NIST Special Publication 800-53
Revision 2 から抜粋

連邦政府情報システムにおける推奨セキュリティ管理策

中位影響レベルのベースライン

National Institute of Standards and Technology
U.S. Department of Commerce

情報セキュリティ

付録 2

コンピュータセキュリティ部門
情報技術ラボラトリ
米国国立標準技術研究所
Gaithersburg, MD 20899-8930

2007 年 12 月

米国商務省
Carlos M. Gutierrez, Secretary

米国国立標準技術研究所
James M. Turner, Acting Director

この文書は下記団体によって翻訳監修されています

IPA 独立行政法人 情報処理推進機構 INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
NRI SECURE TECHNOLOGIES

付録 2

ベースラインセキュリティ管理策

中位影響レベルの情報システム

組織は、法律、大統領令、指令、ポリシーまたは規定（例：連邦政府の情報セキュリティマネジメント法（FISMA： Federal Information Security Management Act、OMB 通達 A-130 の付録第 III 編など）が定めるセキュリティ要件に準拠した、セキュリティ管理策の採用を求められている。組織にとっての課題は、適切なセキュリティ管理策を選択することである。適切なセキュリティ管理策とは、導入後にその有効性が証明されるものであり、かつ費用対効果が高い方法でセキュリティ要件を満たすものでなければならない。組織にとって、特定の（場合によっては一意な）セキュリティ要件を満たすためのセキュリティ管理策を正しく選択することは、重要なタスクである。このタスクを遂行することにより、組織は、セキュリティに対する組織のコミットメントを示し、自身の情報や情報システムの機密性、完全性、可用性を保護するために適切な注意を払っていることを示すことができる。最終的な目標は、脅威に直面しても安心して利用できる情報システムを構築することにある。

本書では、適切なセキュリティ管理策の選択を支援するために、ベースライン管理策の考え方を導入している。ベースライン管理策とは、情報システムに推奨されるセキュリティ管理策の初期セットのことであり、管理策の選択は、FIPS199 のセキュリティ分類をもとに行う。1 表 1に、NIST Special Publication 800-53 の付録 D から抜粋した、中位影響レベルのベースラインのセキュリティ管理策および管理強化策の一覧を示す。パート 1 では、それらの管理策および管理強化策の詳細を記述する。パート 2 では、NIST Special Publication 800-53 の付録 E から抜粋した、中位影響レベルの情報システムに対する必要最低限の保証要件を記述する。

組織は、NIST Special Publication 800-53 の 3.3 章の管理策の調整ガイダンスに従って、中位影響レベルのベースライン管理策を調整することを奨励する。調整された管理策は、組織が、自身の情報システムを保護するための手段や対策を決定する際の、開始点となるものである。組織の業務（ミッション、機能、イメージおよび評判を含む）や資産、および個人に対するリスクを適切に緩和するためには、ベースラインに対する補足（NIST Special Publication 800-53 の 3.4 章を参照）が必要になると思われる。ベースラインへの補足は、組織のリスクアセスメントの結果に基づいて行われ、補足されたベースラインは文章化され、セキュリティ計画の中に盛り込まれる。補足されたベースラインとリスクを適切に低減するためのシステムの利用制限は、セキュリティに関する善管注意義務（security due diligence）を遵守するためのものである。

[1] FIPS 199 のセキュリティ分類は、組織の任務（組織に与えられたミッションの達成、組織の資産の保護、法的責任の遂行、日常の業務の継続、および個人の保護）を支援する情報および情報システムに対して、脅威をもたらす何らかのイベントが発生した場合の、組織または個人への潜在的影響をベースにしている。

表 1: ベースラインセキュリティ管理策の一覧

管理策番号	管理策名	管理策ベースライン		
		低	中	高
アクセス制御				
AC-1	アクセス制御の方針と手順	AC-1	AC-1	AC-1
AC-2	アカウント管理	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
AC-3	アクセス制御の実施	AC-3	AC-3 (1)	AC-3 (1)
AC-4	情報フロー制御の実施	未選択	AC-4	AC-4
AC-5	職務の分離	未選択	AC-5	AC-5
AC-6	特権の最小化	未選択	AC-6	AC-6
AC-7	ログイン試行の失敗	AC-7	AC-7	AC-7
AC-8	システムの利用に関する通知	AC-8	AC-8	AC-8
AC-9	前回のログオンに関する通知	未選択	未選択	未選択
AC-10	同時セッションの管理	未選択	未選択	AC-10
AC-11	セッションのロック	未選択	AC-11	AC-11
AC-12	セッションの終了	未選択	AC-12	AC-12 (1)
AC-13	監視とレビュー － アクセス制御	AC-13	AC-13 (1)	AC-13 (1)
AC-14	識別または認証なしで許可される活動	AC-14	AC-14 (1)	AC-14 (1)
AC-15	自動マーキング	未選択	未選択	AC-15
AC-16	自動ラベリング	未選択	未選択	未選択
AC-17	リモートアクセス	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	無線アクセスの制限	AC-18	AC-18 (1)	AC-18 (1) (2)
AC-19	携帯機器に対するアクセス制御	未選択	AC-19	AC-19
AC-20	外部情報システムの利用	AC-20	AC-20 (1)	AC-20 (1)
意識向上およびトレーニング				
AT-1	セキュリティの意識向上およびトレーニングの方針と手順	AT-1	AT-1	AT-1
AT-2	セキュリティの意識向上	AT-2	AT-2	AT-2
AT-3	セキュリティトレーニング	AT-3	AT-3	AT-3
AT-4	セキュリティトレーニングの記録	AT-4	AT-4	AT-4
AT-5	セキュリティグループまたは関係者との連絡	未選択	未選択	未選択
監査および責任追跡性				
AU-1	監査および責任追跡性の方針と手順	AU-1	AU-1	AU-1
AU-2	監査対象のイベント	AU-2	AU-2 (3)	AU-2 (1) (2) (3)
AU-3	監査記録の内容	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	監査記録の保存容量	AU-4	AU-4	AU-4
AU-5	監査処理の不具合に対する対応	AU-5	AU-5	AU-5 (1) (2)
AU-6	監査記録の監視、分析および報告	未選択	AU-6 (2)	AU-6 (1) (2)
AU-7	監査量の低減と報告書の作成	未選択	AU-7 (1)	AU-7 (1)

管理策番号	管理策名	管理策ベースライン		
		低	中	高
AU-8	タイムスタンプ	AU-8	AU-8 (1)	AU-8 (1)
AU-9	監査情報の保護	AU-9	AU-9	AU-9
AU-10	否認防止	未選択	未選択	未選択
AU-11	監査記録の保持	AU-11	AU-11	AU-11
承認、運用認可、セキュリティ評価				
CA-1	承認、運用認可、セキュリティ評価の方針と手順	CA-1	CA-1	CA-1
CA-2	セキュリティ評価	CA-2	CA-2	CA-2
CA-3	情報システムの接続	CA-3	CA-3	CA-3
CA-4	セキュリティ承認	CA-4	CA-4 (1)	CA-4 (1)
CA-5	行動計画とマイルストーン	CA-5	CA-5	CA-5
CA-6	セキュリティの運用認可	CA-6	CA-6	CA-6
CA-7	継続的な監視	CA-7	CA-7	CA-7
構成管理				
CM-1	構成管理の方針と手順	CM-1	CM-1	CM-1
CM-2	ベースライン構成	CM-2	CM-2 (1)	CM-2 (1) (2)
CM-3	構成変更管理	未選択	CM-3	CM-3 (1)
CM-4	構成変更の監視	未選択	CM-4	CM-4
CM-5	変更のためのアクセス制限	未選択	CM-5	CM-5 (1)
CM-6	構成設定	CM-6	CM-6	CM-6 (1)
CM-7	機能の最小化	未選択	CM-7	CM-7 (1)
CM-8	情報システムコンポーネントのインベントリ	CM-8	CM-8 (1)	CM-8 (1) (2)
緊急時対応計画				
CP-1	緊急時対応計画の方針と手順	CP-1	CP-1	CP-1
CP-2	緊急時対応計画	CP-2	CP-2 (1)	CP-2 (1) (2)
CP-3	緊急時対応トレーニング	未選択	CP-3	CP-3 (1)
CP-4	緊急時対応計画のテストと実習	CP-4	CP-4 (1)	CP-4 (1) (2)
CP-5	緊急時対応計画の更新	CP-5	CP-5	CP-5
CP-6	(情報システムの)代替保管拠点	未選択	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	(情報システムの)代替処理拠点	未選択	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	電気通信サービス	未選択	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	情報システムのバックアップ	CP-9	CP-9 (1) (4)	CP-9 (1) (2) (3) (4)
CP-10	情報システムの復旧と再構成	CP-10	CP-10	CP-10 (1)
識別および認証				
IA-1	識別および認証の方針と手順	IA-1	IA-1	IA-1
IA-2	ユーザ識別および認証	IA-2	IA-2 (1)	IA-2 (2) (3)
IA-3	デバイスの識別および認証	未選択	IA-3	IA-3
IA-4	識別子(identifier)の管理	IA-4	IA-4	IA-4

管理策番号	管理策名	管理策ベースライン		
		低	中	高
IA-5	認証コード（Authenticator）の管理	IA-5	IA-5	IA-5
IA-6	認証コード（Authenticator）のフィードバック	IA-6	IA-6	IA-6
IA-7	暗号モジュールの認証	IA-7	IA-7	IA-7
インシデント対応				
IR-1	インシデント対応の方針と手順	IR-1	IR-1	IR-1
IR-2	インシデント対応のトレーニング	未選択	IR-2	IR-2 (1)
IR-3	インシデント対応のテストと実習	未選択	IR-3	IR-3 (1)
IR-4	インシデントの対応	IR-4	IR-4 (1)	IR-4 (1)
IR-5	インシデントの監視	未選択	IR-5	IR-5 (1)
IR-6	インシデントの報告	IR-6	IR-6 (1)	IR-6 (1)
IR-7	インシデント対応の支援	IR-7	IR-7 (1)	IR-7 (1)
保守				
MA-1	システム保守の方針と手順	MA-1	MA-1	MA-1
MA-2	定期的な保守	MA-2	MA-2 (1)	MA-2 (1) (2)
MA-3	保守ツール	未選択	MA-3	MA-3 (1) (2) (3)
MA-4	遠隔保守	MA-4	MA-4 (1) (2)	MA-4 (1) (2) (3)
MA-5	保守要員	MA-5	MA-5	MA-5
MA-6	時宜を得た保守	未選択	MA-6	MA-6
記録媒体の保護				
MP-1	記録媒体保護の方針と手順	MP-1	MP-1	MP-1
MP-2	記録媒体へのアクセス	MP-2	MP-2 (1)	MP-2 (1)
MP-3	記録媒体へのラベル付け	未選択	未選択	MP-3
MP-4	記録媒体の保管	未選択	MP-4	MP-4
MP-5	記録媒体の輸送	未選択	MP-5 (1) (2)	MP-5 (1) (2) (3)
MP-6	媒体上の記録の抹消と媒体の廃棄	MP-6	MP-6	MP-6 (1) (2)
物理的および環境的な保護				
PE-1	物理的および環境的な保護の方針と手順	PE-1	PE-1	PE-1
PE-2	物理的アクセス権限	PE-2	PE-2	PE-2
PE-3	物理的アクセス制御	PE-3	PE-3	PE-3 (1)
PE-4	伝送媒体へのアクセス制御	未選択	未選択	PE-4
PE-5	表示媒体へのアクセス制御	未選択	PE-5	PE-5
PE-6	物理的アクセスの監視	PE-6	PE-6 (1)	PE-6 (1) (2)
PE-7	来訪者の管理	PE-7	PE-7 (1)	PE-7 (1)
PE-8	アクセス記録	PE-8	PE-8	PE-8 (1) (2)
PE-9	電源装置および電源ケーブル配線	未選択	PE-9	PE-9
PE-10	緊急遮断	未選択	PE-10	PE-10 (1)
PE-11	非常時用電源	未選択	PE-11	PE-11 (1)
PE-12	非常時用照明	PE-12	PE-12	PE-12
PE-13	防火	PE-13	PE-13 (1) (2)	PE-13 (1) (2)

管理策番号	管理策名	管理策ベースライン		
		低	中	高
			(3)	(3)
PE-14	温度および湿度の管理	PE-14	PE-14	PE-14
PE-15	浸水による損害からの保護	PE-15	PE-15	PE-15 (1)
PE-16	荷物の搬入と搬出	PE-16	PE-16	PE-16
PE-17	代替作業拠点	未選択	PE-17	PE-17
PE-18	情報システムコンポーネントの所在地	未選択	PE-18	PE-18 (1)
PE-19	情報の漏洩	未選択	未選択	未選択
計画作成				
PL-1	セキュリティ計画作成の方針と手順	PL-1	PL-1	PL-1
PL-2	システムセキュリティ計画	PL-2	PL-2	PL-2
PL-3	システムセキュリティ計画の更新	PL-3	PL-3	PL-3
PL-4	行動規則	PL-4	PL-4	PL-4
PL-5	プライバシーの影響評価	PL-5	PL-5	PL-5
PL-6	セキュリティ関連の活動計画作成	未選択	PL-6	PL-6
人的セキュリティ				
PS-1	人的セキュリティの方針および手順	PS-1	PS-1	PS-1
PS-2	職位の分類	PS-2	PS-2	PS-2
PS-3	要員に対する審査	PS-3	PS-3	PS-3
PS-4	要員の解雇	PS-4	PS-4	PS-4
PS-5	人事異動	PS-5	PS-5	PS-5
PS-6	アクセス契約	PS-6	PS-6	PS-6
PS-7	第三者の人的セキュリティ	PS-7	PS-7	PS-7
PS-8	要員に対する制裁	PS-8	PS-8	PS-8
リスクアセスメント				
RA-1	リスクアセスメントの方針と手順	RA-1	RA-1	RA-1
RA-2	セキュリティ分類	RA-2	RA-2	RA-2
RA-3	リスクアセスメント	RA-3	RA-3	RA-3
RA-4	リスクアセスメントの更新	RA-4	RA-4	RA-4
RA-5	脆弱性のスキャン（走査）	未選択	RA-5	RA-5 (1) (2)
システムおよびサービスの調達				
SA-1	システムおよびサービスの調達の方針と手順	SA-1	SA-1	SA-1
SA-2	リソースの割り当て	SA-2	SA-2	SA-2
SA-3	ライフサイクルサポート	SA-3	SA-3	SA-3
SA-4	調達	SA-4	SA-4 (1)	SA-4 (1)
SA-5	情報システムの文書化	SA-5	SA-5 (1)	SA-5 (1) (2)
SA-6	ソフトウェアの利用の制限	SA-6	SA-6	SA-6
SA-7	ユーザがインストールしたソフトウェア	SA-7	SA-7	SA-7
SA-8	セキュリティエンジニアリングの原則	未選択	SA-8	SA-8
SA-9	外部の情報システムサービス	SA-9	SA-9	SA-9

管理策番号	管理策名	管理策ベースライン		
		低	中	高
SA-10	開発者による構成管理	未選択	未選択	SA-10
SA-11	開発者によるセキュリティテスト	未選択	SA-11	SA-11
システムおよび通信の保護				
SC-1	システムおよび通信の保護の方針と手順	SC-1	SC-1	SC-1
SC-2	アプリケーションの分離	未選択	SC-2	SC-2
SC-3	セキュリティ機能の隔離	未選択	未選択	SC-3
SC-4	残存情報	未選択	SC-4	SC-4
SC-5	サービス妨害（DoS）からの保護	SC-5	SC-5	SC-5
SC-6	リソースの優先度	未選択	未選択	未選択
SC-7	境界保護	SC-7	SC-7 (1) (2) (3) (4) (5)	SC-7 (1) (2) (3) (4) (5) (6)
SC-8	伝送する情報の完全性	未選択	SC-8	SC-8 (1)
SC-9	伝送する情報の機密性	未選択	SC-9	SC-9 (1)
SC-10	ネットワークの切断	未選択	SC-10	SC-10
SC-11	高信頼経路	未選択	未選択	未選択
SC-12	暗号鍵の確立と管理	未選択	SC-12	SC-12
SC-13	暗号化の利用	SC-13	SC-13	SC-13
SC-14	パブリックアクセスからの保護	SC-14	SC-14	SC-14
SC-15	共同コンピューティング	未選択	SC-15	SC-15
SC-16	セキュリティパラメータの送信	未選択	未選択	未選択
SC-17	公開鍵基盤の承認	未選択	SC-17	SC-17
SC-18	モバイルコード	未選択	SC-18	SC-18
SC-19	ボイスオーバーインターネットプロトコル（VoIP）	未選択	SC-19	SC-19
SC-20	セキュアネーム／アドレスレゾリューションサービス（信頼のおける情報資源）	未選択	SC-20	SC-20
SC-21	セキュアネーム／アドレスレゾリューションサービス（再帰的／キャッシュリゾルバー）	未選択	未選択	SC-21
SC-22	ネーム／アドレスレゾリューションサービスの構成およびサービスの提供	未選択	SC-22	SC-22
SC-23	セッションの真正性	未選択	SC-23	SC-23
システムおよび情報の完全性				
SI-1	システムおよび情報の完全性に対する方針と手順	SI-1	SI-1	SI-1
SI-2	欠陥の修正	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	悪意のコード（不正プログラム）からの保護	SI-3	SI-3 (1) (2)	SI-3 (1) (2)
SI-4	情報システムの監視ツールおよび監視技法	未選択	SI-4 (4)	SI-4 (2) (4) (5)
SI-5	セキュリティ警報と勧告	SI-5	SI-5	SI-5 (1)
SI-6	セキュリティ機能の検証	未選択	未選択	SI-6
SI-7	ソフトウェアおよび情報の完全性	未選択	未選択	SI-7 (1) (2)
SI-8	スパムからの保護	未選択	SI-8	SI-8 (1)
SI-9	情報入力の制限	未選択	SI-9	SI-9

管理策番号	管理策名	管理策ベースライン		
		低	中	高
SI-10	情報の正確さ、完全性、有効性および真正性	未選択	SI-10	SI-10
SI-11	エラー処理	未選択	SI-11	SI-11
SI-12	情報システムからの出力の取扱いと保存	未選択	SI-12	SI-12

セキュリティ管理策のベースラインへの補足(ICS 編)

次の表は、NIST Special Publication 800-53 の付録Dに記載のベースライン管理策に対する、ICS 関連の補足事項（太字で強調表示している）をまとめたものである。

管理策番号	管理策名	管理策のベースライン		
		低	中	高
アクセス制御				
AC-3	アクセス制御	AC-3	AC-3 (1) **(ICS-1)**	AC-3 (1) **(ICS-1)**
構成管理				
CM-3	構成変更管理	未選択	CM-3 **(ICS-1)**	CM-3 (1) **(ICS-1)**
物理的および環境的な保護				
PE-9	電源装置および電源ケーブル配線	未選択	PE-9 **(1)**	PE-9 **(1)**
PE-11	非常時用電源	**PE-11**	PE-11 **(1)**	PE-11 (1) **(2)**

パート I

セキュリティ管理策および管理強化策

中位影響レベルの情報システム

ファミリ: アクセス制御 **クラス:** 技術

AC-1 アクセス制御の方針と手順

管理策：組織は、以下のものを策定および周知徹底し、定期的にレビュー／更新する。(i) 正式に文書化された、アクセス制御に関する方針。これらの方針では、目的、適用範囲、役割、責任、経営陣のコミットメント、組織間の調整、およびコンプライアンスを取り扱う。(ii) 正式に文書化された、セキュリティのアクセス制御方針の導入に関する手順。この手順は、アクセス制御方針の導入、ならびに関連する管理策の導入を容易にするために使用される。

補足ガイダンス：アクセス制御の方針と手順は、適用法、大統領令、指令、方針、規則、基準、およびガイダンスに準拠する。アクセス制御方針は、組織の一般的な情報セキュリティ方針の一部とすることができる。アクセス制御手順は、一般的なセキュリティプログラムの一部として作成することもできれば、必要に応じて特定の情報システムに特化した形で作成することもできる。セキュリティ方針および手順に関するガイダンスは、NIST Special Publication 800-12 に記載されている。

管理強化策：なし。

AC-2 アカウント管理

管理策：組織は、情報システムのアカウント管理(アカウントの作成、有効化、修正、見直し、無効化、削除などを含む)を行う。組織は情報システムアカウントの見直しを、[指定：組織が定める頻度（少なくとも年1回）]間隔で行う。

補足ガイダンス：アカウント管理には、アカウントの種類（個人、グループ、システムなど）の特定、グループに加わるための条件の設定、および関連する権限の付与などが含まれる。組織は、情報システムの利用を許可されたユーザを特定し、彼らのアクセス権を設定する。組織は、以下の条件にもとづいて、情報システムへのアクセスを許可する。(i) 割り当てられた職務、および担当者としてすべてのセキュリティ基準を満たしていることを考慮した結果、情報システムについて知る必要があると判断される場合、または、システムを共有する必要があると判断される場合 (ii) システムを使用する目的が正当である。組織は、アカウント作成要求に対して、身分の証明を要求し、正当な要求であると判断した場合には要求を受け入れる。組織は、ゲストアカウントまたは匿名アカウントの使用を認可し、それらのアカウントの使用状況を監視すると同時に、不要なアカウントを削除または無効化する、もしくは安全策を検討する。情報システムのユーザが、解雇または人事異動を理由に職場を離れる場合には、その旨がアカウントマネージャに通知され、そのユーザのアカウントが削除または無効化される、もしくは安全策が講じられる。情報システムに関してユーザが知るべきことや共有すべきことに変化が生じた場合、または、システムの使用方法が変更された場合にも、その旨がアカウントマネージャに通知される。

管理強化策：

(1) 組織は情報システムのアカウント管理を支援する自動化メカニズムを採用する。

(2) 情報システムは、一時アカウントおよび緊急アカウントを、[指定：組織がアカウントの種類ごとに指定する期間]の経過後に自動的に削除する。

(3) 情報システムは、長期間使用されていないアカウントを、[指定：組織がアカウントの種類ごとに指定する期間]の経過後に自動的に無効化する。

(4) 組織は、アカウントの作成、修正、無効化、および終了活動を監査し、その結果を必要に応じて適切な担当者に通知するための、自動化メカニズムを採用する。

AC-3 アクセス制御の実施

管理策：情報システムは、適用方針に従って、与えられたアクセス制御権を行使する。

補足ガイダンス：アクセス制御方針（識別情報に基づく方針、役割に基づく方針、規則に基づく方針など）および対応するアクセス制御権行使メカニズム（アクセス制御リスト、アクセス制御マトリクス、暗号技術など）は、組織が、ユーザ（またはユーザの作業を代行するプロセス）とオブジェクト（装置、ファイル、レコード、プロセス、プログラム、ドメインなど）間のアクセスを制御するために利用する。組織は、情報システムレベルのアクセス制御に加えて、組織の情報セキュリティの向上のために必要に応じて、アプリケーションレベルのアクセス制御行使メカニズムを採用する。緊急の事象、または他の重大な事象が発生した場合には、自動化メカニズムを代用する手動化メカニズム（統制されているメカニズムで、かつ、監査が完了しているもの）の導入も検討する。アクセス制御行使メカニズムの一環として、情報システムに格納される情報を暗号化する場合は、FIPS 140-2（修正版）に準拠した暗号技術を使用すること。関連セキュリティ管理策：SC-13。

管理強化策：

(1) 情報システムは、特権を要する機能（ハードウェア、ソフトウェア、およびファームウェアに配備されたもの）およびセキュリティ関連情報へのアクセスを、明示的に承認された者に限定する。

管理強化策の補足ガイダンス：明示的に承認された者とは、セキュリティの管理者、システムおよびネットワークの管理者、ならびにこれ以外の特権ユーザなどを指す。特権ユーザとは、システムの制御、監視、または管理機能へのアクセス権を持つ個人のことである。（例：システム管理者、情報システムのセキュリティ担当者、（システムセキュリティの）維持者、システムプログラマなど）

AC-4 情報フロー制御の実施

管理策：情報システムは、適用方針に従って、自システムおよび相互接続されたシステム内の情報の流れを制御する権限を行使する。

補足ガイダンス：情報フロー制御は、特定の情報システム内および相互接続されたシステム間で、情報が往来できる領域を規制する（これは、誰が情報システムにアクセスできるか、という制御とは異なる）。この際、その情報へのアクセスに関しては、考慮しない。アクセス制御というよりは、むしろフロー制御とみなされる制御の一般的な例としては、外部へ出すことが規制されている情報がインターネットに流出しないようにすること、組織内部からの情報にみせかけた外部からの情報の侵入を阻止すること、およびインターネットに対する組織内部のウェブプロキシ以外からのウェブリクエストを通過させないこと、などがある。情報フロー制御の方針や行使メカニズムは、組織が、特定の情報システム内および相互接続されたシステム間の送信元（source）と宛先（destination）（ネットワーク、個人、デバイスなど）間を往来する情報の流れを制御するために使用する。フロー制御は、情報の性質および／または情報の経路に基づいている。フロー制御の具体例としては、プロキシ、ゲートウェイ、暗号化トンネル、ファイアウォール、ルータなどの境界保護デバイスがある。これらのデバイスの中には、ルールセットを使用するものや情報システムの設定を変更しサービスを制限するもの、パケットフィルタリング機能を提供するものなどがある。関連セキュリティ管理策：SC-7。

管理強化策：なし。

AC-5 職務の分離

管理策：情報システムは、（個人またはグループごとに）割り当てられたアクセス認可をもとに、職務の分離を実施する。

補足ガイダンス：組織は、担当者間の責任や職務上の利害対立を避けるために、必要に応じて責任を分割し、職務を分離する。情報システムには、ユーザが、単独で不正活動を行うために必要なすべての権限または情報へのアクセスを取得することを阻止するための、アクセス制御ソフトウェアが備わっている。職務の分離の例には、(i) ミッションにかかわる職務を担当する者（またはロール）と、情報システムのサポートを担当する者（またはロール）を区別する、(ii) 情報システムサポート機能を複数の担当者に振り分ける（たとえば、システム管理、システムプログラミング、品質保証／テスト、構成管理、ネットワークセキュリティなど）、および (iii) アクセス制御機能を管理するセキュリティ担当者は監査機能を管理しない、などである。

管理強化策：なし。

AC-6 特権の最小化

管理策：情報システムは、特定のタスクを実行するユーザ（またはユーザの作業を代行するプロセス）に対して、必要以上の権利／特権を与えたり、アクセスを許可しないようにする。

補足ガイダンス：組織は、リスクアセスメントの結果にもとづき、必要に応じて特権最小化の概念（特定の職務および情報システム（特定のポート、プロトコル、およびサービスを含む）に対する権限を必要以上に与えないこと）を取り入れることによって、組織の業務や資産、および個人に対するリスクを適切に低減する。

管理強化策：なし。

AC-7 ログイン試行の失敗

管理策：情報システムは、ユーザが、［指定：組織が定める期間］ 内に無効なアクセス試行を ［指定：組織が定める回数］分繰り返すことを抑止する。情報システムは、ログイン試行の失敗回数が最大値を超えた場合、自動的に［選択：アカウント／ノード］を［指定：組織が定める期間］間ロックし、次のログインプロンプト表示を［指定：組織が定める遅延アルゴリズム］に従い遅延させる。

補足ガイダンス：情報システムによる自動ロックアウトは、サービス妨害につながる可能性があるため、通常は一時的なものであり、組織があらかじめ設定した時間が経過すると、自動的に解除される。

管理強化策：なし。

AC-8 システムの利用に関する通知

管理策：情報システムは、ユーザに対して、システムへのアクセスを許可する前に、以下のようなシステムの使用に関する留意事項を表示する。(i) ユーザが合衆国政府の情報システムにアクセスしていること、(ii) システムの使用状況が監視、記録、および監査の対象となる場合があること、(iii) システムの不正使用は禁じられており、違反した場合は、刑事および民事上の罰を受けることがあること、および(iv) システムを使用することは、自身のオペレーションが監視され記録されることに同意したものと見なされること。システムの利用に関する通知メッセージには、（関連するプライバシー方針およびセキュリティ方針、またはこれらの要約にもとづき）システムに適したプライバシーおよびセキュリティ関連の通知を表示し、ユーザが明示的なアクション（システムにログオンするなど）を起こすまでの間、画面に表示したままにする。

補足ガイダンス：プライバシーおよびセキュリティの方針は、適用法、大統領令、指令、方針、規則、基準、およびガイダンスに準拠する。システムの利用に関する通知メッセージは、ユーザが情報システムにログインした際に、ワーニングバナー（warning banners）として表示することができる。公的にアクセス可能なシステムでは、(i) システム利用に関する情報をユーザが入手できるようにして、必要な場合は、ユーザにアクセスを許可する前に、適宜表示する。(ii) 監視、記録、および監査に関する照会は、これらのシステムがそのような行為を一般的には禁じているため、公開されることはない。そして、(iii) これらの情報システムを利用する一般ユーザへの通知には、使用許可に関する記述を含める。

管理強化策：なし。

AC-11 セッションのロック

管理策：情報システムは、システムが［指定：組織が定める期間］非稼動状態にある場合、セッションロックし、ユーザが適切な識別および認証手順によってアクセスを再確立するまで、ロック状態を保つ。

補足ガイダンス：ユーザは、セッションロックメカニズムを手動で開始することができる。セッションロックは、情報システムのログアウトに代わるものではない。組織が、ロックを開始するまでのシステムの非稼動期間を定める際には、連邦政府の方針に準拠しなければならない。政府の方針である OMB 通達 06-16 は、リモートアクセスやポータブルアクセスの場合の非稼動期間が、30 分を上回らないことを規定している。

管理強化策：なし。

AC-12 セッションの終了

管理策：情報システムは、システムが［指定：組織が定める期間］非稼動状態にある場合、リモートセッションを自動的に終了する。

補足ガイダンス：リモートセッションは、ユーザ（または、情報システム）が外部のネットワーク（例：インターネットなど）を経由してシステムにアクセスした場合に、開始される。

管理強化策：なし。

AC-13 監視とレビュー ― アクセス制御

管理策：組織は、情報システムのアクセス制御の実施および使用という観点から、ユーザの活動を監視し、レビューする。

補足ガイダンス：組織は、不適切な行動がないかを調べるために、組織の手順に従って監査記録（たとえば、ユーザの活動ログなど）をレビューする。組織は情報システムに関連する異常な活動がないかを調査し、アクセス承認に対する変更を定期的にレビューする。組織は、情報システムに対する重要な役割および責任を有するユーザの活動を、より頻繁にレビューする。監査記録のレビュー範囲は、FIPS199 が定める情報システムの影響レベルに基づくこととする。たとえば、低位影響のシステムの場合、すべてのワークステーションのセキュリティログを頻繁にレビューする必要はなく、むしろ、ウェブプロキシやメールサーバなどの重要なポイントのログのみレビューすればよい場合がある（たとえば、特定の状況により、他の監査記録のレビューの省略が正当化される場合）。コンピュータセキュリティに関するログ管理についてのガイダンスは、NIST Special Publication 800-92 に記載されている。

管理強化策：

(1) 組織は、ユーザ活動のレビューを容易にする自動化メカニズムを採用する。

AC-14 識別または認証なしで許可される活動

管理策：組織は、識別または認証なしに情報システム上で実施できるユーザ活動を特定し、文書化する。

補足ガイダンス：組織は、パブリックウェブサイトや他の公開情報システム（たとえば、連邦情報システムである http://www.firstgov.gov にアクセスする個人など）に対する識別・認証不要の活動を限定する。関連セキュリティ管理策：IA-2。

管理強化策：

(1) 組織は、ユーザが識別および認証なしで実施できる活動を、組織の任務目的達成に必要な範囲内で収めるべきである。

AC-17 リモートアクセス

管理策：組織は、情報システムに対するすべてのリモートアクセス方式を承認、監視、および管理する。

補足ガイダンス：リモートアクセスとは、ユーザが、組織の管理下にはない外部のネットワーク（インターネットなど）を経由して組織の情報システムにアクセスすることをいう。リモートアクセスの方法としては、ダイヤルアップ、ブロードバンドおよび無線などがある。リモートアクセスの制御は、一般のアクセスに対応するために特別に設計されたウェブサーバやシステム以外の情報システムにも、適用することができる。組織は、ダイヤルアップ接続を利用したアクセスの制限（たとえば、要求元別にダイヤルアップアクセスを許可・不許可する）、または、VPN 接続などの利用により、正規の接続の妨害の阻止および不正な接続を阻止するといった処置を講ずること。リモート電子認証についてのガイダンスは、NIST Special Publication 800-63 に記載されている。暗号化されたトークンベースのアクセス制御が採用されている環境で、連邦政府の個人識別情報の検証（PIV）のクレデンシャル（credential）が識別トークンとして使用されている場合には、そのアクセス制御システムは、FIPS201 の要件および NIST Special Publication 800-73 および 800-78 に準拠する。IPsec(インターネットプロトコルセキュリティ)ベースの VPN に関するガイダンスは、NIST Special Publication 800-77 に記載されている。関連セキュリティ管理策：IA-2。

管理強化策：

(1) 組織は、リモートアクセス方式の監視および制御を容易にするために、自動化メカニズムを採用する。

(2) 組織は、リモートアクセスセッションの機密性と完全性を保護するために暗号技術を利用する。

(3) 組織は、すべてのリモートアクセスを、限られた数の、管理されたアクセス制御ポイントを介して制御する。

(4) 組織は、特権機能へのリモートアクセスを、組織の運用上どうしても必要である場合に限り許可する。また、アクセスを許可する根拠を、情報システムのセキュリティ計画の中で文書化する。

AC-18 無線アクセスの制限

管理策：組織は、(i) 無線技術の利用制限、および導入のガイダンスを策定し、(ii) 情報システムへの無線アクセスを承認、監視、および管理する。

補足ガイダンス：無線セキュリティに関するガイダンスは、NIST Special Publication 800-48 および 800-97 に記載されている。また、無線による侵入の検知および阻止に関するガイダンスは、NIST Special Publication 800-94 に記載されている。

管理強化策：

(1) 組織は、情報システムへの不正な無線アクセスからシステムを保護するために、認証および暗号を利用する。

AC-19 携帯機器に対するアクセス制御

管理策：組織は、(i) 組織が管理するポータブルデバイスおよびモバイルデバイスの利用制限および導入のガイダンスを策定し、(ii) これらの機器からの組織のネットワークへのアクセスを、承認、監視、および管理する。

補足ガイダンス：ポータブルデバイスおよびモバイルデバイス（ノートパソコン、携帯端末、携帯電話およびこれ以外のデバイスで、計算や通信機能を備え、ネットワークに接続でき、物理的に異なる場所での定期運用が可能なものなど）は、組織のセキュリティ方針と手順に従う場合に限り、組織の情報システムにアクセスすることが許可される。セキュリティ方針および手順には、デバイスの識別と認証、必須の保護ソフトウェア（悪意のコードの検知ソフトウェア、ファイアウォールなど）の導入、構成管理、悪意のコードをスキャンするデバイス、ウイルス対策ソフトウェアの更新、重要なソフトウェアの更新およびパッチのスキャン、主要オペレーティングシステム（および可能な場合には、システムに導入されている、これ以外のソフトウェア）の完全性確認、不要なハードウェア（無線機能、赤外部など）の無効化などが含まれる。ポータブルデバイスおよびモバイルデバイスに保存されている情報の保護（たとえば、情報の保存時および管理領域外での伝送時に、情報の機密性および完全性を保護するために暗号化メカニズムを使用することなど）については、媒体の保護ファミリで扱っている。関連セキュリティ管理策：MP-4. MP-5。

管理強化策：なし。

AC-20 外部情報システムの利用

管理策：組織は、許可された個人が、以下のようなことを行う際の諸条件を策定する。(1)外部の情報システムから組織の情報システムへアクセスすること、および (2)外部の情報システムを利用して、組織が管理する情報を、処理、格納および／または送受信すること。

補足ガイダンス：外部情報システムとは、組織の認可が及ぶ範囲外にある情報システムまたは情報システムを構成するコンポーネントである。これらのシステムまたはコンポーネントは、通常、組織が定めるセキュリティ管理策の実施を強要したり、組織がじかにセキュリティ管理策の有効性を評価するといったことができないものである。外部の情報システムには、個人が所有する情報システム（コンピュータ、携帯電話または携帯端末など）、商業／公共施設（ホテル、コンベンションセンターまたは空港など）の民間企業が所有する計算／通信機器、および政府が所有するものでもなければ、政府によって運用されるわけでもなく、ま

た、政府の直接的な制御下にあるわけでもないシステムなどが含まれるが、これらに限られるわけではない。

許可された個人とは、組織の担当者、契約者、または組織の情報システムへのアクセスを許可されている個人のことである。本管理策は、一般アクセス向けの情報システムまたは情報（例：連邦政府の情報システムへの公共インターフェースを介して政府の情報をアクセスする個人など）にアクセスするための、外部の情報システムの利用には適用されない。組織は、組織のセキュリティ方針や手順に従って、外部の情報システムを利用するための諸条件を策定する。これらの諸条件には、少なくても以下の事項を含めること。(1)外部の情報システムから組織の情報システムにアクセスすることができるアプリケーションの種類、および(2)外部の情報システムに対して、FIPS199 セキュリティ分類（低位影響、中位影響、高位影響）の、どのレベルまでの情報を処理、格納および送受信可能とするか。

管理強化策：

(1) 組織は、次のような場合を除き、承認された個人であっても、外部の情報システムを用いて組織の情報システムにアクセスしたり、組織が管理する情報の処理、格納または送受信を行うことを禁止する。(i)組織の情報セキュリティ方針およびセキュリティ計画に記載されている管理策が、外部システムによって採用されていることが確認できる場合、または(ii)外部情報システムを管理する組織が、情報システムの接続に関する、または、情報の処理に関する契約にサインし、組織がこれを承認した場合。

ファミリ: 意識向上およびトレーニング **クラス:** 運用

AT-1 セキュリティの意識向上およびトレーニングの方針と手順

管理策：組織は、以下のものを策定および周知徹底し、定期的にレビュー／更新する。(i) 正式に文書化された、セキュリティの意識向上およびトレーニングに関する方針。これらの方針では、目的、適用範囲、役割、責任、経営陣のコミットメント、組織間の調整、およびコンプライアンスを取り扱う。(ii) 正式に文書化された、セキュリティの意識向上およびトレーニング方針の導入に関する手順。この手順は、セキュリティの意識向上およびトレーニングの方針の導入、ならびに関連する管理策の導入を容易にするために使用される。

補足ガイダンス：セキュリティの意識向上およびトレーニングの方針と手順は、適用法、大統領令、指令、方針、規制、基準、およびガイダンスに準拠する。セキュリティ意識の向上およびトレーニングの方針は、組織の一般情報セキュリティ方針の一部とすることができる。セキュリティ意識向上およびトレーニングの手順は、一般的なセキュリティプログラムの一部として作成することもできれば、必要に応じて特定の情報システムに特化した形で作成することもできる。セキュリティの意識向上およびトレーニングに関するガイダンスは、NIST Special Publication 800-16 および 800-50 に記載されている。セキュリティポリシーおよび手順に関するガイダンスは、NIST Special Publication 800-12 に記載されている。

管理強化策：なし。

AT-2 セキュリティの意識向上

管理策：組織は、情報システムへのアクセスを許可する前に、すべてのユーザ（管理者および上級管理者を含む）に対して、基本的なセキュリティ意識向上トレーニングを実施する。このトレーニングは、その後も［指定：組織が定める頻度（少なくとも年1回）］を下回らないように定期的に実施され、また、システムに変更があった場合にも実施されるようにしなければならない。

補足ガイダンス：組織は、組織の要求事項および（アクセスを認可した）情報システムの要求事項基づき、セキュリティの意識向上トレーニングのコンテンツを決定する。組織のセキュリティの意識向上活動は、連邦規制基準（C.F.R. = Code of Federal Regulations） パート 5、C 項（5 C.F.R. 930. 301）および NIST Special Publication 800-50 に記載の要件に準拠する。

管理強化策：なし。

AT-3 セキュリティトレーニング

管理策：組織は、情報システムの開発ライフサイクルにおいて、システムセキュリティに関する重要な役割および責任を担う者を特定し、それらの役割および責任を文書化する。また、情報セキュリティに関する適切なトレーニングを、次のようなタイミングで実施する。(i) 彼らに対してシステムへのアクセスを認可する前、または彼らが任命された職務を実行する前、(ii) システムの変更によりトレーニングが必要となった場合、および(iii) ［指定：組織が定める頻度］を下回らない頻度で。

補足ガイダンス：組織は、組織の要求事項および（アクセスを認可した）情報システムの要求事項基づき、セキュリティの意識向上トレーニングのコンテンツを決定する。さらに組織は、システムマネージャ、システムおよびネットワークの管理者、ならびにシステムレベルのソフトウェアを利用する要員が、与えられた職務を遂行する上で必要な技術を習得できるようにするために、適切な技術トレーニングを提供する。組織のセキュリティの意識向上活動は、連邦規制基準（C.F.R. = Code of Federal Regulations） パート 5、C 項（5 C.F.R.930.301） および NIST Special Publication 800-50 に記載の要件に準拠する。

管理強化策：なし。

AT-4 セキュリティトレーニングの記録

管理策：組織は、情報システムのセキュリティトレーニングに関する活動（基本的なセキュリティ意識向上トレーニングおよび特定の情報システムセキュリティトレーニングを含む）を文書化し、監視する。

補足ガイダンス：なし。

管理強化策：なし。

ファミリ: 監査および責任追跡性 **クラス:** 技術

AU-1 監査および責任追跡性の方針と手順

管理策：組織は、以下のものを策定および周知徹底し、定期的にレビュー／更新する。(i) 正式に文書化された、監査および責任追跡性の方針。これらの方針では、目的、適用範囲、役割、責任、経営陣のコミットメント、組織間の調整、およびコンプライアンスを取り扱う。(ii) 正式に文書化された、監査および責任追跡性の方針の導入に関する手順。この手順は、監査および責任追跡性の方針の導入、ならびに関連する管理策の導入を容易にするために使用される。

補足ガイダンス：監査および責任追跡性の方針と手順は、適用法、大統領令、指令、方針、規制、基準、およびガイダンスに準拠する。監査および責任追跡性の方針は、組織の一般的な情報セキュリティ方針の一部とすることができる。監査および責任追跡性の手順は、一般的なセキュリティプログラムの一部として作成することもできれば、必要に応じて特定の情報システムに特化した形で作成することもできる。セキュリティ方針および手順のガイダンスは、NIST Special Publication 800-12 に記載されている。

管理強化策：なし。

AU-2 監査対象のイベント

管理策：情報システムは、次のような事象に関して、監査記録を作成する ― [指定：組織が定める監査可能な事象]

補足ガイダンス：本管理策の目的は、情報システムのセキュリティにとって重要かつ関連性が高いという点から、監査の必要がある重要な事象を特定することである。組織は、情報システムのどのコンポーネントが、監査を実施するかを指定する。監査活動は、情報システムのパフォーマンスにも影響をおよぼすことがある。したがって組織は、リスクアセスメントの結果に基づき、継続的な監査が必要な事象と、状況に応じて監査が必要な事象を決定する。監査記録は、さまざまなレベル（たとえばネットワーク上を流れる情報のパケット単位）で取ることができる。監査記録を取るにあたって、抽出レベルを正しく選択することは、適切な監査を行うためには重要であり、これにより問題の原因の特定が容易になる。さらに、セキュリティの監査機能は、ネットワークの健康状態監視機能と組み合わせて使用することができ、どの情報をどちらの機能によって記録するかを決めることによって、相互支援が強化される。http://csrc.nist.gov/pcig/cig.html のチェックリストおよび設定ガイドでは、監査可能な事象の推奨リストを提供している。組織は、セキュリティインシデントの事後調査を支援するための監査可能事象を定義する。コンピュータセキュリティに関するログ管理については、NIST Special Publicatoin 800-92 に記載されている。

管理強化策：

(3) 組織は、組織が定義した監査事象のリストを、定期的に見直し、更新する。

AU-3 監査記録の内容

管理策：情報システムは、発生したイベント、イベントの原因、イベントの結果を明らかにできるだけの、十分な情報を含む監査記録を作成する。

補足ガイダンス：たいていの場合監査記録の内容には、以下のものが含まれる。(i) イベントの発生日時、(ii) イベントが発生した情報システムのコンポーネント（ソフトウェアコンポーネント、ハードウェアコンポーネントなど）、(iii) イベントの種類、(iv) ユーザ／サブジェクトの識別情報、および (v) イベントの結果（成功または失敗）。コンピュータセキュリティに関するログ管理については、NIST Special Publication 800-92 に記載されている。

管理強化策：

(1) 情報システムは、種別、場所、またはサブジェクトごとに特定される監査イベントの記録のなかに、より詳細な追加情報を含める機能を有する。

AU-4 監査記録の保存容量

管理策：組織は、監査記録の保存容量を十分に確保し、容量の超過の可能性が少なくなるように監査活動を調整する。

補足ガイダンス：組織は実施すべき監査およびオンラインでの監査処理要件を考慮して、監査記録の保存容量を十分に確保する。関連セキュリティ管理策：AU-2、AU-5、AU-6、AU-7、SI-4。

管理強化策：なし。

AU-5 監査処理の不具合に対する対応

管理策：監査の処理中に不具合が生じた場合、情報システムは、組織の適切な責任者に対して警告を促し、次のような追加措置を取る。[指定：組織が定める措置（情報システムを停止する、最も古い監査記録を上書きする、監査記録の作成を停止するなど）]

補足ガイダンス：監査の処理における不具合には、ソフトウェア／ハードウェアのエラー、イベントを検知するメカニズムの不具合、および監査記録の保存容量が満杯になった（または超過した）場合などが考えられる。関連セキュリティ管理策：AU-4。

管理強化策：なし。

AU-6 監査記録の監視、分析および報告

管理策：組織は、情報システムの監査記録を定期的にレビュー／分析し、不適切または異常な活動の兆候がないかをチェックする。また、疑わしい活動や違反行為について調査し、その結果を適切な責任者に報告するとともに、必要な措置を講じる。

補足ガイダンス：組織は、法執行機関や諜報機関からの通知、またはこれ以外の信頼できる筋からの情報に基づき、組織の業務や資産、または個人に対するリスクが上昇する兆しが見える場合には、随時、情報システムの監査記録の監視および分析活動を強化する。

管理強化策：

(2) 組織は、セキュリティに影響を与える次のような不適切または異常な活動に関して、セキュリティ要員に警告を発するための、自動化メカニズムを採用する。[指定：組織が、警告を発するべきであると定める不適切または異常な活動のリスト]

AU-7 監査量の低減と報告書の作成

管理策：情報システムは、監査量の低減および監査報告の作成機能を提供する。

補足ガイダンス：監査量低減ツール、監査レビューツール、および監査報告ツールを利用することによって、セキュリティインシデントが発生した場合の事後調査を、元の監査記録に修正を加えることなく行うことができる。

管理強化策：

(1) 情報システムは、選択可能なイベント基準をもとに決定された監査対象イベントの、監査記録を自動生成する機能を提供する。

AU-8 タイムスタンプ

管理策：情報システムは、監査記録の作成にタイムスタンプを利用する。

補足ガイダンス：監査記録のタイムスタンプ（日時を含め）は、システムの内部クロックを使用して生成される。

管理強化策：

(1) 組織は、[指定：組織が定める頻度]間隔で、組織内の情報システムの内部クロックの時刻を合わせる。

AU-9 監査情報の保護

管理策：情報システムは、監査情報および監査ツールを、不正なアクセス、改ざん、および削除から保護する。

補足ガイダンス：監査情報には、対象情報システムの活動を首尾よく監査するために必要な、すべての情報（監査記録、監査の設定および監査報告など）が含まれる。

管理強化策：なし。

AU-11 監査記録の保持

管理策：組織は、セキュリティインシデントの事後調査を支援し、規制および組織の情報保持要件を満たすために、［指定：組織が定める期間］の間、監査記録を保持する。

補足ガイダンス：組織は、監査記録が、行政上、法律上、監査上またはそれ以外の運用目的に必要でないと判断されるまで、保持する。監査記録の保持が必要である理由としては、情報公開法（FOIA: Freedom of Information Act）が規定する監査記録の保存や利用可能性についての要求を満たすため、記録の召喚に備えるため、または法律に従うため、などがあげられる。この種の活動に関連する監査記録の標準分類および標準対応プロセスは、現在作成され普及されつつある。コンピュータセキュリティインシデントへの対応および監査記録の保持に関するガイダンスは、NIST Special Publication 800-61 に記載されている。

管理強化策：なし。

ファミリ: 承認、運用認可、セキュリティ評価 **クラス:** 管理

CA-1 承認、運用認可、セキュリティ評価の方針と手順

管理策：組織は、以下のものを策定および周知徹底し、定期的にレビュー／更新する。(i) 正式に文書化された、セキュリティの評価、承認および認可に関する方針。これらの方針では、目的、適用範囲、役割、責任、経営陣のコミットメント、組織間の調整、およびコンプライアンスを取り扱う。(ii) 正式に文書化された、セキュリティの評価、承認および認可に関する方針の導入に関する手順。この手順は、セキュリティの評価、承認および認可に関する方針の導入、ならびに関連する管理策の導入を容易にするために使用される。

補足ガイダンス：セキュリティ評価、承認および運用認可の方針と手順は、適用法、大統領令、指令、方針、規制、基準、およびガイダンスに準拠する。セキュリティ評価、承認および運用認可の方針は、組織の一般的な情報セキュリティ方針の一部とすることができる。セキュリティ評価、承認および認可の手順は、一般的なセキュリティプログラムの一部として作成することもできれば、必要に応じて特定の情報システムに特化した形で作成することもできる。組織は、一貫したセキュリティ再認可を受けるために、情報システムにとって重大な変更とはどのような変更であるかを定義する。セキュリティ管理策の評価に関するガイダンスは、NIST SP 800-53A に記載されている。セキュリティ承認および認可に関するガイダンスは、NIST SP 800-37 に記載されている。セキュリティ方針および手順のガイダンスは、NIST SP 800-12 に記載されている。

管理強化策：なし。

CA-2 セキュリティ評価

管理策：組織は、情報システムのセキュリティ管理策が、どの程度正しく導入され、どの程度意図したとおりに運用され、システムのセキュリティ要求事項に対する適合性の観点から望まれる結果をどの程度産出しているかを判断するために、管理策の評価を行う。この評価は、[指定：組織が定める頻度（少なくとも年1回）]を下回らないように実施する。

補足ガイダンス：この管理策は、主要な情報システムのリストに含まれる個々の情報システムの、管理、運用および技術管理策を、リスクアセスメントの結果によって決まる頻度（※年 1 回を下回ってはいけない）で評価するという、FISMA 要件を満たすためのものである。最低でも 1 年に一度実施されるこの評価は、組織が、すでにセキュリティ承認および運用認可の段階に入っているセキュリティ評価に対して、追加の評価を行うものであると解釈すべきものではない。組織は、FISMA が求める年次的なセキュリティ評価を実施するために、以下に示す（セキュリティ管理策の）評価結果から、適切なものを選んで利用することができるが、これらに限定されるわけではない。(i) 情報システムの運用認可および再運用認可プロセスの一環として実施されるセキュリティ承認（CA-4 参照）、(ii) 継続的な監視活動（CA-7 参照）、または(iii) 進行中のシステム開発ライフサイクルプロセスの一環として行われる情報システムのテストと評価（ただし、テストと評価の結果は、現時点のものとし、セキュリティ管理策の有効性の評価に寄与すること）。既存のセキュリティ評価の結果は、それらが有効である限り再利用され、必要に応じて補足的な評価が追加される。評価結果の再利用は、包括的で費用対効果の高い、統合されたセキュリティ対策の構築には不可欠である。このようなセキュリティ対策によって、情報システムのセキュリティの実情の把握に必要な、証拠の作成が可能になる。

OMB は、組織の情報システムに採用されているすべてのセキュリティ管理策を対象にした、年次的な評価を求めてはいない。OMB の方針に従って、組織は、以下のものをベースにして、セキュリティ管理策のサブセット（それぞれの部分ごと）を評価する。(i) FIPS199 による情報システムのセキュリティ分類 (ii) 情報システムを保護するために組織が選択、採用した、特定のセキュリティ管理策、および(iii) 情報システムのセキュリティ管理策が有効であることを裏付ける保証（または信頼）のレベル。組織は、3 年おきに実施される運用認可プロセスにおいて、システムのすべてのセキュリティ管理策を評価すべきである。組織は、セキュリティ承認によって得られた今年度の評価結果を、FISMA の年次的なセキュリティ評価要件（CA-4 参照）に適合させるために用いることができる。既存の評価結果を含めた評価に関するガイダンスは、NIST Special Publication 800-53A に記載されている。関連セキュリティ管理策：CA-4、CA-6、CA-7、SA-11。

管理強化策：なし。

CA-3 情報システムの接続

管理策：組織は、システム接続に関する契約を交わすことによって、ユーザが組織の情報システムから組織の運用認可が及ぶ範囲外のシステムへ接続することを認可すると同時に、ユーザの活動を監視／制御する。

補足ガイダンス：FIPS 199 セキュリティ分類は個々の情報システムに適用されるものである。したがって、システムを、異なるセキュリティ要件とセキュリティ管理策を有する組織内の（または外部の）システムに接続する場合は、リスクを慎重に考慮するべきである。これには、同一ネットワークを共有している情報システムも含まれる。情報システムの接続に関するガイダンスは、NIST SP 800-47 に記載されている。関連セキュリティ管理策：SC-7、SA-9。

管理強化策：なし。

CA-4 セキュリティ承認

管理策：組織は、情報システムのセキュリティ管理策が、どの程度正しく導入され、どの程度意図したとおりに運用され、システムのセキュリティ要求事項に対する適合性の観点から望まれる結果をどの程度産出しているかを判断するために、管理策の評価を行う。この評価は、［指定：組織が定める頻度（少なくとも年1回）］を下回らないように実施する。

補足ガイダンス：セキュリティ承認は、OMB Circular(通達) A-130 付録 III に記載の情報システムの運用認可要件を満たすことを支援するために、組織によって実施される。セキュリティ承認は、セキュリティ運用認可（すなわち許可）にかかわるすべての判断において重要な要素であり、システム開発ライフサイクル（SDLC: System Development Life Cycle）に組み入れられ、ライフサイクルが終了するまで有効となる。組織は、最初のセキュリティ運用認可期間に、情報システムにおけるすべてのセキュリティ管理策を評価する。その後組織は、OMB の方針に従って、セキュリティ管理策のサブセットに対する年次的な評価を、継続的な監視期間内に実施する（CA-7 参照）。組織は、セキュリティ承認によって得られた今年度の評価結果を、FISMA の年次的なセキュリティ評価要件（CA-4 参照）に適合させるために用いることができる。セキュリティ管理策の評価に関するガイダンスは、NIST SP 800-53A に記載されている。セキュリティ承認および運用認可に関するガイド、NIST SP 800-37 に記載されている。関連セキュリティ管理策：CA-2、CA-6、SA-11。

管理強化策：：

(2) 組織は、情報システムのセキュリティ管理策を評価する独立の承認エージェントまたは承認チームを採用する。

管理強化策の補足ガイダンス：独立した承認エージェントまたは承認チームとは、組織の情報システムを公平に評価することができる、個人、またはグループのことである。「公平」とは、評価者が、情報システムの開発、運用および／または管理の指揮系統内に存在する（または存在すると思われる）利害の衝突、あるいはセキュリティ管理策が有効であるか否かを判断する人たちの間に存在する（または存在すると思われる）利害の衝突とは無縁の者であることを意味する。独立したセキュリティ承認サービスは、組織内の他の部署によって、または組織外部の官民セクタ組織との契約によって調達することができる。契約による承認サービスは、情報システムのオーナーが契約プロセスに直接関与していないこと、または情報システムのセキュリティ管理策を評価する独立の承認エージェントまたは承認チームの独立性が、不当な影響を受けてないことが確認できる場合に、独立しているとみなされる。運用認可権限者は、情報システムの重要性や機密性、および組織の業務や資産、または個人に対する最終的なリスクに基づき、承認者に求められる独立性のレベルを決定する。運用認可権限者は、設定した独立性のレベルが、生成される評価結果が妥当であること、また、信頼性のあるリスクベースの判断に利用できることを保証するレベルであるかどうかを判断する。特別な状況にある場合（たとえば、情報システムを所有する組織の規模が小さい場合、またはシステムの構成により、セキュリティ管理策が、システムのオーナーまたは運用認可権限者の指揮のもとで働く開発担当者、運用担当者および／または管理担当者によって評価されることが求められる場合など）、専門家による独立したチームが、承認を行うこともできる。この場合、それらのチームが、評価結果を慎重にレビュー、分析し、評価結果の完全性、一貫性、および正確さを立証する。運用認可権限者は、監査官室（the Office of the Inspector General）、政府機関の上級情報セキュリティ責任者および最高情報責任者と話しあい、評価者の独立性に関するすべての事項を十分に議論すべきである。

CA-5 行動計画とマイルストーン

管理策：組織は、情報システムの行動計画とマイルストーンを作成し、［指定：組織が定める頻度］間隔で更新する。この行動計画とマイルストーンは、セキュリティ管理策の評価中に発覚した欠陥を是正するための活動、または、システムにおける既知の脆弱性を低減または排除するための活動を文書化したものである。

補足ガイダンス：行動計画とマイルストーンは、運用認可権限者のために作成されるセキュリティ運用認可パッケージに含まれる重要な文書であり、OMB が定める連邦政府への報告書要件の対象となるものである。行動計画とマイルストーンの更新は、セキュリティ管理策の評価結果、セキュリティの影響の分析結果、および継続的な監視活動で検出された事柄に基づき、必要であると判断される場合に行われる。OMB による FISMA 報告書ガイダンスには、組織の行動計画とマイルストーンに関する指示項目が含まれている。情報システムのセキュリティ承認および運用認可に関するガイダンスは、NIST Special Publication 800-37 に記載されている。リスクの低減に関するガイダンスは、NIST Special Publication 800-30 に記載されている。

管理強化策：なし。

CA-6 セキュリティの運用認可

管理策：組織は、情報処理を行うシステムに対して、システムが運用される前に運用を認可（許可）し、［指定：組織が定める頻度（最低でも 3 年に一度）］の間隔で認可を更新する。また、システムに重大な変更があった場合も、認可を更新する。組織の上級責任者が、署名しセキュリティ認可を行う。

補足ガイダンス：OMB Circular A-130 付録 III に、連邦情報システムのセキュリティ運用認可の方針が規定されている。組織は、情報システムで採用されているセキュリティ管理策を、セキュリティ運用認可の裏付けとして認可前に評価する。セキュリティ運用認可の裏付けとして実施されるセキュリティ評価をセキュリティ承認と称する。情報システムのセキュリティ認可は、静的なプロセスではない。包括的かつ継続的な監視プロセス（承認および運用認可プロセスの第 4、および最終段階）を適用することによって、運用認可パッケージ（システムセキュリティ計画、セキュリティの評価報告書、および行動計画とマイルストーンなど）に含まれている重大な情報を最新に保つことができると同時に、運用認可責任者および情報システムのオーナーに対して、情報システムの最新のセキュリティ状態を提供することができる。運用認可責任者は、3 年に一度の再認可プロセスの事務的な処理を軽減するために、継続的な監視プロセスの結果を最大限に活用して、再認可の判断を行う。情報システムのセキュリティ承認および運用認可に関するガイダンスは、NIST SP 800-37 に記載されている。関連セキュリティ管理策：CA-2、CA-4、CA-7。

管理強化策：なし。

CA-7 継続的な監視

管理策：組織は、情報システムのセキュリティ管理策を継続的に監視する。

補足ガイダンス：継続的な監視活動には、情報システムコンポーネントの構成管理と制御、システムの変更によるセキュリティの影響分析、セキュリティ管理策の継続的評価およびセキュリティ状態の報告などがある。組織は、セキュリティ運用認可の期間中に、情報システムのすべてのセキュリティ管理策を評価する。初期のセキュリティ運用認可に続き、組織は、OMB の方針に従って、セキュリティの継続的な監視期間中に管理策のサブセットの年次的な評価を実施する。セキュリティ管理策の適切なサブセットの選択は、(i) FIPS199 による情報システムのセキュリティ分類、(ii) 情報システムを保護するために組織が選択、採用した、特定のセキュリティ管理策、および(iii) 情報システムのセキュリティ管理策が有効であることを裏付ける保証（または信頼）のレベルに基づくこととする。また、組織は、サブセットの選択基準を策定し、情報システムに適用されている管理策のサブセットの中から、評価対象となるものを選択する。さらに組織は、上で述べたような要件が適切に満たされるように、管理策の監視計画も策定する。情報システムの保護に関して不安定な要素を抱えるセキュリティ管理策、または重要であるとみなされる管理策は、少なくても年に一度の評価を実施する。その他の管理策については、3 年に一度の運用認可サイクルの中で、少なくても一度、評価を実施する。組織は、セキュリティ承認によって得られた今年度の評価結果を、FISMA の年次的なセキュリティ評価要件（CA-4 参照）に適合させるために用いることができる。

この管理策は、情報システムに対する設定の変更を監視する活動と密接に関連しており、また、互いに支援するものである。有効、かつ継続的な監視プログラムは、セキュリティ運用認可パッケージの 3 つの重要な文書（情報システムのセキュリティ計画、セキュリティの評価報告書、および行動計画とマイルストーン）の継続的な更新を支援する。継続的な監視プロセスを厳密に首尾よく実施することによって、組織は、情報システムの再認可に必要な作業量を大幅に削減することができる。継続的な監視プロセスに関するガイダンスは、NIST SP 800-37 に記載されている。セキュリティ管理策の評価に関するガイダンスは、NIST SP 800-53A に記載されている。関連セキュリティ管理策：CA-2、CA-4、CA-5、CA-6、CM-4。

管理強化策：なし。

ファミリ: 構成管理 **クラス:** 運用

CM-1 構成管理の方針と手順

管理策：組織は、以下のものを策定および周知徹底し、定期的にレビュー／更新する。(i) 正式に文書化された、構成管理の方針。これらの方針では、目的、適用範囲、役割、責任、経営陣のコミットメント、組織間の調整、およびコンプライアンスを取り扱う。(ii) 正式に文書化された、構成管理に関する手順。この手順は、構成管理の方針の導入および関連する管理策の導入を容易にするために使用される。

補足ガイダンス：構成管理の方針と手順は、適用法、大統領令、指令、方針、規制、基準、およびガイダンスに準拠する。構成管理の方針は、組織の一般的な情報セキュリティ方針の一部とすることができる。構成管理の手順は、一般的なセキュリティプログラムの一部として作成することもできれば、必要に応じて特定の情報システムに特化した形で作成することもできる。セキュリティ方針および手順のガイダンスは、NIST SP 800-12 に記載されている。

管理強化策：なし。

CM-2 ベースライン構成

管理策：組織は、情報システムの最新のベースライン構成を作成し、文書化して維持する。

補足ガイダンス： この管理策は、情報システムのベースライン構成を策定するものである。ベースライン構成は、特定のコンポーネントの構成に関する情報（ワークステーションまたはノートブックコンピュータの標準ソフトウェアロード（最新のパッチ情報も含む）に関する情報）、および、そのコンポーネントがシステムアーキテクチャ内のどの位置（論理的）に設置されているかなどの情報を提供する。また、ベースライン構成は、情報システムを構築する際に必要な仕様を、明確に定義・文書化し、組織に提供する。さらに、必要な場合には、ミッションのニーズや目的を支援するために、それらのニーズや目的への逸脱箇所についても文書化する。情報システムのベースライン構成は、連邦政府機関のエンタープライズアーキテクチャに準拠する。関連セキュリティ管理策：CM-6、CM-8。

管理強化策：

(1) 組織は、コンポーネントの導入に不可欠なプロセスとして、情報システムのベースライン構成を更新する。

CM-3 構成変更管理

管理策：組織は、情報システムに対する変更を承認、文書化し管理する。

補足ガイダンス：組織は、組織が承認するプロセス（公認の構成管理委員会（CCB）など）を用いて、情報システムの構成変更を管理する。構成変更管理には、アップグレードや修正を含む、情報システムへ系統的な変更案、変更に対する正当な理由、変更の導入、テスト／評価、レビューおよび破棄が含まれる。構成変更管理には、情報技術製品（オペレーションシステム、ファイアウォール、ルータなど）の構成設定の変更も含まれる。組織は、緊急な変更も、構成変更管理プロセスに含める。これには、欠陥を修正することにより生じる変更も含まれる。情報システムへの変更が承認されるための条件には、変更に関するセキュリティ分析結果が良好であることが含まれる。組織は、情報システムに対する構成の変更に関する活動を監査する。関連セキュリティ管理策：CM-4、CM-6、SI-2。

管理強化策：なし。

CM-4 構成変更の監視

管理策：組織は、情報システムへの変更を監視すると同時に、変更によるセキュリティへの影響を分析する。

補足ガイダンス：組織は、情報システムへの変更が実施される前に、変更承認プロセスの一環として、情報システムへの変更により生じるセキュリティへの影響を分析する。情報システムが変更（アップグレードおよび修正を含む）された場合、組織は、セキュリティ機能をチェックして、従来どおり適切に機能しているかどうかを確認する。組織は、情報システムへの構成変更に関連する活動を監査する。構成の変更を監視し、セキュリティの影響分析を実施することは、情報システムのセキュリティ管理策を継続的に評価するうえで重要な要素となる。関連セキュリティ管理策：CA-7。

管理強化策：なし。

CM-5 変更のためのアクセス制限

管理策：組織は、(i)それぞれのアクセス権限を承認し、情報システムを変更するための物理的かつ論理的アクセスを制限する、(ii)これらのすべての変更を反映する記録を作成、維持およびレビューする。

補足ガイダンス：情報システムのハードウェア、ソフトウェア、および／またはファームウェアコンポーネントに対する意図的な（または意図しない）変更は、システム全体のセキュリティに重大な影響をもたらすことがある。したがって、情報システムへの変更（アップグレードおよび修正を含む）を目的としてシステムコンポーネントにアクセスすることができるのは、正式な権限を持つ担当者のみとする。

管理強化策：なし。

CM-6 構成設定

管理策：組織は、以下のことを実施する。(i) 情報システム内で利用されている情報技術製品に対して、必須の設定を設ける、(ii) 情報技術製品のセキュリティ設定を、システム運用要件に準拠した最も限定的なモードに設定する、(iii) その構成設定を文書化する、(iv) 情報システムのすべてのコンポーネントに対する構成設定を実施する。

補足ガイダンス：構成設定とは、情報技術製品の構成可能なパラメータを設定することをいう。組織は、組織の方針や手順に従って、構成設定への変更を監視および管理する。OMB における FISMA の報告書通例では、連邦情報システムの構成要件のガイダンスを提供している。情報技術製品の構成設定の作成および利用に関するガイダンスは、NIST SP 800-70 に記載されている。関連セキュリティ管理策：CM-2、CM-3、SI-4。

管理強化策：なし。

CM-7 機能の最小化

管理策：組織は、以下の機能、ポート、プロトコル、および／またはサービスの使用を禁止および／または制限することで、必要なシステム機能のみを提供する。[指定：組織が禁止および／または制限する機能、ポート、プロトコル、および／またはサービスのリスト]

補足ガイダンス：情報システムは、さまざまな機能とサービスを提供することができる。デフォルトで提供される機能やサービスの中には、組織の主要業務（主要なミッション、主要な機能など）をサポートしないものもある。また、情報システムの単一のコンポーネントから複数のサービスを提供することが、便利であることもあるが、他のコンポーネントによって提供されるべきサービスを制限するリスクも増加する。したがって組織は、可能な場合には、デバイス（たとえば、メールサーバ、またはウェブサーバ、あるいは、どちらにも属さないサーバ）一つにつき一つのコンポーネント機能を割り当てるようにする。情報システムまたはシステムコンポーネントが提供する機能やサービスの中で、削除の対象となる機能やサービスを決定する際には、慎重に検討すべきである（たとえば、ボイスオーバーインターネットプロトコル（VoIP）、インスタントメッセージ、ファイル転送プロトコル（FTP）、ハイパーテキスト転送プロトコル（HTTP）、ファイル共有）。

管理強化策：なし。

CM-8 情報システムコンポーネントのインベントリ

管理策：組織は、情報システムの現在のコンポーネントのインベントリ（所有権情報を含む）を作成し、文書化して、維持する。

補足ガイダンス：組織は、マネジメントコントロール（トラッキングおよび報告など）インベントリに含まれるシステムコンポーネントを、どの程度詳細に記述するかについて決定する。システムコンポーネントインベントリには、組織が、適切な管財責任を果たすために必要であると判断した、あらゆる情報（たとえば、製造業者、モデル番号、シリアル番号、ソフトウェアのライセンスに関する情報、システム／コンポーネントのオーナーなど）が含まれる。コンポーネントインベントリは、情報システムの運用認可が及ぶ範囲内に抑える。
関連セキュリティ管理策：CM-2、CM-6。

管理強化策：

(1) 組織は、コンポーネントの導入に不可欠なプロセスとして、情報システムのコンポーネントのインベントリを更新する。

ファミリ: 緊急時対応計画 **クラス:** 運用

CP-1 緊急時対応計画の方針と手順

管理策：組織は、以下のものを策定および周知徹底し、定期的にレビュー／更新する。(i) 正式に文書化された、緊急時対応計画の方針。これらの方針では、目的、適用範囲、役割、責任、経営陣のコミットメント、組織間の調整、およびコンプライアンスを取り扱う。(ii)正式に文書化された、緊急時対応計画の方針の導入に関する手順。この手順は、緊急時対応計画に関する方針の導入、ならびに関連する管理策の導入を容易にするために使用される。

補足ガイダンス：緊急時対応計画の方針と手順は、適用法、大統領令、指令、方針、規制、基準、およびガイダンスに準拠する。緊急時対応計画の方針は、組織の一般的な情報セキュリティ方針の一部とすることができる。緊急時対応計画の手順は、一般的なセキュリティプログラムの一部として作成することもできれば、必要に応じて特定の情報システムに特化した形で作成することもできる。緊急時対応計画の作成に関するガイダンスは、NIST SP 800-34 に記載されている。セキュリティ方針および手順のガイダンスは、NIST SP 800-12 に記載されている。

管理強化策：なし。

CP-2 緊急時対応計画

管理策：組織は、情報システムの緊急時対応計画を作成し導入する。緊急時対応計画には、緊急時の役割、責任、担当者名とその連絡先情報、およびシステムの混乱や障害が発生した場合の復旧関連の活動などを取り扱う。組織内で指定された責任者は、緊急時対応計画をレビュー、承認し、計画のコピーを主な緊急時対応要員に配付する。

補足ガイダンス：なし。

管理強化策：

(1) 組織は、関連する計画に責任を負う組織内の部署と連携して、緊急時対応計画を作成する。

管理強化策の補足ガイダンス：関連する計画の例としては、事業継続計画、災害復旧計画、運用継続計画、事業復興計画、インシデント対応計画、および緊急時行動計画などがあげられる。

CP-3 緊急時対応トレーニング

管理策：組織は、情報システムに関する緊急時の役割と責任について要員をトレーニングし、[指定：組織が定める頻度（少なくとも年 1 回）]間隔で再トレーニングを行う。

補足ガイダンス：なし。

管理強化策：なし。

CP-4 緊急時対応計画のテストと実習

管理策：組織は、(i)[指定：組織が定めるテストおよび／または実習]を通じて、情報システムの緊急時対応計画を、[指定：組織が定める頻度（少なくとも年 1 回）]間隔でテストおよび／または実習し、計画の有効性と組織の計画実施準備状況を判断する、また、(ii)緊急時対応計画のテスト／実習の結果をレビューし、訂正活動に着手する。

補足ガイダンス：緊急時対応計画の潜在的な弱点を特定するには、さまざまなテスト／実習方法がある（たとえば、緊急時対応計画の全面的なテスト、機能ごとの実習／机上での実習など）。緊急時対応計画のテストおよび／または実習の難易度や厳密さは、FIPS199 が定める情報システムの影響レベルによって変わる。緊急時対応計画のテストおよび／または実習には、緊急時対応計画に従って緊急活動が行われた場合の、組織の業務や資産への影響（ミッション能力の削減など）および個人へ影響の特定が含まれる。情報技術の計画および機能をテスト、トレーニングおよび実習するプログラムに関するガイダンスは、NIST SP 800-84 に記載されている。

管理強化策：

(1) 組織は、関連する計画に責任を負う組織内の部署と連携して、緊急時対応計画のテストおよび／または実習を行う。

管理強化策の補足ガイダンス：関連する計画の例としては、事業継続計画、災害復旧計画、運用継続計画、事業復興計画、インシデント対応計画、および緊急時行動計画などがあげられる。

CP-5 緊急時対応計画の更新

管理策：組織は、情報システムの緊急時対応計画を［指定：組織が定める頻度（少なくとも年１回）］間隔でレビューし、必要な場合には、修正する（たとえば、システム／組織の変更に伴う修正、または計画の導入、実施、テスト時に起きた問題に対処するための修正など）。

補足ガイダンス：組織的な変更には、情報システムがサポートするミッション、機能、またはビジネスプロセスの変更が含まれる。組織は、緊急時対応計画（事業継続計画、災害復旧計画、運用継続計画、事業復興計画、インシデント対応計画、または緊急時行動計画など）に責任を持つ組織内の部署に対して、組織的な変更を行う旨を通知する。

管理強化策：なし。

CP-6 （情報システムの）代替保管拠点

管理策：組織は、代替保管拠点を特定し、情報システムのバックアップ情報を保存するのに必要な取り決めに着手する。

補足ガイダンス：情報システムのバックアップを取る頻度およびバックアップ情報を代替保管拠点へ転送する頻度（指定されている場合）は、組織の情報システムの目標復旧時間および目標復旧ポイントによって決まる。

管理強化策：

(1) 組織は、主要保存拠点から地理的に離れた場所を代替保管拠点とし、同一災害の影響を受けないようにする。

(3) 組織は、非常時（区域全体におよぶ混乱や災害が発生した場合など）に発生すると思われる、代替保管拠点へのアクセスにかかわる問題を特定し、それらの問題を緩和するための活動を明確にする。

CP-7 （情報システムの）代替処理拠点

管理策：組織は、代替処理拠点を指定し、主要処理拠点が機能しない場合に、組織の重要なミッション／ビジネス機能を支える情報システムの運用を、代替処理拠点にて［指定：組織が定める期間］内に再開させるための、取り決めに着手する。

補足ガイダンス：業務を再開させるために必要な機器は、代替拠点で入手できる、または、契約により代替拠点へ配送されるようにする。情報システムの再開に要する時間枠は、組織が定める目標復旧時間に準拠する。

管理強化策：

(1) 組織は、主要保存拠点から地理的に離れた場所を代替保管拠点とし、同一災害の影響を受けないようにする。

(2) 組織は、非常時（区域全体におよぶ混乱や災害が発生した場合など）に発生すると思われる、代替保管拠点へのアクセスにかかわる問題を特定し、それらの問題を緩和するための活動を明確にする。

(3) 組織は、組織の可用性要件に従い、代替処理拠点に関する取り決め（サービス優先度に関する規定を含む）を作成する。

CP-8 電気通信サービス

管理策：組織は、主要な通信サービスの他に、代替の通信サービスを指定し、主要な通信サービスが利用できなくなった場合に、組織の重要なミッション／ビジネス機能を支える情報システムの運用を、代替通信サービスにて［指定：組織が定める期間］内に再開させるための、取り決めに着手する。

補足ガイダンス：主要な通信サービス、および／または代替の通信サービスが一般の通信事業者によって提供される場合、組織は、TSP(Telecommunications Service Priority：国家安全保障上の緊急時対応で使用するすべての通信サービスに対する電気通信サービス優先権)を要求する。TSP プログラムついての詳述は http://tsp.ncs.gov を参照のこと。

管理強化策：

(1) 組織は、組織の可用性要件に従い、主要な通信サービスおよび／代替通信サービスに関する取り決め（サービス優先度に関する規定を含む）を作成する。

(2) 組織は、代替通信サービスと主要通信サービスが、単一障害点を持たないようにする。

CP-9 情報システムのバックアップ

管理策：組織は、情報システムに含まれる、ユーザレベル、およびシステムレベルの情報（システム状態についての情報を含む）を［指定：組織が定める頻度］間隔でバックアップし、バックアップ情報を保管場所（または記憶場所）に格納し、保護する。

補足ガイダンス：情報システムのバックアップを取る頻度およびバックアップ情報を代替保管拠点へ転送する頻度（指定されている場合）は、組織の情報システムの目標復旧時間および目標復旧ポイントによって決まる。バックアップする情報に関しては、情報の完全性および可用性の確保が重要である一方で、情報の種類や FIPS199 の影響レベルによっては、情報の不正開示に特別な注意を払わなければならないこともある。また、リスクアセスメントの結果によっては、バックアップ情報の暗号化が必要となる場合もある。転送中のバックアップ情報の保護に関しては、本管理策の範囲外である。関連セキュリティ管理策：MP-4、MP-5。

管理強化策：

(1) 組織は、記録媒体の信頼性と情報の完全性を確認するために、バックアップ情報のテストを［指定：組織が定める頻度］間隔で行う。

(4) 組織は、システムのバックアップ情報を、不正な変更から保護する。

管理強化策の補足ガイダンス：組織は、情報システムのバックアップの完全性を保護するために、適切なメカニズム（電子署名、暗号学的ハッシュ関数など）を採用する。システムバックアップ情報の機密性の保護は、本管理策の範囲外である。関連セキュリティ管理策：MP-4、MP-5。

CP-10 情報システムの復旧と再構成

管理策：組織は、情報システムの混乱または障害の発生後、システムを元の状態に復旧し再構成するための、メカニズムを使用する。

補足ガイダンス：情報システムを元のセキュアな状態に復旧し、再構成するには、すべてのシステムパラメータ（デフォルトまたは組織が設定したもの）に安全な値を再設定する、セキュリティにとって重要なパッチを再適用する、セキュリティ関連の構成設定を復旧する、システム文書および運用手順を利用可能にする、アプリケーションおよびシステムソフトウェアを安全に再インストールし、安全な設定を行う、安全性の確認が取れている最新のバックアップ情報をロードする、システムの全面的なテストを行う、などが必要となる。

管理強化策：なし。

ファミリ: 識別および認証 **クラス:** 技術

IA-1 識別および認証の方針と手順

管理策：組織は、以下のものを策定および周知徹底し、定期的にレビュー／更新する。(i) 正式に文書化された、識別および認証の方針。これらの方針では、目的、適用範囲、役割、責任、経営陣のコミットメント、組織間の調整、およびコンプライアンスを取り扱う。(ii) 正式に文書化された、識別と認証の方針の導入に関する手順。この手順は、識別と認証の方針の導入、ならびに関連する管理策の導入を容易にするために使用される。

補足ガイダンス：識別および認証の方針と手順は、(i) FIPS 201、SP 800-73、800-76、800-78、および (ii) その他の適用法、大統領令、指令、方針、規制、基準、およびガイダンスに準拠する。識別および認証の方針は、組織の一般的な情報セキュリティ方針の一部とすることができる。識別と認証の手順は、一般的なセキュリティプログラムの一部として作成することもできれば、必要に応じて特定の情報システムに特化した形で作成することもできる。セキュリティ方針および手順のガイダンスは、NIST SP 800-12 に記載されている。遠隔電子認証に関するガイダンスは、NIST SP 800-63 に記載されている。

管理強化策：なし。

IA-2 ユーザ識別および認証

管理策：情報システムは、ユーザ（または、ユーザの作業を代行するプロセス）を一意に識別し、認証する。

補足ガイダンス：ユーザは、すべてのアクセスに関して識別および認証される（ただし、組織がセキュリティ管理策のAC-14に従って、明確に識別し文書化しているアクセスを除く）。ユーザ識別情報の認証には、パスワード、トークン、バイオメトリクスなどが使用され、複数因子による認証の場合は、それらの組み合わせが使用される。認証メカニズムの強度を含む、遠隔の電子認証のガイダンスは、NIST SP 800-63に記載されている。本管理策では、管理策の目的を果たすために、SP 800-63が提供するガイダンスが、情報システムへのローカルおよびリモートアクセスの双方に適用されている。リモートアクセスとは、ユーザが、組織の管理下にはない外部のネットワーク（インターネットなど）を経由して、組織の情報システムにアクセスすることをいう。ローカルアクセスとは、ユーザ（または情報システム）が、組織内で管理するネットワーク（例: ローカルネットワークなど）を経由をして組織の情報システムにアクセスすること、または、ネットワークを介さずにデバイスに直接アクセスすることをいう。より厳密な管理強化策が指定されていない限り、情報システムへのローカルおよびリモートアクセスの双方のアクセス認証は、NIST SP 800-63のレベル1に準拠する。FIPS 201、SP 800-73、800-76、および800-78は、連邦政府の職員および請負業者の識別および認証に使用する、個人識別情報の検証（PIV: Personal Identity Verification）のクレデンシャル（credential）について規定している。さらに組織は、システムレベルでのユーザ識別や認証（システムのログオン時など）に加えて必要な場合には、アプリケーションレベルでのユーザ識別や認証を行い、組織の情報セキュリティを向上させる。

OMBの方針および電子認証／電子政府イニシアチブに従い、連邦政府の情報システムにアクセスする一般ユーザに対して、非公開の情報または個人に関する情報を保護するために認証が行われることもある。OMBの通達04-04に従って実施する電子認証のリスクアセスメントは、IA-2の管理策および管理強化策が提供するアクセス制御が、NIST SP 800-63の要求事項に準拠しているかを判断するために、用いられる。システムの拡張性、実用性およびセキュリティについて考慮する時には、組織の業務や資産および個人を保護する必要性と、一般的なアクセスを通じてシステムを利用する際の利便性とのバランスを同時に考慮しなければならない。関連セキュリティ管理策：AC-14、AC-17。

管理強化策：

(1) 情報システムは、NIST SP 800-63[選択：組織が定めるレベル 3、ハードウェア認証デバイスを用いるレベル 3、またはレベル 4]に準拠する複数因子の認証を、リモートシステムへのアクセス認証に使用する。

IA-3 デバイスの識別および認証

管理策：情報システムは、特定の装置との接続を確立する前に、その装置を識別し認証する。

補足ガイダンス： 情報システムは、ローカルエリアネットワークおよび／またはワイドエリアネットワーク上のデバイスを識別し認証するために、通常、既知の共有情報（MACアドレス、TCP/IPアドレスなど）を使用するか、あるいは、組織の認証ソリューション（IEEE 802.1xと拡張認証プロトコル（EAP）、またはEAP-トランスポート層セキュリティ認証が可能なRadiusサーバ）を使用する。デバイスの認証メカニズムに求められる強度は、FIPS199の情報システムのセキュリティ分類によって決まる。通常、装置の認証には、より高位の影響レベルの情報システムに必要な、より強固な認証が求められる。

管理強化策：なし。

IA-4 識別子（Identifier）の管理

管理策：組織は、以下の方法でユーザ識別子を管理する。(i) 各ユーザを一意に識別する、(ii) 各ユーザの身元を確認する、(iii) 組織の適切な担当者から、ユーザ識別子を発行するための認可を受ける、(iv) 該当する相手にユーザ識別子を発行する、(v)[指定：組織が定める期間]の間アクティブでないユーザ識別子を無効化する、および (vi) ユーザ識別子を記録保存する。

補足ガイダンス：識別子管理は、共有の情報システムアカウント(ゲスト（guest）、匿名（anonymous）など)には適用されない。FIPS 201、SPs 800-73、800-76、および 800-78 は、連邦政府の職員および請負業者の識別および認証に使用する、個人識別情報の検証（PIV: Personal Identity Verification）のクレデンシャル（credential）について規定している。

管理強化策：なし。

IA-5 認証コード(Authenticator)の管理

管理策：組織は、以下の方法で情報システムの認証コードを管理する。(i) 初期認証コードの内容を定義する。(ii) 初期認証コードの配付、認証コードの紛失／漏洩または破損時の対処、および認証コードの取消しに関する管理手順を規定する。(iii) 情報システムの導入時にデフォルトの認証コードを変更する。(iv) 認証コードを定期的に変更／更新する。

補足ガイダンス：情報システムの認証コードには、トークン、公開鍵基盤（PKI）認証、バイオメトリックス、パスワード、キーカードなどがある。ユーザは、個人の認証コードを所持し、他人への貸与や共有を行わず、紛失または漏洩した場合は直ちに報告するなど、合理的な手段によって認証コードを保護する。パスワードに基づく認証を行う情報システムでは、(i) パスワードを保存および送信する際に、不正な開示および改ざんから保護する、(ii) 入力時にパスワードが表示されないようにする、(iii) パスワードの最短／最長の有効存続期間の制限を設ける、および (iv) 規定の世代の間、パスワードの再利用を禁止する、といった措置を講じる。PKI に基づく認証を行う情報システムでは、(i) 上位のシステムによって受け入れられているトラストアンカーへの証明経路を構築することにより証明（書）の有効性を確認する、(ii) 対応するプライベート鍵のユーザー制御を規定する、および (iii) ユーザアカウントに対して認証済みの識別情報を対応づける。OMB の方針および電子認証／電子政府イニシアチブに従い、連邦政府の情報システムにアクセスする一般ユーザに対して、非公開の情報または個人に関する情報を保護するために認証が行われることもある。FIPS 201、SP 800-73、800-76、および 800-78 は、連邦政府の職員および請負業者の識別および認証に使用する、個人識別情報の検証（PIV）のクレデンシャル（credential）について規定している。遠隔電子認証に関するガイダンスは、NIST SP 800-63 に記載されている。

管理強化策：なし。

IA-6 認証コード（Authenticator）のフィードバック

管理策：情報システムは、不正使用を試みるユーザからシステムを保護するために、認証プロセスにある認証情報のフィードバックを遮蔽する。

補足ガイダンス：情報システムからのフィードバックには、不正ユーザが認証メカニズムの侵害を目的に利用できる情報は、含めないようにする。たとえば、ユーザが入力するパスワードをアスタリスクで表示する。

管理強化策：なし。

IA-7 暗号モジュールの認証

管理策：情報システムは、適用法、大統領令、指令、方針、規制、基準、および暗号モジュール認証ガイダンスの要件を満たす認証方式を使用する。

補足ガイダンス：暗号モジュールに対する連邦政府基準の認証は、FIPS 140-2(修正版)である。NIST の暗号モジュール試験および認証制度*（Cryptographic Module Validation Program）（FIPS 140-1、FIPS 140-2、および今後の修正を含む）によって交付される証明書は、明示的に無効になるまでは、その有効性が維持される。また、証明書が有効であれば、モジュールの継続的な利用や購入が可能である。認証暗号の利用についての追加情報は、http://csrc.nist.gov/cryptoval から入手することができる

管理強化策：なし。

ファミリ: インシデント対応 **クラス:** 運用

IR-1 インシデント対応の方針と手順

管理策：組織は、以下のものを策定および周知徹底し、定期的にレビュー／更新する。(i) 正式に文書化された、インシデント対応の方針。これらの方針では、目的、適用範囲、役割、責任、経営陣のコミットメント、組織間の調整、およびコンプライアンスを取り扱う。(ii) 正式に文書化された、インシデント対応方針の導入に関する手順。この手順は、インシデント対応方針の導入、ならびに関連する管理策の導入を容易にするために使用される。

補足ガイダンス：インシデント対応の方針と手順は、適用法、大統領令、指令、方針、規制、基準、およびガイダンスに準拠する。インシデント対応の方針は、組織の一般的な情報セキュリティ方針の一部とすることができる。インシデント対応の手順は、一般的なセキュリティプログラムの一部として作成することもできれば、必要に応じて特定の情報システムに特化した形で作成することもできる。セキュリティ方針および手順のガイダンスは、NIST SP 800-12 に記載されている。インシデントの対応および報告に関するガイダンスは、NIST SP 800-61 に記載されている。マルウェアによるインシデントの対処の仕方と防止法についてのガイダンスは、NIST SP 800-83 に記載されている。

管理強化策：なし。

IR-2 インシデント対応のトレーニング

管理策：組織は、情報システムに関するインシデント対応の役割と責任について、要員をトレーニングし、[指定：組織が定める頻度（少なくとも年 1 回）]間隔で再トレーニングを行う。

補足ガイダンス：なし。

管理強化策：なし。

IR-3 インシデント対応のテストと実習

管理策：組織は、[指定：組織が定めるテストおよび／または実習]を通じて、情報システムのインシデント対応能力を、[指定：組織が定める頻度（少なくとも年 1 回）]間隔でテストおよび／または実習し、インシデント対応の有効性を判断し、結果を文書化する。

補足ガイダンス：情報技術の計画および機能をテスト、トレーニングし、実習するためのプログラムに関するガイダンスは、NIST SP 800-84 に記載されている。

管理強化策：なし。

IR-4 インシデントの対応

管理策：組織は、セキュリティインシデントを処理するためのインシデント処理機能を導入する。この機能には、準備、検知と分析、封じ込め、根絶、復旧などが含まれる。

補足ガイダンス：インシデントに関する情報は、監査の監視、ネットワークの監視、物理的なアクセスの監視、およびユーザ／管理者の報告書など、さまざまな情報源から入手することができるが、これらに限定されるわけではない。組織は、継続的なインシデント対応活動から学んだ教訓を、インシデント対応手順に取り入れ、その手順を導入する。関連セキュリティ管理策：AU-6、PE-6。

管理強化策：

(1) 組織は、インシデント対応プロセスをサポートする自動化メカニズムを使用する。

IR-5 インシデントの監視

管理策：組織は、情報システムのセキュリティインシデントを継続的に追跡し、文書化する。

補足ガイダンス：なし。

管理強化策：なし。

IR-6 インシデントの報告

管理策：組織は、インシデント情報を関係当局に迅速に報告する。

補足ガイダンス：報告するインシデント情報の種別、内容、適時性、および報告先の当局または組織は、適用法、大統領令、指令、方針、規制、基準、およびガイダンスに準拠する。組織の担当者は、サイバーセキュリティーインシデントに関する報告を、US-CERT Concept of Operations for Federal Cyber Security Incident Handling が規定する時間内に、US-CERT(US コンピュータ事故緊急対応チーム（http://www.us-cert.gov）に対して行う。また、さらなるセキュリティインシデントを防止するために、発生したインシデント情報以外にも、情報システムの欠点や脆弱性に関する情報を、組織内の適切な担当者に時期を失せず報告する。インシデント報告のガイダンスは、NIST SP 800-61 に記載されている。

管理強化策：

(1) 組織は、セキュリティインシデントの報告を支援する自動化メカニズムを使用する。

IR-7 インシデント対応の支援

管理策：組織は、情報システムのユーザに対して、セキュリティインシデントの対応と報告に関する助言と支援を与える人的資源を提供する。この人的資源は、組織のインシデント対応能力に不可欠である。

補足ガイダンス：インシデント対応を支援するために導入される人的資源には、ヘルプデスクや支援グループなどがある。また、必要に応じて、フォレンジックサービスへのアクセスなどが考えられる。

管理強化策：

(1) 組織は、インシデント処理関連の情報およびサポートを、ユーザが入手しやすくするための、自動化メカニズムを使用する。

ファミリ: 保守 **クラス:** 運用

MA-1 システム保守の方針と手順

管理策：組織は、以下のものを策定および周知徹底し、定期的にレビュー／更新する。(i) 正式に文書化された、情報システム保守の方針。これらの方針では、目的、適用範囲、役割、責任、経営陣のコミットメント、組織間の調整、およびコンプライアンスを取り扱う。(ii) 正式に文書化された、情報システム保守の方針の導入に関する手順。この手順は、情報システム保守の方針の導入、ならびに関連する管理策の導入を容易にするために使用される。

補足ガイダンス：情報システム保守の方針と手順は、適用法、大統領令、指令、方針、規制、基準、およびガイダンスに準拠する。情報システム保守の方針は、組織の一般的な情報セキュリティ方針の一部とすることができる。システム保守の手順は、一般的なセキュリティプログラムの一部として作成することもできれば、必要に応じて特定の情報システムに特化した形で作成することもできる。セキュリティ方針および手順のガイダンスは、NIST SP 800-12 に記載されている。

管理強化策：なし。

MA-2 定期的な保守

管理策：組織は、メーカーまたはベンダーの仕様書および／または組織の要件に従い、情報システムのコンポーネントに対する日常の予防保守および定期保守(修理を含む)を計画、実施し、これを文書化して、その実施記録（結果）をレビューする。

補足ガイダンス：日常の予防保守、定期保守、および修理など全ての保守活動は、現地で行われるものか、または遠隔で行われるものか、備品（部品）は現地で調達されるのか、または別の場所へ移動させるのか、などの管理がされている。組織の担当者は、修理が必要な場合、情報システムまたはそのコンポーネントを施設から取り外す許可を与える。情報システムまたはそのコンポーネントを修理のために現地から移動させる必要がある場合、組織は、承認された手順に従って、関連する記録媒体からすべての情報を消去する。情報システムの保守が完了したのちに、組織は、保守による影響があったと思われるセキュリティ管理策をすべて点検し、これらが従来と同様に正しく機能していることを確認する。

管理強化策：

(1) 組織は、次のような情報を含む、保守記録を維持する。(i) 保守の実施日時、(ii) 保守作業担当者名、(iii) 必要なら、立会い者名、(iv) 実施した保守作業の内容、および (v) 取り外し、または交換した装置のリスト（該当する場合、ID 番号を含む）。

MA-3 保守ツール

管理策：組織は、システム保守ツールの使用を承認、管理、監視し、ツールを継続的に保守する。

補足ガイダンス：本管理策の目的は、診断活動／修理活動を行うために情報システムに導入されるハードウェアやソフトウェア（特定の保守活動を目的として導入される、ハードウェアやソフトウェアのパケットスニッファーなど）を、適切に扱うことである。保守を支援するもののシステムの一部でしかないハードウェアコンポーネントおよび／またはソフトウェアのコンポーネント（「ping」、「ls」、「ipconfig」を導入するソフトウェア、または、Ethernet switch の監視ポート機能をサポートするハードウェアおよびソフトウェアなど）は、本管理策の対象とはならない。

管理強化策：なし。

MA-4 遠隔保守

管理策：組織は、遠隔地から実行する保守および診断活動が採用されている場合、これを承認、管理、監視する。

補足ガイダンス：遠隔地で実施される保守および診断活動は、組織の管理下にはない外部のネットワーク（インターネットなど）を介して、担当者によって実施される。使用する遠隔保守ツールや診断ツールは、組織の方針に準拠するものとし、（組織は）それらのツールを使用する旨を、情報システムのセキュリティ計画に記載する。組織は、遠隔地から行ったすべての保守活動および診断活動の記録を維持する。遠隔保守におけるセキュリティを向上するための技術および／または管理策には、以下のものが含まれる：(i) 通信の暗号化と復号、(ii) NIST SP 800-63 に記述されているレベル 3 または 4 のトークンなど、強固な識別および認証技法、および(iii) リモート切断検証などがある。遠隔保守が完了すると、組織（場合によっては、情報システム）は、すべてのセッションを終了すると同時に、これらの活動を実施する際に確立されたリモート接続も終了する。遠隔保守者の認証に、パスワードに基づく認証が適用される場合、組織は、保守が終了するたびに、パスワードを変更するようにする。媒体をサニタイズ（消去）するためのガイダンスは、NIST SP 800-88 に記載されている。国家安全保障局（NSA: National Security Agency）のホームページ（http://www.nisa.gov/ia/government/mdg.cfm）では、NSA が承認する、媒体消去製品のリストを提供している。関連セキュリティ管理策：IA-2、MP-6。

管理強化策：

(1) 組織は、すべての遠隔保守セッションおよび診断セッションを監査し、組織の適切な担当者が、リモートセッションの保守記録をレビューする。

(2) 組織は、情報システムのセキュリティ計画の中に、遠隔地での保守と診断のリンクの導入および利用について、記載する。

MA-5 保守要員

管理策：組織は、承認された要員のみ、情報システムの保守を許可する。

補足ガイダンス：保守要員（ローカルまたは遠隔で保守を実施する要員）は、保守活動が組織の情報へのアクセスまで及ぶ場合、または情報システムの機密性、完全性、可用性が将来にわたって侵害される恐れがあるために保守を行うといった場合に、適切なアクセス権限を有しているとみなされる。必要なアクセス権限を持っていない保守要員が保守活動に携わる場合には、適切なアクセス権限を持つ組織の担当者が、保守要員を監督する。

管理強化策：なし。

MA-6 時宜を得た保守

管理策：組織は、[指定：組織が定める主要情報システムコンポーネントのリスト]に記載された保守サポートおよび予備部品を、障害発生後[指定：組織が定める期間]内に入手する。

補足ガイダンス：なし。

管理強化策：なし。

ファミリ: 記録媒体の保護 **クラス:** 運用

MP-1 記録媒体保護の方針と手順

管理策：組織は、以下のものを策定および周知徹底し、定期的にレビュー／更新する。(i) 正式に文書化された、記録媒体保護の方針。これらの方針では、目的、適用範囲、役割、責任、経営陣のコミットメント、組織間の調整、およびコンプライアンスを取り扱う。(ii) 正式に文書化された、記録媒体保護の導入に関する手順。この手順は、記録媒体保護方針の導入、ならびに関連する管理策の導入を容易にするために使用される。

補足ガイダンス：記録媒体保護の方針と手順は、適用法、大統領令、指令、方針、規制、基準、およびガイダンスに準拠する。記録媒体保護の方針は、組織の一般的な情報セキュリティ方針の一部とすることができる。記録媒体保護の手順は、一般的なセキュリティプログラムの一部として作成することもできれば、必要に応じて特定の情報システムに特化した形で作成することもできる。セキュリティ方針および手順のガイダンスは、NIST SP 800-12 に記載されている。

管理強化策：なし。

MP-2 記録媒体へのアクセス

管理策：組織は、情報システムの記録媒体へのアクセスを、承認された者にのみ許可する。

補足ガイダンス：情報システムの記録媒体には、デジタル媒体（ディスケット、磁気テープ、外部／リムーバブルハードドライブ、フラッシュ／USB メモリ、コンパクトディスク、デジタルビデオディスクなど）および非デジタル媒体（紙、マイクロフィルムなど）がある。本管理策は、情報を保存する機能を持ち、小型で携帯可能な計算装置や通信装置（ノート型パソコン、携帯端末、携帯電話など）にも適用される。

組織のリスクアセスメントは、アクセス制限が必要な記録媒体（およびそれらの媒体に記録されている情報）の特定を支援する。組織は、方針および手順の中で、アクセス制限が必要な記録媒体やその記録媒体へのアクセスが許可されているユーザ、およびアクセス制限を行うための具体的な方法などを文書化する。本管理策をどこまで厳密に適用するかは、記録媒体に保存されている情報を、FIPS199 のセキュリティ分類に従って分類した結果に依存する。たとえば媒体に含まれる情報が、組織の決定により公共のドメインに置かれる場合、または、一般への公開が可能な情報である場合、あるいは許可されたユーザ以外の者がアクセスした場合でも組織や個人への影響が少ない（または、まったくない）場合には、多くの保護策を要さない。このような場合は、記録媒体が置かれている場所の物理的なアクセス制御が、適切な保護を提供していることが考えられる。

管理強化策：

(1) 組織は、記録媒体の保管場所へのアクセスを制限し、アクセスしようとする者やアクセスを許可された者を監査する自動化メカニズムを使用する。

管理強化策の補足ガイダンス：管理強化策の補足ガイダンス：本管理強化策は主に、膨大な数の記録媒体を保管する組織指定の保管場所に適用されるものであり、ごく僅かな記録媒体を保管している場所（個人の事務所など）に適用されることを意図していない。

MP-4 記録媒体の保管

管理策：組織は、情報システムの記録媒体を、管理された区域に保管し、物理的に制御する。

補足ガイダンス：情報システムの記録媒体には、デジタル媒体（ディスケット、磁気テープ、外付けハードドライブ／リムーバブルハードドライブ、フラッシュ／USB メモリ、コンパクトディスク、デジタルビデオディスクなど）および非デジタル媒体（紙、マイクロフィルム）などがある。管理された区域とは、組織が情報および／または情報システムに対して導入した物理的保護および手続き上の保護が、組織指定の保護要件を十分に満たしていることが確信できるような、場所または空間である。本管理策は、情報を保存する機能を持ち、小型で携帯可能な計算装置や通信装置（ノート型パソコン、携帯端末、携帯電話など）にも適用される。電話システムも情報システムの一種と考えられており、中には情報を保存する機能を有するものもある（ボイスメールなど）。大半の電話システムには、他の情報システムに備わっている識別、認証、および

アクセス制御のメカニズムが備わっていない。このため組織の担当者は、電話のボイスメールシステムに保存されている情報の種類に十分な注意を払わなければならない。

組織のリスクアセスメントは、物理的な保護が必要な記録媒体（およびそれらの媒体に記録されている情報）の特定を支援する。組織は、方針および手順の中で、物理的な保護が必要な記録媒体および媒体を保護するための具体的な対策を文書化する。本管理策をどこまで厳密に適用するかは、記録媒体に保存されている情報を、FIPS199 のセキュリティ分類に従って分類した結果に依存する。たとえば媒体に含まれる情報が、組織の決定により公共のドメインに置かれる場合、または、一般への公開が可能な情報である場合、あるいは許可されたユーザ以外の者がアクセスした場合でも組織や個人への影響が少ない（または、まったくない）場合には、多くの保護策を要さない。このような場合は、記録媒体が置かれている場所の物理的なアクセス制御が、適切な保護を提供していることが考えられる。組織は、情報システムの記録媒体が、承認された装置、技法、および手続きを用いて破壊または完全に消去されるまで保護する。

多重防御の一環として、組織は、二次記憶装置上の情報を、定期的に暗号化することを検討する。FIPS199 のセキュリティ分類は、二次記憶装置の暗号化方式の選択に関するガイドを提供する。組織は、二次記憶装置上の情報の暗号化をサポートする効果的な暗号鍵管理を導入し、ユーザが暗号鍵を紛失した場合にも、情報の可用性が維持できるような保護を提供する。暗号鍵の策定、および暗号鍵の管理についてのガイダンスは、NIST SP 800-56 と 800-57 に記載されている。関連セキュリティ管理策：CP-9、RA-2。

管理強化策：なし。

MP-5 記録媒体の輸送

管理策：組織は、情報システムの記録媒体が組織の管理区域外に輸送されている間、保護、管理する。また、それらの媒体の輸送に関連する活動を、許可された担当者に限定する。

補足ガイダンス：情報システムの記録媒体には、デジタル媒体（ディスケット、磁気テープ、外付けハードドライブ／リムーバブルハードドライブ、フラッシュ／USB メモリ、コンパクトディスク、デジタルビデオディスクなど）および非デジタル媒体（紙、マイクロフィルム）などがある。管理された区域とは、組織が情報および／または情報システムに対して導入した物理的保護および手続き上の保護が、組織指定の保護要件を十分に満たしていることが確信できるような、場所または空間である。本管理策は、情報を保存する機能を持ち、小型で携帯可能な計算装置や通信装置（ノート型パソコン、携帯端末、携帯電話など）が、組織の管理区域外に輸送される場合にも適用される。電話システムも情報システムの一種と考えられており、中には情報を保存する機能を有するものもある（ボイスメールなど）。大半の電話システムには、他の情報システムに備わっている識別、認証、およびアクセス制御のメカニズムが備わっていない。このため組織の担当者は、組織の管理区域外に輸送される電話のボイスメールシステム上の、情報の種類に十分な注意を払わなければならない。組織のリスクアセスメントは、輸送中に物理的な保護が必要な記録媒体（およびその記録媒体に保存されている情報）の特定を支援する。組織は、方針および手順の中で、輸送中に物理的な保護が必要な記録媒体および媒体を保護するための具体的な対策を文書化する。本管理策をどこまで厳密に適用するかは、記録媒体に保存されている情報を、FIPS199 のセキュリティ分類に従って分類した結果に依存する。組織のリスクアセスメントは、非デジタル媒体の輸送に適した保存容器の選択も支援する。許可された輸送要員には、組織の外部の担当者（米国郵政公社、民間輸送、配送サービスなど）が含まれることがある。

管理強化策：

(1) 組織は、以下の方法を用いて、デジタルおよび非デジタル記録媒体が組織の管理区域外に輸送される間、保護する－[指定：組織が定めるセキュリティ対策（鍵付きの容器、暗号化など）]。

管理強化策の補足ガイダンス：デジタルおよび非デジタルの記録媒体を保護するための物理的セキュリティ対策および技術的セキュリティ対策は、組織によって承認されたものである。また、これらの対策は、記録媒体に保存されている情報を、FIPS199 のセキュリティ分類に従って分類した結果に準拠するものであり、適用法、大統領令、指令、方針、規制、基準、およびガイダンスにも準拠するものである。使用する暗号化メカニズムによっては、情報の機密性および／または完全性の保護につながるものもある。

(2) 組織は、情報システムの記録媒体の輸送に関する活動を、[指定：組織が定める記録方法]を利用して、文書化する。

管理強化策の補足ガイダンス： 組織は、組織のリスクアセスメントの結果に従って、情報システムの記録媒体の輸送に関する活動の要求事項を文書化する。

MP-6 媒体上の記録の抹消と媒体の廃棄

管理策：組織は、デジタルおよび非デジタルの記録媒体を廃棄する場合、または、再利用のために手放す場合には、媒体上の情報をサニタイズ(sanitizes：消去)する。

補足ガイダンス：サニタイズとは、情報システムの記録媒体から情報を除去するプロセスであり、これにより情報の復旧や再構築ができないようになり、情報の機密性が確保される。サニタイズの技術には、情報の消去、除去、および破壊などがあり、サニタイズを行うことで媒体の再利用時または廃棄時に、組織の情報が不正なユーザに公開されるのを防ぐことができる。組織は、媒体に含まれる情報が、組織の決定により公共のドメインに置かれる場合、または、一般への公開が可能な情報である場合、あるいは許可されたユーザ以外の者がアクセスした場合でも組織や個人への影響が少ない（または、まったくない）場合には、独自の判断でサニタイズの技術や手順を使用する。記録媒体のサニタイズに関するガイダンスは、NIST SP 800-88 に記載されている。国家安全保障局（NSA = National Security Agency）でも、記録媒体のサニタイズに関するガイダンスを提供しており、承認済みのサニタイズ製品のリストを http://www.nsa.gov/ia/government/mdg.cfm にて公開している。

管理強化策：なし。

ファミリ: 物理的および環境的な保護 **クラス:** 運用

PE-1 物理的および環境的な保護の方針と手順

管理策：組織は、以下のものを策定および周知徹底し、定期的にレビュー／更新する。(i) 正式に文書化された、物理的および環境的な保護の方針。これらの方針では、目的、適用範囲、役割、責任、経営陣のコミットメント、組織間の調整、およびコンプライアンスを取り扱う。(ii) 正式に文書化された、物理的および環境的な保護の方針の導入に関する手順。この手順は、物理的および環境的な保護の方針の導入、ならびに関連する管理策の導入を容易にするために使用される。

補足ガイダンス：物理的および環境的な保護の方針と手順は、適用法、大統領令、指令、方針、規制、基準、およびガイダンスに準拠する。物理的および環境的な保護の方針は、組織の一般的な情報セキュリティ方針の一部とすることができる。物理的および環境的な保護の手順は、一般的なセキュリティプログラムの一部として作成することもできれば、必要に応じて特定の情報システムに特化した形で作成することもできる。セキュリティ方針および手順のガイダンスは、NIST SP 800-12 に記載されている。

管理強化策：なし。

PE-2 物理的アクセス権限

管理策：組織は、情報システムが収容されている施設（施設の中で、外部アクセスが可能な区域として指定された区域を除く）への、アクセスを許可された要員の最新リストを作成、維持し、それらの要員に対して適切な資格認定書（authorization credential）を発行する。組織の中で指定された担当者は、アクセスリストと資格認定書を［指定：組織が定める頻度（少なくとも年 1 回）］間隔でレビューし、承認する。

補足ガイダンス：適切な資格認定書には、バッジ、身分証明書、スマートカードなどがある。組織は、情報システムの収容施設へのアクセスが不要になった要員を、アクセスリストから直ちに削除する。

管理強化策：なし。

PE-3 物理的アクセス制御

管理策：組織は、情報システムが収容されている施設（施設の中で、外部アクセスが可能な区域として指定された区域を除く）への、すべての物理的アクセスポイント（指定された出入口を含む）を管理し、施設へのアクセスを許可する前に、個々のアクセス権限を検証する。組織は、リスクアセスメントの結果に基づき、パブリックアクセスが可能な区域として指定された区域に対しても、適宜、管理を行う。

補足ガイダンス：組織は、物理的なアクセス装置（鍵、錠、ダイヤル錠、カードリーダ）および／または警備員により、情報システム収容施設への入場を管理する。組織は、鍵、ダイヤル錠、およびそのほかのアクセス装置を安全に保管し、それらの装置の目録を定期的に作成する。組織は、鍵およびダイヤル錠を、(i) 定期的に、および (ii) 紛失した場合や錠の番号が漏洩した場合、または要員が異動または解雇された場合に、変更する。組織の情報システム（およびその一部）に接続されるワークステーションおよび関連周辺機器は、適切に管理されることが保証される場合は、パブリックアクセスを許可する区域に設置されることがある。連邦政府の個人識別情報の検証（PIV）のクレデンシャル（credential）が識別トークンとして使用されている区域では、そのアクセス制御システムは、FIPS201、および NIST SP 800-73 の要件に準拠する。トークンベースのアクセス制御機能であり、かつ暗号検証（cryptographic verification）が採用されている場合には、そのアクセス制御システムは、NIST SP 800-78 の要件に準拠する。トークンベースのアクセス制御機能であり、かつバイオメトリック検証（biometric verification）が採用されている場合には、そのアクセス制御機能システムは、NIST SP 800-76 の要件に準拠する。

管理強化策：なし。

PE-5 表示媒体へのアクセス制御

管理策：組織は、情報を表示する情報システム機器への物理的アクセスを制御して、許可されていない個人が出力表示を見ることを防止する。

補足ガイダンス：なし。

管理強化策：なし。

PE-6 物理的アクセスの監視

管理策：組織は、物理的なセキュリティインシデントを検知し対応するために、システムへの物理的アクセスを監視する。

補足ガイダンス：組織は、物理的アクセスログを定期的にレビューし、明らかなセキュリティ侵害または疑わしい物理的アクセス活動について調査する。検知された物理的セキュリティインシデントに対する組織の対応能力は、組織のインシデント対応能力を示す一つの要素である。

管理強化策：

(1) 組織は、リアルタイムの物理的侵入アラームや監視装置により監視を行う。

PE-7 来訪者の管理

管理策：組織は、外部からのアクセスを許可する区域以外の、情報システムの設置場所に対して、アクセスを許可する前に来訪者の認証を行うことで、システムへの物理的アクセスを制御する。

補足ガイダンス：政府の請負業者、およびその他の恒久的な資格認定を受けた者は、来訪者とは見なされない。連邦政府の職員および政府の請負業者の認証に使われる個人識別情報の検証（PIV）のクレデンシャル（credential）は、FIPS201 に準拠する。また、PIV クレデンシャルの発行元は、NIST SP 800-79 の規定により、発行を認可された組織である。

管理強化策：

(1) 組織は、必要に応じて来訪者に同伴し、来訪者の活動を監視する。

PE-8 アクセス記録

管理策：組織は、情報システムが収容されている施設への、来訪者のアクセスログを維持する（外部からのアクセスを許可する区域を除く）。アクセスログには以下の項目が含まれる。(i) 来訪者の氏名および所属組織、(ii) 来訪者の署名、(iii) 身分証明書、(iv) 来訪日、(v) 入出時刻、(vi) 来訪の目的、(vii) 来訪を受けた担当者の氏名および所属組織。組織の中で指定された担当者は、[指定：組織が定める頻度]間隔で、来訪者アクセスログをレビューする。

補足ガイダンス：なし。

管理強化策：なし。

PE-9 電源装置および電源ケーブル配線

管理策：組織は、情報システム用電源装置および電源ケーブル配線を、損傷および破壊から保護する。

補足ガイダンス：なし。

管理強化策：なし。

PE-10 緊急遮断

管理策：組織は、情報システムリソースが集中している施設内の、正常に機能していない、または、脅威をもたらす恐れのある情報システムコンポーネントの電源を、遠隔で遮断できる機能を提供する。この遮断機能は、要員が危険を冒して当該コンポーネントに近づかなくても、施設内の特定の場所から作動できるものでなければならない。

補足ガイダンス：情報システムのリソースが集中する施設とは、データセンター、サーバールーム、およびメインフレームルームなどがある。

管理強化策：なし。

PE-11 非常時用電源

管理策：組織は、一次電源の供給が止まった場合に情報システムの所定のシャットダウンを可能にするための、無停電電源装置（短期間無停電で電力を供給できる装置）を用意する。

補足ガイダンス：なし。

管理強化策：なし。

PE-12 非常時用照明

管理策：組織は、停電が発生した場合に非常口と避難経路を照らすための、自動非常時用照明システムを採用し、これを保守する。

補足ガイダンス：なし。

管理強化策：なし。

PE-13 防火

管理策：組織は、火災発生時に作動する消火および検知装置／システムを使用し、これを保守する。

補足ガイダンス：火災の消火および検知装置／システムには、スプリンクラーシステム、手持ち式の消火器、固定式消火ホース、煙探知器などがあるが、これらに限定されるわけではない。

管理強化策：

(1) 組織は、火災発生時に自動的に作動し、組織および火災の緊急対応者に通知する、火災検知装置／システムを採用する。

(2) 組織は、組織および緊急対応者に対して、装置（またはシステム）がアクティブ化されたことを自動的に通知する、火災消火装置／システムを採用する。

(3) 組織は、非常駐型の自動火災消火機能を施設に備える。

PE-14 温度および湿度の管理

管理策：組織は、情報システムが収容されている施設内の温度と湿度を監視し、常に許容範囲内に収まるようにする。

補足ガイダンス：なし。

管理強化策：なし。

PE-15 浸水による損害からの保護

管理策：組織は、主要な担当者による操作が可能な、適切に動作している主遮断弁を備えることによって、配管系統の破損、またはその他の水漏れ原因による浸水の損害から、情報システムを保護する。

補足ガイダンス：なし。

管理強化策：なし。

PE-16 荷物の搬入と搬出

管理策：組織は、情報システム関連品目の施設への搬出入を許可および管理し、これらの品目についての適切な記録を保守する。

補足ガイダンス：組織は、搬出入区域へのアクセスを制御する。また、可能な場合は、不正なアクセスを防ぐために、その区域を情報システムおよび記録媒体のライブラリから隔離する。

管理強化策：なし。

PE-17 代替作業拠点

管理策：組織は、代替作業拠点において、適切な管理セキュリティ管理策、運用セキュリティ管理策、および技術的セキュリティ管理策を採用する。

補足ガイダンス：組織は、セキュリティ問題が発生した場合に、従業員が情報システムセキュリティスタッフに連絡する手段を提供する。在宅勤務および広帯域通信でのセキュリティに関するガイダンスは、NIST SP 800-46 に記載されている。

管理強化策：なし。

PE-18 情報システムコンポーネントの所在地

管理策：組織は、情報システムのコンポーネントを施設内に適切に配置し、物理的な危険および環境的な危険による損害を最小限に留め、不正アクセスの機会を最小限に食い止めるようにする。

補足ガイダンス：物理的な危険および環境的な危険には、浸水、火災、竜巻、地震、ハリケーン、テロ活動、器物破損、電気的な支障、および電磁放射などがある。組織は、施設の所在地や立地についても、常に、物理的および環境的な危険を考慮する。

管理強化策：なし。

ファミリ: 計画 **クラス:** 管理

PL-1 セキュリティ計画作成の方針と手順

管理策：組織は、以下のものを策定および周知徹底し、定期的にレビュー／更新する。(i) 正式に文書化された、セキュリティ計画の方針。これらの方針では、目的、適用範囲、役割、責任、経営陣のコミットメント、組織間の調整、およびコンプライアンスを取り扱う。(ii) 正式に文書化された、セキュリティ計画の方針の導入に関する手順。この手順は、セキュリティ計画の方針の導入、ならびに関連する管理策の導入を容易にするために使用される。

補足ガイダンス：セキュリティ計画の方針と手順は、適用法、大統領令、指令、方針、規制、基準、およびガイダンスに準拠する。セキュリティ計画の方針は、組織の一般的な情報セキュリティ方針の一部とすることができる。セキュリティ計画の手順は、一般的なセキュリティプログラムの一部として作成することもできれば、必要に応じて特定の情報システムに特化した形で作成することもできる。セキュリティ計画に関するガイダンスは、NIST SP 800-18 に記載されている。セキュリティ方針および手順のガイダンスは、NIST SP 800-12 に記載されている。

管理強化策：なし。

PL-2 システムセキュリティ計画

管理策：組織は、情報システムのセキュリティ計画を作成し、導入する。このセキュリティ計画では、システムのセキュリティ要件の概要、およびその要件を満たすために実施中または計画中のセキュリティ管理策を記述する。組織内の指定された責任者は、セキュリティ計画をレビューし、承認する。

補足ガイダンス：セキュリティ計画は、組織の情報システムアーキテクチャおよび情報セキュリティのアーキテクチャと一致する。セキュリティ計画に関するガイダンスは、NIST SP 800-18 に記載されている。

管理強化策：なし。

PL-3 システムセキュリティ計画の更新

管理策：組織は、情報システムのセキュリティ計画を[指定：組織が定める頻度（少なくとも年1回）]間隔でレビューし、システム／組織上の変更を反映するために、または、計画の実施中に確認された問題およびセキュリティ管理策の評価中に確認された問題に対処するために、修正する。

補足ガイダンス：重要な変更に関しては、事前に定義し、構成管理プロセスで特定できるようにする。セキュリティ計画の更新に関するガイダンスは、NIST SP 800-18 に記載されている。

管理強化策：なし。

PL-4 行動規則

管理策：組織は、情報システムの使用に関するユーザの責任および期待される行動を記述した、一連の規則を策定し、情報システムのすべてのユーザが直ちに利用できるようにする。組織は、情報システム（およびシステムに保存されている情報）へのアクセスを許可する前に、ユーザから署名入りの同意書を受け取る。この同意書は、ユーザが当該行動規則を読み、理解し、遵守することに同意したことを証明する、文書である。

補足ガイダンス：電子署名は、組織の方針により使用が禁止されている場合を除き、行動規則への同意手段として利用することができる。行動規則の作成に関するガイダンスは、NIST SP 800-18 に記載されている。

管理強化策：なし。

PL-5 プライバシーの影響評価

管理策：組織は、OMB の方針に則り、情報システムのプライバシー影響評価を実施する。

補足ガイダンス：2002 年施行の電子政府法のプライバシープロビジョン(privacy provisions)の実施に関するガイダンスは、OMB Memorandum 03-22 に記載されている。

管理強化策：なし。

PL-6 セキュリティ関連の活動計画作成

管理策：組織は、セキュリティ関連の活動がもたらす組織の業務（ミッション、機能、イメージ、および評判など）や資産、および個人への影響を削減するために、これらの活動についてあらかじめ計画を立て、調整を行う。

補足ガイダンス：日常的なセキュリティ関連の活動には、セキュリティ評価、監査、システム用ハードウェアとソフトウェアの保守、セキュリティ承認、およびセキュリティのテスト／実践などがあるが、これらに限定されない。一歩進んだ組織の計画および調整には、緊急事態および非緊急事態（日常事態）が含まれる。

管理強化策：なし。

ファミリ: 人的セキュリティ **クラス:** 運用

PS-1 人的セキュリティの方針および手順

管理策：組織は、以下のものを策定および周知徹底し、定期的にレビュー／更新する。(i) 正式に文書化された、人的セキュリティの方針。これらの方針では、目的、適用範囲、役割、責任、経営陣のコミットメント、組織間の調整、およびコンプライアンスを取り扱う。(ii) 正式に文書化された、人的セキュリティの方針の導入に関する手順。この手順は、人的セキュリティの方針の導入、ならびに関連する管理策の導入を容易にするために使用される。

補足ガイダンス：人的セキュリティの方針と手順は、適用法、大統領令、指令、方針、規制、基準、およびガイダンスに準拠する。人的セキュリティの方針は、組織の一般的な情報セキュリティ方針の一部とすることができる。人的セキュリティの手順は、一般的なセキュリティプログラムの一部として作成することもできれば、必要に応じて特定の情報システムに特化した形で作成することもできる。セキュリティ方針および手順のガイダンスは、NIST SP 800-12 に記載されている。

管理強化策：なし。

PS-2 職位の分類

管理策：組織は、すべての職位に対してリスクレベルを指定し、これらの職位に就く個人の審査基準を定める。組織は、職位に対するリスクレベルを[指定：組織が定める頻度]間隔でレビューし、修正する。

補足ガイダンス：職位に対するリスクは、5 CFR 731.106(a) および人事管理局（Office of Personnel Management）の方針およびガイダンスに準拠する。

管理強化策：なし。

PS-3 要員に対する審査

管理策：組織は、組織の情報および情報システムへのアクセスを必要とするユーザに対して、アクセスを許可する前に審査を行う。

補足ガイダンス：審査は、(i) 5 CFR 731.106、(ii) 人事管理局の方針、規制、およびガイダンス、(iii) 組織の方針、規制、およびガイダンス、(iv) FIPS 201 および SPs 800-73、800-76、および 800-78 ならびに (v) 当該職務に関するリスクを決定するために設けられた判断基準に準拠する。

管理強化策：なし。

PS-4 要員の解雇

管理策：従業員を解雇する場合、組織は、以下のことを行う ― その従業員による情報システムへのアクセスを停止する、その従業員との退職時面接を行う、その従業員から組織の情報システム関連資産を回収する、その従業員が作成しシステムに保存されている公式記録を、組織の適切な要員が参照できるようにする。

補足ガイダンス：情報システム関連の資産には、鍵、身分証明書、入館証などがある。正当な理由により解雇される従業員や契約者に対して、本管理策をタイムリーに実施することは、とても重要である。

管理強化策：なし。

PS-5 人事異動

管理策： 組織は、職員が組織内で配置転換となった場合や、別の職位についた場合に、情報システム／施設へのアクセス権限をレビューし、適切な活動を開始する。

補足ガイダンス：求められる適切な活動には、以下のようなものが考えられる。(i) その職員に、古い鍵、身分証明書および入館証を返却させ、新しいものを発行する、(ii) その職員の古いアカウントを無効化し、新しいアカウントを発行する、(iii) その職員のシステムへのアクセス権限を変更する、および(iv) その職員が前の就業場所で作成した公式記録（古いアカウントで作成したもの）を、組織の適切な要員が参照できるようにする。

管理強化策：なし。

PS-6 アクセス契約

管理策：組織は、組織の情報および情報システムへのアクセスを必要とする要員に対して、アクセスを許可する前に適切なアクセス契約を締結し、[指定：組織が定める頻度]の間隔で、アクセス契約をレビュー／更新する。

補足ガイダンス：アクセス契約には、機密保持契約、利用規定、行動規則、利益相反契約などがある。電子署名は、組織の方針により使用が禁止されている場合を除き、行動規則への同意手段として利用することができる。

管理強化策：なし。

PS-7 第三者の人的セキュリティ

管理策：組織は、第三者プロバイダに対する人的セキュリティ要件（セキュリティの役割や責任を含む）を規定し、プロバイダの法令順守状況を監視する。

補足ガイダンス：第三者プロバイダには、サービス機関、契約者、情報システムの開発を提供する組織やIT サービスを提供する組織、外部委託によるアプリケーションを提供する組織やネットワークおよびセキュリティの管理を提供する組織などが含まれる。組織は、人的セキュリティ要件を、調達関連文書に明示的に含める。情報技術セキュリティサービスに関するガイダンスは、NIST SP 800-35 に記載されている。

管理強化策：なし。

PS-8 要員に対する制裁

管理策：組織は、組織が定めた情報セキュリティ方針および手順に従わない要員を処罰するための、制裁プロセスを採用する。

補足ガイダンス：制裁プロセスは、適用法、大統領令、指令、方針、規制、基準、およびガイダンスに準拠する。制裁プロセスは、組織の一般的な人事方針および手順の一部に含めることができる。

管理強化策：なし。

ファミリ: リスクアセスメント **クラス:** 管理

RA-1 リスクアセスメントの方針と手順

管理策：組織は、以下のものを策定および周知徹底し、定期的にレビュー／更新する。(i) 正式に文書化された、リスクアセスメントの方針。これらの方針では、目的、適用範囲、役割、責任、経営陣のコミットメント、組織間の調整、およびコンプライアンスを取り扱う。(ii) 正式に文書化された、リスクアセスメントの方針の導入に関する手順。この手順は、リスクアセスメントの方針の導入、ならびに関連する管理策の導入を容易にするために使用される。

補足ガイダンス：リスクアセスメントの方針と手順は、適用法、大統領令、指令、方針、規制、基準、およびガイダンスに準拠する。リスクアセスメントの方針は、組織の一般的な情報セキュリティ方針の一部とすることができる。リスクアセスメントの手順は、一般的なセキュリティプログラムの一部として作成することもできれば、必要に応じて特定の情報システムに特化した形で作成することもできる。リスクアセスメントに関するガイダンスは、NIST SP 800-30 に記載されている。セキュリティ方針および手順のガイダンスは、NIST SP 800-12 に記載されている。

管理強化策：なし。

RA-2 セキュリティ分類

管理策：組織は、情報システム、およびシステムが処理、保存、または送受信する情報を適用法、大統領令、指令、方針、規制、基準、およびガイダンスに従って分類し、その結果（裏付けとなる根拠を含む）を文書化し、システムセキュリティ計画に盛り込む。組織内の指定された上級責任者は、セキュリティ分類をレビューし、承認する。

補足ガイダンス：FIPS199 は、国家安全保障にかかわるシステム（または情報）以外のシステム（または情報）の、セキュリティ分類に適用される連邦政府の基準である。組織は、FIPS199 によるセキュリティ分類を、組織全体の活動として実施する。この活動には、組織の最高情報責任者、上級情報セキュリティ責任者、情報システムのオーナー、および情報のオーナーが深く関与する。組織は、情報を分類する際に、自組織以外の組織に対する潜在的な影響も考慮すると同時に、2001 年施行の米国愛国者法（USA Patriot Act）、国土安全に関する大統領指令に従って、国家レベルの影響についても考慮する。多重防御の一環として、組織は、より高位影響の情報システムを、物理的に別のドメイン（または環境）に移動する。また、組織のリスクアセスメントの結果に基づき、これらの情報システムへのネットワークアクセスを制限する、または、禁止することも検討する。情報システム内の情報のセキュリティ分類決定に関するガイダンスは、NIST SP 800-60 に記載されている。関連セキュリティ管理策：MP-4、SC-7。

管理強化策：なし。

RA-3 リスクアセスメント

管理策：組織は、政府機関の業務および資産を支援する情報および情報システム（外部の組織によって管理／運用されている情報および情報システムも含む）への不正なアクセス、使用、開示、妨害、改ざん、または破壊によってもたらされる、潜在的リスクと損害の大きさを評価する。

補足ガイダンス：リスクアセスメントは、脆弱性、脅威源、および計画中または実施中のセキュリティ管理策を考慮に入れ、組織の業務や資産、または個人にもたらされる残留リスクのレベルを、情報システムの運用状況に基づき、判断する。組織は、情報を分類する際に、自組織以外の組織に対する潜在的な影響も考慮すると同時に、2001 年施行の米国愛国者法（USA Patriot Act）、国土安全に関する大統領指令に従って、国家レベルの影響についても考慮する。リスクアセスメントでは、外部の組織（サービスプロバイダ、組織に代わって組織の情報システムを運用する契約者、組織の情報システムにアクセスする個人、外部委託先のエンティティなど）によってもたらされる、組織の業務、資産、個人へのリスクも考慮する。OMB の方針および電子認証／電子政府イニシアチブに従い、連邦政府の情報システムにアクセスする一般ユーザに対して、非公開の情報または個人に関する情報を保護するために認証が行われることもある。このため、組織のリスクアセスメントにおいては、連邦政府の情報システムへの一般的なアクセスも考慮しなければならない。一般調達局（：GSA = General Services Administration）では、連邦政府の情報システムへの一般的なアクセスに関する、リスクアセスメントツールを提供している。脅威、脆弱性および影響評価を含

むリスクアセスメントの実施に関するガイダンスは、NIST SP 800-30 に記載されている。

管理強化策：なし。

RA-4 リスクアセスメントの更新

管理策：組織は、[指定：組織が定める頻度]間隔でリスクアセスメントを更新する。また、情報システムやシステム収容施設に重要な変更があった場合、または、システムのセキュリティ状態や承認状態に影響を与えるような状況が発生した場合にも、リスクアセスメントを更新する。

補足ガイダンス：組織は、特定の変更が、情報システムにとって重要な変更であるかどうかを判断するための基準を作成し、文書化する。リスクアセスメントの更新の実施に関するガイダンスは、NIST SP 800-30 に記載されている。

管理強化策：なし。

RA-5 脆弱性のスキャン（走査）

管理策：組織は、[指定：組織が定める頻度]間隔で、または、システムに影響をおよぼす重大な脆弱性が新たに確認、報告された場合に、システムの脆弱性をスキャンする。

補足ガイダンス：脆弱性のスキャンは、適切なスキャンツールと技法を用いて実施する。組織は、選出した要員に対して、脆弱性スキャンツールと技法の使用法、および保守のためのトレーニングを実施する。脆弱性のスキャンは、定期的に行われる場合もあれば、組織の方針やリスクアセスメントの結果に従って非定期的に行われる場合もある。脆弱性のスキャンによって得られた情報は、他の情報システムに存在する同様の脆弱性を排除するために、組織全体の適切な担当者間で自由に共有できる。特注のソフトウェアおよびアプリケーションの脆弱性分析には、上記の手法以外にも、より専門的な手法が必要になる場合がある（たとえば、アプリケーション用の脆弱性スキャンツール、ソースコードのレビュー、ソースコードの静的分析など）。ネットワークセキュリティのテストに関するガイダンスは、NIST SP 800-42 に記載されている。パッチのあて方とその管理についてのガイダンスは、NIST SP 800-40（Version 2）に記載されている。

管理強化策：なし。

ファミリ: システムおよびサービスの調達 **クラス:** 管理

SA-1 システムおよびサービスの調達の方針と手順

管理策：組織は、以下のものを策定および周知徹底し、定期的にレビュー／更新する。(i) 正式に文書化された、システムおよびサービスの調達方針（情報セキュリティについての検討事項を含む）。これらの方針では、目的、適用範囲、役割、責任、経営陣のコミットメント、組織間の調整、およびコンプライアンスを取り扱う。(ii) 正式に文書化された、システムとサービスの調達方針の導入に関する手順。この手順は、システムとサービスの調達方針の導入、ならびに関連する管理策の導入を容易にするために使用される。

補足ガイダンス：システムおよびサービスの調達方針と手順は、適用法、大統領令、指令、方針、規制、基準、およびガイダンスに準拠する。システムおよびサービスの調達方針は、組織の一般的な情報セキュリティ方針の一部とすることができる。システムおよびサービスの調達手順は、一般的なセキュリティプログラムの一部として作成することもできれば、必要に応じて特定の情報システムに特化した形で作成することもできる。セキュリティ方針および手順のガイダンスは、NIST SP 800-12 に記載されている。

管理強化策：なし。

SA-2 リソースの割り当て

管理策：組織は、資本計画および投資管理プロセスの一環として、情報システムを適切に保護するための、リソースの決定、文書化、および割り当てを行う。

補足ガイダンス：組織は、情報システムのセキュリティ要件の決定事項をミッション／投資対効果計画に含めると同時に、情報システムセキュリティのための個別項目を、組織の計画および予算関係の文書に記載する。資本計画および投資管理プロセスへのセキュリティの統合に関するガイダンスは、NIST SP 800-65 に記載されている。

管理強化策：なし。

SA-3 ライフサイクルサポート

管理策：組織は、システム開発ライフサイクル方法論（情報セキュリティの検討事項を含む）を使用して、情報システムを管理する。

補足ガイダンス：システム開発ライフサイクルにおけるセキュリティ検討事項に関するガイダンスは、NIST SP 800-64 に記載されている。

管理強化策：なし。

SA-4 調達

管理策：組織は、リスクアセスメントの結果にもとづき、また、適用法、大統領令、指令、方針、規制、および基準に従って、セキュリティ要件および／またはセキュリティ仕様を策定し、情報システムの調達契約に明示的に含める、または参照として含める。

補足ガイダンス：

(入札、見積もり、提案などの)要請文書
情報システムおよび情報サービスの要請文書（提案依頼書など）には、以下の項目を明示的にまたは参照として記述する。(i) 必要なセキュリティ機能（セキュリティーニーズ、および必要に応じて、特定のセキュリティ管理策や FISMA 要件など）、(ii) 必要な設計および開発プロセス、(iii) 必要なテストおよび評価手順、(iv) 必要な文書。組織は、要請文書に記載する要件に従って、新たな脅威／脆弱性が確認された場合に、または、新たな技術が導入された場合に、セキュリティ管理策を更新することができる。情報セキュリティ製品の選択に関するガイダンスは、NIST SP 800-36 に記載されている。情報技術セキュリティサービスに関するガイダンスは、NIST SP 800-35 に記載されている。システム開発ライフサイクルにおけるセキュリティ検討事項に関するガイダンスは、NIST SP 800-64 に記載されている。

情報システムの文書化

要請文書には、情報システムの適切な文書化に関する要件が記載されている。この文書化は、ユーザおよびシステム管理者のガイダンス、および情報システムへのセキュリティ管理策の導入に関する情報を扱っている。これらの文書をどこまで詳細に記述するかは、対象システムを FIPS199 のセキュリティ分類に従って分類した結果に依存する。

テストおよび評価が行われ、その有効性が確認されている製品の使用

テスト／評価済みの情報技術製品の調達および使用に関するガイダンスは、NIST SP 800-23 に記載されている。

構成設定および導入ガイダンス

情報システムに必要な文書には、セキュリティの構成設定およびセキュリティの導入ガイダンスが含まれる。OMB の FISMA 報告指示書では、連邦情報システムの構成要件に関するガイダンスを提供している。情報技術製品の構成設定に関するガイダンスは、NIST SP 800-70 に記載されている。

管理強化策：

(1) 組織の要請文書には、情報システムに採用されているセキュリティ管理策の機能特性を、管理策の分析やテストを実施するのに十分な詳細レベルで記述したものが、含まれることが要求される。

SA-5 情報システムの文書化

管理策：組織は、当該情報システムに関する適切な文書を入手し、必要に応じて保護し、これらの文章を許可された者が利用できるようにする。

補足ガイダンス：資料には、管理者およびユーザ用ガイドに加えて、以下の情報が含まれる。(i) 情報システムの構成、導入、および運用に関する情報、ならびに (ii) システムのセキュリティ機能を効果的に利用するための情報。情報システムについての適切な文書が利用できない場合、または存在しない場合（たとえば、システムの経年化やベンダー／製造者から十分なサポートが得られない場合など）、組織は、それらの文書を入手するためのこれまでの試みを文書化し、必要な場合には、代替管理策を提供する。

管理強化策：

(1) 組織は、管理者とユーザ用のガイドに加えて、入手可能な場合は、ベンダー／製造者が作成した資料（情報システムに採用されているセキュリティ管理策の機能特性を、管理策の分析やテストを実施するのに十分な詳細レベルで記述したもの）を入手し、情報システムの資料に含める。

SA-6 ソフトウェアの利用の制限

管理策：組織は、ソフトウェアの利用の制限を順守する。

補足ガイダンス：ソフトウェアおよび関連する文書は、契約内容および著作権法に従って利用する。台数契約によって保護されているソフトウェアや関連文書の場合、組織は、これらのコピーと配付を管理するための、追跡システムを採用する。組織は、外部アクセスが可能なピアツーピアのファイル共有技術の利用を管理、文書化し、この機能が、著作物の不正な配付、表示、実行、または複製に使用されないことを保証する。

管理強化策：なし。

SA-7 ユーザがインストールしたソフトウェア

管理策：組織は、ユーザによるソフトウェアのインストールを管理するための、明示的な規則を実施する。

補足ガイダンス：必要な特権を与えられたユーザは、ソフトウェアを導入することができる。組織は、導入が許可されているソフトウェアの種類（たとえば、既存のソフトウェアへの更新(版)やセキュリティパッチ）と導入が許可されていないソフトウェアの種類（たとえば、政府用ではない個人用のフリーソフト、および潜在的に悪質であるかどうかが判断できない、または、怪しいソフトウェアなど）を特定する。

管理強化策：なし。

SA-8 セキュリティエンジニアリングの原則

管理策：組織は、セキュリティエンジニアリングの原則に従って、情報システムを設計し、導入する。

補足ガイダンス：情報システムのセキュリティエンジニアリングの原則に関するガイダンスは、NIST SP 800-27 に記載されている。セキュリティエンジニアリングの原則の適用は、主に、新規開発の情報システム、または重要なアップグレードを行っているシステムを対象にしたものであり、このようなプロセスは、システム開発のライフサイクルに統合される。旧式の情報システムの場合は、セキュリティエンジニアリングの原則を、システム内のハードウェア、ソフトウェアおよびファームウェアコンポーネントの現在の状態を考慮した上で、可能な範囲内でシステムのアップグレードや修正に適用する。

管理強化策：なし。

SA-9 外部の情報システムサービス

管理策：組織は、(i) 外部の情報システムサービスのプロバイダが、適用法、大統領令、指令、方針、規制、基準、ガイダンス、および締結されたサービス内容の合意書に従って、適切なセキュリティ管理策を使用することを求め、また(ii) セキュリティ管理策の法令順守状況を監視する。

補足ガイダンス：外部の情報システムサービスは、自身のシステムの認定範囲外で実施されるサービス（たとえば、組織の情報システムによって利用されるサービスではあるが、そのシステムの一部ではない）である。外部のサービスプロバイダとの関係は、さまざまな形式で構築される。たとえば、ジョイントベンチャー、ビジネスパートナーシップ、アウトソーシング（契約、組織同士の取り決め、新規の事業の取り決めなど）、ライセンス契約および／またはサプライチェーンの交換などが考えられる。最終的に、外部の情報システムサービスを利用することによって生じる組織の業務や資産、および個人へのリスクを適切に緩和することは、運用認可権限者に委ねられる。よって、運用認可権限者は、組織が情報システムのセキュリティに関するさまざまな問題を扱う場合には、外部のサービスプロバイダとの間に適切なトラストチェーンを構築することを求めなければならない。トラストチェーンの構築には、外部サービスを提供するそれぞれのプロバイダが、複雑になりがちな消費者—提供者の関係において、サービスに対する適切な保護を行っていることが、組織によって確認され、その状態が維持されることが求められる。外部のサービスおよび／またはサービスプロバイダが十分に信頼できない場合、組織は、代替管理策を採用するか、あるいは組織の業務や資産、または個人に対してより大きなリスクを受け入れるかを選択しなければならない。外部情報システムサービスの文書化には、政府、サービスプロバイダ、およびエンドユーザのセキュリティに関する役割と責任、ならびにあらゆるサービス内容の合意事項（SLA）を含める。サービス内容の合意書(SLA)では、各セキュリティ管理策に期待される性能を定義し、予測可能な成果を記述し、要求に準拠していないことが特定された場合の是正および対応要件を記述する。情報技術セキュリティサービスに関するガイダンスは、NIST SP 800-35 に記載されている。システム開発ライフサイクルにおけるセキュリティ検討事項に関するガイダンスは、NIST SP 800-64 に記載されている。

管理強化策：なし。

SA-11 開発者によるセキュリティテスト

管理策：組織は、情報システムの開発者に対して、セキュリティのテストおよび評価計画を作成し、それらの計画を実施すること、また、結果を文書化することを求める。

補足ガイダンス：開発におけるセキュリティテスト結果を使用する際には、開発者によるテスト完了後に、情報システムに対するセキュリティ関連の修正が行われた時は、セキュリティテスト結果はその（修正による）影響を受けることを認識し、テスト結果を十分に確認した上で、最大限に活用すること。テストの結果は、搬入された情報システムのセキュリティ承認および運用認可のプロセスを支援するために用いられることがある。関連セキュリティ管理策：CA-2、CA-4。

管理強化策：なし。

ファミリ: システムおよび通信の保護 **クラス:** 技術

SC-1 システムおよび通信の保護の方針と手順

管理策：組織は、以下のものを策定および周知徹底し、定期的にレビュー／更新する。(i) 正式に文書化された、システムおよび通信の保護方針。これらの方針では、目的、適用範囲、役割、責任、経営陣のコミットメント、組織間の調整、およびコンプライアンスを取り扱う。(ii) 正式に文書化された、システムおよび通信の保護方針の導入に関する手順。この手順は、システムおよび通信の保護方針の導入、ならびに関連する管理策の導入を容易にするために使用される。

補足ガイダンス：システムおよび通信の保護の方針と手順は、適用法、大統領令、指令、方針、規制、基準、およびガイダンスに準拠する。システムおよび通信の保護の方針は、組織の一般的な情報セキュリティ方針の一部とすることができる。システムおよび通信の保護の手順は、一般的なセキュリティプログラムの一部として作成することもできれば、必要に応じて特定の情報システムに特化した形で作成することもできる。セキュリティ方針および手順のガイダンスは、NIST SP 800-12 に記載されている。

管理強化策：なし。

SC-2 アプリケーションの分離

管理策：情報システムは、ユーザ機能（ユーザインターフェースサービスを含む）をシステムの管理機能から分離する。

補足ガイダンス：情報システムは、ユーザインターフェースサービス（たとえば、公共のウェブページ）を、情報の保存および管理サービス（たとえば、データベース管理）から物理的または論理的に分離する。ここで言う分離は、別のコンピュータの使用、別の CPU（中央処理装置）の使用、オペレーティングシステム上の異なるインスタンスの使用、別のネットワークアドレスの使用、または、これらの方法の組合せ、あるいは、その他の方法によっても実現することができる。

管理強化策：なし。

SC-4 残存情報

管理策：情報システムは、情報が、共有システムリソースを介して不正に（または意図しない行為によって）転送されることを防止する。

補足ガイダンス：組織は、情報システムの残存物（データレムナンス(data remnance)とも呼ばれる）を管理することにより、特定のユーザ／ロール（または、これらを代行するユーザ／ロール）によって作成された情報（または暗号化された情報）が、開放済みの共有リソースへのアクセスを取得した別のユーザによって、再利用されないようにすることができる。

管理強化策：なし。

SC-5 サービス妨害（DoS）からの保護

管理策：情報システムは、次にような種類のサービス妨害攻撃の影響からシステムを保護する、またはその影響を制限する。[指定：組織が定めるサービス妨害攻撃の種類のリスト、または現在のリストに対する参考資料]。

補足ガイダンス：サービス妨害攻撃の影響を制限する（場合によっては排除可能な）技法は、多様である。たとえば、境界保護機器を設置することで、特定のタイプのパケットをフィルタリングし、内部のネットワーク上の装置が、じかにサービス妨害攻撃の影響を受けないようにすることができる。公的にアクセス可能な情報システムは、拡張した容量と帯域幅を、サービスの冗長性と組み合わせることによって保護することができる。

管理強化策：なし。

SC-7 境界保護

管理策：情報システムは、システムの外部との境界、およびシステム内部の主要な境界における通信を監視し、制御する。

補足ガイダンス：インターネットまたはそのほかの外部ネットワーク／情報システムへのあらゆる接続は、管理されたインターフェースを介して行われる。このインターフェースは、効果的なアーキテクチャ（たとえば、ファイアウォールを保護するルータ、および非武装地帯（DMZ）と呼ばれる保護されたサブネットワーク上に存在する、アプリケーションゲートウェイなど）上に配備された、適切な境界保護機器（プロキシ、ゲートウェイ、ルータ、ファイアウォール、ガード、暗号化トンネル）によって、構成される。指定された代替処理拠点での情報システムの境界保護レベルは、一次拠点の場合と同じである。

組織は、多重防御策の一環として、より高位の影響の情報システムをいくつかの物理的なドメイン（環境）に分離し、組織のリスクアセスメントを行い、必要であれば上述のような管理されたインターフェースの概念を取り入れて、ネットワークへのアクセスを制限したり、禁止したりすることを検討する。FIPS199 のセキュリティ分類は、分離候補となるドメインの選択を支援する。

組織は、商用通信サービスの利用に関する管理策を導入するにあたって、それらのサービスに本来備わっている「共有」という性質を考慮しなければならない。商用通信サービスは通常、すべての法人顧客によって共有されるコンポーネントおよび統合管理システムをベースにしたものであり、第三者が提供するアクセスラインや他のサービス要素が含まれることもある。したがって、このように相互接続された環境における送受信サービスは、セキュリティに関する契約規定があるにもかかわらず、リスクを増幅させる要因となることもある。IPsec(インターネットプロトコルセキュリティ)ベースの VPN に関するガイダンスは、NIST SP 800-77 に記載されている。関連セキュリティ管理策：MP-4、RA-2。

管理強化策：

(1) 組織は、公的にアクセス可能な情報システムのコンポーネントを、分離された物理的ネットワークインターフェースを利用するサブネットワークに割り当てる。

管理強化策の補足ガイダンス： 公的にアクセス可能な情報システムのコンポーネントには、パブリックウェブサーバなどが含まれる。

(2) 組織は、組織内部のネットワークへの一般からのアクセスを、適切な仲介が行われない限り阻止する。

(3) 組織は、インバウンドおよびアウトバウンドのネットワークトラフィックを適切に監視するために、情報システムに対するアクセスポイントの数を制限する。

(4) 組織は、外部の通信サービスに対するインターフェースとして、管理されたインターフェース（効果的なセキュリティアーキテクチャ上の境界保護機器など）を利用し、送受信される情報の機密性や完全性を保護するための適切な管理策を導入する。

(5) 情報システムは、ネットワークトラフィックをデフォルトで拒否し、例外的に許可するようにする（例：“すべてを拒否”、“例外的に許可”など）。

SC-8 伝送する情報の完全性

管理策：情報システムは、送受信される情報の完全性を保護する。

補足ガイダンス：組織が、情報の送受信サービスを、組織専用のサービスではなく、一般のサービスプロバイダに依存している場合、送受信される情報の完全性を確保するためのセキュリティ管理策が、確実に導入される保証はない。必要なセキュリティ管理策やその管理策の有効性を保証するものが得られない状況においては、組織は、代替管理策を採用するか、あるいはより大きなリスクを受け入れるかを選択しなければならない。TLS（Transport Layer Security）を用いて情報を送受信する際の完全性を保護するためのガイダンスは、NIST SP 800-52 に記載されている。IPsec(インターネットプロトコルセキュリティ)ベースの VPN に関するガイダンスは、NIST SP 800-77 に記載されている。ドメインシネームシステム（DNS）メッセージの認証と完全性の確認のためのガイダンスは、NIST SP 800-81 に記載されている。保護されたディストリビューションシステム（Protective Distribution Systems:PDS）の使用に関するガイダンスは、NSTISSI No. 7003 に記載されている。

管理強化策：なし。

SC-9 伝送する情報の機密性

管理策：情報システムは、送受信される情報の機密性を保護する。

補足ガイダンス：組織が、情報の送受信サービスを、組織専用のサービスではなく、一般のサービスプロバイダに依存している場合、送受信される情報の完全性を確保するためのセキュリティ管理策が、確実に導入される保証はない。必要なセキュリティ管理策やその管理策の有効性を保証するものが得られない状況においては、組織は、代替管理策を採用するか、あるいはより大きなリスクを受け入れるかを選択しなければならない。TLS（Transport Layer Security）を用いて情報を送受信する際の機密性を保護するためのガイダンスは、NIST SP 800-52 に記載されている。IPsec（Security Architecture for Internet Protocol: IPsec）を用いて情報を送受信する際の完全性を保護するためのガイダンスは、NIST SP 800-77 に記載されている。保護されたディストリビューションシステム（Protective Distribution Systems: PDS）の使用に関するガイダンスは、NSTISSI No. 7003 に記載されている。関連セキュリティ管理策：AC-17。

管理強化策：なし。

SC-10 ネットワークの切断

管理策：情報システムは、セッションの終了時、またはセッションが［指定：組織が定める時間］の間アクティブでない場合、ネットワーク接続を終了する。

補足ガイダンス：組織は、本管理策を、リスク管理の一部として適用する。リスク管理では、ミッションまたは運用上の具体的な要件を考慮する。

管理強化策：なし。

SC-12 暗号鍵の確立と管理

管理策：情報システムにとって暗号化が必要であり、かつ実際に採用される場合、組織は、支援手順を備えた自動化メカニズムを使用する、または手動の手順を使用して、暗号鍵を作成し、管理する。

補足ガイダンス：暗号鍵の作成に関するガイダンスは、NIST SP 800-56 に記載されている。暗号鍵管理に関するガイダンスは、NIST SP 800-57 に記載されている。

管理強化策：なし。

SC-13 暗号化の利用

管理策：暗号化による保護が必要な情報システムでは、適用法、大統領令、指令、方針、規定、基準、およびガイダンスに準拠する暗号化メカニズムを、システムに導入する。

補足ガイダンス：国家安全保障にかかわるシステム以外のシステムに対して、暗号化を行う際の連邦基準は、FIPS140-2（修正版）である。NIST の暗号モジュール試験および認証制度(FIPS140-1、FIPS140-2、および今後の修正も含む)によって交付される証明書は、明示的に無効になるまでは、その有効性が維持される。また、証明書が有効であれば、モジュールの継続的な利用や購入が可能である。暗号鍵の作成に関するガイダンスは、NIST SP の 800-56 に、暗号鍵管理に関するガイダンスは、NIST SP の 800-57 に記載されている。有効な暗号化の利用に関する追加情報は、http://csrc.nist.gov/cryptval から入手することができる。

管理強化策：なし。

SC-14 パブリックアクセスからの保護

管理策：情報システムは、公的に入手可能な情報とアプリケーションの、完全性と可用性を保護する。

補足ガイダンス：なし。

管理強化策：なし。

SC-15 共同コンピューティング

管理策：情報システムは、共同コンピューティングメカニズムの遠隔活性化（リモートでアクティブにすること）を禁止する。また、ローカルユーザに対しては、利用法についての明示的な指示を提供する。

補足ガイダンス：共同コンピューティングのメカニズムには、ビデオや電話会議機能などがある。利用法についての明示的な指示には、カメラおよび／またはマイクが利用できる状態になっていることを、ローカルユーザに知らせることなどがある。

管理強化策：なし。

SC-17 公開鍵基盤の承認

管理策：組織は、適切な認証方針に基づき、公開鍵認証を交付する、または承認されたサービスプロバイダから、公開鍵認証を取得する。

補足ガイダンス：ユーザの認証では、それぞれの政府機関が、連邦ブリッジ認証局 FBCA（Federal Bridge Certification Authority）と相互認証型の、独自の認証機関(CA)を設置する（中間レベル、もしくは、より高いレベルの保証を前提）、あるいは、OMB の通達 05-24 に示されているように、認可された共通サービスプロバイダが発行する認証を使用する。公開鍵技術についてのガイダンスは、NIST SP 800-32 に記載されている。遠隔電子認証に関するガイダンスは、NIST SP 800-63 に記載されている。

管理強化策：なし。

SC-18 モバイルコード

管理策：組織は、(i) モバイルコード技術が悪意をもって使用された場合に、情報システムに損害がもたらされる可能性にもとづき、モバイルコードの使用制限を定め、適切な導入ガイダンスを策定する、また、(ii) 情報システムにおけるモバイルコードの利用を許可、監視し、管理する。

補足ガイダンス：モバイルコード技術には、Java、JavaScript、ActiveX、PDF、Postscript、Shockwave ムービー、Flash アニメーション、VBScript などがある。組織が定める使用制限および導入ガイダンスは、組織のサーバに導入されるモバイルコードの選択および使用、ならびに個々のワークステーションにダウンロードされ実行されるモバイルコードの選択および使用のいずれにも適用される。組織は、管理策手順を利用することで、情報システム内で容認されないモバイルコードの開発、調達、または導入を防止することができる。アクティブなコンテンツおよびモバイルコードに関するガイダンスは、NIST SP 800-28 に記載されている。

管理強化策：なし。

SC-19 ボイスオーバーインターネットプロトコル(VoIP)

管理策：組織は、(i) VoIP の技術が悪意をもって使用された場合に、情報システムに損害がもたらされる可能性にもとづき、VoIP の使用制限を定め、導入ガイダンスを策定する、(ii) 情報システムにおける VoIP の利用を許可、監視し、管理する。

補足ガイダンス：情報システムに VoIP 技術を導入する際の、セキュリティの検討事項に関するガイダンスは、NIST SP 800-58 に記載されている。

管理強化策：なし。

SC-20 セキュアネーム／アドレスレゾリューションサービス（信頼のおける情報資源）

管理策：ネーム／アドレスレゾリューションサービスを提供する情報システムは、レゾリューションクエリーへのレスポンスとして、信頼のおけるデータを返すとともに、データの発信元および完全性に関するアーチファクト(artifact)を提供する。

補足ガイダンス：本管理策を適用することで、リモートクライアントは、サービスを経由して入手するネーム／アドレスレゾリューション情報に対する、データ発信元認証や完全性の検証を行うことができる。ドメインネームサーバ（DNS）は、ネーム／アドレスレゾリューションサービスを提供する情報システムの一例であ

る。追加的なアーチファクト(artifact)の例としては、電子署名や暗号鍵があり、信頼のおけるデータの例としては、DNS のリソースレコードがある。セキュアなドメインネームシステムの配備についてのガイダンスは、NIST SP 800-81 に記載されている。

管理強化策：なし。

SC-22 ネーム／アドレスレゾリューションサービスの構成およびサービスの提供

管理策：集合的なネーム／アドレスレゾリューションサービスを組織に提供する情報システムは、フォルトトレラント（耐故障性）であり、役割の分割を実施する。

補足ガイダンス：ドメインネームシステムサーバ（DNS）は、ネーム／アドレスレゾリューションサービスを提供する情報システムの一例である。通常は、単一点障害を排除し冗長性を強化するために、少なくとも 2 つの信頼のおけるドメインネームシステムサーバを用意する。そのうちの 1 つは、プライマリサーバとして使用し、もう一方はセカンダリサーバとして使用する。さらに、これらの 2 つのサーバは、通常、異なるサブネット上に存在し、地理的にも離れた場所に置かれる（物理的に同じ施設の中には設置されない）。組織の IT リソースが、内部ネットワークに属するものと、外部ネットワークに属するものに分かれている場合、それぞれの役割（内部用および外部用）を担う 2 つのドメインネームシステムサーバが設置される。外部の役割を担うドメインネームシステムサーバが、外部 IT リソース関連のネーム／アドレスレゾリューションの情報を提供するのに対し、内部の役割を担うドメインネームシステムサーバは、内部および外部の IT リソース関連のネーム／アドレスレゾリューションの情報を提供する。組織は、特定の役割を担うドメインネームシステムサーバにアクセス可能なクライアントのリストを作成する。セキュアな DNS の配備についてのガイダンスは、NIST SP 800-81 に記載されている。

管理強化策：なし。

SC-23 セッションの真正性

管理策：情報システムは、通信セッションの真正性を保護するメカニズムを提供する。

補足ガイダンス：本管理策は、パケットレベルでの通信の保護とは対象的に、セッションレベルでの通信の保護に特化したものである。この管理策の目的は、必要な場合（たとえば、ウェブベースのサービスを提供するシステムの、サービス指向型アーキテクチャおいて）に、セッションレベルの保護を実施することである。TLS メカニズムの利用についてのガイダンスは、NIST SP 800-52 に記載されている。IPsec(インターネットプロトコルセキュリティ)ベースの VPN に関するガイダンスは、NIST SP 800-77 に記載されている。セキュアなウェブサービスについてのガイダンスは、NIST SP 800-95 に記載されている。

管理強化策：なし。

ファミリ: システムおよび情報の完全性 **クラス:** 運用

SI-1 システムおよび情報の完全性に対する方針と手順

管理策：組織は、以下のものを策定および周知徹底し、定期的にレビュー／更新する。(i) 正式に文書化された、システムおよび情報の完全性に対する方針。これらの方針では、目的、適用範囲、役割、責任、経営陣のコミットメント、組織間の調整、およびコンプライアンスを取り扱う。(ii) 正式に文書化された、システムおよび情報の完全性に対する方針の導入に関する手順。この手順は、システムおよび情報の完全性に対する方針の導入、ならびに関連する管理策の導入を容易にするために使用される。

補足ガイダンス：システムおよび情報の完全性に対する方針と手順は、適用法、大統領令、指令、方針、規制、基準、およびガイダンスに準拠する。システムおよび情報の完全性に対する方針は、組織の一般的な情報セキュリティ方針の一部とすることができる。システムおよび情報の完全性に関する手順は、一般的なセキュリティプログラムの一部として作成することもできれば、必要に応じて特定の情報システムに特化した形で作成することもできる。セキュリティ方針および手順のガイダンスは、NIST SP 800-12 に記載されている。

管理強化策：なし。

SI-2 欠陥の修正

管理策：組織は、情報システムの欠陥を特定し、それらの欠陥を報告するとともに修正する。

補足ガイダンス：組織は、情報システム内のソフトウェアの中で、新たに公表された欠陥（および、この欠陥が原因となる潜在的な脆弱性）の影響を受けるものを特定する。組織（または、ソフトウェアがベンダー／請負業者によって開発、保守されている場合は、ソフトウェア開発者／ベンダー）は、新たにリリースされたセキュリティ関連のパッチ、サービスパック、およびホットフィックスを直ちに入手し、それらが組織の情報システムにもたらす有効性と潜在的悪影響をテストした後、情報システムに導入する。また、セキュリティの評価中や継続的な監視中、インシデントへの対応活動の実施中や情報システムのエラーハンドリング中に発見された欠陥についても、迅速に対処する。欠陥の修正は、緊急な変更として、「設定管理」プロセスに統合される。セキュリティパッチの導入、およびその管理に関するガイダンスは、NIST SP 800-40 に記載されている。関連セキュリティ管理策：CA-2、CA-4、CA-7、CM-3、IR-4、SI-11。

管理強化策：

(2) 組織は、情報システムのコンポーネントの欠陥の修正状態を、定期的にかつ要求に応じて特定するための、自動化メカニズムを採用する。

SI-3 悪意のコード(不正プログラム)からの保護

管理策：情報システムは、悪意のコードから、情報システムを保護する。

補足ガイダンス：組織は、重要な情報システムへの入口点および出口点（たとえば、ファイアウォール、電子メールサーバ、ウェブサーバ、プロキシサーバ、リモートアクセスサーバなど）において、システムを悪意のコードから保護するためのメカニズムを採用する。また、ネットワーク上のワークステーション、サーバ、またはモバイルコンピューティング機器に対しても、同メカニズムを採用する。組織は、(i) 電子メール、電子メールへの添付ファイル、インターネットアクセス、取り外し可能な記録媒体（USB デバイス、ディスケットやコンパクトディスクなど）、そのほかの一般的な手段、または(ii) 情報システムの脆弱性、などを介して送り込まれた悪意のコード（ウイルス、ワーム、トロイの木馬、スパイウェアなどの不正プログラム）を検知して根絶するために、不正プログラム対策メカニズムを利用する。組織は、組織の設定管理の方針と手順に従い、新しいリリースが入手可能な場合はすぐに入手し、保護メカニズム（最新のウイルス定義を含む）を更新する。組織は、複数ベンダー（たとえば、境界デバイスおよびサーバを提供する、あるベンダーと、ワークステーションを提供する別のベンダーなど）が提供する、不正プログラム対策ソフトの利用を検討する。組織は、悪意のコードの検知や根絶のプロセスにおけるフォルスポジティブ（false positives：正常な通信なのに不正と判断する誤検知）を容認するか否か、また、フォルスポジティブがもたらす情報システムの可用性への潜在的影響を受け入れるか否かについても、検討する。悪意のコード対策の実施についてのガイダンスは、NIST SP 800-83 に記載されている。

管理強化策：

(1) 組織は、不正プログラム対策メカニズムを、一元的に管理する。

(2) 情報システムは、それらのメカニズムを自動的に更新する。

SI-4 情報システムの監視ツールおよび監視技法

管理策：組織は、情報システム上のイベントの監視、攻撃の検知、およびシステムの不正使用の特定を行うための、ツールおよび技法を採用する。

補足ガイダンス：情報システムの監視機能は、さまざまなツールや技術（たとえば、侵入検知システム、侵入防止システム、不正プログラム対策ソフト、監査記録監視ソフト、ネットワーク監視ソフトなど）を用いて実現できる。監視デバイスは、必要不可欠な情報収集を目的として、情報システムに戦略的に配備される（たとえば、選択された周辺の区域、重要なアプリケーションを支援するサーバーファームの近辺など）。監視機能は、特定の処理を追跡するために、システム内の臨時の場所にも配備する。さらに、監視デバイスは、情報システムへのセキュリティの変更による影響を追跡するためにも使用される。収集する情報の詳細レベルについては、組織の監視目的、および監視活動を支援する情報システムの性能に基づくものとする。組織は、情報システムのすべての監視活動について、適切な弁護士の助言を得るべきである。組織は、法執行機関や諜報機関からの通知、またはこれ以外の信頼できる筋からの情報に基づき、組織の業務や資産、または個人に対するリスクが上昇する兆しが見える場合には、随時、情報システムの監査記録の監視活動を強化する。さまざまなセキュリティ技術を駆使して情報システムへの攻撃を検知するためのガイダンスは、NIST SP 800-61 に記載されている。不正プログラム対策ソフトを使ってマルウェア（悪意のコード）の攻撃を検知するためのガイダンスは、NIST SP 800-83 に記載されている。コンピュータセキュリティのイベントログの監視と分析に関するガイダンスは、NIST SP 800-92 に記載されている。侵入の検知と防止に関するのガイダンスは、NIST SP 800-94 に記載されている。関連セキュリティ管理策：AC-8。

管理強化策：

(4) 情報システムは、インバウンドおよびアウトバウンドの通信を監視し、異常な活動または不正な活動がないかを確認する。

管理強化策の補足ガイダンス：異常な／不正な活動には、悪意のコードの存在、情報の不正なエクスポート、または外部の情報システムに対する信号の送信などがある。

SI-5 セキュリティ警報と勧告

管理策：組織は、情報システムのセキュリティ警報／勧告を定期的に入手し、適切な要員に伝えるとともに、適切な対応活動を実施する。

補足ガイダンス：組織は、セキュリティ警報／勧告に対して取るべき活動を文書化する。組織は、特別利益団体（情報セキュリティフォーラムなど）との連絡を取り合うことで、次のようなことを実現する。(i) セキュリティに関する情報（脅威、脆弱性および最新のセキュリティ技術に関する情報）の共有を促進する、(ii) セキュリティの専門家が提供するアドバイスへのアクセスを提供する、(iii) セキュリティの最良実施例の知識を向上させる。セキュリティ警報／勧告の監視および配布に関するのガイダンスは、NIST SP 80-40 に記載されている。

管理強化策：なし。

SI-8 スパムからの保護

管理策：情報システムは、スパム対策を導入する。

補足ガイダンス：組織は、重要な情報システムへの入口点（たとえば、ファイアウォール、電子メールサーバ、リモートアクセスサーバ）において、システムをスパムから保護するためのメカニズムを採用する。また、ネットワーク上のワークステーション、サーバ、またはモバイルコンピューティング機器に対しても、同メカニズムを採用する。組織は、電子メール、電子メールへの添付ファイル、インターネットアクセス、またはそのほかの一般的な手段により送り込まれる非請求メッセージを検知し、適切な活動を行うための、スパム対策メカニズムを使用する。組織は、複数ベンダー（たとえば、境界デバイスおよび境界サーバを提供する、あるベンダーと、ワークステーションを提供する別のベンダーなど）が提供する、スパム対策ソフトの利用を検討する。電子メールの安全性に関するガイダンスは、NIST SP 800-45 に記載されている。

管理強化策：なし。

SI-9 情報入力の制限

管理策：組織は、情報システムへの情報入力を、承認された者のみに制限する。

補足ガイダンス：情報システムへの情報入力を承認された者に対する種々の制限は、システムが通常実施するアクセス制御の範囲を超えることがある。また、これらの制限には、特定の運用上の責任／プロジェクトの責任に基づく制限が含まれる場合もある。

管理強化策：なし。

SI-10 情報の正確さ、完全性、有効性および真正性

管理策：情報システムは、情報の正確さ、完全性、有効性および真正性を確認する。

補足ガイダンス：情報の正確さ、完全性、有効性および真正性の確認は、可能な限り情報が入力された時点で行うべきである。組織は、情報システムに入力された情報が、指定された書式および内容に適合しているか否かを確認するために、その情報の構文（Syntax）をチェックする規則を設けて、チェックを実施する。インタプリタに送られる入力は、事前に選別して、入力内容が意図しない形でコマンドとして解釈されないようにする。情報システムが、入力情報の正確さ、完全性、有効性および真正性をどの程度まで確認することができるかは、組織の方針および運用要件に基づくものとする。

管理強化策：なし。

SI-11 エラー処理

管理策：情報システムは、エラーの状態を迅速に特定し処置を行うことで、敵（攻撃者）が利用できるような情報を提供しないようにする。

補足ガイダンス：組織は、エラーメッセージの構成と内容を慎重に検討する。エラーメッセージは、承認されたユーザ以外には通知しない。情報システムが生成するエラーメッセージは、エラーに関するタイムリーかつ有効な情報を、ユーザに提供するためのものであり、有害となりうる情報（たとえば、攻撃者が利用できるような情報）であってはならない。取扱いに慎重を要する情報（口座番号、社会保障番号、クレジットカード番号など）は、エラーログまたは関連する管理者用メッセージには表示しない。情報システムが、エラーの状態をどの程度まで特定し、処置を行えるかは、組織の方針および運用要件に基づくものとする。

管理強化策：なし。

SI-12 情報システムからの出力の取扱いと保存

管理策：組織は、適用法、大統領令、指令、方針、規制、基準および運用の要件に従って、情報システムからの出力を処理し、保存する。

補足ガイダンス：なし。

管理強化策：なし。

パート II

必要最低限の保証要件

中位影響レベルの情報システム

以下に、管理策カタログ内の管理策に対する最低保証要件を示す。ここでいう保証要件は、管理策の開発者および導入者[2]が、管理策が正しく導入され、意図したとおりに運用され、システムのセキュリティ要求事項に対する適合性の観点から望まれる結果を産出しているといった根拠を増やすために、定義し実施する活動に対するものである。保証要件は管理策ごとに適用される。保証要件の後には、要件をどのように適用するかの詳細と補足を、セキュリティ管理策と同様の書式で記載している。

保証要件: セキュリティ管理策が有効であることが確認できること、また、管理策ステートメントで明示的に定義されている機能要件を満たしていること。管理策の開発者／導入者は、管理策の分析およびテストを可能にするために、その機能特性を詳細に記述する。また、管理策の開発者／導入者は、課された責任と具体的な活動を、管理策に確実に盛り込まなければならない。これらの活動により、管理策が導入された場合に、要求されている機能および目的を果たすことができるといった信頼を向上させることができる。これらの活動には、前述の判定を容易にするための、構造と内容を持つ記録の作成などがある。

補足ガイダンス: 中位影響のベースラインに属するセキュリティ管理策は、管理策が正しく導入、運用されていることへの信頼の度合いが増えていることに重きを置く。このケースでは、欠陥が見つかる可能性は低いが（たとえ見つかっても迅速に対処される）、それでも管理策の開発者または導入者は、管理策がその機能や目的を果たしているという根拠を増やすために、特定の機能、手順および文章を管理策に盛り込む。この文書は、管理策の機能特性を分析、テストする評価者にも必要なものである。

2 ここでいう開発者／導入者は、情報システムのセキュリティ管理策の開発または導入に対して責任を負う、個人または個人のグループである。これらの個人または個人のグループには、管理策を提供するハードウェアやソフトウェアのベンダー、管理策を実施する契約者、組織内の情報システムのセキュリティの責任者（情報システムのオーナー、情報システムセキュリティ責任者、システムとネットワークの管理者、またはこれ以外の情報システムセキュリティ責任者など）が含まれることがある。