章	節	項	項目	遵守事項	Googleの回答
情報セキュリティ対策の基本的枠組み					
2.1	導入・計画				
2.1	2.1.1	組織・体制の整備			
2.1	2.1.1	(1)	最高情報セキュリティ責任者及び最高情報セキュリティ副責任者の設置		
2.1	2.1.1	(1)	(a)	機関等は、機関等における情報セキュリティに関する事務を統括する最高情報セキュリティ責任者１人を置くこと。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27002 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27002 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.1	2.1.1	(1)	(b)	機関等は、最高情報セキュリティ責任者を助けて機関等における情報セキュリティに関する事務を整理し、最高情報セキュリティ責任者の命を受けて機関等の情報セキュリティに関する事務を統括する最高情報セキュリティ副責任者１人を必要に応じて置くこと。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27002 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27002 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.1	2.1.1	(2)	情報セキュリティ委員会の設置		
2.1	2.1.1	(2)	(a)	最高情報セキュリティ責任者は、対策基準等の審議を行う機能を持つ組織として、情報セキュリティ対策推進体制及びその他業務を実施する部局の代表者を構成員とする情報セキュリティ委員会を置くこと。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27002 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27002 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.1	2.1.1	(3)	情報セキュリティ監査責任者の設置		
2.1	2.1.1	(3)	(a)	最高情報セキュリティ責任者は、その指示に基づき実施する監査に関する事務を統括する者として、情報セキュリティ監査責任者１人を置くこと。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27002 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27002 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.1	2.1.1	(4)	統括情報セキュリティ責任者・情報セキュリティ責任者等の設置		
2.1	2.1.1	(4)	(a)	最高情報セキュリティ責任者は、業務の特性等から同質の情報セキュリティ対策の運用が可能な組織のまとまりごとに、情報セキュリティ対策に関する事務を統括する者として、情報セキュリティ責任者１人を置くこと。そのうち、情報セキュリティ責任者を統括し、最高情報セキュリティ責任者及び最高情報セキュリティ副責任者を補佐する者として、統括情報セキュリティ責任者１人を選任すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27002 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27002 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.1	2.1.1	(4)	(b)	情報セキュリティ責任者は、遵守事項2.1.1(2)(a)で定める区域ごとに、当該区域における情報セキュリティ対策の事務を統括する区域情報セキュリティ責任者1 人を置くこと。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27002 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27002 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.1	2.1.1	(4)	(c)	情報セキュリティ責任者は、課室ごとに情報セキュリティ対策に関する事務を統括する課室情報セキュリティ責任者1 人を置くこと。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27002 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27002 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.1	2.1.1	(4)	(d)	情報セキュリティ責任者は、所管する情報システムに対する情報セキュリティ対策に関する事務の責任者として、情報システムセキュリティ責任者を、当該情報システムの企画に着手するまでに選任すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27002 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27002 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.1	2.1.1	(5)	最高情報セキュリティアドバイザーの設置		
2.1	2.1.1	(5)	(a)	最高情報セキュリティ責任者は、情報セキュリティについて専門的な知識及び経験を有する者を最高情報セキュリティアドバイザーとして置き、自らへの助言を含む最高情報セキュリティアドバイザーの業務内容を定めること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27002 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27002 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.1	2.1.1	(6)	情報セキュリティ対策推進体制の整備		
		(6)	(a)	最高情報セキュリティ責任者は、機関等の情報セキュリティ対策推進体制を整備し、その役割を規定すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27002 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27002 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
		(6)	(b)	最高情報セキュリティ責任者は、情報セキュリティ対策推進体制の責任者を定めること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27002 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27002 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.1	2.1.1	(7)	情報セキュリティインシデントに備えた体制の整備		
2.1	2.1.1	(7)	(a)	最高情報セキュリティ責任者は、CSIRT を整備し、その役割を明確化すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27002 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27002 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。

2.1	2.1.1	(7)	(b)	最高情報セキュリティ責任者は、職員等のうちからCSIRT に属する職員等として 専門的な知識又は適性を有すると認められる者を選任すること。そのうち、機関等に おける情報セキュリティインシデントに対処するための責任者としてCSIRT 責任者 を置くこと。また、CSIRT 内の業務統括及び外部との連携等を行う職員等を定める こと。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27002 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27002 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.1	2.1.1	(7)	(c)	最高情報セキュリティ責任者は、情報セキュリティインシデントが発生した際、直 ちに自らへの報告が行われる体制を整備すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27002 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27002 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.1	2.1.1	(7)	(d)	最高情報セキュリティ責任者は、CYMAT に属する職員を指名すること。(国の行 政機関に限る。)	ー
2.1	2.1.1	(8)	兼務を禁止する役割		
2.1	2.1.1	(8)	(a)	職員等は、情報セキュリティ対策の運用において、以下の役割を兼務しないこと。 (ア) 承認又は許可(以下本条において「承認等」という。)の申請者と当該承認 等を行う者(以下本条において「承認権限者等」という。) (イ) 監査を受ける者とその監査を実施する者	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てていますGoogle 社員に付与される既定のアクセス権限は、社員用メールやGoogle 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフローツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定　の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud Platform のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.1	2.1.1	(8)	(b)	職員等は、承認等を申請する場合において、自らが承認権限者等であるときその他 承認権限者等が承認等の可否の判断をすることが不適切と認められるときは、当該 承認権限者等の上司又は適切な者に承認等を申請し、承認等を得ること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てていますGoogle 社員に付与される既定のアクセス権限は、社員用メールやGoogle 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフローツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定　の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud Platform のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.1	2.1.2	府省庁対策基準・対策推進計画の策定			
2.1	2.1.2	(1)	府省庁対策基準の策定		
2.1	2.1.2	(1)	(a)	最高情報セキュリティ責任者は、情報セキュリティ委員会における審議を経て、統 一基準に準拠した対策基準を定めること。また、対策基準は、機関等の業務、取り扱 う情報及び保有する情報システムに関するリスク評価の結果を踏まえた上で定める こと。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27001 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27001 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.1	2.1.2	(2)	対策推進計画の策定		
2.1	2.1.2	(2)	(a)	最高情報セキュリティ責任者は、情報セキュリティ委員会における審議を経て、情 報セキュリティ対策を総合的に推進するための計画(以下「対策推進計画」という。) を定めること。また、対策推進計画には、機関等の業務、取り扱う情報及び保有する 情報システムに関するリスク評価の結果を踏まえた全体方針並びに以下に掲げる取 組の方針・重点及びその実施時期を含めること。 (ア) 情報セキュリティに関する教育 (イ) 情報セキュリティ対策の自己点検 (ウ) 情報セキュリティ監査 (エ) 情報システムに関する技術的な対策を推進するための取組 (オ) 前各号に掲げるもののほか、情報セキュリティ対策に関する重要な取組	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27001 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27001 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.2	運用				
2.2	2.2.1	情報セキュリティ関係規程の運用			
2.2	2.2.1	(1)	情報セキュリティ対策の運用		
2.2	2.2.1	(1)	(a)	統括情報セキュリティ責任者は、機関等における情報セキュリティ対策に関する 実施手順を整備(本統一基準で整備すべき者を別に定める場合を除く。)し、実施手 順に関する事務を統括し、整備状況について最高情報セキュリティ責任者に報告す ること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27001 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27001 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。

2.2	2.2.1	(1)	(b)	統括情報セキュリティ責任者は、情報セキュリティ対策における雇用の開始、終了 及び人事異動時等に関する管理の規定を整備すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27001 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27001 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.2	2.2.1	(1)	(c)	情報セキュリティ対策推進体制は、最高情報セキュリティ責任者が規定した当該 体制の役割に応じて必要な事務を遂行すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27001 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27001 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.2	2.2.1	(1)	(d)	情報セキュリティ責任者又は課室情報セキュリティ責任者は、職員等から情報セ キュリティ関係規程に係る課題及び問題点の報告を受けた場合は、統括情報セキュ リティ責任者に報告すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27001 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27001 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.2	2.2.1	(1)	(e)	統括情報セキュリティ責任者は、情報セキュリティ関係規程に係る課題及び問題 点を含む運用状況を適時に把握し、必要に応じて最高情報セキュリティ責任者にそ の内容を報告すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27001 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27001 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.2	2.2.1	(2)	違反への対処		
2.2	2.2.1	(2)	(a)	職員等は、情報セキュリティ関係規程への重大な違反を知った場合は、情報セキュ リティ責任者にその旨を報告すること。	Google は ISO27001 認証を受けています。この基準では、「人的資源のセキュリティ」(ISO27001 2013、附属書 A.7)が規定されています。人的資源の管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、人的資源の管理など、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.2	2.2.1	(2)	(b)	情報セキュリティ責任者は、情報セキュリティ関係規程への重大な違反の報告を 受けた場合及び自らが重大な違反を知った場合には、違反者及び必要な者に情報セ キュリティの維持に必要な措置を講じさせるとともに、統括情報セキュリティ責任 者を通じて、最高情報セキュリティ責任者に報告すること。	Google は ISO27001 認証を受けています。この基準では、「人的資源のセキュリティ」(ISO27001 2013、附属書 A.7)が規定されています。人的資源の管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、人的資源の管理など、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.2	2.2.2	例外措置			
2.2	2.2.2	(1)	例外措置手続の整備		
2.2	2.2.2	(1)	(a)	最高情報セキュリティ責任者は、例外措置の適用の申請を審査する者（以下本款に おいて「許可権限者」という。）及び審査手続を定めること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27001 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27001 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.2	2.2.2	(1)	(b)	統括情報セキュリティ責任者は、例外措置の適用審査記録の台帳を整備し、許可権 限者に対して、定期的に申請状況の報告を求めること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO27001 2013、附属書 A.7.2.2)が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全社員は、入社時研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新入社員は入社時研修でGoogle の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティチームに配属されたエンジニアは、安全なコーディング方法、プロダクト設 計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。 Google Cloud Platform のお客様は、運用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.2	2.2.2	(2)	例外措置の運用		
2.2	2.2.2	(2)	(a)	職員等は、定められた審査手続に従い、許可権限者に規定の例外措置の適用を申請 すること。ただし、業務の遂行に緊急を要し、当該規定の趣旨を充分尊重した扱いを 取ることができる場合であって、情報セキュリティ関係規程の規定とは異なる代替 の方法を直ちに採用すること又は規定されている方法を実施しないことが不可避の ときは、事後速やかに届け出ること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27001 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27001 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.2	2.2.2	(2)	(b)	許可権限者は、職員等による例外措置の適用の申請を、定められた審査手続に従っ て審査し、許可の可否を決定すること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールやGoogle 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフローツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定　の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud Platform のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。

2.2	2.2.2	(2)	(c)	許可権限者は、例外措置の申請状況を台帳に記録し、統括情報セキュリティ責任者 に報告すること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールやGoogle 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフローツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定　の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud Platform のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.2	2.2.2	(2)	(d)	統括情報セキュリティ責任者は、例外措置の申請状況を踏まえた情報セキュリテ ィ関係規程の追加又は見直しの検討を行い、最高情報セキュリティ責任者に報告す ること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27001 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27001 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.2	2.2.3	教育			
2.2	2.2.3	(1)	教育体制の整備・教育実施計画の策定		
2.2	2.2.3	(1)	(a)	統括情報セキュリティ責任者は、情報セキュリティ対策に係る教育について、対策 推進計画に基づき教育実施計画を策定し、その実施体制を整備すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO 27001 2013、附属書 A.7.2.2)が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の委託業者は初期研修でGoogle の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティチームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。
2.2	2.2.3	(1)	(b)	統括情報セキュリティ責任者は、情報セキュリティの状況の変化に応じ職員等に 対して新たに教育すべき事項が明らかになった場合は、教育実施計画を見直すこと。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO 27001 2013、附属書 A.7.2.2)が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の委託業者は初期研修でGoogle の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティチームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。
2.2	2.2.3	(2)	教育の実施		
2.2	2.2.3	(2)	(a)	課室情報セキュリティ責任者は、教育実施計画に基づき、職員等に対して、情報セ キュリティ関係規程に係る教育を適切に受講させること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO 27001 2013、附属書 A.7.2.2)が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の委託業者は初期研修でGoogle の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティチームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。
2.2	2.2.3	(2)	(b)	職員等は、教育実施計画に従って、適切な時期に教育を受講すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO 27001 2013、附属書 A.7.2.2)が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の委託業者は初期研修でGoogle の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティチームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。
2.2	2.2.3	(2)	(c)	課室情報セキュリティ責任者は、情報セキュリティ対策推進体制及びCSIRT に属 する職員等に教育を適切に受講させること。また、国の行政機関における課室情報セ キュリティ責任者は、CYMAT に属する職員にも教育を適切に受講させること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO 27001 2013、附属書 A.7.2.2)が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の委託業者は初期研修でGoogle の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティチームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。
2.2	2.2.3	(2)	(d)	課室情報セキュリティ責任者は、教育の実施状況を記録し、情報セキュリティ責任 者及び統括情報セキュリティ責任者に報告すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO 27001 2013、附属書 A.7.2.2)が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の委託業者は初期研修でGoogle の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティチームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。

2.2	2.2.3	(2)	(e)	統括情報セキュリティ責任者は、教育の実施状況を分析、評価し、最高情報セキュ リティ責任者に情報セキュリティ対策に関する教育の実施状況について報告するこ と。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO 27001 2013、附属書 A.7.2.2) が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の委託業者は初期研修でGoogle の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティチームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。
2.2	2.2.4	情報セキュリティインシデントへの対処			
2.2	2.2.4	(1)	情報セキュリティインシデントに備えた事前準備		
2.2	2.2.4	(1)	(a)	統括情報セキュリティ責任者は、情報セキュリティインシデントの可能性を認知 した際の報告窓口を含む機関等関係者への報告手順を整備し、報告が必要な具体例 を含め、職員等に周知すること。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」(ISO 27001 2013、附属書 A.12.2) が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。 Google では、情報セキュリティチームのメンバーがすべてのネットワーク、システム、サービスのセキュリティ計画を確認しています。このチームはGoogle のプロダクト チームやエンジニアリングチームにプロジェクトごとのコンサルティング サービスを行っています。このチームは、Google のネットワーク上の不審な動作を監視し、情報セキュリティ上の脅威に対処し、セキュリティ評価および監査を日常的に実施し、外部の専門家による定期的なセキュリティ評価を実施します。Google では「プロジェクト ゼロ」という専門チームを作りました。このチームは指定の攻撃を防ぐことを目的とし、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。
2.2	2.2.4	(1)	(b)	統括情報セキュリティ責任者は、情報セキュリティインシデントの可能性を認知 した際の機関等外との情報共有を含む対処手順を整備すること。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」(ISO 27001 2013、附属書 A.12.2) が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。 Google では、情報セキュリティチームのメンバーがすべてのネットワーク、システム、サービスのセキュリティ計画を確認しています。このチームはGoogle のプロダクト チームやエンジニアリングチームにプロジェクトごとのコンサルティング サービスを行っています。このチームは、Google のネットワーク上の不審な動作を監視し、情報セキュリティ上の脅威に対処し、セキュリティ評価および監査を日常的に実施し、外部の専門家による定期的なセキュリティ評価を実施します。Google では「プロジェクト ゼロ」という専門チームを作りました。このチームは指定の攻撃を防ぐことを目的とし、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。
2.2	2.2.4	(1)	(c)	統括情報セキュリティ責任者は、情報セキュリティインシデントに備え、業務の遂行のため特に重要と認めた情報システムについて、緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備すること。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」(ISO 27001 2013、附属書 A.12.2) が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。 Google では、情報セキュリティチームのメンバーがすべてのネットワーク、システム、サービスのセキュリティ計画を確認しています。このチームはGoogle のプロダクト チームやエンジニアリングチームにプロジェクトごとのコンサルティング サービスを行っています。このチームは、Google のネットワーク上の不審な動作を監視し、情報セキュリティ上の脅威に対処し、セキュリティ評価および監査を日常的に実施し、外部の専門家による定期的なセキュリティ評価を実施します。Google では「プロジェクト ゼロ」という専門チームを作りました。このチームは指定の攻撃を防ぐことを目的とし、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。

2.2	2.2.4	(1)	(d)	統括情報セキュリティ責任者は、情報セキュリティインシデントへの対処の訓練の必要性を検討し、業務の遂行のため特に重要と認めた情報システムについて、その 訓練の内容及び体制を整備すること。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」ISO 27001 2013、附属書 A. 12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。 Google では、情報セキュリティチームのメンバーがすべてのネットワーク、システム、サービスのセキュリティ計画を確認しています。このチームはGoogle のプロダクト チームやエンジニアリング チームにプロジェクトごとのコンサルティング サービスを行っています。このチームは、Google のネットワーク上の不審な動作を監視し、情報セキュリティ上の脅威に対処し、セキュリティ評価および監査を日常的に実施し、外部の専門家による定期的なセキュリティ評価を実施します。Google では「プロジェクト ゼロ」という専門チームを作りました。このチームは指定の攻撃を防ぐことを目的とし、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。
2.2	2.2.4	(1)	(e)	統括情報セキュリティ責任者は、情報セキュリティインシデントについて機関等外の者から報告を受けるための窓口を整備し、その窓口への連絡手段を機関等外の 者に明示すること。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」ISO 27001 2013、附属書 A. 12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。 Google では、情報セキュリティチームのメンバーがすべてのネットワーク、システム、サービスのセキュリティ計画を確認しています。このチームはGoogle のプロダクト チームやエンジニアリング チームにプロジェクトごとのコンサルティング サービスを行っています。このチームは、Google のネットワーク上の不審な動作を監視し、情報セキュリティ上の脅威に対処し、セキュリティ評価および監査を日常的に実施し、外部の専門家による定期的なセキュリティ評価を実施します。Google では「プロジェクト ゼロ」という専門チームを作りました。このチームは指定の攻撃を防ぐことを目的とし、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。
2.2	2.2.4	(1)	(f)	統括情報セキュリティ責任者は、対処手順が適切に機能することを訓練等により確認すること。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」ISO 27001 2013、附属書 A. 12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。 Google では、情報セキュリティチームのメンバーがすべてのネットワーク、システム、サービスのセキュリティ計画を確認しています。このチームはGoogle のプロダクト チームやエンジニアリング チームにプロジェクトごとのコンサルティング サービスを行っています。このチームは、Google のネットワーク上の不審な動作を監視し、情報セキュリティ上の脅威に対処し、セキュリティ評価および監査を日常的に実施し、外部の専門家による定期的なセキュリティ評価を実施します。Google では「プロジェクト ゼロ」という専門チームを作りました。このチームは指定の攻撃を防ぐことを目的とし、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。
2.2	2.2.4	(2)	情報セキュリティインシデントへの対処		
2.2	2.2.4	(2)	(a)	職員等は、情報セキュリティインシデントの可能性を認知した場合には、機関等の報告窓口に報告し、指示に従うこと。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」ISO 27001 2013、附属書 A. 12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。 Google では、情報セキュリティチームのメンバーがすべてのネットワーク、システム、サービスのセキュリティ計画を確認しています。このチームはGoogle のプロダクト チームやエンジニアリング チームにプロジェクトごとのコンサルティング サービスを行っています。このチームは、Google のネットワーク上の不審な動作を監視し、情報セキュリティ上の脅威に対処し、セキュリティ評価および監査を日常的に実施し、外部の専門家による定期的なセキュリティ評価を実施します。Google では「プロジェクト ゼロ」という専門チームを作りました。このチームは指定の攻撃を防ぐことを目的とし、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。

2.2	2.2.4	(2)	(b)	CSIRT は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行うこと。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」ISO 27001 2013、附属書 A. 12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。 Google では、情報セキュリティチームのメンバーがすべてのネットワーク、システム、サービスのセキュリティ計画を確認しています。このチームはGoogle のプロダクト チームやエンジニアリングチームにプロジェクトごとのコンサルティング サービスを行っています。このチームは、Google のネットワーク上の不審な動作を監視し、情報セキュリティ上の脅威に対処し、セキュリティ評価および監査を日常的に実施し、外部の専門家による定期的なセキュリティ評価を実施します。Google では「プロジェクト ゼロ」という専門チームを作りました。このチームは指定の攻撃を防ぐことを目的とし、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。
2.2	2.2.4	(2)	(c)	CSIRT 責任者は、情報セキュリティインシデントであると評価した場合、最高情報セキュリティ責任者に速やかに報告すること。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」ISO 27001 2013、附属書 A. 12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。 Google では、情報セキュリティチームのメンバーがすべてのネットワーク、システム、サービスのセキュリティ計画を確認しています。このチームはGoogle のプロダクト チームやエンジニアリングチームにプロジェクトごとのコンサルティング サービスを行っています。このチームは、Google のネットワーク上の不審な動作を監視し、情報セキュリティ上の脅威に対処し、セキュリティ評価および監査を日常的に実施し、外部の専門家による定期的なセキュリティ評価を実施します。Google では「プロジェクト ゼロ」という専門チームを作りました。このチームは指定の攻撃を防ぐことを目的とし、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。
2.2	2.2.4	(2)	(d)	CSIRT は、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示又は勧告 を行うこと。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」ISO 27001 2013、附属書 A. 12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。 Google では、情報セキュリティチームのメンバーがすべてのネットワーク、システム、サービスのセキュリティ計画を確認しています。このチームはGoogle のプロダクト チームやエンジニアリングチームにプロジェクトごとのコンサルティング サービスを行っています。このチームは、Google のネットワーク上の不審な動作を監視し、情報セキュリティ上の脅威に対処し、セキュリティ評価および監査を日常的に実施し、外部の専門家による定期的なセキュリティ評価を実施します。Google では「プロジェクト ゼロ」という専門チームを作りました。このチームは指定の攻撃を防ぐことを目的とし、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。
2.2	2.2.4	(2)	(e)	情報システムセキュリティ責任者は、所管する情報システムについて情報セキュリティインシデントを認知した場合には、機関等で定められた対処手順又はCSIRT の指示若しくは勧告に従って、適切に対処すること。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」ISO 27001 2013、附属書 A. 12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。 Google では、情報セキュリティチームのメンバーがすべてのネットワーク、システム、サービスのセキュリティ計画を確認しています。このチームはGoogle のプロダクト チームやエンジニアリングチームにプロジェクトごとのコンサルティング サービスを行っています。このチームは、Google のネットワーク上の不審な動作を監視し、情報セキュリティ上の脅威に対処し、セキュリティ評価および監査を日常的に実施し、外部の専門家による定期的なセキュリティ評価を実施します。Google では「プロジェクト ゼロ」という専門チームを作りました。このチームは指定の攻撃を防ぐことを目的とし、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。

2.2	2.2.4	(2)	(f)	情報システムセキュリティ責任者は、認知した情報セキュリティインシデントが基盤となる情報システムに関するものであり、当該基盤となる情報システムの情報セキュリティ対策に係る運用管理規程等が定められている場合には、当該運用管理規程等に従い、適切に対処すること。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」(ISO 27001 2013、附属書 A. 12.2)が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。 Google では、情報セキュリティチームのメンバーがすべてのネットワーク、システム、サービスのセキュリティ計画を確認しています。このチームはGoogle のプロダクト チームやエンジニアリングチームにプロジェクトごとのコンサルティング サービスを行っています。このチームは、Google のネットワーク上の不審な動作を監視し、情報セキュリティ上の脅威に対処し、セキュリティ評価および監査を日常的に実施し、外部の専門家による定期的なセキュリティ評価を実施します。Google では「プロジェクト ゼロ」という専門チームを作りました。このチームは指定の攻撃を防ぐことを目的とし、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。
2.2	2.2.4	(2)	(g)	国の行政機関におけるCSIRT は、当該機関の情報システムにおいて、情報セキュリティインシデントを認知した場合には、当該事象について速やかに、内閣官房内閣 サイバーセキュリティセンターに連絡すること。また、独立行政法人及び指定法人におけるCSIRT は、当該法人の情報システムにおいて、情報セキュリティインシデントを認知した場合には、当該事象について速やかに、当該法人を所管する国の行政機関に連絡すること。この連絡を受けた国の行政機関におけるCSIRT は、当該事象に ついて速やかに、内閣官房内閣サイバーセキュリティセンターに連絡すること。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」(ISO 27001 2013、附属書 A. 12.2)が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。 Google では、情報セキュリティチームのメンバーがすべてのネットワーク、システム、サービスのセキュリティ計画を確認しています。このチームはGoogle のプロダクト チームやエンジニアリングチームにプロジェクトごとのコンサルティング サービスを行っています。このチームは、Google のネットワーク上の不審な動作を監視し、情報セキュリティ上の脅威に対処し、セキュリティ評価および監査を日常的に実施し、外部の専門家による定期的なセキュリティ評価を実施します。Google では「プロジェクト ゼロ」という専門チームを作りました。このチームは指定の攻撃を防ぐことを目的とし、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。
2.2	2.2.4	(2)	(h)	CSIRT は、認知した情報セキュリティインシデントがサイバー攻撃又はそのおそれのあるものである場合には、当該情報セキュリティインシデントの内容に応じ、警察への通報・連絡等を行うこと。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」(ISO 27001 2013、附属書 A. 12.2)が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。 Google では、情報セキュリティチームのメンバーがすべてのネットワーク、システム、サービスのセキュリティ計画を確認しています。このチームはGoogle のプロダクト チームやエンジニアリングチームにプロジェクトごとのコンサルティング サービスを行っています。このチームは、Google のネットワーク上の不審な動作を監視し、情報セキュリティ上の脅威に対処し、セキュリティ評価および監査を日常的に実施し、外部の専門家による定期的なセキュリティ評価を実施します。Google では「プロジェクト ゼロ」という専門チームを作りました。このチームは指定の攻撃を防ぐことを目的とし、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。
2.2	2.2.4	(2)	(i)	国の行政機関におけるCSIRT は、認知した情報セキュリティインシデント又は独立行政法人及び指定法人から連絡を受けた情報セキュリティインシデントが、国民の生命、身体、財産若しくは国土に重大な被害が生じ、若しくは生じるおそれのある大規模サイバー攻撃事態又はその可能性がある事態である場合には、「大規模サイバー攻撃事態等への初動対処について（平成22 年3月19 日内閣危機管理監決裁）」に基づく報告連絡を行うこと。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」(ISO 27001 2013、附属書 A. 12.2)が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。 Google では、情報セキュリティチームのメンバーがすべてのネットワーク、システム、サービスのセキュリティ計画を確認しています。このチームはGoogle のプロダクト チームやエンジニアリングチームにプロジェクトごとのコンサルティング サービスを行っています。このチームは、Google のネットワーク上の不審な動作を監視し、情報セキュリティ上の脅威に対処し、セキュリティ評価および監査を日常的に実施し、外部の専門家による定期的なセキュリティ評価を実施します。Google では「プロジェクト ゼロ」という専門チームを作りました。このチームは指定の攻撃を防ぐことを目的とし、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。

2.2	2.2.4	(2)	(j)	CSIRT は、情報セキュリティインシデントに関する対処状況を把握し、必要に応 じて対処全般に関する指示、勧告又は助言を行うこと。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」(ISO 27001 2013、附属書 A.12.2)が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。 Google では、情報セキュリティチームのメンバーがすべてのネットワーク、システム、サービスのセキュリティ計画を確認しています。このチームはGoogle のプロダクト チームやエンジニアリング チームにプロジェクトごとのコンサルティング サービスを行っています。このチームは、Google のネットワーク上の不審な動作を監視し、情報セキュリティ上の脅威に対処し、セキュリティ評価および監査を日常的に実施し、外部の専門家による定期的なセキュリティ評価を実施します。Google では「プロジェクト ゼロ」という専門チームを作りました。このチームは指定の攻撃を防ぐことを目的とし、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。
2.2	2.2.4	(2)	(k)	CSIRT は、情報セキュリティインシデントに関する対処の内容を記録すること。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」(ISO 27001 2013、附属書 A.12.2)が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。 Google では、情報セキュリティチームのメンバーがすべてのネットワーク、システム、サービスのセキュリティ計画を確認しています。このチームはGoogle のプロダクト チームやエンジニアリング チームにプロジェクトごとのコンサルティング サービスを行っています。このチームは、Google のネットワーク上の不審な動作を監視し、情報セキュリティ上の脅威に対処し、セキュリティ評価および監査を日常的に実施し、外部の専門家による定期的なセキュリティ評価を実施します。Google では「プロジェクト ゼロ」という専門チームを作りました。このチームは指定の攻撃を防ぐことを目的とし、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。
2.2	2.2.4	(2)	(l)	CSIRT は、情報セキュリティインシデントに関して、機関等を含む関係機関と情報共有を行うこと。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」(ISO 27001 2013、附属書 A.12.2)が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。 Google では、情報セキュリティチームのメンバーがすべてのネットワーク、システム、サービスのセキュリティ計画を確認しています。このチームはGoogle のプロダクト チームやエンジニアリング チームにプロジェクトごとのコンサルティング サービスを行っています。このチームは、Google のネットワーク上の不審な動作を監視し、情報セキュリティ上の脅威に対処し、セキュリティ評価および監査を日常的に実施し、外部の専門家による定期的なセキュリティ評価を実施します。Google では「プロジェクト ゼロ」という専門チームを作りました。このチームは指定の攻撃を防ぐことを目的とし、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。

2.2	2.2.4	(2)	(m)	CSIRT は、CYMAT の支援を受ける場合には、支援を受けるに当たって必要な情報提供を行うこと。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」ISO 27001 2013、附属書 A. 12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。 Google では、情報セキュリティチームのメンバーがすべてのネットワーク、システム、サービスのセキュリティ計画を確認しています。このチームはGoogle のプロダクト チームやエンジニアリング チームにプロジェクトごとのコンサルティング サービスを行っています。このチームは、Google のネットワーク上の不審な動作を監視し、情報セキュリティ上の脅威に対処し、セキュリティ評価および監査を日常的に実施し、外部の専門家による定期的なセキュリティ評価を実施します。Google では「プロジェクト ゼロ」という専門チームを作りました。このチームは指定の攻撃を防ぐことを目的とし、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。
2.2	2.2.4	(3)	情報セキュリティインシデントの再発防止・教訓の共有		
2.2	2.2.4	(3)	(a)	情報セキュリティ責任者は、CSIRT から応急措置の実施及び復旧に係る指示又は勧告を受けた場合は、当該指示又は勧告を踏まえ、情報セキュリティインシデントの原因を調査するとともに再発防止策を検討し、それを報告書として最高情報セキュリティ責任者に報告すること。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」ISO 27001 2013、附属書 A. 12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。 Google では、情報セキュリティチームのメンバーがすべてのネットワーク、システム、サービスのセキュリティ計画を確認しています。このチームはGoogle のプロダクト チームやエンジニアリング チームにプロジェクトごとのコンサルティング サービスを行っています。このチームは、Google のネットワーク上の不審な動作を監視し、情報セキュリティ上の脅威に対処し、セキュリティ評価および監査を日常的に実施し、外部の専門家による定期的なセキュリティ評価を実施します。Google では「プロジェクト ゼロ」という専門チームを作りました。このチームは指定の攻撃を防ぐことを目的とし、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。
2.2	2.2.4	(3)	(b)	最高情報セキュリティ責任者は、情報セキュリティ責任者から情報セキュリティインシデントについての報告を受けた場合には、その内容を確認し、再発防止策を実施するために必要な措置を指示すること。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」ISO 27001 2013、附属書 A. 12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。 Google では、情報セキュリティチームのメンバーがすべてのネットワーク、システム、サービスのセキュリティ計画を確認しています。このチームはGoogle のプロダクト チームやエンジニアリング チームにプロジェクトごとのコンサルティング サービスを行っています。このチームは、Google のネットワーク上の不審な動作を監視し、情報セキュリティ上の脅威に対処し、セキュリティ評価および監査を日常的に実施し、外部の専門家による定期的なセキュリティ評価を実施します。Google では「プロジェクト ゼロ」という専門チームを作りました。このチームは指定の攻撃を防ぐことを目的とし、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。
2.2	2.2.4	(3)	(c)	CSIRT 責任者は、情報セキュリティインシデント対処の結果から得られた教訓を、統括情報セキュリティ責任者、関係する情報セキュリティ責任者等に共有すること。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」ISO 27001 2013、附属書 A. 12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。 Google では、情報セキュリティチームのメンバーがすべてのネットワーク、システム、サービスのセキュリティ計画を確認しています。このチームはGoogle のプロダクト チームやエンジニアリング チームにプロジェクトごとのコンサルティング サービスを行っています。このチームは、Google のネットワーク上の不審な動作を監視し、情報セキュリティ上の脅威に対処し、セキュリティ評価および監査を日常的に実施し、外部の専門家による定期的なセキュリティ評価を実施します。Google では「プロジェクト ゼロ」という専門チームを作りました。このチームは指定の攻撃を防ぐことを目的とし、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。
2.3	点検				
2.3	2.3.1	情報セキュリティ対策の自己点検			

2.3	2.3.1	(1)		自己点検計画の策定・手順の準備	
2.3	2.3.1	(1)	(a)	統括情報セキュリティ責任者は、対策推進計画に基づき年度自己点検計画を策定すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」（ISO27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全社員は、入社時研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新入社員は入社時研修でGoogle の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティチームに配属されたエンジニアは、安全なコーディング方法、プロダクト設 計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。 Google Cloud Platform のお客様は、運用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.3	2.3.1	(1)	(b)	情報セキュリティ責任者は、年度自己点検計画に基づき、職員等ごとの自己点検票及び自己点検の実施手順を整備すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」（ISO27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全社員は、入社時研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新入社員は入社時研修でGoogle の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティチームに配属されたエンジニアは、安全なコーディング方法、プロダクト設 計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。 Google Cloud Platform のお客様は、運用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.3	2.3.1	(1)	(c)	統括情報セキュリティ責任者は、情報セキュリティの状況の変化に応じ、職員等に対して新たに点検すべき事項が明らかになった場合は、年度自己点検計画を見直すこと。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」（ISO27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全社員は、入社時研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新入社員は入社時研修でGoogle の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティチームに配属されたエンジニアは、安全なコーディング方法、プロダクト設 計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。 Google Cloud Platform のお客様は、運用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.3	2.3.1	(2)		自己点検の実施	
2.3	2.3.1	(2)	(a)	情報セキュリティ責任者は、年度自己点検計画に基づき、職員等に自己点検の実施を指示すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」（ISO27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全社員は、入社時研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新入社員は入社時研修でGoogle の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティチームに配属されたエンジニアは、安全なコーディング方法、プロダクト設 計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。 Google Cloud Platform のお客様は、運用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.3	2.3.1	(2)	(b)	職員等は、情報セキュリティ責任者から指示された自己点検票及び自己点検の手順を用いて自己点検を実施すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」（ISO27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全社員は、入社時研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新入社員は入社時研修でGoogle の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティチームに配属されたエンジニアは、安全なコーディング方法、プロダクト設 計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。 Google Cloud Platform のお客様は、運用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.3	2.3.1	(3)		自己点検結果の評価・改善	
2.3	2.3.1	(3)	(a)	情報セキュリティ責任者は、自己点検結果について、自らが担当する組織のまとまり特有の課題の有無を確認するなどの観点から自己点検結果を分析、評価すること。 また、評価結果を統括情報セキュリティ責任者に報告すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」（ISO27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全社員は、入社時研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新入社員は入社時研修でGoogle の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティチームに配属されたエンジニアは、安全なコーディング方法、プロダクト設 計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。 Google Cloud Platform のお客様は、運用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。
		(3)	(b)	統括情報セキュリティ責任者は、機関等に共通の課題の有無を確認するなどの観点から自己点検結果を分析、評価すること。また、評価結果を最高情報セキュリティ責任者に報告すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」（ISO27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全社員は、入社時研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新入社員は入社時研修でGoogle の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティチームに配属されたエンジニアは、安全なコーディング方法、プロダクト設 計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。 Google Cloud Platform のお客様は、運用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。

2.3	2.3.1	(3)	(c)	最高情報セキュリティ責任者は、自己点検結果を全体として評価し、自己点検の結果により明らかになった問題点について、統括情報セキュリティ責任者及び情報セキュリティ責任者に改善を指示し、改善結果の報告を受けること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」（ISO27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全社員は、入社時研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新入社員は入社時研修でGoogle の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティチームに配属されたエンジニアは、安全なコーディング方法、プロダクト設 計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。 Google Cloud Platform のお客様は、運用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.3	2.3.2	情報セキュリティ監査			
2.3	2.3.2	(1)	監査実施計画の策定		
2.3	2.3.2	(1)	(a)	情報セキュリティ監査責任者は、対策推進計画に基づき監査実施計画を定めること。	Google は ISO27001 認証を受けています。この基準では、「情報システムの監査に対する考慮事項」ISO 27001 2013、附属書 A.12.7）が規定されています。 情報セキュリティの監督管理体制は、社内監査の監督など、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。
2.3	2.3.2	(1)	(b)	情報セキュリティ監査責任者は、情報セキュリティの状況の変化に応じ、対策推進計画で計画された以外の監査の実施が必要な場合には、追加の監査実施計画を定めること。	Google は ISO27001 認証を受けています。この基準では、「情報システムの監査に対する考慮事項」ISO 27001 2013、附属書 A.12.7）が規定されています。 情報セキュリティの監督管理体制は、社内監査の監督など、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。
2.3	2.3.2	(2)	監査の実施		
2.3	2.3.2	(2)	(a)	情報セキュリティ監査責任者は、監査実施計画に基づき、以下の事項を含む監査の実施を監査実施者に指示し、結果を監査報告書として最高情報セキュリティ責任者に報告すること。	Google は ISO27001 認証を受けています。この基準では、「情報システムの監査に対する考慮事項」ISO 27001 2013、附属書 A.12.7）が規定されています。 情報セキュリティの監督管理体制は、社内監査の監督など、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。
2.3	2.3.2	(2)	(a)	(ア) 対策基準に統一基準を満たすための適切な事項が定められていること	Google は ISO27001 認証を受けています。この基準では、「情報システムの監査に対する考慮事項」ISO 27001 2013、附属書 A.12.7）が規定されています。 情報セキュリティの監督管理体制は、社内監査の監督など、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。
2.3	2.3.2	(2)	(a)	(イ) 実施手順が対策基準に準拠していること	Google は ISO27001 認証を受けています。この基準では、「情報システムの監査に対する考慮事項」ISO 27001 2013、附属書 A.12.7）が規定されています。 情報セキュリティの監督管理体制は、社内監査の監督など、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。
2.3	2.3.2	(2)	(a)	(ウ) 被監査部門における実際の運用が情報セキュリティ関係規程に準拠していること	Google は ISO27001 認証を受けています。この基準では、「情報システムの監査に対する考慮事項」ISO 27001 2013、附属書 A.12.7）が規定されています。 情報セキュリティの監督管理体制は、社内監査の監督など、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。
2.3	2.3.2	(3)	監査結果に応じた対処		
2.3	2.3.2	(3)	(a)	最高情報セキュリティ責任者は、監査報告書の内容を踏まえ、指摘事項に対する改善計画の策定等を統括情報セキュリティ責任者及び情報セキュリティ責任者に指示すること。	Google は ISO27001 認証を受けています。この基準では、「情報システムの監査に対する考慮事項」ISO 27001 2013、附属書 A.12.7）が規定されています。 情報セキュリティの監督管理体制は、社内監査の監督など、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。

2.3	2.3.2	(3)	(b)	統括情報セキュリティ責任者は、最高情報セキュリティ責任者からの改善の指示のうち、機関等内で横断的に改善が必要な事項について、必要な措置を行った上で改 善計画を策定し、措置結果及び改善計画を最高情報セキュリティ責任者に報告すること。	Google は ISO27001 認証を受けています。この基準では、「情報システムの監査に対する考慮事項」(ISO 27001 2013、附属書 A.12.7）が規定されています。 情報セキュリティの監督管理体制は、社内監査の監督など、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。
2.3	2.3.2	(3)	(c)	情報セキュリティ責任者は、最高情報セキュリティ責任者からの改善の指示のうち、自らが担当する組織のまとまりに特有な改善が必要な事項について、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を最高情報セキュリティ責任者に報告すること。	Google は ISO27001 認証を受けています。この基準では、「情報システムの監査に対する考慮事項」(ISO 27001 2013、附属書 A.12.7）が規定されています。 情報セキュリティの監督管理体制は、社内監査の監督など、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。
2.4	見直し				
2.4	2.4.1	情報セキュリティ対策の見直し			
2.4	2.4.1	(1)	情報セキュリティ関係規程の見直し		
2.4	2.4.1	(1)	(a)	最高情報セキュリティ責任者は、情報セキュリティの運用及び自己点検・監査等の結果等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報セキュリティ委員会の審議を経て、対策基準について必要な見直しを行うこと。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27001 2013、附属書 A.5）と「情報セキュリティのための組織」(ISO27001 2013、附属書 A.6）が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.4	2.4.1	(1)	(b)	統括情報セキュリティ責任者は、情報セキュリティの運用及び自己点検・監査等の結果等を踏まえて情報セキュリティ対策に関する実施手順を見直し、又は整備した 者に対して規定の見直しを指示し、見直し結果について最高情報セキュリティ責任者に報告すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27001 2013、附属書 A.5）と「情報セキュリティのための組織」(ISO27001 2013、附属書 A.6）が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
2.4	2.4.1	(2)	対策推進計画の見直し		
2.4	2.4.1	(2)	(a)	最高情報セキュリティ責任者は、情報セキュリティ対策の運用及び点検・監査等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報セキュリティ委員会の審議を経て、対策推進計画について定期的な見直しを行うこと。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27001 2013、附属書 A.5）と「情報セキュリティのための組織」(ISO27001 2013、附属書 A.6）が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
情報の取扱い					
3.1	情報の取扱い				
3.1	3.1.1	情報の取扱い			
3.1	3.1.1	(1)	情報の取扱いに係る規定の整備		
3.1	3.1.1	(1)	(a)	統括情報セキュリティ責任者は、以下を含む情報の取扱いに関する規定を整備し、職員等へ周知すること。	―
3.1	3.1.1	(1)	(a)	(ア) 情報の格付及び取扱制限についての定義	―
3.1	3.1.1	(1)	(a)	(イ) 情報の格付及び取扱制限の明示等についての手続	―
3.1	3.1.1	(1)	(a)	(ウ) 情報の格付及び取扱制限の継承、見直しに関する手続	―
3.1	3.1.1	(2)	情報の目的外での利用等の禁止		
3.1	3.1.1	(2)	(a)	職員等は、自らが担当している業務の遂行のために必要な範囲に限って、情報を利用等すること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られたGoogle 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールやGoogle 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合はGoogle のセキュリティポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフローツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定はGoogle Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポートサービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されますGoogle 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud Platform のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。
3.1	3.1.1	(3)	情報の格付及び取扱制限の決定・明示等		
3.1	3.1.1	(3)	(a)	職員等は、情報の作成時及び機関等外の者が作成した情報を入手したことに伴う管理の開始時に、格付及び取扱制限の定義に基づき格付及び取扱制限を決定し、明示等すること。	―
3.1	3.1.1	(3)	(b)	職員等は、情報を作成又は複製する際に、参照した情報又は入手した情報に既に格付及び取扱制限の決定がなされている場合には、元となる情報の機密性に係る格付及び取扱制限を継承すること。	―
3.1	3.1.1	(3)	(c)	職員等は、修正、追加、削除その他の理由により、情報の格付及び取扱制限を見直す必要があると考える場合には、情報の格付及び取扱制限の決定者（決定を引き継いだ者を含む。）又は決定者の上司（以下本款において「決定者等」という。）に確認し、その結果に基づき見直すこと。	―
3.1	3.1.1	(4)	情報の利用・保存		

3.1	3.1.1	(4)	(a)	職員等は、利用する情報に明示等された格付及び取扱制限に従い、当該情報を適切に取り扱うこと。	ー
3.1	3.1.1	(4)	(b)	職員等は、機密性3情報について要管理対策区域外で情報処理を行う場合は、情報システムセキュリティ責任者及び課室情報セキュリティ責任者の許可を得ること。	ー
3.1	3.1.1	(4)	(c)	職員等は、要保護情報について要管理対策区域外で情報処理を行う場合は、必要な安全管理措置を講ずること。	ー
3.1	3.1.1	(4)	(d)	職員等は、保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理すること。なお、独立行政法人及び指定法人における職員等は、機密性3情報を機器等に保存する際、以下の措置を講ずること。 (ア) 機器等に保存する場合は、インターネットや、インターネットに接点を有する情報システムに接続しない端末、サーバ装置等の機器等を使用すること。 (イ) 当該情報に対し、暗号化による保護を行うこと。 (ウ) 当該情報を保存した機器等について、盗難及び不正な持ち出し等の物理的な脅威から保護するための対策を講ずること。	Google は ISO27001 認証を受けています。この基準では、「暗号」(ISO 27001 2013、附属書 A.10)が規定されています。 アップロード、作成されたお客様のデータを暗号化しています。Googleでは複数の暗号化レイヤを使用してデータを保護しています。複数の暗号化レイヤを使用することにより、冗長データ保護機能が追加され、アプリケーションの要件に基づいて最適な手法を選択できるようになります。 Google は、Google Cloud プロダクトと G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud Platform のお客様は、適切な暗号化対策の開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。
3.1	3.1.1	(4)	(e)	職員等は、USB メモリ等の外部電磁的記録媒体を用いて情報を取り扱う際、定められた利用手順に従うこと。	ー
3.1	3.1.1	(5)	情報の提供・公表		
3.1	3.1.1	(5)	(a)	職員等は、情報を公表する場合には、当該情報が機密性1情報に格付されるものであることを確認すること。	ー
3.1	3.1.1	(5)	(b)	職員等は、閲覧制限の範囲外の者に情報を提供する必要が生じた場合は、当該格付及び取扱制限の決定者等に相談し、その決定に従うこと。また、提供先において、当該情報に付された格付及び取扱制限に応じて適切に取り扱われるよう、取扱い上の留意事項を確実に伝達するなどの措置を講ずること。	ー
3.1	3.1.1	(5)	(c)	独立行政法人及び指定法人における職員等は、機密性3情報を閲覧制限の範囲外の者に提供する場合には、課室情報セキュリティ責任者の許可を得ること。	ー
3.1	3.1.1	(5)	(d)	職員等は、電磁的記録を提供又は公表する場合には、当該電磁的記録等からの不用意な情報漏えいを防止するための措置を講ずること。	ー
3.1	3.1.1	(6)	情報の運搬・送信		
3.1	3.1.1	(6)	(a)	職員等は、要保護情報が記録又は記載された記録媒体を要管理対策区域外に持ち出す場合には、安全確保に留意して運搬方法を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。独立行政法人及び指定法人における職員等が、機密性3情報を要管理対策区域外に持ち出す場合には、暗号化措置を施した上で、課室情報セキュリティ責任者が指定する方法により運搬すること。ただし、他機関等の要管理対策区域であって、統括情報セキュリティ責任者があらかじめ定めた区域のみに持ち出す場合は、当該区域を要管理対策区域とみなすことができる。	Google は ISO27001 認証を受けています。この基準では、「暗号」(ISO 27001 2013、附属書 A.10)が規定されています。 インターネットを介した認証と管理者アクセスを保護するために暗号化を使用しています。Googleが管理するマシンにリモートアクセスする場合は、Googleが発行したデジタル証明書と2要素認証を必要とします。 Google は、Google Cloud プロダクトと G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud Platform のお客様は、適切な暗号化対策の開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。
3.1	3.1.1	(6)	(b)	職員等は、要保護情報である電磁的記録を電子メール等で送信する場合には、安全確保に留意して送信の手段を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。独立行政法人及び指定法人における職員等が、機密性3情報を機関等外通信回線（インターネットを除く。）を使用して送信する場合には、暗号化措置を施した上で、課室情報セキュリティ責任者が指定する方法により送信すること。	Google は ISO27001 認証を受けています。この基準では、「暗号」(ISO 27001 2013、附属書 A.10)が規定されています。 インターネットを介した認証と管理者アクセスを保護するために暗号化を使用しています。Googleが管理するマシンにリモートアクセスする場合は、Googleが発行したデジタル証明書と2要素認証を必要とします。 Google は、Google Cloud プロダクトと G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud Platform のお客様は、適切な暗号化対策の開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。
3.1	3.1.1	(7)	情報の消去		
3.1	3.1.1	(7)	(a)	職員等は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去すること。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」(ISO 27001 2013、附属書 A.8.3.2)と「装置のセキュリティを保った処分または再利用」(ISO 27001 2013、附属書 A.11.2.7)が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する 際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。
3.1	3.1.1	(7)	(b)	職員等は、電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消すること。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」(ISO 27001 2013、附属書 A.8.3.2)と「装置のセキュリティを保った処分または再利用」(ISO 27001 2013、附属書 A.11.2.7)が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する 際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。
3.1	3.1.1	(7)	(c)	職員等は、要機密情報である書面を廃棄する場合には、復元が困難な状態にすること。	ー
3.1	3.1.1	(8)	情報のバックアップ		

3.1	3.1.1	(8)	(a)	職員等は、情報の格付に応じて、適切な方法で情報のバックアップを実施すること。	Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001 2013、附属書 A.17.2)と「バックアップ」(ISO27001 2013、附属書 A.12.3)が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェアサービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud Platform のお客様は、データファイル管理をサポートするプロセスの開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。
3.1	3.1.1	(8)	(b)	職員等は、取得した情報のバックアップについて、格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め、適切に管理すること。	Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001 2013、附属書 A.17.2)と「バックアップ」(ISO27001 2013、附属書 A.12.3)が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェアサービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud Platform のお客様は、データファイル管理をサポートするプロセスの開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。
3.1	3.1.1	(8)	(c)	職員等は、保存期間を過ぎた情報のバックアップについては、前条の規定に従い、適切な方法で消去、抹消又は廃棄すること。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」(ISO 27001 2013、附属書 A.8.3.2)と「装置のセキュリティを保った処分または再利用」(ISO 27001 2013、附属書 A.11.2.7)が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する 際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。
3.2	情報を取り扱う区域の管理				
3.2	3.2.1	情報を取り扱う区域の管理			
3.2	3.2.1	(1)	要管理対策区域における対策の基準の決定		
3.2	3.2.1	(1)	(a)	統括情報セキュリティ責任者は、要管理対策区域の範囲を定めること。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティモデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 Google のデータセンタープロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画https://www.youtube.com/watch?v=XZmGGAbHqa0
3.2	3.2.1	(1)	(b)	統括情報セキュリティ責任者は、要管理対策区域の特性に応じて、以下の観点を含む対策の基準を定めること。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティモデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア(データ サーバー フロアなど)に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティバッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティエリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンタープロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0

3.2	3.2.1	(1)	(b)	(ア) 許可されていない者が容易に立ち入ることができないようにするための、施錠可能な扉、間仕切り等の施設の整備、設備の設置等の物理的な対策。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティモデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティバッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティエリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンタープロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0
3.2	3.2.1	(1)	(b)	(イ) 許可されていない者の立入りを制限するため及び立入りを許可された者による立入り時の不正な行為を防止するための入退管理対策。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティモデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティバッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティエリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンタープロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0
3.2	3.2.1	(2)	区域ごとの対策の決定		
3.2	3.2.1	(2)	(a)	情報セキュリティ責任者は、統括情報セキュリティ責任者が定めた対策の基準を踏まえ、施設及び執務環境に係る対策を行う単位ごとの区域を定めること。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティモデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 Google のデータセンタープロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画https://www.youtube.com/watch?v=XZmGGAbHqa0
3.2	3.2.1	(2)	(b)	区域情報セキュリティ責任者は、管理する区域について、統括情報セキュリティ責任者が定めた対策の基準と、周辺環境や当該区域で行う行政事務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定すること。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティモデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 Google のデータセンタープロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画https://www.youtube.com/watch?v=XZmGGAbHqa0
3.2	3.2.1	(3)	要管理対策区域における対策の実施		
3.2	3.2.1	(3)	(a)	区域情報セキュリティ責任者は、管理する区域に対して定めた対策を実施すること。職員等が実施すべき対策については、職員等が認識できる措置を講ずること。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティモデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 Google のデータセンタープロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画https://www.youtube.com/watch?v=XZmGGAbHqa0

3.2	3.2.1	(3)	(b)	区域情報セキュリティ責任者は、災害から要安定情報を取り扱う情報システムを保護するために物理的な対策を講ずること。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性はGoogle のサーバー設計、データ保存方　法、ネットワークやインターネットの接続性、さらにソフトウェアサービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google は、データセンターが所在するリージョンの建築要件と設備要件をすべて満たしています。
3.2	3.2.1	(3)	(c)	職員等は、利用する区域について区域情報セキュリティ責任者が定めた対策に従って利用すること。また、職員等が機関等外の者を立ち入らせる際には、当該機関等 外の者にも当該区域で定められた対策に従って利用させること。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティモデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 Google のデータセンタープロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー　https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画https://www.youtube.com/watch?v=XZmGGAbHqa0
外部委託					
4.1	外部委託				
4.1	4.1.1	外部委託			
4.1	4.1.1	(1)	外部委託に係る規定の整備		
4.1	4.1.1	(1)	(a)	統括情報セキュリティ責任者は、外部委託に係る以下の内容を含む規定を整備すること。	Google は ISO27001 認証を受けています。この基準では、「供給者関係」(ISO 27001 2013、附属書 A.15)が規定されています。 情報セキュリティの監督管理体制は、セキュリティに対するベンダーの取り組みなど、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google では、サービス実施のためのほぼすべてのデータ処理を直接行っています。ただしGoogle は顧客サポートやテクニカル サポートなど、Cloud Platform に関連するサービスを提供するためサードパーティサプライヤーを利用すること があります。サードパーティサプライヤーと提携する前に、Google はサードパーティサプライヤーのセキュリティおよびプライバシー対策について評価を行います。これにより、データへのアクセスや、担当するサービスの範囲に適した水準のセキュリティやプライバシーが確保されていることを確認しますGoogle はサードパーティサプライヤーに付随するリスクを評価した上で、所定のセキュリティ、機密保持、プライバシーの各契約を締結することをサプライヤーに義務付けています。
4.1	4.1.1	(1)	(a)	(ア)委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準(以下本款において「委託判断基準」という。)	Google は ISO27001 認証を受けています。この基準では、「供給者関係」(ISO 27001 2013、附属書 A.15)が規定されています。 情報セキュリティの監督管理体制は、セキュリティに対するベンダーの取り組みなど、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google では、サービス実施のためのほぼすべてのデータ処理を直接行っています。ただしGoogle は顧客サポートやテクニカル サポートなど、Cloud Platform に関連するサービスを提供するためサードパーティサプライヤーを利用すること があります。サードパーティサプライヤーと提携する前に、Google はサードパーティサプライヤーのセキュリティおよびプライバシー対策について評価を行います。これにより、データへのアクセスや、担当するサービスの範囲に適した水準のセキュリティやプライバシーが確保されていることを確認しますGoogle はサードパーティサプライヤーに付随するリスクを評価した上で、所定のセキュリティ、機密保持、プライバシーの各契約を締結することをサプライヤーに義務付けています。
4.1	4.1.1	(1)	(a)	(イ)委託先の選定基準	Google は ISO27001 認証を受けています。この基準では、「供給者関係」(ISO 27001 2013、附属書 A.15)が規定されています。 情報セキュリティの監督管理体制は、セキュリティに対するベンダーの取り組みなど、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google では、サービス実施のためのほぼすべてのデータ処理を直接行っています。ただしGoogle は顧客サポートやテクニカル サポートなど、Cloud Platform に関連するサービスを提供するためサードパーティサプライヤーを利用すること があります。サードパーティサプライヤーと提携する前に、Google はサードパーティサプライヤーのセキュリティおよびプライバシー対策について評価を行います。これにより、データへのアクセスや、担当するサービスの範囲に適した水準のセキュリティやプライバシーが確保されていることを確認しますGoogle はサードパーティサプライヤーに付随するリスクを評価した上で、所定のセキュリティ、機密保持、プライバシーの各契約を締結することをサプライヤーに義務付けています。
4.1	4.1.1	(2)	外部委託に係る契約		
4.1	4.1.1	(2)	(a)	情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託判断基準に従って外部委託を実施すること。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。機密保持に関する統制についても、第三者機関によるレビューと検証を受け SOC 2、Type II の報告書を取得しています。 詳しくは、契約上の義務や契約内容をまとめたGoogle の利用規約とSLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://gsuite.google.com/terms/2013/1/premier_terms.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
4.1	4.1.1	(2)	(b)	情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部委託を実施する際には、選定基準及び選定手続に従って委託先を選定すること。また、以 下の内容を含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様内容にも含めること。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。機密保持に関する統制についても、第三者機関によるレビューと検証を受け SOC 2、Type II の報告書を取得しています。 詳しくは、契約上の義務や契約内容をまとめたGoogle の利用規約とSLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://gsuite.google.com/terms/2013/1/premier_terms.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/

4.1	4.1.1	(2)	(b)	(ア) 委託先に提供する情報の委託先における目的外利用の禁止	Google Cloud と G Suite は、クラウドプロバイダのための ISO27017 認証を受けています。機密保持に関する統制についても、第三者機関によるレビューと検証を受け SOC 2、Type II の報告書を取得しています。 詳しくは、契約上の義務や契約内容をまとめたGoogle の利用規約と SLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://gsuite.google.com/terms/2013/1/premier_terms.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
4.1	4.1.1	(2)	(b)	(イ)委託先における情報セキュリティ対策の実施内容及び管理体制	Google Cloud と G Suite は、クラウドプロバイダのための ISO27017 認証を受けています。機密保持に関する統制についても、第三者機関によるレビューと検証を受け SOC 2、Type II の報告書を取得しています。 詳しくは、契約上の義務や契約内容をまとめたGoogle の利用規約と SLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://gsuite.google.com/terms/2013/1/premier_terms.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
4.1	4.1.1	(2)	(b)	(ウ)委託事業の実施に当たり、委託先企業若しくはその従業員、再委託先又はその他の者によって、機関等の意図せざる変更が加えられないための管理体制	Google Cloud と G Suite は、クラウドプロバイダのための ISO27017 認証を受けています。機密保持に関する統制についても、第三者機関によるレビューと検証を受け SOC 2、Type II の報告書を取得しています。 詳しくは、契約上の義務や契約内容をまとめたGoogle の利用規約と SLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://gsuite.google.com/terms/2013/1/premier_terms.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
4.1	4.1.1	(2)	(b)	(エ)委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に 関する情報提供	Google Cloud と G Suite は、クラウドプロバイダのための ISO27017 認証を受けています。機密保持に関する統制についても、第三者機関によるレビューと検証を受け SOC 2、Type II の報告書を取得しています。 詳しくは、契約上の義務や契約内容をまとめたGoogle の利用規約と SLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://gsuite.google.com/terms/2013/1/premier_terms.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
4.1	4.1.1	(2)	(b)	(オ)情報セキュリティインシデントへの対処方法	Google Cloud と G Suite は、クラウドプロバイダのための ISO27017 認証を受けています。機密保持に関する統制についても、第三者機関によるレビューと検証を受け SOC 2、Type II の報告書を取得しています。 詳しくは、契約上の義務や契約内容をまとめたGoogle の利用規約と SLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://gsuite.google.com/terms/2013/1/premier_terms.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
4.1	4.1.1	(2)	(b)	(カ)情報セキュリティ対策その他の契約の履行状況の確認方法	Google Cloud と G Suite は、クラウドプロバイダのための ISO27017 認証を受けています。機密保持に関する統制についても、第三者機関によるレビューと検証を受け SOC 2、Type II の報告書を取得しています。 詳しくは、契約上の義務や契約内容をまとめたGoogle の利用規約と SLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://gsuite.google.com/terms/2013/1/premier_terms.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
4.1	4.1.1	(2)	(b)	(キ)情報セキュリティ対策の履行が不十分な場合の対処方法	Google Cloud と G Suite は、クラウドプロバイダのための ISO27017 認証を受けています。機密保持に関する統制についても、第三者機関によるレビューと検証を受け SOC 2、Type II の報告書を取得しています。 詳しくは、契約上の義務や契約内容をまとめたGoogle の利用規約と SLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://gsuite.google.com/terms/2013/1/premier_terms.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
4.1	4.1.1	(2)	(c)	情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託する業務において取り扱う情報の格付等を勘案し、必要に応じて以下の内容を仕様に含めること。	Google Cloud と G Suite は、クラウドプロバイダのための ISO27017 認証を受けています。機密保持に関する統制についても、第三者機関によるレビューと検証を受け SOC 2、Type II の報告書を取得しています。 詳しくは、契約上の義務や契約内容をまとめたGoogle の利用規約と SLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://gsuite.google.com/terms/2013/1/premier_terms.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
4.1	4.1.1	(2)	(c)	(ア)情報セキュリティ監査の受入れ	Google Cloud と G Suite は、クラウドプロバイダのための ISO27017 認証を受けています。機密保持に関する統制についても、第三者機関によるレビューと検証を受け SOC 2、Type II の報告書を取得しています。 詳しくは、契約上の義務や契約内容をまとめたGoogle の利用規約と SLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://gsuite.google.com/terms/2013/1/premier_terms.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/

4.1	4.1.1	(2)	(c)	(イ)サービスレベルの保証	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。機密保持に関する統制についても、第三者機関によるレビューと検証を受け SOC 2、Type II の報告書を取得しています。 詳しくは、契約上の義務や契約内容をまとめたGoogle の利用規約と SLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://gsuite.google.com/terms/2013/1/premier_terms.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
4.1	4.1.1	(2)	(d)	情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、上記(b)(c)の措置の実施を委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を機関等に提供し、機関等の承認を受けるよう、仕様内容に含めること。 また、委託判断基準及び委託先の選定基準に従って再委託の承認の可否を判断すること。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。機密保持に関する統制についても、第三者機関によるレビューと検証を受け SOC 2、Type II の報告書を取得しています。 詳しくは、契約上の義務や契約内容をまとめたGoogle の利用規約と SLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://gsuite.google.com/terms/2013/1/premier_terms.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
4.1	4.1.1	(3)	外部委託における対策の実施		
4.1	4.1.1	(3)	(a)	情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、契約に基づき、委託先における情報セキュリティ対策の履行状況を確認すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO 27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全社員および全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の社員および委託業者は初期研修で Google の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティチームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。
4.1	4.1.1	(3)	(b)	情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等 を認知した場合又はその旨の報告を職員等より受けた場合は、委託事業を一時中断するなどの必要な措置を講じた上で、契約に基づく対処を委託先に講じさせること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO 27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全社員および全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の社員および委託業者は初期研修で Google の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティチームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。
4.1	4.1.1	(3)	(c)	情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託した業務の終了時に、委託先において取り扱われた情報が確実に返却、又は抹消されたこ とを確認すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO 27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全社員および全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の社員および委託業者は初期研修で Google の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティチームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。
4.1	4.1.1	(4)	外部委託における情報の取扱い		
4.1	4.1.1	(4)	(a)	職員等は、委託先への情報の提供等において、以下の事項を遵守すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO 27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全社員および全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の社員および委託業者は初期研修で Google の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティチームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。
4.1	4.1.1	(4)	(a)	(ア) 委託先に要保護情報を提供する場合は、提供する情報を必要最小限とし、あらかじめ定められた安全な受渡し方法により提供すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO 27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全社員および全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の社員および委託業者は初期研修で Google の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティチームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。
4.1	4.1.1	(4)	(a)	(イ) 提供した要保護情報が委託先において不要になった場合は、これを確実に返却又は抹消させること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO 27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全社員および全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の社員および委託業者は初期研修で Google の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティチームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。

4.1	4.1.1	(4)	(a)	(ウ) 委託業務において、情報セキュリティインシデント、情報の目的外利用等を認知した場合は、速やかに情報システムセキュリティ責任者又は課室情報セキュリティ責任者に報告すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO 27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全社員および全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の社員および委託業者は初期研修でGoogle の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティチームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。
4.1	4.1.2	約款による外部サービスの利用			
4.1	4.1.2	(1)	約款による外部サービスの利用に係る規定の整備		
4.1	4.1.2	(1)	(a)	統括情報セキュリティ責任者は、以下を含む約款による外部サービスの利用に関する規定を整備すること。また、当該サービスの利用において要機密情報が取り扱わ れないよう規定すること。	Google Cloud と G Suite は、クラウドプロバイダのためのISO27017 認証を受けています。機密保持に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 詳しくは、契約上の義務や契約内容をまとめたGoogle の利用規約とSLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://gsuite.google.com/terms/2013/1/premier_terms.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
4.1	4.1.2	(1)	(a)	(ア)約款による外部サービスを利用してよい業務の範囲	Google Cloud と G Suite は、クラウドプロバイダのためのISO27017 認証を受けています。機密保持に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 詳しくは、契約上の義務や契約内容をまとめたGoogle の利用規約とSLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://gsuite.google.com/terms/2013/1/premier_terms.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
4.1	4.1.2	(1)	(a)	(イ)業務に利用できる約款による外部サービス	Google Cloud と G Suite は、クラウドプロバイダのためのISO27017 認証を受けています。機密保持に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 詳しくは、契約上の義務や契約内容をまとめたGoogle の利用規約とSLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://gsuite.google.com/terms/2013/1/premier_terms.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
4.1	4.1.2	(1)	(a)	(ウ)利用手続及び運用手順	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27001 2013、附属書 A.5）、「情報セキュリティのための組織」(ISO27001 2013、附属書 A.6）、「運用の手順および責任」(ISO 27001 2013、附属書 A.12.1）が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、運用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。
4.1	4.1.2	(1)	(b)	情報セキュリティ責任者は、約款による外部サービスを利用する場合は、利用するサービスごとの責任者を定めること。	Google は ISO27001 認証を受けています。この基準では、「人的資源のセキュリティ」(ISO27001 2013、附属書 A.7）が規定されています。人的資源の管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 全社員は Google の行動規範（https://abc.xyz/investor/other/google-code-of-conduct.html）に同意し、倫理とコンプライアンスに関する研修を受けています。 Google Cloud Platform のお客様は、運用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。
4.1	4.1.2	(2)	約款による外部サービスの利用における対策の実施		
4.1	4.1.2	(2)	(a)	職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、 適切な措置を講じた上で利用すること。	Google は ISO27001 認証を受けています。この基準では、「情報システムの監査に対する考慮事項」(ISO 27001 2013、附属書 A.12.7）、「物理的セキュリティ境界」(ISO 27001 2013、附属書 A.11.1）、「オフィス、部屋及び施設のセキュリティ」(ISO 27001 2013、附属書 A.11.3）と「外部及び環境の脅威からの保護」(ISO 27001 2013、附属書 A.11.4）が規定されています。 情報セキュリティの監督管理体制は、社内監査の監督など、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleは、セキュリティ、プライバシー及びコンプライアンス統制を検証するために、独立した第三者機関による監査を定期的に受けています。これは、独立した監査人が我々のデータセンターやインフラストラクチャ、オペレーションにおける統制を検査するということです。 第三者機関による監査は、Googleの機密性、完全性、可用性に関する情報セキュリティレベルに保証を与えるため、総合的なアプローチとなるよう設計されています。お客様はこれらの第三者機関による監査をGoogleの製品がお客様のコンプライアンスやデータ処理のニーズ対応可能か評価する際に利用できます。 最新の監査報告書は、Google Cloud Platform(GCP)とG Suiteのコンプライアンスページからご確認いただけます。 https://cloud.google.com/security/compliance/. お客様の監査の権利については、Google terms of service section 7.5.2, "Customer's Audit Rights"に記載しています。 また、GoogleはGoogle Cloud Platformのデータセンターのロケーションについて、外部の文書を提供しています。 https://cloud.google.com/about/locations/.
4.1	4.1.3	ソーシャルメディアサービスによる情報発信			
4.1	4.1.3	(1)	ソーシャルメディアサービスによる情報発信時の対策		
4.1	4.1.3	(1)	(a)	統括情報セキュリティ責任者は、機関等が管理するアカウントでソーシャルメディアサービスを利用することを前提として、以下を含む情報セキュリティ対策に関する運用手順等を定めること。また、当該サービスの利用において要機密情報が取り扱われないよう規定すること。	ー
4.1	4.1.3	(1)	(a)	(ア) 機関等のアカウントによる情報発信が実際の機関等のものであると明らかとするために、アカウントの運用組織を明示するなどの方法でなりすましへの対策を講ずること。	ー

4.1	4.1.3	(1)	(a)	(イ)パスワード等の主体認証情報を適切に管理するなどの方法で不正アクセスへの対策を講ずること。	ー
4.1	4.1.3	(1)	(b)	情報セキュリティ責任者は、機関等において情報発信のためにソーシャルメディアサービスを利用する場合は、利用するソーシャルメディアサービスごとの責任者を定めること。	ー
4.1	4.1.3	(1)	(c)	職員等は、要安定情報の国民への提供にソーシャルメディアサービスを用いる場合は、機関等の自己管理ウェブサイトに当該情報を掲載して参照可能とすること。	ー
4.1	4.1.4	クラウドサービスの利用			
4.1	4.1.4	(1)	クラウドサービスの利用における対策		
4.1	4.1.4	(1)	(a)	情報システムセキュリティ責任者は、クラウドサービス（民間事業者が提供するものに限らず、機関等が自ら提供するものを含む。以下同じ。）を利用するに当たり、取り扱う情報の格付及び取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断すること。	Google は ISO27001 認証を受けています。この基準では、「情報システムの監査に対する考慮事項」(ISO 27001 2013、附属書 A.12.7)、「物理的セキュリティ境界」(ISO 27001 2013、附属書 A.11.1)、「オフィス、部屋及び施設のセキュリティ」(ISO 27001 2013、附属書 A.11.3)と「外部及び環境の脅威からの保護」(ISO 27001 2013、附属書 A.11.4)が規定されています。 情報セキュリティの監督管理体制は、社内監査の監督など、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleは、セキュリティ、プライバシー及びコンプライアンス統制を検証するために、独立した第三者機関による監査を定期的に受けています。これは、独立した監査人が我々のデータセンターやインフラストラクチャ、オペレーションにおける統制を検査するということです。 第三者機関による監査は、Googleの機密性、完全性、可用性に関する情報セキュリティレベルに保証を与えるため、総合的なアプローチとなるよう設計されています。お客様はこれらの第三者機関による監査をGoogleの製品がお客様のコンプライアンスやデータ処理のニーズ対応可能か評価する際に利用できます。 最新の監査報告書は、Google Cloud Platform(GCP)とG Suiteのコンプライアンスページからご確認いただけます。 https://cloud.google.com/security/compliance/. お客様の監査の権利については、Google terms of service section 7.5.2, "Customer's Audit Rights"に記載しています。 また、GoogleはGoogle Cloud Platformのデータセンターのロケーションについて、外部の文書を提供しています。 https://cloud.google.com/about/locations/.
4.1	4.1.4	(1)	(b)	情報システムセキュリティ責任者は、クラウドサービス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るリスクを評価して委託先を選定し、必要に応じて委託事業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こと。	Google は ISO27001 認証を受けています。この基準では、「情報システムの監査に対する考慮事項」(ISO 27001 2013、附属書 A.12.7)、「物理的セキュリティ境界」(ISO 27001 2013、附属書 A.11.1)、「オフィス、部屋及び施設のセキュリティ」(ISO 27001 2013、附属書 A.11.3)と「外部及び環境の脅威からの保護」(ISO 27001 2013、附属書 A.11.4)が規定されています。 情報セキュリティの監督管理体制は、社内監査の監督など、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleは、セキュリティ、プライバシー及びコンプライアンス統制を検証するために、独立した第三者機関による監査を定期的に受けています。これは、独立した監査人が我々のデータセンターやインフラストラクチャ、オペレーションにおける統制を検査するということです。 第三者機関による監査は、Googleの機密性、完全性、可用性に関する情報セキュリティレベルに保証を与えるため、総合的なアプローチとなるよう設計されています。お客様はこれらの第三者機関による監査をGoogleの製品がお客様のコンプライアンスやデータ処理のニーズ対応可能か評価する際に利用できます。 最新の監査報告書は、Google Cloud Platform(GCP)とG Suiteのコンプライアンスページからご確認いただけます。 https://cloud.google.com/security/compliance/. お客様の監査の権利については、Google terms of service section 7.5.2, "Customer's Audit Rights"に記載しています。 また、GoogleはGoogle Cloud Platformのデータセンターのロケーションについて、外部の文書を提供しています。 https://cloud.google.com/about/locations/.
4.1	4.1.4	(1)	(c)	情報システムセキュリティ責任者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、委託先を選定する際の要件とすること。	Google は ISO27001 認証を受けています。この基準では、「情報システムの監査に対する考慮事項」(ISO 27001 2013、附属書 A.12.7)、「物理的セキュリティ境界」(ISO 27001 2013、附属書 A.11.1)、「オフィス、部屋及び施設のセキュリティ」(ISO 27001 2013、附属書 A.11.3)と「外部及び環境の脅威からの保護」(ISO 27001 2013、附属書 A.11.4)が規定されています。 情報セキュリティの監督管理体制は、社内監査の監督など、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleは、セキュリティ、プライバシー及びコンプライアンス統制を検証するために、独立した第三者機関による監査を定期的に受けています。これは、独立した監査人が我々のデータセンターやインフラストラクチャ、オペレーションにおける統制を検査するということです。 第三者機関による監査は、Googleの機密性、完全性、可用性に関する情報セキュリティレベルに保証を与えるため、総合的なアプローチとなるよう設計されています。お客様はこれらの第三者機関による監査をGoogleの製品がお客様のコンプライアンスやデータ処理のニーズ対応可能か評価する際に利用できます。 最新の監査報告書は、Google Cloud Platform(GCP)とG Suiteのコンプライアンスページからご確認いただけます。 https://cloud.google.com/security/compliance/. お客様の監査の権利については、Google terms of service section 7.5.2, "Customer's Audit Rights"に記載しています。 また、GoogleはGoogle Cloud Platformのデータセンターのロケーションについて、外部の文書を提供しています。 https://cloud.google.com/about/locations/.

4.1	4.1.4	(1)	(d)	情報システムセキュリティ責任者は、クラウドサービスの特性を考慮した上で、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定めること。	Google は ISO27001 認証を受けています。この基準では、「情報システムの監査に対する考慮事項」(ISO 27001 2013、附属書 A.12.7)、「物理的セキュリティ境界」(ISO 27001 2013、附属書 A.11.1)、「オフィス、部屋及び施設のセキュリティ」(ISO 27001 2013、附属書 A.11.3)と「外部及び環境の脅威からの保護」(ISO 27001 2013、附属書 A.11.4)が規定されています。 情報セキュリティの監督管理体制は、社内監査の監督など、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleは、セキュリティ、プライバシー及びコンプライアンス統制を検証するために、独立した第三者機関による監査を定期的に受けています。これは、独立した監査人が我々のデータセンターやインフラストラクチャ、オペレーションにおける統制を検査するということです。 第三者機関による監査は、Googleの機密性、完全性、可用性に関する情報セキュリティレベルに保証を与えるため、総合的なアプローチとなるよう設計されています。お客様はこれらの第三者機関による監査をGoogleの製品がお客様のコンプライアンスやデータ処理のニーズ対応可能か評価する際に利用できます。 最新の監査報告書は、Google Cloud Platform(GCP)とG Suiteのコンプライアンスページからご確認いただけます。 https://cloud.google.com/security/compliance/. お客様の監査の権利については、Google terms of service section 7.5.2, "Customer's Audit Rights"に記載しています。 また、GoogleはGoogle Cloud Platformのデータセンターのロケーションについて、外部の文書を提供しています。 https://cloud.google.com/about/locations/.
4.1	4.1.4	(1)	(e)	情報システムセキュリティ責任者は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断すること。	Google は ISO27001 認証を受けています。この基準では、「情報システムの監査に対する考慮事項」(ISO 27001 2013、附属書 A.12.7)が規定されています。 情報セキュリティの監督管理体制は、社内監査の監督など、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。
情報システムのライフサイクル					
5.1	情報システムに係る文書等の整備				
5.1	5.1.1	情報システムに係る台帳等の整備			
5.1	5.1.1	(1)	情報システム台帳の整備		
5.1	5.1.1	(1)	(a)	統括情報セキュリティ責任者は、全ての情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳に整備すること。	Google は ISO27001 認証を受けています。この基準では、「装置」(ISO 27001 2013、附属書 A.11.2)が規定されています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティモデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 Google のデータセンタープロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
5.1	5.1.1	(1)	(b)	情報システムセキュリティ責任者は、情報システムを新規に構築し、又は更改する際には、当該情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について統括情報セキュリティ責任者に報告すること。	Google は ISO27001 認証を受けています。この基準では、「装置」(ISO 27001 2013、附属書 A.11.2)が規定されています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティモデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 Google のデータセンタープロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
5.1	5.1.1	(2)	情報システム関連文書の整備		
5.1	5.1.1	(2)	(a)	情報システムセキュリティ責任者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を網羅した情報システム関連文書を整備すること。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」(附属書A.8.1)、「媒体の処分」(附属書 A.8.3.2)、「装置のセキュリティを保った処分または再利用」(附属書A.11.2.7)、「運用ソフトウェアの管理」(附属書 A. 12.5)が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する 際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
5.1	5.1.1	(2)	(a)	(ア)情報システムを構成するサーバ装置及び端末関連情報	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」(附属書A.8.1)、「媒体の処分」(附属書 A.8.3.2)、「装置のセキュリティを保った処分または再利用」(附属書A.11.2.7)、「運用ソフトウェアの管理」(附属書 A. 12.5)が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する 際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。

5.1	5.1.1	(2)	(a)	(イ)情報システムを構成する通信回線及び通信回線装置関連情報	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する 際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
5.1	5.1.1	(2)	(a)	(ウ)情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する 際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
5.1	5.1.1	(2)	(a)	(エ)情報セキュリティインシデントを認知した際の対処手順	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する 際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
5.1	5.1.2	機器等の調達に係る規定の整備			
5.1	5.1.2	(1)	機器等の調達に係る規定の整備		
5.1	5.1.2	(1)	(a)	統括情報セキュリティ責任者は、機器等の選定基準を整備すること。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられ ない管理がなされ、その管理を機関等が確認できることを加えること。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する 際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
5.1	5.1.2	(1)	(b)	統括情報セキュリティ責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備すること。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する 際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
5.2	情報システムのライフサイクルの各段階における対策				
5.2	5.2.1	情報システムの企画・要件定義			
5.2	5.2.1	(1)	実施体制の確保		
5.2	5.2.1	(1)	(a)	情報システムセキュリティ責任者は、情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制の確保を、最高情報セキュリティ責任者に求めること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」（ISO 27002 2013、附属書 A.5）と「情報セキュリティのための組織」（ISO27002 2013、附属書 A.6）が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
5.2	5.2.1	(1)	(b)	情報システムセキュリティ責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システムを整備し運用管理する機関等が定める運用管理規程等に応じた体制の確保を、最高情報セキュリティ責任者に求めること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」（ISO 27002 2013、附属書 A.5）と「情報セキュリティのための組織」（ISO27002 2013、附属書 A.6）が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。

			(c)	最高情報セキュリティ責任者は、前二項で求められる体制の確保に際し、情報システムを統括する責任者（情報化統括責任者（CIO））の協力を得ることが必要な場合は、当該情報システムを統括する責任者に当該体制の全部又は一部の整備を求めること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27002 2013、附属書 A.5）と「情報セキュリティのための組織」(ISO27002 2013、附属書 A.6）が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
5.2	5.2.1	(2)	情報システムのセキュリティ要件の策定		
5.2	5.2.1	(2)	(a)	情報システムセキュリティ責任者は、情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等に基づき、構築 する情報システムをインターネットや、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離することの要否を判断した上で、以下の事項を含む情報システムのセキュリティ要件を策定すること。	Google は ISO27001 認証を受けています。この基準では、「システムの取得、開発および保守」(ISO 27001 2013、附属書 A.14）が規定されています。 Google Cloud Platform のお客様は、システム開発プロセスの管理など、お使いの環境を設定、管理するすべての権利と責任を保有します。
5.2	5.2.1	(2)	(a)	(ア)情報システムに組み込む主体認証、アクセス制御、権限管理、ログ管理、暗号化機能等のセキュリティ機能要件	Google は ISO27001 認証を受けています。この基準では、「システムの取得、開発および保守」(ISO 27001 2013、附属書 A.14）が規定されています。 Google Cloud Platform のお客様は、システム開発プロセスの管理など、お使いの環境を設定、管理するすべての権利と責任を保有します。
5.2	5.2.1	(2)	(a)	(イ) 情報システム運用時の監視等の運用管理機能要件（監視するデータが暗号化されている場合は、必要に応じて復号すること）	Google は ISO27001 認証を受けています。この基準では、「システムの取得、開発および保守」(ISO 27001 2013、附属書 A.14）が規定されています。 Google Cloud Platform のお客様は、システム開発プロセスの管理など、お使いの環境を設定、管理するすべての権利と責任を保有します。
5.2	5.2.1	(2)	(a)	(ウ)情報システムに関連する脆弱性についての対策要件	Google は ISO27001 認証を受けています。この基準では、「システムの取得、開発および保守」(ISO 27001 2013、附属書 A.14）が規定されています。 Google Cloud Platform のお客様は、システム開発プロセスの管理など、お使いの環境を設定、管理するすべての権利と責任を保有します。
5.2	5.2.1	(2)	(b)	情報システムセキュリティ責任者は、インターネット回線と接続する情報システムを構築する場合は、接続するインターネット回線を定めた上で、標的型攻撃を始め とするインターネットからの様々なサイバー攻撃による情報の漏えい、改ざん等のリスクを低減するための多重防御のためのセキュリティ要件を策定すること。	Google は ISO27001 認証を受けています。この基準では、「通信のセキュリティ」(ISO 27001 2013、附属書 A.13）と「公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮」(ISO27002 2013、附属書 A.14.1.2）が規定されています。 Google Cloud Platform のお客様は、外部接続の管理など、お使いの環境を設定、管理するすべての権利と責任を保有します。
5.2	5.2.1	(2)	(c)	情報システムセキュリティ責任者は、機器等を調達する場合には、「IT 製品の調達におけるセキュリティ要件リスト」を参照し、利用環境における脅威を分析した上で、 当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定すること。	Google は ISO27001 認証を受けています。この基準では、「システムの取得、開発および保守」(ISO 27001 2013、附属書 A.14）が規定されています。 Google Cloud Platform のお客様は、システム開発プロセスの管理など、お使いの環境を設定、管理するすべての権利と責任を保有します。
5.2	5.2.1	(2)	(d)	情報システムセキュリティ責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システム全体の情報セキュリティ水準を低下させることのないように、基盤となる情報システムの情報セキュリティ対策に関する運用管理規程等に基づいたセキュリティ要件を適切に策定すること。	Google は ISO27001 認証を受けています。この基準では、「システムの取得、開発および保守」(ISO 27001 2013、附属書 A.14）が規定されています。 Google Cloud Platform のお客様は、システム開発プロセスの管理など、お使いの環境を設定、管理するすべての権利と責任を保有します。
5.2	5.2.1	(3)	情報システムの構築を外部委託する場合の対策		
5.2	5.2.1	(3)	(a)	情報システムセキュリティ責任者は、情報システムの構築を外部委託する場合は、以下の事項を含む委託先に実施させる事項を、調達仕様書に記載するなどして、適切 に実施させること。	Google Cloud と G Suite は、クラウドプロバイダのための ISO27017 認証を受けています。機密保持に関する統制についても、第三者機関によるレビューと検証を受け SOC 2、Type II の報告書を取得しています。 詳しくは、契約上の義務や契約内容をまとめたGoogle の利用規約と SLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://gsuite.google.com/terms/2013/1/premier_terms.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
5.2	5.2.1	(3)	(a)	(ア)情報システムのセキュリティ要件の適切な実装	Google Cloud と G Suite は、クラウドプロバイダのための ISO27017 認証を受けています。機密保持に関する統制についても、第三者機関によるレビューと検証を受け SOC 2、Type II の報告書を取得しています。 詳しくは、契約上の義務や契約内容をまとめたGoogle の利用規約と SLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://gsuite.google.com/terms/2013/1/premier_terms.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
5.2	5.2.1	(3)	(a)	(イ)情報セキュリティの観点に基づく試験の実施	Google Cloud と G Suite は、クラウドプロバイダのための ISO27017 認証を受けています。機密保持に関する統制についても、第三者機関によるレビューと検証を受け SOC 2、Type II の報告書を取得しています。 詳しくは、契約上の義務や契約内容をまとめたGoogle の利用規約と SLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://gsuite.google.com/terms/2013/1/premier_terms.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
5.2	5.2.1	(3)	(a)	(ウ)情報システムの開発環境及び開発工程における情報セキュリティ対策	Google Cloud と G Suite は、クラウドプロバイダのための ISO27017 認証を受けています。機密保持に関する統制についても、第三者機関によるレビューと検証を受け SOC 2、Type II の報告書を取得しています。 詳しくは、契約上の義務や契約内容をまとめたGoogle の利用規約と SLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://gsuite.google.com/terms/2013/1/premier_terms.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
5.2	5.2.1	(4)	情報システムの運用・保守を外部委託する場合の対策		

5.2	5.2.1	(4)	(a)	情報システムセキュリティ責任者は、情報システムの運用・保守を外部委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件 について、調達仕様書に記載するなどして、適切に実施させること。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。機密保持に関する統制についても、第三者機関によるレビューと検証を受け SOC 2、Type II の報告書を取得しています。 詳しくは、契約上の義務や契約内容をまとめたGoogle の利用規約と SLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://gsuite.google.com/terms/2013/1/premier_terms.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
5.2	5.2.1	(4)	(b)	情報システムセキュリティ責任者は、情報システムの運用・保守を外部委託する場合は、委託先が実施する情報システムに対する情報セキュリティ対策を適切に把握 するため、当該対策による情報システムの変更内容について、速やかに報告させること。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。機密保持に関する統制についても、第三者機関によるレビューと検証を受け SOC 2、Type II の報告書を取得しています。 詳しくは、契約上の義務や契約内容をまとめたGoogle の利用規約と SLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://gsuite.google.com/terms/2013/1/premier_terms.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
5.2	5.2.2	情報システムの調達・構築			
5.2	5.2.2	(1)	機器等の選定時の対策		
5.2	5.2.2	(1)	(a)	情報システムセキュリティ責任者は、機器等の選定時において、選定基準に対する機器等の適合性を確認し、その結果を機器等の選定における判断の一要素として活用すること。	Google は ISO27001 認証を受けています。この基準では、「システムの取得、開発および保守」(ISO 27001 2013、附属書 A.14）が規定されています。 Google Cloud Platform のお客様は、システム開発プロセスの管理など、お使いの環境を設定、管理するすべての権利と責任を保有します。
5.2	5.2.2	(2)	情報システムの構築時の対策		
5.2	5.2.2	(2)	(a)	情報システムセキュリティ責任者は、情報システムの構築において、情報セキュリティの観点から必要な措置を講ずること。	Google は ISO27001 認証を受けています。この基準では、「開発環境、試験環境および運用環境の分離」(ISO 27001 2013、附属書 A.12.1.4）と「開発およびサポートプロセスにおけるセキュリティ」(ISO 27001 2013、附属書 A.14.2）が規定されています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
5.2	5.2.2	(2)	(b)	情報システムセキュリティ責任者は、構築した情報システムを運用保守段階へ移行するに当たり、移行手順及び移行環境に関して、情報セキュリティの観点から必要な措置を講ずること。	Google は ISO27001 認証を受けています。この基準では、「開発環境、試験環境および運用環境の分離」(ISO 27001 2013、附属書 A.12.1.4）と「開発およびサポートプロセスにおけるセキュリティ」(ISO 27001 2013、附属書 A.14.2）が規定されています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
5.2	5.2.2	(3)	納品検査時の対策		
5.2	5.2.2	(3)	(a)	情報システムセキュリティ責任者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認すること。	Google は ISO27001 認証を受けています。この基準では、「開発環境、試験環境および運用環境の分離」(ISO 27001 2013、附属書 A.12.1.4）と「開発およびサポートプロセスにおけるセキュリティ」(ISO 27001 2013、附属書 A.14.2）が規定されています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
5.2	5.2.2	(3)	(b)	情報システムセキュリティ責任者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる 項目に、情報セキュリティ対策に必要な内容が含まれていることを確認すること。	Google は ISO27001 認証を受けています。この基準では、「開発環境、試験環境および運用環境の分離」(ISO 27001 2013、附属書 A.12.1.4）と「開発およびサポートプロセスにおけるセキュリティ」(ISO 27001 2013、附属書 A.14.2）が規定されています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
5.2	5.2.3	情報システムの運用・保守			
5.2	5.2.3	(1)	情報システムの運用・保守時の対策		
5.2	5.2.3	(1)	(a)	情報システムセキュリティ責任者は、情報システムの運用・保守において、情報システムに実装されたセキュリティ機能を適切に運用すること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てていますGoogle 社員に付与される既定のアクセス権限は、社員用メールやGoogle 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフローツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定　の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud Platform のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。
5.2	5.2.3	(1)	(b)	情報システムセキュリティ責任者は、基盤となる情報システムを利用して構築された情報システムを運用する場合は、基盤となる情報システムを整備し運用管理する機関等との責任分界に応じた運用管理体制の下、基盤となる情報システムの運用管理規程等に従い、基盤全体の情報セキュリティ水準を低下させることのないよう、 適切に情報システムを運用すること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てていますGoogle 社員に付与される既定のアクセス権限は、社員用メールやGoogle 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフローツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定　の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud Platform のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。

5.2	5.2.3	(1)	(c)	情報システムセキュリティ責任者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理すること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフローツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定　の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud Platform のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。
5.2	5.2.4	情報システムの更改・廃棄			
5.2	5.2.4	(1)	情報システムの更改・廃棄時の対策		
5.2	5.2.4	(1)	(a)	情報システムセキュリティ責任者は、情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、以下の措置を適切に講ずること。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」(ISO 27001 2013、附属書 A.8.3.2)と「装置のセキュリティを保った処分または再利用」(ISO 27001 2013、附属書 A.11.2.7)が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する 際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。
5.2	5.2.4	(1)	(a)	(ア)情報システム更改時の情報の移行作業における情報セキュリティ対策	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」(ISO 27001 2013、附属書 A.8.3.2)と「装置のセキュリティを保った処分または再利用」(ISO 27001 2013、附属書 A.11.2.7)が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する 際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。
5.2	5.2.4	(1)	(a)	(イ)情報システム廃棄時の不要な情報の抹消	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」(ISO 27001 2013、附属書 A.8.3.2)と「装置のセキュリティを保った処分または再利用」(ISO 27001 2013、附属書 A.11.2.7)が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する 際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。
5.2	5.2.5	情報システムについての対策の見直し			
5.2	5.2.5	(1)	情報システムについての対策の見直し		
5.2	5.2.5	(1)	(a)	情報システムセキュリティ責任者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講ずること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27001 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27001 2013、附属書 A.6)が規定されています。 情報セキュリティポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
5.3	情報システムの運用継続計画				
5.3	5.3.1	情報システムの運用継続計画の整備・整合的運用の確保			
5.3	5.3.1	(1)	情報システムの運用継続計画の整備・整合的運用の確保		
5.3	5.3.1	(1)	(a)	統括情報セキュリティ責任者は、機関等において非常時優先業務を支える情報システムの運用継続計画を整備する必要がある場合は、非常時における情報セキュリティに係る対策事項を検討すること。	Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001 2013、附属書 A.17.2)と「バックアップ」(ISO27001 2013、附属書 A.12.3)が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud Platform のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。

5.3	5.3.1	(1)	(b)	統括情報セキュリティ責任者は、情報システムの運用継続計画の教育訓練や維持改善を行う際等に、非常時における情報セキュリティに係る対策事項が運用可能で あるかを確認すること。	Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001 2013、附属書 A.17.2)と「バックアップ」(ISO27001 2013、附属書 A.12.3)が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性はGoogle のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェアサービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud Platform のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。
情報システムのセキュリティ要件					
6.1	情報システムのセキュリティ機能				
6.1	6.1.1	主体認証機能			
6.1	6.1.1	(1)	主体認証機能の導入		
6.1	6.1.1	(1)	(a)	情報システムセキュリティ責任者は、情報システムや情報へのアクセス主体を特定し、それが正当な主体であることを検証する必要がある場合、主体の識別及び主体認証を行う機能を設けること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てていますGoogle 社員に付与される既定のアクセス権限は、社員用メールやGoogle 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフローツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定　の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
6.1	6.1.1	(1)	(b)	情報システムセキュリティ責任者は、国民・企業と機関等との間の申請、届出等のオンライン手続を提供する情報システムを構築する場合は、オンライン手続におけるリスクを評価した上で、主体認証に係る要件を策定すること。	Google は ISO27001 認証を受けています。この基準では、「情報システムの監査に対する考慮事項」(ISO 27001 2013、附属書 A.12.7)、「物理的セキュリティ境界」(ISO 27001 2013、附属書 A.11.1)、「オフィス、部屋及び施設のセキュリティ」(ISO 27001 2013、附属書 A.11.3)と「外部及び環境の脅威からの保護」(ISO 27001 2013、附属書 A.11.4)が規定されています。 情報セキュリティの監督管理体制は、社内監査の監督など、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleは、セキュリティ、プライバシー及びコンプライアンス統制を検証するために、独立した第三者機関による監査を定期的に受けています。これは、独立した監査人が我々のデータセンターやインフラストラクチャ、オペレーションにおける統制を検査するということです。 第三者機関による監査は、Googleの機密性、完全性、可用性に関する情報セキュリティレベルに保証を与えるため、総合的なアプローチとなるよう設計されています。お客様はこれらの第三者機関による監査をGoogleの製品がお客様のコンプライアンスやデータ処理のニーズ対応可能か評価する際に利用できます。 最新の監査報告書は、Google Cloud Platform(GCP)とG Suiteのコンプライアンスページからご確認いただけます。 https://cloud.google.com/security/compliance/. お客様の監査の権利については、Google terms of service section 7.5.2, "Customer's Audit Rights"に記載しています。 また、GoogleはGoogle Cloud Platformのデータセンターのロケーションについて、外部の文書を提供しています。 https://cloud.google.com/about/locations/.
6.1	6.1.1	(1)	(c)	情報システムセキュリティ責任者は、主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講ずること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てていますGoogle 社員に付与される既定のアクセス権限は、社員用メールやGoogle 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフローツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定　の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
6.1	6.1.1	(2)	識別コード及び主体認証情報の管理		
6.1	6.1.1	(2)	(a)	情報システムセキュリティ責任者は、情報システムにアクセスする全ての主体に対して、識別コード及び主体認証情報を適切に付与し、管理するための措置を講ずること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google では、アクセスの妥当性を確認するために、全システムへの論理的アクセスの審査を定期的に実施しています。さらに、Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud Platform のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。

6.1	6.1.1	(2)	(b)	情報システムセキュリティ責任者は、主体が情報システムを利用する必要がなくなった場合は、当該主体の識別コード及び主体認証情報の不正な利用を防止するための措置を速やかに講ずること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google では、アクセスの妥当性を確認するために、全システムへの論理的アクセスの審査を定期的に実施しています。さらに、Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud Platform のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。
6.1	6.1.2	アクセス制御機能			
6.1	6.1.2	(1)	アクセス制御機能の導入		
6.1	6.1.2	(1)	(a)	情報システムセキュリティ責任者は、情報システムの特性、情報システムが取り扱う情報の格付及び取扱制限等に従い、権限を有する者のみがアクセス制御の設定等 を行うことができる機能を設けること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフローツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポートサービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud Platform のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。
6.1	6.1.2	(1)	(b)	情報システムセキュリティ責任者は、情報システム及び情報へのアクセスを許可する主体が確実に制限されるように、アクセス制御機能を適切に運用すること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフローツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポートサービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud Platform のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。
6.1	6.1.3	権限の管理			
6.1	6.1.3	(1)	権限の管理		
6.1	6.1.3	(1)	(a)	情報システムセキュリティ責任者は、主体から対象に対するアクセスの権限を適切に設定するよう、措置を講ずること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google では、アクセスの妥当性を確認するために、全システムへの論理的アクセスの審査を定期的に実施しています。さらに、Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud Platform のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。
6.1	6.1.3	(1)	(b)	情報システムセキュリティ責任者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化する ための措置及び、内部からの不正操作や誤操作を防止するための措置を講ずること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティトレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud Platform のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。
6.1	6.1.4	ログの取得・管理			
6.1	6.1.4	(1)	ログの取得・管理		
6.1	6.1.4	(1)	(a)	情報システムセキュリティ責任者は、情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログを取得すること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフローツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定　の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。

6.1	6.1.4	(1)	(b)	情報システムセキュリティ責任者は、情報システムにおいて、その特性に応じてログを取得する目的を設定した上で、ログを取得する対象の機器等、ログとして取得する情報項目、ログの保存期間、要保護情報の観点でのログ情報の取扱方法、及びログが取得できなくなった場合の対処方法等について定め、適切にログを管理すること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフローツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定　の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
6.1	6.1.4	(1)	(c)	情報システムセキュリティ責任者は、情報システムにおいて、取得したログを定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施すること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフローツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定　の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
6.1	6.1.5	暗号・電子署名			
6.1	6.1.5	(1)	暗号化機能・電子署名機能の導入		
6.1	6.1.5	(1)	(a)	情報システムセキュリティ責任者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、以下の措置を講ずること。	Google は ISO27001 認証を受けています。この基準では、「暗号」(ISO 27001 2013、附属書 A.10)が規定されています。 アップロード、作成されたお客様のデータを暗号化しています。Googleでは複数の暗号化レイヤを使用してデータを保護しています。複数の暗号化レイヤを使用することにより、冗長データ保護機能が追加され、アプリケーションの要件に基づいて最適な手法を選択できるようになります。 Google は、Google Cloud プロダクトと G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud Platform のお客様は、適切な暗号化対策の開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。
6.1	6.1.5	(1)	(a)	(ア)要機密情報を取り扱う情報システムについては、暗号化を行う機能の必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。	Google は ISO27001 認証を受けています。この基準では、「暗号」(ISO 27001 2013、附属書 A.10)が規定されています。 アップロード、作成されたお客様のデータを暗号化しています。Googleでは複数の暗号化レイヤを使用してデータを保護しています。複数の暗号化レイヤを使用することにより、冗長データ保護機能が追加され、アプリケーションの要件に基づいて最適な手法を選択できるようになります。 Google は、Google Cloud プロダクトと G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud Platform のお客様は、適切な暗号化対策の開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。
6.1	6.1.5	(1)	(a)	(イ)要保全情報を取り扱う情報システムについては、電子署名の付与及び検証を行う機能を設ける必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。	Google は ISO27001 認証を受けています。この基準では、「ログ取得及び監視」(ISO 27001 2013、附属書 A. 12.4)が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google のセキュリティ モニタリング プログラムは、内部ネットワークトラフィックから収集されている情報、社員によるシステム上の操作、外部に知られている脆弱性に焦点を当てています。Google のグローバル ネットワークのさまざまな箇所で、内部トラフィックに疑わしい動作（たとえば、トラフィックにボットネットに接続している可能性が見られるなど）がないか検査しています。この分析では、オープンソースのツールと商用ツールを組み合わせて使用し、トラフィックのキャプチャと解析を行っています。Google の技術を基に構築された独自の相関システムもこの解析をサポートしています。こうしたネットワーク解析に加え、顧客データへのアクセスの試行などの異常な動向を特定するために、システムログを精査しています。Google のセキュリティ エンジニアは、Google のインフラストラクチャに影響する可能性があるセキュリティ上のインシデントを検知する永続的な検索アラートを一般公開データ リポジトリに設定しています。また、受信したセキュリティレポートの確認や、公開のメーリングリスト、ブログ、Wiki のモニタリングを積極的に行っています。自動ネットワーク解析は、未知の脅威が発生した可能性がある状態を検知して Google セキュリティ スタッフに通知します。ネットワーク解析に加え、システムログの自動解析も行われています。 Google Cloud Platform のお客様は、不正データや未確認データを検出するためのモニタリング設定など、お使いの環境を設定、管理するすべての権利と責任を保有します。
6.1	6.1.5	(1)	(b)	情報システムセキュリティ責任者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照した上で、情報システムで使用する暗号及び電子署名のアルゴリズム並びにそれを利用した安全なプロトコル及びその運用方法について、以下の事項を含めて定めること。	Google は ISO27001 認証を受けています。この基準では、「暗号」(ISO 27001 2013、附属書 A.10)が規定されています。 アップロード、作成されたお客様のデータを暗号化しています。Googleでは複数の暗号化レイヤを使用してデータを保護しています。複数の暗号化レイヤを使用することにより、冗長データ保護機能が追加され、アプリケーションの要件に基づいて最適な手法を選択できるようになります。 Google は、Google Cloud プロダクトと G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud Platform のお客様は、適切な暗号化対策の開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。

6.1	6.1.5	(1)	(b)	(ア) 職員等が暗号化及び電子署名に対して使用するアルゴリズム及びそれを利用した安全なプロトコルについて、「電子政府推奨暗号リスト」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用させること。	Google は ISO27001 認証を受けています。この基準では、「暗号」(ISO 27001 2013、附属書 A.10)が規定されています。 アップロード、作成されたお客様のデータを暗号化しています。Googleでは複数の暗号化レイヤを使用してデータを保護しています。複数の暗号化レイヤを使用することにより、冗長データ保護機能が追加され、アプリケーションの要件に基づいて最適な手法を選択できるようになります。 Google は、Google Cloud プロダクトと G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud Platform のお客様は、適切な暗号化対策の開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。
6.1	6.1.5	(1)	(b)	(イ) 情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、「電子政府推奨暗号リスト」に記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用すること。	Google は ISO27001 認証を受けています。この基準では、「暗号」(ISO 27001 2013、附属書 A.10)が規定されています。 アップロード、作成されたお客様のデータを暗号化しています。Googleでは複数の暗号化レイヤを使用してデータを保護しています。複数の暗号化レイヤを使用することにより、冗長データ保護機能が追加され、アプリケーションの要件に基づいて最適な手法を選択できるようになります。 Google は、Google Cloud プロダクトと G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud Platform のお客様は、適切な暗号化対策の開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。
6.1	6.1.5	(1)	(b)	(ウ) 暗号化及び電子署名に使用するアルゴリズムが危殆化した場合又はそれを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定めること。	Google は ISO27001 認証を受けています。この基準では、「暗号」(ISO 27001 2013、附属書 A.10)が規定されています。 アップロード、作成されたお客様のデータを暗号化しています。Googleでは複数の暗号化レイヤを使用してデータを保護しています。複数の暗号化レイヤを使用することにより、冗長データ保護機能が追加され、アプリケーションの要件に基づいて最適な手法を選択できるようになります。 Google は、Google Cloud プロダクトと G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud Platform のお客様は、適切な暗号化対策の開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。
6.1	6.1.5	(1)	(b)	(エ) 暗号化された情報の復号又は電子署名の付与に用いる鍵について、管理手順を定めること。	Google は ISO27001 認証を受けています。この基準では、「暗号」(ISO 27001 2013、附属書 A.10)が規定されています。 Google は、Google Cloud PlatformプロダクトとG Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud Platform のお客様は、暗号鍵管理プロセスの開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。
6.1	6.1.5	(1)	(c)	情報システムセキュリティ責任者は、機関等における暗号化及び電子署名のアルゴリズム及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ 適用可能な電子証明書を政府認証基盤（GPKI）が発行している場合は、それを使用するように定めること。	ー
6.1	6.1.5	(2)	暗号化・電子署名に係る管理		
6.1	6.1.5	(2)	(a)	情報システムセキュリティ責任者は、暗号及び電子署名を適切な状況で利用するため、以下の措置を講ずること。	Google は ISO27001 認証を受けています。この基準では、「暗号」(ISO 27001 2013、附属書 A.10)が規定されています。 アップロード、作成されたお客様のデータを暗号化しています。Googleでは複数の暗号化レイヤを使用してデータを保護しています。複数の暗号化レイヤを使用することにより、冗長データ保護機能が追加され、アプリケーションの要件に基づいて最適な手法を選択できるようになります。 Google は、Google Cloud プロダクトと G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud Platform のお客様は、適切な暗号化対策の開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。
6.1	6.1.5	(2)	(a)	(ア) 電子署名の付与を行う情報システムにおいて、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全な方法で提供すること。	Google は ISO27001 認証を受けています。この基準では、「ログ取得及び監視」(ISO 27001 2013、附属書 A. 12.4)が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google のセキュリティモニタリング プログラムは、内部ネットワークトラフィックから収集されている情報、社員によるシステム上の操作、外部に知られている脆弱性に焦点を当てています。Google のグローバル ネットワークのさまざまな箇所で、内部トラフィックに疑わしい動作（たとえば、トラフィックにボットネットに接続している可能性が見られるなど）がないか検査しています。この分析では、オープンソースのツールと商用ツールを組み合わせて使用し、トラフィックのキャプチャと解析を行っています。Google の技術を基に構築された独自の相関システムもこの解析をサポートしています。こうしたネットワーク解析に加え、顧客データへのアクセスの試行などの異常な動向を特定するために、システムログを精査しています。Google のセキュリティエンジニアは、Google のインフラストラクチャに影響する可能性があるセキュリティ上のインシデントを検知する永続的な検索アラートを一般公開データレポジトリに設定しています。また、受信したセキュリティレポートの確認や、公開のメーリングリスト、ブログ、Wiki のモニタリングを積極的に行っています。自動ネットワーク解析は、未知の脅威が発生した可能性がある状態を検知してGoogle セキュリティ スタッフに通知します。ネットワーク解析に加え、システムログの自動解析も行われています。 Google Cloud Platform のお客様は、不正データや未確認データを検出するためのモニタリング設定など、お使いの環境を設定、管理するすべての権利と責任を保有します。

6.1	6.1.5	(2)	(a)	(イ) 暗号化を行う情報システム又は電子署名の付与若しくは検証を行う情報システムにおいて、暗号化又は電子署名のために選択されたアルゴリズムの危 殆化及びプロトコルの脆弱性に関する情報を定期的に入手し、必要に応じて、職員等と共有を図ること。	Google は ISO27001 認証を受けています。この基準では、「暗号」(ISO 27001 2013、附属書 A.10)が規定されています。 アップロード、作成されたお客様のデータを暗号化しています。Googleでは複数の暗号化レイヤを使用してデータを保護しています。複数の暗号化レイヤを使用することにより、冗長データ保護機能が追加され、アプリケーションの要件に基づいて最適な手法を選択できるようになります。 Google は、Google Cloud プロダクトと G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud Platform のお客様は、適切な暗号化対策の開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。
6.2	情報セキュリティの脅威への対策				
6.2	6.2.1	ソフトウェアに関する脆弱性対策			
6.2	6.2.1	(1)	ソフトウェアに関する脆弱性対策の実施		
6.2	6.2.1	(1)	(a)	情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開された脆弱性についての対策を実施すること。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」(附属書A.12.2)が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。
6.2	6.2.1	(1)	(b)	情報システムセキュリティ責任者は、公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上でとり得る対策がある場合は、当該対策を実施すること。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」(附属書A.12.2)が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。
6.2	6.2.1	(1)	(c)	情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェアにおける脆弱性対策の状況を定期的に確認すること。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」(附属書A.12.2)が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。
6.2	6.2.1	(1)	(d)	情報システムセキュリティ責任者は、脆弱性対策の状況の定期的な確認により、脆弱性対策が講じられていない状態が確認された場合並びにサーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずること。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」(附属書A.12.2)が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。
6.2	6.2.2	不正プログラム対策			
6.2	6.2.2	(1)	不正プログラム対策の実施		
6.2	6.2.2	(1)	(a)	情報システムセキュリティ責任者は、サーバ装置及び端末に不正プログラム対策ソフトウェア等を導入すること。ただし、当該サーバ装置及び端末で動作可能な不正プログラム対策ソフトウェア等が存在しない場合を除く。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」(附属書A.12.2)が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。
6.2	6.2.2	(1)	(b)	情報システムセキュリティ責任者は、想定される不正プログラムの感染経路の全てにおいて、不正プログラム対策ソフトウェア等により対策を講ずること。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」(附属書A.12.2)が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくはhttps://www.google.com/about/appsecurity/ をご覧ください。

6.2	6.2.2	(1)	(c)	情報システムセキュリティ責任者は、不正プログラム対策の状況を適宜把握し、必要な対処を行うこと。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」（附属書A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。
6.2	6.2.3	サービス不能攻撃対策			
6.2	6.2.3	(1)	サービス不能攻撃対策の実施		
6.2	6.2.3	(1)	(a)	情報システムセキュリティ責任者は、要安定情報を取り扱う情報システム（インターネットからアクセスを受ける情報システムに限る。以下本条において同じ。）については、サービス提供に必要なサーバ装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手段を用いてサービス不能攻撃への対策を行うこと。	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワークサービスへのアクセス」（ISO 27001 2013、附属書 A.9.1.2）と「ネットワーク セキュリティ管理」（ISO 27001 2013、附属書 A.13.1）が規定されています。 Google では厳格なインシデント管理プロセスにより、システムやデータの機密性、完全性、または可用性に影響を与える可能性があるセキュリティイベントに対応しています。インシデントが発生した場合、セキュリティチームはインシデントを 記録して、重大度に応じて優先順位を設定します。直接お客様に影響を与えるイベントには、特に高い優先順位が設定されます。このプロセスでは、行動方針や、通知、エスカレーション、対処、および文書化のための手順が指定されています。中心となるスタッフは、イベント発生に備えて、サードパーティツールや独自ツールの使用など、フォレンジクスや証拠取り扱いの訓練を受けています。お客様の機密情報を保存するシステムなどの重要な領域では、インシデント対応計画のテストを実施しています。こうしたテストでは、内部関係者による脅威やソフトウェアの脆弱性など、さまざまなシナリオが考慮されています。セキュリティ上のインシデントを早期解決するため、Google のセキュリティ チームは、24 時間体制で全社員からの問い合わせに対応しています。インシデントでお客様のデータが影響を受ける場合、Google またはそのパートナーはお客様にその旨を通知し、Google のサポートチームを通じて調査活動に協力します。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するほか、不正アクセスを検知、レビューするすべての権利と責任を保有します。
6.2	6.2.3	(1)	(b)	情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けた場合の影響を最小とする手段を備えた情報システムを構築すること。	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワークサービスへのアクセス」（ISO 27001 2013、附属書 A.9.1.2）と「ネットワーク管理策」（ISO 27001 2013、附属書 A.13.1）が規定されています。 Google では厳格なインシデント管理プロセスにより、システムやデータの機密性、完全性、または可用性に影響を与える可能性があるセキュリティイベントに対応しています。インシデントが発生した場合、セキュリティチームはインシデントを 記録して、重大度に応じて優先順位を設定します。直接お客様に影響を与えるイベントには、特に高い優先順位が設定されます。このプロセスでは、行動方針や、通知、エスカレーション、対処、および文書化のための手順が指定されています。中心となるスタッフは、イベント発生に備えて、サードパーティツールや独自ツールの使用など、フォレンジクスや証拠取り扱いの訓練を受けています。お客様の機密情報を保存するシステムなどの重要な領域では、インシデント対応計画のテストを実施しています。こうしたテストでは、内部関係者による脅威やソフトウェアの脆弱性など、さまざまなシナリオが考慮されています。セキュリティ上のインシデントを早期解決するため、Google のセキュリティ チームは、24 時間体制で全社員からの問い合わせに対応しています。インシデントでお客様のデータが影響を受ける場合、Google またはそのパートナーはお客様にその旨を通知し、Google のサポートチームを通じて調査活動に協力します。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するほか、不正アクセスを検知、レビューするすべての権利と責任を保有します。
6.2	6.2.3	(1)	(c)	情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定し、監視すること。	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワークサービスへのアクセス」（ISO 27001 2013、附属書 A.9.1.2）と「ネットワーク セキュリティ管理」（ISO 27001 2013、附属書 A.13.1）が規定されています。 Google では厳格なインシデント管理プロセスにより、システムやデータの機密性、完全性、または可用性に影響を与える可能性があるセキュリティイベントに対応しています。インシデントが発生した場合、セキュリティチームはインシデントを 記録して、重大度に応じて優先順位を設定します。直接お客様に影響を与えるイベントには、特に高い優先順位が設定されます。このプロセスでは、行動方針や、通知、エスカレーション、対処、および文書化のための手順が指定されています。中心となるスタッフは、イベント発生に備えて、サードパーティツールや独自ツールの使用など、フォレンジクスや証拠取り扱いの訓練を受けています。お客様の機密情報を保存するシステムなどの重要な領域では、インシデント対応計画のテストを実施しています。こうしたテストでは、内部関係者による脅威やソフトウェアの脆弱性など、さまざまなシナリオが考慮されています。セキュリティ上のインシデントを早期解決するため、Google のセキュリティ チームは、24 時間体制で全社員からの問い合わせに対応しています。インシデントでお客様のデータが影響を受ける場合、Google またはそのパートナーはお客様にその旨を通知し、Google のサポートチームを通じて調査活動に協力します。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するほか、不正アクセスを検知、レビューするすべての権利と責任を保有します。
6.2	6.2.4	標的型攻撃対策			
6.2	6.2.4	(1)	標的型攻撃対策の実施		
6.2	6.2.4	(1)	(a)	情報システムセキュリティ責任者は、情報システムにおいて、標的型攻撃による組織内部への侵入を低減する対策（入口対策）を講ずること。	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワークサービスへのアクセス」（ISO 27001 2013、附属書 A.9.1.2）と「ネットワーク セキュリティ管理」（ISO 27001 2013、附属書 A.13.1）が規定されています。 Google では厳格なインシデント管理プロセスにより、システムやデータの機密性、完全性、または可用性に影響を与える可能性があるセキュリティイベントに対応しています。インシデントが発生した場合、セキュリティチームはインシデントを 記録して、重大度に応じて優先順位を設定します。直接お客様に影響を与えるイベントには、特に高い優先順位が設定されます。このプロセスでは、行動方針や、通知、エスカレーション、対処、および文書化のための手順が指定されています。中心となるスタッフは、イベント発生に備えて、サードパーティツールや独自ツールの使用など、フォレンジクスや証拠取り扱いの訓練を受けています。お客様の機密情報を保存するシステムなどの重要な領域では、インシデント対応計画のテストを実施しています。こうしたテストでは、内部関係者による脅威やソフトウェアの脆弱性など、さまざまなシナリオが考慮されています。セキュリティ上のインシデントを早期解決するため、Google のセキュリティ チームは、24 時間体制で全社員からの問い合わせに対応しています。インシデントでお客様のデータが影響を受ける場合、Google またはそのパートナーはお客様にその旨を通知し、Google のサポートチームを通じて調査活動に協力します。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するほか、不正アクセスを検知、レビューするすべての権利と責任を保有します。

6.2	6.2.4	(1)	(b)	情報システムセキュリティ責任者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）を講ずること。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」（附属書A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受けSOC 2、Type II の報告書を取得しています。 Googleはセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソースツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。
6.3	アプリケーション・コンテンツの作成・提供				
6.3	6.3.1	アプリケーション・コンテンツの作成時の対策			
6.3	6.3.1	(1)	アプリケーション・コンテンツの作成に係る規定の整備		
6.3	6.3.1	(1)	(a)	統括情報セキュリティ責任者は、アプリケーション・コンテンツの提供時に機関等外の情報セキュリティ水準の低下を招く行為を防止するための規定を整備すること。	―
6.3	6.3.1	(2)	アプリケーション・コンテンツのセキュリティ要件の策定		
6.3	6.3.1	(2)	(a)	情報システムセキュリティ責任者は、機関等外の情報システム利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション・コンテンツについて以下の内容を仕様に含めること。	―
6.3	6.3.1	(2)	(a)	(ア)提供するアプリケーション・コンテンツが不正プログラムを含まないこと。	―
6.3	6.3.1	(2)	(a)	(イ)提供するアプリケーションが脆弱性を含まないこと。	―
6.3	6.3.1	(2)	(a)	(ウ)実行プログラムの形式以外にコンテンツを提供する手段がない場合を除き、実行プログラムの形式でコンテンツを提供しないこと。	―
6.3	6.3.1	(2)	(a)	(エ)電子証明書を用いた署名等、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段をアプリケーション・コンテンツの提供先に与えること。	―
6.3	6.3.1	(2)	(a)	(オ)提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンのOSやソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、OSやソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。	―
6.3	6.3.1	(2)	(a)	(カ)サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。	―
6.3	6.3.1	(2)	(b)	職員等は、アプリケーション・コンテンツの開発・作成を外部委託する場合において、前項各号に掲げる内容を調達仕様に含めること。	―
6.3	6.3.2	アプリケーション・コンテンツ提供時の対策			
6.3	6.3.2	(1)	政府ドメイン名の使用		
6.3	6.3.2	(1)	(a)	情報システムセキュリティ責任者は、機関等外向けに提供するウェブサイト等が実際の機関等提供のものであることを利用者が確認できるように、政府ドメイン名を情報システムにおいて使用すること。ただし、次に掲げる場合を除く。	―
6.3	6.3.2	(1)	(a)	(ア) 指定法人が政府ドメイン名を登録する資格を持たない場合。この場合において、当該法人は、組織の属性が資格条件となっており、不特定の個人及び組織 が取得することのできないドメイン名を使用すること。	―
6.3	6.3.2	(1)	(a)	(イ) 独立行政法人及び指定法人のうち教育機関である法人が、高等教育機関向けのドメイン名を使用する場合。この場合において、当該法人は、あらかじめ、 情報セキュリティの確保の観点から、政府ドメイン名と高等教育機関向けのドメイン名のどちらを使用するべきかを比較考慮の上、判断すること。	―
6.3	6.3.2	(1)	(a)	(ウ)4.1.3 に掲げるソーシャルメディアサービスによる情報発信を行う場合	―
6.3	6.3.2	(1)	(b)	職員等は、機関等外向けに提供するウェブサイト等の作成を外部委託する場合においては、前項各号列記以外の部分、同項ア)及び(イ)の規定に則り当該機関等に適するドメイン名を使用するよう調達仕様に含めること。	―
6.3	6.3.2	(2)	不正なウェブサイトへの誘導防止		
6.3	6.3.2	(2)	(a)	情報システムセキュリティ責任者は、利用者が検索サイト等を経由して機関等のウェブサイトになりすました不正なウェブサイトへ誘導されないよう対策を講ずること。	―
6.3	6.3.2	(3)	アプリケーション・コンテンツの告知		
6.3	6.3.2	(3)	(a)	職員等は、アプリケーション・コンテンツを告知する場合は、告知する対象となるアプリケーション・コンテンツに利用者が確実に誘導されるよう、必要な措置を講ずること。	―
6.3	6.3.2	(3)	(b)	職員等は、機関等外の者が提供するアプリケーション・コンテンツを告知する場合は、告知するURL 等の有効性を保つこと。	―
情報システムの構成要素					
7.1	端末・サーバ装置等				

7.1	7.1.1	端末			
7.1	7.1.1	(1)	端末の導入時の対策		
7.1	7.1.1	(1)	(a)	情報システムセキュリティ責任者は、要保護情報を取り扱う端末について、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。	Google は ISO27001 認証を受けています。この基準では、「装置」(ISO 27001 2013、附属書 A.11.2)が規定されています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティモデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 Google のデータセンタープロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
7.1	7.1.1	(1)	(b)	情報システムセキュリティ責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」(附属書A.8.1)、「媒体の処分」(附属書 A.8.3.2)、「装置のセキュリティを保った処分または再利用」(附属書A.11.2.7)、「運用ソフトウェアの管理」(附属書 A. 12.5)が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する 際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
7.1	7.1.1	(2)	端末の運用時の対策		
7.1	7.1.1	(2)	(a)	情報システムセキュリティ責任者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行うこと。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」(附属書A.8.1)、「媒体の処分」(附属書 A.8.3.2)、「装置のセキュリティを保った処分または再利用」(附属書A.11.2.7)、「運用ソフトウェアの管理」(附属書 A. 12.5)が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する 際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
7.1	7.1.1	(2)	(b)	情報システムセキュリティ責任者は、所管する範囲の端末で利用されている全てのソフトウェアの状態を定期的に調査し、不適切な状態にある端末を検出等した場合には、改善を図ること。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」(附属書A.8.1)、「媒体の処分」(附属書 A.8.3.2)、「装置のセキュリティを保った処分または再利用」(附属書A.11.2.7)、「運用ソフトウェアの管理」(附属書 A. 12.5)が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する 際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
7.1	7.1.1	(3)	端末の運用終了時の対策		
7.1	7.1.1	(3)	(a)	情報システムセキュリティ責任者は、端末の運用を終了する際に、端末の電磁的記録媒体の全ての情報を抹消すること。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」(ISO 27001 2013、附属書 A.8.3.2)と「装置のセキュリティを保った処分または再利用」(ISO 27001 2013、附属書 A.11.2.7)が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する 際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。
7.1	7.1.1	(4)	要機密情報を取り扱う機関等が支給する端末(要管理対策区域外で使用する場合に限る)及び機関等支給以外の端末の導入及び利用時の対策		
7.1	7.1.1	(4)	(a)	統括情報セキュリティ責任者は、要機密情報を取り扱う機関等が支給する端末(要管理対策区域外で使用する場合に限る)及び機関等支給以外の端末について、以下の安全管理措置に関する規定を整備すること。	ー
7.1	7.1.1	(4)	(a)	(ア) 盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための技術的な措置	ー
7.1	7.1.1	(4)	(a)	(イ) 機関等支給以外の端末において不正プログラムの感染等により情報窃取されることを防止するための利用時の措置	ー
7.1	7.1.1	(4)	(b)	情報セキュリティ責任者は、機関等支給以外の端末を用いた機関等の業務に係る情報処理に関する安全管理措置の実施状況を管理する責任者(以下「端末管理責任者」という。)を定めること。	ー
7.1	7.1.1	(4)	(c)	次の各号に掲げる責任者は、職員等が当該各号に定める端末を用いて要機密情報を取り扱う場合は、当該端末について(a)(ア)の安全管理措置を講ずること。	ー
7.1	7.1.1	(4)	(c)	(ア) 情報システムセキュリティ責任者 機関等が支給する端末(要管理対策区域外で使用する場合に限る)	ー
7.1	7.1.1	(4)	(c)	(イ) 端末管理責任者 機関等支給以外の端末	ー

7.1	7.1.1	(4)	(d)	端末管理責任者は、要機密情報を取り扱う機関等支給以外の端末について、前項の規定にかかわらず(a)(ア)に定める安全管理措置のうち自ら講ずることができないもの、及び(a)(イ)に定める安全管理措置を職員等に講じさせること。	ー
7.1	7.1.1	(4)	(e)	職員等は、要機密情報を取り扱う機関等支給以外の端末について、前項において(a)(ア)に定める安全管理措置のうち端末管理責任者が講ずることができないもの、及び(a)(イ)に定める安全管理措置を講ずること。	ー
7.1	7.1.2	サーバ装置			
7.1	7.1.2	(1)	サーバ装置の導入時の対策		
7.1	7.1.2	(1)	(a)	情報システムセキュリティ責任者は、要保護情報を取り扱うサーバ装置について、サーバ装置の盗難、不正な持ち出し、不正な操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。	Google は ISO27001 認証を受けています。この基準では、「装置」(ISO 27001 2013、附属書 A.11.2)が規定されています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティモデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 Google のデータセンタープロセスについて詳しくは、Google セキュリティホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
7.1	7.1.2	(1)	(b)	情報システムセキュリティ責任者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、要安定情報を取り扱う情報システムについて、サービス提供に必要なサーバ装置を冗長構成にするなどにより可用性を確保すること。	Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001 2013、附属書 A.17.2)が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェアサービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud Platform のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。
7.1	7.1.2	(1)	(c)	情報システムセキュリティ責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、サーバ装置で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」(附属書 A.8.1)、「媒体の処分」(附属書 A.8.3.2)、「装置のセキュリティを保った処分または再利用」(附属書 A.11.2.7)、「運用ソフトウェアの管理」(附属書 A. 12.5)が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する 際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
7.1	7.1.2	(1)	(d)	情報システムセキュリティ責任者は、通信回線を経由してサーバ装置の保守作業を行う際に送受信される情報が漏えいすることを防止するための対策を講ずること。	Google は ISO27001 認証を受けています。この基準では、「暗号」(ISO 27001 2013、附属書 A.10)が規定されています。 インターネットを介した認証と管理者アクセスを保護するために暗号化を使用しています。Googleが管理するマシンにリモートアクセスする場合は、Googleが発行したデジタル証明書と2要素認証を必要とします。 Google は、Google Cloud プロダクトと G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud Platform のお客様は、適切な暗号化対策の開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。
7.1	7.1.2	(2)	サーバ装置の運用時の対策		
7.1	7.1.2	(2)	(a)	情報システムセキュリティ責任者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行うこと。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」(附属書 A.8.1)、「媒体の処分」(附属書 A.8.3.2)、「装置のセキュリティを保った処分または再利用」(附属書 A.11.2.7)、「運用ソフトウェアの管理」(附属書 A. 12.5)が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する 際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。

7.1	7.1.2	(2)	(b)	情報システムセキュリティ責任者は、所管する範囲のサーバ装置の構成やソフトウェアの状態を定期的に確認し、不適切な状態にあるサーバ装置を検出等した場合 には改善を図ること。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する 際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
7.1	7.1.2	(2)	(c)	情報システムセキュリティ責任者は、サーバ装置上での不正な行為、無許可のアクセス等の意図しない事象の発生を検知する必要がある場合は、当該サーバ装置を監視するための措置を講ずること。ただし、サーバ装置の利用環境等から不要と判断できる場合はこの限りではない。	Google は ISO27001 認証を受けています。この基準では、「ログ取得及び監視」（ISO 27001 2013、附属書 A. 12.4）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google のセキュリティ モニタリング プログラムは、内部ネットワークトラフィックから収集されている情報、社員によるシステム上の操作、外部に知られている脆弱性に焦点を当てています。Google のグローバル ネットワークのさまざまな箇所で、内部トラフィックに疑わしい動作（たとえば、トラフィックにボットネットに接続している可能性が見られるなど）がないか検査しています。この分析では、オープンソースのツールと商用ツールを組み合わせて使用し、トラフィックのキャプチャと解析を行っています。Google の技術を基に構築された独自の相関システムもこの解析をサポートしています。こうしたネットワーク解析に加え、顧客データへのアクセスの試行などの異常な動向を特定するために、システムログを精査しています。Google のセキュリティ エンジニアは、Google のインフラストラクチャに影響する可能性があるセキュリティ上のインシデントを検知する永続的な検索アラートを一般公開データ リポジトリに設定しています。また、受信したセキュリティレポートの確認や、公開のメーリングリスト、ブログ、Wiki のモニタリングを積極的に行っています。自動ネットワーク解析は、未知の脅威が発生した可能性がある状態を検知して Google セキュリティ スタッフに通知します。ネットワーク解析 に加え、システムログの自動解析も行われています。
7.1	7.1.2	(2)	(d)	情報システムセキュリティ責任者は、要安定情報を取り扱うサーバ装置について、サーバ装置が運用できなくなった場合に正常な運用状態に復元することが可能とな るよう、必要な措置を講ずること。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。
7.1	7.1.2	(3)	サーバ装置の運用終了時の対策		
7.1	7.1.2	(3)	(a)	情報システムセキュリティ責任者は、サーバ装置の運用を終了する際に、サーバ装置の電磁的記録媒体の全ての情報を抹消すること。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する 際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。
7.1	7.1.3	複合機・特定用途機器			
7.1	7.1.3	(1)	複合機		
7.1	7.1.3	(1)	(a)	情報システムセキュリティ責任者は、複合機を調達する際には、当該複合機が備える機能、設置環境並びに取り扱う情報の格付及び取扱制限に応じ、適切なセキュリティ要件を策定すること。	ー
7.1	7.1.3	(1)	(b)	情報システムセキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講ずること。	ー
7.1	7.1.3	(1)	(c)	情報システムセキュリティ責任者は、複合機の運用を終了する際に、複合機の電磁的記録媒体の全ての情報を抹消すること。	ー
7.1	7.1.3	(2)	IoT機器を含む特定用途機器		
7.1	7.1.3	(2)	(a)	情報システムセキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により脅威が存在する場合には、当該機器の特性に応じた対策を講ずること。	ー
7.2	電子メール・ウェブ等				
7.2	7.2.1	電子メール			
7.2	7.2.1	(1)	電子メールの導入時の対策		
7.2	7.2.1	(1)	(a)	情報システムセキュリティ責任者は、電子メールサーバが電子メールの不正な中継を行わないように設定すること。	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワーク サービスへのアクセス」（ISO 27001 2013、附属書 A.9.1.2）と「ネットワーク セキュリティ管理」（ISO 27001 2013、附属書 A.13.1）が規定されています。 Google では厳格なインシデント管理プロセスにより、システムやデータの機密性、完全性、または可用性に影響を与える可能性があるセキュリティイベントに対応しています。インシデントが発生した場合、セキュリティ チームはインシデントを 記録して、重大度に応じて優先順位を設定します。直接お客様に影響を与えるイベントには、特に高い優先順位が設定されます。このプロセスでは、行動方針や、通知、エスカレーション、対処、および文書化のための手順が指定されています。中心となるスタッフは、イベント発生に備えて、サードパーティ ツールや独自ツールの使用など、フォレンジクスや証拠取り扱いの訓練を受けています。お客様の機密情報を保存するシステムなどの重要な領域では、インシデント対応計画のテストを実施しています。こうしたテストでは、内部関係者による脅威やソフトウェアの脆弱性など、さまざまなシナリオが考慮されています。セキュリティ上のインシデントを早期解決するため Google のセキュリティ チームは、24 時間体制で全社員からの問い合わせに対応しています。インシデントでお客様のデータが影響を受ける場合、Google またはそのパートナーはお客様にその旨を通知し、Google のサポートチームを通じて調査活動に協力します。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するほか、不正アクセスを検知、レビューするすべての権利と責任を保有します。

7.2	7.2.1	(1)	(b)	情報システムセキュリティ責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に主体認証を行う機能を備えること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールやGoogle 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフローツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定　の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
7.2	7.2.1	(1)	(c)	情報システムセキュリティ責任者は、電子メールのなりすましの防止策を講ずること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールやGoogle 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフローツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定　の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
7.2	7.2.1	(1)	(d)	情報システムセキュリティ責任者は、インターネットを介して通信する電子メールの盗聴及び改ざんの防止のため、電子メールのサーバ間通信の暗号化の対策を講ずること。	Google は ISO27001 認証を受けています。この基準では、「暗号」(ISO 27001 2013、附属書 A.10)が規定されています。 インターネットを介した認証と管理者アクセスを保護するために暗号化を使用しています。Googleが管理するマシンにリモートアクセスする場合は、Googleが発行したデジタル証明書と2要素認証を必要とします。 Google は、Google Cloud プロダクトと G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud Platform のお客様は、適切な暗号化対策の開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。
7.2	7.2.2	ウェブ			
7.2	7.2.2	(1)	ウェブサーバの導入・運用時の対策		
7.2	7.2.2	(1)	(a)	情報システムセキュリティ責任者は、ウェブサーバの管理や設定において、以下の事項を含む情報セキュリティ確保のための対策を講ずること。	Google は ISO27001 認証を受けています。この基準では、「システムの取得、開発および保守」(ISO 27001 2013、附属書 A.14)が規定されています。 Google Cloud Platform のお客様は、システム開発プロセスの管理など、お使いの環境を設定、管理するすべての権利と責任を保有します。
7.2	7.2.2	(1)	(a)	(ア)ウェブサーバが備える機能のうち、不要な機能を停止又は制限すること。	Google は ISO27001 認証を受けています。この基準では、「システムの取得、開発および保守」(ISO 27001 2013、附属書 A.14)が規定されています。 Google Cloud Platform のお客様は、システム開発プロセスの管理など、お使いの環境を設定、管理するすべての権利と責任を保有します。
7.2	7.2.2	(1)	(a)	(イ)ウェブコンテンツの編集作業を担当する主体を限定すること。	―
7.2	7.2.2	(1)	(a)	(ウ)公開してはならない又は無意味なウェブコンテンツが公開されないように管理すること。	―
7.2	7.2.2	(1)	(a)	(エ)ウェブコンテンツの編集作業に用いる端末を限定し、識別コード及び主体認証情報を適切に管理すること。	―
7.2	7.2.2	(1)	(a)	(オ) インターネットを介して転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化及び電子証明書による認証の対策を講じること。	―
7.2	7.2.2	(1)	(b)	情報システムセキュリティ責任者は、ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認すること。	―
7.2	7.2.2	(2)	ウェブアプリケーションの開発時・運用時の対策		
7.2	7.2.2	(2)	(a)	情報システムセキュリティ責任者は、ウェブアプリケーションの開発において、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講ずること。また、運用時においても、これらの対策に漏れが無いか定期的に確認し、対策に漏れがある状態が確認された場合は対処を行うこと。	―
7.2	7.2.3	ドメインネームシステム(DNS)			
7.2	7.2.3	(1)	DNS の導入時の対策		

7.2	7.2.3	(1)	(a)	情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムの名前解決を提供するコンテンツサーバにおいて、名前解決を停止させないための措置を講ずること。	Google は ISO27001 認証を受けています。この基準では、「容量・能力の管理」(ISO 27001 2013、附属書 A. 12.1.3)が規定されています。 Google Cloud Platform のお客様は、リソース管理など、お使いの環境を設定、管理するすべての権利と責任を保有します。
7.2	7.2.3	(1)	(b)	情報システムセキュリティ責任者は、キャッシュサーバにおいて、名前解決の要求への適切な応答をするための措置を講ずること。	Google は ISO27001 認証を受けています。この基準では、「容量・能力の管理」(ISO 27001 2013、附属書 A. 12.1.3)が規定されています。 Google Cloud Platform のお客様は、リソース管理など、お使いの環境を設定、管理するすべての権利と責任を保有します。
7.2	7.2.3	(1)	(c)	情報システムセキュリティ責任者は、コンテンツサーバにおいて、機関等のみで使用する名前の解決を提供する場合、当該コンテンツサーバで管理する情報が外部に漏えいしないための措置を講ずること。	Google は ISO27001 認証を受けています。この基準では、「ログ取得及び監視」(ISO 27001 2013、附属書 A. 12.4)が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google のセキュリティ モニタリング プログラムは、内部ネットワークトラフィックから収集されている情報、社員によるシステム上の操作、外部に知られている脆弱性に焦点を当てています。Google のグローバル ネットワークのさまざまな箇所で、内部トラフィックに疑わしい動作(たとえば、トラフィックにボットネットに接続している可能性が見られるなど)がないか検査しています。この分析では、オープンソースのツールと商用ツールを組み合わせて使用し、トラフィックのキャプチャと解析を行っています。Google の技術を基に構築された独自の相関システムもこの解析をサポートしています。こうしたネットワーク解析に加え、顧客データへのアクセスの試行などの異常な動向を特定するために、システムログを精査しています。Google のセキュリティエンジニアは、Google のインフラストラクチャに影響する可能性があるセキュリティ上のインシデントを検知する永続的な検索アラートを一般公開データレポジトリに設定しています。また、受信したセキュリティレポートの確認や、公開のメーリングリスト、ブログ、Wiki のモニタリングを積極的に行っています。自動ネットワーク解析は、未知の脅威が発生した可能性がある状態を検知して Google セキュリティ スタッフに通知します。ネットワーク解析に加え、システムログの自動解析も行われています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理、モニタリングするすべての権利と責任を保有します。
7.2	7.2.3	(2)	DNS の運用時の対策		
7.2	7.2.3	(2)	(a)	情報システムセキュリティ責任者は、コンテンツサーバを複数台設置する場合は、管理するドメインに関する情報についてサーバ間で整合性を維持すること。	ー
7.2	7.2.3	(2)	(b)	情報システムセキュリティ責任者は、コンテンツサーバにおいて管理するドメインに関する情報が正確であることを定期的に確認すること。	Google は ISO27001 認証を受けています。この基準では、「ログ取得及び監視」(ISO 27001 2013、附属書 A. 12.4)が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google のセキュリティ モニタリング プログラムは、内部ネットワークトラフィックから収集されている情報、社員によるシステム上の操作、外部に知られている脆弱性に焦点を当てています。Google のグローバル ネットワークのさまざまな箇所で、内部トラフィックに疑わしい動作(たとえば、トラフィックにボットネットに接続している可能性が見られるなど)がないか検査しています。この分析では、オープンソースのツールと商用ツールを組み合わせて使用し、トラフィックのキャプチャと解析を行っています。Google の技術を基に構築された独自の相関システムもこの解析をサポートしています。こうしたネットワーク解析に加え、顧客データへのアクセスの試行などの異常な動向を特定するために、システムログを精査しています。Google のセキュリティエンジニアは、Google のインフラストラクチャに影響する可能性があるセキュリティ上のインシデントを検知する永続的な検索アラートを一般公開データレポジトリに設定しています。また、受信したセキュリティレポートの確認や、公開のメーリングリスト、ブログ、Wiki のモニタリングを積極的に行っています。自動ネットワーク解析は、未知の脅威が発生した可能性がある状態を検知して Google セキュリティ スタッフに通知します。ネットワーク解析に加え、システムログの自動解析も行われています。 Google Cloud Platform のお客様は、お使いの環境を設定、管理、モニタリングするすべての権利と責任を保有します。
7.2	7.2.3	(2)	(c)	情報システムセキュリティ責任者は、キャッシュサーバにおいて、名前解決の要求への適切な応答を維持するための措置を講ずること。	Google は ISO27001 認証を受けています。この基準では、「容量・能力の管理」(ISO 27001 2013、附属書 A. 12.1.3)が規定されています。 Google Cloud Platform のお客様は、リソース管理など、お使いの環境を設定、管理するすべての権利と責任を保有します。
7.2	7.2.4	データベース			
7.2	7.2.4	(1)	データベースの導入・運用時の対策		
7.2	7.2.4	(1)	(a)	情報システムセキュリティ責任者は、データベースに対する内部不正を防止するため、管理者アカウントの適正な権限管理を行うこと。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフローツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポートサービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud Platform のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。
7.2	7.2.4	(1)	(b)	情報システムセキュリティ責任者は、データベースに格納されているデータにアクセスした利用者を特定できるよう、措置を講ずること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフローツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポートサービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud Platform のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。

7.2	7.2.4	(1)	(c)	情報システムセキュリティ責任者は、データベースに格納されているデータに対するアクセス権を有する利用者によるデータの不正な操作を検知できるよう、対策を講ずること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフローツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定　の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。
7.2	7.2.4	(1)	(d)	情報システムセキュリティ責任者は、データベース及びデータベースへアクセスする機器等の脆弱性を悪用した、データの不正な操作を防止するための対策を講ずること。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」(附属書 A.12.2)が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け SOC 2、Type II の報告書を取得しています。 Google はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。
7.2	7.2.4	(1)	(e)	情報システムセキュリティ責任者は、データの窃取、電磁的記録媒体の盗難等による情報の漏えいを防止する必要がある場合は、適切に暗号化をすること。	Google は ISO27001 認証を受けています。この基準では、「暗号」(ISO 27001 2013、附属書 A.10)が規定されています。 アップロード、作成されたお客様のデータを暗号化しています。Google では複数の暗号化レイヤを使用してデータを保護しています。複数の暗号化レイヤを使用することにより、冗長データ保護機能が追加され、アプリケーションの要件に基づいて最適な手法を選択できるようになります。 Google は、Google Cloud プロダクトと G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud Platform のお客様は、適切な暗号化対策の開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。
7.3	通信回線				
7.3	7.3.1	通信回線			
7.3	7.3.1	(1)	通信回線の導入時の対策		
7.3	7.3.1	(1)	(a)	情報システムセキュリティ責任者は、通信回線構築時に、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限に応じた適切な回線種別を選択し、情報セキュリティインシデントによる影響を回避するために、通信回線に対して必要な対策を講ずること。	Google は ISO27001 認証を受けています。この基準では、「通信のセキュリティ」(ISO 27001 2013、附属書 A.13)と「公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮」(ISO27002 2013、附属書 A.14.1.2)が規定されています。 Google Cloud Platform のお客様は、外部接続の管理など、お使いの環境を設定、管理するすべての権利と責任を保有します。
7.3	7.3.1	(1)	(b)	情報システムセキュリティ責任者は、通信回線において、サーバ装置及び端末のアクセス制御及び経路制御を行う機能を設けること。	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワークサービスへのアクセス」(ISO 27001 2013、附属書 A.9.1.2)と「ネットワーク セキュリティ管理」(ISO 27001 2013、附属書 A.13.1)が規定されています。 Google では厳格なインシデント管理プロセスにより、システムやデータの機密性、完全性、または可用性に影響を与える可能性があるセキュリティイベントに対応しています。インシデントが発生した場合、セキュリティ チームはインシデントを 記録して、重大度に応じて優先順位を設定します。直接お客様に影響を与えるイベントには、特に高い優先順位が設定されます。このプロセスでは、行動方針や、通知、エスカレーション、対処、および文書化のための手順が指定されています。中心となるスタッフは、イベント発生に備えて、サードパーティ ツールや独自ツールの使用など、フォレンジクスや証拠取り扱いの訓練を受けています。お客様の機密情報を保存するシステムなどの重要な領域では、インシデント対応計画のテストを実施しています。こうしたテストでは、内部関係者による脅威やソフトウェアの脆弱性など、さまざまなシナリオが考慮されています。セキュリティ上のインシデントを早期解決するため、Google のセキュリティ チームは、24 時間体制で全社員からの問い合わせに対応しています。インシデントでお客様のデータが影響を受ける場合、Google またはそのパートナーはお客様にその旨を通知し、Google のサポートチームを通じて調査活動に協力します。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するほか、不正アクセスを検知、レビューするすべての権利と責任を保有します。
7.3	7.3.1	(1)	(c)	情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムを通信回線に接続する際に、通信内容の秘匿性の確保が必要と考える場合は、通信内容の秘匿性を確保するための措置を講ずること。	Google は ISO27001 認証を受けています。この基準では、「暗号」(ISO 27001 2013、附属書 A.10)が規定されています。 インターネットを介した認証と管理者アクセスを保護するために暗号化を使用しています。Google が管理するマシンにリモートアクセスする場合は、Google が発行したデジタル証明書と 2 要素認証を必要とします。 Google は、Google Cloud プロダクトと G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud Platform のお客様は、適切な暗号化対策の開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。
7.3	7.3.1	(1)	(d)	情報システムセキュリティ責任者は、職員等が通信回線へ情報システムを接続する際に、当該情報システムが接続を許可されたものであることを確認するための措置を講ずること。機関等内通信回線へ機関等支給以外の端末を接続する際も同様とする。	Google は ISO27001 認証を受けています。この基準では、「通信のセキュリティ」(ISO 27001 2013、附属書 A.13)と「公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮」(ISO27002 2013、附属書 A.14.1.2)が規定されています。 Google Cloud Platform のお客様は、外部接続の管理など、お使いの環境を設定、管理するすべての権利と責任を保有します。

7.3	7.3.1	(1)	(e)	情報システムセキュリティ責任者は、通信回線装置を要管理対策区域に設置すること。ただし、要管理対策区域への設置が困難な場合は、物理的な保護措置を講ずるなどして、第三者による破壊や不正な操作等が行われないようにすること。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェアサービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google は、データセンターが所在するリージョンの建築要件と設備要件をすべて満たしています。
7.3	7.3.1	(1)	(f)	情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムが接続される通信回線について、当該通信回線の継続的な運用を可能とするための措置を講ずること。	Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001 2013、附属書 A.17.2)が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェアサービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud Platform のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。
7.3	7.3.1	(1)	(g)	情報システムセキュリティ責任者は、機関等内通信回線にインターネット回線、公衆通信回線等の機関等外通信回線を接続する場合には、機関等内通信回線及び当該機関等内通信回線に接続されている情報システムの情報セキュリティを確保するための措置を講ずること。	ー
7.3	7.3.1	(1)	(h)	情報システムセキュリティ責任者は、機関等内通信回線と機関等外通信回線との間で送受信される通信内容を監視するための措置を講ずること。	ー
7.3	7.3.1	(1)	(i)	情報システムセキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアを定め、ソフトウェアを変更する際の許可申請手順を整備すること。ただし、ソフトウェアを変更することが困難な通信回線装置の場合は、この限りでない。	ー
7.3	7.3.1	(1)	(j)	情報システムセキュリティ責任者は、保守又は診断のために、遠隔地から通信回線装置に対して行われるリモートアクセスに係る情報セキュリティを確保すること。	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワークサービスへのアクセス」(ISO 27001 2013、附属書 A.9.1.2)と「ネットワークセキュリティ管理」(ISO 27001 2013、附属書 A.13.1)が規定されています。 Google では厳格なインシデント管理プロセスにより、システムやデータの機密性、完全性、または可用性に影響を与える可能性があるセキュリティイベントに対応しています。インシデントが発生した場合、セキュリティチームはインシデントを 記録して、重大度に応じて優先順位を設定します。直接お客様に影響を与えるイベントには、特に高い優先順位が設定されます。このプロセスでは、行動方針や、通知、エスカレーション、対処、および文書化のための手順が指定されています。中心となるスタッフは、イベント発生に備えて、サードパーティツールや独自ツールの使用など、フォレンジクスや証拠取り扱いの訓練を受けています。お客様の機密情報を保存するシステムなどの重要な領域では、インシデント対応計画のテストを実施しています。こうしたテストでは、内部関係者による脅威やソフトウェアの脆弱性など、さまざまなシナリオが考慮されています。セキュリティ上のインシデントを早期解決するため、Google のセキュリティ チームは、24 時間体制で全社員からの問い合わせに対応しています。インシデントでお客様のデータが影響を受ける場合、Google またはそのパートナーはお客様にその旨を通知し、Google のサポートチームを通じて調査活動に協力します。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するほか、不正アクセスを検知、レビューするすべての権利と責任を保有します。
7.3	7.3.1	(1)	(k)	情報システムセキュリティ責任者は、電気通信事業者の通信回線サービスを利用する場合には、当該通信回線サービスの情報セキュリティ水準及びサービスレベルを確保するための措置について、情報システムの構築を委託する事業者と契約時に取り決めておくこと。	Google は ISO27001 認証を受けています。この基準では、「通信のセキュリティ」(ISO 27001 2013、附属書 A.13)と「公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮」(ISO27002 2013、附属書 A.14.1.2)が規定されています。 Google Cloud Platform のお客様は、外部接続の管理など、お使いの環境を設定、管理するすべての権利と責任を保有します。
7.3	7.3.1	(2)	通信回線の運用時の対策		
7.3	7.3.1	(2)	(a)	情報システムセキュリティ責任者は、情報セキュリティインシデントによる影響を防止するために、通信回線装置の運用時に必要な措置を講ずること。	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワークサービスへのアクセス」(ISO 27001 2013、附属書 A.9.1.2)と「ネットワークセキュリティ管理」(ISO 27001 2013、附属書 A.13.1)が規定されています。 Google では厳格なインシデント管理プロセスにより、システムやデータの機密性、完全性、または可用性に影響を与える可能性があるセキュリティイベントに対応しています。インシデントが発生した場合、セキュリティチームはインシデントを 記録して、重大度に応じて優先順位を設定します。直接お客様に影響を与えるイベントには、特に高い優先順位が設定されます。このプロセスでは、行動方針や、通知、エスカレーション、対処、および文書化のための手順が指定されています。中心となるスタッフは、イベント発生に備えて、サードパーティツールや独自ツールの使用など、フォレンジクスや証拠取り扱いの訓練を受けています。お客様の機密情報を保存するシステムなどの重要な領域では、インシデント対応計画のテストを実施しています。こうしたテストでは、内部関係者による脅威やソフトウェアの脆弱性など、さまざまなシナリオが考慮されています。セキュリティ上のインシデントを早期解決するため、Google のセキュリティ チームは、24 時間体制で全社員からの問い合わせに対応しています。インシデントでお客様のデータが影響を受ける場合、Google またはそのパートナーはお客様にその旨を通知し、Google のサポートチームを通じて調査活動に協力します。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するほか、不正アクセスを検知、レビューするすべての権利と責任を保有します。

7.3	7.3.1	(2)	(b)	情報システムセキュリティ責任者は、経路制御及びアクセス制御を適切に運用し、通信回線や通信要件の変更の際及び定期的に、経路制御及びアクセス制御の設定の見直しを行うこと。	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワークサービスへのアクセス」（ISO 27001 2013、附属書 A.9.1.2）と「ネットワークセキュリティ管理」（ISO 27001 2013、附属書 A.13.1）が規定されています。 Google では厳格なインシデント管理プロセスにより、システムやデータの機密性、完全性、または可用性に影響を与える可能性があるセキュリティイベントに対応しています。インシデントが発生した場合、セキュリティチームはインシデントを 記録して、重大度に応じて優先順位を設定します。直接お客様に影響を与えるイベントには、特に高い優先順位が設定されます。このプロセスでは、行動方針や、通知、エスカレーション、対処、および文書化のための手順が指定されています。中心となるスタッフは、イベント発生に備えて、サードパーティツールや独自ツールの使用など、フォレンジクスや証拠取り扱いの訓練を受けています。お客様の機密情報を保存するシステムなどの重要な領域では、インシデント対応計画のテストを実施しています。こうしたテストでは、内部関係者による脅威やソフトウェアの脆弱性など、さまざまなシナリオが考慮されています。セキュリティ上のインシデントを早期解決するため、Google のセキュリティ チームは、24 時間体制で全社員からの問い合わせに対応しています。インシデントでお客様のデータが影響を受ける場合、Google またはそのパートナーはお客様にその旨を通知し、Google のサポートチームを通じて調査活動に協力します。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するほか、不正アクセスを検知、レビューするすべての権利と責任を保有します。
7.3	7.3.1	(2)	(c)	情報システムセキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアの状態を定期的に調査し、許可されていないソフトウェアがインストールされているなど、不適切な状態にある通信回線装置を認識した場合には、改善を図ること。	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワークサービスへのアクセス」（ISO 27001 2013、附属書 A.9.1.2）と「ネットワークセキュリティ管理」（ISO 27001 2013、附属書 A.13.1）が規定されています。 Google では厳格なインシデント管理プロセスにより、システムやデータの機密性、完全性、または可用性に影響を与える可能性があるセキュリティイベントに対応しています。インシデントが発生した場合、セキュリティチームはインシデントを 記録して、重大度に応じて優先順位を設定します。直接お客様に影響を与えるイベントには、特に高い優先順位が設定されます。このプロセスでは、行動方針や、通知、エスカレーション、対処、および文書化のための手順が指定されています。中心となるスタッフは、イベント発生に備えて、サードパーティツールや独自ツールの使用など、フォレンジクスや証拠取り扱いの訓練を受けています。お客様の機密情報を保存するシステムなどの重要な領域では、インシデント対応計画のテストを実施しています。こうしたテストでは、内部関係者による脅威やソフトウェアの脆弱性など、さまざまなシナリオが考慮されています。セキュリティ上のインシデントを早期解決するため、Google のセキュリティ チームは、24 時間体制で全社員からの問い合わせに対応しています。インシデントでお客様のデータが影響を受ける場合、Google またはそのパートナーはお客様にその旨を通知し、Google のサポートチームを通じて調査活動に協力します。 Google Cloud Platform のお客様は、お使いの環境を設定、管理するほか、不正アクセスを検知、レビューするすべての権利と責任を保有します。
7.3	7.3.1	(2)	(d)	情報システムセキュリティ責任者は、情報システムの情報セキュリティの確保が困難な事由が発生した場合には、当該情報システムが他の情報システムと共有している通信回線について、共有先の他の情報システムを保護するため、当該通信回線とは別に独立した閉鎖的な通信回線に構成を変更すること。	Google は ISO27001 認証を受けています。この基準では、「通信のセキュリティ」（ISO 27001 2013、附属書 A.13）と「公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮」（ISO27002 2013、附属書 A.14.1.2）が規定されています。 Google Cloud Platform のお客様は、外部接続の管理など、お使いの環境を設定、管理するすべての権利と責任を保有します。
7.3	7.3.1	(3)	通信回線の運用終了時の対策		
7.3	7.3.1	(3)	(a)	情報システムセキュリティ責任者は、通信回線装置の運用を終了する場合には、当該通信回線を構成する通信回線装置が運用終了後に再利用された時又は廃棄された後に、運用中に保存していた情報が漏えいすることを防止するため、当該通信回線装置の電磁的記録媒体に記録されている全ての情報を抹消するなど適切な措置を講ずること。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する 際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。
7.3	7.3.1	(4)	リモートアクセス環境導入時の対策		
7.3	7.3.1	(4)	(a)	情報システムセキュリティ責任者は、職員等の業務遂行を目的としたリモートアクセス環境を、機関等外通信回線を経由して機関等の情報システムへリモートアクセスする形態により構築する場合は、VPN 回線を整備するなどして、通信経路及びアクセス先の情報システムのセキュリティを確保すること。	ー
7.3	7.3.1	(5)	無線LAN 環境導入時の対策		
7.3	7.3.1	(5)	(a)	情報システムセキュリティ責任者は、無線LAN 技術を利用して機関等内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、通信内容の秘匿性を確保するために通信路の暗号化を行った上で、その他の情報セキュリティ確保のために必要な措置を講ずること。	ー
7.3	7.3.2	IPv6 通信回線			
7.3	7.3.2	(1)	IPv6 通信を行う情報システムに係る対策		
7.3	7.3.2	(1)	(a)	情報システムセキュリティ責任者は、IPv6 技術を利用する通信を行う情報システムを構築する場合は、製品として調達する機器等について、IPv6 Ready Logo Program に基づくPhase-2 準拠製品を、可能な場合には選択すること。	ー
7.3	7.3.2	(1)	(b)	情報システムセキュリティ責任者は、IPv6 通信の特性等を踏まえ、IPv6 通信を想定して構築する情報システムにおいて、以下の事項を含む脅威又は脆弱性に対する検討を行い、必要な措置を講ずること。	ー
7.3	7.3.2	(1)	(b)	(ア)グローバルIPアドレスによる直接の到達性における脅威	ー
7.3	7.3.2	(1)	(b)	(イ)IPv6通信環境の設定不備等に起因する不正アクセスの脅威	ー
7.3	7.3.2	(1)	(b)	(ウ)IPv4通信とIPv6通信を情報システムにおいて共存させる際の処理考慮漏れに起因する脆弱性の発生	ー
7.3	7.3.2	(1)	(b)	(エ)アプリケーションにおけるIPv6アドレスの取扱い考慮漏れに起因する脆弱性の発生	ー
7.3	7.3.2	(2)	意図しないIPv6 通信の抑止・監視		
7.3	7.3.2	(2)	(a)	情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置を、IPv6 通信を想定していない通信回線に接続する場合には、自動トンネリング機能で 想定外のIPv6 通信パケットが到達する脅威等、当該通信回線から受ける不正なIPv6 通信による情報セキュリティ上の脅威を防止するため、IPv6 通信を抑止するなどの措置を講ずること。	ー
8.1	情報システムの利用				
8.1	8.1.1	情報システムの利用			

8.1	8.1.1	(1)	情報システムの利用に係る規定の整備		
8.1	8.1.1	(1)	(a)	統括情報セキュリティ責任者は、機関等の情報システムの利用のうち、情報セキュリティに関する規定を整備すること。	ー
8.1	8.1.1	(1)	(b)	統括情報セキュリティ責任者は、職員等が機関等が支給する端末（要管理対策区域外で使用する場合に限る）及び機関等支給以外の端末を用いて要保護情報を取り扱う場合について、これらの端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた利用手順及び許可手続を定めること。	ー
8.1	8.1.1	(1)	(c)	統括情報セキュリティ責任者は、要管理対策区域外において機関等外通信回線に接続した端末（支給外端末を含む）を要管理対策区域で機関等内通信回線に接続することについての可否を判断した上で、可と判断する場合は、当該端末（支給外端末を含む）から機関等内通信回線を経由して情報システムが不正プログラムに感染するリスクを踏まえた安全管理措置に関する規定及び許可手続を定めること。	ー
8.1	8.1.1	(1)	(d)	統括情報セキュリティ責任者は､USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順を定めること。当該手順には、以下の事項を含めること。	ー
8.1	8.1.1	(1)	(d)	(ア) 職員等は、国の行政機関、独立行政法人又は指定法人が支給する外部電磁的記録媒体、又は本項に規定する利用手順において定められた外部電磁的記録媒体を用いた情報の取扱いの遵守を契約により機関等との間で取り決めた機関等外の組織から受け取った外部電磁的記録媒体を使用すること。	ー
8.1	8.1.1	(1)	(d)	(イ) 自組織以外の組織から受け取った外部電磁的記録媒体は、自組織と当該組織との間で情報を運搬する目的に限って使用することとし、当該外部電磁的記録媒体から情報を読み込む場合及びこれに情報を書き出す場合の安全確保のために必要な措置を講ずること。	ー
8.1	8.1.1	(1)	(e)	統括情報セキュリティ責任者は、機密性3情報、要保全情報又は要安定情報が記録されたUSBメモリ等の外部電磁的記録媒体を要管理対策区域外に持ち出す際の許可手続を定めること。	ー
8.1	8.1.1	(2)	情報システム利用者の規定の遵守を支援するための対策		
8.1	8.1.1	(2)	(a)	情報システムセキュリティ責任者は、職員等による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から支援する範囲を検討し、当該機能を持つ情報システムを構築すること。	ー
8.1	8.1.1	(3)	情報システムの利用時の基本的対策		
8.1	8.1.1	(3)	(a)	職員等は、業務の遂行以外の目的で情報システムを利用しないこと。	ー
8.1	8.1.1	(3)	(b)	職員等は、情報システムセキュリティ責任者が接続許可を与えた通信回線以外に機関等の情報システムを接続しないこと。	ー
8.1	8.1.1	(3)	(c)	職員等は、機関等内通信回線に、情報システムセキュリティ責任者の接続許可を受けていない情報システムを接続しないこと。	ー
8.1	8.1.1	(3)	(d)	職員等は、情報システムで利用を禁止するソフトウェアを利用しないこと。また、情報システムで利用を認めるソフトウェア以外のソフトウェアを職務上の必要により利用する場合は、情報システムセキュリティ責任者の承認を得ること。	ー
8.1	8.1.1	(3)	(e)	職員等は、接続が許可されていない機器等を情報システムに接続しないこと。	ー
8.1	8.1.1	(3)	(f)	職員等は、情報システムの設置場所から離れる場合等、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するための措置を講ずること。	ー
8.1	8.1.1	(3)	(g)	職員等は、機関等が支給する端末（要管理対策区域外で使用する場合に限る）及び機関等支給以外の端末を用いて要保護情報を取り扱う場合は、定められた利用手順に従うこと。	ー
8.1	8.1.1	(3)	(h)	職員等は、次の各号に掲げる端末を用いて当該各号に定める情報を取り扱う場合は、課室情報セキュリティ責任者の許可を得ること。	ー
8.1	8.1.1	(3)	(h)	(ア)機関等が支給する端末（要管理対策区域外で使用する場合に限る）機密性3情報、要保全情報又は要安定情報	ー
8.1	8.1.1	(3)	(h)	(イ)機関等支給以外の端末要保護情報	ー
8.1	8.1.1	(3)	(i)	職員等は、要管理対策区域外において機関等外通信回線に接続した端末（支給外端末を含む）を要管理対策区域で機関等内通信回線に接続する場合には、定められた安全管理措置を講ずること。	ー
8.1	8.1.1	(3)	(j)	職員等は、要管理対策区域外において機関等外通信回線に接続した端末（支給外端末を含む）を要管理対策区域で機関等内通信回線に接続する場合には、課室情報セキュリティ責任者の許可を得ること。	ー
8.1	8.1.1	(3)	(k)	職員等は、機密性3情報、要保全情報又は要安定情報が記録されたUSB メモリ等の外部電磁的記録媒体を要管理対策区域外に持ち出す場合には、課室情報セキュリティ責任者の許可を得ること。	ー

8.1	8.1.1	(4)	電子メール・ウェブの利用時の対策		
8.1	8.1.1	(4)	(a)	職員等は、要機密情報を含む電子メールを送受信する場合には、それぞれの機関等が運営し、又は外部委託した電子メールサーバにより提供される電子メールサービスを利用すること。	ー
8.1	8.1.1	(4)	(b)	職員等は、機関等外の者と電子メールにより情報を送受信する場合は、当該電子メールのドメイン名に政府ドメイン名を使用すること。ただし、次に掲げる場合は除く。	ー
8.1	8.1.1	(4)	(b)	(ア)指定法人が、政府ドメイン名を登録する資格を持たない場合。この場合において、当該法人は、組織の属性が資格条件となっており、不特定の個人及び組織が取得することのできないドメイン名を使用すること。	ー
8.1	8.1.1	(4)	(b)	(イ)独立行政法人及び指定法人のうち教育機関である法人が、高等教育機関向けのドメイン名を使用すると判断する場合。	ー
8.1	8.1.1	(4)	(b)	(ウ)電子メールを受信する機関等外の者が、職員等から送信された電子メールであることを認知できる場合（政府ドメイン名又は前二号に基づき取得したドメイン名が使用できない場合に限る。）。	ー
8.1	8.1.1	(4)	(c)	職員等は、不審な電子メールを受信した場合には、あらかじめ定められた手順に従い、対処すること。	ー
8.1	8.1.1	(4)	(d)	職員等は、ウェブクライアントの設定を見直す必要がある場合は、情報セキュリティに影響を及ぼすおそれのある設定変更を行わないこと。	ー
8.1	8.1.1	(4)	(e)	職員等は、ウェブクライアントが動作するサーバ装置又は端末にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認すること。	ー
8.1	8.1.1	(4)	(f)	職員等は、閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合には、以下の事項を確認すること。	ー
8.1	8.1.1	(4)	(f)	(ア)送信内容が暗号化されること	ー
8.1	8.1.1	(4)	(f)	(イ)当該ウェブサイトが送信先として想定している組織のものであること	ー
8.1	8.1.1	(5)	識別コード・主体認証情報の取扱い		
8.1	8.1.1	(5)	(a)	職員等は、主体認証の際に自己に付与された識別コード以外の識別コードを用いて情報システムを利用しないこと。	ー
8.1	8.1.1	(5)	(b)	職員等は、自己に付与された識別コードを適切に管理すること。	ー
8.1	8.1.1	(5)	(c)	職員等は、管理者権限を持つ識別コードを付与された場合には、管理者としての業務遂行時に限定して、当該識別コードを利用すること。	ー
8.1	8.1.1	(5)	(d)	職員等は、自己の主体認証情報の管理を徹底すること。	ー
8.1	8.1.1	(6)	暗号・電子署名の利用時の対策		
8.1	8.1.1	(6)	(a)	職員等は、情報を暗号化する場合及び情報に電子署名を付与する場合には、定められたアルゴリズム及び方法に従うこと。	ー
8.1	8.1.1	(6)	(b)	職員等は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、定められた鍵の管理手順等に従い、これを適切に管理すること。	ー
8.1	8.1.1	(6)	(c)	職員等は、暗号化された情報の復号に用いる鍵について、鍵のバックアップ手順に従い、そのバックアップを行うこと。	ー
8.1	8.1.1	(7)	不正プログラム感染防止		
8.1	8.1.1	(7)	(a)	職員等は、不正プログラム感染防止に関する措置に努めること。	ー
8.1	8.1.1	(7)	(b)	職員等は、情報システム（支給外端末を含む）が不正プログラムに感染したおそれがあることを認識した場合は、感染した情報システム（支給外端末を含む）の通信回線への接続を速やかに切断するなど、必要な措置を講ずること。	ー
8.2	機関等支給以外の端末の利用				
8.2	8.2.1	機関等支給以外の端末の利用			
8.2	8.2.1	(1)	機関等支給以外の端末の利用可否の判断		
8.2	8.2.1	(1)	(a)	最高情報セキュリティ責任者は、機関等支給以外の端末の利用について、取り扱うこととなる情報の格付及び取扱制限、機関等が講じる安全管理措置、当該端末の管理は機関等ではなくその所有者が行うこと等を踏まえ、求められる情報セキュリティの水準の達成の見込みを勘案し、機関等における機関等支給以外の端末の利用の可否を判断すること。	ー
8.2	8.2.1	(2)	機関等支給以外の端末の利用規定の整備・管理		
8.2	8.2.1	(2)	(a)	統括情報セキュリティ責任者は、職員等が機関等支給以外の端末を用いて機関等の業務に係る情報処理を行う場合の許可等の手続を定めること。	ー
8.2	8.2.1	(3)	機関等支給以外の端末の利用時の対策		
8.2	8.2.1	(3)	(a)	職員等は、機関等支給以外の端末を用いて機関等の業務に係る情報処理を行う場合には、端末管理責任者の許可を得ること。	ー
8.2	8.2.1	(3)	(b)	職員等は、情報処理の目的を完了した場合は、要保護情報を機関等支給以外の端末から消去すること。	ー