資料２

「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チェックリストによる調査」結果への対応状況について

１　現状

調査結果（回答）の「１」を「２」へ、「２」を「３」へ、最終的には全てが３になるようセキュリティ強化対策の実施を依頼し、各市町村においてセキュリティ対策の強化を図っているところ。

特に重点的に取り組む項目として、重要点検７項目を設定。

H15.2 回答

回答	割合
１	１２．６%
２	１９．１%
３	５８．１%

⇒

H15.6 回答

回答	割合
１	６．５%
２	１７．９%
３	６６．４%

⇒ 現在、各市町村において回答「１」をなくすことを最優先に、セキュリティ対策強化を実施中

〈参考：重要点検項目〉

	項目番号	管　理　状　況
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	14-2	端末機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
③	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している
④	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
⑤	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
⑥	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
⑦	45-4	公開サーバ等には最新のパッチを当てている

２　今後の対応

早期にサポートチームを立ち上げ、「１」を解消できない市町村を中心に現地に出向き、チェックリストに基づく技術的助言・支援を重点的に行うこととしたい。

（全ての項目について「３」となるよう助言・支援。特に重要点検項目については全て「３」とする。）

なお、総務省は、セキュリティ対策のために必要な経費について、地方財政措置を講じることとしている。

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

回答3	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	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	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	長野県（H15.2回答）			長野県（H15.6回答）			備考
		回答３	回答２	回答１	回答３	回答２	回答１	
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	57.1%	38.7%	3.4%	75.6%	22.7%	1.7%	
	１－２ システム管理者を任命している	58.0%	39.5%	1.7%	76.5%	22.7%	0.8%	
	１－３ 本人確認情報管理責任者を任命している	40.3%	37.0%	20.2%	57.1%	28.6%	14.3%	
	１－４ セキュリティ責任者を任命している	42.9%	38.7%	16.0%	61.3%	26.1%	12.6%	
	１－５ セキュリティ会議を開催している	17.6%	63.9%	14.3%	35.3%	57.1%	5.9%	
	２－１ セキュリティ組織規程を作成している	53.8%	37.8%	8.4%	70.6%	25.2%	4.2%	
	２－２ アクセス管理規程を作成している	41.2%	31.9%	25.2%	58.8%	26.9%	12.6%	
	２－３ 情報資産管理規程を作成している	37.8%	26.1%	32.8%	58.0%	22.7%	17.6%	
	２－４ 委託管理規程を作成している	32.8%	23.5%	37.8%	48.7%	26.9%	20.2%	
	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	73.9%	22.7%	3.4%	81.5%	18.5%	0.0%	
	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	68.9%	22.7%	7.6%	73.1%	23.5%	3.4%	
	５－１ 緊急時対応計画を整備している	63.0%	31.1%	5.9%	74.8%	21.8%	3.4%	
	５－２ 庁内の緊急時連絡網を整備している	58.8%	36.1%	5.0%	70.6%	28.6%	0.8%	
	５－３ 都道府県・市町村間の連絡網に登録している	68.1%	21.0%	10.1%	74.8%	19.3%	5.0%	
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	63.9%	12.6%	5.0%	67.2%	10.9%	5.9%	
	７－１ 入退室管理規程を作成している	35.3%	21.0%	23.5%	47.9%	18.5%	17.6%	重要機能室「有り」の場合に回答
	７－２ 鍵又はカードの管理責任者を定めている	53.8%	16.8%	10.9%	58.8%	17.6%	9.2%	
	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	51.3%	15.1%	15.1%	57.1%	17.6%	10.9%	
	７－４ 物品の搬出入は職員が内容確認している	48.7%	19.3%	12.6%	55.5%	21.8%	7.6%	
	７－５ 入退室者を記録している	30.3%	14.3%	34.5%	42.9%	20.2%	21.8%	
	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	10.9%	3.4%	0.0%	12.6%	0.0%	0.0%	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	7.6%	4.2%	0.8%	8.4%	3.4%	0.0%	
	８－３ 入室可能な者を限定している	6.7%	5.0%	1.7%	9.2%	2.5%	0.8%	
	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	54.6%	18.5%	18.5%	67.2%	17.6%	7.6%	
	９－２ 事務室への入退室管理を行っている	41.2%	21.0%	31.9%	53.8%	23.5%	16.0%	
３	１０－１ＯＳのユーザＩＤの管理者を決めている	77.3%	7.6%	10.1%	82.4%	8.4%	6.7%	

	調 査 項 目	長野県（H15.2回答）			長野県（H15.6回答）			備考
		回答３	回答２	回答１	回答３	回答２	回答１	
システムの管理	１０－２ユーザＩＤの所有者を明確にしている	81.5%	6.7%	10.1%	86.6%	7.6%	4.2%	
	１０－３ユーザＩＤに付与された権限が明確である	79.8%	8.4%	10.1%	84.0%	8.4%	5.9%	
	１０－４不要なユーザＩＤは登録していない	89.1%	5.0%	0.8%	89.9%	4.2%	1.7%	
	１１－１ＯＳのパスワードに有効期限を設定している	18.5%	7.6%	64.7%	41.2%	32.8%	21.8%	
	１１－２ＯＳのパスワードをマニュアルなどに記載していない	73.1%	15.1%	9.2%	79.0%	16.8%	1.7%	
	１１－３容易に推測されるパスワードを使用していない	67.2%	24.4%	6.7%	73.9%	22.7%	1.7%	
	１１－４ＯＳのパスワードは利用者が設定している	57.1%	17.6%	16.0%	67.2%	16.0%	8.4%	
	１１－５ＯＳのパスワードの最低桁数等の制限をしている	55.5%	16.8%	21.0%	66.4%	16.8%	10.9%	
	１２－１ＯＳに対するログオン失敗履歴を記録している	12.6%	5.9%	75.6%	37.8%	31.9%	26.1%	
	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	17.6%	3.4%	71.4%	41.2%	29.4%	25.2%	
	１２－３フォルダの共有設定を行っていない	78.2%	17.6%	2.5%	81.5%	15.1%	1.7%	
	１２－４不要なプログラムを起動していない	85.7%	9.2%	1.7%	87.4%	8.4%	1.7%	
	１３－１標準的にインストールされるソフトを決めている	65.5%	14.3%	16.0%	70.6%	15.1%	11.8%	
	１３－２追加的なソフト導入ができない設定である	16.0%	48.7%	31.9%	43.7%	42.9%	10.1%	
	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	32.8%	36.1%	26.1%	48.7%	35.3%	12.6%	
	１３－４端末機でワープロ、表計算ソフトを使用していない	83.2%	8.4%	2.5%	86.6%	9.2%	0.0%	
	１４－１ウィルス発見時の対処手続を定めている	67.2%	28.6%	3.4%	77.3%	20.2%	1.7%	
	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	92.4%	5.9%	0.0%	98.3%	0.0%	0.0%	
	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	73.9%	21.0%	4.2%	77.3%	16.8%	4.2%	
	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	68.1%	21.0%	8.4%	73.9%	20.2%	3.4%	
	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	82.4%	10.1%	5.9%	91.6%	6.7%	0.8%	
	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	83.2%	10.9%	5.0%	89.1%	5.9%	4.2%	
	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	68.1%	21.8%	9.2%	77.3%	19.3%	3.4%	
	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	80.7%	17.6%	1.7%	87.4%	10.9%	1.7%	
	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	76.5%	20.2%	3.4%	84.0%	14.3%	1.7%	
	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	75.6%	21.0%	3.4%	84.0%	13.4%	2.5%	
	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	58.0%	24.4%	16.8%	68.9%	22.7%	8.4%	
	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	28.6%	23.5%	43.7%	48.7%	29.4%	20.2%	
	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	78.2%	15.1%	5.0%	83.2%	16.0%	0.8%	
	１７－３容易に推測されるパスワードを使用していない	73.9%	18.5%	6.7%	79.0%	19.3%	1.7%	
	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	73.1%	20.2%	4.2%	79.8%	19.3%	0.0%	
	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	54.6%	19.3%	23.5%	62.2%	27.7%	8.4%	

調 査 項 目	長野県（H15.2回答）			長野県（H15.6回答）			備考
	回答３	回答２	回答１	回答３	回答２	回答１	
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	78.2%	16.8%	4.2%	86.6%	10.9%	1.7%	
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	66.4%	14.3%	15.1%	76.5%	12.6%	6.7%	
１９－１アプリケーションの操作履歴をチェックしている	42.9%	42.0%	11.8%	60.5%	31.9%	5.9%	
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	46.2%	31.1%	19.3%	60.5%	26.9%	10.9%	
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	57.1%	21.8%	20.2%	68.1%	21.0%	10.1%	
２０－２機器等を接続する場合、責任者に報告している	68.9%	15.1%	13.4%	76.5%	18.5%	2.5%	
２０－３構成機器、ソフト等の台帳記録を作成している	42.0%	18.5%	36.1%	51.3%	25.2%	21.8%	
２０－４台帳と現況が一致することを確認している	45.4%	18.5%	31.9%	53.8%	26.1%	17.6%	
２０－５登録されていない機器等を使用していない	74.8%	12.6%	6.7%	80.7%	10.9%	2.5%	
２１－１保守内容及び点検項目を明確にしている	86.6%	6.7%	5.9%	89.9%	5.9%	3.4%	
２１－２保守実施内容の記録を保管している	89.9%	4.2%	5.0%	93.3%	3.4%	2.5%	
２２－１重要機器の保守を行う場合、職員が立ち合っている	84.9%	9.2%	5.9%	88.2%	10.1%	1.7%	
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	77.3%	11.8%	8.4%	81.5%	10.1%	5.0%	
２３－２余分なハブ等は設置していない	82.4%	8.4%	6.7%	84.0%	7.6%	3.4%	
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	75.6%	14.3%	8.4%	79.8%	16.0%	2.5%	
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	86.6%	5.0%	6.7%	88.2%	7.6%	1.7%	
２４－３通信機器ラック等の鍵を適切に管理している	85.7%	7.6%	5.0%	88.2%	6.7%	2.5%	
２５－１磁気ディスクの保管場所は施錠している	85.7%	8.4%	2.5%	85.7%	8.4%	1.7%	
２５－２定められた場所に保管し関係者に周知している	82.4%	10.9%	3.4%	83.2%	11.8%	1.7%	
２６－１磁気ディスクの複写、廃棄等の記録を作成している	44.5%	26.1%	23.5%	52.1%	30.3%	12.6%	
２６－２データの受渡しごとに保管状況を確認している	60.5%	22.7%	11.8%	63.9%	23.5%	7.6%	
２６－３取扱担当者が決められている	73.9%	17.6%	4.2%	75.6%	16.8%	3.4%	
２６－４記号等により他の磁気ディスクと識別している	62.2%	19.3%	12.6%	71.4%	18.5%	5.0%	
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	54.6%	23.5%	10.1%	62.2%	19.3%	5.9%	
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	59.7%	20.2%	16.8%	68.9%	19.3%	9.2%	
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	67.2%	21.0%	8.4%	74.8%	16.8%	5.9%	
２９－１ドキュメントの複写、廃棄等の記録を作成している	26.9%	31.9%	34.5%	35.3%	38.7%	21.8%	
２９－２ドキュメントの取扱担当者が決められている	59.7%	23.5%	11.8%	65.5%	21.8%	7.6%	
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	58.8%	22.7%	11.8%	65.5%	17.6%	10.9%	
３１－１必要のない本人確認情報の検索を行っていない	66.4%	25.2%	6.7%	76.5%	20.2%	3.4%	
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	82.4%	7.6%	8.4%	86.6%	7.6%	5.9%	
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	84.9%	5.9%	8.4%	88.2%	7.6%	4.2%	

	調 査 項 目	長野県（H15.2回答）			長野県（H15.6回答）			備考
		回答３	回答２	回答１	回答３	回答２	回答１	
	３１－４画面のハードコピーをとっていない	70.6%	17.6%	10.1%	77.3%	16.0%	6.7%	
	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	48.7%	26.1%	10.1%	61.3%	23.5%	6.7%	
	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	52.9%	10.1%	3.4%	64.7%	11.8%	2.5%	
	３２－１帳票の管理対象を明確にしている	58.0%	15.1%	9.2%	63.0%	18.5%	4.2%	
	３２－２帳票を施錠のできる書庫等に保管している	52.9%	13.4%	13.4%	58.0%	19.3%	6.7%	
	３２－３帳票の廃棄時は焼却、溶解等を実施している	68.9%	10.9%	2.5%	72.3%	12.6%	1.7%	
	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	68.9%	10.1%	8.4%	73.9%	12.6%	3.4%	
	３３－２出力した帳票を出力装置に放置していない	71.4%	6.7%	5.0%	78.2%	9.2%	2.5%	
	３４－１障害発見時に責任者に報告を行っている	68.1%	27.7%	4.2%	76.5%	21.8%	1.7%	
	３４－２不正アクセス発見時に責任者に報告を行っている	68.9%	27.7%	3.4%	77.3%	21.0%	1.7%	
	３５－１バックアップを定期的に行っている	84.9%	5.9%	5.9%	89.1%	3.4%	5.0%	
	３５－２バックアップの実施記録簿を保管している	69.7%	7.6%	18.5%	78.2%	10.1%	8.4%	
	３５－３バックアップ媒体を別の場所に保管している	64.7%	11.8%	20.2%	76.5%	10.1%	10.9%	
	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	52.1%	32.8%	12.6%	60.5%	30.3%	6.7%	
	３６－２回復する手続が定められ、関係者に周知されている	51.3%	31.1%	15.1%	57.1%	31.1%	9.2%	
	３７－１委託先の社会的信用と能力を確認している	79.0%	10.1%	5.9%	80.7%	10.9%	3.4%	
	３８－１委託業務の範囲を明確に定めている	89.9%	2.5%	3.4%	92.4%	1.7%	0.8%	
	３８－２委託先にｾｷｭﾘﾃｨ対策を実施させている	64.7%	27.7%	3.4%	73.9%	19.3%	0.8%	
	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	52.9%	28.6%	14.3%	72.3%	16.8%	5.9%	
	３８－４委託作業者の名簿を作成している	51.3%	17.6%	23.5%	60.5%	19.3%	14.3%	
	３９－１再委託を制限している	80.7%	1.7%	8.4%	84.0%	1.7%	5.0%	
	３９－２再委託時に事前申請及び承認を行っている	53.8%	5.0%	12.6%	61.3%	3.4%	9.2%	
	３９－３再委託先及び再委託業務を明確にしている	56.3%	4.2%	12.6%	59.7%	4.2%	9.2%	
	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	22.7%	7.6%	7.6%	26.9%	9.2%	5.0%	
	４０－２事業者間の情報交換を行っている	21.0%	6.7%	5.9%	25.2%	8.4%	4.2%	
	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	29.4%	3.4%	5.9%	33.6%	5.9%	4.2%	
	４１－２セキュリティに関する指導・教育を行っている	28.6%	4.2%	5.9%	32.8%	7.6%	3.4%	
４既設ネッ	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	17.6%	0.8%	2.5%	20.2%	0.0%	0.0%	
	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	91.6%	3.4%	0.0%	95.0%	0.0%	0.0%	
	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	91.6%	1.7%	1.7%	95.0%	0.0%	0.0%	
	４２－４ファイアウォールのアクセスログを保存している	87.4%	8.4%	0.0%	89.9%	6.7%	0.0%	
	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	21.0%	70.6%	3.4%	68.9%	23.5%	1.7%	

	調 査 項 目	長野県（H15.2回答）			長野県（H15.6回答）			備考
		回答３	回答２	回答１	回答３	回答２	回答１	
トワークとの接続	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	72.3%	15.1%	10.9%	81.5%	11.8%	4.2%	
	４３－２既設ネットワークの管理者を定めている	71.4%	14.3%	12.6%	78.2%	12.6%	5.9%	
	４３－３セキュリティ管理者を任命している	68.1%	16.0%	14.3%	76.5%	14.3%	6.7%	
	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	58.8%	6.7%	14.3%	64.7%	10.1%	9.2%	
	４５－１インターネットへの接続を行っていない	68.1%	10.1%	15.1%	74.8%	10.9%	7.6%	
	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	36.1%	8.4%	3.4%	42.0%	3.4%	0.0%	
	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	70.6%	5.0%	1.7%	75.6%	0.0%	0.0%	
	４５－４公開サーバ等に最新のパッチを当てている	63.0%	2.5%	0.8%	69.7%	0.0%	0.0%	
	４５－５内部ネットワークへの侵入検知の仕組みがある	30.3%	15.1%	15.1%	38.7%	21.0%	5.0%	
	４５－６遠隔保守等を行っていない	10.9%	58.0%	12.6%	22.7%	59.7%	2.5%	
	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	69.7%	1.7%	5.0%	77.3%	2.5%	1.7%	
	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	67.2%	10.1%	17.6%	73.1%	11.8%	8.4%	
	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	68.1%	7.6%	20.2%	73.1%	14.3%	6.7%	
	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	70.6%	16.0%	10.9%	74.8%	17.6%	4.2%	
	４７－２各端末の管理簿を整備している	43.7%	16.8%	35.3%	52.1%	20.2%	23.5%	
	４７－３標準的にインストールされるソフトを決めている	56.3%	17.6%	21.8%	65.5%	19.3%	10.1%	
	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	59.7%	21.0%	16.0%	67.2%	21.0%	7.6%	