監査
実施手順書

作成者	恩納村　総務課
作成日	平成 29 年 11 月 30 日
最終更新日	

目　　次

１．目的

本手順書は、恩納村情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）及び情報セキュリティ実施手順に基づき、情報セキュリティ対策が適切に実施されているかを確認するための監査（内部監査及び外部監査並びに監査に係る是正処置及び予防処置）の手順を定めることを目的とする。

２．定義

（１）内部監査

職員等自らが行う監査であって、外部委託等を行わないものをいう。

（２）外部監査

第三者の視点による客観性や専門性を確保するため、外部の事業者や専門家に委託して行う監査をいう。

３．内部監査

（１）方針

情報セキュリティポリシー及び情報セキュリティ実施手順に基づき実施する情報セキュリティ対策について、次に掲げる観点から、内部監査を計画、実施する。

① 情報セキュリティ対策に関連する法令等を遵守していること。

② 情報セキュリティポリシー及び情報セキュリティ実施手順に基づき、情報セキュリティ対策を実施していること。

③ 情報セキュリティ対策が有効に実施され、維持されていること。

（２）内部監査の種類

内部監査は、次の２つの種類に類別する。

項目	内容
定期内部監査	定期的に実施される内部監査であり、情報セキュリティ監査統括責任者の指示のもと、実施する。
臨時内部監査	定期内部監査以外に、臨時の内部監査を実施するものであり、次の場合に実施する。 ・関係する規程の改定、組織の変更、業務内容の変更等の重大な変更があった場合 ・最高情報セキュリティ責任者又は情報セキュリティ監査統括責任者が必要と判断した場合

（３）監査結果の種別

内部監査で使用する監査結果の種別を次のように設定する。なお、指摘事項以外は、情報セキュリティポリシーを満たしているものと判断し、指摘事項のみ報告書に記載する。

種別	内容
指摘事項	・法令等への違反又は情報セキュリティの維持に重大な影響を及ぼすおそれがある場合（要求事項の欠落、手順からの大きな逸脱） ・要求事項の一つにおいて、部分的又は一時的に欠落がある場合 ・要求事項の欠落とはいえないが、改善の余地がある場合

（４）内部監査のプロセス

①　実施方法

最高情報セキュリティ責任者は、情報セキュリティ監査統括責任者を指名し、情報システム及びネットワーク等の情報資産における情報セキュリティ対策状況について、内部監査を実施させる。

②　内部監査員の育成

情報セキュリティ監査統括責任者は、内部監査員を指名して内部監査を実施することになるが、内部監査員は、監査及び情報セキュリティについて、専門的知識を有していることを必要とする。

そのため、情報セキュリティ監査統括責任者は、内部監査員の育成を行い、次に掲げるいずれかの者を内部監査員として認定する。

ア　情報セキュリティ委員会事務局（以下「事務局」という。）が企画・実施する外部講師による内部監査員研修・訓練の修了者

イ　外部で行われるアと同等の研修・訓練を受講した者

ウ　内部監査を２回以上実施した内部監査員が実施する内部監査員養成研修・訓練の修了者

エ　ISMS 審査員補又は情報セキュリティ監査人補等の監査の資格を有する者

③　内部監査員の資格認定

ア　事務局は、内部監査員の資格認定された者について、様式「資格認定書」に記録する。外部機関等で修了証が発行される場合、それをもって資格認定されたこととする。

イ　様式「資格認定書」は、情報セキュリティ監査統括責任者が承認する。

④　監査員の選定

情報セキュリティ監査統括責任者は、事務局と協力し、様式「資格認定書」に記載されている職員等の中から、内部監査員を選出する。内部監査員にはリーダーとメンバーを選出し、２名以上の監査チームを編成する。

また、監査の客観性及び公平性を確保するため、監査対象部署に所属する者からは、内部監査員を選定しない。

選出に当たっては、事務局が、内部監査員の業務の都合等を考慮し、調整する。選出の結果については、情報セキュリティ監査統括責任者から、口頭又はメールにより通知を行う。

⑤　監査実施計画書の作成

監査チームのリーダーは、事務局と協力して、様式「監査実施計画書」を作成する。作成後は、情報セキュリティ監査統括責任者の承認を受け、監査実施予定日の１週間前までに監査対象部署へ周知する。

⑥　チェックリストの作成

内部監査員は、監査実施時の質問事項等を明確にするため、監査対象部署に応じて、様式「監査チェックリスト」を作成する。

⑦　監査の実施

監査チームのリーダーは、監査開始に先立ち、様式「監査実施計画書」に基づき、監査対象部署に対して監査目的の説明、スケジュール等の確認を行う。

内部監査員は、様式「監査実施計画書」及び様式「監査チェックリスト」に基づき、監査対象部署の監査を実施する。

監査チームのリーダーは、監査終了後に各メンバーを集め、監査結果についてまとめる。

監査チームのリーダーは、監査対象部署に対して、監査結果の概要を口頭にて説明する。

⑧　改善の要求

監査チームのリーダーは、監査結果を様式「監査報告書」に記載し、事務局に提出する。

事務局は、様式「監査報告書」を取りまとめて、情報セキュリティ監査統括責任者へ報告する。

情報セキュリティ監査責任者は、CISO の指示に基づき、監査対象部署に対して、様式「監査報告書」を提示し、指摘事項に対する改善を要求する。

監査対象部署の情報セキュリティ管理者及び職員は、指摘事項に対する対応を様式「監査報告書」に記載し、事務局に提出する。指摘事項がない場合は、内容を確認して、その旨を記載し、事務局に提出する。

⑨　監査結果の報告

事務局は、様式「監査報告書」を取りまとめて情報セキュリティ監査統括責任者に報告する。

情報セキュリティ監査統括責任者は、様式「監査報告書」の内容を確認し、承認する。

⑩　情報セキュリティ委員会への報告

情報セキュリティ監査統括責任者は、様式「監査報告書」に基づき、監査結果について、情報セキュリティ委員会に報告する。

⑪　記録、様式の管理

事務局は、情報セキュリティ監査統括責任者の指示に基づき、内部監査にかかわる記録を管理する。

４．外部監査

外部監査については、原則として、監査を行う者の指示に従って実施する。外部監査において指摘された事項への対応及び改善措置については、「５．改善措置及び予防措置」に基づき、実施する。

５．改善措置及び予防措置

監査により、指摘事項が発生し、又は発見された場合、次のとおり、改善措置を実施する。また、指摘事項の内容が、監査対象部署だけにとどまらない場合、予防措置（指摘されていないが、同様の事象が想定される場合、組織の枠に関係なく事前に対処すること。）の実施を検討する。

（１）改善措置及び予防措置の対象となる指摘事項

改善措置及び予防措置は、次の場合に実施する。ただし、内部監査における指摘事項の対応については、「３．内部監査」に基づき、実施する。

①　情報セキュリティポリシーの運用・維持に支障をきたす、又は規程及び手順類の遵守事項を逸脱して業務を行っている等の指摘事項が報告された場合

②　外部監査により指摘事項が報告された場合

③　その他情報セキュリティ委員会が必要と認めた場合

（２）改善措置の実施方法

①　指摘事項の確認

監査対象部署の職員は、指摘事項の内容について、様式「監査報告書」に従い、確認する。ただし、類似の指摘事項が多発する可能性があり、緊急性を要する場合、事務局と連携し応急措置を実施することができる。その場合は、実施内容を様式「監査報告書」に必ず記載する。

②　原因の特定と改善措置の決定

監査対象部署の職員は、発見された指摘事項について、原因を特定し、様式「監査報告書」に記載するとともに、改善措置を検討する。

監査対象部署の情報セキュリティ管理者は、次に掲げる事項に基づき、改善措置の妥当性を判断し、決定する。

ア　再発した場合の損害

イ　是正処置に要するコスト

ウ　過去に発生した類似の指摘事項

エ　情報セキュリティに関する社会の動向

③　改善措置の実施

監査対象部署の職員は、改善措置を実施し、様式「監査報告書」に記載する。

情報セキュリティ管理者は、実施した改善措置を確認し、様式「監査報告書」を事務局へ提出する。

事務局は、報告どおり改善措置が実施されていることを確認し、監査結果対応の完了を承認する。

④　改善措置の承認

事務局は、計画どおり是正処置が実施されていることを確認し、情報セキュリティ監査統括責任者に報告する。

情報セキュリティ監査統括責任者は、様式「監査報告書」の内容を確認し、承認するとともに、監査結果を情報セキュリティ委員会に報告する。

⑤　予防措置の必要性

情報セキュリティ監査統括責任者は、指摘事項の内容から必要と認めた場合、予防措置の実施を支持する。

また、情報セキュリティ管理者は、改善措置の実施結果から予防措置が必要と認めた場合、情報セキュリティ監査統括責任者に予防措置の実施を求めることができる。

［改定履歴］

版	更新年月日	改定理由及び内容	承認	審査	担当
1.0 版	平成 29 年 11 月 30 日	新規制定			

<様式>

資格認定書

資格認定日	平成　　年　　月　　日
承認者	

次の者を内部監査の資格認定者として認定する。

氏名	氏名コード	研修・訓練内容	備考
		・外部講師による受講 ・内部認定 ・有資格（　　　　　　　　）	
		・外部講師による受講 ・内部認定 ・有資格（　　　　　　　　）	
		・外部講師による受講 ・内部認定 ・有資格（　　　　　　　　）	
		・外部講師による受講 ・内部認定 ・有資格（　　　　　　　　）	
		・外部講師による受講 ・内部認定 ・有資格（　　　　　　　　）	
		・外部講師による受講 ・内部認定 ・有資格（　　　　　　　　）	
		・外部講師による受講 ・内部認定 ・有資格（　　　　　　　　）	
		・外部講師による受講 ・内部認定 ・有資格（　　　　　　　　）	
		・外部講師による受講 ・内部認定 ・有資格（　　　　　　　　）	
		・外部講師による受講 ・内部認定 ・有資格（　　　　　　　　）	
		・外部講師による受講 ・内部認定 ・有資格（　　　　　　　　）	
		・外部講師による受講 ・内部認定 ・有資格（　　　　　　　　）	

＜様式＞

監査実施計画書

承 認	作 成
(H . .)	(H . .)

1	監査方針	
2	監査の目的	
3	対象部署(範囲)	
4	監査年月日	
5	監査チーム	リーダー: メンバー:

【監査の基準】

6	適用規程類	「情報セキュリティポリシー」 制改訂日 年 月 日

【監査の方法、範囲】

	監査日時	対象部署(対応者)	監査項目
7 監査スケジュール			

＜様式＞

監 査 チェックリスト

管理番号:		監査日　平成　　年　　月　　日
対象部署:	対応者:	監査員:

項番	情報セキュリティポリシーの内容	作成等されるべき帳票類	結　果	メ　モ

＜様式＞

監 査 報 告 書

<table>
<tr><td>1</td><td>対象部署／監査年月日</td><td colspan="2"></td><td>年　　月　　日実施</td></tr>
<tr><td>2</td><td>監査チーム</td><td colspan="3">リーダー:　　メンバー:</td></tr>
<tr><td rowspan="2">3</td><td rowspan="2">指摘事項等の内容</td><td colspan="3">件数　合計　　件</td></tr>
<tr><td colspan="3">●指摘項目　　件
①(　　)
②(　　)
③(　　)
④(　　)
⑤(　　)</td></tr>
<tr><td colspan="2" rowspan="2">判定結果</td><td rowspan="2">上記のような判定結果になりましたので確認願います。

無し　／　有り（該当項番:　　）</td><td>情報セキュリティ監査統括責任者</td><td>監査チームリーダー</td></tr>
<tr><td>(H　.　.　)</td><td>(H　.　.　)</td></tr>
<tr><td>4</td><td>改善措置
（指摘に対して、何が原因でどのような対策を行うのか記入してください）</td><td colspan="3">項番:__（原因:　　）
（改善措置:
）
項番:__（原因:　　）
（改善措置:
）
項番:__（原因:　　）
（改善措置:
）
項番:__（原因:　　）
（改善措置:
）
項番:__（原因:　　）
（改善措置:
）</td></tr>
<tr><td>5</td><td>監査結果に対するコメントと監査対象部署確認
（情報セキュリティ管理者）</td><td colspan="2">監査報告書を確認しました。
or
指摘事項を確認し、是正処置を上記のとおり実施しました。</td><td>確認欄

(H　.　.　)</td></tr>
</table>

記載方法:①監査チームリーダーが、1～3及び判定結果を記入。
②情報セキュリティ監査統括責任者が、内容、判定結果を確認し、監査対象部署に通知。
③監査対象部署で、4～5を記入。記入後、事務局へ提出。4は判定結果が「有り」の場合のみ。

＜様式＞

監査報告書（記入例）

1	対象部署／監査年月日	○○課	平成29年　月　日実施
2	監査チーム	リーダー：山田太郎　　メンバー：田中一郎	
3	指摘事項等の内容	件数　合計　3　件 ●重大な指摘　　0　件 ①（業務中でしたが、住民の納税情報が、ほかの住民から容易に確認できるところに置いてありました。） ②（一部の職員のシステムログインパスワードが4桁でした。　　） ③（情報セキュリティポリシーがどこで閲覧できるか知りませんでした。　　） ④（　　） ⑤（　　）	

判定結果	上記のような判定結果になりましたので確認願います。 無し　／　有り（該当項番：　　）	情報セキュリティ監査統括責任者	監査チームリーダー
		◎◎課長 （H28. 9. 7）	△△　△△ （H28. 9. 5）

4	改善措置 （指摘に対して、何が原因でどのような対策を行うのか記入してください）	項番：①（原因：情報セキュリティ対策より業務遂行を優先したためでした。） （改善措置：情報は、カウンターに置かず、自分の机の上に置くことを周知徹底しました。） 項番：②（原因：桁数について理解できていませんでした。　　） （改善措置：システムログインパスワードを、全職員分確認し、すべて8桁以上での設定に変更しました。　　） 項番：③（原因：研修で学んだことを失念していました。　　） （改善措置：課内で再度研修会を開き、把握させました。　　） 項番：＿（原因：　　） （改善措置：　　） 項番：＿（原因：　　） （改善措置：　　）

5	監査結果に対するコメントと監査対象部署確認 （情報セキュリティ管理者）	監査報告書を確認しました。 or 指摘事項を確認し、是正処置を上記のとおり実施しました。	確認欄 □□　□□ （H28. 9. 20）

記載方法：①監査チームリーダーが、1～3及び判定結果を記入。
②情報セキュリティ監査統括責任者が、内容、判定結果を確認し、監査対象部署に通知。
③監査対象部署で、4～5を記入。記入後、事務局へ提出。4は判定結果が「有り」の場合のみ。