監査の結果に基づき措置を講じた旨の通知に係る事項の公告

地方自治法（昭和２２年法律第６７号）第２５２条の３８第６項の規定により、平成２２年度包括外部監査の結果に基づき措置を講じた旨の通知があったので、次のとおり公表します。

平成２４年3月３０日

奈良県監査委員　廣　野　隆　信
同　南　田　昭　典
同　井　岡　正　徳
同　森　川　喜　之

監査の特定事件（テーマ）

情報システムに係る財務事務の執行について

監査結果	措置内容
◎　セキュリティーポリシー	
①　情報セキュリティ監査の未実施 「奈良県情報セキュリティ基本方針」では、「基本方針及び対策基準への遵守状況を検証するため、必要に応じて情報セキュリティ監査を実施する」と規定されている。 しかし、平成15、16年度に実施されて以降、情報セキュリティ監査は実施されていない。 情報システム委員会等で、情報セキュリティの現状を認識した上で、情報セキュリティ監査を実施することが必要である。	平成24年１月、２月に情報セキュリティ内部監査を実施した。今後は、以下のスケジュールで情報セキュリティ監査を実施する。 ・　平成24年度 内部監査、セルフチェックの実施 （内部監査、セルフチェックは以降毎年実施予定） ・　平成25年度 外部監査、内部監査、セルフチェックの実施 （外部監査は、以降５年に１回程度実施予定）
◎　職員へのセキュリティ教育の状況	
①　パスワードルールの逸脱 ○　「奈良県情報セキュリティ対策基準」では、システムの利用者に対して、推測が困難なパスワードを設定するよう規定しているが、現に監査人が所管課におけるシステムの管理状況を観察した際にも、連続数値等、非常に簡便なパスワードしか設定していないシステムが発見されている。このような状況において、情報システム課として、研修等による指導は行っているものの、各所管課、あるいは個人に対する具体的な指導は行っていない。アンケートにより規程への違反が把握されている以上、情報セキュリティ主任を通して個別的な指導を行う等の対応が必要である。 ○　「奈良県情報セキュリティ対策基準」に反したパスワードは設定できないようにする等、システムの機能で対応を行っていくことが必要である。また現在稼動しているシステムに対して、上記の対応を行って行くことは困難な場合も想定されるため、今後、新たに導入するシステムについては、一定のパスワードの強度を担保できるような仕組みを構築することが必要である。	セキュリティ主任は、毎年、(財)地方自治情報センターのセキュリティ研修を受講するとともに、セキュリティ主任が、セキュリティ担当者、一般職員等にセキュリティ研修を実施し、パスワードルール等周知徹底を行っている。 現在、平成23年10月に運用を開始した認証システムで、ID、パスワードの一元管理を行っている。また、システムの新規導入や再構築に合わせて、原則として認証システムを利用することにより、パスワードの強度を確保することとしている。 パスワードについては、下記ポリシーで実施している。 ・　文字数：８文字～10文字 ・　再利用制限：３回 ・　利用文字：英大文字、英小文字、数字 ・　有効期限：90日 ・　有効期限切れの警告：14日前 ・　単純なパスワードは使用不可
◎　個別システムのセキュリティ状況	
①　アクセス制限の未実施 奈良県情報セキュリティ対策基準」では、システムに対しパスワード、利用者カード等を使用したアクセス制限を行うことが規定されている。 システムにアクセス制限の機能がない場合においては、OSの起動時にパスワードを設定した上で、一定時間操作がなければ再度パスワードが必要になる設定を行う等、権限を有さない第三者のシステムの不正利用を防止できる対策を講じることが必要である。	平成22年度アクセス制限未実施システムについては、ID、パスワードの対策を実施済みである。 端末を一定時間操作しなかった場合に備えて、パスワード付きのスクリーンセイバーを設定することをセルフチェックにより確認している。
②　ID等の共有使用 IDが共有で使用されていると、操作した者を特定することができず、悪意のある者又は過失によってデータの改ざんや消失がなされてしまう可能性が高くなる。そのため、個人別にIDとパスワードの設定を行うことが必要である。	今後、新規導入や再構築に合わせて、原則として認証システムを利用することにより、個人毎にID、パスワードを設定する仕組みとした。
③　パスワード定期変更の未実施 長期にわたりパスワードの変更が行われていない場合、本来権限を有さない第三者にシステムを利用される可能性が高くなり、情報が漏洩する可能性が高くなる。そのため、各システムについて、定期的なパスワードの変更を行うことが必要である。 その際、システムの機能を用いて、定期的にユーザにパスワードの変更を促す、あるいは、システム管理者がユーザに対して書面で変更を促すとともに、変更後は実施結果の報告を受ける等の方法も考えられる。	システムの新規導入や再構築に合わせて、原則として認証システムを利用することにより、強制的にパスワード変更を行う仕組みとした。

監査結果	措置内容
◎　所管課におけるサーバの管理状況	
①　管理者カード及びUSBメモリの管理ルールの逸脱 ○　管理者用のFSSカードについては「ICカードセキュリティシステム運用管理規程」で、公用USBメモリについては「公用USB管理要領」で、それぞれ貸出簿を作成することが要求されている。しかし、所管課において、当管理簿の有無を確認したところ、管理者用カードについては１課、公用USBメモリについては使用実績がないとの理由があるものの、２課で作成されていなかった。 　データの持ち出しは、情報資産の漏洩のリスクを伴う行為であるため、策定された管理規程に従い、適切に管理を行うことが必要である。 ○　管理者用カード及び公用USBメモリの保管場所について、夜間等、使用頻度が落ちる時間帯には施錠のできるところに保管する等、不正な使用に対して、一定の牽制をかけることが必要である。	管理者カード、公用USBの管理簿を作成していなかった２課については,管理簿の作成を行った。 　今後、貸出簿の作成、公用USBメモリの利用の確認については、情報セキュリティ担当者への研修で周知を図ると共に、セルフチェックで確認を行う。 　また、管理者用カード、公用USBメモリの保管場所は施錠できる場所とするよう、セキュリティ研修テキストに明記し、周知を行った。
②　遊休状態のパソコン端末の管理不十分 　遊休になっているパソコン端末については、資産の有効活用の観点から、速やかに情報システム課に届ける等して、別の業務へ転用することが必要である。 　また、一方で、十分な管理がされていないまま放置され、さらにそのパソコン端末の中に重要な情報が残されたまま放置されていることがあるとすれば、情報が漏洩する可能性が高くなる。そのため、壊れている、あるいはパソコン端末が古く、今後の使用が困難なものについては、必要なデータは他のパソコン端末に引き継いだ上で、速やかに処分することが必要である。	平成22年度末に遊休パソコンの処分を実施した。さらに平成23年度以降も遊休パソコンの処分を適宜実施する。