様式 2-3

内部監査に係る報告書

年　月　日

ISMAP 運営委員会　宛

申請者住所：
申請者名：
代表者役職名：
代表者名：

言明の対象となるクラウドサービスに関し、以下のとおり内部監査を実施しました。また、必要な情報セキュリティに係る内部統制を整備及び運用しています。

なお、ISMAP 運営委員会の要請があれば、内部監査の詳細について必要な資料を提出します。

記

１.対象クラウドサービス名称

２.内部監査体制

３.内部監査における重要事項

４.内部監査の対象とした統制目標
　別紙のとおり

５.内部監査対象期間

６.内部監査実施期間

７.内部監査の実施方法

８.内部監査の実施内容
　別紙のとおり

９.内部監査の結果の概要

以上

（様式 2-3 記載例）

内部監査に係る報告書

202X 年 X 月 XX 日

ISMAP 運営委員会　宛

申請者住所：〒113-65XX
東京都文京区本駒込
X 丁目 XX 番 XX 号
申請者名：XX クラウドサービス
株式会社
代表者役職名：代表取締役社長
代表者名：○○　○○

言明の対象となるクラウドサービスに関し、以下のとおり内部監査を実施しました。また、必要な情報セキュリティに係る内部統制を整備及び運用しています。

なお、ISMAP 運営委員会の要請があれば、内部監査の詳細について必要な資料を提出します。

記

１.対象クラウドサービス名称

XX サービス（言明対象サービスを記載）

２.内部監査体制

【責任者について】

責任者の所属部署/役職：○○部部長

責任者の監査に関する資格、経験等

＜資格＞

・公認情報システム監査人（CISA）を 20XX 年○月取得

＜経験＞

・20XX 年○月　○○社における内部監査において、サブリーダーを務める

・20XX 年○月　○○社における内部監査において、品質管理者を務める

【責任者以外の概要】

（責任者を除く、内部監査担当者の所属及び人数を記載）

３．内部監査における重要事項

内部監査人が、内部監査に際し重要な事項と判断した統制の重大な変更及び監査領域・項目は以下のとおりである。

【統制の重大な変更】

・管理策番号 x.x.x について、前年度の外部監査にて発見事項が識別されたため、統制内容やコントロールオーナーの大幅な変更が生じた。

【監査領域・項目】

・前年度の外部監査にて発見事項が識別された管理策番号 y.y.y

・前年度の内部監査にて発見事項が識別された管理策番号 z.z.z

・全社的なサイバーセキュリティの施策において重視されている、ネットワーク関連の領域

（内部監査の計画策定や実施段階で内部監査人が重要な事項と判断して監査手続を実施した重大な統制の変更や、領域・項目を記載する。）

４．内部監査の対象とした統制目標

別紙のとおり

５．内部監査対象期間

2021 年 4 月 1 日～2021 年 12 月 31 日

（内部監査の対象期間を記載）

６．内部監査実施期間

2022 年 1 月 1 日～2022 年 3 月 31 日

（内部監査の実施期間を記載。実施期間末日が内部監査結果報告日と一致すること。）

７.内部監査の実施方法

以下の手続により内部監査を実施した。

・コントロールセルフアセスメントの結果の閲覧と質問、内部監査人による一部のサンプルに対する再テストの実施

・内部監査人自らのウォークスルーの実施による整備状況評価と独自のサンプルテストによる運用状況評価の実施

・他のマネジメントシステムにおける内部監査の実施と、その結果を用いた ISMAP 詳細管理策への適合性の検証と内部監査人による一部の管理策に対する独自のサンプルテストの実施の組み合わせ

（どのような監査手続を用いたのかを記載する。上記は例示である。）

８.内部監査の実施内容

別紙のとおり

９.内部監査の結果の概要

内部監査の結果、XX 件の発見事項が識別された。当監査対象期間中に改善済ものは XX 件、未改善のものは XX 件である。なお、詳細は別紙のとおりである。

以上

（別紙）内部監査を実施した統制目標と内部監査結果の概要

対象クラウドサービス名称:

該当に〇入力　該当に〇入力　該当に〇入力　該当に〇入力　該当に〇入力　該当に〇入力　該当に〇入力　該当に〇入力　該当に〇入力　記述　選択　記述　記述　記入（X.X.X.X.PB）　選択（変更可）　選択（変更可）　選択（変更可）　記述　記入（YYYY/MM/DD）　選択　記入（YYYY/MM/DD）　記入（YYYY/MM）　記述

YYYY
当年度
2022 ←要入力

YYYY/MM/DD　YYYY/MM/DD～YYYY/MM/DD
要記入→ 内部監査報告日 2022/3/31　内部監査監査対象期間 2021/4/1～2021/12/31

有 / 無　　有 / 無　　高 / 中 / 低　　高 / 中 / 低　　高 / 中 / 低　　改善未着手 / 改善中 / 改善済

管理策番号P：クラウドサービスに特有のものとして、クラウドサービス事業者が特に考慮すべき管理策

※ISMAP-LIU初回登録年度以前の年度は記載不要

連番	ISMAP管理基準 令和2年6月3日（令和4年4月1日最終改定）							当年度内部監査対象				前年度内部監査対象		前々年度内部監査対象		当年度内部監査結果														備考
	章	管理策番号					統制目標	2022		2022		2021		2020		2022														
		1桁目	2桁目	管理目的	3桁目	P		非採用管理策（3桁レベル）	内部監査対象管理策（3桁レベル）	前年度内部監査発見事項の改善状況の監査	前年度外部監査発見事項の改善状況の監査	非採用管理策（3桁レベル）	内部監査対象管理策（3桁レベル）	非採用管理策（3桁レベル）	内部監査対象管理策（3桁レベル）	統制の重大な変更の有無	統制の重大な変更の内容（内部監査に影響を及ぼす可能性のある統制の重大な変更について、内容を詳細に記載する）※軽微な変更については記載不要	発見事項の有無	発見事項の内容（発見した事実を詳細に記載する）	発見事項の直接的な影響	対応する管理策番号（4桁レベル）	発見事項の影響度	発見事項の発生可能性	発見事項の重要度（リスク）	改善計画（内部監査人が把握した改善計画の内容を記載する）	改善日（または改善予定日）	改善状況	【参考情報】改善状況に対する内部監査の実施日	【参考情報】（未改善の場合）改善状況に対する内部監査の実施予定時期	
1	第5章管理策基準	5情報セキュリティのための方針群	5.1情報セキュリティのための経営陣の方向性	情報セキュリティのための経営陣の方向性及び支持を、事業上の要求事項並びに関連する法令及び規制に従って提示するため。	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	第5章管理策基準	5情報セキュリティのための方針群	5.1情報セキュリティのための経営陣の方向性	情報セキュリティのための経営陣の方向性及び支持を、事業上の要求事項並びに関連する法令及び規制に従って提示するため。	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	第5章管理策基準	6情報セキュリティのための組織	6.1内部組織	組織内で情報セキュリティの実施及び運用に着手し、これを統制するための管理上の枠組みを確立するため。	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	第5章管理策基準	6情報セキュリティのための組織	6.1内部組織	組織内で情報セキュリティの実施及び運用に着手し、これを統制するための管理上の枠組みを確立するため。	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。																							
5	第5章管理策基準	6情報セキュリティのための組織	6.1内部組織	組織内で情報セキュリティの実施及び運用に着手し、これを統制するための管理上の枠組みを確立するため。	6.1.3		関係当局との適切な連絡体制を維持する。																							
6	第5章管理策基準	6情報セキュリティのための組織	6.1内部組織	組織内で情報セキュリティの実施及び運用に着手し、これを統制するための管理上の枠組みを確立するため。	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。																							
7	第5章管理策基準	6情報セキュリティのための組織	6.1内部組織	組織内で情報セキュリティの実施及び運用に着手し、これを統制するための管理上の枠組みを確立するため。	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。																							
8	第5章管理策基準	6情報セキュリティのための組織	6.2モバイル機器及びテレワーキング	モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため。	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。																							
9	第5章管理策基準	6情報セキュリティのための組織	6.2モバイル機器及びテレワーキング	モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため。	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。																							
10	第5章管理策基準	6情報セキュリティのための組織	6.3.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関係	情報セキュリティマネジメントのための、クラウドサービス利用者及びクラウドサービス提供者間の共同責任の関係を説明するため。	6.3.1.P	〇	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。																							
11	第5章管理策基準	7人的資源のセキュリティ	7.1雇用前	従業員及び契約相手がその責任を理解し、求められている役割にふさわしいことを確実にするため。	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。																							
12	第5章管理策基準	7人的資源のセキュリティ	7.1雇用前	従業員及び契約相手がその責任を理解し、求められている役割にふさわしいことを確実にするため。	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。																							
13	第5章管理策基準	7人的資源のセキュリティ	7.2雇用期間中	従業員及び契約相手が、情報セキュリティの責任を認識し、かつ、その責任を遂行することを確実にするため。	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。																							
14	第5章管理策基準	7人的資源のセキュリティ	7.2雇用期間中	従業員及び契約相手が、情報セキュリティの責任を認識し、かつ、その責任を遂行することを確実にするため。	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。																							
15	第5章管理策基準	7人的資源のセキュリティ	7.2雇用期間中	従業員及び契約相手が、情報セキュリティの責任を認識し、かつ、その責任を遂行することを確実にするため。	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。																							
16	第5章管理策基準	7人的資源のセキュリティ	7.3雇用の終了及び変更	雇用の終了又は変更のプロセスの一部として、組織の利益を保護するため。	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。																							
17	第5章管理策基準	8資産の管理	8.1資産に対する責任	組織の資産を特定し、適切な保護の責任を定めるため。	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。																							
18	第5章管理策基準	8資産の管理	8.1資産に対する責任	組織の資産を特定し、適切な保護の責任を定めるため。	8.1.2		目録の中で維持される資産は、管理する。																							
19	第5章管理策基準	8資産の管理	8.1資産に対する責任	組織の資産を特定し、適切な保護の責任を定めるため。	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。																							
20	第5章管理策基準	8資産の管理	8.1資産に対する責任	組織の資産を特定し、適切な保護の責任を定めるため。	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。																							
21	第5章管理策基準	8資産の管理	8.1資産に対する責任	組織の資産を特定し、適切な保護の責任を定めるため。	8.1.5.P	〇	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、時期を失せずに返却または除去する。																							
22	第5章管理策基準	8資産の管理	8.2情報分類	組織に対する情報の重要性に応じて、情報の適切なレベルでの保護を確実にするため。	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。																							
23	第5章管理策基準	8資産の管理	8.2情報分類	組織に対する情報の重要性に応じて、情報の適切なレベルでの保護を確実にするため。	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。																							
24	第5章管理策基準	8資産の管理	8.2情報分類	組織に対する情報の重要性に応じて、情報の適切なレベルでの保護を確実にするため。	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。																							
25	第5章管理策基準	8資産の管理	8.3媒体の取扱い	媒体に保存された情報の認可されていない開示、変更、除去又は破壊を防止するため。	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。																							
26	第5章管理策基準	8資産の管理	8.3媒体の取扱い	媒体に保存された情報の認可されていない開示、変更、除去又は破壊を防止するため。	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。																							
27	第5章管理策基準	8資産の管理	8.3媒体の取扱い	媒体に保存された情報の認可されていない開示、変更、除去又は破壊を防止するため。	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。																							
28	第5章管理策基準	9アクセス制御	9.1アクセス制御に対する業務上の要求事項	情報及び情報処理施設へのアクセスを制限するため。	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。																							
29	第5章管理策基準	9アクセス制御	9.1アクセス制御に対する業務上の要求事項	情報及び情報処理施設へのアクセスを制限するため。	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。																							
30	第5章管理策基準	9アクセス制御	9.2利用者アクセスの管理	システム及びサービスへの、認可された利用者のアクセスを確実にし、認可されていないアクセスを防止するため。	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。																							
31	第5章管理策基準	9アクセス制御	9.2利用者アクセスの管理	システム及びサービスへの、認可された利用者のアクセスを確実にし、認可されていないアクセスを防止するため。	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。																							
32	第5章管理策基準	9アクセス制御	9.2利用者アクセスの管理	システム及びサービスへの、認可された利用者のアクセスを確実にし、認可されていないアクセスを防止するため。	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。																							
33	第5章管理策基準	9アクセス制御	9.2利用者アクセスの管理	システム及びサービスへの、認可された利用者のアクセスを確実にし、認可されていないアクセスを防止するため。	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。																							
34	第5章管理策基準	9アクセス制御	9.2利用者アクセスの管理	システム及びサービスへの、認可された利用者のアクセスを確実にし、認可されていないアクセスを防止するため。	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。																							
35	第5章管理策基準	9アクセス制御	9.2利用者アクセスの管理	システム及びサービスへの、認可された利用者のアクセスを確実にし、認可されていないアクセスを防止するため。	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。																							
36	第5章管理策基準	9アクセス制御	9.3利用者の責任	利用者に対して、自らの秘密認証情報を保護する責任をもたせるため。	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。																							
37	第5章管理策基準	9アクセス制御	9.4システム及びアプリケーションのアクセス制御	システム及びアプリケーションへの、認可されていないアクセスを防止するため。	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。																							
38	第5章管理策基準	9アクセス制御	9.4システム及びアプリケーションのアクセス制御	システム及びアプリケーションへの、認可されていないアクセスを防止するため。	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。																							
39	第5章管理策基準	9アクセス制御	9.4システム及びアプリケーションのアクセス制御	システム及びアプリケーションへの、認可されていないアクセスを防止するため。	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。																							
40	第5章管理策基準	9アクセス制御	9.4システム及びアプリケーションのアクセス制御	システム及びアプリケーションへの、認可されていないアクセスを防止するため。	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。																							
41	第5章管理策基準	9アクセス制御	9.4システム及びアプリケーションのアクセス制御	システム及びアプリケーションへの、認可されていないアクセスを防止するため。	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。																							
42	第5章管理策基準	9アクセス制御	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	共有化されたクラウドコンピューティング上の仮想環境における情報セキュリティを確実にするため。	9.5.1.P	〇	クラウドサービス利用者のクラウドサービス上の仮想環境は、他のクラウドサービス利用者及び認可されていない者から保護する。																							
43	第5章管理策基準	9アクセス制御	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	共有化されたクラウドコンピューティング上の仮想環境における情報セキュリティを確実にするため。	9.5.2.P	〇	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。																							
44	第5章管理策基準	10暗号	10.1暗号による管理策	情報の機密性、真正性及び／又は完全性を保護するために、暗号の適切かつ有効な利用を確実にするため。	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。																							
45	第5章管理策基準	10暗号	10.1暗号による管理策	情報の機密性、真正性及び／又は完全性を保護するために、暗号の適切かつ有効な利用を確実にするため。	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。																							
46	第5章管理策基準	11物理的及び環境的セキュリティ	11.1セキュリティを保つべき領域	組織の情報及び情報処理施設に対する認可されていない物理的アクセス、損傷及び妨害を防止するため。	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。																							
47	第5章管理策基準	11物理的及び環境的セキュリティ	11.1セキュリティを保つべき領域	組織の情報及び情報処理施設に対する認可されていない物理的アクセス、損傷及び妨害を防止するため。	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。																							
48	第5章管理策基準	11物理的及び環境的セキュリティ	11.1セキュリティを保つべき領域	組織の情報及び情報処理施設に対する認可されていない物理的アクセス、損傷及び妨害を防止するため。	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。																							
49	第5章管理策基準	11物理的及び環境的セキュリティ	11.1セキュリティを保つべき領域	組織の情報及び情報処理施設に対する認可されていない物理的アクセス、損傷及び妨害を防止するため。	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。																							
50	第5章管理策基準	11物理的及び環境的セキュリティ	11.1セキュリティを保つべき領域	組織の情報及び情報処理施設に対する認可されていない物理的アクセス、損傷及び妨害を防止するため。	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。																							
51	第5章管理策基準	11物理的及び環境的セキュリティ	11.1セキュリティを保つべき領域	組織の情報及び情報処理施設に対する認可されていない物理的アクセス、損傷及び妨害を防止するため。	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。																							
52	第5章管理策基準	11物理的及び環境的セキュリティ	11.2装置	資産の損失、損傷、盗難又は劣化、及び組織の業務に対する妨害を防止するため。	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。																							

通番	ISMAP管理基準 令和2年6月3日（令和4年4月1日最終改定）							当年度内部監査対象				前年度内部監査対象		前々年度内部監査対象		当年度内部監査結果														備考
	章	管理策番号					統制目標	2022		2022		2021		2020		2022														
		1桁目	2桁目	管理目的	3桁目	P		非採用管理策（3桁レベル）	内部監査対象（管理項（3桁レベル）	前年度内部監査の発見事項の改善状況の監査	前年度内部監査の発見事項の改善状況の監査	非採用管理策（3桁レベル）	内部監査対象（管理項（3桁レベル）	非採用管理策（3桁レベル）	内部監査対象（管理項（3桁レベル）	統制の重大な変更の有無	統制の重大な変更の内容 （内部監査に影響を及ぼす可能性のある統制の重大な変更について、内容を詳細に記載する） ※統制の変更については記載不要	発見事項の有無	（発見した事実を詳細に記載する）	発見事項の指摘内容	発見事項の影響	対応する管理策番号（4桁レベル）	発見事項の影響度	発見事項の発生可能性	発見事項の重要度（リスク）	改善計画 （内部監査人が把握した、改善計画の内容を記載する）	改善日 （または改善予定日）	改善状況	【参考情報】 改善状況に対する内部監査の実施日	【参考情報】 （未改善の場合） 改善状況に対する内部監査の実施予定時期	
53	5.5.2管理策基準	7.1物理的及び環境的セキュリティ	7.1.2設備	資産の損失、盗難、破損又は妨害、及び組織の業務に対する妨害を防止するため。	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。																							
54	5.5.2管理策基準	7.1物理的及び環境的セキュリティ	7.1.2設備	資産の損失、盗難、破損又は妨害、及び組織の業務に対する妨害を防止するため。	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。																							
55	5.5.2管理策基準	7.1物理的及び環境的セキュリティ	7.1.2設備	資産の損失、盗難、破損又は妨害、及び組織の業務に対する妨害を防止するため。	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。																							
56	5.5.2管理策基準	7.1物理的及び環境的セキュリティ	7.1.2設備	資産の損失、盗難、破損又は妨害、及び組織の業務に対する妨害を防止するため。	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。																							
57	5.5.2管理策基準	7.1物理的及び環境的セキュリティ	7.1.2設備	資産の損失、盗難、破損又は妨害、及び組織の業務に対する妨害を防止するため。	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。																							
58	5.5.2管理策基準	7.1物理的及び環境的セキュリティ	7.1.2設備	資産の損失、盗難、破損又は妨害、及び組織の業務に対する妨害を防止するため。	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、全ての取扱いに機密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つて書きていることを確実にするために、検証する。																							
59	5.5.2管理策基準	7.1物理的及び環境的セキュリティ	7.1.2設備	資産の損失、盗難、破損又は妨害、及び組織の業務に対する妨害を防止するため。	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。																							
60	5.5.2管理策基準	7.1物理的及び環境的セキュリティ	7.1.2設備	資産の損失、盗難、破損又は妨害、及び組織の業務に対する妨害を防止するため。	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な取り扱い方針、並びに情報処理設備に対するクリアスクリーンな方針を適用する。クリアデスク・クリアスクリーンの方針において、組織の、情報分類、法的及び契約上の要求事項、並びにそれらに対応する リスクを考慮する。																							
61	5.5.3管理策基準	7.2運用のセキュリティ	7.2.1運用の手順及び責任	情報処理設備の正確かつセキュリティを保った運用を確実にするため。	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。																							
62	5.5.3管理策基準	7.2運用のセキュリティ	7.2.1運用の手順及び責任	情報処理設備の正確かつセキュリティを保った運用を確実にするため。	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。																							
63	5.5.3管理策基準	7.2運用のセキュリティ	7.2.1運用の手順及び責任	情報処理設備の正確かつセキュリティを保った運用を確実にするため。	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。																							
64	5.5.3管理策基準	7.2運用のセキュリティ	7.2.1運用の手順及び責任	情報処理設備の正確かつセキュリティを保った運用を確実にするため。	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。																							
65	5.5.3管理策基準	7.2運用のセキュリティ	7.2.1運用の手順及び責任	情報処理設備の正確かつセキュリティを保った運用を確実にするため。	12.1.3.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。																							
66	5.5.3管理策基準	7.2運用のセキュリティ	7.2マルウェアからの保護	情報及び情報処理施設がマルウェアから保護されることを確実にするため。	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。																							
67	5.5.3管理策基準	7.2運用のセキュリティ	7.2.3バックアップ	データの消失から保護するため。	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。																							
68	5.5.3管理策基準	7.2運用のセキュリティ	7.2.4ログ取得及び監視	イベントを記録し、証拠を作成するため。	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、イベントログを取得し、保持し、定期的にレビューする。																							
69	5.5.3管理策基準	7.2運用のセキュリティ	7.2.4ログ取得及び監視	イベントを記録し、証拠を作成するため。	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。																							
70	5.5.3管理策基準	7.2運用のセキュリティ	7.2.4ログ取得及び監視	イベントを記録し、証拠を作成するため。	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。																							
71	5.5.3管理策基準	7.2運用のセキュリティ	7.2.4ログ取得及び監視	イベントを記録し、証拠を作成するため。	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。																							
72	5.5.3管理策基準	7.2運用のセキュリティ	7.2.4ログ取得及び監視	イベントを記録し、証拠を作成するため。	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。																							
73	5.5.3管理策基準	7.2運用のセキュリティ	7.2.5運用ソフトウェアの管理	運用システムの完全性を確実にするため。	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。																							
74	5.5.3管理策基準	7.2運用のセキュリティ	7.2.6技術的ぜい弱性管理	技術的ぜい弱性の悪用を防止するため。	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。																							
75	5.5.3管理策基準	7.2運用のセキュリティ	7.2.6技術的ぜい弱性管理	技術的ぜい弱性の悪用を防止するため。	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。																							
76	5.5.3管理策基準	7.2運用のセキュリティ	7.2.7情報システムの監査に対する考慮事項	運用システムに対する監査活動の影響を最小限にするため。	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、業務プロセスにおける中断を最小限にするために、慎重に計画し、合意する。																							
77	5.5.4管理策基準	7.3通信のセキュリティ	7.3.1ネットワークセキュリティ管理	ネットワークにおける情報の保護、及びネットワークを支える情報処理施設の保護を確実にするため。	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。																							
78	5.5.4管理策基準	7.3通信のセキュリティ	7.3.1ネットワークセキュリティ管理	ネットワークにおける情報の保護、及びネットワークを支える情報処理施設の保護を確実にするため。	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。																							
79	5.5.4管理策基準	7.3通信のセキュリティ	7.3.1ネットワークセキュリティ管理	ネットワークにおける情報の保護、及びネットワークを支える情報処理施設の保護を確実にするため。	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。																							
80	5.5.4管理策基準	7.3通信のセキュリティ	7.3.1ネットワークセキュリティ管理	ネットワークにおける情報の保護、及びネットワークを支える情報処理施設の保護を確実にするため。	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。																							
81	5.5.4管理策基準	7.3通信のセキュリティ	7.3.2情報の転送	組織の内部及び外部に転送した情報のセキュリティを維持するため。	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。																							
82	5.5.4管理策基準	7.3通信のセキュリティ	7.3.2情報の転送	組織の内部及び外部に転送した情報のセキュリティを維持するため。	13.2.2		情報転送に関する合意では、組織と外部関係者との間の業務情報のセキュリティを扱った転送について、取り扱う。																							
83	5.5.4管理策基準	7.3通信のセキュリティ	7.3.2情報の転送	組織の内部及び外部に転送した情報のセキュリティを維持するため。	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。																							
84	5.5.4管理策基準	7.3通信のセキュリティ	7.3.2情報の転送	組織の内部及び外部に転送した情報のセキュリティを維持するため。	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。																							
85	5.5.5管理策基準	7.4システムの取得、開発及び保守	7.4.1情報システムのセキュリティ要求事項	ライフサイクル全体にわたって、情報セキュリティが情報システムに欠くことのできない部分であることを確実にするため。これには、公衆ネットワークを介して サービスを提供する情報システムのための要求事項も含む。	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。																							
86	5.5.5管理策基準	7.4システムの取得、開発及び保守	7.4.1情報システムのセキュリティ要求事項	ライフサイクル全体にわたって、情報セキュリティが情報システムに欠くことのできない部分であることを確実にするため。これには、公衆ネットワークを介して サービスを提供する情報システムのための要求事項も含む。	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。																							
87	5.5.5管理策基準	7.4システムの取得、開発及び保守	7.4.1情報システムのセキュリティ要求事項	ライフサイクル全体にわたって、情報セキュリティが情報システムに欠くことのできない部分であることを確実にするため。これには、公衆ネットワークを介して サービスを提供する情報システムのための要求事項も含む。	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 -認可されていないメッセージの変更 -認可されていない開示 -認可されていないメッセージの複製又は再生																							
88	5.5.5管理策基準	7.4システムの取得、開発及び保守	7.4.2開発及びサポートプロセスにおけるセキュリティ	情報システムの開発サイクルの中で情報セキュリティを設計し、実施することを確実にするため。	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。																							
89	5.5.5管理策基準	7.4システムの取得、開発及び保守	7.4.2開発及びサポートプロセスにおけるセキュリティ	情報システムの開発サイクルの中で情報セキュリティを設計し、実施することを確実にするため。	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。																							
90	5.5.5管理策基準	7.4システムの取得、開発及び保守	7.4.2開発及びサポートプロセスにおけるセキュリティ	情報システムの開発サイクルの中で情報セキュリティを設計し、実施することを確実にするため。	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、試験する。																							
91	5.5.5管理策基準	7.4システムの取得、開発及び保守	7.4.2開発及びサポートプロセスにおけるセキュリティ	情報システムの開発サイクルの中で情報セキュリティを設計し、実施することを確実にするため。	14.2.4		パッケージソフトウェアの変更は、抑止し、必要な変更だけに留る。また、全ての変更は、厳重に管理する。																							
92	5.5.5管理策基準	7.4システムの取得、開発及び保守	7.4.2開発及びサポートプロセスにおけるセキュリティ	情報システムの開発サイクルの中で情報セキュリティを設計し、実施することを確実にするため。	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。																							
93	5.5.5管理策基準	7.4システムの取得、開発及び保守	7.4.2開発及びサポートプロセスにおけるセキュリティ	情報システムの開発サイクルの中で情報セキュリティを設計し、実施することを確実にするため。	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。																							
94	5.5.5管理策基準	7.4システムの取得、開発及び保守	7.4.2開発及びサポートプロセスにおけるセキュリティ	情報システムの開発サイクルの中で情報セキュリティを設計し、実施することを確実にするため。	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。																							
95	5.5.5管理策基準	7.4システムの取得、開発及び保守	7.4.2開発及びサポートプロセスにおけるセキュリティ	情報システムの開発サイクルの中で情報セキュリティを設計し、実施することを確実にするため。	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。																							
96	5.5.5管理策基準	7.4システムの取得、開発及び保守	7.4.2開発及びサポートプロセスにおけるセキュリティ	情報システムの開発サイクルの中で情報セキュリティを設計し、実施することを確実にするため。	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。																							
97	5.5.5管理策基準	7.4システムの取得、開発及び保守	7.4.3試験データ	試験に用いるデータの保護を確実にするため。	14.3.1		試験データは、注意深く選定し、保護し、管理する。																							
98	5.5.6管理策基準	7.5供給者関係	7.5.1供給者関係における情報セキュリティ	供給者がアクセスできる組織の資産の保護を確実にするため。	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低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。																							
99	5.5.6管理策基準	7.5供給者関係	7.5.1供給者関係における情報セキュリティ	供給者がアクセスできる組織の資産の保護を確実にするため。	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。																							
100	5.5.6管理策基準	7.5供給者関係	7.5.1供給者関係における情報セキュリティ	供給者がアクセスできる組織の資産の保護を確実にするため。	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。																							
101	5.5.6管理策基準	7.5供給者関係	7.5.2供給者のサービス提供の管理	供給者との合意に沿って、情報セキュリティ及びサービス提供について合意したレベルを維持するため。	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、監査する。																							
102	5.5.6管理策基準	7.5供給者関係	7.5.2供給者のサービス提供の管理	供給者との合意に沿って、情報セキュリティ及びサービス提供について合意したレベルを維持するため。	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。																							
103	5.5.7管理策基準	7.6情報セキュリティインシデントの管理及びその改善	16.1情報セキュリティインシデントの管理及びその改善	セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取組みを確実にするため。	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。																							
104	5.5.7管理策基準	7.6情報セキュリティインシデントの管理及びその改善	16.1情報セキュリティインシデントの管理及びその改善	セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取組みを確実にするため。	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。																							

通番	ISMAP管理基準 令和2年8月3日（令和4年4月1日最終改定）							当年度内部監査対象				前年度内部監査対象		前々年度内部監査対象		当年度内部監査結果													備考
	章	管理策番号					統制目標	2022		2022		2021		2020		2022													
		1桁目	2桁目	管理目的	3桁目	P		非採用管理策（3桁レベル）	内部監査対象管理策（3桁レベル）	前々年度内部監査対象（発見事項の改善状況の監査	前々年度内部監査対象（発見事項の改善状況の監査	非採用管理策（3桁レベル）	内部監査対象管理策（3桁レベル）	非採用管理策（3桁レベル）	内部監査対象管理策（3桁レベル）	統制の重大な変更の有無	統制の重大な変更の内容 （内部監査に影響を及ぼす可能性のある統制の重大な変更について、内容を詳細に記載する） ※統制の変更については記載不要	発見事項の有無	発見した事実を詳細に記載する）	発見事項の直接的な影響	対応する管理策番号（4桁レベル）	発見事項の影響度	発見事項の発生可能性	発見事項の重要度（リスク）	改善計画 （内部監査人が把握した、改善計画の内容を記載する）	改善日 （または改善予定日）	改善状況	【参考情報】 改善状況に対する内部監査の実施日	【参考情報】 （未改善の場合） 改善状況に対する内部監査の実施予定時期	
105	5 組織的管理策群	5.1情報セキュリティインシデント管理	5.1.1情報セキュリティインシデントの管理及びその改善	セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取組みを確実にするため。	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。																					
106	5 組織的管理策群	5.1情報セキュリティインシデント管理	5.1.1情報セキュリティインシデントの管理及びその改善	セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取組みを確実にするため。	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。																					
107	5 組織的管理策群	5.1情報セキュリティインシデント管理	5.1.1情報セキュリティインシデントの管理及びその改善	セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取組みを確実にするため。	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。																					
108	5 組織的管理策群	5.1情報セキュリティインシデント管理	5.1.1情報セキュリティインシデントの管理及びその改善	セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取組みを確実にするため。	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。																					
109	5 組織的管理策群	5.1情報セキュリティインシデント管理	5.1.1情報セキュリティインシデントの管理及びその改善	セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取組みを確実にするため。	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。																					
110	5 組織的管理策群	17.事業継続マネジメントにおける情報セキュリティの側面	17.1情報セキュリティ継続	情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込むため。	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。																					
111	5 組織的管理策群	17.事業継続マネジメントにおける情報セキュリティの側面	17.1情報セキュリティ継続	情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込むため。	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。																					
112	5 組織的管理策群	17.事業継続マネジメントにおける情報セキュリティの側面	17.1情報セキュリティ継続	情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込むため。	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。																					
113	5 組織的管理策群	17.事業継続マネジメントにおける情報セキュリティの側面	17.2冗長性	情報処理施設の可用性を確実にするため。	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。																					
114	5 組織的管理策群	18.順守	18.1法的及び契約上の要求事項の順守	情報セキュリティに関連する法的、規制又は契約上の義務に対する違反、及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。	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。																					
115	5 組織的管理策群	18.順守	18.1法的及び契約上の要求事項の順守	情報セキュリティに関連する法的、規制又は契約上の義務に対する違反、及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。	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。																					
116	5 組織的管理策群	18.順守	18.1法的及び契約上の要求事項の順守	情報セキュリティに関連する法的、規制又は契約上の義務に対する違反、及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。	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。																					
117	5 組織的管理策群	18.順守	18.1法的及び契約上の要求事項の順守	情報セキュリティに関連する法的、規制又は契約上の義務に対する違反、及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。	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。																					
118	5 組織的管理策群	18.順守	18.1法的及び契約上の要求事項の順守	情報セキュリティに関連する法的、規制又は契約上の義務に対する違反、及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。	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。																					
119	5 組織的管理策群	18.順守	18.2情報セキュリティのレビュー	組織の方針及び手順に従って情報セキュリティが実施され、運用されることを確実にするため。	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。																					
120	5 組織的管理策群	18.順守	18.2情報セキュリティのレビュー	組織の方針及び手順に従って情報セキュリティが実施され、運用されることを確実にするため。	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、及び他のすべ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。																					
121	5 組織的管理策群	18.順守	18.2情報セキュリティのレビュー	組織の方針及び手順に従って情報セキュリティが実施され、運用されることを確実にするため。	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。																					

（別紙）内部監査を資産した統制目標と内部監査結果の概要

対象クラウドサービス名称:

当初にCOん力	当初にCOん力	当初にCOん力	当初にCOん力	当初にCOん力	当初にCOん力	当初にCOん力	当初にCOん力	当初にCOん力	当初にCOん力	記述	選択	記述	記述	記入（L,X,X,X,円）	選択（変更可）	選択（変更可）	選択（変更可）	記述	記入（YYYY/MM/DD）	選択	記入（YYYY/MM/DD）	記入（YYYY/MM）	記述
YYYY										YYYY/MM/DD		YYYY/MM/DD-YYYY/MM/DD											
当年度										内部監査報告日		内部監査監査対象期間			高	高	高			改善未着手			
2022	←記入								前記入→	2022/3/31		2021/4/1~2021/12/31			中	中	中			改善中			
											有				低	低	低			改善済			
											無												

管理策番号とISMAP管理基準の対応関係については、クラウドサービス本事業者が用いる考えで決定すること

※ISMAP-LIU対応者登録年度以前の年度は記載不要

通番	ISMAP管理基準 令和2年6月3日（令和4年4月1日最終改定）							当年度内部監査対象				前年度内部監査対象				前々年度内部監査対象				当年度内部監査結果														備考
	章	管理策番号					統制目標	2022				2022				2021				2020				2022										
		1桁目	2桁目	管理的	3桁目	P		非採用管理策（3桁レベル）	内部監査対象管理策（3桁レベル）	前年度内部監査対象管理策の改善状況の監査	前年度外部監査対象管理策の改善状況の監査	非採用管理策（3桁レベル）	内部監査対象管理策（3桁レベル）	非採用管理策（3桁レベル）	内部監査対象管理策（3桁レベル）	統制の重大な変更の有無	統制の重大な変更の内容（内部監査に影響を及ぼす可能性のある統制の重大な変更について、内容を詳細に記載する）※前期から変更については記載不要	発見事項の有無	発見事項の内容（発見しない事項を詳細に記載する）	発見事項の直接的な影響	対応する管理策番号（4桁レベル）	発見事項の影響度	発見事項の発生可能性	発見事項の重要度（リスク）	改善計画（内部監査人が把握した改善計画の内容を記載する）	改善日（または改善予定日）	改善状況	【参考情報】改善状況に対する内部監査の実施日	【参考情報】（未改善の場合）改善状況に対する内部監査の実施予定時期	
9	9.1.1	9.1.1a	9.1.1b	9.1.1c	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。											無														
9	9.1.1	9.1.1a	9.1.1b	9.1.1c	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。								○			無														
9	9.1.1	9.1.1a	9.1.1b	9.1.1c	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。						○					無														
9	9.1.1	9.1.1a	9.1.1b	9.1.1c	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。		○									無														
9	9.1.1	9.1.1a	9.1.1b	9.1.1c	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。		○		○							無														
32	9.1.1	9.1.1a	9.1.1b	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。		○						○	従前までで作業できていた、特権的アクセス権の割当、制限、管理に関して、特権的アクセス権の払い出しシステムを導入し、従前のプロセスを削除した。また、それに伴い、コントロールオーナー部署がシステム運用グループから、システムリスク管理グループへと変更となった。	無															
31	9.1.1	9.1.1a	9.1.1b	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当初当てるために、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。		○									有	内部監査対象期間中のの作成のサンプル25件の5%3件について、システムリスク管理グループ長の承認が無いまま、作成されていた。 また、内部監査対象期間中に作成されたシステム利用者数の2/3の2/3で1/3で、システムリスク管理グループ長の承認が無いままが成されていた。 なお、使用しているワークフローシステムにおいて、利用者ロの登録の際には、システムリスク管理グループ長の承認が無くても作成できる設定へと、2021/5/1に変更されていた。	当該3つのIDに関しては、事後的にシステムリスク管理グループ長の承認が得られており、適切な職務の割れ、この件完されたものであり、本質的な事故やセキュリティインデント等に直接影響を及ぼすものではなかったことを確かめた。	9.2.2.1 9.2.2.4	低	低	低	ワークフローシステム上で、eシステム利用者ロの登録の際には、システムリスク管理グループ長の承認がが必須となる設定に変更する。 また、当該設定を含む、ワークフローシステムの設定が、所定のバラメーターから変更されていないことを半期ごとに様かめる統制を、システムリスク管理グループの担当者が実施し、システムリスク管理グループ長に報告する。	2021/12/01	改善済	2021/12/27		
30	9.1.1	9.1.1a	9.1.1b	9.2利用者アクセスの管理	システム及びサービスへの、認可された利用者のアクセスを確実にし、認可されていないアクセスを防止するため、	9.2.1		アクセス権の割当て前に、利用者の登録及び登録時期についての正式なプロセスを実施する。		○							有	内部監査対象期間中に実施された、コントロールオーナーのシステムリスク管理グループによるコントロールセルフアセスメントの結果を閲覧したところ、システムについて、1名の退職者のロが削除されずに残った状態の状態であった。 内部監査対象期間中の退職者32名のうち、1名の退職者のロのみが抜けた。 また、本部ごとに実施されるロの棚卸において、当該ロも棚卸すべきおよんで適切に識別されていなかった。	当該退職者のロは退職日以降に、複数回ログインがされていたが、特定の操作のログの取得方法及び定めなどにより、行われた操作の全容を特定することはできなかった。 なお、当該ロにはeシステムの本番環境のデータを更新する権限が付与されていた。 ログを閲覧した限りは、ログイン情報のみが記録されており、情報資ういやデータの更新等の操作は識別されなかった。 また、eシステムに起因するインシデント等は内部監査対象期間及び実施期間には識別されなかった。	9.2.1.3 9.2.1.4	高	中	高	人事システムと連携をし、退職日の翌日に退職者のアカウントが自動的に無効化される仕組みを導入する。 また、操作ログの取得条件を見直し、設定に記載させた3えで、必要な操作ログが取得されるようにする。	2022-/05-01	改善中		2022-/05	

以下に留意して発見事項の内容を記載をする。
・内部監査で実施した手続とその結果（例：コントロールセルフアセスメントの結果の閲覧、サンプルテスト等）
・発見した原因と評価
・代替統制や補完統制の有無とその内容

発見事項により固改化した影響を記載する。

発見事項の潜在的な重要度を記載する（固定化しているかにかかわらず発見事項が引き起こしうるセキュリティインシデントや手続き、重要度を記載する）。
一例として、通常900の発見事項であれば、Xシステムの未移データが本部長職者のIDによって変更されている可能性があるので、評価は「高」と評価する。
また、今回は是正のIDは1件のみであったが、統制統制が有効に運用していなかったことから、共通の手法が今後も発生する可能性も一定程度存在すると考え、発生可能性は「中」と評価する。
上記を踏まえ、潜在的の重要度は「高」と判断をする）
重要度は、内部監査人が判断した結果を記載する。また、ら選択肢は、影響度（高中低の3段階）× 発生可能性（高）= 重要度（高）の一般的な計算式を前提としているが、例えば影響度を1段度で評価しているが、特長の評価方法を採用している場合は、選択肢をカスタマイズしてもよい（両の追加・削除は原則等の制定上不可）。

統制のどの箇所をどのように改善するのか、詳細を記載する。

別紙 1

SaaS の利用に係る業務・情報の影響度評価基準

1. 総則

本規則第5章に基づき、SaaSで取り扱われ処理される各業務に係わる情報において、「政府機関等のサイバーセキュリティ対策のための統一基準群」（令和３年７月７日サイバーセキュリティ戦略本部決定）で定める機密性・完全性・可用性が損なわれた場合の影響度を評価し、それぞれの業務・情報の影響度について低位、中位、高位の評価を行う。

2. 業務・情報の影響度評価における評価観点

影響度評価においては「SaaSの利用において想定されるリスク」①～⑥を基本的な評価観点とする。「SaaSの利用において想定されるリスク」は、「政府機関等の対策基準策定のためのガイドライン（令和３年度版）」　第6部 情報システムのセキュリティ要件の遵守事項6.1.1(1)(b)に記載の、「オンライン手続において想定されるリスク」を参考とし、SaaSの特性より政府機関内の業務におけるサービス利用が主となることを踏まえリスクを設定している。

SaaS の利用において想定されるリスク

① 国民に不便、苦痛を与える、又は機関等が信頼を失う
② 利用者に金銭的被害や賠償責任が生じるなど、財務上の影響を与える
③ 機関等の活動計画や公共の利益に対して影響を与える
④ 個人情報等の機微な情報が漏えいする
⑤ 利用者の身の安全に影響を与える
⑥ 法律に違反する

3. 各評価観点における影響度

各評価観点における影響度のレベルは、「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」付録A「７．各リスクの種類による影響度の導出」をもとに、SaaSの特性を踏まえ内容の整理を行った。

政府機関等は、各評価観点における影響度のレベルを考慮の上、業務に係わる情報の影響度評価を実施することが求められる。なお、個々の業務に係わる情報の影響度評価としてはN/Aの結果もあり得るが、SaaSで取り扱われる各業務に係わる一連の評価を総合した結果（これを総合評価と定める）については、低位、中位、高位の3段階で評価を行うものとする。

「１． 国民に不便、苦痛を与える、又は機関等が信頼を失う」リスクの影響度

レベル	内容
N/A	リスクがない（想定されない）。
低位	限定的かつ短期間の不便や苦痛又は、機関等の地位や評判に対し軽微な影響がある。
中位	深刻かつ短期間又は限定的かつ長期間の不便や苦痛又は、機関等の地位や評判に対する影響がある。
高位	深刻又は長期間の不便や苦痛又は、機関等の地位や評判に対する影響がある。この影響は、特に深刻な影響や多くの機関等の利用者に影響する状況をいう。

「２． 利用者に金銭的被害や賠償責任が生じるなど、財務上の影響を与える」リスクの影響度

レベル	内容
N/A	リスクがない（想定されない）。
低位	機関等の軽微又は若干の財務上の損失、若しくは機関等の軽微又は若干の賠償責任が生じる。
中位	機関等の深刻な財務上の損失、若しくは機関等の深刻な賠償責任が生じる。
高位	機関等の壊滅的な財務上の損失、若しくは機関の深刻又は壊滅的な賠償責任が生じる。

「３． 機関等の活動計画や公共の利益に対して影響を与える 」リスクの影響度

レベル	内容
N/A	リスクがない（想定されない）。
低位	機関等の運営又は資産、若しくは公共の利益に対する限定的な悪影響がある。限定的な悪影響の例としては以下が考えられる。(i) 機関等の主要な機能が「著しく」低下した状態が継続し、業務能力の劣化が生じている。(ii) 機関等の資産や公共の利益の軽微な損害が生じる。
中位	機関等の運営又は資産、若しくは公共の利益に対する深刻な悪影響がある。深刻な悪影響の例としては以下が考えられる。(i) 機関等の主要な機能が「大幅に」低下した状態が継続し、業務能力の大幅な劣化が生じている。(ii) 機関等の資産や公共の利益の重大な損害が生じる。
高位	機関等の運営又は資産、若しくは公共の利益に対する重大又は壊滅的な悪影響がある。重大又は壊滅的な悪影響の例としては以下が考えられる。(i) 機関等の主要な機能の１つ以上が実施できない状態が継続し、業務能

	力の激しい劣化又は喪失が生じている。(ii) 機関等の資産又は公共の利益の際立った損害が生じている。

「４． 個人情報等の機微な情報が漏えいする」リスクの影響度

レベル	内容
N/A	リスクがない（想定されない)。
低位	公開許可のない個人情報、政府の機密情報又は企業秘密の限定的な公開により、機関等の活動や資産、又は利用者に機密性喪失の限定的な悪影響をもたらすことが予測される。
中位	公開許可のない個人情報、政府の機密情報又は企業秘密の公開により、機関等の活動や資産、又は利用者に機密性損失の重大な悪影響をもたらすことが予測される。
高位	公開許可のない個人情報、政府の機密情報又は企業秘密の公開により、機関等の活動や資産、又は利用者に致命的又は壊滅的な機密性損失の悪影響をもたらすことが予測される。

「５． 利用者の身の安全に影響を与える 」リスクの影響度

レベル	内容
N/A	リスクがない（想定されない)。
低位	医療措置を必要としない軽症の影響を与える。
中位	軽症が生じる中程度のリスク又は医療措置を必要とする負傷が生じる限定的な影響を与える。
高位	深刻な負傷又は死亡の影響を与える。

「６． 法律に違反する」リスクの影響度

レベル	内容
N/A	リスクがない（想定されない)。
低位	法執行の対象とならないような性質の民事上又は刑事上の法律違反のリスクがある。
中位	法執行の対象となる可能性のある民事上又は刑事上の法律違反のリスクがある。
高位	法執行の計画で、特に重要とされている民事上又は刑事上の法律違反のリスクがある。