参考資料　クラウドサービスが遵守すべき ISMAP 管理策基準
（統制目標、末尾にＢが付された詳細管理策）

No	ISMAP管理策番号	クラウドサービスが遵守すべきISMAP管理策
1	5.1.1	情報セキュリティのための方針群は、これを定義し、管理層が承認し、発行し、従業員及び関連する外部関係者に通知する。 (脚注）管理層には、経営陣及び管理者が含まれる。ただし、実務管理者（administrator）は除かれる。
2	5.1.2	情報セキュリティのための方針群は、あらかじめ定めた間隔で、又は重大な変化が発生した場合に、それが引き続き適切、妥当かつ有効であることを確実にするためにレビューする。
3	6.1.1	全ての情報セキュリティの責任を定め、割り当てる。
4	6.1.1.13.PB	クラウドサービス事業者は、クラウドサービス利用者、クラウドサービス事業者及び供給者と、情報セキュリティの役割及び責任の適切な割当てについて合意し、文書化する。
5	6.1.2	相反する職務及び責任範囲は、組織の資産に対する、認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために、分離する。
6	6.1.3	関係当局との適切な連絡体制を維持する。
7	6.1.3.3.PB	クラウドサービス事業者は、クラウドサービス利用者に、クラウドサービス事業者の組織の地理的所在地、及びクラウドサービス事業者がクラウドサービス利用者のデータを保管する可能性のある国々及びその法管轄を通知する。
8	6.1.4	情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持する。
9	6.1.5	プロジェクトの種類にかかわらず、プロジェクトマネジメントにおいては、情報セキュリティに取り組む。
10	6.2.1	モバイル機器を用いることによって生じるリスクを管理するために、方針及びその方針を支援するセキュリティ対策を採用する。
11	6.2.2	テレワーキングの場所でアクセス、処理及び保存される情報を保護するために、方針及びその方針を支援するセキュリティ対策を実施する。
12	6.3.1.P	クラウドサービス利用者及びクラウドサービス事業者の両者は、クラウドサービスの利用における情報セキュリティの共同責任について、文書化し、公表し、伝達し、実装する。
13	6.3.1.1.PB	クラウドサービス事業者は、クラウドサービス利用の一環としてクラウドサービス利用者が実施及び管理を必要とする情報セキュリティの役割と責任に加え、クラウドサービスの利用に対する、クラウドサービス事業者の情報セキュリティ管理策及び責任を文書化し、通知する。
14	7.1.1	全ての従業員候補者についての経歴などの確認は、関連する法令、規制及び倫理に従って行う。また、この確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行う。
15	7.1.2	従業員及び契約相手との雇用契約書には、情報セキュリティに関する各自の責任及び組織の責任を記載する。
16	7.2.1	経営陣は、組織の確立された方針及び手順に従った情報セキュリティの適用を、全ての従業員及び契約相手に要求する。
17	7.2.2	組織の全ての従業員、及び関係する場合には契約相手は、職務に関連する組織の方針及び手順についての、適切な、意識向上のための教育及び訓練を受け、また、定めに従ってその更新を受ける。
18	7.2.2.19.PB	クラウドサービス事業者は、クラウドサービス利用者のデータ及びクラウドサービスの派生データの適切な取扱いに関して、従業員に意識向上のための教育及び訓練を提供し、かつ同じことをするよう契約相手に要請する。
19	7.2.3	情報セキュリティ違反を犯した従業員に対して処置をとるための、正式かつ周知された懲戒手続を備える。
20	7.3.1	雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め、その従業員又は契約相手に伝達し、かつ、遂行させる。
21	8.1.1	情報、情報に関連するその他の資産及び情報処理施設を特定する。また、これらの資産の目録を、作成し、維持する。
22	8.1.1.6.PB	クラウドサービス事業者の資産目録は、クラウドサービス利用者のデータ及びクラウドサービスの派生データを明確に特定する。
23	8.1.2	目録の中で維持される資産は、管理する。
24	8.1.2.7.PB	クラウドサービス事業者は、クラウドサービス利用者に対し、当該利用者の資産（バックアップを含む）を管理するため、次のいずれかを提供する。 (a)当該利用者の管理する資産を、記録媒体に記録する（バックアップを含む）前に暗号化し、当該利用者が暗号鍵を管理し消去する機能 (b) 当該利用者が、当該利用者の管理する資産を記録媒体に記録する（バックアップを含む）前に暗号化し、暗号鍵を管理し消去する機能を実装するために必要となる情報
25	8.1.3	情報の利用の許容範囲、並びに情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は、明確にし、文書化し、実施する。
26	8.1.4	全ての従業員及び外部の利用者は、雇用、契約又は合意の終了時に、自らが所持する組織の資産の全てを返却する。
27	8.1.5.P	クラウドサービス事業者の領域上にあるクラウドサービス利用者の資産は、クラウドサービス利用の合意の終了時に、時機を失せずに返却または除去する。
28	8.2.1	情報は、法的要求事項、価値、重要性、及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から、分類する。
29	8.2.2	情報のラベル付けに関する適切な一連の手順は、組織が採用した情報分類体系に従って策定し、実施する。
30	8.2.2.7.PB	クラウドサービス事業者は、クラウドサービス利用者が扱う情報及び関連資産を当該利用者が分類し、ラベル付けするためのサービス機能について文書化し、開示する。
31	8.2.3	資産の取扱いに関する手順は、組織が採用した情報分類体系に従って策定し、実施する。
32	8.3.1	組織が採用した分類体系に従って、取外し可能な媒体の管理のための手順を実施する。
33	8.3.2	媒体が不要になった場合は、正式な手順を用いて、セキュリティを保って処分する。
34	8.3.3	情報を格納した媒体は、輸送の途中における、認可されていないアクセス、不正使用又は破損から保護する。
35	9.1.1	アクセス制御方針は、業務及び情報セキュリティの要求事項に基づいて確立し、文書化し、レビューする。
36	9.1.2	利用することを特別に認可したネットワーク及びネットワークサービスへのアクセスだけを、利用者に提供する。
37	9.2.1	アクセス権の割当てを可能にするために、利用者の登録及び登録削除についての正式なプロセスを実施する。
38	9.2.1.6.PB	クラウドサービスのユーザによるクラウドサービスへのアクセスをクラウドサービス利用者が管理するため、クラウドサービス事業者は、クラウドサービス利用者に、ユーザの登録及び登録削除の機能及び仕様を提供する。
39	9.2.2	全ての種類の利用者について、全てのシステム及びサービスへのアクセス権を割り当てる又は無効化するために、利用者アクセスの提供についての正式なプロセスを実施する。
40	9.2.2.8.PB	クラウドサービス事業者は、クラウドサービスのユーザのアクセス権を管理する機能及び仕様を提供する。
41	9.2.3	特権的アクセス権の割当て及び利用は、制限し、管理する。
42	9.2.3.11.PB	クラウドサービス事業者は、特定したリスクに応じて、クラウドサービスの管理能力にあわせたクラウドサービス利用者の管理者認証に、十分に強固な認証技術を提供する。
43	9.2.4	秘密認証情報の割当ては、正式な管理プロセスによって管理する。
44	9.2.4.9.PB	クラウドサービス事業者は、秘密認証情報を割り当てる手順、及びユーザ認証手順を含む、クラウドサービス利用者の秘密認証情報の管理手順について、情報を提供する。
45	9.2.5	資産の管理責任者は、利用者のアクセス権を定められた間隔でレビューする。
46	9.2.6	全ての従業員及び外部の利用者の情報及び情報処理施設に対するアクセス権は、雇用、契約又は合意の終了時に削除し、また、変更に合わせて修正する。
47	9.3.1	秘密認証情報の利用時に、組織の慣行に従うことを、利用者に要求する。
48	9.4.1	情報及びアプリケーションシステム機能へのアクセスは、アクセス制御方針に従って、制限する。
49	9.4.1.8.PB	クラウドサービス事業者は、クラウドサービスへのアクセス、クラウドサービス機能へのアクセス、及びサービスにて保持されるクラウドサービス利用者のデータへのアクセスを、クラウドサービス利用者が制限できるよう、アクセス制御を提供する。
50	9.4.2	アクセス制御方針で求められている場合には、システム及びアプリケーションへのアクセスは、セキュリティに配慮したログオン手順によって制御する。
51	9.4.2.2.B	強い認証及び識別情報の検証が必要な場合には、パスワードに代えて、暗号による手段、スマートカード、トークン、生体認証などの認証方法を用いる。

No	ISMAP管理策番号	クラウドサービスが遵守すべきISMAP管理策
52	9.4.3	パスワード管理システムは、対話式とすること、また、良質なパスワードを確実にするものとする。
53	9.4.4	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理する。
54	9.4.5	プログラムソースコードへのアクセスは、制限する。
55	9.5.P	共有化された仮想環境におけるクラウドサービス利用者のデータのアクセス制御
56	9.5.2.P	クラウドコンピューティング環境における仮想マシンは、事業上のニーズを満たすため、要塞化する。
57	9.5.2.1.PB	クラウドサービス事業者は、仮想マシンを設定する際には、適切に要塞化し(例えば、クラウドサービスを実行するのに必要なポート、プロトコル及びサービスのみを有効とする）、利用する各仮想マシンに適切な技術的管理策(例えば、マルウェア対策、ログ取得）を実施する。
58	10.1.1	情報を保護するための暗号による管理策の利用に関する方針は、策定し、実施する。
59	10.1.1.9.PB	クラウドサービス事業者は、クラウドサービス利用者に、当該利用者が処理する情報を保護するために暗号技術を利用する機能を提供し、または、暗号技術を利用する環境についての情報を提供する。
60	10.1.2	暗号鍵の利用、保護及び有効期間（lifetime）に関する方針を策定し、そのライフサイクル全体にわたって実施する。
61	10.1.2.20.PB	クラウドサービス事業者は、クラウドサービス利用者に、当該利用者の管理する情報の暗号化に用いる暗号鍵を当該利用者が管理する機能を提供し、または、当該利用者が暗号鍵を管理する方法についての情報を提供する。
62	11.1.1	取扱いに慎重を要する又は重要な情報及び情報処理施設のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いる。
63	11.1.2	セキュリティを保つべき領域は、認可された者だけにアクセスを許すことを確実にするために、適切な入退管理策によって保護する。
64	11.1.3	オフィス、部屋及び施設に対する物理的セキュリティを設計し、適用する。
65	11.1.4	自然災害、悪意のある攻撃又は事故に対する物理的な保護を設計し、適用する。
66	11.1.5	セキュリティを保つべき領域での作業に関する手順を設計し、適用する。
67	11.1.6	荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所は、管理する。また、認可されていないアクセスを避けるために、それらの場所を情報処理施設から離す。
68	11.2.1	装置は、環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置し、保護する。
69	11.2.2	装置は、サポートユーティリティの不具合による、停電、その他の故障から保護する。
70	11.2.3	データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護する。
71	11.2.4	装置は、可用性及び完全性を継続的に維持することを確実にするために、正しく保守する。
72	11.2.5	装置、情報又はソフトウェアは、事前の認可なしでは、構外に持ち出さない。
73	11.2.6	構外にある資産に対しては、構外での作業に伴った、構内での作業とは異なるリスクを考慮に入れて、セキュリティを適用する。
74	11.2.7	記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又はセキュリティを保って上書きしていることを確実にするために、検証する。
75	11.2.7.4.PB	クラウドサービス事業者は、資源（例えば、装置、データストレージ、ファイル、メモリ）のセキュリティを保った処分又は再利用の取り決めを、時期を失せずに行うことを確実にする仕組みを整備する。
76	11.2.8	利用者は、無人状態にある装置が適切な保護対策を備えていることを確実にする仕組みを整備する。
77	11.2.9	書類及び取外し可能な記憶媒体に対するクリアデスク方針、並びに情報処理設備に対するクリアスクリーン方針を適用する。 （脚注）クリアデスクとは、机上に書類を放置しないことをいう。また、クリアスクリーンとは、情報をスクリーンに残したまま離席しないことをいう。
78	12.1.1	操作手順は、文書化し、必要とする全ての利用者に対して利用可能とする。
79	12.1.2	情報セキュリティに影響を与える、組織、業務プロセス、情報処理設備及びシステムの変更は、管理する。
80	12.1.2.11.PB	クラウドサービス事業者は、クラウドサービス利用者の情報セキュリティに悪影響を及ぼす可能性のあるクラウドサービスの変更に関する情報を、クラウドサービス利用者に提供する。
81	12.1.3	要求された主要なシステム資源の使用を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要とする容量・能力を予測する。
82	12.1.3.9.PB	クラウドサービス事業者は、資源不足による情報セキュリティインシデントを防ぐため、全資源の容量を監視する。
83	12.1.4	開発環境、試験環境及び運用環境は、運用環境への認可されていないアクセス又は変更によるリスクを低減するために、分離する。
84	12.1.5.P	クラウドコンピューティング環境の、管理のための操作手順を定義し、文書化し、監視する。
85	12.1.5.1.PB	クラウドサービス事業者は、重要な操作及び手順に関する文書を、それを求めるクラウドサービス利用者に提供する。
86	12.2.1	マルウェアから保護するために、利用者に適切に認識させることと併せて、検出、予防及び回復のための管理策を実施する。
87	12.3.1	情報、ソフトウェア及びシステムイメージのバックアップは、合意されたバックアップ方針に従って定期的に取得し、検査する。
88	12.4.1	利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、保持し、定期的にレビューする。
89	12.4.1.15.PB	クラウドサービス事業者は、クラウドサービス利用者に、ログ取得機能を提供する。
90	12.4.2	ログ機能及びログ情報は、改ざん及び認可されていないアクセスから保護する。
91	12.4.3	システムの実務管理者及び運用担当者の作業は、記録し、そのログを保護し、定期的にレビューする。
92	12.4.4	組織又はセキュリティ領域内の関連する全ての情報処理システムのクロックは、単一の参照時刻源と同期させる。
93	12.4.4.4.PB	クラウドサービス事業者は、クラウドサービス利用者に、クラウドサービス事業者のシステムで利用するクロックに関する情報及びクラウドサービス利用者がクラウドサービスのクロックにローカルクロックを同期させる方法についての情報を提供する。
94	12.4.5.P	クラウドサービス利用者は、利用するクラウドサービスの操作を監視する機能を有する。
95	12.5.1	運用システムに関わるソフトウェアの導入を管理するための手順を実施する。
96	12.6.1	利用中の情報システムの技術的ぜい弱性に関する情報は、時機を失せずに獲得する。また、そのようなぜい弱性に組織がさらされている状況を評価する。さらに、それらと関連するリスクに対処するために、適切な手段をとる。
97	12.6.1.18.PB	クラウドサービス事業者は、提供するクラウドサービスに影響を及ぼす可能性のある技術的ぜい弱性の管理についての情報を、クラウドサービス利用者が利用可能となるようにする。
98	12.6.2	利用者によるソフトウェアのインストールを管理する規則を確立し、実施する。
99	12.7.1	運用システムの検証を伴う監査要求事項及び監査活動は、業務プロセスの中断を最小限に抑えるために、慎重に計画し、合意する。
100	13.1.1	システム及びアプリケーション内の情報を保護するために、ネットワークを管理し、制御する。
101	13.1.2	組織が自ら提供するか外部委託しているかを問わず、全てのネットワークサービスについて、セキュリティ機能、サービスレベル及び管理上の要求事項を特定し、また、ネットワークサービス合意書にもこれらを盛り込む。
102	13.1.3	情報サービス、利用者及び情報システムは、ネットワーク上で、グループごとに分離する。
103	13.1.4.P	仮想ネットワークを設定する際には、クラウドサービス事業者のネットワークセキュリティ方針に基づき、仮想ネットワークと物理ネットワークの設定の整合性を検証する。

No	ISMAP管理策番号	クラウドサービスが遵守すべきISMAP管理策
104	13.2.1	あらゆる形式の通信設備を利用した情報転送を保護するために、正式な転送方針、手順及び管理策を備える。
105	13.2.2	合意では、組織と外部関係者との間の業務情報のセキュリティを保った転送について、取り扱う。
106	13.2.3	電子的メッセージ通信に含まれた情報は、適切に保護する。
107	13.2.4	情報保護に対する組織の要件を反映する秘密保持契約又は守秘義務契約のための要求事項は、特定し、定めに従ってレビューし、文書化する。
108	14.1.1	情報セキュリティに関連する要求事項は、新しい情報システム又は既存の情報システムの改善に関する要求事項に含める。
109	14.1.2	公衆ネットワークを経由するアプリケーションサービスに含まれる情報は、不正行為、契約紛争、並びに認可されていない開示及び変更から保護する。
110	14.1.3	アプリケーションサービスのトランザクションに含まれる情報は、次の事項を未然に防止するために、保護する。 ・不完全な通信 ・誤った通信経路設定
111	14.2.1	ソフトウェア及びシステムの開発のための規則は、組織内において確立し、開発に対して適用する。
112	14.2.1.13.PB	クラウドサービス事業者は、開示方針に反しない範囲で、セキュリティを保つための開発手順及び慣行についての情報を提供する。
113	14.2.2	開発のライフサイクルにおけるシステムの変更は、正式な変更管理手順を用いて管理する。
114	14.2.3	オペレーティングプラットフォームを変更するときは、組織の運用又はセキュリティに悪影響がないことを確実にするために、重要なアプリケーションをレビューし、試験する。
115	14.2.4	パッケージソフトウェアの変更は、抑止し、必要な変更だけに限る。また、全ての変更は、厳重に管理する。
116	14.2.5	セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの実装に対して適用する。
117	14.2.6	組織は、全てのシステム開発ライフサイクルを含む、システムの開発及び統合の取組みのためのセキュリティに配慮した開発環境を確立し、適切に保護する。
118	14.2.7	組織は、外部委託したシステム開発活動を監督し、監視する。
119	14.2.8	セキュリティ機能（functionality）の試験は、開発期間中に実施する。
120	14.2.9	新しい情報システム、及びその改訂版・更新版のために、受入れ試験のプログラム及び関連する基準を確立する。
121	14.3.1	試験データは、注意深く選定し、保護し、管理する。
122	15.1.1	組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について、供給者と合意し、文書化する。
123	15.1.1.14.B	組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、情報、情報処理施設及び移動が必要なその他のものの移行の管理、並びにその移行期間全体にわたって情報セキュリティが維持されることの確実化を含める。
124	15.1.1.16.B	当該事業者が提供するサービス上で取り扱われる情報に対して国内法以外の法令が適用された結果、クラウドサービス利用者の意図しないまま当該利用者の管理する情報にアクセスされ、又は処理されるリスクを評価して外部委託先を選定し、必要に応じて委託業務の実施場所及び契約に定める準拠法・裁判管轄を指定する。
125	15.1.2	関連する全ての情報セキュリティ要求事項を確立し、組織の情報に対して、アクセス、処理、保存若しくは通信を行う、又は組織の情報のためのIT 基盤を提供する可能性のあるそれぞれの供給者と、この要求事項について合意する。
126	15.1.2.18.PB	クラウドサービス事業者は、クラウドサービス事業者とクラウドサービス利用者の間に誤解が生じないように、クラウドサービス事業者が実行する適切な情報セキュリティ対策を、合意の一環として定める。
127	15.1.3	供給者との合意には、情報通信技術（以下「ICT」という。）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含める。
128	15.2.1	組織は、供給者のサービス提供を定常的に監視し、レビューし、監査する。
129	15.2.2	関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、供給者によるサービス提供の変更（現行の情報セキュリティの方針群、手順及び管理策の保守及び改善を含む）を管理する。
130	16.1.1	情報セキュリティインシデントに対する迅速、効果的かつ順序だった対応を確実にするために、管理層の責任及び手順を確立する。
131	16.1.2	情報セキュリティ事象は、適切な管理者への連絡経路を通して、できるだけ速やかに報告する。
132	16.1.3	組織の情報システム及びサービスを利用する従業員及び契約相手に、システム又はサービスの中で発見した又は疑いをもった情報セキュリティ弱点は、どのようなものでも記録し、報告するように要求する。
133	16.1.4	情報セキュリティ事象は、これを評価し、情報セキュリティインシデントに分類するか否かを決定する。
134	16.1.5	情報セキュリティインシデントは、文書化した手順に従って対応する。
135	16.1.6	情報セキュリティインシデントの分析及び解決から得られた知識は、インシデントが将来起こる可能性又はその影響を低減するために用いる。
136	16.1.7	組織は、証拠となり得る情報の特定、収集、取得及び保存のための手順を定め、適用する。
137	16.1.7.13.PB	クラウドサービス事業者は、クラウドサービス利用者と、クラウドコンピューティング環境内の潜在的なディジタル形式の証拠、又はその他の情報の要求に対応する手順を合意する。
138	17.1.1	組織は、困難な状況（adverse situation）（例えば、危機又は災害）における、情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定する。
139	17.1.2	組織は、困難な状況の下で情報セキュリティ継続に対する要求レベルを確実にするための、プロセス、手順及び管理策を確立し、文書化し、実施し、維持する。
140	17.1.3	確立及び実施した情報セキュリティ継続のための管理策が、困難な状況の下で妥当かつ有効であることを確実にするために、組織は、定められた間隔でこれらの管理策を検証する。
141	17.2.1	情報処理施設は、可用性の要求事項を満たすのに十分な冗長性をもって、導入する。
142	18.1.1	各情報システム及び組織について、全ての関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを、明確に特定し、文書化し、また、最新に保つ。
143	18.1.2	知的財産権及び権利関係のあるソフトウェア製品の利用に関連する、法令、規制及び契約上の要求事項の順守を確実にするための適切な手順を実施する。
144	18.1.2.13.PB	クラウドサービス事業者は、知的財産権の順守に対応するためのプロセスを確立する。
145	18.1.3	記録は、法令、規制、契約及び事業上の要求事項に従って、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護する。
146	18.1.3.13.PB	クラウドサービス事業者は、クラウドサービス利用者に、クラウドサービスの利用に関して、クラウドサービス事業者が収集し、蓄積する記録の保護について、情報を提供する。
147	18.1.4	プライバシー及び個人識別情報（PII） の保護は、関連する法令及び規制が適用される場合には、その要求に従って確実に行う。
148	18.1.5	暗号化機能は、関連する全ての協定、法令及び規制を順守して用いる。
149	18.1.5.7.PB	クラウドサービス事業者は、クラウドサービス利用者に、適用する協定、法令及び規則を順守していることをレビューするため、クラウドサービス事業者が実装した暗号による管理策の記載を、提供する。
150	18.2.1	情報セキュリティ及びその実施の管理（例えば、情報セキュリティのための管理目的、管理策、方針、プロセス、手順）に対する組織の取組みについて、あらかじめ定めた間隔で、又は重大な変化が生じた場合に、独立したレビューを実施する。
151	18.2.2	管理者は、自分の責任の範囲内における情報処理及び手順が、適切な情報セキュリティのための方針群、標準類、及び他の全てのセキュリティ要求事項を順守していることを定期的にレビューする。
152	18.2.3	情報システムを、組織の情報セキュリティのための方針群及び標準の順守に関して、定めに従ってレビューする。