情報セキュリティ対策地図

マルウェア対策

三途の川図法　V0.4989

2011年　JNSA情報セキュリティ対策マップWG

目的界

手段界

対策の実現例

0:マルウェアに対する【対策】を実施する。

1:マルウェアの被害発生のリスクを包括的に軽減するための【対策】を実施する。

2:【色々な場面において】マルウェアの被害発生を防止する【対策】を実施する。

3:マルウェアの被害拡大を防止する【対策】を実施する。

4:マルウェアの被害からの回復のための【対策】を実施する。

5:【感染時の経済的損害の補償】をする。

6:再発の防止のための事後対策を行う。

7:マルウェアが侵入しにくくする。

8:脆弱性をなくす。

9:マルウェアの拡散防止を行う。

10:【ツール】を利用して、【媒介物】を介して送り込まれた【悪意のコード】を検知する。

11:速やかな復旧・回復が行えるように事前の対策を行う。

12:駆除を行いマルウェアを根絶する。

13:【入手経路】から入手した許可されない【資産】の使用を禁止する。

14:組織内部のすべてのユーザに、【意識すべきこと】を意識させる。

15:事態収束後にマルウェアの感染について報告する。

16:再発防止のため、【振り返りの会議】を開催する。

17:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】をする。

18:【侵入防止】のため、ウイルス対策ソフトウェアを導入する。

19:【各種アプリケーション】のセキュリティ設定を適切に行う。

20:ホストの【強化措置】を行う。

21:【情報】に関する最新情報を入手する。

22:正しい情報とデマ情報を識別する。

23:【色々な対象】の脆弱性診断を実施する。

24:【色々な対象】の脆弱性を【適切に対処】する。

25:システムへの適切なアクセスを実現する【アクセス管理策】を導入する。

26:マルウェアの感染を報告する。

27:【検出】のため、ウイルス対策ソフトウェアを導入する。

28:ウイルス対策ソフトウェアを正しく設定する。

29:ウイルス対策ソフトウェアでスキャンする。

30:複数ベンダーが提供する、ウイルス対策ソフトを利用する。

31:ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】。

32:プログラムやデータのバックアップを取得する。

33:プログラムのオリジナルファイルにはライトプロテクトを施して保管する。

34:システムの変更管理を行う。

35:【駆除】のため、ウイルス対策ソフトウェアを導入する。

36:保険を適用する。

37:【IPフィルタリングデバイス】を導入する。

38:ウェブ閲覧時にマルウェア検出のための【スキャン対策】をする。

39:ウイルス対策ソフトウェアで定期的にスキャンする。

40:ウイルス対策ソフトウェアでリアルタイムにスキャンする。

41:ダウンロードファイルに対してマルウェア検出のための使用前スキャンをする。

42:すべての電子メールの添付ファイルをスキャンし、疑わしい電子メールの添付ファイルを特定し、【処理】する。

43:取り外し可能な【記録媒体】上のファイルに対する、マルウェア検出のための使用前スキャンをする。

44:ウイルス対策ソフトウェアでローカルファイルを定期的にスキャンする。

フィルタリングソフト

ウイルス対策ソフト製品

セキュリティ情報サイト

セキュリティ情報提供サービス

脆弱性スキャナ製品

ファイアウォール製品

ウイルス対策ソフト製品

ウイルス対策ソフト製品

保険サービス

			メソッド																						
ID	簡易表現	正式表現	について検討する	について計画する	のコストを算定する	の対策を確立する	のためのリソースを確保する	を導入する（機材の場合は「設定する」を含む）	を保守（維持）する	について文書化する	の手順を確立する	の手順を明確化する	の手順を文書化する	の責任者を明確化する	を実施する	の実施を記録する	の実施時に注意を払う	について利用者を教育（訓練）する	についてレビューする	対策を見直す	の実施状況を監査する	の有効性（効果）の測定方法を決める	の有効性（効果）を測定する	を改善する	を廃止する
13	【入手経路】から入手した許可されない【資産】の使用禁止	【入手経路：{外部ネットワーク}、{＊}】から入手した許可されない【資産：{ソフトウェア}、{ファイル}】の使用を禁止する。	「【入手経路】から入手した許可されない【資産】の使用禁止」について検討する	「【入手経路】から入手した許可されない【資産】の使用禁止」について計画する	「【入手経路】から入手した許可されない【資産】の使用禁止」のコストを算定する	「【入手経路】から入手した許可されない【資産】の使用禁止」の対策を確立する	「【入手経路】から入手した許可されない【資産】の使用禁止」のためのリソースを確保する	「【入手経路】から入手した許可されない【資産】の使用禁止」を導入する（機材の場合は「設定する」を含む）	「【入手経路】から入手した許可されない【資産】の使用禁止」を保守（維持）する	「【入手経路】から入手した許可されない【資産】の使用禁止」について文書化する	「【入手経路】から入手した許可されない【資産】の使用禁止」の手順を確立する	「【入手経路】から入手した許可されない【資産】の使用禁止」の手順を明確化する	「【入手経路】から入手した許可されない【資産】の使用禁止」の手順を文書化する	「【入手経路】から入手した許可されない【資産】の使用禁止」の責任者を明確化する	「【入手経路】から入手した許可されない【資産】の使用禁止」を実施する	「【入手経路】から入手した許可されない【資産】の使用禁止」の実施を記録する	「【入手経路】から入手した許可されない【資産】の使用禁止」の実施時に注意を払う	「【入手経路】から入手した許可されない【資産】の使用禁止」について利用者を教育（訓練）する	「【入手経路】から入手した許可されない【資産】の使用禁止」についてレビューする	「【入手経路】から入手した許可されない【資産】の使用禁止」対策を見直す	「【入手経路】から入手した許可されない【資産】の使用禁止」の実施状況を監査する	「【入手経路】から入手した許可されない【資産】の使用禁止」の有効性（効果）の測定方法を決める	「【入手経路】から入手した許可されない【資産】の使用禁止」の有効性（効果）を測定する	「【入手経路】から入手した許可されない【資産】の使用禁止」を改善する	「【入手経路】から入手した許可されない【資産】の使用禁止」を廃止する
14	組織内部のすべてのユーザに、【意識すべきこと】を意識させること	組織内部のすべてのユーザに、【意識すべきこと：{マルウェアの侵入、感染、および拡散の方法}、{マルウェアがもたらすリスク}、{技術的管理策ではすべてのインシデントは防げないこと}、{インシデントを防ぐうえでユーザが重要な役割を果たすこと}】を意識させ	「組織内部のすべてのユーザに、【意識すべきこと】を意識させること」について検討する	「組織内部のすべてのユーザに、【意識すべきこと】を意識させること」について計画する	「組織内部のすべてのユーザに、【意識すべきこと】を意識させること」のコストを算定する	「組織内部のすべてのユーザに、【意識すべきこと】を意識させること」の対策を確立する	「組織内部のすべてのユーザに、【意識すべきこと】を意識させること」のためのリソースを確保する	「組織内部のすべてのユーザに、【意識すべきこと】を意識させること」を導入する（機材の場合は「設定する」を含む）	「組織内部のすべてのユーザに、【意識すべきこと】を意識させること」を保守（維持）する	「組織内部のすべてのユーザに、【意識すべきこと】を意識させること」について文書化する	「組織内部のすべてのユーザに、【意識すべきこと】を意識させること」の手順を確立する	「組織内部のすべてのユーザに、【意識すべきこと】を意識させること」の手順を明確化する	「組織内部のすべてのユーザに、【意識すべきこと】を意識させること」の手順を文書化する	「組織内部のすべてのユーザに、【意識すべきこと】を意識させること」の責任者を明確化する	「組織内部のすべてのユーザに、【意識すべきこと】を意識させること」を実施する	「組織内部のすべてのユーザに、【意識すべきこと】を意識させること」の実施を記録する	「組織内部のすべてのユーザに、【意識すべきこと】を意識させること」の実施時に注意を払う	「組織内部のすべてのユーザに、【意識すべきこと】を意識させること」について利用者を教育（訓練）する	「組織内部のすべてのユーザに、【意識すべきこと】を意識させること」についてレビューする	「組織内部のすべてのユーザに、【意識すべきこと】を意識させること」対策を見直す	「組織内部のすべてのユーザに、【意識すべきこと】を意識させること」の実施状況を監査する	「組織内部のすべてのユーザに、【意識すべきこと】を意識させること」の有効性（効果）の測定方法を決める	「組織内部のすべてのユーザに、【意識すべきこと】を意識させること」の有効性（効果）を測定する	「組織内部のすべてのユーザに、【意識すべきこと】を意識させること」を改善する	「組織内部のすべてのユーザに、【意識すべきこと】を意識させること」を廃止する
15	事態収束後にマルウェアの感染についての報告	事態収束後にマルウェアの感染について報告する。	「事態収束後にマルウェアの感染についての報告」について検討する	「事態収束後にマルウェアの感染についての報告」について計画する	「事態収束後にマルウェアの感染についての報告」のコストを算定する	「事態収束後にマルウェアの感染についての報告」の対策を確立する	「事態収束後にマルウェアの感染についての報告」のためのリソースを確保する	「事態収束後にマルウェアの感染についての報告」を導入する（機材の場合は「設定する」を含む）	「事態収束後にマルウェアの感染についての報告」を保守（維持）する	「事態収束後にマルウェアの感染についての報告」について文書化する	「事態収束後にマルウェアの感染についての報告」の手順を確立する	「事態収束後にマルウェアの感染についての報告」の手順を明確化する	「事態収束後にマルウェアの感染についての報告」の手順を文書化する	「事態収束後にマルウェアの感染についての報告」の責任者を明確化する	「事態収束後にマルウェアの感染についての報告」を実施する	「事態収束後にマルウェアの感染についての報告」の実施を記録する	「事態収束後にマルウェアの感染についての報告」の実施時に注意を払う	「事態収束後にマルウェアの感染についての報告」について利用者を教育（訓練）する	「事態収束後にマルウェアの感染についての報告」についてレビューする	「事態収束後にマルウェアの感染についての報告」対策を見直す	「事態収束後にマルウェアの感染についての報告」の実施状況を監査する	「事態収束後にマルウェアの感染についての報告」の有効性（効果）の測定方法を決める	「事態収束後にマルウェアの感染についての報告」の有効性（効果）を測定する	「事態収束後にマルウェアの感染についての報告」を改善する	「事態収束後にマルウェアの感染についての報告」を廃止する
16	再発防止のための【振り返りの会議】の開催	再発防止のため、【振り返りの会議：{反省会}、{レビュー}、{その他の取り組み}】を開催する。	「再発防止のための【振り返りの会議】の開催」について検討する	「再発防止のための【振り返りの会議】の開催」について計画する	「再発防止のための【振り返りの会議】の開催」のコストを算定する	「再発防止のための【振り返りの会議】の開催」の対策を確立する	「再発防止のための【振り返りの会議】の開催」のためのリソースを確保する	「再発防止のための【振り返りの会議】の開催」を導入する（機材の場合は「設定する」を含む）	「再発防止のための【振り返りの会議】の開催」を保守（維持）する	「再発防止のための【振り返りの会議】の開催」について文書化する	「再発防止のための【振り返りの会議】の開催」の手順を確立する	「再発防止のための【振り返りの会議】の開催」の手順を明確化する	「再発防止のための【振り返りの会議】の開催」の手順を文書化する	「再発防止のための【振り返りの会議】の開催」の責任者を明確化する	「再発防止のための【振り返りの会議】の開催」を実施する	「再発防止のための【振り返りの会議】の開催」の実施を記録する	「再発防止のための【振り返りの会議】の開催」の実施時に注意を払う	「再発防止のための【振り返りの会議】の開催」について利用者を教育（訓練）する	「再発防止のための【振り返りの会議】の開催」についてレビューする	「再発防止のための【振り返りの会議】の開催」対策を見直す	「再発防止のための【振り返りの会議】の開催」の実施状況を監査する	「再発防止のための【振り返りの会議】の開催」の有効性（効果）の測定方法を決める	「再発防止のための【振り返りの会議】の開催」の有効性（効果）を測定する	「再発防止のための【振り返りの会議】の開催」を改善する	「再発防止のための【振り返りの会議】の開催」を廃止する
17	15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】	ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】をする。	「15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】」について検討する	「15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】」について計画する	「15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】」のコストを算定する	「15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】」の対策を確立する	「15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】」のためのリソースを確保する	「15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】」を導入する（機材の場合は「設定する」を含む）	「15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】」を保守（維持）する	「15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】」について文書化する	「15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】」の手順を確立する	「15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】」の手順を明確化する	「15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】」の手順を文書化する	「15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】」の責任者を明確化する	「15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】」を実施する	「15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】」の実施を記録する	「15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】」の実施時に注意を払う	「15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】」について利用者を教育（訓練）する	「15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】」についてレビューする	「15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】」対策を見直す	「15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】」の実施状況を監査する	「15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】」の有効性（効果）の測定方法を決める	「15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】」の有効性（効果）を測定する	「15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】」を改善する	「15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】」を廃止する
18	【侵入防止】のためのウイルス対策ソフトウェアの導入	【侵入防止】のため、ウイルス対策ソフトウェアを導入する	「【侵入防止】のためのウイルス対策ソフトウェアの導入」について検討する	「【侵入防止】のためのウイルス対策ソフトウェアの導入」について計画する	「【侵入防止】のためのウイルス対策ソフトウェアの導入」のコストを算定する	「【侵入防止】のためのウイルス対策ソフトウェアの導入」の対策を確立する	「【侵入防止】のためのウイルス対策ソフトウェアの導入」のためのリソースを確保する	「【侵入防止】のためのウイルス対策ソフトウェアの導入」を導入する（機材の場合は「設定する」を含む）	「【侵入防止】のためのウイルス対策ソフトウェアの導入」を保守（維持）する	「【侵入防止】のためのウイルス対策ソフトウェアの導入」について文書化する	「【侵入防止】のためのウイルス対策ソフトウェアの導入」の手順を確立する	「【侵入防止】のためのウイルス対策ソフトウェアの導入」の手順を明確化する	「【侵入防止】のためのウイルス対策ソフトウェアの導入」の手順を文書化する	「【侵入防止】のためのウイルス対策ソフトウェアの導入」の責任者を明確化する	「【侵入防止】のためのウイルス対策ソフトウェアの導入」を実施する	「【侵入防止】のためのウイルス対策ソフトウェアの導入」の実施を記録する	「【侵入防止】のためのウイルス対策ソフトウェアの導入」の実施時に注意を払う	「【侵入防止】のためのウイルス対策ソフトウェアの導入」について利用者を教育（訓練）する	「【侵入防止】のためのウイルス対策ソフトウェアの導入」についてレビューする	「【侵入防止】のためのウイルス対策ソフトウェアの導入」対策を見直す	「【侵入防止】のためのウイルス対策ソフトウェアの導入」の実施状況を監査する	「【侵入防止】のためのウイルス対策ソフトウェアの導入」の有効性（効果）の測定方法を決める	「【侵入防止】のためのウイルス対策ソフトウェアの導入」の有効性（効果）を測定する	「【侵入防止】のためのウイルス対策ソフトウェアの導入」を改善する	「【侵入防止】のためのウイルス対策ソフトウェアの導入」を廃止する
19	【各種アプリケーション】の適切なセキュリティ設定	【各種アプリケーション：{メーラー}、{ブラウザ}、{ビジネスソフト}、{＊}】のセキュリティ設定を適切に行う。	「【各種アプリケーション】の適切なセキュリティ設定」について検討する	「【各種アプリケーション】の適切なセキュリティ設定」について計画する	「【各種アプリケーション】の適切なセキュリティ設定」のコストを算定する	「【各種アプリケーション】の適切なセキュリティ設定」の対策を確立する	「【各種アプリケーション】の適切なセキュリティ設定」のためのリソースを確保する	「【各種アプリケーション】の適切なセキュリティ設定」を導入する（機材の場合は「設定する」を含む）	「【各種アプリケーション】の適切なセキュリティ設定」を保守（維持）する	「【各種アプリケーション】の適切なセキュリティ設定」について文書化する	「【各種アプリケーション】の適切なセキュリティ設定」の手順を確立する	「【各種アプリケーション】の適切なセキュリティ設定」の手順を明確化する	「【各種アプリケーション】の適切なセキュリティ設定」の手順を文書化する	「【各種アプリケーション】の適切なセキュリティ設定」の責任者を明確化する	「【各種アプリケーション】の適切なセキュリティ設定」を実施する	「【各種アプリケーション】の適切なセキュリティ設定」の実施を記録する	「【各種アプリケーション】の適切なセキュリティ設定」の実施時に注意を払う	「【各種アプリケーション】の適切なセキュリティ設定」について利用者を教育（訓練）する	「【各種アプリケーション】の適切なセキュリティ設定」についてレビューする	「【各種アプリケーション】の適切なセキュリティ設定」対策を見直す	「【各種アプリケーション】の適切なセキュリティ設定」の実施状況を監査する	「【各種アプリケーション】の適切なセキュリティ設定」の有効性（効果）の測定方法を決める	「【各種アプリケーション】の適切なセキュリティ設定」の有効性（効果）を測定する	「【各種アプリケーション】の適切なセキュリティ設定」を改善する	「【各種アプリケーション】の適切なセキュリティ設定」を廃止する
20	ホストの【強化措置】	ホストの【強化措置：{ハードニング}、{セキュリティ機能強化}】を行う。	「ホストの【強化措置】」について検討する	「ホストの【強化措置】」について計画する	「ホストの【強化措置】」のコストを算定する	「ホストの【強化措置】」の対策を確立する	「ホストの【強化措置】」のためのリソースを確保する	「ホストの【強化措置】」を導入する（機材の場合は「設定する」を含む）	「ホストの【強化措置】」を保守（維持）する	「ホストの【強化措置】」について文書化する	「ホストの【強化措置】」の手順を確立する	「ホストの【強化措置】」の手順を明確化する	「ホストの【強化措置】」の手順を文書化する	「ホストの【強化措置】」の責任者を明確化する	「ホストの【強化措置】」を実施する	「ホストの【強化措置】」の実施を記録する	「ホストの【強化措置】」の実施時に注意を払う	「ホストの【強化措置】」について利用者を教育（訓練）する	「ホストの【強化措置】」についてレビューする	「ホストの【強化措置】」対策を見直す	「ホストの【強化措置】」の実施状況を監査する	「ホストの【強化措置】」の有効性（効果）の測定方法を決める	「ホストの【強化措置】」の有効性（効果）を測定する	「ホストの【強化措置】」を改善する	「ホストの【強化措置】」を廃止する
21	【情報】に関する最新情報の入手	【情報：{Os等のセキュリティホール}、{Webアプリケーションの脆弱性}、{マルウェアに対する情報}】に関する最新情報を入手する。	「【情報】に関する最新情報の入手」について検討する	「【情報】に関する最新情報の入手」について計画する	「【情報】に関する最新情報の入手」のコストを算定する	「【情報】に関する最新情報の入手」の対策を確立する	「【情報】に関する最新情報の入手」のためのリソースを確保する	「【情報】に関する最新情報の入手」を導入する（機材の場合は「設定する」を含む）	「【情報】に関する最新情報の入手」を保守（維持）する	「【情報】に関する最新情報の入手」について文書化する	「【情報】に関する最新情報の入手」の手順を確立する	「【情報】に関する最新情報の入手」の手順を明確化する	「【情報】に関する最新情報の入手」の手順を文書化する	「【情報】に関する最新情報の入手」の責任者を明確化する	「【情報】に関する最新情報の入手」を実施する	「【情報】に関する最新情報の入手」の実施を記録する	「【情報】に関する最新情報の入手」の実施時に注意を払う	「【情報】に関する最新情報の入手」について利用者を教育（訓練）する	「【情報】に関する最新情報の入手」についてレビューする	「【情報】に関する最新情報の入手」対策を見直す	「【情報】に関する最新情報の入手」の実施状況を監査する	「【情報】に関する最新情報の入手」の有効性（効果）の測定方法を決める	「【情報】に関する最新情報の入手」の有効性（効果）を測定する	「【情報】に関する最新情報の入手」を改善する	「【情報】に関する最新情報の入手」を廃止する
22	正しい情報とデマ情報の識別	正しい情報とデマ情報を識別する	「正しい情報とデマ情報の識別」について検討する	「正しい情報とデマ情報の識別」について計画する	「正しい情報とデマ情報の識別」のコストを算定する	「正しい情報とデマ情報の識別」の対策を確立する	「正しい情報とデマ情報の識別」のためのリソースを確保する	「正しい情報とデマ情報の識別」を導入する（機材の場合は「設定する」を含む）	「正しい情報とデマ情報の識別」を保守（維持）する	「正しい情報とデマ情報の識別」について文書化する	「正しい情報とデマ情報の識別」の手順を確立する	「正しい情報とデマ情報の識別」の手順を明確化する	「正しい情報とデマ情報の識別」の手順を文書化する	「正しい情報とデマ情報の識別」の責任者を明確化する	「正しい情報とデマ情報の識別」を実施する	「正しい情報とデマ情報の識別」の実施を記録する	「正しい情報とデマ情報の識別」の実施時に注意を払う	「正しい情報とデマ情報の識別」について利用者を教育（訓練）する	「正しい情報とデマ情報の識別」についてレビューする	「正しい情報とデマ情報の識別」対策を見直す	「正しい情報とデマ情報の識別」の実施状況を監査する	「正しい情報とデマ情報の識別」の有効性（効果）の測定方法を決める	「正しい情報とデマ情報の識別」の有効性（効果）を測定する	「正しい情報とデマ情報の識別」を改善する	「正しい情報とデマ情報の識別」を廃止する
23	【色々な対象】の脆弱性診断の実施	【色々な対象：{Webアプリケーション}、{ネットワーク}、{サーバ}】の脆弱性診断を実施する。	「【色々な対象】の脆弱性診断の実施」について検討する	「【色々な対象】の脆弱性診断の実施」について計画する	「【色々な対象】の脆弱性診断の実施」のコストを算定する	「【色々な対象】の脆弱性診断の実施」の対策を確立する	「【色々な対象】の脆弱性診断の実施」のためのリソースを確保する	「【色々な対象】の脆弱性診断の実施」を導入する（機材の場合は「設定する」を含む）	「【色々な対象】の脆弱性診断の実施」を保守（維持）する	「【色々な対象】の脆弱性診断の実施」について文書化する	「【色々な対象】の脆弱性診断の実施」の手順を確立する	「【色々な対象】の脆弱性診断の実施」の手順を明確化する	「【色々な対象】の脆弱性診断の実施」の手順を文書化する	「【色々な対象】の脆弱性診断の実施」の責任者を明確化する	「【色々な対象】の脆弱性診断の実施」を実施する	「【色々な対象】の脆弱性診断の実施」の実施を記録する	「【色々な対象】の脆弱性診断の実施」の実施時に注意を払う	「【色々な対象】の脆弱性診断の実施」について利用者を教育（訓練）する	「【色々な対象】の脆弱性診断の実施」についてレビューする	「【色々な対象】の脆弱性診断の実施」対策を見直す	「【色々な対象】の脆弱性診断の実施」の実施状況を監査する	「【色々な対象】の脆弱性診断の実施」の有効性（効果）の測定方法を決める	「【色々な対象】の脆弱性診断の実施」の有効性（効果）を測定する	「【色々な対象】の脆弱性診断の実施」を改善する	「【色々な対象】の脆弱性診断の実施」を廃止する
24	【色々な対象】の脆弱性の【適切な対処】	【色々な対象：{Webアプリケーション}、{ネットワーク}、{サーバ}】の脆弱性を【適切に対処：{除去}、{セキュリティパッチの適用}、{軽減}】する。	「【色々な対象】の脆弱性の【適切な対処】」について検討する	「【色々な対象】の脆弱性の【適切な対処】」について計画する	「【色々な対象】の脆弱性の【適切な対処】」のコストを算定する	「【色々な対象】の脆弱性の【適切な対処】」の対策を確立する	「【色々な対象】の脆弱性の【適切な対処】」のためのリソースを確保する	「【色々な対象】の脆弱性の【適切な対処】」を導入する（機材の場合は「設定する」を含む）	「【色々な対象】の脆弱性の【適切な対処】」を保守（維持）する	「【色々な対象】の脆弱性の【適切な対処】」について文書化する	「【色々な対象】の脆弱性の【適切な対処】」の手順を確立する	「【色々な対象】の脆弱性の【適切な対処】」の手順を明確化する	「【色々な対象】の脆弱性の【適切な対処】」の手順を文書化する	「【色々な対象】の脆弱性の【適切な対処】」の責任者を明確化する	「【色々な対象】の脆弱性の【適切な対処】」を実施する	「【色々な対象】の脆弱性の【適切な対処】」の実施を記録する	「【色々な対象】の脆弱性の【適切な対処】」の実施時に注意を払う	「【色々な対象】の脆弱性の【適切な対処】」について利用者を教育（訓練）する	「【色々な対象】の脆弱性の【適切な対処】」についてレビューする	「【色々な対象】の脆弱性の【適切な対処】」対策を見直す	「【色々な対象】の脆弱性の【適切な対処】」の実施状況を監査する	「【色々な対象】の脆弱性の【適切な対処】」の有効性（効果）の測定方法を決める	「【色々な対象】の脆弱性の【適切な対処】」の有効性（効果）を測定する	「【色々な対象】の脆弱性の【適切な対処】」を改善する	「【色々な対象】の脆弱性の【適切な対処】」を廃止する
25	システムへの適切なアクセスを実現する【アクセス管理策】の導入	システムへの適切なアクセスを実現する【アクセス管理策：{ファイルに対するアクセス制限機能}、{本人確認機能}、{IDの不正使用防止機能}】を導入する	「システムへの適切なアクセスを実現する【アクセス管理策】の導入」について検討する	「システムへの適切なアクセスを実現する【アクセス管理策】の導入」について計画する	「システムへの適切なアクセスを実現する【アクセス管理策】の導入」のコストを算定する	「システムへの適切なアクセスを実現する【アクセス管理策】の導入」の対策を確立する	「システムへの適切なアクセスを実現する【アクセス管理策】の導入」のためのリソースを確保する	「システムへの適切なアクセスを実現する【アクセス管理策】の導入」を導入する（機材の場合は「設定する」を含む）	「システムへの適切なアクセスを実現する【アクセス管理策】の導入」を保守（維持）する	「システムへの適切なアクセスを実現する【アクセス管理策】の導入」について文書化する	「システムへの適切なアクセスを実現する【アクセス管理策】の導入」の手順を確立する	「システムへの適切なアクセスを実現する【アクセス管理策】の導入」の手順を明確化する	「システムへの適切なアクセスを実現する【アクセス管理策】の導入」の手順を文書化する	「システムへの適切なアクセスを実現する【アクセス管理策】の導入」の責任者を明確化する	「システムへの適切なアクセスを実現する【アクセス管理策】の導入」を実施する	「システムへの適切なアクセスを実現する【アクセス管理策】の導入」の実施を記録する	「システムへの適切なアクセスを実現する【アクセス管理策】の導入」の実施時に注意を払う	「システムへの適切なアクセスを実現する【アクセス管理策】の導入」について利用者を教育（訓練）する	「システムへの適切なアクセスを実現する【アクセス管理策】の導入」についてレビューする	「システムへの適切なアクセスを実現する【アクセス管理策】の導入」対策を見直す	「システムへの適切なアクセスを実現する【アクセス管理策】の導入」の実施状況を監査する	「システムへの適切なアクセスを実現する【アクセス管理策】の導入」の有効性（効果）の測定方法を決める	「システムへの適切なアクセスを実現する【アクセス管理策】の導入」の有効性（効果）を測定する	「システムへの適切なアクセスを実現する【アクセス管理策】の導入」を改善する	「システムへの適切なアクセスを実現する【アクセス管理策】の導入」を廃止する
26	マルウェアの感染報告	マルウェアの感染後に報告する。	「マルウェアの感染報告」について検討する	「マルウェアの感染報告」について計画する	「マルウェアの感染報告」のコストを算定する	「マルウェアの感染報告」の対策を確立する	「マルウェアの感染報告」のためのリソースを確保する	「マルウェアの感染報告」を導入する（機材の場合は「設定する」を含む）	「マルウェアの感染報告」を保守（維持）する	「マルウェアの感染報告」について文書化する	「マルウェアの感染報告」の手順を確立する	「マルウェアの感染報告」の手順を明確化する	「マルウェアの感染報告」の手順を文書化する	「マルウェアの感染報告」の責任者を明確化する	「マルウェアの感染報告」を実施する	「マルウェアの感染報告」の実施を記録する	「マルウェアの感染報告」の実施時に注意を払う	「マルウェアの感染報告」について利用者を教育（訓練）する	「マルウェアの感染報告」についてレビューする	「マルウェアの感染報告」対策を見直す	「マルウェアの感染報告」の実施状況を監査する	「マルウェアの感染報告」の有効性（効果）の測定方法を決める	「マルウェアの感染報告」の有効性（効果）を測定する	「マルウェアの感染報告」を改善する	「マルウェアの感染報告」を廃止する
27	【検出】のためのウイルス対策ソフトウェアの導入	【導入目的：{マルウェアの侵入の防止}、{スパイウェアの検出}、{スパイウェアの駆除}】のため、ウイルス対策ソフトウェアを導入する	「【検出】のためのウイルス対策ソフトウェアの導入」について検討する	「【検出】のためのウイルス対策ソフトウェアの導入」について計画する	「【検出】のためのウイルス対策ソフトウェアの導入」のコストを算定する	「【検出】のためのウイルス対策ソフトウェアの導入」の対策を確立する	「【検出】のためのウイルス対策ソフトウェアの導入」のためのリソースを確保する	「【検出】のためのウイルス対策ソフトウェアの導入」を導入する（機材の場合は「設定する」を含む）	「【検出】のためのウイルス対策ソフトウェアの導入」を保守（維持）する	「【検出】のためのウイルス対策ソフトウェアの導入」について文書化する	「【検出】のためのウイルス対策ソフトウェアの導入」の手順を確立する	「【検出】のためのウイルス対策ソフトウェアの導入」の手順を明確化する	「【検出】のためのウイルス対策ソフトウェアの導入」の手順を文書化する	「【検出】のためのウイルス対策ソフトウェアの導入」の責任者を明確化する	「【検出】のためのウイルス対策ソフトウェアの導入」を実施する	「【検出】のためのウイルス対策ソフトウェアの導入」の実施を記録する	「【検出】のためのウイルス対策ソフトウェアの導入」の実施時に注意を払う	「【検出】のためのウイルス対策ソフトウェアの導入」について利用者を教育（訓練）する	「【検出】のためのウイルス対策ソフトウェアの導入」についてレビューする	「【検出】のためのウイルス対策ソフトウェアの導入」対策を見直す	「【検出】のためのウイルス対策ソフトウェアの導入」の実施状況を監査する	「【検出】のためのウイルス対策ソフトウェアの導入」の有効性（効果）の測定方法を決める	「【検出】のためのウイルス対策ソフトウェアの導入」の有効性（効果）を測定する	「【検出】のためのウイルス対策ソフトウェアの導入」を改善する	「【検出】のためのウイルス対策ソフトウェアの導入」を廃止する
28	ウイルス対策ソフトウェアの正しい設定	ウイルス対策ソフトウェアを正しく設定する。	「ウイルス対策ソフトウェアの正しい設定」について検討する	「ウイルス対策ソフトウェアの正しい設定」について計画する	「ウイルス対策ソフトウェアの正しい設定」のコストを算定する	「ウイルス対策ソフトウェアの正しい設定」の対策を確立する	「ウイルス対策ソフトウェアの正しい設定」のためのリソースを確保する	「ウイルス対策ソフトウェアの正しい設定」を導入する（機材の場合は「設定する」を含む）	「ウイルス対策ソフトウェアの正しい設定」を保守（維持）する	「ウイルス対策ソフトウェアの正しい設定」について文書化する	「ウイルス対策ソフトウェアの正しい設定」の手順を確立する	「ウイルス対策ソフトウェアの正しい設定」の手順を明確化する	「ウイルス対策ソフトウェアの正しい設定」の手順を文書化する	「ウイルス対策ソフトウェアの正しい設定」の責任者を明確化する	「ウイルス対策ソフトウェアの正しい設定」を実施する	「ウイルス対策ソフトウェアの正しい設定」の実施を記録する	「ウイルス対策ソフトウェアの正しい設定」の実施時に注意を払う	「ウイルス対策ソフトウェアの正しい設定」について利用者を教育（訓練）する	「ウイルス対策ソフトウェアの正しい設定」についてレビューする	「ウイルス対策ソフトウェアの正しい設定」対策を見直す	「ウイルス対策ソフトウェアの正しい設定」の実施状況を監査する	「ウイルス対策ソフトウェアの正しい設定」の有効性（効果）の測定方法を決める	「ウイルス対策ソフトウェアの正しい設定」の有効性（効果）を測定する	「ウイルス対策ソフトウェアの正しい設定」を改善する	「ウイルス対策ソフトウェアの正しい設定」を廃止する
29	ウイルス対策ソフトウェアによるスキャン	ウイルス対策ソフトウェアでスキャンする。	「ウイルス対策ソフトウェアによるスキャン」について検討する	「ウイルス対策ソフトウェアによるスキャン」について計画する	「ウイルス対策ソフトウェアによるスキャン」のコストを算定する	「ウイルス対策ソフトウェアによるスキャン」の対策を確立する	「ウイルス対策ソフトウェアによるスキャン」のためのリソースを確保する	「ウイルス対策ソフトウェアによるスキャン」を導入する（機材の場合は「設定する」を含む）	「ウイルス対策ソフトウェアによるスキャン」を保守（維持）する	「ウイルス対策ソフトウェアによるスキャン」について文書化する	「ウイルス対策ソフトウェアによるスキャン」の手順を確立する	「ウイルス対策ソフトウェアによるスキャン」の手順を明確化する	「ウイルス対策ソフトウェアによるスキャン」の手順を文書化する	「ウイルス対策ソフトウェアによるスキャン」の責任者を明確化する	「ウイルス対策ソフトウェアによるスキャン」を実施する	「ウイルス対策ソフトウェアによるスキャン」の実施を記録する	「ウイルス対策ソフトウェアによるスキャン」の実施時に注意を払う	「ウイルス対策ソフトウェアによるスキャン」について利用者を教育（訓練）する	「ウイルス対策ソフトウェアによるスキャン」についてレビューする	「ウイルス対策ソフトウェアによるスキャン」対策を見直す	「ウイルス対策ソフトウェアによるスキャン」の実施状況を監査する	「ウイルス対策ソフトウェアによるスキャン」の有効性（効果）の測定方法を決める	「ウイルス対策ソフトウェアによるスキャン」の有効性（効果）を測定する	「ウイルス対策ソフトウェアによるスキャン」を改善する	「ウイルス対策ソフトウェアによるスキャン」を廃止する
30	複数ベンダーが提供するウイルス対策ソフトの利用	複数ベンダーが提供する、不正プログラム対策ソフトを利用する。	「複数ベンダーが提供するウイルス対策ソフトの利用」について検討する	「複数ベンダーが提供するウイルス対策ソフトの利用」について計画する	「複数ベンダーが提供するウイルス対策ソフトの利用」のコストを算定する	「複数ベンダーが提供するウイルス対策ソフトの利用」の対策を確立する	「複数ベンダーが提供するウイルス対策ソフトの利用」のためのリソースを確保する	「複数ベンダーが提供するウイルス対策ソフトの利用」を導入する（機材の場合は「設定する」を含む）	「複数ベンダーが提供するウイルス対策ソフトの利用」を保守（維持）する	「複数ベンダーが提供するウイルス対策ソフトの利用」について文書化する	「複数ベンダーが提供するウイルス対策ソフトの利用」の手順を確立する	「複数ベンダーが提供するウイルス対策ソフトの利用」の手順を明確化する	「複数ベンダーが提供するウイルス対策ソフトの利用」の手順を文書化する	「複数ベンダーが提供するウイルス対策ソフトの利用」の責任者を明確化する	「複数ベンダーが提供するウイルス対策ソフトの利用」を実施する	「複数ベンダーが提供するウイルス対策ソフトの利用」の実施を記録する	「複数ベンダーが提供するウイルス対策ソフトの利用」の実施時に注意を払う	「複数ベンダーが提供するウイルス対策ソフトの利用」について利用者を教育（訓練）する	「複数ベンダーが提供するウイルス対策ソフトの利用」についてレビューする	「複数ベンダーが提供するウイルス対策ソフトの利用」対策を見直す	「複数ベンダーが提供するウイルス対策ソフトの利用」の実施状況を監査する	「複数ベンダーが提供するウイルス対策ソフトの利用」の有効性（効果）の測定方法を決める	「複数ベンダーが提供するウイルス対策ソフトの利用」の有効性（効果）を測定する	「複数ベンダーが提供するウイルス対策ソフトの利用」を改善する	「複数ベンダーが提供するウイルス対策ソフトの利用」を廃止する
31	ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと	定義ファイルおよびスキャンエンジンを【最新に保つ：{正しい設定により自動的に更新する}{新しいリリースが入手可能な場合はすぐに入手し定めに従って更新する}、{最新に保つための管理サーバを置く}】。	「ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと」について検討する	「ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと」について計画する	「ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと」のコストを算定する	「ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと」の対策を確立する	「ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと」のためのリソースを確保する	「ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと」を導入する（機材の場合は「設定する」を含む）	「ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと」を保守（維持）する	「ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと」について文書化する	「ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと」の手順を確立する	「ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと」の手順を明確化する	「ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと」の手順を文書化する	「ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと」の責任者を明確化する	「ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと」を実施する	「ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと」の実施を記録する	「ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと」の実施時に注意を払う	「ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと」について利用者を教育（訓練）する	「ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと」についてレビューする	「ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと」対策を見直す	「ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと」の実施状況を監査する	「ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと」の有効性（効果）の測定方法を決める	「ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと」の有効性（効果）を測定する	「ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと」を改善する	「ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと」を廃止する
32	プログラムやデータのバックアップの取得	プログラムやデータのバックアップを取得する	「プログラムやデータのバックアップの取得」について検討する	「プログラムやデータのバックアップの取得」について計画する	「プログラムやデータのバックアップの取得」のコストを算定する	「プログラムやデータのバックアップの取得」の対策を確立する	「プログラムやデータのバックアップの取得」のためのリソースを確保する	「プログラムやデータのバックアップの取得」を導入する（機材の場合は「設定する」を含む）	「プログラムやデータのバックアップの取得」を保守（維持）する	「プログラムやデータのバックアップの取得」について文書化する	「プログラムやデータのバックアップの取得」の手順を確立する	「プログラムやデータのバックアップの取得」の手順を明確化する	「プログラムやデータのバックアップの取得」の手順を文書化する	「プログラムやデータのバックアップの取得」の責任者を明確化する	「プログラムやデータのバックアップの取得」を実施する	「プログラムやデータのバックアップの取得」の実施を記録する	「プログラムやデータのバックアップの取得」の実施時に注意を払う	「プログラムやデータのバックアップの取得」について利用者を教育（訓練）する	「プログラムやデータのバックアップの取得」についてレビューする	「プログラムやデータのバックアップの取得」対策を見直す	「プログラムやデータのバックアップの取得」の実施状況を監査する	「プログラムやデータのバックアップの取得」の有効性（効果）の測定方法を決める	「プログラムやデータのバックアップの取得」の有効性（効果）を測定する	「プログラムやデータのバックアップの取得」を改善する	「プログラムやデータのバックアップの取得」を廃止する
33	プログラムのオリジナルファイルにライトプロテクトを施して保管	プログラムのオリジナルファイルにはライトプロテクトを施して保管する。	「プログラムのオリジナルファイルにライトプロテクトを施して保管」について検討する	「プログラムのオリジナルファイルにライトプロテクトを施して保管」について計画する	「プログラムのオリジナルファイルにライトプロテクトを施して保管」のコストを算定する	「プログラムのオリジナルファイルにライトプロテクトを施して保管」の対策を確立する	「プログラムのオリジナルファイルにライトプロテクトを施して保管」のためのリソースを確保する	「プログラムのオリジナルファイルにライトプロテクトを施して保管」を導入する（機材の場合は「設定する」を含む）	「プログラムのオリジナルファイルにライトプロテクトを施して保管」を保守（維持）する	「プログラムのオリジナルファイルにライトプロテクトを施して保管」について文書化する	「プログラムのオリジナルファイルにライトプロテクトを施して保管」の手順を確立する	「プログラムのオリジナルファイルにライトプロテクトを施して保管」の手順を明確化する	「プログラムのオリジナルファイルにライトプロテクトを施して保管」の手順を文書化する	「プログラムのオリジナルファイルにライトプロテクトを施して保管」の責任者を明確化する	「プログラムのオリジナルファイルにライトプロテクトを施して保管」を実施する	「プログラムのオリジナルファイルにライトプロテクトを施して保管」の実施を記録する	「プログラムのオリジナルファイルにライトプロテクトを施して保管」の実施時に注意を払う	「プログラムのオリジナルファイルにライトプロテクトを施して保管」について利用者を教育（訓練）する	「プログラムのオリジナルファイルにライトプロテクトを施して保管」についてレビューする	「プログラムのオリジナルファイルにライトプロテクトを施して保管」対策を見直す	「プログラムのオリジナルファイルにライトプロテクトを施して保管」の実施状況を監査する	「プログラムのオリジナルファイルにライトプロテクトを施して保管」の有効性（効果）の測定方法を決める	「プログラムのオリジナルファイルにライトプロテクトを施して保管」の有効性（効果）を測定する	「プログラムのオリジナルファイルにライトプロテクトを施して保管」を改善する	「プログラムのオリジナルファイルにライトプロテクトを施して保管」を廃止する
34	システムの変更管理の実施	システムの変更管理を行う。	「システムの変更管理の実施」について検討する	「システムの変更管理の実施」について計画する	「システムの変更管理の実施」のコストを算定する	「システムの変更管理の実施」の対策を確立する	「システムの変更管理の実施」のためのリソースを確保する	「システムの変更管理の実施」を導入する（機材の場合は「設定する」を含む）	「システムの変更管理の実施」を保守（維持）する	「システムの変更管理の実施」について文書化する	「システムの変更管理の実施」の手順を確立する	「システムの変更管理の実施」の手順を明確化する	「システムの変更管理の実施」の手順を文書化する	「システムの変更管理の実施」の責任者を明確化する	「システムの変更管理の実施」を実施する	「システムの変更管理の実施」の実施を記録する	「システムの変更管理の実施」の実施時に注意を払う	「システムの変更管理の実施」について利用者を教育（訓練）する	「システムの変更管理の実施」についてレビューする	「システムの変更管理の実施」対策を見直す	「システムの変更管理の実施」の実施状況を監査する	「システムの変更管理の実施」の有効性（効果）の測定方法を決める	「システムの変更管理の実施」の有効性（効果）を測定する	「システムの変更管理の実施」を改善する	「システムの変更管理の実施」を廃止する
35	【駆除】のためのウイルス対策ソフトウェアの導入	【駆除】のため、ウイルス対策ソフトウェアを導入する	「【駆除】のためのウイルス対策ソフトウェアの導入」について検討する	「【駆除】のためのウイルス対策ソフトウェアの導入」について計画する	「【駆除】のためのウイルス対策ソフトウェアの導入」のコストを算定する	「【駆除】のためのウイルス対策ソフトウェアの導入」の対策を確立する	「【駆除】のためのウイルス対策ソフトウェアの導入」のためのリソースを確保する	「【駆除】のためのウイルス対策ソフトウェアの導入」を導入する（機材の場合は「設定する」を含む）	「【駆除】のためのウイルス対策ソフトウェアの導入」を保守（維持）する	「【駆除】のためのウイルス対策ソフトウェアの導入」について文書化する	「【駆除】のためのウイルス対策ソフトウェアの導入」の手順を確立する	「【駆除】のためのウイルス対策ソフトウェアの導入」の手順を明確化する	「【駆除】のためのウイルス対策ソフトウェアの導入」の手順を文書化する	「【駆除】のためのウイルス対策ソフトウェアの導入」の責任者を明確化する	「【駆除】のためのウイルス対策ソフトウェアの導入」を実施する	「【駆除】のためのウイルス対策ソフトウェアの導入」の実施を記録する	「【駆除】のためのウイルス対策ソフトウェアの導入」の実施時に注意を払う	「【駆除】のためのウイルス対策ソフトウェアの導入」について利用者を教育（訓練）する	「【駆除】のためのウイルス対策ソフトウェアの導入」についてレビューする	「【駆除】のためのウイルス対策ソフトウェアの導入」対策を見直す	「【駆除】のためのウイルス対策ソフトウェアの導入」の実施状況を監査する	「【駆除】のためのウイルス対策ソフトウェアの導入」の有効性（効果）の測定方法を決める	「【駆除】のためのウイルス対策ソフトウェアの導入」の有効性（効果）を測定する	「【駆除】のためのウイルス対策ソフトウェアの導入」を改善する	「【駆除】のためのウイルス対策ソフトウェアの導入」を廃止する
36	保険の適用	保険を適用する。	「保険の適用」について検討する	「保険の適用」について計画する	「保険の適用」のコストを算定する	「保険の適用」の対策を確立する	「保険の適用」のためのリソースを確保する	「保険の適用」を導入する（機材の場合は「設定する」を含む）	「保険の適用」を保守（維持）する	「保険の適用」について文書化する	「保険の適用」の手順を確立する	「保険の適用」の手順を明確化する	「保険の適用」の手順を文書化する	「保険の適用」の責任者を明確化する	「保険の適用」を実施する	「保険の適用」の実施を記録する	「保険の適用」の実施時に注意を払う	「保険の適用」について利用者を教育（訓練）する	「保険の適用」についてレビューする	「保険の適用」対策を見直す	「保険の適用」の実施状況を監査する	「保険の適用」の有効性（効果）の測定方法を決める	「保険の適用」の有効性（効果）を測定する	「保険の適用」を改善する	「保険の適用」を廃止する