を実施している	2.896	74.6 %	7.9 %	0.4 %	2.723	0.173	

	調　査　項　目	平均値	回答３	回答２	回答１	前回平均値	向上率	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	2.890	79.5 %	8.3 %	0.7 %	2.679	0.211	
	33-2 出力した帳票を出力装置に放置していない	2.922	78.3 %	5.8 %	0.4 %	2.761	0.161	
	34-1 障害発見時に責任者に報告を行っている	2.846	84.4 %	14.6 %	0.4 %	2.629	0.217	
	34-2 不正アクセス発見時に責任者に報告を行っている	2.855	85.3%	13.6 %	0.4 %	2.638	0.217	
	35-1 バックアップを定期的に行っている	2.937	93.8 %	5.7 %	0.3 %	2.806	0.131	
	35-2 バックアップの実施記録簿を保管している	2.810	81.1 %	14.5 %	2.0 %	2.253	0.557	
	35-3 バックアップ媒体を別の場所に保管している	2.837	85.1 %	11.3 %	2.4 %	2.417	0.420	
	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	2.766	77.5 %	20.4 %	1.4 %	2.419	0.347	
	36-2 回復する手続が定められ、関係者に周知されている	2.704	72.0 %	25.0 %	2.2 %	2.319	0.385	
	37-1 委託先の社会的信用と能力を確認している	2.907	87.1 %	7.6 %	0.6 %	2.721	0.186	
	38-1 委託業務の範囲を明確に定めている	2.927	88.8 %	5.5 %	0.7 %	2.733	0.194	
	38-2 委託先にｾｷｭﾘﾃｨ対策を実施させている	2.749	72.1 %	21.9 %	1.0 %	2.509	0.240	
	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	2.642	64.1 %	25.9 %	3.9 %	2.007	0.635	
	38-4 委託作業者の名簿を作成している	2.733	71.5 %	20.5 %	2.3 %	2.092	0.641	
	39-1 再委託を制限している	2.858	60.2 %	8.1 %	0.9 %	2.496	0.362	
	39-2 再委託時に事前申請及び承認を行っている	2.825	50.5 %	8.4 %	1.1 %	2.411	0.414	
	39-3 再委託先及び再委託業務を明確にしている	2.838	50.4 %	7.3 %	1.1 %	2.401	0.437	
	40-1 複数の事業者に委託する場合、作業範囲及び責任範囲を文書化している	2.760	26.5 %	6.7 %	0.7 %	2.345	0.415	
	40-2 事業者間の情報交換を行っている	2.737	24.9 %	7.2 %	0.7 %	2.357	0.380	
	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	2.818	31.0 %	5.8 %	0.5 %	2.468	0.350	
	41-2 セキュリティに関する指導・教育を行っている	2.749	28.2 %	8.1 %	0.6 %	2.414	0.335	

	調　査　項　目	平均値	回答３	回答２	回答１	前回平均値	向上率	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	2.919	44.0 %	1.8 %	1.0 %	2.443	0.476	
	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【重要点検項目】	3.000	93.7 %	0.0 %	0.0 %	2.871	0.129	
	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【重要点検項目】	3.000	93.5 %	0.0 %	0.0 %	2.853	0.147	
	42-4 ファイアウォールのアクセスログを保存している	2.774	76.5 %	17.4 %	2.2 %	2.374	0.400	
	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	2.658	66.3%	26.3 %	3.2 %	2.122	0.536	
	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	2.880	87.3 %	8.8 %	1.4 %	2.605	0.275	
	43-2 既設ネットワークの管理者を定めている	2.883	87.2 %	9.2 %	1.1 %	2.601	0.282	
	43-3 セキュリティ管理者を任命している	2.850	84.6 %	10.8 %	1.9 %	2.465	0.385	
	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	2.864	72.2 %	7.7 %	1.7 %	2.584	0.280	
	45-1 インターネットへの接続を行っていない	2.862	79.1 %	8.4 %	1.9 %	2.565	0.297	
	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【重点点検項目】	3.000	34.3 %	0.0 %	0.0 %	2.634	0.366	
	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【重要点検項目】	3.000	42.0 %	0.0 %	0.0 %	2.577	0.423	
	45-4 公開サーバ等に最新のパッチを当てている【重要点検項目】	3.000	32.6 %	0.0 %	0.0 %	2.495	0.505	
	45-5 内部ネットワークへの侵入検知の仕組みがある	2.572	27.4 %	16.5 %	1.5 %	2.166	0.406	
	45-6 遠隔保守等を行っていない	2.606	45.5 %	23.9 %	2.1 %	2.171	0.435	
	45-7 ダイアルアップ接続は、コールバック、発信番号確認等を行っている	2.838	48.9 %	6.1 %	1.5 %	2.422	0.416	
	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	2.860	83.7 %	9.7 %	1.8 %	2.591	0.269	
	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	2.874	85.1 %	9.5 %	1.3 %	2.626	0.248	
	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	2.868	84.8 %	10.6 %	1.1 %	2.604	0.264	

	調　査　項　目	平均値	回答３	回答２	回答１	前回平均値	向上率	備考
	47-2 各端末の管理簿を整備している	2.719	72.1 %	19.8 %	3.5 %	2.175	0.544	
	47-3 標準的にインストールされるソフトを決めている	2.772	75.8 %	18.7 %	1.6 %	2.466	0.306	
	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	2.791	77.5 %	17.5 %	1.3 %	2.533	0.258	