消去用ソフトウェアの利用など)」との質問に対して、「はい」が８８％、「いいえ」が３％、「『はい』『いいえ』どちらの場合もある」が７％であった。

【意　見】

情報資産管理責任者は、重要な情報資産が含まれる文書や記録媒体の廃棄については、廃棄を回収・処分業者に外部委託する場合には、業者から溶解証明書やデータ消去の報告を取り付けたり、機密保持について契約条項の中に盛り込むなど、所要のセキュリティ対策を講じられたい。

また、職員自らが廃棄を行う場合には、記録媒体を物理的に破壊するなど、適切に処理されたい。

「重要な情報資産を分類していない」場合は、分類のうえ、廃棄方法を決定されたい。

イ　人的情報セキュリティ対策について改善を要するもの

①　私物パソコン等を庁舎内に持ち込み・使用する場合の手続き

【監査結果】

県の対策基準において、職員が業務を処理するに当たり、私物パソコン等を持ち込み・使用することは原則禁止されており、やむを得ず持ち込み・使用する場合には、情報セキュリティ管理者の許可を得ることとされている。

私物パソコン等を庁舎内に持ち込み・使用する場合の手続きの状況は、次のとおりであった。

・情報セキュリティ管理者の許可（実績なし）　１９０所属
・情報セキュリティ管理者の許可（実績あり）　１１所属
・情報セキュリティ管理者の許可を得ていないものがある　８所属
・その他　１１所属
※「その他」には、課内室である６所属等が含まれる。

実地監査したところ、公有財産として短期大学校や専門学校が管理しているパソコン以外に、学生等が学内で私物パソコンを使用していた。

【意　見】

職員の私物パソコン等については、使用しているソフトウェアやウィルス対策が、パソコンの所有者により管理されているという点で、セキュリティ上、リスクの可能性が考えられる。

そのため、職員の私物パソコン等の持ち込み・使用は原則禁止であり、業務上やむを得ず持ち込み・使用する場合には、情報セキュリティ管理者の許可を得るとともに、情報資産の取り扱いについて十分留意する必要がある。

また、学生等が学内で私物パソコンを使用している場合については、学内において私物パソコンを使用する場合の遵守事項を定めるなど、セキュリティ対策に努められたい。

教育委員会の対策基準には、所属長の許可など、私物パソコンを庁舎内へ持ち込み・使用する場合の手続きについては特段規定されていないが、職員が私物パソコンを取り扱う場合のセキュリティ対策には十分留意されたい。また、私物パソコンのネットワークへの接続は禁止されているので遵守されたい。

②　所管する情報システムについて、利用者の登録及び抹消等に関する手順及び記録の有無

【監査結果】

県の対策基準において、情報システム管理者は、利用者の登録、変更、抹消等、登録情報の管理については、あらかじめ方法を定めて行い、使用権限のない者が情報システムを利用できないようにしなければならないこと、また、登録された利用者についても定期的に、その利用権限が妥当であるか確認を行うこととされている。

所管する情報システムについて、利用者の登録及び抹消等に関する手順及び記録の有無の状況は次のとおりであった。

・手順があり、記録を保存している　４７システム
・手順があるが、記録を保存していない　１８システム
・手順・記録なし　４２システム
・その他　３システム
※「その他」には、情報システムの管理主体が国である１システムや、県の他のシステムの一部を利用する１システム等が含まれる。

実地監査したところ、利用者の登録及び抹消等に関する手順や承認手続きにおいて、実施手順では、利用者管理簿を作成することとなっているが、利用者管理簿が未作成なものがあった。（３システム）

また、一部のシステムでパスワードの変更について、実施手順に沿った管理が行われていないなど、セキュリティ対策の不十分なものがあった。（３システム）

その他、情報システムの認証等に用いるＩＣカードを管理している所属があった。

【意　見】

利用者権限の管理がなされていない場合、使用権限のないユーザＩＤや不要なユーザＩＤが残余する可能性も考えられる。

情報システム管理者は、所管する情報システムについて、実施手順に沿った利用者の登録及び抹消等に関する手順や承認手続きを実施されたい。

また、登録された利用者については、定期的にその利用権限が妥当であるか確認し、使用権限のないユーザＩＤや不要なＩＤは抹消する必要がある。

利用者の登録及び抹消等にあたっては、利用者管理簿を作成するなど、適切な管理が望まれる。

情報システム管理者及び情報システムの利用者は、パスワードの定期的な変更について、実施手順に沿ったパスワード管理を実施されたい。

認証等に用いるＩＣカードを管理している所属については、貸付簿による管理を行うなど、定期的に確認することが望まれる。

ウ　物理的情報セキュリティ対策について改善を要するもの

①　所管する情報システムの運用停止による影響

【監査結果】

所管する情報システムが運用停止した場合の業務等に及ぼす影響については、次のとおりであった。

・業務執行が困難となる	３７システム
・代替手段がなく、影響が大きい	１２システム
・短時間であれば代替手段によることも可能だが、影響がある	３４システム
・代替手段があり、影響が少ない	２２システム
・その他	５システム

※「その他」には、情報システムの管理主体が国である３システム等が含まれる。

システムの運用停止が業務等に及ぼす影響について、「業務執行が困難となる」、あるいは「代替手段がなく、影響が大きい」と回答したものが４９システムあり、全体の約４５％を占めていた。このうち、運用停止を回避するための対策の有無について、「特になし」と回答したものが１２システムあった。

【意　見】

各所属が所管する情報システムやネットワークについては、運用が停止した場合、当該所属が中心となって、再稼動させることとなっている。

県民が利用する情報システムや県民へのサービス提供を行っている情報システムについては、非常時において、再稼動の問い合わせが寄せられる可能性もあることから、情報システム管理者及びネットワーク管理者は、継続的なサービス提供が必要な情報システムやネットワークについて、運用停止を回避するための対策や円滑な業務復旧のための対応について検討されたい。

②　サーバ室及びコンピュータ室の入退室管理

【監査結果】

県の対策基準においては、許可のない者の出入防止のため、サーバ室及びコンピュータ室の入退室管理について定められている。

サーバ室及びコンピュータ室の入退室管理の状況は次のとおりであった。

なお、集計にあたり、「サーバ室及びコンピュータ室なし」と回答した６５システムは除いた。

・許可のある者のみが入室できる	３３システム
・入退室の制限はされていない	８システム
・その他	４システム

※「その他」には、情報システムの管理主体が国である１システムや、県の他のシステムの一部を利用する２システム等が含まれる。

「許可のある者のみが入室できる」と回答した３３システムのうち、「ＩＣカードによる入退室制限」と回答したものが１７システム、「入退室管理簿への記載」と回答したものが５システム、「方法は定めていない」と回答したものが３システムなどであった。

【意　見】

サーバ室及びコンピュータ室内への入退室を行えるのは、情報システム管理者又はネットワーク管理者により許可された者に限定されることから、入退室の制限がなされていない所属や入退室の管理方法を定めていない所属については、情報システム管理者及びネットワーク管理者は、入退室管理簿等による入退室の管理を徹底されたい。

エ　技術的情報セキュリティ対策について改善を要するもの

①　重要な情報資産のバックアップについて

【監査結果】

県の対策基準において、情報システム管理者は、情報資産についてその重要度に応じて期間を設定し、定期的にバックアップ用の複製を採らなければならないとされている。

重要な情報資産のバックアップの実施状況は次のとおりであった。

なお、集計にあたり、「重要な情報資産を分類していない又は取り扱っていない」と回答した６８所属は除いた。

・バックアップを定期的に実施している	８２所属

・バックアップを実施しているが、不定期である　３９所属
・バックアップを実施していない　１８所属
・その他　１３所属
※「その他」には、課内室である６所属等が含まれる。

重要な情報資産のバックアップを実施していると回答した１２１所属のうち、バックアップした記録媒体の保管場所について、「保管庫等に保管」と回答した所属が４０所属、「執務室に保管」と回答した所属が５６所属、「業者に委託している」と回答した所属が６所属などであった。

また、バックアップした記録媒体の保管方法については、「原本やサーバから離れた場所に保管」と回答した所属が４８所属、「原本やサーバに隣接した場所に保管」と回答した所属が６０所属であった。

実地監査したところ、バックアップした記録媒体を、執務室内の金庫で保管しているものやサーバ室又はコンピュータ室から離れた場所で世代管理し、保管しているものがあったが、一部のシステムで、バックアップがサーバー（原本）と同じラック内に保管されているものや隣接した場所に保管されているものがあった。（１１所属）

また、個人情報など重要な情報が記録された記録媒体が、他の記録媒体と一緒に保管されており、識別が困難なものがあった。（１所属）

【意　見】

災害等によるシステムダウンがあった場合、システムの復旧にはバックアップした記録媒体等が必要となることから、情報システム管理者は、情報資産の重要性に応じて期間を設定し、定期的にバックアップを実施されたい。

また、重要な情報をバックアップした記録媒体については、他の記録媒体と識別できるよう適切な管理が望まれる。

県の対策基準において、バックアップした複製は原本と物理的に離れた場所に保管することが望ましいとされているので留意されたい。

「重要な情報資産を分類していない」場合は、分類のうえ、バックアップ方法を決定されたい。

②　所管する情報システムの障害に対する処理及び問題等の記録・保存

【監査結果】

県の対策基準において、情報システム管理者及びネットワーク管理者は、職員から報告のあった所管する情報システムの障害に対する処理及び問題等は障害記録として体系的に記録し、常に活用できるよう保存しなければならないとされている。

所管する情報システムの障害に対する処理及び問題等の記録・保存の状況は次のとおりであった。

・記録・保存されている　４７システム
・一部について記録・保存されている　１６システム
・記録・保存されていない　３８システム
・その他　９システム
※１「記録・保存されていない」には、現在までに実際に障害が発生したことがないため記録がない情報システムが含まれており、実地監査対象所属の情報システムの約９割が、現在まで障害が発生したことがないとのことであった。
※２「その他」には、情報システムの管理主体が国である４システムや、県の他のシステムの一部を利用する２システム等が含まれる。

実地監査したところ、障害が発生した場合、県から保守業者への障害対応依頼や、保守業者から県への対応報告について、電話等のみで行い、障害に対する処理及び問題等を記録・管理していない場合があった。

【意　見】

障害に対する処理及び問題等を記録・保存していない場合、障害の傾向分析や障害案件の対応状況の管理が困難となり、結果として、障害案件が未解決のまま放置されたり、再発防止策が講じられなかったりする可能性がある。情報システム管理者及びネットワーク管理者は、障害記録の体系的整理と保存・活用の徹底を図られたい。

③　所管する情報システムのシステム変更など、保守委託先がシステムに加えた作業内容の記録保管

【監査結果】

県の対策基準において、情報システム管理者及びネットワーク管理者は、所管する情報システムにおいて行った変更等の作業については記録を作成し、適切な管理を行わなければならないとされている。

所管する情報システムのシステム変更など、保守委託先がシステムに加えた作業内容の記録保管の状況は次のとおりであった。

なお、集計にあたり、「委託していない」及び「システム変更なし」と回答した４９システムは除いた。

・全て保管している　４１システム
・一部について保管している　５システム
・保管していない　８システム
・その他　７システム

※「その他」には、情報システムの管理主体が国である４システムや、県の他のシステムの一部を利用する２システム等が含まれる。

【意　見】

システムの仕様書が入手されていない場合や、仕様書があってもシステムの変更の都度、仕様書の見直しが行われていない場合、県が意図したとおり、システムの変更が行われているかを検証できず、システム変更が適切に実施されていることを確認できなくなるおそれがあるので、情報システム管理者及びネットワーク管理者は、変更等の作業に係る記録を作成し、適切な管理を徹底されたい。

また、業務上必要としない者による利用を防止するため、情報システム仕様書等は、業務上必要とする者のみが閲覧できる場所に保管されたい。

④　不正プログラムによる誤動作を発見したときの対応について

【監査結果】

アンケート調査によると、コンピュータウィルスに感染のおそれがある場合や不正プログラムによる誤動作を発見したときの対応は、次のとおりであった。

・対応を知っている	９２％
・対応を知らない	８％

【意　見】

職員は、コンピュータウィルスに感染のおそれがある場合や、不正プログラムによる誤動作の発見時には、所要の対応が迅速になされるよう、平素から研修の機会などを利用して理解に努められたい。また、情報政策課は、引き続き研修等を通じて周知徹底を図られたい。

なお、各所属で管理しているパソコンについては、ウィルスチェックを定期的に実施するなど不正プログラム対策を実施されたい。

教育委員会においては、「県立学校教育情報化推進事業により整備されたパソコン（ハイユースパソコン）内の情報管理の徹底及び個人情報流出の防止について」（平成20年2月27日付け教高第2518号）により、ハイユースパソコンの管理及び個人情報の管理の徹底等について通知されているので遵守されたい。

オ　運用における情報セキュリティ対策に改善を要するもの

①　県の対策基準に基づく情報セキュリティ実施手順の策定状況

【監査結果】

県の基本方針において、基本方針及び対策基準に基づき、情報セキュリティ対策を実施するため、個々の情報システムについて、具体的な実施手順を明記した情報セキュリティ実施手順を策定することとされている。

情報セキュリティ実施手順の策定状況は次のとおりであった。

・策定している	６２システム
・策定していない	４２システム
・その他	６システム

※「その他」には、情報システムの管理主体が国である３システムや、県の他のシステムの一部を利用する２システム等が含まれる。

実地監査したところ、実施手順が定められているが、実施手順どおり実施されていないものや、実施手順の内容が実態と合っていないもの、内容の具体性に乏しいものがあった。（２システム）

（例）

- 実施手順に、「長期間（３０日以上）利用のないユーザＩＤは速やかに抹消する。」と記載されていたが、実施されていなかった。
- 情報システムが保有する情報として、個人情報を取り扱っていたが、実施手順の情報資産の分類において、機密性のレベルが低く分類されているものがあった。
- 実施手順に、「バックアップはその都度実施し・・・」と記載されているが、バックアップの実施方法について、具体的な記述がなかった。

【意　見】

個々の情報システムの実態を勘案しておらず、不十分な実施手順が見受けられたので、情報システム管理者は、早急にリスクを洗い出し、実効性のある実施手順に改善されたい。

また、県の情報セキュリティポリシーの適用のある情報システムのうち、実施手順のない情報システムについては、早急に策定されたい。

②　県の対策基準に基づく緊急時対応計画の策定状況

【監査結果】

県の対策基準において、情報セキュリティに関する事故等が発生した場合に対応するため、情報システム管理者及びネットワーク管理者は、実施手順において緊急時対応計画を策定することとされている。

実施手順を策定している６２システムのうち、緊急時対応計画の策定状況は次のとおりであった。

・策定している　５０システム
・策定していない　１２システム

【意　見】
緊急時対応計画を策定していない情報システムについては、情報セキュリティに関する事故等が発生した場合に、迅速かつ的確な対応を行うため、計画を早急に策定されたい。

③　情報システムの運用・保守の外部委託契約書等における情報セキュリティに関する特記事項の添付の有無

【監査結果】
県の対策基準においては、所管する情報システムの管理運用等を外部委託する場合は、委託事業者に対し必要な情報セキュリティの要件を記載した契約書による契約を締結しなければならないとされている。
また、「外部委託に係る情報セキュリティ対策基準」においては、情報システム管理者及びネットワーク管理者は、情報システム等の開発、運用等を委託するにあたっては、情報セキュリティに関する特記事項（以下「特記事項」という。）を遵守できる者を選定すること、また、委託契約に係る契約書に委託先事業者が特記事項を遵守する旨を記載し、特記事項を契約書に添付することとされている。
「情報システム等に係る運用及び保守等の業務の外部委託契約」や「情報システム等の運用及び保守等を含む機器等の賃貸借契約」の契約書等における情報セキュリティに関する特記事項の添付の有無の状況は次のとおりであった。
なお、集計にあたり、当該外部委託契約及び賃貸借契約がない等のため、「該当なし」と回答した４５システムは除いた。

・あり　３７システム
・なし　１４システム
・一部なし　７システム
・その他　７システム
※「その他」には、情報システムの管理主体が国である３システムや、県の他のシステムの一部を利用する２システム等が含まれる。

【意　見】
山梨県個人情報保護条例第８条第２項において、個人情報取扱事務を実施機関以外のものに委託する場合は、個人情報の適切な管理のために必要な措置を講じなければならないとされており、具体的には、県の対策基準及び「外部委託に係る情報セキュリティ対策基準」に基づき、それぞれの委託に応じて情報セキュリティの確保に努めることとされている。
情報システム管理者及びネットワーク管理者は、「情報システム等に係る運用及び保守等の業務の外部委託契約」や「情報システム等の運用及び保守等を含む機器等の賃貸借契約」を締結する際には、契約書に委託先事業者が特記事項を遵守する旨を記載し、特記事項を添付することとされたい。
また、契約書等の書面を作成しない契約の場合は、特記事項を契約事項として委託先事業者に書面で交付することとされているので留意されたい。

④　外部委託先からの情報セキュリティ対策実施状況報告書の提出状況

【監査結果】
県の対策基準においては、委託に関する責任を有する情報システム管理者は、委託先において必要な情報セキュリティ対策が確保されていることを確認することとされている。また、「外部委託に係る情報セキュリティ対策基準」では、情報システムの運用・保守業務等の委託先事業者から情報セキュリティ対策実施状況報告書の提出を受け、情報セキュリティ対策が確保されていることを確認することとされている。
外部委託先からの情報セキュリティ対策実施状況報告書の提出状況については、次のとおりであった。
なお、集計にあたり、「該当なし」と回答した５７システムは除いた。

・あり　２３システム
・なし　１７システム
・一部なし　７システム
・その他　６システム
※「その他」には、情報システムの管理主体が国である３システムや、県の他のシステムの一部を利用する２システム等が含まれる。

【意　見】
県が保有する情報資産には、業務上重要な情報が多数含まれることから、情報資産の安全性を確保することが重要である。情報システムの運用・保守業務等の外部委託先のセキュリティレベルが低い場合、情報資産の滅失や漏洩等のリスクが高まることも考えられる。
情報システム管理者及びネットワーク管理者は、情報システムの運用・保守業務等を委託する際には、外部委託先から情報セキュリティ対策の報告の提出を受け、情報セキュリティ対策の状況について確認されたい。
また、「外部委託に係る情報セキュリティ対策基準」には、再委託がある場合は、再委託先事業者から情報セキュリティ対策実施状況報告書の提出を受けることや、長期継