参考資料1

仙台市情報セキュリティ対策
改善取組報告書
（概要版）

平成26年度

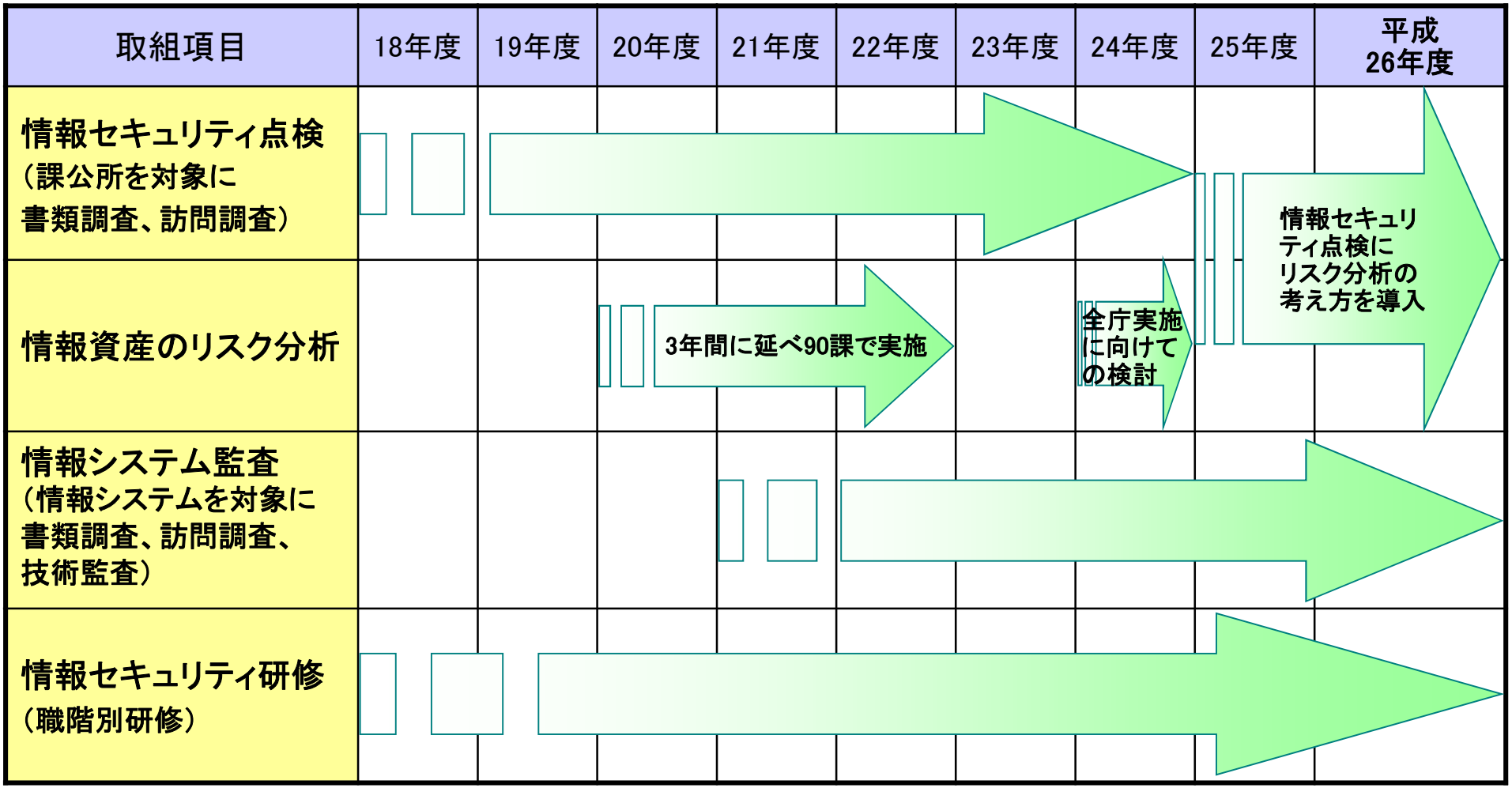
情報システム監査株式会社

目次

1．平成26年度の取組みと経緯

（1）取組みと経緯

仙台市では、平成18年度から情報セキュリティへの取組みを、4つのカテゴリー（情報セキュリティ点検、情報資産のリスク分析、情報システム監査、情報セキュリティ研修）で推進してきました。
平成25年度からは、情報セキュリティ点検にリスク分析の考え方を取入れることにより、リスク分析を全庁的な取組みとしています。これまでの取組みと経緯を、以下に示します。



（2）平成26年度の取組み内容

【情報セキュリティ点検】 **平成26年7月～平成27年3月 全庁422課を対象として実施**

（書類調査）

情報セキュリティポリシーの掲げる項目を遵守しているかどうかを点検・評価しました。

・セキュリティマネジメント点検（人的マネジメントについての点検）

・リスク対策状況点検（各課で保有する情報資産の取扱いにおけるリスク対策状況の評価）

（訪問調査）

書類調査結果と実態が合っているかを確認し、優良事例や新たな課題を収集しました。

【情報システム監査】 **平成26年6月～平成27年3月 68システムを対象として実施**

（書類調査・訪問調査）

システムの運用管理に係る情報セキュリティ対策状況が、情報セキュリティポリシーの掲げる項目を遵守しているかどうかを調査しました。

（技術監査）

診断ツール等により、システム設定等における情報セキュリティのぜい弱性を診断しました。

【情報セキュリティ研修】 **平成26年5月～平成26年10月　計14回開催**

情報セキュリティ対策を実施するために、職階別の対応事項等をまとめて研修を実施しました。

（局(区)情報管理者研修） 1回開催 28名受講

（情報管理者研修） **講義コース**：4回開催 167名受講　**演習コース**：4回開催 67名受講

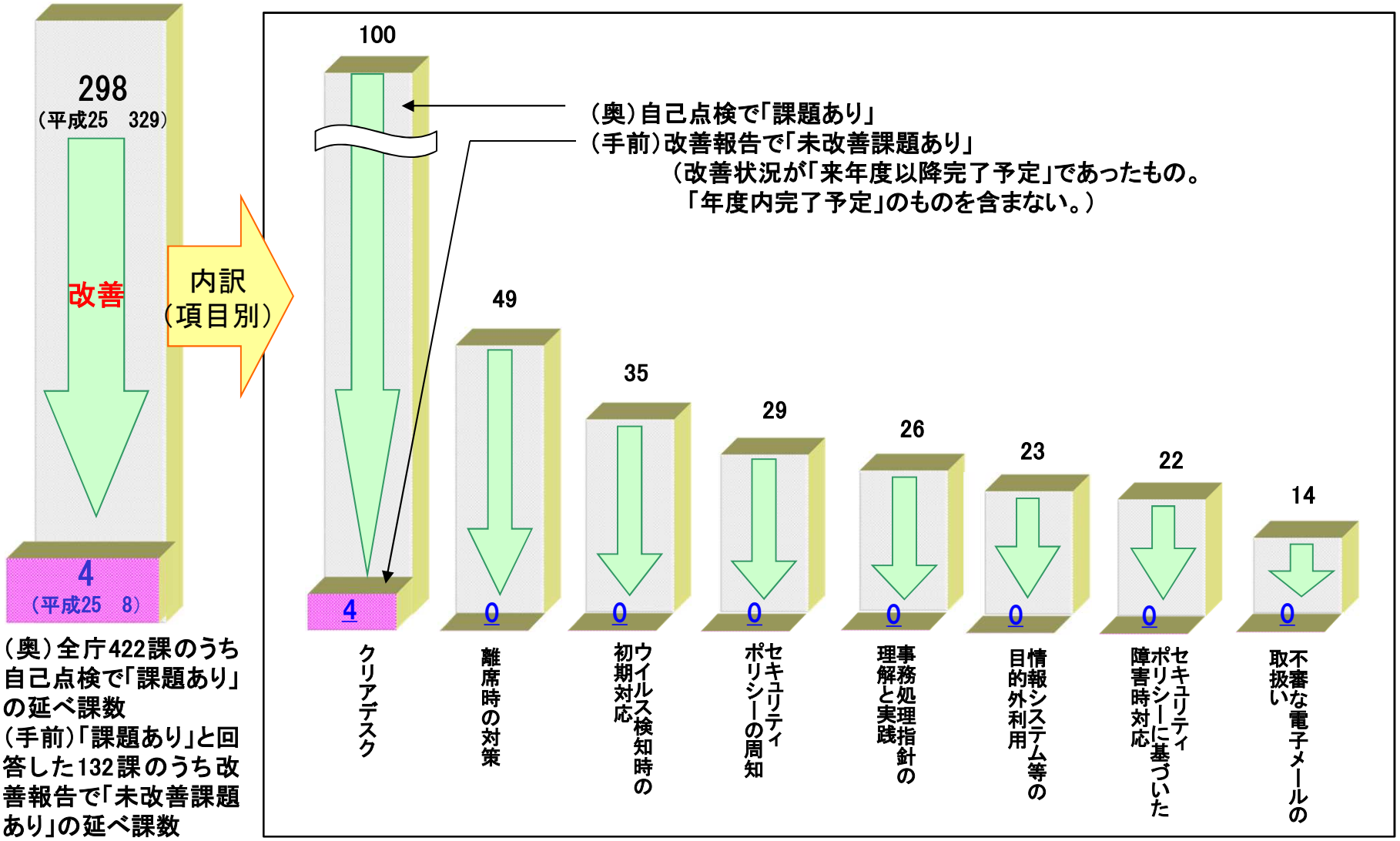
（一般職員研修） **基礎編**：3回開催 271名受講　**応用編**：2回開催 109名受講

情報セキュリティの確保

2. 情報セキュリティ点検

（1）セキュリティマネジメント点検結果（課題の改善状況）

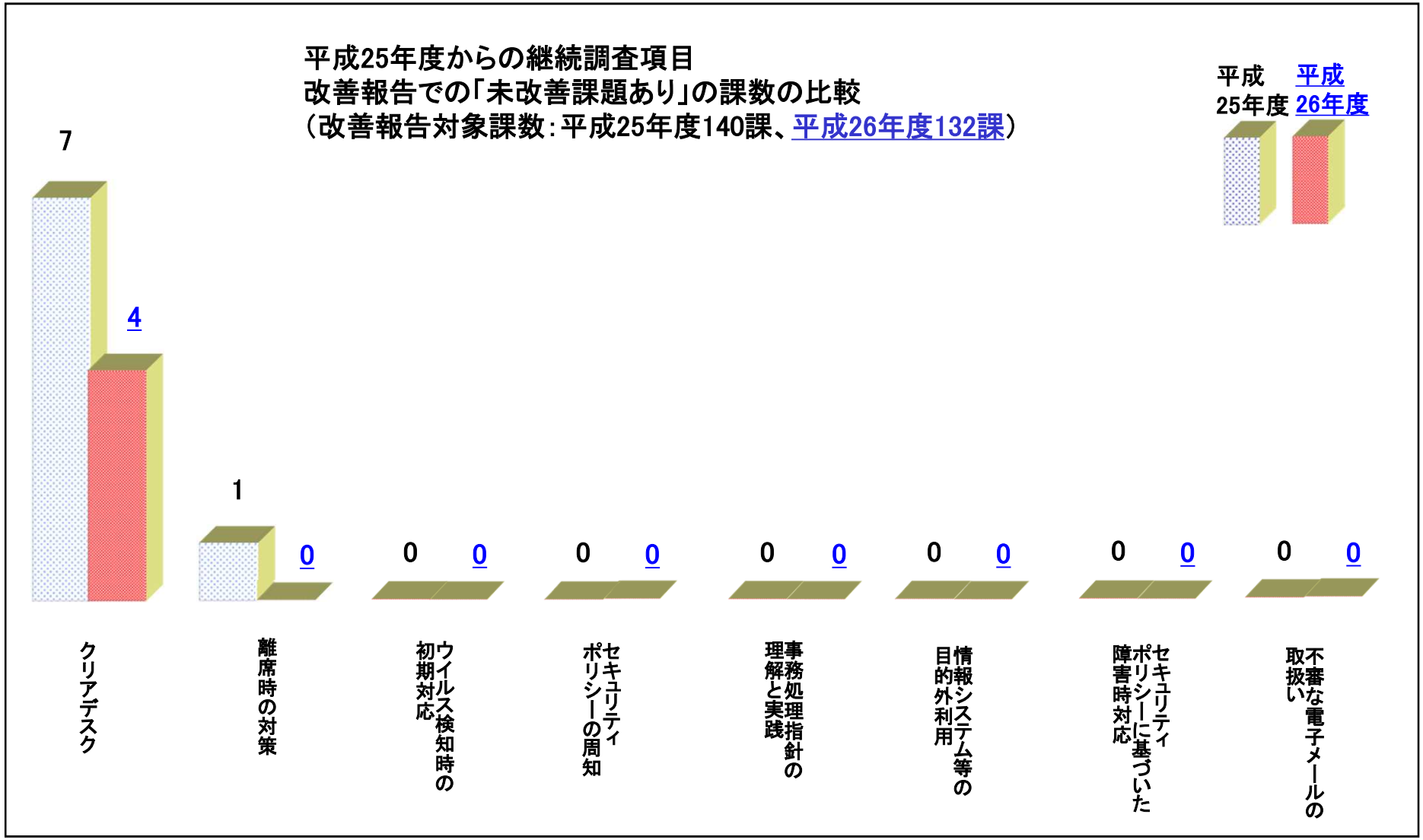
セキュリティマネジメント点検の結果、自己点検で検出された課題は速やかに改善されています。
また、課題ありの延べ課数及び未改善課題の延べ課数は、平成25年度より減少しています。



（奥）全庁422課のうち自己点検で「課題あり」の延べ課数
（手前）「課題あり」と回答した132課のうち改善報告で「未改善課題あり」の延べ課数

（2）セキュリティマネジメント点検における未改善課題ありの課数（平成25年度との比較）

各課が課題の改善に取組んだ結果、未改善課題が残った課は極めて少なく、
全庁レベルで情報セキュリティ対策におけるマネジメントが十分機能していると考えます。



（3）リスク対策状況点検結果（主要な情報資産の保有状況）

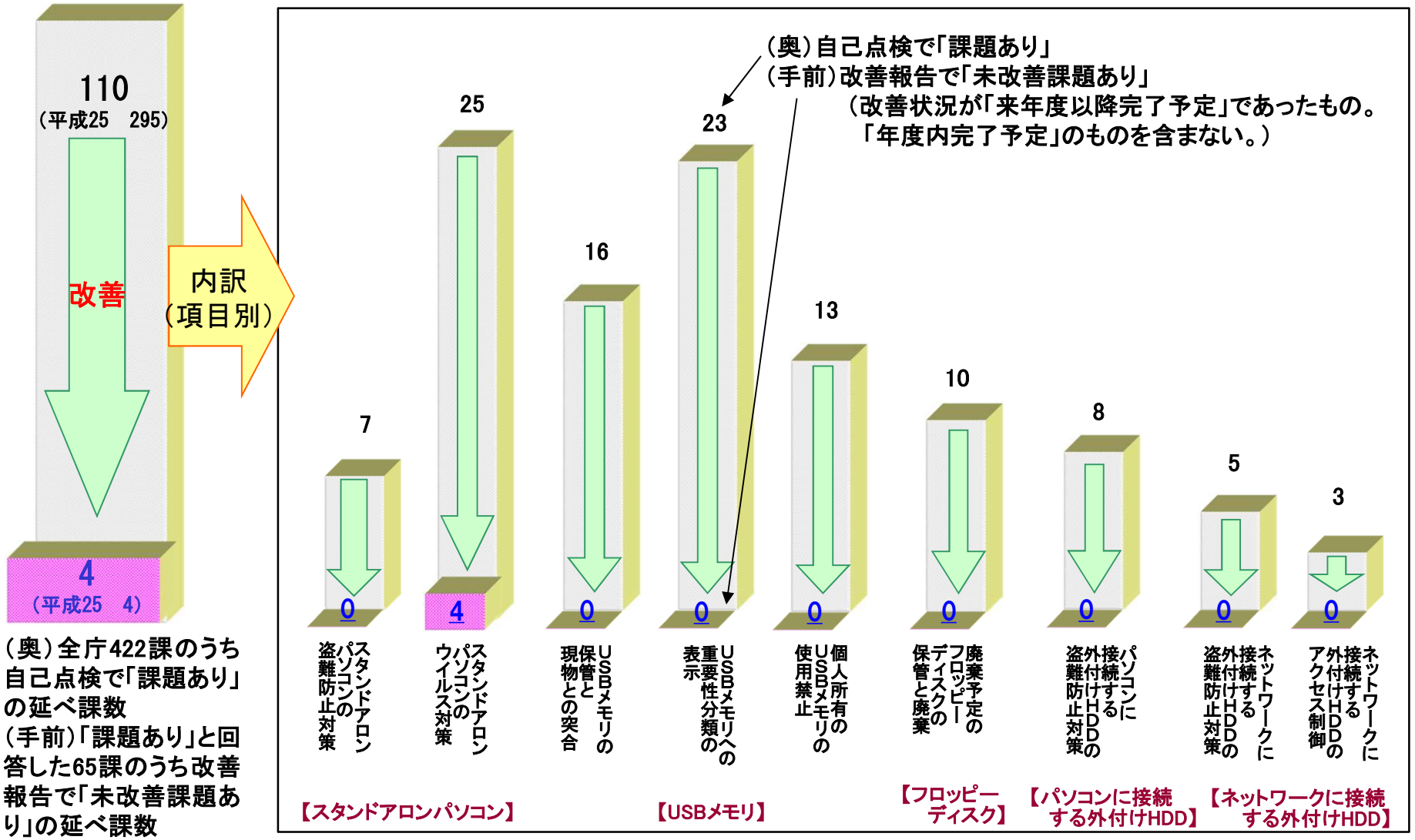
各課における主要な情報資産の保有状況と主な用途を調査しました。
また、各課が保有するスタンドアロンのパソコン、USBメモリ、フロッピーディスク、
外付けハードディスク（パソコンに接続するタイプ及びネットワークに接続するタイプ）について、
想定されるリスクへの対策状況の自己点検を実施しました。

No.	情報資産名	平成25年度					平成26年度				
		課数		保有率※	保有数	平均保有数	課数		保有率※	保有数	平均保有数
		有	無				有	無			
1	スタンドアロンのパソコン	282	140	67%	1,114	4.0	280	142	66%	1,150	4.1
2	USBメモリ	366	56	87%	4,262	11.6	386	36	91%	4,438	11.5
3	フロッピーディスク	159	263	38%	5,175	32.5	105	316	25%	4,000	38.1
4	MOメディア	125	297	30%	2,486	19.9	111	309	26%	2,208	19.9
5	デジタルカメラ	356	66	84%	1,058	3.0	363	59	86%	1,085	3.0
6	メモリカード（デジカメ用）	332	90	79%	1,196	3.6	347	75	82%	1,238	3.6
7	パソコンに接続するタイプの外付けハードディスク	179	243	42%	457	2.6	208	214	49%	552	2.7
8	ネットワークに接続するタイプの外付けハードディスク	83	339	20%	148	1.8	91	331	22%	155	1.7
9	携帯電話	146	276	35%	633	4.3	156	266	37%	663	4.3
10	スマートフォン	5	417	1%	34	6.8	15	407	4%	52	3.5
11	タブレット型端末	11	411	3%	42	3.8	23	399	5%	72	3.1

※　本表の「保有率」は、リスク対策状況点検対象課数（422課）を分母とした比率です。

（4）リスク対策状況点検結果（課題の改善状況）

リスク対策状況点検の結果、各課が自己点検で検出した課題は速やかに改善されています。
また、調査項目数は平成25年度と同じ9項目で、課題ありの延べ課数は大幅に減少していますが、
スタンドアロンパソコンのウイルス対策において未改善課題が残っています。



（奥）全庁422課のうち自己点検で「課題あり」の延べ課数
（手前）「課題あり」と回答した65課のうち改善報告で「未改善課題あり」の延べ課数

（5）評価事項と課題事項

全庁的な書類調査、及び5課を対象に実施した訪問調査で確認した評価事項・課題事項は、下記のとおりです。

評価事項

課の業務実態に合った周知の実施

訪問調査では、課で作成したマニュアルや要点資料による周知、セルフチェックシートや理解度テストによる理解度確認、確認結果を踏まえたフォローアップ研修等、各課の業務実態に合わせてセキュリティポリシーの周知方法が工夫され、定期的な注意喚起が行われている事例を確認しました。

課の業務に応じた対策の実施

訪問調査では、USBメモリの保管方法の工夫により現物の有無確認を容易にして紛失を防止する対策が実施されている事例、スタンドアロンパソコン向けのウイルス対策ソフトの導入や定義ファイル更新作業の当番制及び作業記録の作成により、ウイルス対策が確実に実施されている事例を確認しました。

これらの優良事例を「課題・対策事例集」で紹介し、各課での取り組みの参考とすることにより、課題の減少が期待できます。

課題事項

スタンドアロンパソコンの管理における課題

自己点検では、「ウイルス対策」等のスタンドアロンパソコンの管理に関する課題を多く検出し、改善報告でも未改善課題が残っています。

情報セキュリティポリシーを再確認し、守るべき情報資産とその脅威及び対策について周知を図り、確実に実施することが必要です。

USBメモリの管理における課題

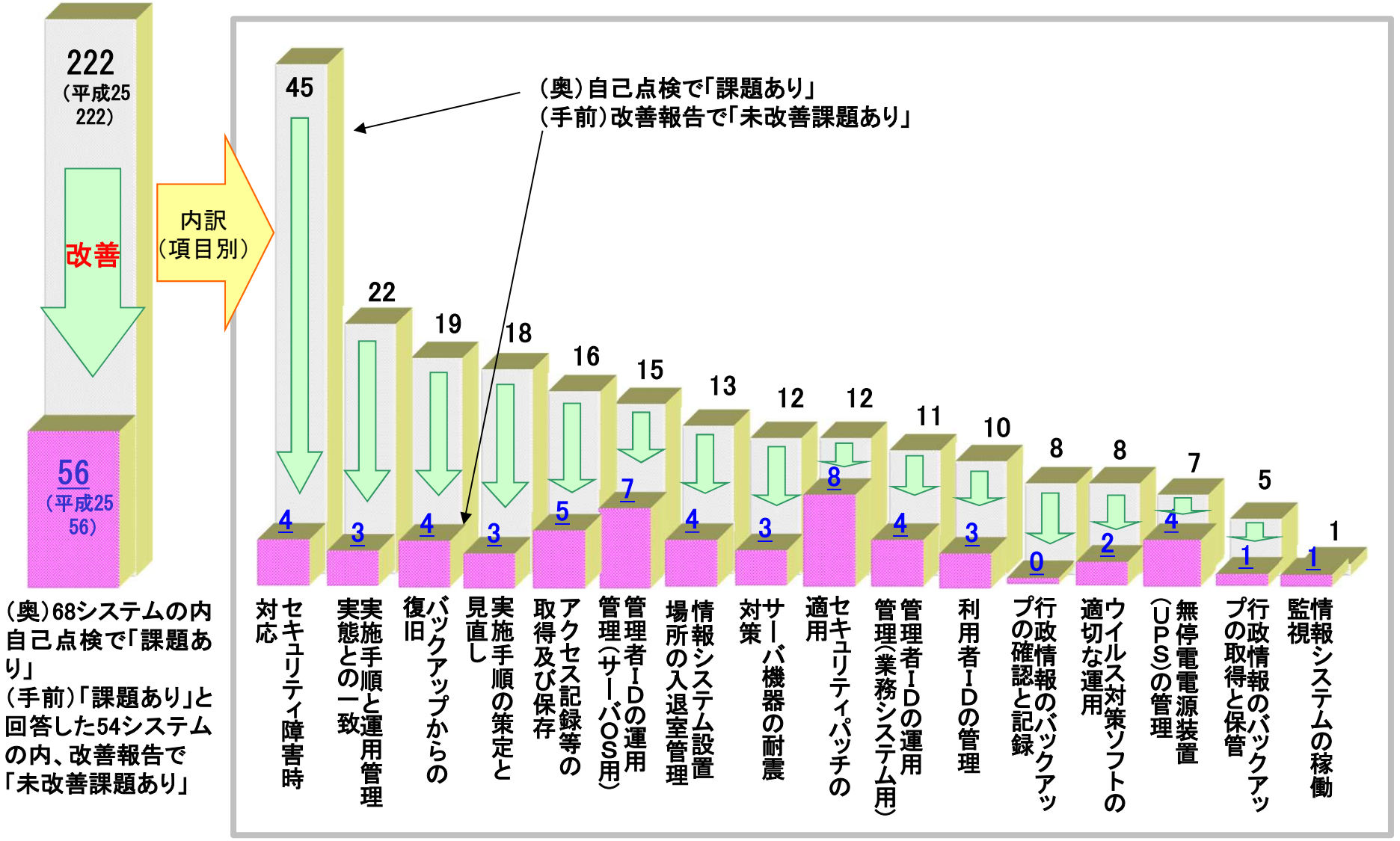
個人所有のUSBメモリの使用禁止の周知・確認について、必要な対策は実施していると評価しているにもかかわらず、周知や確認を定期的に実施していない課が多くあります。

職員の情報セキュリティ意識の低下を防ぐために、定期的に、様々な方法で繰り返し周知を行うことが必要です。

3. 情報システム監査

（1）書類調査結果（課題の改善状況）

書類調査の結果、運用面の対策で改善可能な課題については速やかに対応されていますが、
技術面の対策が必要な課題については、様々な制約から改善が進みにくい傾向があります。



（奥）68システムの内自己点検で「課題あり」
（手前）「課題あり」と回答した54システムの内、改善報告で「未改善課題あり」

（2）評価事項と課題事項

68システムを対象とした書類調査、及び10システムを対象に実施した訪問調査で確認した評価事項・課題事項は、下記のとおりです。

評価事項

運用面の課題の速やかな改善

情報システムでは、技術的な課題は、システム上の制約、保守契約、費用面等の理由で改善が進みにくい状況がありますが、「障害時対応訓練の実施」、「実施手順の見直し」等の運用面の課題については、システム所管課だけで改善が可能であるため、速やかな対応が実施されました。

点検に基づく改善というPDCAサイクルが、有効に機能しているものと考えます。

リスク低減策によるリスクコントロールの定着

ソフトウェアのぜい弱性対策である「セキュリティパッチの適用」については、システムへの影響などの理由で適用していないシステムがあります。しかし、このようなシステムの大部分がリスク低減策を実施することによって、パッチ未適用のリスクをコントロールしていると回答しています。技術面の対策が難しい状況においても、運用面の対策によってリスク低減を図ることが定着したものと考えます。

課題事項

「実施手順」の実効性における課題

自己点検では、「実施手順」関係で40項目の課題を検出しています。これらの課題は速やかに改善されていますが、「実施手順」がシステム更改時に見直されていないことや、内容が運用管理実態と一致していない状況は、「実施手順」の実効性が確保できていないということです。

平成26年度は、「実施手順」のひな形の見直しを行いました。新ひな形への移行によって「実施手順」の実効性が向上するものと考えます。

管理者ID（サーバOS用）の課題

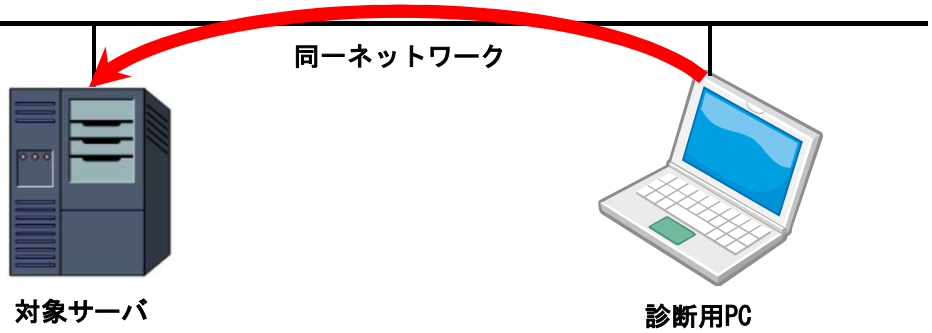
システム設定の中で管理者IDを使用しており、パスワードの変更によって障害が発生する可能性がある等の理由により、パスワードの変更が行われていないシステムがありました。

管理者ID（サーバOS用）の不正利用を防止するためには、パスワード変更以外にも、設置環境の物理的セキュリティ対策の強化、システム設定の見直し等による対策を実施することが必要です。

（3）技術監査（診断方式）

情報システムに内在するぜい弱性を診断するため、以下の2つの方式で技術監査を実施しました。

【オンサイト診断】



対象システムのサーバ・機器に対して同一ネットワークから診断を行い、オペレーティングシステム、ソフトウェア、ネットワーク設定などにセキュリティ上の不備がないかを診断します。

【リモート診断】

対象システムのサーバ・機器、又はWebサイトに対してインターネット経由で診断を行い、サーバ・機器やWebアプリケーションにセキュリティ上の不備がないかを診断します。

（4）技術監査結果

技術監査の結果、一部を除いて緊急度の高いぜい弱性は検出されませんでした。
ソフトウェアのセキュリティ更新に関するマネジメントが、概ね機能していることを確認しました。

対象システム	診断内容	診断方式	診断結果
Aシステム	サーバ・機器診断 （内部サーバ）	オンサイト診断	ぜい弱性をいくつか検出しましたが、本システムは、セキュリティレベルの高い庁内LANの内側からしか利用できないため、検出したぜい弱性が攻撃される可能性は低いと判断しました。
Gシステム	サーバ・機器診断 （内部サーバ）	オンサイト診断	セキュリティパッチ未適用のぜい弱性を検出しました。しかし、対象の内部サーバは、一部の部署からのアクセスしか認めていないため、検出したぜい弱性が攻撃される可能性は低いと判断しました。 上記以外にも設定の不備と考えられるぜい弱性をいくつか検出しましたが、サーバの利用形態、設定理由等を確認したうえで、対策の要否を判断することが必要です。
	サーバ・機器診断 （外部公開サーバ）	オンサイト診断 リモート診断	外部公開されているWebサーバから、ぜい弱性をいくつか検出しました。対象のWebサーバは、インターネットからアクセス可能であるため、対策の検討が必要であると判断しました。 また、サポートが終了したOSの使用を検出したサーバについては、至急OSを更新するか、使用を停止することが必要です。
	Webアプリケーション診断 （外部公開サーバ）	リモート診断	外部公開されているWebサイト（パソコン用）で、閲覧者のパソコン上で悪意のあるプログラムを実行させられたり、パスワードが平文でやりとりされるぜい弱性を検出しました。市民が利用するサイトであるため、Webアプリケーションの改修が必要です。

４．総括
（１）総括（情報セキュリティ点検）

【書類調査】

（セキュリティマネジメント点検）

平成25年度に比べ課題や未改善課題は減少していることが確認できましたが、クリアデスクについては、他の調査項目と比較するとまだ未改善課題が残されており、根気よく対策を継続することが重要です。

（リスク対策状況点検）

各課で保有する主要な情報資産の動向を把握できるようになりました。

また、リスク分析の考え方を取り入れて具体的な対策の実施状況を確認したことにより、どのような未対策のぜい弱性が多いか等の具体的な課題が明確になりました。

【訪問調査】

USBメモリの保管と現物との突合、重要性分類の表示において、自己点検では課題なしと判断されたものの、訪問調査でいくつかの課題を確認しました。

また、セキュリティポリシーの周知、スタンドアロンパソコンのウイルス対策、USBメモリの保管と現物との突合に関する対策等のいくつかの優良事例を確認しました。

（2）総括（情報システム監査）

【書類調査】

自己点検及び改善報告の結果から、情報システムにおける情報セキュリティ対策では、技術面の課題には改善が難しいものがあり、運用面の課題は速やかに改善されるという傾向があります。

改善が困難な技術面の課題（「セキュリティパッチの適用」など）については、リスク低減策の実施によってリスクをコントロールしているシステムが増加している状況を確認しています。

「セキュリティパッチの適用」については、「なぜ適用できないのか」を再確認する取組みと並行して、本当に適用できないのであれば「リスク低減策を実施しているか」を確認して、情報セキュリティリスクの低減を推進しました。

【訪問調査】

訪問調査では、簡易なパスワードが設定されている、バックアップの取得結果を確認していないため、失敗を検知できないなど、システム所管課の見落とし又は認識不足であると判断した課題を検出しています。このように情報システムの実態を踏まえた調査によって、より具体的な改善やリスク低減策の推進につながるものと考えます。

【技術監査】

診断ツールによるサーバ・機器診断とWebアプリケーションのぜい弱性診断を実施しました。

1システムでは、いくつかのぜい弱性を検出しましたが、庁内LANの内側からのアクセスに限定されていることと、複数の対策による多層防御が機能しているため、対策の必要性は低いと判断しました。

他の1システムでは、インターネットに公開されているサーバの1台に、サポートが終了したOSが使用されている緊急度の高いぜい弱性を検出しました。また、他の公開サーバ上で動作するWebアプリケーションからも対策が必要なぜい弱性を検出しました。

（３）今後必要な取組み（情報セキュリティ点検）

（ｉ）継続的な取り組みが必要

クリアデスクについての予算措置等の環境面での対策を含めた継続的な改善とともに、各課で対策の実施状況を見直し、新たな対策の必要性を検討する好機である情報セキュリティ点検や、情報セキュリティ対策についての認識を深める機会となる職員研修を、継続して実施することが必要です。

（ⅱ）情報資産の保有状況の変化により想定される新たなリスクへの対策の検討と実施

リスク対策状況点検を実施することにより、主要な情報資産の保有状況の変化を把握し、今後増加が見込まれる情報資産について想定されるリスクと新たな対策の検討が必要です。

また、取扱う行政情報の重要性分類の視点と外部記録媒体・機器そのものの管理の視点の双方からリスクを評価することが必要です。

（4）今後必要な取組み（情報システム監査）

（ｉ）訪問調査の継続

情報システムは、システム形態、規模、接続するネットワーク、保有する行政情報、可用性要件などの違いにより、情報セキュリティ対策の実施レベルが異なります。そのため書類調査のような画一的な方法だけでは評価できない部分があります。特に技術面の課題は、実施が困難な理由やリスク低減策の実施状況を確認したうえで、システムの運用管理実態にあった改善提案を行うことが重要になります。そのため、継続的に訪問調査を実施して、情報システムの運用管理実態に合った改善を推進していくことが重要であると考えます。

（ⅱ）ぜい弱性の影響を受けやすい情報システムを優先した技術監査の実施

情報セキュリティに対する脅威は、毎年のように新しい手法や手段が登場している状況であり、インターネットに公開している情報システムだけでなく、利用者端末がインターネットサービスを利用している情報システムにおいても、同様のリスクがあるといえます。

今後も、技術監査が最も効果的な情報システムとして、インターネットに公開しているシステムや利用者端末がインターネットサービスを利用しているシステムを、優先的に技術監査対象とすることが効果的であると考えます。