第１　監査のテーマと趣旨

１　監査のテーマ

「情報セキュリティ対策について」

２　監査の趣旨

情報システムの利用拡大に伴い、事務処理の効率化が進む一方で、事故の未然防止等、セキュリティ上の対策も重要な課題となっている。

本県においても、情報セキュリティの推進を図るため、平成１５年６月に「山梨県情報セキュリティ基本方針」及び「山梨県情報セキュリティ対策基準」が制定されている。

そこで、本県において、「山梨県情報セキュリティ基本方針」や「山梨県情報セキュリティ対策基準」に基づいた情報セキュリティ対策が適切に実施されているか等の観点から、今後の情報セキュリティ対策の改善に資することを目的として監査を実施するものである。

第２　監査の実施状況

１　監査の実施期間

平成２３年８月１２日から平成２４年１月２４日まで

２　監査対象期間

原則として平成２２年度（ただし、必要に応じて平成２１年度以前も対象とする。）

３　監査の着眼点

（１）情報セキュリティ対策を推進、管理する体制は整備されているか。
（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が遵守されているか。
（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。
（４）パソコン等関連物品の管理は適正か。

４　監査の対象及び対象所属

（１）監査の対象

監査対象所属が平成２２年度に実施（継続を含む）した、情報セキュリティ対策のための取り組み。

（２）監査対象所属

知事部局、企業局、議会事務局、教育委員会、各行政委員会事務局、警察本部の各所属（合計２５９所属）

５　監査の方法

（１）山梨県情報セキュリティ基本方針の対象となる知事部局、企業局、議会事務局、教育委員会、各行政委員会事務局の合計２２０所属については、山梨県情報セキュリティ基本方針等の実施状況を調査するための行政監査調査票（以下「調査票」という。）を作成し、県のセキュリティ対策について監査した。

調査票では、各所属における情報セキュリティ対策を監査するとともに、各所属が所管する情報システムのうちから１１０システムを抽出し、情報システムごとの情報セキュリティ対策の状況を監査した。抽出にあたっては、情報システムの目的や情報システムで取り扱っている情報の重要性等を考慮した。

（２）（１）の２２０所属のうち、５２所属を抽出して実地監査を行った。抽出にあたっては、調査票の回答状況等を考慮した。

（３）教育委員会については、山梨県教育委員会情報セキュリティ基本方針の対象でもあるため、（１）の調査票による調査と並行して、実地監査において、教育委員会の情報セキュリティ対策についても監査した。

（４）すべての監査対象所属について、職員の情報セキュリティに対する意識や行動の状況を把握するため、各所属において無作為に抽出した職員１名について、アンケート調査を実施した。

（５）警察本部の３９所属については、警察独自の規定により情報セキュリティ対策を実施しているため、（１）の調査票による調査の対象外であることから、（４）と同様な方法により、アンケート調査のみを実施した。

（６）県及び教育委員会の情報セキュリティ対策の所管課に対して聞き取りを行った。

［実地監査対象所属］

ア　知事部局及び企業局（４１所属）

県民生活・男女参画課、生涯学習文化課、管財課、私学文書課、市町村課、消防防災課、児童家庭課、健康増進課、大気水質保全課、治山林道課、農村振興課、畜産課、耕地課、技術管理課、砂防課、都市計画課、出納局管理課、企業局総務課、峡東地域県民センター、富士・東部地域県民センター、中北保健福祉事務所（本所）、峡東保健福祉事務所、峡南保健福祉事務所、中央児童相談所、都留児童相談所、甲陽学園、障害者相談所、あけぼの医療福祉センター、育精福祉センター、峡南林務環境事務所、富士・東部林務環境事務所、山梨県工業技術センター、山梨県富士工業技術センター、宝石美術専門学校、産業技術短期大学校、峡東農務事務所、東部家畜保健衛生所、酪農試験場、

専門学校農業大学校、中北建設事務所（本所）、富士・東部建設事務所（本所）

イ　教育委員会（１１所属）

スポーツ健康課、図書館、博物館、総合教育センター、甲府城西高等学校、増穂商業高等学校、身延高等学校、上野原高等学校、吉田高等学校、ひばりが丘高等学校、盲学校

［県及び教育委員会の情報セキュリティ対策の所管課］

情報政策課、高校教育課

第３　情報セキュリティ対策の概要

１　情報セキュリティの概要

（１）情報セキュリティ対策とは

自治体や企業などの組織体で使用する情報は、大多数が情報システムに蓄積・管理されたデータとして存在している。

情報システムの信頼性・安全性を確保することが、自治体や企業の活動を円滑に遂行するための主要な前提条件となる。

このような情報システムの安全性の確保のための諸施策が情報セキュリティ対策であり、この諸施策は、情報システムの企画・開発、運用・保守、廃棄・廃止の各段階において必要なものである。

（２）情報セキュリティポリシーとは

ア　脅威とリスク

情報セキュリティに関する阻害要因を脅威といい、脅威により情報資産に対して被害を及ぼす可能性のことをリスクという。

情報セキュリティ対策を講じるために検討されなければならない脅威としては、次のようなものが考えられる。

・情報の漏洩や改ざん、破壊
・災害、停電、回線の障害などによるシステムの停止
・データの入力ミスやソフトウェア自体のエラーなどによるシステムの誤処理

これらは、いわゆる「情報セキュリティ対策の三要素」といわれる次の要素に反する事態が発生することを意味するものである。

・機密性　情報資産が正当な使用者に対してのみ、適切な手段で利用される状態
・完全性　情報資産が破壊、改ざん又は消去されていない状態
・可用性　情報資産が必要とされているときに、正当な使用者が適切な手段で使用できる状態

イ　情報セキュリティポリシーの意義

リスクを低減するためには、予防、発見及び復旧の３つの対策が考えられる。

具体的には、災害等の影響の少ない場所への情報システムの設置、組織体制の確立、教育・訓練等による情報セキュリティ対策の周知徹底、さらには不正アクセスやコンピュータウィルスへの対策等が考えられる。

また、自己点検や監査によってリスクを適切に評価しているか、評価結果に基づいて必要な対策が講じられているか、検証していくことも重要である。

これらの情報システム等に対するリスクに応じたセキュリティ対策に関する基準や手順を定めたものが、情報セキュリティポリシーといわれる。

２　山梨県における情報セキュリティ対策

（１）情報セキュリティポリシーの構成

山梨県においては、平成１５年６月、情報セキュリティポリシーが定められたが、その内容は、山梨県の情報セキュリティに関する統一的かつ基本的な方針である「山梨県情報セキュリティ基本方針」（以下「県の基本方針」という。）及び、その基本方針を実行に移すための具体的な対策として、情報セキュリティ対策を実施するにあたっての遵守すべき事項や判断等の基本的な基準を定めた「山梨県情報セキュリティ対策基準」（以下「県の対策基準」という。）によって構成されている。また、情報セキュリティポリシーに基づき、個々の情報システムごとの具体的な情報セキュリティ対策の実施手順を記述した「情報セキュリティ実施手順」（以下「実施手順」という。）が作成されている。

（２）情報セキュリティ対策の内容

県の基本方針において、情報セキュリティ対策として次の４つが規定されている。

ア　人的情報セキュリティ対策

情報セキュリティに関する権限や責任及び遵守すべき事項を定め、職員等に対する周知及び徹底を図るとともに、十分な教育啓発が行われるよう必要な人的対策を講ずる。

イ　物理的情報セキュリティ対策

情報資産を有する施設への不正な立入り、損傷、盗難等の事故及び災害から情報資産を保護するための物理的な対策を講ずる。

ウ　技術的情報セキュリティ対策

情報資産を不正アクセス等やウィルスから保護するため、情報資産へのアクセス制御、ウィルス対策等の技術的対策を講ずる。

エ　運用による情報セキュリティ対策

情報資産の管理、セキュリティ対策の遵守状況の確認、緊急事態発生時の危機管理対策等、セキュリティ対策の運用面の対策を講ずる。

（3）情報セキュリティ向上に向けた取り組み

ア　組織体制

県の情報セキュリティ管理を統括している最高情報統括責任者（知事）のもと、各所属長は、情報セキュリティ管理者として、当該所属の情報セキュリティを管理するとともに、情報資産管理責任者として、各所属で保有する情報資産を管理することとされている。

また、各情報システムを所管する所属長は、情報システム管理者とされ、各ネットワークを管理する所属長は、ネットワーク管理者とされている。

情報セキュリティポリシーの運用支援、評価、見直し等を行い、県の情報セキュリティの一層の向上を図るため、情報セキュリティ委員会が設置されている。

イ　職員への情報セキュリティ教育

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。平成２２年度における研修の実施状況は次のとおりである。

新任職員研修	対象 内容	新任職員 情報セキュリティ対策の必要性 情報セキュリティポリシー 情報セキュリティの確保とこれに対する脅威 パソコンの利用
臨時職員等に対する情報セキュリティ研修 （職場研修）	対象 内容	臨時職員、非常勤嘱託職員等 パソコンで業務を処理する際の遵守事項 電子メール、インターネット、パスワード管理、ウィルス対策等
個人情報保護・情報セキュリティ説明会 （私学文書課と合同開催）	対象 内容	総括課長補佐、出先次長 情報セキュリティ対策等 情報セキュリティ対策と職場研修の実施 情報漏えい発生時の対応
PCリーダー研修	対象 内容	各所属PCリーダー 情報セキュリティに関わる現状 情報セキュリティに関わる県の諸規定 情報セキュリティ職場研修の実施、点検 情報システムの適正な運用 一人一台パソコン機器等の利用
情報セキュリティ研修 （職場研修）	対象 内容	全所属 情報セキュリティポリシーの概要 職員の遵守事項 Winnyを知る（情報流出の仕組み） メール利用時の情報流出の防止 ファイルの暗号化・圧縮 ファイルへのパスワード設定
ｅラーニングによる情報セキュリティ研修	対象 内容	PCリーダー、職場研修指導者、新任職員、情報システム職員、希望者 地方自治情報センター主催のｅラーニングを受講
Webサーバ等公開系システム管理者向け研修	対象 内容	公開系サーバ管理担当職員（庁内及び市町村） 講師：　地方自治情報センター Web感染型マルウェアとは マルウェアから身を守るために必要なこと Web感染型マルウェア検知事業の紹介 講師：　山梨県警サイバー犯罪係 サイバー犯罪の最近の傾向 万が一の場合の対処・連絡方法

ウ　監査及び自己点検

県の基本方針において、情報セキュリティが確保されていることを確認するために、定期的又は必要に応じて情報セキュリティ監査及び自己点検を行うと規定されている。

情報政策課は、平成１８年度より、情報セキュリティに関する内部監査を実施している。

エ　評価及び見直し

県の基本方針において、情報セキュリティの検証の結果等に基づき、情報セキュリティの状況を評価するとともに、情報セキュリティを取り巻く状況の変化に対応するため、必要に応じて、基本方針、対策基準及び実施手順の見直しを実施すると規定されている。

オ　情報セキュリティ関連規定

本県においては、県の対策基準のほか、情報セキュリティに関連する主な規定として、次のようなものがある。

・インターネット利用基準
・電子メール利用基準
・不正プログラム対策基準
・パスワード設定管理基準
・外部委託に係る情報セキュリティ対策基準
・標準ソフトウェアで作成、保存された情報資産の持出し・転送許可の取扱基準
・山梨県情報セキュリティ内部監査実施要領
・山梨県施設管理要領

カ　情報セキュリティに関する注意喚起

過去、本県において、ファイル交換ソフトＷｉｎｎｙ（ウィニー）を通じての個人情報の流出や、個人情報が記録された外部記録媒体（ＵＳＢメモリー）の紛失等の事例があり、情報政策課より、個人情報を含む情報資産の適切な管理について徹底するよう、情報セキュリティに関する注意喚起がなされた。

3　教育委員会における情報セキュリティ対策

教育委員会は、県の基本方針及び対策基準とは別に、情報セキュリティ対策に関する独自の規定を設けている。

教育委員会においては、平成１８年度、県立学校の教職員用一人一台パソコン等が更新され、県立学校教育イントラネットが山梨県情報ハイウェイに接続され、学校間の回線通信速度が高速化されるなど、県立学校のＩＣＴ教育環境がリニューアルされたことに伴い、それまで運営されていた山梨県教育情報ネットワークの運営管理要綱や山梨県ハイユースパソコン等管理要綱等の全体的な見直しが必要となった。

平成１９年度より、教育委員会の要綱改訂やセキュリティポリシーについて検討を行い、平成２１年４月に「山梨県教育委員会情報セキュリティ基本方針」（以下、「教育委員会の基本方針」という。）を、また「山梨県教育委員会情報セキュリティ対策基準」（以下「教育委員会の対策基準」という。）を制定し、情報セキュリティの確保について徹底を図っている。

第４　監査結果及び意見

１　監査の着眼点ごとにみた監査結果及び意見

第２の３「監査の着眼点」の項目ごとにみた監査結果及び意見は、次のとおりである。

（１）情報セキュリティ対策を推進、管理する体制は整備されているか。

ア　情報セキュリティ確保に向けたマネジメントシステムの定着を図るべきもの

①　情報セキュリティ監査の実施状況

【監査結果】

県の基本方針において、情報セキュリティが確保されていることを確認するために、定期的又は必要に応じて情報セキュリティ監査を行うこととされている。

監査対象とした１１０システムについて、情報セキュリティ監査の実施状況は次のとおりであった。

・実施され、指示事項なし　３システム
・実施され、指示事項あり　２１システム
・実施されていない（今後実施予定を含む）　７９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システム等が含まれる。

情報セキュリティ監査について、「実施され、指示事項あり」と回答した２１システムのうち、「すべて改善している」と回答したものは９システム、「一部改善している」と回答したものは１２システム、「改善していない」と回答したものはなかった。

実地監査したところ、情報政策課においては、平成１８年度より、情報セキュリティ監査を順次実施しており、現在、監査が実施されていない情報システムについても、今後、県の基本方針に沿って、定期的又は必要に応じて情報セキュリティ監査を実施していくとのことであった。

教育委員会においては、教育委員会の基本方針において、情報セキュリティが確保されていることを確認するために、定期的に監査を行うこととされているが、監査が実施されていなかった。

なお、教育委員会の対策基準において、情報セキュリティ委員会を設置することとされているが、実際は、これに代わるものとして、ハイユースＰＣ定例会など個別の定例会により運営管理が行われていた。

【意　見】

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（サーバ室の入退室管理が不十分、外部記録媒体の保管場所が不適切、障害記録の保管の不徹底、セキュリティパッチの適用の未実施等）は、事故の原因となる可能性もあることから、対策の優先順位を定め、改善に努められたい。

教育委員会においては、教育委員会の基本方針に基づき、定期的に監査を実施されたい。また、情報セキュリティ委員会として実施すべき事項については、委員会を適宜開催するなど、教育委員会の対策基準に沿った運営に努められたい。

②　情報セキュリティの自己点検の実施状況

【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及びネットワークについて、定期的に又は必要に応じて自己点検を実施することとされている。

情報セキュリティの自己点検の実施状況は次のとおりであった。

・点検を実施している　１０７システム
・点検を実施していない　３システム

※数値は、平成 19 年度から平成 22 年度までの情報セキュリティの自己点検実施状況の集計

【意　見】

情報セキュリティ対策は、対策基準等の策定（Ｐｌａｎ）、実践（Ｄｏ）、評価（Ｃｈｅｃｋ）、改善（Ａｃｔｉｏｎ）のマネジメントサイクルを定着させることによって、その水準の向上が図られるものである。

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等について、今後も引き続き情報セキュリティマネジメントサイクルを行い、定期的又は必要に応じて自己点検を実施し、管理体制の強化に努められたい。

（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が遵守されているか。

ア　情報資産の分類と取り扱いについて改善を要するもの

①　重要な情報資産の分類と取り扱い

【監査結果】

県の基本方針によると、「情報資産」とは、

・ネットワーク、情報システム及びこれらに関する設備並びに電磁的記録媒体
・ネットワーク及び情報システムで取り扱う情報（これを印刷した文書を含む。）
・ネットワーク及び情報システムに関連する文書

とされている。

「重要な情報資産」とは、機密性、完全性及び可用性の観点から、重要性が高いと分類された情報資産をいい、個人情報及び業務上必要とする最小限の者のみが扱うべき情報資産、公開することを予定していない情報又は業務上重要な情報資産などが県の対策基準の中で例示されている。情報資産のリスク分析を行うためには、その対象となる情報資産を特定する必要がある。

また、情報システム管理者は、情報資産の整理を行い、各所属が所管する情報システムについて作成する実施手順において、情報資産を分類のうえ、取り扱いを決定することとされている。

重要な情報資産の分類と取り扱いの状況は次のとおりであった。

・重要な情報資産を分類し、取り扱いを決定している	５８システム
・重要な情報資産を分類していない	１３システム
・重要な情報資産を取り扱っていない	３４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県以外（国及び独立行政法人）である３システム等が含まれる。

「重要な情報資産を分類していない」と回答した１３システムのうち、実施手順を作成していない情報システムは８システムあった。

【意　見】

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、情報資産の分類と取り扱いを決定していない情報システムについては、情報資産のリスク分析とその対象となる情報資産を特定するためにも、情報資産を分類のうえ、取り扱いを決定する必要がある。

情報システム管理者は、各所属が所管する情報システムについて、実施手順を作成し、その中で、具体的な情報資産の分類と取り扱いについて決定されたい。

②　重要な情報資産の廃棄方法

【監査結果】

調査票による調査を実施した２２０所属について、重要な情報資産の廃棄方法は、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７２所属は除いた。

・職員が行っている	７９所属
・他の管理担当部局に依頼している	１０所属
・外部委託している	２１所属
・その他	３８所属

※「その他」には、廃棄実績のない１０所属等が含まれる。

「外部委託している」と回答した２１所属のうち、「回収・処分業者と契約書等の書面により秘密保持を明確にしている」と回答した所属は１６所属で、「契約書等の書面によらず口頭により指示している」と回答した所属は５所属であった。

実地監査したところ、情報システム等で取り扱う重要な情報を印刷した文書の廃棄については、本庁においては、一括して外部委託しており、出先機関においては、外部委託しているものや、他所属に依頼しているもの、職員自らがごみ焼却施設に赴き直接焼却処分しているものがあった。

また、重要性の高い情報を記録した記録媒体の廃棄については、本庁においては、各職員が記録媒体を物理的に破壊したうえで、一括して外部委託しており、出先機関においては、外部委託しているものや、各職員が記録媒体を物理的に破壊したうえで、他所属に依頼し、指定された場所に廃棄しているものがあった。

アンケート調査によると、「重要な情報資産を保存している機器や記録媒体を廃棄等する場合、情報を消去の上、復元できないようにしているか。（物理的な破壊やデータ