1.実験結果

・実験結果を設問ごとに下表にまとめる.
・設問は，「ISO/IEC 27017:2015の実施の手引き」のタイトルを記載する.
・設問に対し，①正解が適合，②正解が不適合のデータをそれぞれ用意して，実験をしている
・プロンプトに対し，LLM予測がどうだったか，その根拠が適切/不適切のどちらだったかを記載した.
・正解が不適合については，不適合データがどういった分類であったか，不適合データ分類を記載した.
・②正解が不適合データの実験に関しては，LLM予測が適合だったもの（＝失敗しているもの）については，追加プロンプトで実験を行っている.
・②正解が不適合データについては，LLMの根拠の分類も記載している

設問	①正解が適合		②正解が不適合						備考
ISO/IEC 27017:2015の実施の手引き	初回プロンプト		不適合データ分類	初回プロンプト			追加プロンプト		
	LLM予測	根拠		LLM予測	根拠	根拠の分類	LLM予測	根拠	追加質問概要など
6.1.3　関係当局との連絡	1.適合	適切	3.一部不足	2.不適合	不適切	推測	2.部分的に適合	適切	NG：追加質問で不変データ部分の解釈変更がある。 NG不適合の根拠：組織の所在地の根拠を記載していない。
CLD.6.3.1 クラウドコンピューティング環境における役割及び責任の共有及び分担	1.適合	適切	3.一部不足	1.適合	不適切	拡大解釈	1.適合	不適切	追加質問①判断した箇所を確認 追加質問②十分であるか確認 ★人間が読むと対比バランスが悪すぎると判断できるが、多少含んでいるため、適合と判断している。
8.1.1　資産目録	1.適合	適切	3.一部不足	1.適合	不適切	専門用語	1.適合	不適切	★NG適合判断：専門用語の不理解。派生データに設計書を含めている。（２回目も同様）
9.2.1　利用者登録及び登録削除	1.適合	適切	2.隣接機能	1.適合	不適切	推測	（判断できない）	適切	追加質問①判断した箇所を確認 ★NG適合判断：機能から推測した模様
9.2.3　特権的アクセス権の管理	1.適合	適切	2.隣接機能	2.部分的に適合	適切	—	2.—	—	特になし
9.2.4　利用者の秘密認証情報の管理	1.適合	不適切	1.包括概論	1.適合	不適切	拡大解釈	2.不適合（部分的）	適切	追加質問①具体的に該当手順が含まれているか確認 追加質問②監査の結論が変更ないか確認 ★NG適合判断：拡大解釈。データ・アプリケーションセキュリティなどが秘密認証情報の保護にも寄与する、
9.4.1　情報へのアクセス制限	1.適合	適切	2.隣接機能	1.適合	不適切	—	2.不適合	適切	追加質問①具体的な記述の確認 追加質問②監査結果に変更ないか確認 ★NG適合判断：推測。該当機能の記述はないが、提供された文から該当機能があることを推測して適合としている。
10.1.1　暗号による管理策の利用方針	1.適合	適切	2.隣接機能	2.不適合	適切	—	—	—	追加質問①判断した箇所を教えてください.

12.4.1 イベントログ取得	1.適合	適切	1.内容乖離	1.適合	不適切	推測	2.不適合	適切	追加質問①具体的な根拠とした文章の確認 追加質問②監査結果の再評価依頼 ★NG適合判断：推測。ログ取得していそうな機能があるため、推測して適合と判断している。 ★注意事項：ユ―ザが誤認しそうな表現（ログ取得していると断言）している。
12.4.4 クロックの同期	1.適合	適切	1.内容乖離	2.不適合	適切	―	2.―	―	特になし
CLD.12.1.5 実務管理者の運用のセキュリティ	1.適合	適切	2.レベル違い	1.適合	不適切	レベル感	2.部分的に不適合	適切	追加質問①判断した箇所を教えてください 追加質問②手順・操作が明確か ★NG適合判断：レベル感。見出し上に合致する文言があり、本文の記載があるため、内容は不明瞭でもＯＫ出してしまう。
CLD.12.4.5 クラウドサ―ビスの監視	1.適合	適切	1.内容乖離	2.不適合	適切	―	2.―	―	
12.6.1 技術的ぜい弱性の管理	1.適合	適切	1.包括概論	1.適合	不適切	拡大解釈	2.不適合	適切	①判断した箇所を教えてください. ★NG適合判断：①拡大解釈。「技術的脆弱性の管理」の拡大解釈
14.1.1 情報セキュリティ要求事項の分析及び仕様化	1.適合	適切	1.内容乖離	1.適合	不適切	厳密さの欠如	2.不適合	適切	①具体的な記載箇所を確認→（内容的には変わらず。 追加質問②十分であるか確認→ ★NG適合判断：厳密さの欠如。「情報セキュリティ機能」と問いにあるので、ITシステムの機能を有無を考慮してほしかったが、非機能関連のセキュリティに影響ある機能の記載をもって適合とした。 ★追加質問②では、想定以上の範囲が不足として列挙された。これは役立つかもしれない。
16.1.1 責任及び手順	1.適合	適切	3.一部不足	2.不適合	不適切	厳密さの欠如	2.―	―	NG不適合の根拠：大体OKだが、記載のある目標時間の情報まで記載なしと記述
16.1.2 情報セキュリティ事象の報告	1.適合	適切	2.隣接機能	1.適合	不適切	拡大解釈	2.一部適合	適切	追加質問①一部適合の選択肢を追加した場合の結果確認。 ★NG適合判断：少し無理に機能を拡大解釈して、推測して適合としている（一部適合の選択肢だけで、拡大解釈をやめて不適合部分と判断）

※LLM予測については、ChatGPTの表現を採用しているためばらつきがあるが、適合以外はすべて適合回答として扱っている。

2.プロンプト

実際に用いたプロンプト例を記載する.

2.1.初回プロンプト

初回プロンプトとして，汎用的に用いたものが下記である.

```
あなたはIT分野やクラウドサービス、セキュリティに詳しい監査員です。
とあるクラウドサービスについて、監査をしてください。
下記の[文章]から文末までで、[管理策]に続く文章に適合しているかを回答し、根拠を記載してください。
以下は回答フォーマットです。
◆根拠：
条件は以下です。
・[文章]の文からのみ判断してください。
・[文章]の内容は該当クラウドサービスから提供されている文書です。
[管理策]
<設問を記載する。>
[文章]
<データを記載する>
```

2.2.追加プロンプト例

追加プロンプトに用いた例は下記の通りである.

2.2.1.根拠の確認

設問：：12.4.1　イベントログ取得

```
「クラウドサービスはユーザーのアクティビティや例外処理に関連するログ取得機能を提供しています。」の根拠とした文章を教えてください。
```

2.2.3.十分性の確認：

設問：14.1.1　情報セキュリティ要求事項の分析及び仕様化

```
情報セキュリティ機能として十分でしょうか
```

3.出典元

適合データ,不適合データ作成時に一般に公開されている利用約款や,サービス仕様書,Webページなどから抽出して利用した

その出典元は下記である。

3.1.適合データの出典元

6.1.3 関係当局との連絡	https://aws.amazon.com/jp/compliance/shared-responsibility-model/
CLD.6.3.1 クラウドコンピューティング環境における役割及び	https://aws.amazon.com/jp/compliance/shared-responsibility-model/
8.1.1 資産目録	（出典なし）筆者により作成
9.2.1 利用者登録及び登録削除	https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/introduction.html
	https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_users_manage.html
9.2.3 特権的アクセス権の管理	https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/introduction.html
	https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_users_create.html
	https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_mfa.html
	https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_users_manage.html
9.2.4 利用者の秘密認証情報の管理	https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/introduction.html
	https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_users_create.html
	https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_mfa.html
	https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_users_manage.html
9.4.1 情報へのアクセス制限	https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_roles_terms-and-concepts.html
10.1.1 暗号による管理策の利用方針	https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/UsingEncryption.html
	https://docs.aws.amazon.com/ja_jp/vpc/latest/userguide/data-protection.html
	https://docs.aws.amazon.com/ja_jp/AmazonRDS/latest/UserGuide/Overview.Encryption.html
12.4.1 イベントログ取得	https://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/userguide/cloudtrail-user-guide.html
	https://aws.amazon.com/jp/security/security-bulletins/AWS-2023-014/
	https://aws.amazon.com/jp/security/security-bulletins/AWS-2023-013/
12.4.4 クロックの同期	https://jpn.nec.com/king-of-time/data/agreement/8-1_specification_20181101.pdf
CLD.12.1.5 実務管理者の運用のセキュリティ	https://docs.aws.amazon.com/ja_jp/AmazonRDS/latest/UserGuide/USER_DeleteInstance.html
CLD.12.4.5 クラウドサービスの監視	https://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/userguide/cloudtrail-user-guide.html
	https://aws.amazon.com/jp/security/security-bulletins/AWS-2023-014/
	https://aws.amazon.com/jp/security/security-bulletins/AWS-2023-013/
14.1.1 情報セキュリティ要求事項の分析及び仕様化	https://jpn.nec.com/king-of-time/data/agreement/8-1_specification_20181101.pdf
16.1.1 責任及び手順	https://docs.aws.amazon.com/ja_jp/health/latest/ug/aws-health-concepts-and-terms.html
	https://docs.aws.amazon.com/ja_jp/health/latest/ug/aws-health-dashboard-status.html
16.1.2 情報セキュリティ事象の報告	https://aws.amazon.com/jp/security/security-bulletins

	https://aws.amazon.com/jp/security/security-bulletins/AWS-2023-014/
	https://aws.amazon.com/jp/security/security-bulletins/AWS-2023-013/

3.2.不適合データの出典元

不適合データについては，出典元データから改変したケースもある.

設問	URL
6.1.3 関係当局との連絡	https://jpn.nec.com/king-of-time/data/agreement/8-1_specification_20181101.pdf
CLD.6.3.1 クラウドコンピューティング環境における役割及び	https://aws.amazon.com/jp/compliance/shared-responsibility-model/
8.1.1 資産目録	（出典なし）筆者により作成
9.2.1 利用者登録及び登録削除	https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_mfa.html
9.2.3 特権的アクセス権の管理	https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_users_create.html
9.2.4 利用者の秘密認証情報の管理	https://aws.amazon.com/jp/security/security-bulletins
	https://aws.amazon.com/jp/security/security-bulletins/AWS-2023-014/
	https://aws.amazon.com/jp/security/security-bulletins/AWS-2023-013/
9.4.1 情報へのアクセス制限	https://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/userguide/cloudtrail-user-guide.html
	https://docs.aws.amazon.com/ja_jp/guardduty/latest/ug/what-is-guardduty.html
	https://console.aws.amazon.com/guardduty
	https://aws.amazon.com/jp/guardduty/features/
10.1.1 暗号による管理策の利用方針	https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/introduction.html
	https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_users_create.html
	https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_mfa.html
	https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_users_manage.html
12.4.1 イベントログ取得	https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/introduction.html
	https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_users_create.html
	https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_mfa.html
	https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_users_manage.html
12.4.4 クロックの同期	https://jpn.nec.com/king-of-time/data/agreement/8-1_specification_20181101.pdf
CLD.12.1.5 実務管理者の運用のセキュリティ	https://docs.aws.amazon.com/ja_jp/AmazonRDS/latest/UserGuide/USER_DeleteInstance.html
CLD.12.4.5 クラウドサービスの監視	https://docs.aws.amazon.com/ja_jp/accounts/latest/reference/manage-acct-closing.html?shortFooter=true
12.6.1 技術的ぜい弱性の管理	https://aws.amazon.com/jp/what-is/cybersecurity/
14.1.1 情報セキュリティ要求事項の分析及び仕様化	https://jpn.nec.com/king-of-time/data/agreement/8-1_specification_20181101.pdf
16.1.1 責任及び手順	https://aws.amazon.com/jp/blogs/news/data_disposal/
16.1.2 情報セキュリティ事象の報告	https://docs.aws.amazon.com/ja_jp/health/latest/ug/aws-health-concepts-and-terms.html
	https://docs.aws.amazon.com/ja_jp/health/latest/ug/aws-health-dashboard-status.html