・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

続契約の場合における定期的な委託先事業者の調査等の実施についても規定されているので、留意されたい。

（3）職員に対する情報セキュリティ基本方針等の周知はなされているか。

ア　職員に対する情報セキュリティ基本方針等の周知を継続すべきもの

①　職員の情報セキュリティに関する研修等への参加状況

【監査結果】

情報システム管理者又は情報セキュリティ管理者の情報セキュリティに関する研修等への参加状況は、次のとおりであった。

・情報政策課の研修に参加したことがある。	１４６所属
・その他の研修に参加したことがある	２５所属
・参加したことがない	２１所属
・その他	２８所属

※「その他」には、職場研修を行った８所属や、ｅラーニングを行った２所属等が含まれる。

情報政策課は、平成１６年度より、情報セキュリティの意識の向上等を目的とした教育研修を実施している。

情報システム管理者又は情報セキュリティ管理者については、概ね「研修に参加したことがある」との回答であった。

また、職員に対するアンケート調査では、「過去、情報セキュリティに関する研修又は訓練を受けたことはあるか。」との質問については、「はい」が９４％、「いいえ」が５％であった。

【意　見】

職員に対する情報セキュリティの周知については、情報セキュリティ研修などを通じて、適宜行われていた。

研修に関しては、必要に応じて職員に対するアンケートを実施するなど、効果的な研修の実施に努められたい。

②　非常勤嘱託職員及び臨時職員採用時における情報セキュリティポリシーの遵守すべき内容の周知

【監査結果】

非常勤嘱託職員及び臨時職員採用時における情報セキュリティポリシーの遵守すべき内容の周知の状況は、次のとおりであった。

なお、集計にあたり、「該当職員なし」と回答した３９所属は除いた。

・周知している	１５７所属
・周知していない	８所属
・周知している場合と周知していない場合がある。	４所属
・その他	１２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、周知方法としては、採用の際に説明する、研修の機会を利用する等であった。

【意　見】

情報セキュリティを確保するためには、非常勤嘱託職員や臨時職員を含めた職員全体が情報セキュリティ対策の必要性や内容を十分に理解し実践することが不可欠である。

情報セキュリティポリシーの周知方法として、研修の機会を利用して周知している場合もあったが、採用から研修を受講するまでの間、情報セキュリティが確保されないおそれも考えられる。情報セキュリティ管理者は、情報資産の取り扱いや安全性の確保のためにも、県の基本方針や対策基準及び実施手順のうち遵守すべき内容について、非常勤嘱託職員や臨時職員の採用の際に周知されたい。

（4）パソコン等関連物品の管理は適正か。

ア　所属管理パソコンの管理の徹底を図るべきもの

①　所属管理パソコンの有無

【監査結果】

所属管理パソコンとは、各所属において調達し、管理している一人一台パソコン以外のパソコンである。

各所属における所属管理パソコンの有無は次のとおりであった。

・あり	１５３所属
・なし	４７所属
・その他	２０所属

※「その他」には、課内室である７所属等が含まれる。

所属管理パソコンについて「あり」と回答した１５３所属のうち、スタンドアロンで使用しているものが「あり」と回答した所属が９４所属、「なし」と回答した所属が５９

所属であった。（スタンドアロンとは、コンピュータをネットワークと接続せずに単独で動作させているもの）

実地監査したところ、パソコンをスタンドアロンで使用している所属においては、データの集計作業や印刷物の作成、機器の制御、写真の管理など、様々な用途に使用されていた。

【意　見】

所属管理パソコンのうちスタンドアロンで使用しているパソコンについては、ネットワークに接続されていないため、外部への情報漏洩のおそれが少ないともいえるが、機密情報などを保存している場合も考えられるため、盗難防止など適切な管理に努められたい。

② 所属管理パソコンのうち、現在使用していないもの（修理等の予備用を含む。）の有無

【監査結果】

県の対策基準において、情報資産管理責任者は、不要となった情報資産を廃棄する場合には、無意味なデータを上書きし又は当該記録媒体を物理的に破壊して媒体上の情報の復元が完全に不可能な状態にした上で廃棄しなければならないとされている。

所属管理パソコンのうち、現在使用していないもの（修理等の予備用を含む。）の有無は次のとおりであった。

・あり　６７所属
・なし　８５所属
・不明　１所属

実地監査したところ、現在使用されていないパソコンの中には、内部データの登録状況が不明確なものや、内部データの消去方法がわからないまま保管されているものがあった。また、保管場所が適切でなく、盗難等のリスクがあるものがあった。

【意　見】

現在使用していないパソコンについては、資産の有効活用の観点から、別の業務へ転用をはかることや、今後使用見込みのないものについては、必要なデータを引き継いだうえで、県の対策基準に沿った方法により内部データを消去し、処分について検討していく必要がある。

イ　ソフトウェアの管理方法について検討を要するもの

ソフトウェアの管理方法について、平成２２年度におけるソフトウェアの調達実績、ライセンス証書等の保管状況及びソフトウェアをパソコン端末にインストールする場合の手続きは、次のとおりであった。

a. 平成２２年度におけるソフトウェアの調達実績の有無

【監査結果】

平成２２年度におけるソフトウェアの調達実績の状況は次のとおりであった。

・実績あり　７２所属
・実績なし　１２７所属
・その他　２１所属

※「その他」には、課内室である７所属等が含まれる。

b. 平成２２年度におけるソフトウェアの調達形態別の調達状況

【監査結果】

平成２２年度におけるソフトウェアの調達形態別の調達所属数及び調達件数は次のとおりであった。

調達形態	支出科目	調達所属数	調達件数
ＣＤ－ＲＯＭ等記憶媒体を購入	需用費	27	258
	備品購入費	24	115
パソコン本体にインストール済みの状態で購入	備品購入費	16	94
パソコン本体にインストール済みの状態で賃借	使用料及び賃借料	8	11
使用許諾契約による複製による調達	使用料及び賃借料	2	2
バージョンアップ（ＣＤ－ＲＯＭ等記憶媒体を購入）	需用費	5	41
	備品購入費	5	13
バージョンアップ（インターネット等から直接ダウンロード）	役務費	3	37
ＣＤ－ＲＯＭ等による定期刊行物の購入	需用費	2	24
ＣＤ－ＲＯＭの法令集追録等の購入	需用費	1	1
	備品購入費	0	0
	使用料及び賃借料	1	1
その他		7	389
計		101	986

※　「その他」には、使用許諾契約による複製による調達（需用費・備品購入費）の375件などが含まれる。なお、一所属において複数の調達形態により調達している所属があるため、「調達所属数」が、ａで「実績あり」と回答した所属数と異なる。

c. 平成２２年度に調達したソフトウェアについて、ライセンス証書、使用許諾書、契約書等の保管状況

【監査結果】

調達したソフトウェアについて、ライセンス証書、使用許諾書、契約書等の保管状況

は、次のとおりであった。

・全てのソフトウェアについて保管している　３７所属
・原則保管している　３３所属
・保管していない　２所属

d. 平成２２年度におけるソフトウェアをパソコン端末にインストールする場合の手続き

【監査結果】

県の対策基準において、①情報システム管理者は、所管する情報システムについて標準実装としてインストールするべきソフトウェアを確定するものとする、②原則として、標準実装以外のソフトウェアを端末へインストールしてはならない。業務上の必要からやむを得ず標準実装以外のソフトウェアを端末へインストールする場合は、事前に情報システム管理者及びネットワーク管理者の許可を受けなければならないとされている。

ソフトウェアをパソコン端末にインストールする場合の手続きの状況は、次のとおりであった。

・情報システム管理者の許可を得ている　６２所属
・許可を得ていないものがある　９所属
・不明　１所属

一人一台パソコンについては、平成１６年から、職員がソフトウェアを自由にインストールできないよう、一元的に管理できる仕組みを整備しており、ソフトウェアのインストールにあたっては、情報政策課への書面による申請と許可が必要となっている。

また、本庁の情報システム所管課（情報政策課以外）で調達され、各出先機関等に配置されたパソコンについては、導入当初は個別に管理されていたものもあったが、パソコン端末の更新等に伴い、順次本庁による一元的な管理に移行してきている。

一方、各所属で管理しているパソコンの中には、各所属で所管する情報システムにおいて使用している専用端末（情報政策課で管理しているものを除く。）や、各所属で調達し管理しているパソコン、スタンドアロンで使用しているパソコンなど多数あるところであり、これらの所属管理パソコンについては、一部の端末を除き、ソフトウェアのインストールについては、それぞれの所属で管理されている。

【意　見】

ソフトウェアについては、調達形態が様々であり、県の財務規則に定める物品の管理の対象とならない場合もあり、管理方法も多様である。

しかし、ソフトウェアは著作物であり、著作権により保護されているため、ソフトウェアの使用にあたっては、ライセンス証書や使用許諾書など契約に定められた範囲内で正しく使用しなければならない。

各所属で管理しているパソコンにソフトウェアをインストールする場合に、情報システム管理者の許可を得ていないものがあったので、許可を得るとともに、職員は、ソフトウェアの適正な取り扱いに努められたい。

また、ソフトウェアのライセンス証書や使用許諾書、その他のライセンスを有することを証明できるもの、オリジナルディスクの保管についても、適切に管理されたい。

本庁の情報システム所管課（情報政策課以外）で調達され、各出先機関等に配置されたパソコンについては、本庁の所管課は、ソフトウェアをインストールする場合の手続きについて周知するなど、管理の徹底を図られたい。

教育委員会においては、「教職員一人一台パソコン（ハイユースパソコン）等管理要領」において、ハイユースパソコンにソフトウェアをインストールする場合の条件等が定められているので、この条件を遵守するとともに、要領の適切な運用に努められたい。

2　総括的な意見

今回の監査では、情報セキュリティ対策を推進・管理する体制の整備や情報セキュリティ基本方針等に定められた情報セキュリティ対策の遵守の状況、パソコン等関連物品の管理状況等について監査を行ったが、監査を通しての総括的な意見は次のとおりである。

（1）情報セキュリティを推進・管理する体制については、情報セキュリティ監査で指摘されたセキュリティ上の不備が未改善であるものがあったので、対策の優先順位を定め、改善に努められたい。また、教育委員会においては、監査体制を整備し、定期的に監査を実施されたい。

（2）情報セキュリティ基本方針等に定められた情報セキュリティ対策の遵守の状況については、所管する情報システムについて、情報資産が分類されていないものや、情報資産の重要性に応じた取り扱いが決定されていないものがあったので、県の対策基準に基づき、実施手順を作成し、情報資産の分類と取り扱いを決定されたい。

（3）システムの運用停止が業務等に及ぼす影響が大きい情報システムについては、運用停止を回避するための対策が講じられていないものがあったので、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、県の対策基準に基づき、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。

（4）情報システムの運用・保守の外部委託契約等については、契約書や外部委託先からの報告に関して、情報セキュリティ対策が不十分なものがあったので、情報資産の安全性を確

保するため、県の対策基準や、「外部委託に係る情報セキュリティ対策基準」に基づいた委託契約を行うなど情報セキュリティ対策を講じられたい。

（5）ソフトウェアの管理については、各所属で所管する情報システムにおいて使用している専用端末（情報政策課で管理しているものを除く。）や、各所属で調達し管理しているパソコンにソフトウェアをインストールする場合について、県の対策基準に沿った取り扱いとなっていないものがあったので、県の対策基準を遵守するとともに、職員はソフトウェアの適正な取り扱いに努められたい。

発行者　山梨県　甲府市丸の内一丁目六番一号　印刷所　㈱サンニチ印刷　甲府市北口二丁目六番