参考資料５－２

政府機関における多言語自動翻訳システムの導入のための参照技術要件集

令和２年３月

政府機関等に向けた多言語自動翻訳システム利活用ガイドライン検討会

内　容

はじめに

政府は、平成 30 年 6 月、政府情報システムの構築、更新を行う際、クラウドの利用を第一候補とする「クラウド・バイ・デフォルトの原則」（政府情報システムにおけるクラウドサービスの利用に係る基本方針）を発表、クラウド利用検討の際の基本的な考え方を示しました。 政府機関におけるクラウドサービスの利用促進の観点から、関係機関においては大きな転換を迎えたものといえます。

各省庁がクラウドを活用して確実に成果をあげるには、システムのセキュリティや可用性の向上、コストの削減など、クラウドの長所を正しく理解し導入を検討することになる一方で、政府が取りまとめた方針を基に、クラウド検討や事業者の選定を行うことは容易でなく、クラウドに対する一定の知見、経験が求められます。

本資料は、クラウドサービス（SaaS）を用いた多言語自動翻訳システム（以下、本サービス）に対し、各省庁がクラウドの特徴と対象業務・システムに最適なクラウドサービスを選定する際に参照できる技術要件集として取り纏めることを目的としています。

これによって、これまで省庁内で経験のない担当者においては、導入に向け一定の評価方法を含めた検討プロセスを共有することが出来ます。

1. 本参照技術要件集の位置づけ

1.1. 本参照技術要件集の目的

本参照技術要件集は、政府が掲げた「クラウド・バイ・デフォルトの原則」に即し、政府機関が本サービスの導入に向け、技術・運用要件を具体にしたものです。

1.2. 本要件集のサービス内容

本要件集は、クラウド環境による多言語自動翻訳サービスを対象に作成しています。具体的には、文書（テキスト）翻訳及び音声翻訳サービスです。

1.3. サービス利用対象

本要件集は、政府機関の府省及び出先機関において、機密性２情報を取り扱う業務を想定し作成しています。

機密性３情報など、そもそも多言語自動翻訳システムなどの外部システムの利用自体が適さない情報などについては、利用できないよう各府省の情報セキュリティポリシーに即した運用が必要です。

守秘性の低い機密性１情報のみを取り扱う業務については、政府統一基準「4.1.2 約款による外部サービスの利用」に基づき、別途対策等を講じることにしています。

また、要機密性情報を取り扱わない場合でも、職員が要機密性情報を取り扱わないことを確認あるいは、運用による対策を講じる必要があります。このため、このような職員が規定に外れる利用をした場合のリスク対策として、要機密性情報を扱うセキュリティ対策が講じられたサービスを採用することも有効です。

1.4. 関連規定等との関係

本要件集は、以下に示すガイドライン及び規定に即しています。

- 政府情報システムにおけるクラウドサービスの利用に係る基本方針(平成 30 年 6 月 7 日　各府省情報化統括責任者（CIO）連絡会議決定
- 政府機関等の情報セキュリティ対策のための統一規範（平成 30 年 7 月 25 日改訂）
- 政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）
- 政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）（平成 30 年 7 月 25 日　内閣官房　内閣サイバーセキュリティセンター

また、情報セキュリティに関しては、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」（平成 30 年 9 月）に即し、対策区分から要件をまとめています。調達に関わる基本的な方針及び事項については、「デジタル・ガバメント推進標準ガイドライン」（平成 30 年 3 月）の共通ルールに基づいています。

2. 本要件集活用における留意事項

（１） 遵守事項について

本要件集は、政府機関において、民間サービス事業者のクラウドサービス(SaaS)による多言語自動翻訳サービスの導入・利活用に資するものです。このため、サービス事業者に対し、政府機関における情報セキュリティ対策全体を明示することに役立ちます。また、サービス事業者においては、組織のセキュリティ対策内容及び水準について確認及び具体的な対策への実施に繋がります。

他方、府省においては、本サービスを調達する際、府省の情報セキュリティポリシーとの整合や確認に用いることができます。

（２） 「望ましい」の記載について

（１）で示した遵守事項について、記載されている項目への対応可否の判断について、すべての項目をやみくもに要求することは、調達不調の原因となり、「クラウド・バイ・デフォルトの原則」に逆行する懸念があります。

従って、「望ましい」として示されている要件の項目については、サービス利用者とサービス事業者間で情報セキュリティ対策に対し漏れなく講じることを踏まえつつ、利便性、コスト等に鑑みて内容を精査し、合意することが肝要です。

（３） ISO/IEC 取得と活用について

先に示したように ISO 認証を取得{JIS Q 27001:2014 (ISO/IEC 27001:2013)、JIS Q 27017:2016 (ISO/IEC 27017:2015)}しているサービス事業者は、セキュリティ対策の体制、監査、運用面において第三者の監査を定期的に受けていることを意味します。特に、ISO/IEC 27017 の特徴となっている要求事項「対策内容の利用者への表明」は、利用者に対して期待される情報セキュリティが遵守され運用されている事を宣言（コミットメント）しています。このため、サービス利用者は、サービス事業者の ISO 取得有無を調査することで、サービス事業者の情報セキュリティ対策に対する内容の確認や、合意事項が実施されているかどうかの判断に役立ちます。

（補足）

ISO/IEC 27001 クラウドセキュリティ認証（JIS Q 27017:2016 (ISO/IEC 27017:2015)）については、サービス単位での取得となっています。本サービスでは、多言語自動翻訳サービスとして、文書翻訳サービス、音声翻訳サービスの２つが該当します。現時点でこの２つのサービスに対し取得している事業者数は少ないことから、例えば、ISO 取得を入札参加の条件することは、結果として参入事業者の排除に繋がる可能性があります。このため、事業者の取得状況を踏まえ

適切な活用が求められます。

（参考）　参照技術要件集の活用

（１） 本要件集の読み方

本要件集は、1.4 で示した政府機関等の対策基準策定のためのガイドラインの項目に即し、詳細項目（約 500 項目）について、本サービスにおける要件を固めています。

また、本サービスはクラウドサービス（SaaS）による提供を前提にしていることから、サービス利用者及びサービス事業者各々について、遵守すべき事項をまとめています。本要件集において、政府機関はサービス利用者として位置づけ、クラウドサービスを提供する事業者をサービス事業者とし、政府統一基準における対策事項に対し、利用者/事業者において要求事項として示しています。

（２） IT マネジメント

本要件集は、政府調達として予算要求から業務の見直し、要件定義に活用できます。

- 特に、これまで経験のない機関においては、クラウドサービスにおける技術要件の具体化が難しくまた、対策基準から読み解くには、時間を要すると考えます。このため、本要件集においては、対策の視点への理解を高めるため、各遵守すべき事項には解説を設けています。
- 先に示すように本要件集は、政府統一基準に即していることから、機関内で設定されている情報セキュリティポリシーとの整合を図ることができ、利活用業務に対するセキュリティ要件の確認に繋がります。
- 関係事業者に対する事前ヒアリング等において、本要件集を用いることで事業ごとの技術・運用面での状況を画することが可能です。

（３） サービス事業者の技術要件

本要件集は、政府機関の基準及びルールの準拠とともに国際認証規格（ISMS）との照合を行っています。

- ISMS とは、個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用することです。ISMS が達成すべきことは、リスクマネジメントプロセスを適用することによって情報の機密性、完全性及び可用性をバランス良く維持・改善し、リスクを適切に管理しているという信頼を利害関係者に与えることにある。そのためには、ISMS

を組織のプロセス及びマネジメント構造全体の一部として組み込むことが重要です。

- 本要件集の利用において事業者（候補）の選定の際、ISMS 認証の取得によって、事業者のリスク管理を図ることで、客観的かつ効率的に確認にすることが可能です。本要件集については、情報セキュリティ及びクラウド情報セキュリティ管理に関わる規格との整合を重視し、具体的には、JIS Q 27001:2014（ISO/IEC 27001:2013)、JIS Q 27002：2014（ISO/IEC 27002：2013)、JIS Q 27017:2016（ISO/IEC 27017:2015)の各事項との整合を確認しました。

- 参考：JIS Q 27001:2014（ISO/IEC 27001:2013)は、組織のニーズ及び目的、情報セキュリティ要求事項、組織が用いるプロセス、並びに、組織の規模及び構造を考慮して、ISMS の確立及び実施を行います。これにより、組織が扱う情報量の増加などの、取り巻くリスクの変化に、組織のマネジメント及び業務プロセスが対応できる組織基盤を構築する事が可能です。
- また、JIS Q 27001:2014（ISO/IEC 27001:2013)は、情報セキュリティ要求事項を満たす組織の能力をパフォーマンス評価及び内部監査などの組織の内部で評価する基準として採用することができます。加えて第二者監査・第三者監査といわれる、外部関係者が評価するための基準として用いることもできます。

（４） 業務に適した技術要件の設定

本要件集は、先に示した「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」で示されている技術対策に即し、本要件集の事項と整合を図っています。このため、対象となる業務と取り扱う情報等に基づき本サービスにおける対策を確認することができます。

政府機関における多言語自動翻訳システムの導入のための参照技術要件集

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件		C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件		D.ISO/IEC27001、27002、27017との照合			
							B1.サービス利用者の遵守すべき 要件に対する解説		C1.サービス事業者の遵守すべき 要件に対する解説	①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
部	章	節	項		項目								
1	総則												
1	1.1	本統一基準の目的・適用範囲											
1	1.1		(1)		本統一基準の目的								
1	1.1		(2)		本統一基準の適用範囲								
1	1.1		(3)		本統一基準の改訂								
1	1.1		(4)		法令等の遵守								
1	1.1		(5)		対策項目の記載事項								
1	1.2	情報の格付の区分・取り扱い制限											
1	1.1		(1)		情報の格付けの区分								
1	1.1		(2)		情報の取扱制限								
1	1.3	用語定義											
2	情報セキュリティ対策の基本的枠組み												
2	2.1	導入・計画											
2	2.1	2.1.1	組織・体制の整備										
2	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	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。	サービス利用者は、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。	多様なクラウドサービスの利用を想定し、クラウドサービス利用時の、情報セキュリティに関する責任者の設置方針を、整理しておくことが望ましい。 サービス利用者は、最高情報セキュリティ責任者の権限と責務に本サービスの利用に関する事項を割り当てることが望ましい。	サービス事業者は、本サービス提供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。	本サービス提供に関する、最高情報セキュリティ責任者を配置し、その権限と責務を明確にすること。	5.1 リーダーシップ及びコミットメント5.3 組織の役割、責任及び権限 ※下記の注記を参照	6.1.1 関連情報を参照	追加要求事項なし	6.1.1 情報セキュリティの役割及び責任 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
2	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。	サービス利用者は、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。	多様なクラウドサービスの利用を想定し、クラウドサービス利用時の、情報セキュリティに関する責任者の設置方針を、整理しておくことが望ましい。 サービス利用者は、最高情報セキュリティ副責任者の権限と責務に本サービスの利用に関する事項を割り当てることが望ましい。	サービス事業者は、本サービス提供に際して、最高情報セキュリティ責任者を支援し、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。		5.1 リーダーシップ及びコミットメント5.3 組織の役割、責任及び権限 ※大規模組織では副責任者が任命されることもあります。	6.1.1 情報セキュリティの役割及び責任	追加要求事項なし	6.1.1 情報セキュリティの役割及び責任 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
2	2.1	2.1.1	(2)		情報セキュリティ委員会の設置								
2	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。	最高情報セキュリティ責任者は、本サービス利用に関する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した委員会等を設置し、本サービス利用時の情報セキュリティに関わる対策基準等を検討すること。	サービス利用者は、本サービス利用に関する情報セキュリティ委員会の審議事項に、本サービスの利用に関する事項を、割り当てることが望ましい。	サービス事業者の最高情報セキュリティ責任者は、必要に応じて情報セキュリティに関わる対策基準等を検討する会議体を置くこと。		A.6.1.1 情報セキュリティの役割及び責任 ※ISO 27001では、情報セキュリティ委員会の設置を求めていませんが、多くの組織は委員会組織で運用されています。	6.1.1 情報セキュリティの役割及び責任	6.1.1 情報セキュリティの役割及び責任 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	6.1.1 情報セキュリティの役割及び責任 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
2	2.1	2.1.1	(3)		情報セキュリティ監査責任者の設置								
2	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。	最高情報セキュリティ責任者は、自ら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、本サービス利用に際する、情報セキュリティ監査責任者 1 人を置くこと。	最高情報セキュリティ責任者は、情報セキュリティ監査責任者の役割及び責任に本サービスの利用に関する事項を割り当てることが望ましい。 最高情報セキュリティ責任者は、情報セキュリティ監査責任者の任命に際し、情報セキュリティ監査責任者が、本サービスの内部監査の実施に当たり、適切なクラウド及び本サービスに関する知識を保有しているか確認すること。	最高情報セキュリティ責任者は、本サービス提供に際する、情報セキュリティ監査責任者 1 人を置くこと。	情報セキュリティ監査責任者は、情報セキュリティの内部監査の実施に当たり、最新のクラウドサービス及び本サービスについての情報を保有していることが望ましい。	5.1 リーダーシップ及びコミットメント ※大規模組織では、特定の情報セキュリティ監査責任者が任命されることがありますが、情報セキュリティ管理責任者が監査責任者を兼務することがあります。	追加要求事項なし	追加要求事項なし	追加要求事項なし
2	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	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。	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、情報セキュリティ責任者を 1 人づつ置くこと。それぞれの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 人を情報セキュリティ責任者の中から選任すること。	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と統括情報セキュリティ責任者が統括する事務には本サービス利用に関する事項を含めることが望ましい。	最高情報セキュリティ責任者は、必要に応じて、情報セキュリティ責任者と統括情報セキュリティ責任者を設置すること。	情報セキュリティ責任者と統括情報セキュリティ責任者を任命した場合は、その情報セキュリティに関する役割・責任を明確にすることが望ましい。	A.6.1.1 情報セキュリティの役割及び責任 ※多くの組織では、部署ごとに情報セキュリティ責任者が任命されています。	6.1.1 関連情報を参照	追加要求事項なし	6.1.1 情報セキュリティの役割及び責任 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
2	2.1	2.1.1	(4)	(b)	情報セキュリティ責任者は、遵守事項 3.2.1(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。	情報セキュリティ責任者は、本サービス利用に際し、遵守事項 3.2.1(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を必要に応じて設置すること。	区域情報セキュリティ責任者が統括する事務には本サービス利用に関する事項を含めることが望ましい。	最高情報セキュリティ責任者は、必要に応じて、区域情報セキュリティ責任者を設置すること。 区域情報セキュリティ責任者が統括する事務には本サービス利用に関する事項を含めること。	区域情報セキュリティ責任者を任命した場合は、その情報セキュリティに関する役割・責任を明確にすることが望ましい。	A.6.1.1 情報セキュリティの役割及び責任 ※多くの組織では、部署ごとに情報セキュリティ責任者が任命されています。	6.1.1 関連情報を参照	追加要求事項なし	6.1.1 情報セキュリティの役割及び責任 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
2	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。	情報セキュリティ責任者は、本サービス利用に際し、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を、必要に応じて設置すること。	課室情報セキュリティ責任者が統括する事務には本サービス利用に関する事項を含めることが望ましい。	最高情報セキュリティ責任者は、必要に応じて、課室情報セキュリティ責任者を設置すること。 課室情報セキュリティ責任者が統括する事務には本サービス利用に関する事項を含めること。	課室情報セキュリティ責任者を任命した場合は、その情報セキュリティに関する役割・責任を明確にすることが望ましい。	A.6.1.1 情報セキュリティの役割及び責任 ※大規模組織では、課室毎に情報セキュリティ責任者が任命される場合があります。	6.1.1 関連情報を参照	追加要求事項なし	6.1.1 情報セキュリティの役割及び責任 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

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
2	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。	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、本サービス利用に関する情報システムセキュリティ責任者を本サービスの企画に着手するまでに選任すること。	情報システムセキュリティ責任者の役割・責任には、以下の事項を含めることが望ましい。 ・本サービス利用に関する手順を順守し、情報セキュリティ対策が有効に機能することを確認すること ・本サービスの情報セキュリティ対策が有効に機能していることを定期的に監視すること ・サービス事業者との窓口を設置し、本サービスの変更及び情報セキュリティインシデント等に対応すること	サービス事業者は、本サービスの企画担当者を設置し、サービス利用者に通知する。	サービス事業者は企画（選定者）の提供に際し、本サービスのシステムセキュリティに関する情報を提供すること。	A.6.1.5 プロジェクトマネジメントにおける情報セキュリティ	6.1.5 プロジェクトマネジメントにおける情報セキュリティ	追加要求事項なし	追加要求事項なし
2	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	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。	最高情報セキュリティ責任者は、業務の特性等を考慮し、必要に応じて、本サービス利用に際する、最高情報セキュリティアドバイザーを設置すること。	高情報セキュリティ責任者は、業務の特性等を考慮し、必要に応じて、本サービス利用に際する、最高情報セキュリティアドバイザーを設置すること。 また、最高情報セキュリティアドバイザーは、本サービスを含むクラウドサービス全般の動向等を踏まえ、適切な助言を行う役割を担うこと。	最高情報セキュリティ責任者は、外部よりクラウドセキュリティ対策に関する支援や助言を入手する仕組みを構築すること。	サービス事業者は、クラウドセキュリティ対策の支援や助言を得るために、外部の有識者から助言及び指導を受けていることが望ましい。 これには、ISO/IEC27001やISO/IEC27017などの第三者認証審査も含む。	A.6.1.4 専門組織との連絡 ※組織内に最高情報セキュリティアドバイザーに適任がいない場合には、外部の専門組織を活用する場合があります。	6.1.4 専門組織との連絡 ※組織内に再考情報セキュリティアドバイザーに適任がいない場合には、外部の専門組織を活用する場合があります。	追加要求事項なし	追加要求事項なし
2	2.1	2.1.1	(6)	情報セキュリティ対策推進体制の整備									
2	2.1	2.1.1	(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。	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。	最高情報セキュリティ責任者は、本サービス利用に関する以下の事項を含む情報セキュリティ対策推進体制の役割を規定することが望ましい。 ・情報セキュリティ関係規程及び対策推進計画の策定に係る事務 ・情報セキュリティ関係規程の運用に係る事務 ・例外措置に係る事務 ・情報セキュリティ対策の教育の実施に係る事務 ・情報セキュリティ対策の自己点検に係る事務 ・情報セキュリティ関係規程及び対策推進計画の見直しに係る事務	最高情報セキュリティ責任者は、本サービス提供に関する情報セキュリティ対策推進体制を整備すること。	サービス事業者は、以下の事項を明確にした規定をサービス利用者に提供することが望ましい。 ・情報セキュリティ関係規程及び対策推進計画の策定に係る事務 ・情報セキュリティ関係規程の運用に係る事務 ・例外措置に係る事務 ・情報セキュリティ対策の教育の実施に係る事務 ・情報セキュリティ対策の自己点検に係る事務 ・情報セキュリティ関係規程及び対策推進計画の見直しに係る事務 公表においてはクラウドサービスにおける第三者認証審査を受けるセキュリティマネジメントシステム（ISO/IEC27017等）の仕組みの下で公表することが望ましい。	5.3 組織の役割、責任及び権限 A.6.1.1 情報セキュリティの役割及び責任	6.1.1 情報セキュリティの役割及び責任	追加要求事項なし	追加要求事項なし
2	2.1	2.1.1	(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。	本サービスに該当しない		本サービスに該当しない		A.6.1.1 情報セキュリティの役割及び責任	6.1.1 情報セキュリティの役割及び責任	追加要求事項なし	追加要求事項なし
2	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	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。	最高情報セキュリティ責任者は、本サービス利用に関するCSIRT（Computer Security Incident Response Team） を整備し、その役割を明確化すること。	最高情報セキュリティ責任者は、以下の事項を含むCSIRT の役割を規定すること。 ・機関等に関わる情報セキュリティインシデント発生時の対処の一元管理 ・機関等全体における情報セキュリティインシデント対処の管理 ・情報セキュリティインシデントの可能性の報告受付 ・機関等における情報セキュリティインシデントに関する情報の集約 ・所管する独立行政法人及び指定法人における情報セキュリティインシデントに関する情報の集約（当該法人を所管する国の行政機関に限る。） ・情報セキュリティインシデントの最高情報セキュリティ責任者等への報告 ・情報セキュリティインシデントへの対処に関する指示系統の一本化 ・情報セキュリティインシデントへの迅速かつ的確な対処 ・情報セキュリティインシデントであるかの評価 ・被害の拡大防止を図るための応急措置の指示又は勧告を含む情報セキュリティインシデントへの対処全般に関する指示、勧告又は助言 ・内閣官房内閣サイバーセキュリティセンターへの連絡（国の行政機関に限る。） ・法人を所管する国の行政機関への連絡（独立行政法人及び指定法人に限る。） ・外部専門機関等からの情報セキュリティインシデントに係る情報の収集 ・他の機関等への情報セキュリティインシデントに係る情報の共有 ・情報セキュリティインシデントへの対処に係る専門的知見の提供、対処作業の実施	最高情報セキュリティ責任者は、本サービス提供に関するCSIRTを整備し、その役割を明確化すること。	最高情報セキュリティ責任者は、以下を含むCSIRT の役割を規定すること。 ・本サービス提供に関わる情報セキュリティインシデント発生時の対処の一元管理 ・情報セキュリティインシデントへの迅速かつ的確な対処	A.6.1.1 情報セキュリティの役割及び責任 A.16.1 情報セキュリティインシデント管理	6.1.1 情報セキュリティの役割及び責任 16.1.1 責任及び手順（情報セキュリティインシデント管理）	16.1.1 責任及び手順（情報セキュリティインシデント管理）	16.1.1 責任及び手順（情報セキュリティインシデント管理）

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
2	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。	最高情報セキュリティ責任者は、サービス利用者のうちから CSIRT に属するサービス利用者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CSIRT責任者を定めること	最高情報セキュリティ責任者は、実務担当者を含めた実効性のあるCSIRT 体制を構築すること。	最高情報セキュリティ責任者は、サービス事業者のうちから CSIRT に属するサービス事業者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し、CSIRT 内の業務統括及び外部との連携等を行う責任者として CSIRT 責任者を置くこと。	最高情報セキュリティ責任者は、実務担当者を含めた実効性のあるCSIRT 体制を構築すること。	A.6.1.1 情報セキュリティの役割及び責任 A.16.1 情報セキュリティインシデント管理	6.1.1 情報セキュリティの役割及び責任 16.1.1 責任及び手順（情報セキュリティインシデント管理）	16.1.1 責任及び手順（情報セキュリティインシデント管理）	16.1.1 責任及び手順（情報セキュリティインシデント管理）
2	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。	最高情報セキュリティ責任者は、本サービス利用に際して、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。	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に、情報セキュリティインシデント対処に関する知見を有する外部の専門家等による必要な支援を速やかに得られる体制を構築しておくこと。	最高情報セキュリティ責任者は、本サービス提供に際して、情報セキュリティインシデントが発生した際に、情報セキュリティインシデント対処に関する知見を有する外部の専門家等による必要な支援を速やかに得られる体制を整備すること。	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に、情報セキュリティインシデント対処に関する知見を有する外部の専門家等による必要な支援を速やかに得られる体制を構築しておくこと。	A.16.1.2 情報セキュリティ事象の報告 A.16.1.3 情報セキュリティ弱点の報告	16.1.2 情報セキュリティ事象の報告 16.1.3 情報セキュリティ弱点の報告	16.1.2 情報セキュリティ事象の報告	16.1.2 情報セキュリティ事象の報告
2	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。）	最高情報セキュリティ責任者は、CYMAT が取り扱う情報セキュリティインシデントに、本サービス利用に際して発生した情報セキュリティインシデントも含まれることを確かにすること。	最高情報セキュリティ責任者は、機関等全体における情報セキュリティインシデント対処について、CSIRT、情報セキュリティインシデントの当事者及びその他関係者の役割分担を規定すること。	最高情報セキュリティ責任者は、CYMAT が取り扱う情報セキュリティインシデントに、本サービス提供に際して発生した情報セキュリティインシデントも含まれることを確認すること。	最高情報セキュリティ責任者は、機関等全体における情報セキュリティインシデント対処について、CSIRT、情報セキュリティインシデントの当事者及びその他関連部局の役割分担を規定すること。	A.16.1.2 情報セキュリティ事象の報告 A.16.1.3 情報セキュリティ弱点の報告	16.1.2 情報セキュリティ事象の報告 16.1.3 情報セキュリティ弱点の報告	16.1.2 情報セキュリティ事象の報告	16.1.2 情報セキュリティ事象の報告
2	2.1	2.1.1	(8)	兼務を禁止する役割									
2	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	サービス利用者は、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てはならない (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	承認又は許可が必要な手続きには、以下の事項を含めることが望ましい。 ・本サービス利用に関する情報システムのすべての変更 ・サービス利用者の登録、変更及び削除 ・本サービスの保守・診断作業 ・本サービスの改善処置 ・本サービスに対する監査の実施	本サービスに該当しない		A.6.1.2 職務の分離	6.1.2 職務の分離	追加要求事項なし	追加要求事項なし
2	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。	サービス利用者は、本サービス利用に際し、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は上司又は適切な者に承認等を申請し、承認等を得ること。		本サービスに該当しない		A.6.1.2 職務の分離	6.1.2 職務の分離	追加要求事項なし	追加要求事項なし
2	2.1	2.1.2	対策基準・対策推進計画の策定										
2	2.1	2.1.2	(1)	対策基準の策定									
2	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。	最高情報セキュリティ責任者は、対策基準に、本サービス利用に関わる事項が含まれていることを確認しなければならない。	対策基準には、以下の事項を含めることが望ましい。 ・マルチテナント環境等、本サービスの提供に関わるクラウド固有の情報セキュリティリスクが存在する可能性があることを踏まえること ・本サービス利用に関する個人情報/プライバシー保護に関する法律および方針の順守等、法的要件を含めること ・本サービス利用に関する情報セキュリティ運営方針を明確にし、セキュリティを順守する組織、活動、プロセス、製品及びサービスの種類を規定すること ・本サービス利用に関する情報セキュリティ運営規定にて、該当する人員の力量を定義すること	サービス事業者は、本サービス提供に関する情報セキュリティリスク評価を定期的に実施し、その結果を踏まえた対策を策定すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・対策基準には、本サービス提供に関する情報セキュリティリスクとして、マルチテナント環境等、本サービスの提供に関わるクラウド固有の情報セキュリティリスクが存在する可能性があることを踏まえる ・本サービス提供に関する法規制（個人情報保護/プライバシー保護）を特定し、本サービスの提供・運用がこれらを順守していることを確実にする ・本サービス提供に関する情報セキュリティ運営方針を明確にし、セキュリティを順守する組織、活動、プロセス、製品及びサービスの種類を規定する ・ 本サービス提供に関する情報セキュリティ運営規定にて、該当する人員の力量を定義する	7.5 文書化した情報 7.5.1 一般	追加要求事項なし	追加要求事項なし	追加要求事項なし

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
2	2.1	2.1.2	(2)		対策推進計画の策定								
2	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、本サービス利用に関する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	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、本サービス利用に関する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	最高情報セキュリティ責任者は、対策推進計画に、本サービス利用に関するリスク評価結果を踏まえた方針・重点及び実施時期を組み込むことが望ましい。	最高情報セキュリティ責任者は、本サービス提供に関する情報セキュリティ対策を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、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	サービス事業者は、本要件に対し、情報システム及びサービスに関する第三者の監査を受けるセキュリティマネジメントシステム（ISO2700, ISO/IEC27017等）の仕組みの下で遂行することが望ましい。	6.2 情報セキュリティ目的及びそれを達成するための計画策定	追加要求事項なし	追加要求事項なし	追加要求事項なし
2	2.2	運用											
2	2.2	2.2.1	情報セキュリティ関係規程の運用										
2	2.2	2.2.1	(1)	情報セキュリティ対策の運用									
2	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。	統括情報セキュリティ責任者は、本サービス利用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。	実施手順には、本サービス利用に関して特定された以下の情報セキュリティリスクや要件を考慮することが望ましい。 ・音声翻訳機能を利用する現場での情報セキュリティリスク ・文書自動翻訳機能を利用する場合の情報セキュリティリスク ・本サービス利用に際して順守すべき法規制要件（個人情報保護/プライバシー保護等）	情報セキュリティ責任者は、本サービス提供に関する情報セキュリティ対策に関する実施手順を整備し、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。	実施手順には、サービス利用者において特定された情報セキュリティリスクを考慮し、以下の事項を含むことが望ましい。 ・音声翻訳機能を利用する現場での情報セキュリティリスク ・文書自動翻訳機能を利用する場合の情報セキュリティリスク ・本サービス利用に際して順守すべき法規制要件（個人情報保護/プライバシー保護等）	7.5.1 一般 7.5.2 作成及び更新 9.3 マネジメントレビュー	追加要求事項なし	追加要求事項なし	追加要求事項なし
2	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。	統括情報セキュリティ責任者は、本サービス利用に関する、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。		情報セキュリティ責任者は、本サービス提供に関する、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。	サービス事業者は、本要件に対し、情報システム及びサービスに関する第三者の監査を受けるセキュリティマネジメントシステム（ISO2700, ISO/IEC27017等）の仕組みの下で遂行することが望ましい。	A.7.1.2 雇用条件 A.7.3.1 雇用の終了又は変更に関する責任	7.1.2 雇用条件 7.3.1 雇用の終了又は変更に関する責任	追加要求事項なし	追加要求事項なし
2	2.2	2.2.1	(1)	(c)	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。	情報セキュリティ対策推進体制は、本サービス利用に際して、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。	遵守事項2.1.1(6)(a)で定めた以下の当該体制の役割に、本サービス利用に関する事項が含まれる場合、本サービスに関する事項に応じて以下の事務を遂行することが望ましい。 ・情報セキュリティ関係規程及び対策推進計画の策定に係る事務 ・情報セキュリティ関係規程の運用に係る事務 ・例外措置に係る事務 ・情報セキュリティ対策の教育の実施に係る事務 ・情報セキュリティ対策の自己点検に係る事務 ・情報セキュリティ関係規程及び対策推進計画の見直しに係る事務	情報セキュリティ責任者は、本サービス提供に際し、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。	サービス事業者は、本要件に対し、情報システム及びサービスに関する第三者の監査を受けるセキュリティマネジメントシステム（ISO2700, ISO/IEC27017等）の仕組みの下で遂行することが望ましい。	8.1 運用の計画及び管理 A.7.2.1 経営陣の責任	7.2.1 経営陣の責任	追加要求事項なし	追加要求事項なし
2	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。	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、サービス利用者から、本サービス利用に際する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。		サービス利用者から、本サービス利用に際する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、セキュリティ責任者に報告すること。		9.3 マネジメントレビュー（10.2 継続的改善）	追加要求事項なし	追加要求事項なし	追加要求事項なし
2	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。	サービス利用者の統括情報セキュリティ責任者は、本サービス利用に際する、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。		情報セキュリティ責任者は、本サービス提供に際する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。		9.3 マネジメントレビュー（10.2 継続的改善）	追加要求事項なし	追加要求事項なし	追加要求事項なし
2	2.2	2.2.1	(2)	違反への対処									
2	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。	サービス利用者は、本サービス利用に関する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。		本サービス提供の担当者は、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。		A.7.2.3 懲戒手続 A.16.1.2 情報セキュリティ事象の報告 A.16.1.3 情報セキュリティ弱点の報告	7.2.3 懲戒手続 16.1.2 情報セキュリティ事象の報告 16.1.3 情報セキュリティ弱点の報告	追加要求事項なし	追加要求事項なし

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
2	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。	サービス利用者の情報セキュリティ責任者は、本サービス利用に関する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。		情報セキュリティ責任者は、本サービス提供に関する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、最高情報セキュリティ責任者に報告すること。		A.7.2.3 懲戒手続 A.16.1.2 情報セキュリティ事象の報告 A.16.1.3 情報セキュリティ弱点の報告	7.2.3 懲戒手続 16.1.2 情報セキュリティ事象の報告 16.1.3 情報セキュリティ弱点の報告	追加要求事項なし	追加要求事項なし
2	2.2	2.2.2	例外措置										
2	2.2	2.2.2	(1)	例外措置手続の整備									
2	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。	最高情報セキュリティ責任者は、本サービス利用に際して、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。		最高情報セキュリティ責任者は、本サービス提供に際して、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。		※該当要件なし	※該当要件なし	※該当要件なし	※該当要件なし
2	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。	サービス利用者の統括情報セキュリティ責任者は、本サービス利用に際して、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。		情報セキュリティ責任者は、本サービス提供に際して、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。		※該当要件なし	※該当要件なし	※該当要件なし	※該当要件なし
2	2.2	2.2.2	(2)	例外措置の運用									
2	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。	サービス利用者は、本サービス利用に際して、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。		サービス事業者は、本サービス提供に際して、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、サービスの維持業務に緊急を要し、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類（セキュリティマニュアル等も含む）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。		※該当要件なし	※該当要件なし	※該当要件なし	※該当要件なし
2	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。	サービス利用者の許可権限者は、本サービス利用に際して、サービス利用者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。		サービス事業者の許可権限者は、本サービス提供に際して、サービス利用者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。		※該当要件なし	※該当要件なし	※該当要件なし	※該当要件なし
2	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。	サービス利用者の許可権限者は、本サービス利用に際して、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。		サービス事業者の許可権限者は、本サービス提供に際して、例外措置の申請状況を台帳に記録し、情報セキュリティ責任者に報告すること。		※該当要件なし	※該当要件なし	※該当要件なし	※該当要件なし
2	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。	サービス利用者の統括情報セキュリティ責任者は、本サービス利用に際して、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。		情報セキュリティ責任者は、本サービス運用に際して、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類（セキュリティマニュアル等も含む）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。		※該当要件なし	※該当要件なし	※該当要件なし	※該当要件なし
2	2.2	2.2.3	教育										
2	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	2.2.3	(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。	統括情報セキュリティ責任者は、本サービス利用に関する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。	情報セキュリティ対策に係る教育実施計画には、本サービス利用に関する以下の事項を含めることが望ましい。 ・適用範囲のサービス利用者に対して、本サービスの情報セキュリティに関する研修を年一回以上定期的に実施すること ・新規にサービス利用者が入ってきた場合または最高情報セキュリティ責任者が必要と判断した場合は、随時教育を行うこと ・本サービスを利用する際の手引きについて教育すること	情報セキュリティ責任者は、本サービス提供に関する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。	サービス事業者は、本要件に対し、情報システム及びサービスに関する第三者の監査を受けるセキュリティマネジメントシステム（ISO/IEC27001, ISO/IEC27017等）の仕組みの下で遂行することが望ましい。	7.2 力量 7.3 認識 7.4 コミュニケーション A.7.2.2 情報セキュリティの意識向上、教育及び訓練	7.2.2 情報セキュリティの意識向上、教育及び訓練	7.2.2 情報セキュリティの意識向上、教育及び訓練	7.2.2 情報セキュリティの意識向上、教育及び訓練
2	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。	サービス利用者の統括情報セキュリティ責任者は、本サービス利用に際して、情報セキュリティの状況の変化に応じサービス利用者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。		情報セキュリティ責任者は、本サービス提供に際して、情報セキュリティの状況の変化に応じサービス提供担当者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。	サービス事業者は、本要件に対し、情報システム及びサービスに関する第三者の監査を受けるセキュリティマネジメントシステム（ISO/IEC27001, ISO/IEC27017等）の仕組みの下で遂行することが望ましい。	7.2 力量 7.3 認識 7.4 コミュニケーション A.7.2.2 情報セキュリティの意識向上、教育及び訓練	7.2.2 情報セキュリティの意識向上、教育及び訓練	7.2.2 情報セキュリティの意識向上、教育及び訓練	7.2.2 情報セキュリティの意識向上、教育及び訓練
2	2.2	2.2.3	(2)	教育の実施									
2	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。	課室情報セキュリティ責任者は、本サービス利用に際し、教育実施計画に基づき、サービス利用者に対して、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。	情報セキュリティ対策に係る教育実施計画には、本サービス利用に関する以下の事項を含めることが望ましい。 ・適用範囲のサービス利用者に対して、本サービスの情報セキュリティに関する研修を年一回以上定期的に実施すること ・新規にサービス利用者が入ってきた場合または最高情報セキュリティ責任者が必要と判断した場合は、随時教育を行うこと ・本サービスを利用する際の手引きについて教育すること	情報セキュリティ責任者は、教育実施計画に基づき、サービス提供担当者に対して、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。	サービス事業者は、本要件に対し、情報システム及びサービスに関する第三者の監査を受けるセキュリティマネジメントシステム（ISO/IEC27001, ISO/IEC27017等）の仕組みの下で遂行することが望ましい。	7.2 力量 7.3 認識 7.4 コミュニケーション A.7.2.2 情報セキュリティの意識向上、教育及び訓練	7.2.2 情報セキュリティの意識向上、教育及び訓練	7.2.2 情報セキュリティの意識向上、教育及び訓練	7.2.2 情報セキュリティの意識向上、教育及び訓練
2	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。	サービス利用者は、教育実施計画に従って、適切な時期に教育を受講しなければならない。		サービス事業者は、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。	サービス事業者は、本要件に対し、情報システム及びサービスに関する第三者の監査を受けるセキュリティマネジメントシステム（ISO/IEC27001, ISO/IEC27017等）の仕組みの下で遂行することが望ましい。	7.2 力量 7.3 認識 7.4 コミュニケーション A.7.2.2 情報セキュリティの意識向上、教育及び訓練	7.2.2 情報セキュリティの意識向上、教育及び訓練	7.2.2 情報セキュリティの意識向上、教育及び訓練	7.2.2 情報セキュリティの意識向上、教育及び訓練

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
2	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。	サービス利用者の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 に属するサービス利用者に本サービス利用に関する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 に属する職員にも本サービス利用に関する教育を適切に受講させなければならない。		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 に属するサービス提供担当者に本サービス利用に関する教育を適切に受講させること。	サービス事業者は、本要件に対し、情報システム及びサービスに関する第三者の監査を受けるセキュリティマネジメントシステム（ISO/IEC27001, ISO/IEC27017等）の仕組みの下で遂行することが望ましい。	A.7.2.2 情報セキュリティの意識向上、教育及び訓練 ※組織によっては、CSIRTがISO 27001認証範囲外にある場合があります。	7.2.2 情報セキュリティの意識向上、教育及び訓練	7.2.2 情報セキュリティの意識向上、教育及び訓練	7.2.2 情報セキュリティの意識向上、教育及び訓練
2	2.2	2.2.3	(2)	(d)	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。	サービス利用者の課室情報セキュリティ責任者は、本サービス利用に関する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。		情報セキュリティ責任者は、本サービス利用に関する教育の実施状況を記録し、最高情報セキュリティ責任者に報告すること。	サービス事業者は、本要件に対し、情報システム及びサービスに関する第三者の監査を受けるセキュリティマネジメントシステム（ISO/IEC27001, ISO/IEC27017等）の仕組みの下で遂行することが望ましい。	7.3 認識 9.3 マネジメントレビュー A.7.2.2 情報セキュリティの意識向上、教育及び訓練 ※多くの組織がマネジメントレビューで教育の実施状況を経営者に報告しています。	7.2.2 情報セキュリティの意識向上、教育及び訓練	7.2.2 情報セキュリティの意識向上、教育及び訓練	7.2.2 情報セキュリティの意識向上、教育及び訓練
2	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。	サービス利用者の統括情報セキュリティ責任者は、本サービス利用に関する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。		情報セキュリティ責任者は、本サービス提供に関する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。	サービス事業者は、本要件に対し、情報システム及びサービスに関する第三者の監査を受けるセキュリティマネジメントシステム（ISO/IEC27001, ISO/IEC27017等）の仕組みの下で遂行することが望ましい。	7.3 認識 9.3 マネジメントレビュー A.7.2.2 情報セキュリティの意識向上、教育及び訓練 ※多くの組織がマネジメントレビューで教育の実施状況を経営者に報告しています。	7.2.2 情報セキュリティの意識向上、教育及び訓練	7.2.2 情報セキュリティの意識向上、教育及び訓練	7.2.2 情報セキュリティの意識向上、教育及び訓練
2	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	2.2.4	(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	2.2.4	(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。	サービス利用者の統括情報セキュリティ責任者は、本サービス利用に関する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、サービス利用者に周知すること。		サービス事業者は、本サービス提供に関する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と報告手順を整備し、報告が必要な具体例を含め、サービス利用者に周知すること。		A.16.1.1 責任及び手順 A.16.1.2 情報セキュリティ事象の報告 A.16.1.3 情報セキュリティ弱点の報告	16.1.1 責任及び手順 16.1.2 情報セキュリティ事象の報告 16.1.3 情報セキュリティ弱点の報告	16.1.1 責任及び手順 16.1.2 情報セキュリティ事象の報告	16.1.1 責任及び手順 16.1.2 情報セキュリティ事象の報告
2	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。	サービス利用者の統括情報セキュリティ責任者は、本サービス利用に際する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。	統括情報セキュリティ責任者はサービス事業者が以下の仕組みを持っていることを確認すること。 ・サービス事業者が検知した情報セキュリティインシデントの可能性及び情報セキュリティインシデント事象をサービス利用者に報告する仕組み ・サービス利用者がサービス事業者から報告を受けた情報セキュリティインシデントの可能性及び情報セキュリティインシデント事象の状況を追跡／確認する仕組み	サービス事業者は、本サービス利用に際する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サービス利用者との情報共有を含む対処手順を整備すること。	サービス事業者は、本要件に対し、情報システム及びサービスに関する第三者の監査を受けるセキュリティマネジメントシステム（ISO2700, ISO/IEC27017等）の仕組みの下で遂行することが望ましい。	A.6.1.3 関係当局との連絡	6.1.3 関係当局との連絡	6.1.3 関係当局との連絡	6.1.3 関係当局との連絡
2	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。	サービス利用者の統括情報セキュリティ責任者は、本サービス利用に関する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。		サービス事業者は、本サービス運用に関する情報セキュリティインシデントに備え、サービスシステムについて、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。 本サービス運用に際する情報セキュリティインシデントの可能性又は事象を認知した際の利用者との情報共有を含む対処手順を整備すること。	同上	A.16.1.1 責任及び手順	16.1.1 責任及び手順	16.1.1 責任及び手順	16.1.1 責任及び手順
2	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。	サービス利用者の統括情報セキュリティ責任者は、本サービス利用に関する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。		サービス事業者は、本サービス運用に関する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、サービス運用システムについて、その訓練の内容及び体制を整備すること。		A.17.1.3 情報セキュリティ継続の検証、レビュー及び評価	17.1.3 情報セキュリティ継続の検証、レビュー及び評価	追加要求事項なし	追加要求事項なし
2	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。	サービス利用者の統括情報セキュリティ責任者は、本サービス利用に関する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。		サービス事業者は、本サービス運用に関する情報セキュリティインシデントについて利用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サービス利用者に明示すること。		（A.16.1.2 情報セキュリティ事象の報告）	16.1.2 情報セキュリティ事象の報告	16.1.2 情報セキュリティ事象の報告	16.1.2 情報セキュリティ事象の報告
2	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。	サービス利用者の統括情報セキュリティ責任者は、本サービス利用に関する対処手順が適切に機能することを訓練等により確かにすること。		サービス事業者は、本サービス利用に関する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。		A.17.1.3 情報セキュリティ継続の検証、レビュー及び評価	17.1.3 情報セキュリティ継続の検証、レビュー及び評価	追加要求事項なし	追加要求事項なし
2	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	2.2.4	(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。	サービス利用者は、本サービス利用に関する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。		サービス事業者は、本サービス運用に関する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、情報セキュリティ責任者もしくはCSIRTに報告し、指示に従うこと。		A.16.1.1 責任及び手順 A.16.1.2 情報セキュリティ事象の報告 A.16.1.3 情報セキュリティ弱点の報告	16.1.1 責任及び手順 16.1.2 情報セキュリティ事象の報告 16.1.3 情報セキュリティ弱点の報告	16.1.1 責任及び手順 16.1.2 情報セキュリティ事象の報告	16.1.1 責任及び手順 16.1.2 情報セキュリティ事象の報告
2	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。	CSIRT は、本サービス利用に関する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。		CSIRT は、本サービス運用に関する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。		A.16.1.4 情報セキュリティ事象の評価及び決定 ※CSIRTが役割・責任を持っている場合	16.1.4 情報セキュリティ事象の評価及び決定 ※CSIRTが役割・責任を持っている場合	16.1.1 責任及び手順 16.1.2 情報セキュリティ事象の報告	16.1.1 責任及び手順 16.1.2 情報セキュリティ事象の報告
2	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。	CSIRT 責任者は、本サービス利用に関する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。		CSIRT 責任者は、本サービス運用に関する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。		A.16.1.5 情報セキュリティインシデントへの対応 ※CSIRTが役割・責任を持っている場合	16.1.5 情報セキュリティインシデントへの対応 ※CSIRTが役割・責任を持っている場合	16.1.1 責任及び手順 16.1.2 情報セキュリティ事象の報告	16.1.1 責任及び手順 16.1.2 情報セキュリティ事象の報告

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
2	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。	CSIRT は、本サービス利用に関する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。		CSIRT は、本サービス運用に関する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すること。		A.16.1.5 情報セキュリティインシデントへの対応 ※CSIRTが役割・責任を持っている場合	16.1.5 情報セキュリティインシデントへの対応 ※CSIRTが役割・責任を持っている場合	16.1.1 責任及び手順 16.1.2 情報セキュリティ事象の報告	16.1.1 責任及び手順 16.1.2 情報セキュリティ事象の報告
2	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。	サービス利用者の情報システムセキュリティ責任者は、本サービス利用に関する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。		サービス事業者の情報セキュリティ責任者は、本サービス運用に関する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、規定類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。		A.16.1.5 情報セキュリティインシデントへの対応 ※CSIRTが役割・責任を持っている場合	16.1.5 情報セキュリティインシデントへの対応 ※CSIRTが役割・責任を持っている場合	16.1.1 責任及び手順 16.1.2 情報セキュリティ事象の報告	16.1.1 責任及び手順 16.1.2 情報セキュリティ事象の報告
2	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。	本サービスに該当しない		本サービスに該当しない		A.16.1.5 情報セキュリティインシデントへの対応	16.1.5 情報セキュリティインシデントへの対応	16.1.1 責任及び手順 16.1.2 情報セキュリティ事象の報告	16.1.1 責任及び手順 16.1.2 情報セキュリティ事象の報告
2	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。	国の行政機関における CSIRT は、本サービス利用に関する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。		CSIRT は利用者が国の行政機関で有る場合、本サービス利用に関する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、利用者に連絡すること。		A.6.1.3 関係当局との連絡 A.16.1.5 情報セキュリティインシデントへの対応 ※CSIRTが役割・責任を持つ場合	6.1.3 関係当局との連絡 16.1.5 情報セキュリティインシデントへの対応 ※CSIRTが役割・責任を持つ場合	16.1.2情報セキュリティ事象の報告	16.1.2情報セキュリティ事象の報告
2	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。	CSIRT は、本サービスにおいて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。		CSIRT は、本サービス提供に関する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。		A.6.1.3 関係当局との連絡 A.16.1.5 情報セキュリティインシデントへの対応 ※CSIRTが役割・責任を持つ場合	6.1.3 関係当局との連絡 16.1.5 情報セキュリティインシデントへの対応 ※CSIRTが役割・責任を持つ場合	16.1.2情報セキュリティ事象の報告	16.1.2情報セキュリティ事象の報告
2	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	国の行政機関における CSIRT は、本サービス利用に関する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。		CSIRT は利用者が国の行政機関で有る場合、本サービス利用に関する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）」に基づき報告連絡すること。		A.6.1.3 関係当局との連絡 ※CSIRTが役割・責任を持つ場合	6.1.3 関係当局との連絡 ※CSIRTが役割・責任を持つ場合	6.1.3 関係当局との連絡	6.1.3 関係当局との連絡
2	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。	CSIRT は、本サービス利用に関する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。		CSIRT は、本サービス提供に関する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、勧告又は助言すること。		A.16.1.5 情報セキュリティインシデントへの対応 ※CSIRTが役割・責任を持つ場合	16.1.5 情報セキュリティインシデントへの対応 ※CSIRTが役割・責任を持つ場合	※該当要件なし	※該当要件なし
2	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。	CSIRT は、本サービス利用に関する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。		CSIRT は、本サービス提供に関する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。		A.16.1.7 証拠の収集 ※CSIRTが役割・責任を持つ場合	16.1.7 証拠の収集 ※CSIRTが役割・責任を持つ場合	16.1.7 証拠の収集	16.1.7 証拠の収集
2	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。	CSIRT は、本サービス利用に関する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。		CSIRT は、本サービス提供に関する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すること。		A.6.1.3 関係当局との連絡 ※CSIRTが役割・責任を持つ場合	6.1.3 関係当局との連絡 ※CSIRTが役割・責任を持つ場合	追加要求事項なし	追加要求事項なし
2	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。	CSIRT は、本サービス利用に関する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。		本サービスに該当しない		A.6.1.3 関係当局との連絡 ※CSIRTが役割・責任を持つ場合	6.1.3 関係当局との連絡 ※CSIRTが役割・責任を持つ場合	追加要求事項なし	追加要求事項なし
2	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	2.2.4	(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。	サービス利用者の情報セキュリティ責任者は、本サービス利用に際して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。		サービス事業者の情報セキュリティ責任者は、本サービス運用に際して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。		A.16.1.5 情報セキュリティインシデントへの対応 10.2 不適合及び是正処置 ※CSIRTが役割・責任を持つ場合	16.1.5 情報セキュリティインシデントへの対応 ※CSIRTが役割・責任を持つ場合	追加要求事項なし	追加要求事項なし

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
2	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。	最高情報セキュリティ責任者は、本サービス利用に際して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。		最高情報セキュリティ責任者は、本サービス運用に際して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。		A.16.1.5 情報セキュリティインシデントへの対応 10.2 不適合及び是正処置	16.1.5 情報セキュリティインシデントへの対応 ※情報セキュリティインシデント対応についての役割・責任に依存します。	追加要求事項なし	追加要求事項なし
2	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。	CSIRT 責任者は、本サービス利用に関する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。		CSIRT 責任者は、本サービス運用に関する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。		A.16.1.6 情報セキュリティインシデントからの学習 ※CSIRTが役割・責任を持つ場合	16.1.6 情報セキュリティインシデントからの学習 ※CSIRTが役割・責任を持つ場合	追加要求事項なし	追加要求事項なし
2	2.3	点検											
2	2.3	2.3.1	情報セキュリティ対策の自己点検										
2	2.3	2.3.1	(1)	自己点検計画の策定・手順の準備									
2	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。	サービス利用者の統括情報セキュリティ責任者は、年度自己点検計画に、本サービス利用に関する事項が含まれていることを確かにする。		本サービスに該当しない		9.1 監視、測定、分析及び評価 9.2 内部監査 A.18.2.1 情報セキュリティの独立したレビュー A.18.2.2 情報セキュリティのための方針群及び標準の順守 A.18.2.3 技術的順守のレビュー	18.2.1 情報セキュリティの独立したレビュー 18.2.2 情報セキュリティのための方針群及び標準の順守 18.2.3 技術的順守のレビュー	18.2.1 情報セキュリティの独立したレビュー	18.2.1 情報セキュリティの独立したレビュー
2	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。	サービス利用者の情報セキュリティ責任者は、本サービス利用に際する年度自己点検計画に基づき、サービス利用者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。		本サービスに該当しない		9.1 監視、測定、分析及び評価 A.18.2.2 情報セキュリティのための方針群及び標準の順守 ※職員毎に自己点検を行っている組織は多いです。	18.2.2 情報セキュリティのための方針群及び標準の順守	追加要求事項なし	追加要求事項なし
2	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。	サービス利用者の統括情報セキュリティ責任者は、本サービス利用に際する情報セキュリティの状況の変化に応じ、サービス利用者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。		本サービスに該当しない		9.1 監視、測定、分析及び評価 A.18.2.1 情報セキュリティの独立したレビュー	18.2.1 情報セキュリティの独立したレビュー	18.2.1 情報セキュリティの独立したレビュー	18.2.1 情報セキュリティの独立したレビュー
2	2.3	2.3.1	(2)	自己点検の実施									
2	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。	サービス利用者の情報セキュリティ責任者は、本サービス利用に際する年度自己点検計画に基づき、サービス利用者に自己点検の実施を指示すること。		本サービスに該当しない		9.1 監視、測定、分析及び評価 A.18.2.2 情報セキュリティのための方針群及び標準の順守 A.18.2.3 技術的順守のレビュー	18.2.2 情報セキュリティのための方針群及び標準の順守 18.2.3 技術的順守のレビュー	追加要求事項なし	追加要求事項なし
2	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。	サービス利用者は、本サービス利用に際して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。		本サービスに該当しない		9.1 監視、測定、分析及び評価 A.18.2.2 情報セキュリティのための方針群及び標準の順守 A.18.2.3 技術的順守のレビュー	18.2.2 情報セキュリティのための方針群及び標準の順守 18.2.3 技術的順守のレビュー	追加要求事項なし	追加要求事項なし
2	2.3	2.3.1	(3)	自己点検結果の評価・改善									
2	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。	サービス利用者の情報セキュリティ責任者は、本サービス利用に際する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、評価しなければならない。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。		本サービスに該当しない		9.1 監視、測定、分析及び評価 9.3 マネジメントレビュー	18.2.2 情報セキュリティのための方針群及び標準の順守 18.2.3 技術的順守のレビュー	追加要求事項なし	追加要求事項なし
2	2.3	2.3.1	(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。	サービス利用者の統括情報セキュリティ責任者は、本サービス利用に際して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、評価しなければならない。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。		本サービスに該当しない		9.1 監視、測定、分析及び評価 9.3 マネジメントレビュー	18.2.2 情報セキュリティのための方針群及び標準の順守 18.2.3 技術的順守のレビュー	追加要求事項なし	追加要求事項なし
2	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。	最高情報セキュリティ責任者は、本サービス利用に際する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。		本サービスに該当しない		9.1 監視、測定、分析及び評価 9.3 マネジメントレビュー	18.2.2 情報セキュリティのための方針群及び標準の順守 18.2.3 技術的順守のレビュー	追加要求事項なし	追加要求事項なし
2	2.3	2.3.2	情報セキュリティ監査										
2	2.3	2.3.2	(1)	監査実施計画の策定									
2	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。	サービス利用者の情報セキュリティ監査責任者は、監査実施計画に本サービス利用に関わる事項が含まれていることご確かにすること。		サービス事業者は、監査実施計画に本サービス提供に関わる事項を含むこと。		9.2 内部監査 A.18.2.1 情報セキュリティの独立したレビュー A.18.2.2 情報セキュリティのための方針群及び標準の順守 A.18.2.3 技術的順守のレビュー	18.2.1 情報セキュリティの独立したレビュー 18.2.2 情報セキュリティのための方針群及び標準の順守 18.2.3 技術的順守のレビュー	18.2.1 情報セキュリティの独立したレビュー	18.2.1 情報セキュリティの独立したレビュー

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
2	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。	サービス利用者の情報セキュリティ監査責任者は、本サービス利用に際する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。		サービス事業者は、本サービス利用に際する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。		9.2 内部監査 A.18.2.1 情報セキュリティの独立したレビュー A.18.2.2 情報セキュリティのための方針群及び標準の順守 A.18.2.3 技術的順守のレビュー	18.2.1 情報セキュリティの独立したレビュー 18.2.2 情報セキュリティのための方針群及び標準の順守 18.2.3 技術的順守のレビュー	18.2.1 情報セキュリティの独立したレビュー	18.2.1 情報セキュリティの独立したレビュー
2	2.3	2.3.2	(2)	監査の実施									
2	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	サービス利用者の情報セキュリティ監査責任者は、本サービス利用に際する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。		サービス事業者の情報セキュリティ監査責任者は、本サービス運用に際する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。		9.2 内部監査 9.3 マネジメントレビュー	18.2.1 情報セキュリティの独立したレビュー 18.2.2 情報セキュリティのための方針群及び標準の順守	追加要求事項なし	追加要求事項なし
2	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	(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		(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ること。		9.2 内部監査 9.3 マネジメントレビュー ※対策基準及び統一基準はISO 27001管理策の追加要件になる可能性があります。	18.2.1 情報セキュリティの独立したレビュー 18.2.2 情報セキュリティのための方針群及び標準の順守	追加要求事項なし	追加要求事項なし
2	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	(イ) 実施手順が対策基準に準拠していること		(イ) 実施手順が対策基準に準拠すること。		9.2 内部監査 9.3 マネジメントレビュー ※対策基準及び統一基準はISO 27001管理策の追加要件になる可能性があります。	18.2.1 情報セキュリティの独立したレビュー 18.2.2 情報セキュリティのための方針群及び標準の順守	追加要求事項なし	追加要求事項なし
2	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	(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		(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すること。		9.2 内部監査 9.3 マネジメントレビュー ※対策基準及び統一基準はISO 27001管理策の追加要件になる可能性があります。	18.2.1 情報セキュリティの独立したレビュー 18.2.2 情報セキュリティのための方針群及び標準の順守	追加要求事項なし	追加要求事項なし
2	2.3	2.3.2	(3)	監査結果に応じた対処									
2	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。	最高情報セキュリティ責任者は、本サービス利用に際する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。		最高情報セキュリティ責任者は、本サービス運用に際する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。		10.1 不適合及び是正処置	追加要求事項なし	追加要求事項なし	追加要求事項なし
2	2.3	2.3.2	(3)	(b)	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	サービス利用者の情報セキュリティ責任者は、本サービス利用に際する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。		サービス事業者の情報セキュリティ責任者は、本サービス運用に際する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。		10.1 不適合及び是正処置 9.3 マネジメントレビュー	追加要求事項なし	追加要求事項なし	追加要求事項なし
2	2.3	2.3.2	(3)	(c)	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	サービス利用者の統括情報セキュリティ責任者は、本サービス利用に際する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。		サービス事業者の統括情報セキュリティ責任者は、本サービス運用に際する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。		10.1 不適合及び是正処置 9.3 マネジメントレビュー	追加要求事項なし	追加要求事項なし	追加要求事項なし
2	2.4	見直し											
2	2.4	2.4.1	情報セキュリティ対策の見直し										
2	2.4	2.4.1	(1)	情報セキュリティ関係規程の見直し									
2	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。	最高情報セキュリティ責任者は、本サービス利用に際する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。		最高情報セキュリティ責任者は、本サービス利用に際する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、対策基準について必要に応じて見直すこと。		7.5.1 （文書化した情報）一般 10.2 継続的改善	追加要求事項なし	追加要求事項なし	追加要求事項なし
2	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	サービス利用者の統括情報セキュリティ責任者は、本サービス利用に際する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。		サービス事業者の情報セキュリティ責任者は、本サービス運用に際する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。		7.5.1 （文書化した情報）一般 9.3 マネジメントレビュー	追加要求事項なし	追加要求事項なし	追加要求事項なし
2	2.4	2.4.1	(2)	対策推進計画の見直し									
2	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	最高情報セキュリティ責任者は、本サービス利用に際する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。		最高情報セキュリティ責任者は、本サービス利用に際する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、対策推進計画について定期的に見直すこと。		8.1 運用の計画及び管理	追加要求事項なし	追加要求事項なし	追加要求事項なし

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
3	情報の取扱い												
3	3.1	情報の取扱い											
3	3.1	3.1.1	情報の取扱い										
3	3.1	3.1.1	(1)	情報の取扱いに係る規定の整備									
3	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。	サービス利用者の統括情報セキュリティ責任者は、本サービス利用に際して、以下を含む情報の取扱いに関する規定を整備し、サービス利用者へ周知すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・本サービスに関する情報資産管理台帳を作成すること ・情報資産管理台帳には、本サービス利用により生成された一時保存の情報を含むこと ・本サービスの情報は、情報区分に基づき分類すること ・本サービスで生成された電子データを一時保存する場合は、ファイルサーバもしくは、機関として利用を許可したクラウドサービス上でアクセス制限をして管理すること ・電子媒体、紙媒体を配布・送信・使用する場合は、定められた範囲内に限り行うこと 翻訳情報にPII(個人を特定する情報）・個人情報・機微情報が含まれる場合、以下の事項を確認することが望ましい。 ・情報の翻訳に際して、個人情報の主体と個人情報の利用目的等 ・業務目的を達成するために必要な情報だけを収集して処理すること ・利用者端末（PC、タブレット、専用情報端末）又は翻訳システムに保存される情報は識別し管理されること ・ 利用者端末（PC、タブレット、専用情報端末）に保存する情報は暗号化すること ・ 業務目的の達成後、利用者端末（PC、タブレット、専用情報端末）内の情報は直ちに削除又は廃棄すること ・ 業務目的のために他機関又は他拠点に情報を開示する場合には、個人情報の主体にそのことを通知するとともに、開示したことを記録すること ・ 業務目的を達成した後、開示した情報を直ちに削除すること ・紙媒体は、機密度の高い情報を有する場合施錠管理を行うこと	サービス事業者は、サービス利用者が定める情報の格付け及び取り扱い制限には配慮したサービスを提供すること。	要件を満たすため、以下の施策を実施することが望ましい。 サービス事業者は、サービス利用者の情報の格付け及び取扱制限に従ってサービスを提供、翻訳情報にPII・個人情報・機微情報が含まれる場合、以下の事項を確認する。 ・ 翻訳対象の文書の一部又は音声データの一部を選択して翻訳する機能を提供 ・ 翻訳に関係しない箇所をシステムで処理しない ・ 翻訳システムのログ情報に個人情報・機微情報を含まない ・ 翻訳システムが生成する一時ファイルは、翻訳処理終了後又は定められた周期で削除 ・ 翻訳システムで利用者端末（PC、タブレット、専用情報端末）に配信するまで一時保管される翻訳情報は暗号化され、配信後に速やかに削除 ・ トラブル調査の目的で取得される翻訳情報は、アクセス制御され、調査終了後に速やかに削除 ・ 翻訳システムの性能向上のために再利用する翻訳情報に、PII・個人情報・機微情報が含まれる場合、翻訳情報の匿名化・偽名化等の処理を実施 ・ 翻訳情報の変更や削除は、適切な権限の下で実施、変更を記録	7.5.1 （文書化した情報） 一般 7.5.3 文書化した情報の管理	追加要求事項なし	追加要求事項なし	追加要求事項なし
3	3.1	3.1.2	(2)	(a)	(ア) 情報の格付及び取扱制限についての定義	(ア) 情報の格付及び取扱制限についての定義	同上	(ア) 情報の格付及び取扱制限についての定義	同上	7.5.1 （文書化した情報） 一般 7.5.4 文書化した情報の管理	追加要求事項なし	追加要求事項なし	追加要求事項なし
3	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	(イ) 情報の格付及び取扱制限の明示等についての手続	同上	(イ) 情報の格付及び取扱制限の明示等についての手続	同上	A.8.2.1 情報の分類 A.8.2.2 資産のラベル付け	8.2.1 情報の分類 8.2.2 資産のラベル付け	8.2.2 資産のラベル付け	8.2.2 資産のラベル付け
3	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	(ウ) 情報の格付及び取扱制限の継承、見直しに関する手続	同上	(ウ) 情報の格付及び取扱制限の継承、見直しに関する手続	同上	8.1 運用の計画及び管理	追加要求事項なし	追加要求事項なし	追加要求事項なし
3	3.1	3.1.1	(2)	情報の目的外での利用等の禁止									
3	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。	サービス利用者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、本サービス利用に関する情報を利用等すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・本サービス利用に関する情報を特定した情報資産管理台帳を作成し、情報資産の管理責任者を特定すること ・本サービスの情報資産の利用の範囲と場所を明確にすること 情報及び情報システムと関連する資産の利用の許容範囲については、以下の事項を含めることが望ましい。 ・管理情報は、利用の範囲と場所を明確にして取り扱うこと ・利用者端末（PC、タブレット、専用情報端末）及び外部記録媒体の保管と利用の場所を明確にし、定められた場所からの持ち出しを禁止すること ・組織内構築ネットワークの利用範囲をネットワーク構成図により、明確にすること ・建物、居室、マシンルームの利用範囲をフロアレイアウトにより、明確にすること ・業務を通じて知った情報を家族や友人に話すことを禁止すること	サービス事業者は、本サービスを通じて知りえたサービス利用者の情報は必要な範囲に限って利用すること。	本サービス利用に関する情報を特定した情報資産管理台帳を作成し、情報資産の管理責任者を特定すること。 本サービスの情報資産の利用の範囲と場所を明確にすること。 情報及び情報システムと関連する資産の利用の許容範囲については、以下の手順を参考にすることが望ましい。 ・管理情報は、利用範囲と場所を明確 ・利用者端末（PC、タブレット、専用情報端末）及び外部記録媒体の保管と利用の場所を明確、所定場所からの持ち出しを禁止 ・組織内構築ネットワークの利用範囲をネットワーク構成図による明確 ・建物、居室、マシンルームの利用範囲をフロアレイアウトによる明確 ・業務を通じて知った情報を家族や友人に話すことを禁止	A.8.1.2 資産の管理責任 A.8.1.3 資産利用の許容範囲	8.1.2 資産の管理責任 8.1.3 資産利用の許容範囲	8.1.2 資産の管理責任	8.1.2 資産の管理責任
3	3.1	3.1.1	(3)	情報の格付及び取扱制限の決定・明示等									
3	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。	サービス利用者は、本サービス利用に際して、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。	要件を満たすため、遵守すべき事項に加え、以下の事項を実施することが望ましい。 ・本サービスにおいて作成された機械学習のデータセットについて、サービス事業者との間で、利用範囲を明確にするとともに、仕様書において取扱制限を決定、明示する ・機械学習のデータセットについて、機微な情報が含まれる場合、元となる情報の機密性に係る格付け及び取扱制限を継承する ・また、本サービスにおいて作成された機械学習のデータセットについて、予め、サービス事業者との間で権利関係等を仕様書及び契約書により明確にする	サービス事業者は、本サービス提供に際して、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、明示すること。	要件を満たすため、遵守すべき事項に加え、以下の事項を実施することが望ましい。 ・本サービスにおいて作成された機械学習のデータセットについて、サービス利用者との間で、利用範囲を明確にするとともに、仕様書において取扱制限を決定、明示する ・機械学習のデータセットについて、機微な情報が含まれる場合、元となる情報の機密性に係る格付け及び取扱制限を継承する ・また、本サービスにおいて作成された機械学習のデータセットについて、予め、サービス利用者との間で権利関係等を仕様書及び契約書により明確にする	A.8.2.1 情報の分類 A.8.2.2 資産のラベル付け	8.2.1 情報の分類 8.2.2 資産のラベル付け	8.2.2 資産のラベル付け	8.2.2 資産のラベル付け

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
3	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。	サービス利用者は、本サービス利用に関する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。	同上	サービス事業者は、本サービス提供に関する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。	同上	A.8.2.1 情報の分類 A.8.2.2 資産のラベル付け	8.2.1 情報の分類 8.2.2 資産のラベル付け	8.2.2 資産のラベル付け	8.2.2 資産のラベル付け
3	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。	サービス利用者は、修正、追加、削除その他の理由により、本サービス利用に関する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。	要件を満たすため、遵守すべき事項に加え、以下の事項を実施することが望ましい。 ・本サービスにおいて作成された機械学習のデータセットについて、修正、追加、削除、情報の格付および取扱制限を見直す必要がある場合、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	サービス事業者は、修正、追加、削除その他の理由により、本サービス提供に関する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。	要件を満たすため、遵守すべき事項に加え、以下の事項を実施することが望ましい。 ・本サービスにおいて作成された機械学習のデータセットについて、サービス利用者より、修正、追加、削除、情報の格付けおよび取扱制限を見直しが行われた場合、3.1.1(1)（a)に即して、確認する	A.8.1.2 資産の管理責任	8.1.2 資産の管理責任	8.1.2 資産の管理責任	8.1.2 資産の管理責任
3	3.1	3.1.1	(4)	情報の利用・保存									
3	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。	サービス利用者は、本サービスで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。		サービス事業者は、本サービスで提供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。		A.8.2.3 情報の取扱い	8.2.3 情報の取扱い	追加要求事項なし	追加要求事項なし
3	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。	原則として、本サービスでは機密性３情報を扱わないものとする		本サービスには該当しない		A.8.1.2 資産の管理責任	8.1.2 資産の管理責任 ※機密性区分がスペシフィックなため一般に適用するには読み換えが必要です。	8.1.2 資産の管理責任	8.1.2 資産の管理責任
3	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。	サービス利用者は、本サービス利用に際して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。		本サービスには該当しない		A.8.3.3 物理的媒体の輸送 A.11.1.4 外部及び環境の脅威からの保護 A.11.2.5 資産の移動 A.11.2.6 郊外にある装置及び資産のセキュリティ	8.3.3 物理的媒体の輸送 11.1.4 外部及び環境の脅威からの保護 11.2.5 資産の移動 11.2.6 郊外にある装置及び資産のセキュリティ	追加要求事項なし	追加要求事項なし
3	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。	サービス利用者は、本サービス利用に伴い保存される情報にアクセス制限を設定するなど、情報の格付け及び取扱制限に従って情報を適切に管理すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・電子データは、ファイルサーバもしくは、機関として利用を許可したASPサービス上でアクセス制限をして管理すること ・紙媒体は、機密度の高い情報を有する場合施錠管理を行うこと ・電子媒体、紙媒体を配布・送信・使用する場合は、定められた範囲内に限り行うこと ・個人用PCを業務で使用する場合、申請を行い、承認されたもののみ許可すること ・情報資産及び情報システムへのアクセスは、定められたアクセス制御の方針、運用ルールを規定し、それに従って適切に制限すること ・管理情報の利用者の範囲は、「情報管理規程」に従い、情報管理責任者が、当該情報を業務上知ることが必要不可欠であると認めた、且つ、情報区分に応じた利用者に限定すること ・any公開は特に理由がない限り許可しない。例えばセキュリティグループ等により制限をかけること ・各種サービスへのアクセスは、サービス提供事業者オフィスおよび、事前承認されたIPアドレスからのみに限定すること ・特定のインスタンスは、必要に応じて直接アクセスを許可しない。例えばAWSEC2は踏み台経由のアクセスとすること ・管理画面へのアクセスは多要素認証を実施すること	サービス事業者は、サービス利用者データに、アクセス制限を設定するなど、サービス利用者と同様に情報の格付け及び取扱制限に従って情報を適切に管理すること。 提供するサービス上に一時保存されるデータは、サービス利用者のアクセス制御方針を満たすこと。	要件を満たすため、以下の事項を実施することが望ましい。 ・電子データは、ファイルサーバもしくは、機関として利用を許可したASPサービス上でアクセス制限をして管理 ・紙媒体は、機密度の高い情報を有する場合施錠管理 ・電子媒体、紙媒体を配布・送信・使用する場合は、定められた範囲内に限る ・個人用PCを業務で使用する場合、申請を行い、承認されたもののみ許可 ・情報資産及び情報システムへのアクセスは、定められたアクセス制御の方針、運用ルールを規定し、それに従って適切に制限 ・管理情報の利用者の範囲は、「情報管理規程」に従い、情報管理責任者が、業務上必要不可欠であると認めた情報区分に限定 ・各種サービスへのアクセスは、サービス提供事業者オフィス及び事前承認されたIPアドレスからのみに限定 ・すべてのサーバは、直接アクセスを不許可 ・管理画面へのアクセスは多要素認証を実施	A.8.2.3 情報の取扱い A.9.4.1 情報へのアクセス制限	8.2.3 情報の取扱い 9.4.1 情報へのアクセス制限	9.4.1 情報へのアクセス制限 CLD.9.5.2 仮想マシンの要塞化	9.4.1 情報へのアクセス制限 CLD.9.5.1 仮想コンピューティング環境における分離 CLD.9.5.2 仮想マシンの要塞化
					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。	本サービスには該当しない		本サービスには該当しない		A.8.1.2 資産の管理責任	8.1.2 資産の管理責任	8.1.2 資産の管理責任	8.1.2 資産の管理責任
3	3.1	3.1.1	(4)	(d)	(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。	本サービスには該当しない		本サービスには該当しない		A.9.4.1 情報へのアクセス制限	9.4.1 情報へのアクセス制限 13.1.1 ネットワーク管理策	9.4.1 情報へのアクセス制限	9.4.1 情報へのアクセス制限
3	3.1	3.1.1	(4)	(d)	(イ) 当該情報に対し、暗号化による保護を行うこと。	本サービスには該当しない		本サービスには該当しない		A.10.1.1 暗号による管理策の利用方針 ※可搬PCのHDの暗号化は多くの企業で実施されています。	10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
3	3.1	3.1.1	(4)	(d)	(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。	本サービスには該当しない		本サービスには該当しない		A.11.1.1 物理的セキュリティ境界 A.11.1.2 物理的入退管理策 A.11.1.3 オフィス，部屋及び施設のセキュリティ A.11.1.4 外部及び環境の脅威からの保護 A.11.1.5 セキュリティを保つべき領域での作業 A.11.1.6 受渡場所 A.11.2.1 装置の設置及び保護	11.1.1 物理的セキュリティ境界 11.1.2 物理的入退管理策 11.1.3 オフィス，部屋及び施設のセキュリティ 11.1.4 外部及び環境の脅威からの保護 11.1.5 セキュリティを保つべき領域での作業 11.1.6 受渡場所 11.2.1 装置の設置及び保護	追加要求事項なし	追加要求事項なし
3	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。	サービス利用者は、本サービス利用に際して、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場合、定められた利用手順に従うこと。	要件を満たすため、以下の事項を実施することが望ましい。 ・外部記録媒体は組織内で個体識別管理し、保管・貸出・返却・施錠等の利用状況管理を実施すること ・外部記録媒体の返却時は、残留データがないことを確認し、残留データがある場合は消去すること ・記録媒体の送付時は、指定された配送業者を利用し、配送記録を残すこと	サービス事業者は、本サービス提供に際して、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場合、定められた利用手順に従うこと。	要件を満たすため、以下の事項を実施することが望ましい。 ・外部記録媒体は組織内で個体識別管理し、保管・貸出・返却・施錠等の利用状況管理を実施 ・外部記録媒体の返却時は、残留データがないことを確認し、残留データがある場合は消去 ・記録媒体の送付時は、指定された配送業者を利用し、配送記録化	A.8.3.1 取外し可能な媒体の管理 A.8.3.2 媒体の処分 A.8.3.3 物理的媒体の輸送	8.3.1 取外し可能な媒体の管理 8.3.2 媒体の処分 8.3.3 物理的媒体の輸送	追加要求事項なし	追加要求事項なし
3	3.1	3.1.1	(5)	情報の提供・公表									
3	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。	サービス利用者は、本サービス利用に際して得られた情報について、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。		本サービスには該当しない		A.8.2.1 情報の分類 A.8.2.2 情報のラベル付け ※情報の分類基準についてCSPと情報共有する必要があります。	8.2.1 情報の分類 8.2.2 情報のラベル付け ※機密性区分がスペシフィックなため一般に適用するには読み換えが必要です。	8.2.2 情報のラベル付け	8.2.2 情報のラベル付け
3	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。	サービス利用者は、本サービス利用に際して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。		本サービスには該当しない		A.8.1.2 資産の管理責任 A.8.1.3 資産利用の許容範囲	8.1.2 資産の管理責任 8.1.3 資産利用の許容範囲	8.1.2 資産の管理責任	8.1.2 資産の管理責任
3	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。	本サービスには該当しない		本サービスには該当しない		A.8.1.2 資産の管理責任 A.8.1.3 資産利用の許容範囲 A.8.2.1 情報の分類 A.8.2.2 情報のラベル付け ※情報の分類基準についてCSPと情報共有する必要があります。	8.1.2 資産の管理責任 8.1.3 資産利用の許容範囲 8.2.1 情報の分類 8.2.2 情報のラベル付け ※機密性区分がスペシフィックなため一般に適用するには読み換えが必要です。	8.1.2 資産の管理責任 8.2.2 情報のラベル付け	8.1.2 資産の管理責任 8.2.2 情報のラベル付け
3	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。	サービス利用者は、本サービス利用に際して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。	要件を満たすため、以下の事項を実施することが望ましい。 ・すべての電磁的記録の提供又は公表は記録すること ・電磁的記録は暗号化し、提供先だけが複合できるようにすること ・提供又は公表する電磁的記録は、提供先に直接届くようにすること ・提供先が電磁的記録の使用用途/目的を達成した際には、電磁的記録は提供先から返却されるか、提供先自身で破壊されることを確認すること	本サービスには該当しない		A.6.2.1 モバイル機器の方針 A.8.3.1 取外し可能な媒体の管理 A.8.3.2 媒体の処分 A.11.2.1 装置の設置及び保護 A.13.2.1 情報転送の方針及び手順	6.2.1 モバイル機器の方針 8.3.1 取外し可能な媒体の管理 8.3.2 媒体の処分 11.2.1 装置の設置及び保護 13.2.1 情報転送の方針及び手順	追加要求事項なし	追加要求事項なし
3	3.1	3.1.1	(6)	情報の運搬・送信									
3	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。	サービス利用者は、本サービス利用に際して取得した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。		本サービスには該当しない		A.6.2.1 モバイル機器の方針 A.8.3.1 取外し可能な媒体の管理 A.11.1.4 外部及び環境の脅威からの保護 A.11.2.5 資産の移動 A.11.2.6 構外にある装置及び資産のセキュリティ ※機密性区分がスペシフィックなため一般に適用するには読み換えが必要です。	6.2.1 モバイル機器の方針 8.3.1 取外し可能な媒体の管理 11.1.4 外部及び環境の脅威からの保護 11.2.5 資産の移動 11.2.6 構外にある装置及び資産のセキュリティ ※機密性区分がスペシフィックなため一般に適用するには読み換えが必要です。	追加要求事項なし	追加要求事項なし

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
3	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	サービス利用者は、本サービス利用に際して取得した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。		本サービスには該当しない		A.13.2.1 情報転送の方針及び手順 A.13.2.2 情報転送に関する合意 A.13.2.3 電子的メッセージ通信 A.10.1.1 暗号による管理策の利用方針 ※機密性区分がスペシフィックなため一般に適用するには読み換えが必要です。	13.2.1 情報転送の方針及び手順 13.2.2 情報転送に関する合意 13.2.3 電子的メッセージ通信 10.1.1 暗号による管理策の利用方針 ※機密性区分がスペシフィックなため一般に適用するには読み換えが必要です。	10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針
3	3.1	3.1.1	(7)	情報の消去									
3	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。	サービス利用者は、本サービス利用に際して取得した要保護情報が保存された電磁的記録媒体が職務上不要となった場合は、速やかに情報を消去しなければならない。		本サービスには該当しない		A.8.3.2 媒体の処分 A.11.2.7 装置のセキュリティを保った処分又は再利用	8.1.4 資産の返却 14.3.1 試験データの保護	CLD.8.1.5 クラウドサービスカスタマの資産の除去	CLD.8.1.5 クラウドサービスカスタマの資産の除去
3	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。	サービス利用者は、本サービス利用に際して取得した要保護情報が保存された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。		本サービスには該当しない		A.8.3.2 媒体の処分 A.11.2.7 装置のセキュリティを保った処分又は再利用	8.3.2 媒体の処分 11.2.7 装置のセキュリティを保った処分又は再利用	11.2.7 装置のセキュリティを保った処分又は再利用	11.2.7 装置のセキュリティを保った処分又は再利用
3	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。	サービス利用者は、本サービス利用に際して取得した要保護情報が記載された書面を廃棄する場合には、復元が困難な状態にすること。		本サービスには該当しない		A.8.3.2 媒体の処分	8.3.2 媒体の処分	追加要求事項なし	追加要求事項なし
3	3.1	3.1.1	(8)	情報のバックアップ									
3	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。	サービス利用者は、情報の格付に応じて、適切な方法で本サービス利用に際して、情報のバックアップを実施すること。	本サービスで取り扱う情報のバックアップ機能が本サービスに存在する場合、バックアップ情報が漏洩しない手段を講じること。	サービス事業者は、バックアップ機能を提供する場合は、その仕様及びセキュリティ対策の内容をサービス利用者に提供すること。		A.12.3.1 情報のバックアップ	12.3.1 情報のバックアップ	12.3.1 情報のバックアップ	12.3.1 情報のバックアップ
3	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。	サービス利用者は、本サービス利用に際して、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、適切に管理しなければならない。		サービス事業者は、バックアップ機能を提供する場合は、保存場所、保存方法、保存期間等についてサービス仕様書等に含めること。		A.12.3.1 情報のバックアップ A.8.3.1 取外し可能な媒体の管理 ※バックアップを外部記憶媒体に保存しないケースが多くなっています。	12.3.1 情報のバックアップ 8.3.1 取外し可能な媒体の管理	12.3.1 情報のバックアップ	12.3.1 情報のバックアップ
3	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。	サービス利用者は、保存期間を過ぎた本サービス利用に際する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。		サービス事業者は、バックアップ機能を提供する場合は、保存場所、保存方法、保存期間等についてサービス仕様書等に含めること。		A.8.3.2 媒体の処分 A.11.2.7 装置のセキュリティを保った処分又は再利用	8.3.2 媒体の処分 11.2.7 装置のセキュリティを保った処分又は再利用	11.2.7 装置のセキュリティを保った処分又は再利用	11.2.7 装置のセキュリティを保った処分又は再利用
3	3.2	情報を取り扱う区域の管理											
3	3.2	3.2.1	情報を取り扱う区域の管理										
3	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	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。	サービス利用者の統括情報セキュリティ責任者は、本サービス利用の要管理対策区域の範囲を定めること。	要管理対策区域は、以下の事項を考慮して定めること。 ・本サービスに関連する情報資産（ネットワーク機器、PC等）の配置を考慮して物理的境界を定めること ・サービス利用者以外が端末等にアクセスすることを防止する手段を講じること	本サービスには該当しない		A.11.1.1 物理的セキュリティ境界	11.1.1 物理的セキュリティ境界	追加要求事項なし	追加要求事項なし
3	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。	サービス利用者の統括情報セキュリティ責任者は、本サービス利用に際し、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。	要件を満たすため、以下の事項を実施することが望ましい。 ・セキュリティ上の要求事項のあるセキュリティエリアには、入退室を制御するシステム等の導入	本サービスには該当しない		A.11.1.1 物理的セキュリティ境界	11.1.1 物理的セキュリティ境界	追加要求事項なし	追加要求事項なし
3	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。	(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。	同上	本サービスには該当しない		A.11.1.2 物理的入退管理策 A.11.2.1 装置の設置及び保護	11.1.2 物理的入退管理策 11.2.1 装置の設置及び保護	追加要求事項なし	追加要求事項なし
3	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。	(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。	同上	本サービスには該当しない		A.11.1.2 物理的入退管理策	11.1.2 物理的入退管理策	追加要求事項なし	追加要求事項なし
3	3.2	3.2.1	(2)	区域ごとの対策の決定									
3	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。	サービス利用者の情報セキュリティ責任者は、本サービス利用に際して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。		サービス事業者の情報セキュリティ責任者は、本サービス利用に際して自ら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。		A.11.1.1 物理的セキュリティ境界	11.1.1 物理的セキュリティ境界	追加要求事項なし	追加要求事項なし
3	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業務の内容、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。	サービス利用者の区域情報セキュリティ責任者は、本サービス利用に際する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業務の内容、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。		本サービスには該当しない		A.11.1.3 オフィス、部屋及び施設のセキュリティ A.11.1.4 外部及び環境の脅威からの保護 A.11.1.5 セキュリティを保つべき領域での作業 A.11.1.6 受渡場所	11.1.3 オフィス、部屋及び施設のセキュリティ 11.1.4 外部及び環境の脅威からの保護 11.1.5 セキュリティを保つべき領域での作業 11.1.6 受渡場所	追加要求事項なし	追加要求事項なし

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
3	3.2	3.2.1	(3)		要管理対策区域における対策の実施								
3	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。	サービス利用者の区域情報セキュリティ責任者は、本サービス利用に際して、管理する区域に対して定めた対策を実施しなければならない。サービス利用者が実施すべき対策については、サービス利用者が認識できる措置を講ずること。		本サービスには該当しない		A.11.1.5 セキュリティを保つべき領域での作業	11.1.5 セキュリティを保つべき領域での作業	追加要求事項なし	追加要求事項なし
3	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。	サービス利用者の区域情報セキュリティ責任者は、本サービス利用に際して、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。		本サービスには該当しない		A.11.2.1 装置の設置及び保護	11.2.1 装置の設置及び保護	追加要求事項なし	追加要求事項なし
3	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。	サービス利用者は、本サービス利用に際して、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。		本サービスには該当しない		A.11.1.5 セキュリティを保つべき領域での作業	11.1.5 セキュリティを保つべき領域での作業	追加要求事項なし	追加要求事項なし
4	外部委託												
4	4.1	外部委託											
4	4.1	4.1.1	外部委託										
4	4.1	4.1.1	(1)		外部委託に係る規定の整備								
4	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。	サービス利用者の統括情報セキュリティ責任者は、本サービス利用に際して、以下に係る規定を整備すること。		サービス事業者は、サービス利用者とサービス事業者との間の情報セキュリティに関する以下の内容を含むサービス仕様書を整備すること。 本サービス提供に際して、その一部を外部委託業者に委託する場合は、以下の内容を含む規定を整備すること。	サービス事業者は、サービス利用者との間で本サービスの実施に係る情報セキュリティ対策を特定し、合意を得ること。 合意内容については、サービス仕様書又は契約書により確認すること。	A.15.1.1 供給者関係のための情報セキュリティの方針 A.15.1.3 ICTサプライチェーン	15.1.1 供給者関係のための情報セキュリティの方針 15.1.3 ICTサプライチェーン	15.1.1 供給者関係のための情報セキュリティの方針 15.1.3 ICTサプライチェーン	15.1.3 ICTサプライチェーン
4	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。）	(ア) 本サービスで扱う業務及び取り扱う情報の範囲を判断する基準	基準を設定するにあたり、本サービスの対象業務を想定し、業務の特性および情報の取り扱い等について整理、確認することが望ましい。	本サービスには該当しない		A.15.1.1 供給者関係のための情報セキュリティの方針 A.15.1.3 ICTサプライチェーン	15.1.1 供給者関係のための情報セキュリティの方針 15.1.3 ICTサプライチェーン	15.1.1 供給者関係のための情報セキュリティの方針	15.1.3 ICTサプライチェーン
4	4.1	4.1.1	(1)	(a)	(イ) 委託先の選定基準	(イ) サービス事業者の選定基準	4.1.1(2)に基づいて策定することが望ましい。	本サービスには該当しない		A.15.1.1 供給者関係のための情報セキュリティの方針 A.15.1.3 ICTサプライチェーン	15.1.1 供給者関係のための情報セキュリティの方針 15.1.3 ICTサプライチェーン	15.1.1 供給者関係のための情報セキュリティの方針	15.1.3 ICTサプライチェーン
4	4.1	4.1.1	(2)		外部委託に係る契約								
4	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。	サービス利用者の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、本サービス利用に際し、委託判断基準に従ってサービス利用をすること。	情報システムセキュリティ責任者は、６章及び７章で示す情報セキュリティ対策に準じた委託判断基準を設定すること。	サービス事業者は、サービス利用者の委託判断基準を確認し、サービス提供可否を判断すること。	サービス事業者は、６章及び７章で示す情報セキュリティ対策を確認、提供可否の判断材料とすること。	A.15.1.1 供給者関係のための情報セキュリティの方針 A.15.1.3 ICTサプライチェーン	15.1.1 供給者関係のための情報セキュリティの方針 15.1.3 ICTサプライチェーン	15.1.1 供給者関係のための情報セキュリティの方針	15.1.3 ICTサプライチェーン
4	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。	サービス利用者の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、本サービス利用する際には、選定基準及び選定手続に従ってサービス提供先を選定すること。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サービス提供先の選定条件とし、仕様内容にも含めること。		選定を受けた場合は、サービス利用者との間で委託契約を締結すること。		A.15.1.2 供給者との合意におけるセキュリティの取扱い A.15.1.3 ICTサプライチェーン	15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICTサプライチェーン	15.1.2 供給者との合意におけるセキュリティの取扱い	15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICTサプライチェーン
4	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	(ア) サービス事業者における情報の目的外利用の禁止をサービス仕様書及び委託仕様書に明記すること。		サービス事業者は、サービス利用者との間で、取り扱う情報について、サービス仕様書及び委託仕様書に利用目的を明記すること。	サービス事業者は、サービス利用者が設定する６章及び７章で示す情報セキュリティ対策を確認しつつ、サービス品質向上に資する情報の取り扱いを協議することが望ましい。 また、サービス品質向上に資する情報の取り扱いについては、サービス仕様書及び委託仕様書に明記、両者で合意を得ること。	A.15.1.2 供給者との合意におけるセキュリティの取扱い A.15.1.3 ICTサプライチェーン	15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICTサプライチェーン	15.1.2 供給者との合意におけるセキュリティの取扱い	15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICTサプライチェーン
4	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	(イ) サービス事業者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をサービス仕様書及び委託仕様書に明記すること。		サービス事業者は、サービス利用者との間で、サービス提供に関する情報セキュリティ対策の実施について、サービス仕様書及び委託仕様書に明記すること。	サービス事業者は、サービス利用者が設定する６章及び７章で示す情報セキュリティ対策を確認、履行可能な管理体制を整備すること。 サービス事業者は、サービス利用者の情報処理または情報資産管理を受託する場合、委託契約にて守秘義務の条項を含め締結すること。	A.13.2.4 秘密保持契約又は守秘義務契約 A.15.1.2 供給者との合意におけるセキュリティの取扱い A.15.1.3 ICTサプライチェーン	13.2.4 秘密保持契約又は守秘義務契約 15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICTサプライチェーン	15.1.2 供給者との合意におけるセキュリティの取扱い	15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICTサプライチェーン
4	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	(ウ) 本サービス利用に当たり、サービス提供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、組織等の意図せざる変更が加えられないための管理体制をサービス仕様書及び委託仕様書に明記すること。	クラウドサービスは技術や時代と共にサービスが進化してくため利用者の利便性とセキュリティ要件を満たす範囲を明確にするため許容される変更範囲を委託仕様書及びサービス仕様書に記載し両者で合意することが望ましい。	本サービス提供に当たり、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、組織等の意図せざる変更が加えられないための管理体制をサービス仕様書及び委託仕様書に明記すること。	サービス事業者は、システム操作ログ等について証跡可能な機能を備えること。 監査の内容や頻度については、委託仕様書及びサービス仕様書に明記することが望ましい。	A.15.1.2 供給者との合意におけるセキュリティの取扱い A.15.2.1 供給者のサービス提供の監視及びレビュー A.15.1.3 ICTサプライチェーン	15.1.2 供給者との合意におけるセキュリティの取扱い 15.2.1 供給者のサービス提供の監視及びレビュー 15.1.3 ICTサプライチェーン	15.1.2 供給者との合意におけるセキュリティの取扱い	15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICTサプライチェーン
4	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	(エ) サービス事業者の資本関係・役員等の情報、実施場所、サービス事業者従事者の所属・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をサービス仕様書及び委託仕様書に明記。	外部委託の実施において、サービス事業者の概況を確認する目的としては、以下の視点が考えられる。 ・経営状況：サービスの持続的かつ安定した提供 ・役員の配置：親企業との関係など経営方針への影響度 ・委託場所： 拠点における保全管理、災害対応など強靭性等 ・従業者 ： 本サービスおよび情報セキュリティに係る専門性	本サービス提供のに当たり、企業の資本関係・役員等の情報、実施場所、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をサービス仕様書及び委託仕様書に明記すること。	サービス事業者は、サービス利用者が委託判断在材料として求める各種情報について最新の情報を提供することが望ましい。	A.15.2.2 供給者のサービス提供の変更に対する管理	15.2.2 供給者のサービス提供の変更に対する管理	追加要求事項なし	追加要求事項なし

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
4	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	(オ) 2.2.4章で定めた情報セキュリティインシデントへの対処方法の内、サービス事業者に求める対処方法についてサービス仕様書及び委託仕様書に明記。	情報セキュリティインシデントへの適切な対処および履行するため、以下の事項を確認することが望ましい。 ・情報セキュリティインシデント対応結果をレビューするに際し、委託仕様書及びサービス仕様書又は契約要件との整合 ・新たな事象等の発生による情報セキュリティインシデント対応については、6章及び7章で示すセキュリティ対策の確認とともに５章で示す情報システム対策の見直しへの反映	2.2.4章で定めたサービス提供に関する情報セキュリティインシデントへの対処方法をサービス仕様書及び委託仕様書に明記すること。	サービス事業者は、委託仕様書にインシデントの対処方法の要求事項を記載し合意すること。	A.15.2.2 供給者のサービス提供の変更に対する管理	15.2.2 供給者のサービス提供の変更に対する管理	追加要求事項なし	追加要求事項なし
4	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	(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をサービス仕様書及び委託仕様書に明記。	本サービスにおける情報セキュリティ対策の履行を確認するため、以下の事項を仕様書に記載することが望ましい。 ・サービス利用者に対し定期的な報告 ・外部事業者による情報セキュリティ監査	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をサービス仕様書に明記すること。	サービス事業者は、サービス利用者の要求に対し、以下の情報セキュリティ対策を履行、確認にすること。 ・サービス事業者に対し定期的な報告 ・第三者認証機関等による情報セキュリティ監査	A.15.1.2 供給者との合意におけるセキュリティの取扱い A.16.1.5 情報セキュリティインシデントへの対応 A.15.1.3 ICTサプライチェーン	15.1.2 供給者との合意におけるセキュリティの取扱い 16.1.5 情報セキュリティインシデントへの対応 15.1.3 ICTサプライチェーン	15.1.2 供給者との合意におけるセキュリティの取扱い	15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICTサプライチェーン
4	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	(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をサービス仕様書及び委託仕様書に明記。	本サービスにおいて、外部環境の変化等からサービス事業者による情報セキュリティ対策の履行が不十分な場合が発生する可能性があるため、本サービスを含むクラウドサービスに関した外部環境変化についてサービス事業者とともに定期的な情報交換を実施することが望ましい。 サービス事業者の同業他社の動きなどサービス利用者自身で関連する情報を収集しておくことが望ましい。 サービス利用者は、サービス事業者に対し改善計画要求および暫定対策を要求することが望ましい。 サービス事業者により講じられる対策により改善しないと判断した場合、サービス事業者に対しその旨を報告するとともに、事後について協議することが望ましい。	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をサービス仕様書及び委託仕様書に明記すること。	サービス事業者は、サービス利用者からの改善要求および暫定対策要求に対し適切に対処すること。 サービス事業者は、要求された対策により改善しないと判断した場合、サービス利用者に対しその旨を報告するとともに、事後について協議すること。	A.15.2.1 供給者のサービス提供の監視及びレビュー	15.2.1 供給者のサービス提供の監視及びレビュー	追加要求事項なし	追加要求事項なし
4	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。	サービス利用者の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、本サービス利用に際し、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サービス仕様書及び委託仕様書に含めること。		サービス事業者はサービス利用者間で、業務で取り扱う情報について、業務対象の範囲を確認すること。	サービス事業者は、本サービスの特性として、音声データ、ファイル、テキストに対し、情報のセキュリティ格付けによる排除が行えないことから、格付けの上位のセキュリティ対策をサービス仕様書及び委託仕様書で明記することが望ましい。	A.15.2.2 供給者のサービス提供の変更に対する管理	15.2.2 供給者のサービス提供の変更に対する管理	追加要求事項なし	追加要求事項なし
4	4.1	4.1.1	(2)	(c)	(ア) 情報セキュリティ監査の受入れ	(ア) 情報セキュリティ監査の受入れ	情報セキュリティ監査の受入れについて、サービス事業者と協議し情報セキュリティ監査を定期的又は必要に応じて実施することが望ましい。 監査は、契約の履行状況を確認することが第一義であるが、それ以外に監査を通して新たな課題の発見など環境変化への対応において有効である。 加えて、サービス事業者の経営状況等の変化から内部環境における課題も顕現化される場合があることも留意しておくこと。	情報セキュリティ監査の受け入れ内容をサービス仕様書及び委託仕様書に明記すること。	情報セキュリティ監査の受入れについて、サービス利用者との間でその内容及び頻度を協議・合意した上で情報セキュリティ監査を受け入れること。 例えば本要件に対し、情報システム及びサービスに関する第三者の監査を受けるセキュリティマネジメントシステム（ISO2700, ISO/IEC27017等）の仕組みの下で遂行することが望ましい。	A.15.1.2 供給者との合意におけるセキュリティの取扱い A.15.1.3 ICTサプライチェーン	15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICTサプライチェーン	15.1.2 供給者との合意におけるセキュリティの取扱い	15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICTサプライチェーン
4	4.1	4.1.1	(2)	(c)	(イ) サービスレベルの保証	(イ) サービスレベルの保証	原則、本サービスでは要安定情報は取り扱わない。 要安定情報を扱う場合、サービス事業者との合意にはサービスレベルの保証についての記載を含むこと。	本サービスに該当しない		A.15.1.2 供給者との合意におけるセキュリティの取扱い A.15.2.1 供給者のサービス提供の監視及びレビュー A.15.1.3 ICTサプライチェーン	15.1.2 供給者との合意におけるセキュリティの取扱い 15.2.1 供給者のサービス提供の監視及びレビュー 15.1.3 ICTサプライチェーン	15.1.2 供給者との合意におけるセキュリティの取扱い	15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICTサプライチェーン
4	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。	サービス利用者の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、サービス事業者がサービス運用の一部を外部に再委託する場合は、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対策が十分に確保されるよう、上記(b)(c)の実施内容をサービス事業者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、仕様内容に含めなければならない。また、委託判断基準及びサービス事業者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。	本サービスを含むクラウドサービスにおいては、多様なビジネスモデルをもってサービス提供が行われている。そのなかには、企業と連携し他社との差別化などを進めている企業も多い。 こうした点を踏まえ、サービス利用者は、目的と期待効果に即したクラウドサービスの利用の視点から、委託判断およびサービス事業者選定基準を設定することになる。 その際、再委託先を含む場合、情報セキュリティ水準維持を前提に再委託先における情報セキュリティ対応状況や対策実施について確認、再委託の可否を判断すること。	本サービス提供に際し、サービス運用の一部を外部に再委託する場合は、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)の措置の実施を確認するとともに、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。	サービス事業者は、本サービスの提供に際して、再委託先のサービスを利用する場合、情報セキュリティ水準を自身のサービス利用者に対するものと同等又はそれ以上に保ち、再委託先に経営状況や管理運用、人員についても併せて確認すること。	A.15.1.2 供給者との合意におけるセキュリティの取扱い A.15.1.3 ICTサプライチェーン	15.1.1 供給者関係のための情報セキュリティの方針 15.1.3 ICTサプライチェーン	15.1.1 供給者関係のための情報セキュリティの方針	15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICTサプライチェーン

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
4	4.1	4.1.1	(3)	外部委託における対策の実施									
4	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、サービス事業者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。	サービス利用者の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、本サービス利用に際し、契約に基づき、サービス事業者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。	サービス事業者への情報セキュリティ監査を計画し、実施し、結果を評価すること。監査項目には以下の事項を含めることが望ましい。 ・目的外利用の禁止 ・情報セキュリティ対策の実施内容及び管理体制 ・変更が加えられないための管理体制 ・資本関係・役員等の情報、実施場所、サービス事業者の所属・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 ・情報セキュリティインシデントへの対処方法 ・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 ・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 ・情報セキュリティ監査の受入れ ・サービスレベルの保証 サービス事業者への情報セキュリティ監査が現実的ではないと判断される場合には、代替手段（例えば、第三者認証の維持状況、サービス事業者の内部監査結果等のレビュー）を検討すること。	本サービス利用に際し、契約に基づき、サービス利用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。	サービス事業者は、サービス利用者間で情報セキュリティ監査を計画し、実施し、結果を評価すること。監査には、以下の項目を含むことが望ましい。 ・目的外利用の禁止 ・情報セキュリティ対策の実施内容及び管理体制 ・変更が加えられないための管理体制 ・資本関係・役員等の情報、実施場所、サービス事業者の所属・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 ・情報セキュリティインシデントへの対処方法 ・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 ・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 ・情報セキュリティ監査の受入れ ・サービスレベルの保証 情報セキュリティ監査が現実的ではないと判断される場合には、代替手段（例えば、第三者認証の維持状況、サービス事業者の内部監査結果等のレビュー）を検討すること。	A.15.2.1 供給者のサービス提供の監視及びレビュー	15.2.1 供給者のサービス提供の監視及びレビュー	追加要求事項なし	追加要求事項なし
4	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。	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、サービス利用において、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サービス利用者より受けた場合は、本サービスの利用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サービス事業者に講じさせること。	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については、サービス利用者およびサービス事業者においては、致命的な事象に発展する可能性が高い。とりわけ、機密性情報を含む情報の取り扱いにおいては、その他業務への影響も想定しておくこと。 このため、まず被害を最小限度に抑える行動を第一義とし、次に事象の影響を確認の後、サービス事業者に対し、対処を求めることが望ましい。 その際、クラウドサービスは資源、サービスの共有が前提となることから、他機関への影響を考慮するため、他機関間での情報交換等を進めた実施が肝要である。	サービス利用において、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サービス利用者より受けた場合は、本サービスを一時中断するなどの必要な措置を講じた上で、委託契約に基づく対処をサービス事業者に講じること。	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については、サービス利用者およびサービス事業者においては、致命的な事象に発展する可能性が高い。とりわけ、機密性情報を含む情報の取り扱いにおいては、その他業務への影響も想定しておくべきである。 このため、まず被害を最小限度に抑える行動を第一義とし、次に事象の影響を確認の後、サービス事業者は、適切に対策を講じる。 その際、クラウドサービスは資源、サービスの共有が前提となることから、他機関への影響を考慮するため、サービス利用者と協議し進めることが肝要である。	A.15.1.3 ICTサプライチェーン	15.1.3 ICTサプライチェーン	追加要求事項なし	15.1.3 ICTサプライチェーン
4	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。	サービス利用者の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、本サービス利用に際し、サービス利用の終了時に、サービス事業者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。	本サービス利用においてサービス利用の終了時については、サービス仕様書又は契約条件に本サービス利用終了時の情報の返却又は抹消について取り決めを含めること。 業務終了時において、返却される情報および抹消される情報を特定しておくことが望ましい。 情報セキュリティ水準維持に即した返却、抹消方法についてサービス事業者に確認すること。	サービス事業者は、サービス利用の終了時に、サービス利用の取り決めに従い取り扱われた情報を確実に返却又は抹消すること。	サービス利用の終了時については、サービス仕様書又は契約条件に本サービス利用終了時の情報の返却又は抹消について取り決めを含める。 また、サービス利用終了時において、返却される情報及び抹消される情報を特定しておくことが望ましい。 加えて、情報セキュリティ水準維持に即した返却、抹消方法についてサービス利用者と確認する。	A.8.1.4 資産の返却	8.1.4 資産の返却	CLD.8.1.5 クラウドサービスカスタマの資産の除去	CLD.8.1.5 クラウドサービスカスタマの資産の除去
4	4.1	4.1.1	(4)	外部委託における情報の取扱い									
4	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。	サービス利用者は、サービス事業者への情報の提供等において、以下の事項を遵守すること。				A.15.1.2 供給者との合意におけるセキュリティの取扱い	15.1.2 供給者との合意におけるセキュリティの取扱い	15.1.2 供給者との合意におけるセキュリティの取扱い	15.1.2 供給者との合意におけるセキュリティの取扱い
4	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。	(ア) 本サービス利用に際し要保護情報を取り扱う場合は、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。	本サービスの利用において要保護情報を取り扱う場合には、情報漏洩等による影響を最小化することを前提にし、本サービスのアプリケーションを使用した情報の授受に限定されていることを確認すること。 トラブルシューティング等の目的で、要保護情報を本サービスのアプリケーション以外の手段でサービス事業者に提供する際には、情報セキュリティ責任者の許可を得て行い、目的が達成された後、直ちに情報が削除されることを確認すること。この場合、情報の授受は記録することが望ましい。	サービス事業者は、原則として本サービスのアプリケーションを使用した情報の授受に限定すること。	本サービスの利用において要保護情報を取り扱う場合には、情報漏洩等による影響を最小化することを前提にし、以下の視点を確かにすること。 ・本サービスのアプリケーションを使用した情報の授受に限定 ・トラブルシューティング等の目的で、要保護情報を本サービスのアプリケーション以外の手段で取り扱う場合、情報セキュリティ責任者の許可を得て行い、目的が達成された後、速やかに情報を削除 ・例外的な情報の授受は記録することが望ましい。	A.8.2.3 資産の取扱い A.13.2.2 情報転送に関する合意 A.13.2.3 電子的メッセージ通信	8.2.3 資産の取扱い 13.2.2 情報転送に関する合意 13.2.3 電子的メッセージ通信	追加要求事項なし	追加要求事項なし
4	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。	(イ) 本サービス利用に際し、 提供した要保護情報がサービス事業者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。	本サービスのアプリケーションで要保護情報を取り扱う場合の返却又は消去については、6.1.4のログの取得・管理の要件を確認すること。	6.1.4のログの取得・管理の要件の実施を確かにすること。		A.8.1.4 資産の返却	8.1.4 資産の返却	CLD.8.1.5 クラウドサービスカスタマの資産の除去	CLD.8.1.5 クラウドサービスカスタマの資産の除去
4	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。	(ウ) 本サービス利用において、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。		サービス事業者は、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、速やかにサービス利用者に報告すること。		A.15.1.2 供給者との合意におけるセキュリティの取扱い	15.1.2 供給者との合意におけるセキュリティの取扱い	15.1.2 供給者との合意におけるセキュリティの取扱い	追加要求事項なし
4	4.1	4.1.2	約款による外部サービスの利用										
4	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	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	本サービスは外部委託による利用を前提としているため、本項目については対象外とする。 要機密情報を取り扱わない場合であって、サービス事業者における高いレベルの 情報管理を要求する必要が無い場合には、別途情報セキュリティ対策を講じること。		本サービスに該当しない		A.13.2.4 秘密保持契約又は守秘義務契約 A.15.1.2 供給者との合意におけるセキュリティの取扱い A.15.1.3 ICT サプライチェーン	13.2.4 秘密保持契約又は守秘義務契約 15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICT サプライチェーン	15.1.2 供給者との合意におけるセキュリティの取扱い	15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICT サプライチェーン
4	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	本サービスに該当しない		本サービスに該当しない		A.15.1.2 供給者との合意におけるセキュリティの取扱い A.15.1.3 ICT サプライチェーン	15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICT サプライチェーン	15.1.2 供給者との合意におけるセキュリティの取扱い	15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICT サプライチェーン
4	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	本サービスに該当しない		本サービスに該当しない		A.15.1.3 ICT サプライチェーン	15.1.3 ICT サプライチェーン	追加要求事項なし	15.1.3 ICT サプライチェーン
4	4.1	4.1.2	(1)	(a)	(ウ) 利用手続及び運用手順	本サービスに該当しない		本サービスに該当しない		A.15.1.3 ICT サプライチェーン	15.1.3 ICT サプライチェーン	追加要求事項なし	15.1.3 ICT サプライチェーン

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
4	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。	本サービスに該当しない		本サービスに該当しない		A.15.1.3 ICT サプライチェーン	15.1.3 ICT サプライチェーン	追加要求事項なし	15.1.3 ICT サプライチェーン
4	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	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。	本サービスに該当しない		本サービスに該当しない		A.15.1.3 ICT サプライチェーン	15.1.3 ICT サプライチェーン	追加要求事項なし	15.1.3 ICT サプライチェーン
4	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	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	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。	本サービスに該当しない		本サービスに該当しない		A.13.2.3 電子的メッセージ通信	13.2.3 電子的メッセージ通信	追加要求事項なし	追加要求事項なし
4	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。	本サービスに該当しない		本サービスに該当しない		A.9.4.2 セキュリティに配慮したログオン手順 A.13.2.3 電子的メッセージ通信	9.4.2 セキュリティに配慮したログオン手順 13.2.3 電子的メッセージ通信	追加要求事項なし	追加要求事項なし
4	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。	本サービスに該当しない。		本サービスに該当しない。		A.9.2.1 利用者登録及び登録削除 A.9.2.2 利用者アクセスの提供 A.9.2.4 利用者の秘密情報の管理	9.2.1 利用者登録及び登録削除 9.2.2 利用者アクセスの提供 9.2.4 利用者の秘密情報の管理	9.2.1 利用者登録及び登録削除 9.2.2 利用者アクセスの提供 9.2.4 利用者の秘密情報の管理	9.2.1 利用者登録及び登録削除 9.2.2 利用者アクセスの提供 9.2.4 利用者の秘密情報の管理
4	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。	本サービスに該当しない		本サービスに該当しない		A.13.2.3 電子的メッセージ通信	13.2.3 電子的メッセージ通信 ※サービスごとの責任者に関する要件はISO 27002にはありません。	追加要求事項なし	追加要求事項なし
4	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。	本サービスに該当しない		本サービスに該当しない		※該当要件なし	※該当要件なし	※該当要件なし	※該当要件なし
4	4.1	4.1.4	クラウドサービスの利用										
4	4.1	4.1.4	(1)	クラウドサービスの利用における対策									
4	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。	サービス利用者の情報セキュリティ責任者は、本サービスの利用の決定に際して、取り扱う情報の格付及び取扱制限を考慮すること。	情報セキュリティ責任者は、本サービスの利用の決定に際して、情報セキュリティリスクアセスメントを実施し、本サービスで取り扱う情報の格付及び取扱制限を評価すること。 情報セキュリティリスクアセスメントの結果、受容できないリスクがあった場合には、サービス事業者に要件を満たすための対策を指示するかあるいは、要件を満たすサービスを検討すること。	サービス事業者は、サービス利用者が定める情報セキュリティ方針に配慮し、対策を講じること。	サービス事業者は、サービス利用者が許容できないリスクを特定した場合、適切に対応、提案すること 提案したリスク対応をサービス仕様書及び委託仕様書に反映し実施するに反映し、確かにすること。 リスクが受容されるよう必要に応じてシステムを改修すること。	A.15.1.1 供給者関係のための情報セキュリティの方針	15.1.1 供給者関係のための情報セキュリティの方針	15.1.1 供給者関係のための情報セキュリティの方針	追加要求事項なし
4	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。	サービス利用者は、サービス事業者が取り扱う音声データ・対訳等の文字データが保存されるサーバが日本国内に存在することを確認すること。サービス事業者がクラウドサーバ(IaaS)を利用している場合、サーバが国内に設置され、かつ国内法の適用受ける約款若しくは契約等のもとで利用していることを確認すること。		本サービス提供にあたりクラウドサーバ(IaaS)を利用する場合、サーバが国内に設置され、かつ国内法の適用受ける約款若しくは契約等のもとで利用すること。		A.15.1.2 供給者との合意におけるセキュリティの取扱い	15.1.2 供給者との合意におけるセキュリティの取扱い	18.1.1 適用法令及び契約上の要求事項の特定	18.1.1 適用法令及び契約上の要求事項の特定
4	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。	サービス利用者は、本サービス利用に際し、データ移行性、サービスレベル保証の義務事項とペナルティ、サービス終了の事前通知義務を契約書において確認すること。また、サービスレベルの保証に対する運用実績数値について、サービス事業者から入手し、選定の判断材料にすること。		本サービス提供に際し、データ移行性、サービスレベル保証の義務事項とペナルティ、サービス終了の事前通知義務をサービス仕様書又は契約書に記載すること。		A.15.1.1 供給者関係のための情報セキュリティの方針	15.1.1 供給者関係のための情報セキュリティの方針	15.1.1 供給者関係のための情報セキュリティの方針	追加要求事項なし
4	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。	情報システムセキュリティ責任者は、本サービスの特性を考慮した上で、本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。	6章、7章記載のセキュリティ要件項目を含めること。	サービス利用者が本サービスの流通経路全般にわたるセキュリティの要件を知るために必要な情報を提供すること。	提供する情報には6章、7章記載のセキュリティ要件項目を含めること。	A.13.1.2 ネットワークサービスのセキュリティ A.13.1.3 ネットワークの分離	13.1.2 ネットワークサービスのセキュリティ 13.1.3 ネットワークの分離	13.1.3 ネットワークの分離	13.1.3 ネットワークの分離

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
4	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。	サービス利用者の情報システムセキュリティ責任者は、本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、本サービス及び当該サービス事業者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。	クラウドサービス事業者および当該サービスの信頼性を総合的に判断するためには、取り扱う情報の機密性、完全性、可用性が確保されていることが前提となる。 また、情報セキュリティ対策が適切に整備されるためには、サービス事業者の経営など事業全般による評価が重要となる。 このため、サービス事業者は、サービス事業者における監査報告結果をはじめISMS等の認証取得状況（例：ISO/IEC27001、27017）を踏まえ、総合的に評価することが望ましい。	サービス事業者は、サービス事業者が主張する情報セキュリティ管理策の実施を立証するために、サービス利用者に文書化した証拠を提供すること。	サービス事業者は、情報セキュリティに関する第三者認証取得状況を提示すること。	A.15.2.1 供給者のサービス提供の監視及びレビュー	15.2.1 供給者のサービス提供の監視及びレビュー	18.2.1 情報セキュリティの独立したレビュー	18.2.1 情報セキュリティの独立したレビュー
5	情報システムのライフサイクル												
5	5.1	情報システムに係る文書等の整備											
5	5.1	5.1.1	情報システムに係る台帳等の整備										
5	5.1	5.1.1	(1)	情報システム台帳の整備									
5	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。	サービス利用者の統括情報セキュリティ責任者は、本サービス利用に際し、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。 情報システム名 管理課室 当該情報システムセキュリティ責任者の氏名及び連絡先 システム構成 接続する機関等外通信回線の種別 取り扱う情報の格付及び取扱制限に関する事項 当該情報システムの設計・開発、運用・保守に関する事項 また、民間事業者等が提供する情報処理サービスにより情報システムを構築する場合は、以下を含む内容についても台帳として整備すること。 情報処理サービス名 契約事業者 契約期間 情報処理サービスの概要 ドメイン名		サービス事業者は、サービス利用者が、本サービス利用に関わる情報システムのセキュリティ要件及び関連する事項について、情報システム台帳の整備に必要な情報を提供すること。	ユーザーマニュアルあるいは、ISO/IEC27017に基づくセキュリティ関連の開示資料を提示すること。	A.12.1.1 操作手順書 ※情報システム台帳をシステム毎の操作手順書と読み換えました。	12.1.1 操作手順書 ※情報システム台帳をシステム毎の操作手順書と読み換えました。	CLD.12.1.5 実務管理者の運用のセキュリティ	CLD.12.1.5 実務管理者の運用のセキュリティ
5	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。	情報システムセキュリティ責任者は、台帳の記載内容に更改がある場合には、記載内容を更新し、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。		更改する場合には、台帳の記載内容を通知すること。		A.12.1.1 操作手順書 ※情報システム台帳をシステム毎の操作手順書と読み換えました。	12.1.1 操作手順書 ※情報システム台帳をシステム毎の操作手順書と読み換えました。	CLD.12.1.5 実務管理者の運用のセキュリティ	CLD.12.1.5 実務管理者の運用のセキュリティ
5	5.1	5.1.1	(2)	情報システム関連文書の整備									
5	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。	サービス利用者の情報システムセキュリティ責任者は、本サービス利用に際し、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。	要件を満たすため、以下の事項を実施していることが望ましい。 ・システム管理者は、情報システムの利用マニュアル等し、必要とする人が利用できるようにすること。	本サービスの提供に関連する（ア）～（エ）の情報を提供すること。	AWS等を利用している場合は、その旨の情報を提供すること。 ISO/IEC27017に基づくセキュリティの監査結果等を開示することが望ましい。	A.12.1.1 操作手順書 ※情報システム台帳をシステム毎の操作手順書と読み換えました。	12.1.1 操作手順書 ※情報システム台帳をシステム毎の操作手順書と読み換えました。	CLD.12.1.5 実務管理者の運用のセキュリティ	CLD.12.1.5 実務管理者の運用のセキュリティ
5	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	(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	７章に即して関連情報を整備すること。	(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	AWS等を利用している場合は、その旨の情報を提供すること。 ISO/IEC27017に基づくセキュリティの監査結果等を開示することが望ましい。	A.12.1.1 操作手順書 ※情報システム台帳をシステム毎の操作手順書と読み換えました。	12.1.1 操作手順書 ※情報システム台帳をシステム毎の操作手順書と読み換えました。	CLD.12.1.5 実務管理者の運用のセキュリティ	CLD.12.1.5 実務管理者の運用のセキュリティ
5	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	(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	同上	(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	同上	A.12.1.1 操作手順書	12.1.1 操作手順書	CLD.12.1.5 実務管理者の運用のセキュリティ	CLD.12.1.5 実務管理者の運用のセキュリティ
5	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	(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	セキュリティ維持に関する手順については６章を参照し関連文書を整備すること。	(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 サービス事業者は、本サービスのセキュリティ維持情報	同上	A.12.1.1 操作手順書	12.1.1 操作手順書	CLD.12.1.5 実務管理者の運用のセキュリティ	CLD.12.1.5 実務管理者の運用のセキュリティ
5	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	(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	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については、4.1.1(2) (b) オ、カ、キを参照し、関連文書として整備すること。	(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 サービス事業者は、本サービスのインシデントを認知した際の対応方法に関する情報	同上	A.12.1.1 操作手順書	12.1.1 操作手順書	CLD.12.1.5 実務管理者の運用のセキュリティ	CLD.12.1.5 実務管理者の運用のセキュリティ
5	5.1	5.1.2	機器等の調達に係る規定の整備										
5	5.1	5.1.2	(1)	機器等の調達に係る規定の整備									
5	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。	本サービスに該当しない		本サービスに該当しない		A.15.1.3 ICT サプライチェーン	15.1.3 ICT サプライチェーン	追加要求事項なし	15.1.3 ICT サプライチェーン

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
5	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。	本サービスに該当しない		本サービスに該当しない		A.15.1.3 ICT サプライチェーン	15.1.3 ICT サプライチェーン	追加要求事項なし	15.1.3 ICT サプライチェーン
5	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	5.2	5.2.1	情報システムの企画・要件定義										
5	5.2	5.2.1	(1)	実施体制の確保									
5	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。	サービス利用者の情報システムセキュリティ責任者は、本サービス利用に際し、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。	要件を満たすため、以下の事項を実施することが望ましい。 ・サービス事業者と情報セキュリティの役割及び責任の適切な割り当てについて合意し、割り当てられた役割及び責任を遂行できることを確認すること。 ・両当事者の情報セキュリティの役割及び責任は契約書に記載すること。	情報システムセキュリティ責任者は、本サービス提供に際し、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。	要件を満たすため、以下の事項を実施することが望ましい。 ・情報セキュリティ責任者を任命 ・本サービスシステムのセキュリティに関する主管組織、システム管理者を明確 ・サービス利用者と情報セキュリティの役割及び責任の適切な割り当てについて合意し、割り当てられた役割及び責任を遂行できることを確認 ・両当事者の情報セキュリティの役割及び責任は契約書に記載	A.6.1.1 情報セキュリティの役割及び責任	6.1.1 情報セキュリティの役割及び責任	6.1.1 情報セキュリティの役割及び責任	6.1.1 情報セキュリティの役割及び責任
5	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。	本サービスに該当しない		本サービスに該当しない		A.6.1.1 情報セキュリティの役割及び責任	6.1.1 情報セキュリティの役割及び責任	6.1.1 情報セキュリティの役割及び責任	6.1.1 情報セキュリティの役割及び責任
5	5.2	5.2.1	(1)	(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。	最高情報セキュリティ責任者は、5.2.1.(1)(a)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なければならない。		本サービスに該当しない		A.6.1.1 情報セキュリティの役割及び責任 ※CIOの設置について特定の要件にはありませんが、情報セキュリティ体制にCISが任命されている場合もあります。	6.1.1 情報セキュリティの役割及び責任	6.1.1 情報セキュリティの役割及び責任	6.1.1 情報セキュリティの役割及び責任
5	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	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。	サービス利用者の情報システムセキュリティ責任者は、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、本サービスの通信経路の論理的分離及び通信の秘匿性等のへの対策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。	サービス利用者は、６章、７章に記載の要件を策定し、調達仕様書に記載すること。	本サービスに該当しない		A.6.1.5 プロジェクトマネジメントにおける情報セキュリティ A.13.1.2 ネットワークサービスのセキュリティ A.14.1.1 情報セキュリティ要求事項の分析及び仕様化	6.1.5 プロジェクトマネジメントにおける情報セキュリティ 13.1.2 ネットワークサービスのセキュリティ 14.1.1 情報セキュリティ要求事項の分析及び仕様化	14.1.1 情報セキュリティ要求事項の分析及び仕様化	14.1.1 情報セキュリティ要求事項の分析及び仕様化
5	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	(ア) サービス利用者は、クライアント端末およびPC等から本サービスを利用する時に必要な通信路の物理的分離、通信路の論理的分離、通信路の暗号化、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	サービス利用者は、６章、７章に記載の要件を策定し、調達仕様書に記載すること。	本サービスに該当しない		A.14.1.1 情報セキュリティ要求事項の分析及び仕様化	14.1.1 情報セキュリティ要求事項の分析及び仕様化	14.1.1 情報セキュリティ要求事項の分析及び仕様化	14.1.1 情報セキュリティ要求事項の分析及び仕様化
5	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）	(イ) サービス利用者がサービス事業者のサービス稼働状況を監視する必要がある場合、運用管理機能要件	サービス利用者は、６章、７章に記載の要件を策定し、調達仕様書に記載すること。	本サービスに該当しない		A.13.1.2 ネットワークサービスのセキュリティ	13.1.2 ネットワークサービスのセキュリティ	追加要求事項なし	追加要求事項なし
5	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	(ウ) 本サービス利用に際する情報システムに関連する脆弱性についての対策要件	サービス利用者は、６章、７章に記載の要件を策定し、調達仕様書に記載すること。	本サービスに該当しない		12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理
5	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。	情報システムセキュリティ責任者は、本サービスとの接続にインターネット回線を用いる場合は、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。	サービス利用者は、６章、７章に記載の要件を策定し、調達仕様書に記載すること。	本サービスに該当しない		A.13.1.1 ネットワーク管理策 A.13.1.2 ネットワークサービスのセキュリティ	13.1.1 ネットワーク管理策 13.1.2 ネットワークサービスのセキュリティ	追加要求事項なし	CLD.9.5.1 仮想コンピューティング環境における分離 CLD.9.5.2 仮想マシンの要塞化
5	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。	サービス利用者は、本サービスの利用に用いるクライアント端末内に保存されるデータの漏洩に対して、データの暗号化、端末利用時の認証、外部機器への送信禁止措置、本サービス以外のクラウドへのアップロード禁止措置等の対策が取られているか確認すること。これらを満たしていない場合には端末運用上の対策によってこれらが代替できるかを確認すること。	サービス利用者は、６章、７章に記載の要件を策定し、調達仕様書に記載すること。	本サービスに該当しない		A.13.1.1 ネットワーク管理策 A.13.1.2 ネットワークサービスのセキュリティ	13.1.1 ネットワーク管理策 13.1.2 ネットワークサービスのセキュリティ	追加要求事項なし	CLD.9.5.1 仮想コンピューティング環境における分離 CLD.9.5.2 仮想マシンの要塞化

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
5	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。	本サービスに該当しない		本サービスに該当しない		A.14.1.1 情報セキュリティ要求事項の分析及び仕様化	14.1.1 情報セキュリティ要求事項の分析及び仕様化	14.1.1 情報セキュリティ要求事項の分析及び仕様化	14.1.1 情報セキュリティ要求事項の分析及び仕様化
5	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	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。	本サービスに該当しない		本サービスに該当しない		A.14.2.7 外部委託による開発 A.15.1.2 供給者との合意におけるセキュリティの取扱い A.15.1.3 ICTサプライチェーン	14.2.7 外部委託による開発 15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICTサプライチェーン	15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICTサプライチェーン	15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICTサプライチェーン
5	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	本サービスに該当しない		本サービスに該当しない		A.14.2.7 外部委託による開発 A.15.1.2 供給者との合意におけるセキュリティの取扱い A.15.1.3 ICTサプライチェーン	14.2.7 外部委託による開発 15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICTサプライチェーン	15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICTサプライチェーン	15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICTサプライチェーン
5	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	本サービスに該当しない		本サービスに該当しない		A.14.2.7 外部委託による開発 A.15.1.2 供給者との合意におけるセキュリティの取扱い A.15.1.3 ICTサプライチェーン	14.2.7 外部委託による開発 15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICTサプライチェーン	15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICTサプライチェーン	15.1.2 供給者との合意におけるセキュリティの取扱い 15.1.3 ICTサプライチェーン
5	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	本サービスに該当しない		本サービスに該当しない		A.14.2.5 セキュリティに配慮したシステム構築の原則 A.14.2.6 セキュリティに配慮した開発環境	14.2.5 セキュリティに配慮したシステム構築の原則 14.2.6 セキュリティに配慮した開発環境	14.2.1 セキュリティに配慮した開発のための方針	14.2.1 セキュリティに配慮した開発のための方針
5	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	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。	サービス利用者の情報システムセキュリティ責任者は、本サービス利用に際して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。	サービス利用者は、６章、７章に記載の要件を策定し、調達仕様書に記載すること。	本サービスに該当しない		A.15.1.2 供給者との合意におけるセキュリティの取扱い	15.1.2 供給者との合意におけるセキュリティの取扱い	15.1.2 供給者との合意におけるセキュリティの取扱い	15.1.2 供給者との合意におけるセキュリティの取扱い
5	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。	サービス利用者の情報システムセキュリティ責任者は、本サービス利用に際してサービス事業者が実施する情報システムに対し、情報セキュリティ対策の変更内容についても把握すること。	サービス利用者は、６章、７章に記載の要件を策定し、調達仕様書に記載すること。	本サービスに該当しない		A.15.2.2 供給者のサービス提供の変更に対する管理	15.2.2 供給者のサービス提供の変更に対する管理	追加要求事項なし	追加要求事項なし
5	5.2	5.2.2	情報システムの調達・構築										
5	5.2	5.2.2	(1)	機器等の選定時の対策									
5	5.2	5.2.2	(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。	本サービスに該当しない		本サービスに該当しない		※該当要件なし	※該当要件なし	※該当要件なし	※該当要件なし
5	5.2	5.2.2	(2)	情報システムの構築時の対策									
5	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。	本サービスに該当しない		本サービスに該当しない。		A.13.1.1 ネットワーク管理策 A.13.1.2 ネットワークサービスのセキュリティ A.14.1.1 情報セキュリティ要求事項の分析及び仕様化	13.1.1 ネットワーク管理策 13.1.2 ネットワークサービスのセキュリティ 14.1.1 情報セキュリティ要求事項の分析及び仕様化	14.1.1 情報セキュリティ要求事項の分析及び仕様化	CLD.13.1.4 仮想及び物理ネットワークのセキュリティ管理の整合
5	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。	本サービスに該当しない		本サービスに該当しない		A.14.2.9 システムの受入れ試験	14.2.9 システムの受入れ試験	追加要求事項なし	追加要求事項なし
5	5.2	5.2.2	(3)	納品検査時の対策									
5	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。	サービス利用者の情報システムセキュリティ責任者は、本サービスの受入れ時の確認・検査において、仕様書等定められた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。		本サービスに該当しない		A.14.2.9 システムの受入れ試験	14.2.9 システムの受入れ試験	追加要求事項なし	追加要求事項なし

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
5	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	本サービスに該当しない		本サービスに該当しない		A.14.2.9 システムの受入れ試験	14.2.9 システムの受入れ試験	追加要求事項なし	追加要求事項なし
5	5.2	5.2.3	情報システムの運用・保守										
5	5.2	5.2.3	(1)	情報システムの運用・保守時の対策									
5	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。	サービス利用者の情報システムセキュリティ責任者は、サービス事業者が講じているセキュリティ対策内容を確認し、セキュリティ対策が運用されていることを確認すること。		サービス事業者は、重要な操作及び手順を文書化して運用すること。サービス事業者は、情報セキュリティ対策の水準を維持するための体制や仕組みを講ずること。		A.12 運用のセキュリティ	12 運用のセキュリティ	CLD.12.1.5 実務管理者の運用のセキュリティ CLD.12.4.5 クラウドサービスの監視	CLD.12.1.5 実務管理者の運用のセキュリティ CLD.12.4.5 クラウドサービスの監視
5	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。	本サービスに該当しない		本サービスに該当しない		A.12 運用のセキュリティ	12 運用のセキュリティ	CLD.12.1.5 実務管理者の運用のセキュリティ	CLD.12.1.5 実務管理者の運用のセキュリティ
5	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。	サービス利用者は、サービス事業者がセキュリティ要件を維持するために講じている運用対策内容を確認し、セキュリティ要件が維持されることを確認しなければならない。 情報セキュリティ責任者は、サービス事業者に対してサービス利用者の操作履歴の提供を求める。 情報セキュリティ責任者は、システムに関わるインシデント発生もしくは疑いがある場合には、サービス事業者に調査を求める。		要件を満たすため、以下の事項を実施することが望ましい。 ・サービス事業者は、サービス利用者に、ログ取得機能を提供 ・サービス事業者は、サービス利用者の操作履歴を提供 ・サービス事業者は、サービス利用者からシステムに関わるインシデント発生もしくは疑いがある報告を受けた場合の調査に対応		A.12.4.1 イベントログ取得 A.12.4.3 実務管理者及び運用担当者の作業ログ	12.4.1 イベントログ取得 12.4.3 実務管理者及び運用担当者の作業ログ	12.4.1 イベントログ取得 12.4.3 実務管理者及び運用担当者の作業ログ CLD.12.4.5 クラウドサービスの監視	12.4.1 イベントログ取得 12.4.3 実務管理者及び運用担当者の作業ログ CLD.12.4.5 クラウドサービスの監視
5	5.2	5.2.4	情報システムの更改・廃棄										
5	5.2	5.2.4	(1)	情報システムの更改・廃棄時の対策									
5	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。	サービス事業者が政府統一基準を満たすクラウドIaaSサービスを利用している場合には、当該項目は適用外となるが、 自社サーバー利用の場合は、サービス利用者の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じなければならない。 本サービスでは原則該当しない。 ただし情報システムの移行を行う場合は、情報システムセキュリティ責任者は、サービス事業者と作業手順を合意する。	サービス事業者が自社サーバー利用している場合は、サービス事業者が以下の事項を実施していることを確認することが望ましい。 ・管理情報を含む媒体を破棄する場合は、正式な手順で実施すること ・システム内情報(ディスクの場合)は、廃棄業者に委託又は、論理削除を行うこと ・保管期間の過ぎたDVDはシュレッダーで裁断することにより、破棄すること ・破棄対象のUSBメモリをフォーマットし、OS標準の暗号化機能で暗号化する又は、物理的に破壊すること ・PC廃棄業者に廃棄対象PCを送付/回収依頼し、廃棄証明を受け取り、保管すること ・物理マシンがセキュリティを保った処分又は再利用の為の方針があることを確認すること	要件を満たすため、以下の事項を実施することが望ましい。 ・サービス事業者は、本サービスに影響を与える可能性のある本サービスの変更について、本サービスカスタマに情報を提供 ・情報システムの移行を行う場合は、サービス利用者と作業手順を合意の上実施	自社サーバー利用している場合は、要件を満たすため以下の事項を実施することが望ましい。 ・管理情報を含む媒体を破棄する場合は、正式な手順で実施すること ・システム内情報(ディスクの場合)は、廃棄業者に委託又は、論理削除を行うこと ・保管期間の過ぎたDVDはシュレッダーで裁断することにより、破棄すること ・破棄対象のUSBメモリをフォーマットし、OS標準の暗号化機能で暗号化する又は、物理的に破壊すること ・PC廃棄業者に廃棄対象PCを送付/回収依頼し、廃棄証明を受け取り、保管すること ・物理マシンがセキュリティを保った処分又は再利用の為の方針があることを確認すること	A.12.1.2 変更管理	12.1.2 変更管理	12.1.2 変更管理	12.1.2 変更管理
5	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	同上		要件を満たすため、以下の事項を実施することが望ましい。 ・本サービスに運用サイトの機能が存在する場合、当該サイトを定期的に参照し、メンテナンス内容が利用サービスに影響が無いことを確認する	同上	要件を満たすため、以下の事項を実施していることが望ましい。 ・メンテナンス等でサービスを停止する際は、事前にサービス利用者に通知する	A.12.1.2 変更管理	12.1.2 変更管理	12.1.2 変更管理	12.1.2 変更管理
5	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	同上		要件を満たすため、以下の事項を実施することが望ましい。 ・本サービスの利用終了時のデータの削除を含むサービス利用終了に関する説明を要求すること ・サービス事業者からの本サービスの利用終了時のデータ削除の完了通知を要求すること	サービス事業者は、本サービス利用のための合意終了時における、サービス利用者の全ての資産の返却及び除去の取り決めについて、情報を提供すること。	要件を満たすため、以下の事項を実施していることが望ましい。 ・本サービス利用終了時におけるデータの削除取り決めについて、サービス利用者と合意する ・本サービス利用終了時の取り決めに従って、データ及びインスタンスを削除する ・サービス利用者にデータ削除を完了した通知を行う	A.8.3.2 媒体の処分 A.11.2.7 装置のセキュリティを保った処分又は再利用	8.3.2 媒体の処分 11.2.7 装置のセキュリティを保った処分又は再利用	11.2.7 装置のセキュリティを保った処分又は再利用 CLD.8.1.5 クラウドサービスカスタマの資産の除去	11.2.7 装置のセキュリティを保った処分又は再利用 CLD.8.1.5 クラウドサービスカスタマの資産の除去
5	5.2	5.2.5	情報システムについての対策の見直し										
5	5.2	5.2.5	(1)	情報システムについての対策の見直し									
5	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。	サービス利用者は、サービス事業者に、提供を受ける本サービスに影響し得る技術的脆弱性の管理に関する情報を要求しなければならない。 情報システムセキュリティ責任者は、新たな脅威が発生した場合に、サービス事業者に対策を要求する。		要件を満たすため、以下の事項を実施することが望ましい。 ・外部のセキュリティ部門から、脆弱性情報を収集し、組織内構築システムへ必要に応じて対策を講じること ・サポートが終了したソフトウェアを確認し次第、該当ソフト利用者に対して使用禁止である旨の連絡をすること ・サービス事業者に提供されるサービスの脆弱性管理について情報を確認すること	サービス事業者は、提供する本サービスに影響し得る技術的脆弱性の管理に関する情報をサービス利用者が利用できるようにすること。 サービス事業者は、サービス利用者から新たな脅威に対する対策を求められた場合は、対策を実施すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・外部のセキュリティ部門から、脆弱性情報を収集し、社内構築システムへ必要に応じて対策を講じる ・管理部は、サポートが終了したソフトウェアを確認し次第、該当ソフト利用者に対して使用禁止である旨の連絡をする ・システム管理者は必要に応じて対策を実施し、管理部に報告する ・サービス利用者から要望があった場合、脆弱性診断に基づく判断の結果を提供する	A.12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
5	5.3	情報システムの運用継続計画											
5	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	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	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。	統括情報セキュリティ責任者は、本サービス利用に際し、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しなければならない。 本サービスを非常時優先業務に利用するか確認する。 非常時優先業務に利用する場合には、本サービスで提供される機能により非常時の利用手順を定める。	要件を満たすため、以下の事項を実施することが望ましい。 ・困難な状況（会社が被災、長期間の停電時など）が生じた場合の情報セキュリティ継続のため、ソースコード等の可用性確保の対策を要求すること。 例）異なる地域のサーバにソースコードを確保しておく。サービス運用におけるディザスタリカバリ対策など。	サービス事業者は、本サービス利用に際し、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。 サービス事業者は、本サービスを非常時優先業務に利用するか確認すること。 非常時優先業務に利用する場合には、本サービスで提供される機能により非常時の利用手順を定めること。 あらかじめサービス利用者と非常時の運用について検討し合意すること。		A.17.1.1 情報セキュリティ継続の計画	17.1.1 情報セキュリティ継続の計画	追加要求事項なし	追加要求事項なし
5	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	統括情報セキュリティ責任者は、本サービス利用に際し、情報システムの運用継続計画において、定期的に対策事項を見直し、課題を発見した場合は改善すること。		サービス事業者は、合意した内容について課題が発見された場合には対策を見直すこと。		A.17.1.3 情報セキュリティ継続の検証，レビュー及び評価	17.1.3 情報セキュリティ継続の検証，レビュー及び評価	追加要求事項なし	追加要求事項なし
6	情報システムのセキュリティ要件												
6	6.1	情報システムのセキュリティ機能											
6	6.1	6.1.1	主体認証機能										
6	6.1	6.1.1	(1)	主体認証機能の導入									
6	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。	サービス利用者の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、正当な主体であることを検証する必要がある場合、本サービスにおいて、アクセス主体の特定、識別及び認証ができることを確認すること。	情報システムセキュリティ責任者は、本サービスの利用に際して、本サービスの主体の識別及び主体認証機能には、以下の要件が確実に満たされていることを確認すること。 ・正当な主体以外の主体認証を受諾しないこと(誤認の防止) （多要素認証の採用も考慮） ・正当な主体が本人の責任ではない理由で主体認証を拒否されないこと(誤否の防止) ・正当な主体が容易に他の主体に主体認証情報の付与(発行、更新及び変更を含む。)及び貸与ができないこと(代理の防止) ・主体認証情報が容易に複製できないこと(複製の防止) （多要素認証の採用も考慮） ・情報システムセキュリティ責任者の判断により、ログインを個々に無効化でき る手段があること(無効化の確保) ・必要時に中断することなく主体認証が可能であること(可用性の確保) ・新たな主体を追加するために、外部からの情報や装置の供給を必要とする場合 には、それらの供給が情報システムの耐用期間の間、十分受けられること(継続性の確保) ・主体に付与した主体認証情報を利用することが不可能になった際に、正当な主 体に対して主体認証情報を安全に再発行できること(再発行の確保)	サービス事業者は、アクセス主体を特定するための識別および認証機能を提供すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・正当な主体以外の主体認証を受諾しないこと(誤認の防止) （多要素認証の採用も考慮） ・正当な主体が本人の責任ではない理由で主体認証を拒否されないこと(誤否の防止) ・正当な主体が容易に他の主体に主体認証情報の付与(発行、更新及び変更を含む。)及び貸与ができないこと(代理の防止) ・主体認証情報が容易に複製できないこと(複製の防止) （多要素認証の採用も考慮） ・情報システムセキュリティ責任者の判断により、ログインを個々に無効化でき る手段があること(無効化の確保) ・必要時に中断することなく主体認証が可能であること(可用性の確保) ・新たな主体を追加するために、外部からの情報や装置の供給を必要とする場合 には、それらの供給が情報システムの耐用期間の間、十分受けられること(継続性の確保) ・主体に付与した主体認証情報を利用することが不可能になった際に、正当な主 体に対して主体認証情報を安全に再発行できること(再発行の確保)	A.9.2.2 利用者アクセスの提供 A.9.2.3 特権的アクセス権の管理 A.9.2.4 利用者の秘密認証情報の管理 A.9.4.2 セキュリティに配慮したログオン手順	9.2.2 利用者アクセスの提供 9.2.3 特権的アクセス権の管理 9.2.4 利用者の秘密認証情報の管理 9.4.2 セキュリティに配慮したログオン手順	9.2.2 利用者アクセスの提供 9.2.3 特権的アクセス権の管理 9.2.4 利用者の秘密認証情報の管理	9.2.2 利用者アクセスの提供 9.2.3 特権的アクセス権の管理 9.2.4 利用者の秘密認証情報の管理
6	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	本サービスに該当しない		本サービスに該当しない		※固有のシチュエーションが想定されていますが、一般的に設定します。 A.9.4.2 セキュリティに配慮したログオン手順	9.4.2 セキュリティに配慮したログオン手順	追加要求事項なし	追加要求事項なし
6	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。	情報システムセキュリティ責任者は、パスワードなどの秘密情報を管理するシステムが不正アクセスや不正行為を防止する処置が取られていることを確認すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・サービス利用者は個人毎の一意な識別子（ID）の使用 ・付与したユーザアカウントはアカウント管理簿で管理 ・初期パスワードを発行する場合は、速やかに容易に推測できないパスワードに変更 ・パスワードの再発行時は、利用者の本人確認を実施後、初期パスワードを発行 ・仮パスワードの発行時には、利用者本人にのみ通知	サービス事業者は、本システムが不正アクセスや不正行為を防止するための機能を提供すること。	要件を満たすため、以下のような機能を提供するのが望ましい。 ・利用者のみにパスワードを通知 ・不正利用発覚に資する機能 例）前回ログイン日時の表示、パスワード間違えた場合のアカウントロックなど	A.9.2.2 利用者アクセスの提供 A.9.2.4 利用者の秘密認証情報の管理	9.2.2 利用者アクセスの提供 9.2.4 利用者の秘密認証情報の管理	9.2.4 利用者の秘密認証情報の管理	9.2.2 利用者アクセスの提供 9.2.4 利用者の秘密認証情報の管理
6	6.1	6.1.1	(2)	識別コード及び主体認証情報の管理									
6	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。	情報システムセキュリティ責任者は、サービスで提供される利用登録・登録削除の機能及びそれを利用するための仕様を確認し、利用者の識別コードの運用策を講ずること。 サービス事業者の主体に対して同様の対策が講じられているか検証すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・情報システムセキュリティ責任者は、本サービスが提供する利用者登録、登録削除の機能が提供されることを確認 ・利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を付与 ・主体に付与した識別コード(共用識別コー ドを除く。)を別の主体に対して付与することを禁止 ・主体への識別コードの付与に関する記録を消去する場合の情報セキュリティ 責任者からの事前の許可を得る ・主体へ安全な方法で主体認証情報を配布 ・初期設定の主体認証情報(必要に応じて、初期設定の識 別コードも)を速やかに変更するよう促す	サービス事業者は、サービス利用者に利用登録・登録削除の機能を提供すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・利用者登録、登録削除の機能を提供する ・サービス事業者が利用者登録、削除を実施する場合、当該仕様を提示する ・利用者登録後、パスワードを変更する機能を提供する ・利用者登録が完了後、本人にのみ主体情報を配布する機能を提供する	A.9.2.1 利用者登録及び登録削除	9.2.1 利用者登録及び登録削除	追加要求事項なし	9.2.1 利用者登録及び登録削除

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
6	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。	情報システムセキュリティ責任者は、本サービス利用に際し、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。	同上	サービス事業者は、本サービス利用に際し、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。		A.9.2.6 アクセス権の削除又は修正	9.2.6 アクセス権の削除又は修正	追加要求事項なし	追加要求事項なし
6	6.1	6.1.2	アクセス制御機能										
6	6.1	6.1.2	(1)	アクセス制御機能の導入									
6	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。	情報システムセキュリティ責任者は、利用するサービスの管理機能が提供されている場合、サービス利用者の主体に対してアクセス権限が設定でき、適切に運用できることを確認すること。	要件を満たすため、以下の事項を実施していることが望ましい。 ・不必要な権限付与の防止のため、各自の職務及び責任範囲を明確にし、これを順守 ・同一主体による複数アクセスの禁止 ・特定IPアドレスからの利用の制限 ・本サービスのアクセス制御方針については、サービス仕様書及び委託仕様書で確認	サービス事業者は、本サービスの利用に際し、業務上必要な主体のみにアクセスを許可し、リスク軽減すること。	要件を満たすため、以下の事項を実施することが望ましい。 不必要な権限付与の防止のため、各自の職務及び責任範囲を明確にし、順守する ・特定のIPアドレスからのアクセスに制限できる機能を提供する ・同一主体からの複数のアクセスを制御する機能を提供する ・サービス利用者は個人毎の一意な識別子（ID）を使用する	A.9.2.1 利用者登録及び登録削除 A.9.2.3 特権的アクセス権の管理	9.2.1 利用者登録及び登録削除 9.2.3 特権的アクセス権の管理	9.2.3 特権的アクセス権の管理	9.2.1 利用者登録及び登録削除 9.2.3 特権的アクセス権の管理
6	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。	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。	同上	サービス事業者は、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。	サービス事業者は、機能の利用方法についてマニュアルなどで明示すること	A.9.2.3 特権的アクセス権の管理	9.2.3 特権的アクセス権の管理	9.2.3 特権的アクセス権の管理	9.2.3 特権的アクセス権の管理
6	6.1	6.1.3	権限の管理										
6	6.1	6.1.3	(1)	権限の管理									
6	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。	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。	要件を満たすため、以下の事項を実施することが望ましい。 ・アクセス権限を付与する対象者は必要最小限に設定 ・対象者に付与するアクセス権限は必要最小限に設定 ・情報システムセキュリティ責任者に承認を得た対象者にアクセス権限を付与	サービス事業者は、主体に対して権限が適切に設定するための機能を整備すること。	以下の機能を提供することが望ましい。 ・利用者の役割に応じたアクセス権限を付与・削除できる機能 ・利用者に付与されているアクセス権限が確認できる機能	A.9.1.1 アクセス制御方針 A.9.1.2 ネットワーク及びネットワークサービスへのアクセス	9.1.1 アクセス制御方針 9.1.2 ネットワーク及びネットワークサービスへのアクセス	9.1.2 ネットワーク及びネットワークサービスへのアクセス	追加要求事項なし
6	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。	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	要件を満たすため、以下の事項を実施することが望ましい。 ・管理者アカウント（特権ユーザ）は利用者アカウントとは別のアカウントを付与 ・管理者アカウントの割当は必要最小限の人数に制限	サービス事業者は、本サービスにおいて、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機能を整備すること。	以下の機能を提供すること。 ・管理者権限を付与・削除 ・管理者、運用者の役割に応じた最小権限の付与 ・権限変更操作におけるログの記録 以下の事項を実施することが望ましい。 ・不正付与を検知・確認できる機能	A.9.2.3 特権的アクセス権の管理 A.9.4.4 特権的なユーティリティプログラムの使用	9.2.3 特権的アクセス権の管理 9.4.4 特権的なユーティリティプログラムの使用	9.2.3 特権的アクセス権の管理 9.4.4 特権的なユーティリティプログラムの使用	9.2.3 特権的アクセス権の管理 9.4.4 特権的なユーティリティプログラムの使用
6	6.1	6.1.4	ログの取得・管理										
6	6.1	6.1.4	(1)	ログの取得・管理									
6	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。	情報システムセキュリティ責任者は、利用者のシステムへのアクセスを操作ログとして管理すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・サービス事業者から操作ログを取得 ・使用端末において本サービスへのアクセスを操作ログとして取得	サービス事業者は、サービス利用者のシステムへのアクセスを操作ログとして管理すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・サービス事業者は、利用者のアクセスを操作ログとして記録する ・サービス事業者は、利用者の操作ログを取得できるような手段を講じる ・システムのクロックはマスタクロックに同期する ・マスタクロックはNTPサーバや公開NTPサーバと同期する	A.12.4.1 イベントログ取得	12.4.1 イベントログ取得	12.4.1 イベントログ取得	12.4.1 イベントログ取得
6	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。	情報システムセキュリティ責任者は、システムの特性に応じて取得するログの情報項目、保護方法、保管期間等を明確にしてサービスを選定すること。	要件を満たすため、以下の事項を実施していることが望ましい。 ログの管理 ・情報システムセキュリティ責任者は、サービス事業者のログの管理が利用者のセキュリティポリシーに合致していることを確認 ・操作履歴、アクセス履歴など、区分毎に保管期間、保管場所、管理方法を合意 データの管理 ・情報システムセキュリティ責任者は、本システムで扱うデータ（翻訳対象の文書ファイル、会話内容など）の保存期間、保管場所、管理方法を設定 ・情報システムセキュリティ責任者は、本サービスを利用する業務の特性について、調達時および運用変更時等において、サービス事業者との合意の下、保管期間、保管場所、管理方法を設定	サービス事業者は、サービス利用者に対しシステムの特性に応じて取得するログの情報項目、保護方法、保管期間等を明確にすること。	要件を満たすため、以下の事項を実施することが望ましい。 ・ログの利用目的を明確にする。 例)利用状況の把握 システム保全 サービス品質向上 マーケティングなど ・取得する情報項目を定めて管理する 例)利用者ID、システムの操作、ログの日時及び操作、端末ID、成功・失敗の記録、特権の利用、アクセスされたファイル及びアクセスの種類、アクセス制御システムからの警報、システムの開始・停止等 ・システム障害の原因を特定する情報を取得する ・本システムで扱うデータ（翻訳対象の文書ファイル、会話内容など）については、利用者の合意の下、保存期間、保管場所、管理方法を設定する ・ログ及びデータは物理的または論理的にアクセス権限の限定された場所に保管し、一時的な利用を除き、管理利用者端末には保管しない ・システム管理者はログ及びデータの保管場所へのアクセス権を最小とし、消去や改竄が行われないようにする	A.12.4.2 ログ情報の保護 A.12.4.3 実務管理者及び運用担当者の作業ログ A.18.1.3 記録の保護	12.4.2 ログ情報の保護 12.4.3 実務管理者及び運用担当者の作業ログ 18.1.3 記録の保護	12.4.3 実務管理者及び運用担当者の作業ログ 18.1.3 記録の保護	18.1.3 記録の保護
6	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。	情報システムセキュリティ責任者は、本サービスで提供されたログを定期的に点検又は分析し、不正操作等の有無を確認すること。 サービス事業者からネットワーク外部からの不正侵入の監視状況及び結果について報告を受けること。	要件を満たすため、以下の事項を実施することが望ましい。 ・情報システムセキュリティ責任者は操作ログを定期的に点検又は分析 ・点検・分析の頻度や精度を高めるため必要に応じて、専任担当部署あるいは、外部専業事業者への委託を検討 ・サービス事業者の合意の下点検分析結果の管理方法を設定	サービス事業者のセキュリティ責任者は、本サービスに関わるログを定期的に点検又は分析し、不正操作等の有無を確認すること。 ネットワーク外部からの不正侵入の監視状況及び結果について、サービス利用者に対して報告すること。	要件を満たすため、以下の事項を実施していることが望ましい。 ・ 特権的なシステム操作のログは変更及び削除から適切に保護され、特権を行使するシステム管理者等がログを変更できないように講じる ・ネットワーク外部からの翻訳システムへの不正侵入/不正アクセスの試みは常時監視する ・システム運用保守における操作ログを定期的に点検又は分析する ・利用者の合意の下点検分析結果の管理方法を設定する	A.12.4.1 イベントログ取得	12.4.1 イベントログ取得	12.4.1 イベントログ取得	12.4.1 イベントログ取得

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
6	6.1	6.1.5	暗号・電子署名										
6	6.1	6.1.5	(1)	暗号化機能・電子署名機能の導入									
6	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。								
6	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。	サービス利用者は、認証情報を要機密情報と特定し、暗号化機能による管理策を実施されていることを確認すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・サービス利用者は、ファイルやデータベースに認証情報を保存する場合、データを暗号化し、適切に保護 ・本サービスが提供する暗号化機能が十分な強度を持つことを確認	サービス事業者は、認証情報を要機密情報と特定し、暗号化機能による管理策を実施すること。	要件を満たすため、以下の事項を実施していることが望ましい。 ・ファイルやデータベースに保存する場合は、当該データを暗号化し、適切に保護する ・送受信する場合は暗号化通信を用いるか、データを暗号化する	A.10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針
6	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。	本サービスに該当しない。		本サービスに該当しない。		A.14.1.3 アプリケーションサービスのトランザクションの保護	14.1.3 アプリケーションサービスのトランザクションの保護	追加要求事項なし	追加要求事項なし
6	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。					※固有の要件ですが、一般的な要件と読み換えて： A.10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針
6	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。	情報システムセキュリティ責任者は、システムで使用されている暗号化及び電子署名が、電子政府推奨暗号リストに記載されたアルゴリズムであるかを確認すること。	・「電子政府推奨暗号リスト」に記載されたアルゴリズムの採用を確認 ・「電子政府推奨暗号リスト」に記載されたアルゴリズム以外のものを採用されている場合は、「推奨候補暗号リスト」や「運用監視暗号リスト」に記載された安全性が高いアルゴリズムの採用を確認	本サービ事業者は、使用可能な場合には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を適用すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・「電子政府推奨暗号リスト」に記載されたアルゴリズムを採用することが原則する ・「電子政府推奨暗号リスト」に記載されたアルゴリズム以外のものを採用するこ場合は「推奨候補暗号リスト」や「運用監視暗号リスト」を参照の上、安全性が高いアルゴリズムを採用する	※固有の要件ですが、一般的な要件と読み換えて： A.10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針
6	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。	本サービス利用に伴い、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されているか確認すること。	・「電子政府推奨暗号リスト」に記載されたアルゴリズムの採用を確認 ・「電子政府推奨暗号リスト」に記載されたアルゴリズム以外のものを採用されている場合は、「推奨候補暗号リスト」や「運用監視暗号リスト」に記載された安全性が高いアルゴリズムの採用を確認	サービス事業者は、本サービス利用に伴い暗号化又は電子署名を導入する場合、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。	要件を満たすため、以下の事項を実施することが望ましい。 ・「電子政府推奨暗号リスト」に記載されたアルゴリズムを採用することが原則する ・「電子政府推奨暗号リスト」に記載されたアルゴリズム以外のものを採用するこ場合は「推奨候補暗号リスト」や「運用監視暗号リスト」を参照の上、安全性が高いアルゴリズムを採用する	※固有の要件ですが、一般的な要件と読み換えて： A.10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針
6	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。	サービス利用者は、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の対応をサービス事業者に確認すること。	サービス事業者より通知される対策を確認し、速やかに実施すること。	サービス事業者は、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、サービス利用者へ対応を通知すること。	要件を満たすため、以下の事項を実施していることが望ましい。 ・危殆化やプロトコルに脆弱性に関する情報を速やかに入手する策を講じる ・速やかに安全なアルゴリズに移行する ・利用者に対策を通知する	A.12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理
6	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。	情報システムセキュリティ責任者は、サービス事業者より暗号鍵及び電子署名を付与する鍵が提供される場合は、管理方法を具体的に定めること。	要件を満たすため、以下の事項を実施することが望ましい。 ・情報システムセキュリティ管理者は暗号鍵のライフサイクル（生成、配送、保管、利用、期限切れ、更新、廃棄）を考慮した管理手順を策定 ・情報システムセキュリティ責任者は、定期的（例：1回/年）に暗号鍵を確認し、不要アクセスの有無を確認	サービス事業者は、暗号鍵及び電子署名を付与する鍵を利用者に提供する場合は、管理手順を定め利用者に提示すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・サービス事業者は、鍵のライフサイクル（生成、配送、保管、利用、期限切れ、更新、廃棄）を考慮した管理手順を策定する ・サービス事業者は、定期的（例：1回/年）に暗号鍵を確認し、不要アクセスの有無を確認する	A.10.1.2 鍵管理	10.1.2 鍵管理	10.1.2 鍵管理	追加要求事項なし
6	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。	本サービスに該当しない。		本サービスに該当しない。		※固有の要件ですが、一般的な要件と読み換えて： A.10.1.1 暗号による管理策の利用方針 A.10.1.2 鍵管理	10.1.1 暗号による管理策の利用方針 10.1.2 鍵管理	10.1.1 暗号による管理策の利用方針 10.1.2 鍵管理	追加要求事項なし
6	6.1	6.1.5	(2)	暗号化・電子署名に係る管理									
6	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。					A.10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針
6	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。	情報システムセキュリティ責任者は、本サービスの電子署名の正当性を検証すること。		サービス事業者は、本サービスの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。		A.10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
6	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。	サービス利用者は、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の対応をサービス事業者に確認すること。	サービス事業者より通知される対策を確認し、速やかに実施すること。	サービス事業者は、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、サービス利用者へ対応を通知すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・危殆化やプロトコルに脆弱性に関する情報を速やかに入手する策を講じる ・速やかに安全なアルゴリズに移行する ・利用者に対策を通知する	A.12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理
6	6.2	情報セキュリティの脅威への対策											
6	6.2	6.2.1	ソフトウェアに関する脆弱性対策										
6	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	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。	情報システムセキュリティ責任者は、本サービス利用に際して、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。 情報システムセキュリティ責任者は、本サービス利用に際し、当該機器上で利用するソフトウエアに関する脆弱性および影響、対策方法を入手するとともに、脆弱性を悪用する不正プログラムの流通状況を確認すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・サービス利用者が使用する端末、通信装置のOS及びアプリケーションなどの脆弱性情報を収集し、必要に応じた対策 ・サポートが終了したソフトウェアを確認し次第、利用者に対して対策を実施 ・最新のセキュリティパッチを適切に適用 ・マルウェア対策ソフトを端末にインストールし、端末を保護 ・認可されていないソフトウェアのインストールを禁止し、マルウェア感染リスクを管理 ・安全性が確認されていないWEBサイトへのアクセスを禁止	サービス事業者は、本サービスで利用するソフトウエアに関する脆弱性および影響、対策方法を入手するとともに、適宜対策を実施すること。 サービス利用者において対策を講じる必要がある場合、サービス利用者へ脆弱性および影響、対策方法を通知すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・脆弱性情報を収集し、必要に応じて対策を講じる ・サポートが終了したソフトウェアを確認し次第、利用者に対してその旨を通知する ・翻訳システムの要塞化及びマルウェア対策、ログ取得等の技術的な対策を施し、維持する ・翻訳システムの利用のセキュリティ維持するためにシステムを監視し不正アクセスを検出する ・翻訳システムに影響し得る技術的脆弱性を特定し、高リスクには時機を失せずに対応する（CVSS評価値に基づく対応等） ・技術的脆弱性への対応をスケジュール化して対応する	A.12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理
6	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。	情報システムセキュリティ責任者は、本サービス利用に際し、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。	要件を満たすため、以下の事項を実施することが望ましい。 ・マルウェア対策ソフトを端末にインストールし、端末を保護 ・認可されていないソフトウェアのインストールを禁止し、マルウェア感染リスクを管理 ・安全性が確認されていないWEBサイトへのアクセスを禁止	サービス事業者は、本サービス利用に際し、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。	同上	A.12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理
6	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。	情報システムセキュリティ責任者は、本サービス利用に際し、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。	システムセキュリティ責任者は、サービス事業者に対し、以下について定期的に確認することが望ましい。 ・端末ソフトウエアのバージョンを把握し、脆弱性の有無を確認	サービス事業者は、、本サービス利用に際し、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。	サービス事業者は、サービス利用者に対し、以下について定期的に確認し、適宜報告することが望ましい。 ソフトウエアのバージョン管理を把握し、脆弱性の有無を確認する。 定期的に脆弱性診断を実施する。	A.12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理
6	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。	情報システムセキュリティ責任者は、脆弱性対策の状況について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、サービス事業者に対応を行うように要求すること。 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、脆弱性対策計画を策定し措置を講じること。		サービス事業者は、脆弱性対策の状況について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、脆弱性対策計画を策定し措置を講じること。	本サービス利用における情報システムに対し脆弱性が判明したものについて、一時回避方法が情報システムに与える影響を考慮し必要な策を講じること。 また、脆弱性対策を実施するにあたり、実施予定時期を明確にし、本サービス利用に報告することが望ましい。	A.12.6.1 技術的ぜい弱性の管理 A.14.2.3 オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー	12.6.1 技術的ぜい弱性の管理 14.2.3 オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー	12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理
6	6.2	6.2.2	不正プログラム対策										
6	6.2	6.2.2	(1)	不正プログラム対策の実施									
6	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。	情報システムセキュリティ責任者は、利用するサービスが適切なレベルの不正プログラム対策が講じられていることを確認すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・コンピュータウイルスを含む悪意のあるソフトウェアから情報システムを保護するため、ウイルス対策プログラム等の適切な手段を利用 ・利用者に配布された端末（PC、タブレット、専用情報端末）にはウイルス対策を実施	サービス事業者は、利用するサービスが適切なレベルの不正プログラム対策が講じられていることを確かにすること。	要件を満たすため、以下の事項を実施することが望ましい。 ・コンピュータウイルスを含む悪意のあるソフトウェアから情報システムを保護するため、ウイルス対策プログラム等の適切な手段を利用する ・サービス利用者に必要な対策手段を周知、かつ適切に利用を促す ・サーバ装置にはウイルス対策を行う ・専用端末にはウイルス対策を行う	A.12.2.1 マルウェアに対する管理策	12.2.1 マルウェアに対する管理策	追加要求事項なし	追加要求事項なし
6	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。	情報システムセキュリティ責任者は、利用するサービスの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じられていることを確認すること。	同上	サービス事業者は、利用するサービスの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じられていることを確かにすること。	同上	A.12.2.1 マルウェアに対する管理策	12.2.1 マルウェアに対する管理策	追加要求事項なし	追加要求事項なし
6	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。	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。	ウィルス対策プログラムの導入状況を把握する手段を講じること。 定義ファイルの適用状況を把握する手段を講じること。 要件を満たすため、以下の事項を実施することが望ましい。 ・OSやアプリケーションに関し、セキュリティパッチ等の定義が最新化されていない端末はサービス利用させない仕組みを導入	本サービスサービス事業者は、不正プログラム対策の状況を適宜把握し、必要な対処を実施すること。	ウィルス対策プログラムの導入状況を把握する手段を講じること。 定義ファイルの適用状況を把握する手段を講じること。 以下の事項を実施していることが望ましい。 ・OSやアプリケーションに関し、セキュリティパッチ等の定義が最新化されていない端末はサービス利用させない仕組みを導入する	A.12.2.1 マルウェアに対する管理策	12.2.1 マルウェアに対する管理策	追加要求事項なし	追加要求事項なし

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
6	6.2	6.2.3	サービス不能攻撃対策										
6	6.2	6.2.3	(1)	サービス不能攻撃対策の実施									
6	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。	原則、本サービスでは要安定情報を取り扱わない		原則、本サービスでは要安定情報を取り扱わない		A.13.1.1 ネットワーク管理策 A.13.1.2 ネットワークサービスのセキュリティ	13.1.1 ネットワーク管理策 13.1.2 ネットワークサービスのセキュリティ	CLD.9.5.2 仮想マシンの要塞化	CLD.9.5.1 仮想コンピューティング環境における分離 CLD.9.5.2 仮想マシンの要塞化
6	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。	原則、本サービスでは要安定情報を取り扱わない		原則、本サービスでは要安定情報を取り扱わない		A.13.1.1 ネットワーク管理策 A.13.1.2 ネットワークサービスのセキュリティ	13.1.1 ネットワーク管理策 13.1.2 ネットワークサービスのセキュリティ	CLD.9.5.2 仮想マシンの要塞化	CLD.9.5.1 仮想コンピューティング環境における分離 CLD.9.5.2 仮想マシンの要塞化
6	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。	原則、本サービスでは要安定情報を取り扱わない		原則、本サービスでは要安定情報を取り扱わない		A.13.1.1 ネットワーク管理策 A.13.1.2 ネットワークサービスのセキュリティ	13.1.1 ネットワーク管理策 13.1.2 ネットワークサービスのセキュリティ	CLD.12.4.5 クラウドサービスの監視	CLD.12.4.5 クラウドサービスの監視
6	6.2	6.2.4	標的型攻撃対策										
6	6.2	6.2.4	(1)	標的型攻撃対策の実施									
6	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。	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。	サービス利用者は、6章で規定する情報セキュリティ対策が実施されていることを、サービス事業者に確認すること。	サービス事業者は、本サービスが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）を講じること。	サービス事業者は、6章で規定する情報セキュリティ対策を講じること。	A.13.1.1 ネットワーク管理策 A.13.1.2 ネットワークサービスのセキュリティ	13.1.1 ネットワーク管理策 13.1.2 ネットワークサービスのセキュリティ	CLD.9.5.2 仮想マシンの要塞化	CLD.9.5.2 仮想マシンの要塞化
6	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。	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。	サービス利用者は、6章で規定する情報セキュリティ対策が実施されていることを、サービス事業者に確認すること。	サービス事業者は、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）を講じること。	サービス事業者は、6章で規定する情報セキュリティ対策を講じること。	A.13.1.1 ネットワーク管理策 A.13.1.2 ネットワークサービスのセキュリティ	13.1.1 ネットワーク管理策 13.1.2 ネットワークサービスのセキュリティ	CLD.9.5.2 仮想マシンの要塞化 CLD.12.4.5 クラウドサービスの監視	CLD.9.5.1 仮想コンピューティング環境における分離 CLD.9.5.2 仮想マシンの要塞化 CLD.12.4.5 クラウドサービスの監視
6	6.3	アプリケーション・コンテンツの作成・提供											
6	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	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	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。	本サービスに該当しない		本サービスに該当しない		A.14.2.1 セキュリティに配慮した開発のための方針	14.2.1 セキュリティに配慮した開発のための方針	14.2.1 セキュリティに配慮した開発のための方針	14.2.1 セキュリティに配慮した開発のための方針
6	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	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。	本サービスに該当しない		本サービスに該当しない		A.14.1.1 情報セキュリティ要求事項の分析及び仕様化	14.1.1 情報セキュリティ要求事項の分析及び仕様化	14.1.1 情報セキュリティ要求事項の分析及び仕様化	14.1.1 情報セキュリティ要求事項の分析及び仕様化
6	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。	本サービスに該当しない		本サービスに該当しない		A.14.1.1 情報セキュリティ要求事項の分析及び仕様化 A.14.2.1 セキュリティに配慮した開発のための方針 A.14.2.2 システムの変更管理手順	14.1.1 情報セキュリティ要求事項の分析及び仕様化 14.2.1 セキュリティに配慮した開発のための方針 14.2.2 システムの変更管理手順	14.1.1 情報セキュリティ要求事項の分析及び仕様化 14.2.1 セキュリティに配慮した開発のための方針	14.1.1 情報セキュリティ要求事項の分析及び仕様化 14.2.1 セキュリティに配慮した開発のための方針
6	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。	本サービスに該当しない		本サービスに該当しない		A.14.2.2 システムの変更管理手順	14.2.2 システムの変更管理手順	追加要求事項なし	追加要求事項なし
6	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。	本サービスに該当しない		本サービスに該当しない		A.12.5.1 運用システムに関わるソフトウェアの導入 ※この要件に符合する規格要件は見つけられませんでしたが、文脈から判断しました。	12.5.1 運用システムに関わるソフトウェアの導入	追加要求事項なし	追加要求事項なし
6	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。	本サービスに該当しない		本サービスに該当しない		A.12.5.1 運用システムに関わるソフトウェアの導入 ※この要件に符合する規格要件は見つけられませんでしたが、文脈から判断しました。	12.5.1 運用システムに関わるソフトウェアの導入	追加要求事項なし	追加要求事項なし

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
6	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。	本サービスに該当しない		本サービスに該当しない		A.12.5.1 運用システムに関わるソフトウェアの導入 ※この要件に符合する規格要件は見つけられませんでしたが、文脈から判断しました。	12.5.1 運用システムに関わるソフトウェアの導入	追加要求事項なし	追加要求事項なし
6	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。	本サービスに該当しない		本サービスに該当しない		A.14.2.5 セキュリティに配慮したシステム構築の原則 ※この要件に符合する規格要件は見つけられませんでしたが、文脈から判断しました。	14.2.5 セキュリティに配慮したシステム構築の原則	追加要求事項なし	追加要求事項なし
6	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。	本サービスに該当しない		本サービスに該当しない		A.14.2.7 外部委託による開発	14.2.7 外部委託による開発	追加要求事項なし	追加要求事項なし
6	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	6.3	6.3.2	(1)	政府ドメイン名の使用									
6	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。	本サービスに該当しない		本サービスに該当しない		A.14.1.2 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 ※ドメイン名に関する固有の要件はありませんが、文脈から判断しました。	14.1.2 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	追加要求事項なし	追加要求事項なし
6	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。	本サービスに該当しない		本サービスに該当しない		A.14.1.2 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 ※ドメイン名に関する固有の要件はありませんが、文脈から判断しました。	14.1.2 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	追加要求事項なし	追加要求事項なし
6	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。	本サービスに該当しない		本サービスに該当しない		A.14.1.2 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 ※ドメイン名に関する固有の要件はありませんが、文脈から判断しました。	14.1.2 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	追加要求事項なし	追加要求事項なし
6	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	本サービスに該当しない		本サービスに該当しない		A.14.1.2 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 ※ドメイン名に関する固有の要件はありませんが、文脈から判断しました。	14.1.2 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	追加要求事項なし	追加要求事項なし
6	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。	本サービスに該当しない		本サービスに該当しない		A.14.1.2 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 ※ドメイン名に関する固有の要件はありませんが、文脈から判断しました。	14.1.2 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	追加要求事項なし	追加要求事項なし
6	6.3	6.3.2	(2)	不正なウェブサイトへの誘導防止									
6	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。	本サービスに該当しない		本サービスに該当しない		A.14.1.2 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	14.1.2 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	追加要求事項なし	追加要求事項なし
6	6.3	6.3.2	(3)	アプリケーション・コンテンツの告知									
6	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。	本サービスに該当しない		本サービスに該当しない		A.14.1.2 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	14.1.2 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	追加要求事項なし	追加要求事項なし
6	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。	本サービスに該当しない		本サービスに該当しない		A.14.1.2 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	14.1.2 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	追加要求事項なし	追加要求事項なし

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合 ①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017 利用者（政府機関）	③ISO/IEC27017 事業者
7	情報システムの構成要素												
7	7.1	端末・サーバ装置等											
7	7.1	7.1.1	端末										
7	7.1	7.1.1	(1)	端末の導入時の対策									
7	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。	サービス利用者の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利用者端末（PC、タブレット、専用情報端末）について、利用者端末の盗難、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。	要件を満たすため、以下の事項を実施することが望ましい。 ・サービス利用者は、利用者端末（PC、タブレット、専用情報端末）を利用しない時（帰宅時等）はロッカー、キャビネット等へ施錠保管、またはセキュリティワイヤーで固定 ・利用者端末（PC、タブレット、専用情報端末）の盗み身を防止するために、スクリーンロック設定やのぞき見防止フィルタを取り付け	サービス事業者は、専用端末を提供する場合、専用端末の盗難、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機能を提供すること。 サービス事業者は、市販品を利用する端末として提供する場合、専用端末と同水準の機能を具備しているかを確認すること。	要件を満たすため、以下の要件を満たす機能を備えることが望ましい。 ・端末ロック機能	A.11.2.1 装置の設置及び保護	11.2.1 装置の設置及び保護	追加要求事項なし	追加要求事項なし
7	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。	サービス利用者の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、本サービスで使用する利用者端末（PC、タブレット、専用情報端末）について、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。	要件を満たすため、以下の事項を実施することが望ましい。 ・サービス利用者の情報システムセキュリティ責任者は、本サービスで提供されるソフトウェアのみ利用許諾 ・サービス利用者の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のリストを作成 ・サービス利用者は、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のリストに基づいてソフトウェアを利用	サービス事業者は、専用端末を提供する場合、ソフトウェアの導入を抑止する機能を提供することが望ましい。 また、サービス事業者は、市販品を利用する端末として提供する場合、専用端末と同水準の機能を具備しているかを確認する。	専用端末は、以下の要件を満たす機能を備えることが望ましい。 ・ソフトウェアの導入を禁止する。 ・本サービスで提供される機能以外は使用できない。 （WEBブラウジングができないなど）	A.12.6.2 ソフトウェアのインストールの制限	12.6.2 ソフトウェアのインストールの制限	追加要求事項なし	追加要求事項なし
7	7.1	7.1.1	(2)	端末の運用時の対策									
7	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。	サービス利用者の情報システムセキュリティ責任者は、本サービス利用に関して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すこと。	要件を満たすため、以下の事項を実施すること。 ・情報システムセキュリティ責任者は、定期的に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リストの見直し ・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に脆弱性が発見された場合は、速やかに利用を禁止	本サービスに該当しない		A.12.6.2 ソフトウェアのインストールの制限 A.18.2.3 技術的順守のレビュー	12.6.2 ソフトウェアのインストールの制限 18.2.3 技術的順守のレビュー	追加要求事項なし	追加要求事項なし
7	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。	サービス利用者の情報システムセキュリティ責任者は、本サービス利用に関して所管する範囲の用者端末（PC、タブレット、専用情報端末）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利用者端末（PC、タブレット、専用情報端末）を検出等した場合には、改善を図ること。	要件を満たすため、以下の事項を実施すること。 ・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について、脆弱性などの情報を定期的に収集し、脆弱性が発見された場合は、直ちに利用を禁止する又は脆弱性が解消されたバージョンにアップデート	サービス事業者は、専用端末を提供する場合、専用端末に導入されているソフトウェアについて脆弱性などの情報を収集し、脆弱性が発見された場合に、対策を講じること。 サービス事業者は、市販品を利用する端末として提供する場合、専用端末と同水準の機能を具備しているかを確認すること。	専用端末は、以下の要件を満たす機能を備えることが望ましい。 ・サービス利用者に脆弱性対策の情報を通知する ・脆弱性に対応するためのセキュリてパッチを提供する ・脆弱性に対応したソフトウェアのバージョンアップ版を提供する	A.18.2.3 技術的順守のレビュー	18.2.3 技術的順守のレビュー	追加要求事項なし	追加要求事項なし
7	7.1	7.1.1	(3)	端末の運用終了時の対策									
7	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。	サービス利用者の情報システムセキュリティ責任者は、本サービス利用で使用した利用者端末（PC、タブレット、専用情報端末）の運用を終了する際に、利用者端末（PC、タブレット、専用情報端末）の電磁的記録媒体の全ての情報を抹消すること。	要件を満たすため、以下の事項を実施すること。 ・再利用しない場合、端末の電磁記録媒体を破壊するなどデータを抹消したうえで処分 ・再利用する場合、端末初期化などにより論理削除	サービス事業者は、専用端末を提供する場合、端末の情報を削除する機能を提供すること。 また、サービス事業者は、市販品を利用する端末として提供する場合、専用端末と同水準の機能を具備しているかを確認すること。	専用端末は、以下の要件を満たす機能を備えることが望ましい。 ・端末内情報の一括削除	A.8.3.2 媒体の処分 A.11.2.7 装置のセキュリティを保った処分又は再利用	8.3.2 媒体の処分 11.2.7 装置のセキュリティを保った処分又は再利用	CLD.8.1.6 クラウドサービスカスタマの資産の除去	CLD.8.1.6 クラウドサービスカスタマの資産の除去
7	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	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	サービス利用者の統括情報セキュリティ責任者は、本サービス利用で使用する要機密情報を取り扱う機関等が支給する利用者端末（PC、タブレット、専用情報端末）（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利用者端末（PC、タブレット、専用情報端末）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。		サービス事業者が専用端末を提供する場合、以下の安全管理措置に関する規定を整備すること。 サービス事業者は、市販品を利用する端末として提供する場合、安全管理措置に係る機能を確認し、必要に応じて規定を整備すること。		A.11.2.6 構外にある装置及び資産のセキュリティ	11.2.6 構外にある装置及び資産のセキュリティ	追加要求事項なし	追加要求事項なし
7	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	(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	下記の措置について規定することが望ましい。 ・端末の電磁記録装置を暗号化 ・ウィルス対策ソフトウェアの導入 ・最新のセキュリティパッチを適用 ・端末利用時に主体認証を実施	サービス事業者は、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を講じること。	専用端末は、以下の要件を満たす機能を備えることが望ましい。 ・外部からのソフトウェアやデータの持ち込みを制限するためのウイルス対策やウィルス対策ソフトウェアを導入 ・導入ソフウェアを最新化し既知の脆弱性から保護 ・電磁記録装置を暗号化 ・セキュリティパッチを提供 ・主体認証による端末ロック機能を提供 ・リモートで端末のデータを削除する機能を提供	A.11.2.1 装置の設置及び保護 A.11.2.6 構外にある装置及び資産のセキュリティ A.12.2.1 マルウェアに対する管理策	11.2.1 装置の設置及び保護 11.2.6 構外にある装置及び資産のセキュリティ 12.2.1 マルウェアに対する管理策	追加要求事項なし	追加要求事項なし
7	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	(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	下記の措置について規定することが望ましい。 ・端末の電磁記録装置の暗号化 ・ウィルス対策ソフトウェアの導入 ・最新のセキュリティパッチを適用 ・端末利用時に主体認証を実施 ・利用を禁止されたソフトウェアの削除 ・許可されないネットワークへのアクセスを遮断	本サービスに該当しない		A.12.2.1 マルウェアに対する管理策 A.12.6.1 技術的ぜい弱性の管理	12.2.1 マルウェアに対する管理策 12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理
7	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	サービス利用者の情報セキュリティ責任者は、本サービス利用に関して機関等支給以外の利用者端末（PC、タブレット、専用情報端末）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。		本サービスに該当しない		A.6.1.1 責任及び手順 A.8.1.2 資産の管理責任	6.1.1 責任及び手順 8.1.2 資産の管理責任	8.1.2 資産の管理責任	8.1.2 資産の管理責任

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
7	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。	次の各号に掲げるサービス利用者の責任者は、本サービス利用で使用するサービス利用者が当該各号に定める利用者端末（PC、タブレット、専用情報端末）を用いて、要機密情報を取り扱う場合は、当該利用者端末（PC、タブレット、専用情報端末）について(a)(ア)の安全管理措置を講ずること。		本サービスに該当しない		A.6.1.1 責任及び手順 A.8.1.2 資産の管理責任	6.1.1 責任及び手順 8.1.2 資産の管理責任	8.1.2 資産の管理責任	8.1.2 資産の管理責任
7	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）	(ア) 情報システムセキュリティ責任者 機関等が支給する利用者端末（PC、タブレット、専用情報端末）（要管理対策区域外で使用する場合に限る）		本サービスに該当しない		A.6.1.1 責任及び手順 A.8.1.2 資産の管理責任	6.1.1 責任及び手順 8.1.2 資産の管理責任	8.1.2 資産の管理責任	8.1.2 資産の管理責任
7	7.1	7.1.1	(4)	(c)	(イ) 端末管理責任者 機関等支給以外の利用者端末	(イ) 端末管理責任者 機関等支給以外の利用者端末（PC、タブレット、専用情報端末）		本サービスに該当しない		A.6.1.1 責任及び手順 A.8.1.2 資産の管理責任	6.1.1 責任及び手順 8.1.2 資産の管理責任	8.1.2 資産の管理責任	8.1.2 資産の管理責任
7	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	端末管理責任者は、本サービス利用で使用する要機密情報を取り扱う機関等支給以外の利用者端末（PC、タブレット、専用情報端末）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サービス利用者に講ずること。		本サービスに該当しない		A.6.1.1 責任及び手順 A.8.1.2 資産の管理責任	6.1.1 責任及び手順 8.1.2 資産の管理責任	8.1.2 資産の管理責任	8.1.2 資産の管理責任
7	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	サービス利用者は、本サービス利用で使用する要機密情報を取り扱う機関等支給以外の利用者端末（PC、タブレット、専用情報端末）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利用者端末（PC、タブレット、専用情報端末）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。		本サービスに該当しない		A.6.1.1 責任及び手順 A.8.1.2 資産の管理責任	6.1.1 責任及び手順 8.1.2 資産の管理責任	8.1.2 資産の管理責任	8.1.2 資産の管理責任
7	7.1	7.1.2	サーバ装置										
7	7.1	7.1.2	(1)	サーバ装置の導入時の対策									
7	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。	本サービスに該当しない。		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。	サービス事業者は、本サービスでIaaSを利用する場合、IaaS事業者の対策を確認すること。	A.11.2.1 装置の設置及び保護	11.2.1 装置の設置及び保護	追加要求事項なし	追加要求事項なし
7	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。	サービス利用者は、本サービスの可用性が確保されていることをサービス事業者に確認すること。		サービス事業者は、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、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。 確保した可用性の度合いをサービス利用者に提示すること。	サーバ装置は、要件を満たすため、以下の機能を備えることが望ましい。 ・同一システムを２系統で構成する ・系統毎に遠隔地で配置する ・負荷分散装置等を用いてラウンドロビン等によるアルゴリズで負荷分散する ・コールドスタンバイ方式など障害時に代替システムへ迅速な切替を行う	A.17.2.1 情報処理施設の可用性	17.2.1 情報処理施設の可用性	追加要求事項なし	追加要求事項なし
7	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。	本サービスに該当しない。		サービス事業者は、サーバ装置に本サービスを提供するのに必要なソフトウェアのみ導入すること。 削除が困難である不要なソフトウェアは停止すること。 サービス事業者は、サーバ装置に導入しているソフトウェア及びそのバージョン等の情報を管理すること。		A.12.6.2 ソフトウェアのインストールの制限	12.6.2 ソフトウェアのインストールの制限	追加要求事項なし	追加要求事項なし
7	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。	本サービスに該当しない。		サービス事業者は、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。	要件を満たすため、以下のような対策が実施すること。 ・IPアドレスによるアクセス元を制限する ・暗号化通信を使用する	A.11.2.4 装置の保守 A.13.1.1 ネットワーク管理策	11.2.4 装置の保守 13.1.1 ネットワーク管理策	追加要求事項なし	追加要求事項なし
7	7.1	7.1.2	(2)	サーバ装置の運用時の対策									
7	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。	本サービスに該当しない。		サービス事業者は、サーバ装置に導入しているソフトウェア及びそのバージョン等を定期的に見直すこと。		A.12.6.2 ソフトウェアのインストールの制限 A.18.2.3 技術的順守のレビュー	12.6.2 ソフトウェアのインストールの制限 18.2.3 技術的順守のレビュー	追加要求事項なし	追加要求事項なし
7	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。	本サービスに該当しない。		サービス事業者は、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。	要件を満たすため、以下の事項を実施すること。 ・定期的な内部監査によるサーバ装置の構成やソフトウェアの導入状況を確認する ・脆弱性が発見されたソフトウェアを導入していた場合は、速やかに対策を実施する	A.12.6.1 技術的ぜい弱性の管理 A.18.2.3 技術的順守のレビュー	12.6.1 技術的ぜい弱性の管理 18.2.3 技術的順守のレビュー	12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理
7	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。	本サービスに該当しない。		サービス事業者は、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ために、当該サーバ装置を監視するための措置を講ずること。	要件を満たすため、以下の事項を実施すること。 ・IDS／IPS、ウィルス対策ソフトウェアを導入する ・システム操作で使用するアカウントは主体認証を確実にし、認証情報が漏洩しないように運用規定を策定する ・システム運用保守における操作ログを定期的に点検又は分析する ・操作ログは変更及び削除から適切に保護され、特権を行使するシステム管理者等がログを変更できないように講じる ・システム操作の承認、作業記録を残す	A.12.6.1 技術的ぜい弱性の管理 A.18.2.3 技術的順守のレビュー	12.6.1 技術的ぜい弱性の管理 18.2.3 技術的順守のレビュー	12.6.1 技術的ぜい弱性の管理	12.6.1 技術的ぜい弱性の管理

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
7	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。	本サービスに該当しない。		サービス事業者は、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。	要件を満たすため、サーバ装置は、以下のような対策を実施すること。 ・本サービスの運用に必要な情報の定期的なバックアップを行う ・本サービスの提供に必要なソフトウェア及びそのソースコードは別に管理し保管する ・本サービスの復元に必要な手順を事前に用意する	A.12.1.1 操作手順書 A.12.3.1 情報のバックアップ	12.1.1 操作手順書 12.3.1 情報のバックアップ	12.3.1 情報のバックアップ	12.3.1 情報のバックアップ
7	7.1	7.1.2	(3)	サーバ装置の運用終了時の対策									
7	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。	本サービスに該当しない。		サービス事業者は、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。	サービス事業者は、本サービスでIaaSを利用する場合、IaaS事業者の対策を確認する。	A.8.3.2 媒体の処分 A.11.2.7 装置のセキュリティを保った処分又は再利用	8.3.2 媒体の処分 11.2.7 装置のセキュリティを保った処分又は再利用	11.2.7 装置のセキュリティを保った処分又は再利用	11.2.7 装置のセキュリティを保った処分又は再利用
7	7.1	7.1.3	複合機・特定用途機器										
7	7.1	7.1.3	(1)	複合機						※複合機に特化した要件はありませんが、11.2 装置等の管理策を適用することになります。			
7	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。	本サービスに該当しない。		本サービスに該当しない。		※複合機に特化した要件はありませんが、11.2 装置等の管理策を適用することになります。			
7	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。	本サービスに該当しない。		本サービスに該当しない。		A.15.1.3 ICTサプライチェーン	15.1.3 ICTサプライチェーン	追加要求事項なし	追加要求事項なし
7	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。	本サービスに該当しない。		本サービスに該当しない。		A.8.3.2 媒体の処分 A.11.2.7 装置のセキュリティを保った処分又は再利用	8.3.2 媒体の処分 11.2.7 装置のセキュリティを保った処分又は再利用	追加要求事項なし	追加要求事項なし
7	7.1	7.1.3	(2)	IoT 機器を含む特定用途機器									
7	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。	本サービスに該当しない。		本サービスに該当しない。		A.15.1.3 ICTサプライチェーン	15.1.3 ICTサプライチェーン	追加要求事項なし	追加要求事項なし
7	7.2	電子メール・ウェブ等											
7	7.2	7.2.1	電子メール										
7	7.2	7.2.1	(1)	電子メールの導入時の対策									
7	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。	本サービスに該当しない。		本サービスに該当しない。		A.13.1.1 ネットワーク管理策 A.13.2.3 電子的メッセージ通信	13.1.1 ネットワーク管理策 13.2.3 電子的メッセージ通信	追加要求事項なし	追加要求事項なし
7	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。	本サービスに該当しない。		本サービスに該当しない。		A.9.4.2 セキュリティに配慮したログオン手順 A.13.2.3 電子的メッセージ通信	9.4.2 セキュリティに配慮したログオン手順 13.2.3 電子的メッセージ通信	追加要求事項なし	追加要求事項なし
7	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。	本サービスに該当しない。		本サービスに該当しない。		A.9.4.2 セキュリティに配慮したログオン手順 A.13.2.3 電子的メッセージ通信	9.4.2 セキュリティに配慮したログオン手順 13.2.3 電子的メッセージ通信	追加要求事項なし	追加要求事項なし
7	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。	本サービスに該当しない。		本サービスに該当しない。		A.13.2.1 情報転送の方針及び手順 A.13.2.3 電子的メッセージ通信	13.2.1 情報転送の方針及び手順 13.2.3 電子的メッセージ通信	追加要求事項なし	追加要求事項なし
7	7.2	7.2.2	ウェブ										
7	7.2	7.2.2	(1)	ウェブサーバの導入・運用時の対策									
7	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。	本サービスに該当しない。		サービス事業者は、本サービス利用に関する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。		A.14.1.2 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	14.1.2 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	追加要求事項なし	追加要求事項なし
7	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。	本サービスに該当しない。		(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	要件を満たすため、以下の事項を実施すること。 ・ウェブサーバを構築した際に不要な機能が動作しないように設定する。 ・ウェブサーバ上のソフトウエアは既知の脆弱性から保護されたバージョンを使用する ・ウェブサーバのコンテンツ構成やソフトウェアバージョンなどの情報を外部から取得できないようにする	A.14.1.2 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	14.1.2 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	CLD.9.5.2 仮想マシンの要塞化	CLD.9.5.2 仮想マシンの要塞化
7	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。	本サービスに該当しない。		(イ) ウェブコンテンツの編集作業を担当する主体を限定	要件を満たすため、以下のような事項を実施すること。 ・ウェブアプリケーション開発におけるコードレビューや試験によって品質を確実にする ・権限のないものがソフトウェアの改変できないようにウェブアプリケーションソフトウェアのソースコードを管理する 例) ソースコードの修正者と承認者を分ける	A.14.2.2 システムの変更管理手順 ※ウェブコンテンツに特化した要件はありませんので、14.2.2を適用しました。	14.2.2 システムの変更管理手順	追加要求事項なし	追加要求事項なし

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
7	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。	本サービスに該当しない。		(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	要件を満たすため、以下の事項を実施すること。 ・ウェブサーバ標準で用意されているコンテンツやテストコンテンツが表示されないように設定する	A.14.2.2 システムの変更管理手順 ※ウェブコンテンツに特化した要件はありませんので、14.2.2を適用しました。	14.2.2 システムの変更管理手順	追加要求事項なし	追加要求事項なし
7	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。	本サービスに該当しない。		(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	要件を満たすため、以下の事項を実施すること。 ・本サービスウェブアプリケーションを更新する端末または主体を限定する	A.9.4.2 セキュリティに配慮したログオン手順	9.4.2 セキュリティに配慮したログオン手順	追加要求事項なし	追加要求事項なし
7	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。	本サービスに該当しない。		(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	要件を満たすため、以下の事項を実施すること。 ・Web上で通信するアプリケーションを構築する場合は、HTTPSによる通信を行う	A.14.1.2 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	14.1.2 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	追加要求事項なし	追加要求事項なし
7	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。	本サービスに該当しない。		サービス事業者の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。		A.14.2.2 システムの変更管理手順 ※ウェブコンテンツに特化した要件はありませんので、14.2.2を適用しました。	14.2.2 システムの変更管理手順	追加要求事項なし	追加要求事項なし
7	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	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。	本サービスに該当しない。		サービス事業者の情報システムセキュリティ責任者は、本サービス利用に関する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じること。 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すること。	要件を満たすため、以下の事項を実施すること。 ・システム開発時にコーディングのレビューを行い不正プログラムが行われていないことを確実にする ・WEBアプリケーションに対する脆弱性試験を定期的に実施する ・脆弱性が検知された場合にはWEBアプリケーションを、速やかに対策を講じる	A.14.2.5 セキュリティに配慮したシステム構築の原則	14.2.1 セキュリティに配慮した開発のための方針 14.2.5 セキュリティに配慮したシステム構築の原則	14.2.1 セキュリティに配慮した開発のための方針	14.2.1 セキュリティに配慮した開発のための方針
7	7.2	7.2.3	ドメインネームシステム（DNS）										
7	7.2	7.2.3	(1)	DNS の導入時の対策									
7	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。	本サービスでは、原則、要安定情報を扱わないため、サービス利用者は、本サービスの可用性が確保されていることをサービス事業者に確認すること。		サービス事業者は、本サービスで使用するドメインの名前解決を提供するコンテンツサーバの可用性について対策を講じることが望ましい。		A.17.2.1 情報処理施設の可用性	17.2.1 情報処理施設の可用性	追加要求事項なし	追加要求事項なし
7	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。	情報システムセキュリティ責任者は、名前解決の要求への適切な応答をするための措置が取られているか確認すること。	以下の対策を実施されているか確認することが望ましい。 ・DNSキャッシュポイズニング攻撃からの保護	サービス事業者は、本サービスの名前解決にキャッシュサーバを利用している場合、名前解決の要求への適切な応答をするための措置を講じること。 また、キャッシュサーバと同等の機能を有する名前解決のサービスを利用している場合、利用しているサービスが名前解決の要求への適切な応答をするための措置を講じていることを確認すること。	以下の対策を実施することが望ましい。 ・DNSキャッシュポイズニング攻撃からの保護	A.13.1.1 ネットワーク管理策	13.1.1 ネットワーク管理策	追加要求事項なし	追加要求事項なし
7	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。	本サービスに該当しない。（本サービスは、クラウドサービス提供が前提であり、機関等に閉じた利用は想定していない）		機関等を本サービス提供環境に置き換える場合の記載。 本サービス提供環境内でのみ使用する名前解決を用いる場合は、当該コンテンツサーバで管理する情報が外部に漏洩しないための措置を講じること。		A.13.1.1 ネットワーク管理策	13.1.1 ネットワーク管理策	追加要求事項なし	CLD.9.5.1 仮想コンピューティング環境における分離
7	7.2	7.2.3	(2)	DNS の運用時の対策									
7	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。	情報システムセキュリティ責任者は、本サービスのドメインに関する情報について整合性が維持されていることを確認すること。		サービス事業者は、本サービス利用に関するコンテンツサーバを複数台設置する場合、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。		A.17.2.1 情報処理施設の可用性	17.2.1 情報処理施設の可用性	追加要求事項なし	追加要求事項なし
7	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。	情報システムセキュリティ責任者は、本サービスのドメインに関する情報について情報が正確であることを定期的に確認すること。		サービス事業者は、サービス利用者に対し、本サービス利用においてコンテンツサーバについて管理するドメイン情報を確認し、定期的に報告することが望ましい。		A.13.1.1 ネットワーク管理策	13.1.1 ネットワーク管理策	追加要求事項なし	追加要求事項なし
7	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。	情報システムセキュリティ責任者は、本サービスのドメインに関する情報につ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が講じられていることを確認すること。		サービス事業者は、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。		A.13.1.1 ネットワーク管理策	13.1.1 ネットワーク管理策	追加要求事項なし	追加要求事項なし
7	7.2	7.2.4	データベース										
7	7.2	7.2.4	(1)	データベースの導入・運用時の対策									
7	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。	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が行われていることを確認すること。	要件を満たすため、以下の事項が実施されていることが望ましい。 ・使用者ごとに一意のアカウントを付与 ・データベース管理者とシステム管理者のアカウント分離 ・使用者への管理者アカウント発行および承認フローの整備	サービス事業者は、本サービス利用に関する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。	要件を満たすため、以下の事項を実施していることが望ましい。 ・使用者ごとに一意のアカウントを付与 ・データベース管理者とシステム管理者のアカウント分離 ・使用者への管理者アカウント発行および承認フローの整備	A.9.2.3 特権的アクセス権の管理 A.9.4.4 特権的なユーティリティプログラムの使用	9.2.3 特権的アクセス権の管理 9.4.4 特権的なユーティリティプログラムの使用	9.2.3 特権的アクセス権の管理 9.4.4 特権的なユーティリティプログラムの使用	9.2.3 特権的アクセス権の管理 9.4.4 特権的なユーティリティプログラムの使用

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
7	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。	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アカウントを特定できるよう、措置が講じられていることを確認すること。	要件を満たすため、以下の事項が実施されていることが望ましい。 ・データ取得のログの記録	サービス事業者は、データベースに格納されているデータにアクセスしたアカウントを特定できるよう、措置を講ずること。	要件を満たすため、以下の事項を実施していることが望ましい。 ・データ取得のログの記録	A.9.2.3 特権的アクセス権の管理 A.9.4.2 セキュリティに配慮したログオン手順 A.9.4.4 特権的なユーティリティプログラムの使用 A.12.4.1 イベントログ取得	9.2.3 特権的アクセス権の管理 9.4.2 セキュリティに配慮したログオン手順 9.4.4 特権的なユーティリティプログラムの使用 12.4.1 イベントログ取得	9.2.3 特権的アクセス権の管理 9.4.4 特権的なユーティリティプログラムの使用 12.4.1 イベントログ取得	9.2.3 特権的アクセス権の管理 9.4.4 特権的なユーティリティプログラムの使用 12.4.1 イベントログ取得
7	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。	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、対策が講じられていることを確認すること。	要件を満たすため、以下の事項が実施されていることが望ましい。 ・ログの定期的な監査 ・データ取得の監視	サービス事業者は、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。	要件を満たすため、以下の事項を実施していることが望ましい。 ・ログの定期的な監査 ・データ取得の監視	A.9.2.3 特権的アクセス権の管理 A.9.4.2 セキュリティに配慮したログオン手順 A.12.4.1 イベントログ取得	9.2.3 特権的アクセス権の管理 9.4.2 セキュリティに配慮したログオン手順 12.4.1 イベントログ取得	9.2.3 特権的アクセス権の管理 9.4.2 セキュリティに配慮したログオン手順 12.4.1 イベントログ取得	9.2.3 特権的アクセス権の管理 9.4.2 セキュリティに配慮したログオン手順 12.4.1 イベントログ取得
7	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。	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が講じられていることを確認すること。	要件を満たすため、以下の事項が実施されていることが望ましい。 ・SQLインジェクションに対する脆弱性対応 ・ウェブアプリケーションファイアウォールの導入 ・データベースファイアウォールの導入	サービス事業者は、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。	要件を満たすため、以下の事項を実施していることが望ましい。 ・SQLインジェクションに対する脆弱性対応 ・ウェブアプリケーションファイアウォールの導入 ・データベースファイアウォールの導入	A.9.2.3 特権的アクセス権の管理 A.9.4.4 特権的なユーティリティプログラムの使用	9.2.3 特権的アクセス権の管理 9.4.4 特権的なユーティリティプログラムの使用	9.2.3 特権的アクセス権の管理 9.4.4 特権的なユーティリティプログラムの使用	9.2.3 特権的アクセス権の管理 9.4.4 特権的なユーティリティプログラムの使用
7	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。	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、適切に暗号化されていることを確認すること。	要件を満たすため、以下の事項に対して暗号化されていることが望ましい。 ・辞書や翻訳メモリなどのサービス利用者が登録したデータ	サービス事業者は、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。	要件を満たすため、以下の事項に対して暗号化を実施していることが望ましい。 ・辞書や翻訳メモリなどのサービス利用者が登録したデータ	A.10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針
7	7.3	通信回線											
7	7.3	7.3.1	通信回線										
7	7.3	7.3.1	(1)	通信回線の導入時の対策									
7	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。	情報システムセキュリティ責任者は、本サービス利用に関する通信回線構築時に、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。	要件を満たすため、以下の事項を実施することが望ましい。 ・業務に必要な通信速度を確保した通信回線（専用線、VPN）の採用 ・業務に必要な通信プロトコルに対応した通信回線の採用	サービス事業者は、サービス利用者が指定する通信回線で接続できること。 サービス利用者が要件に応じて通信回線を選択できるようにすること。	本サービスを利用できるよう、専用線・VPNなどで対応することが望ましい。	A.13.1.1 ネットワーク管理策 A.13.1.2 ネットワークサービスのセキュリティ	13.1.1 ネットワーク管理策 13.1.2 ネットワークサービスのセキュリティ	追加要求事項なし	追加要求事項なし
7	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。	情報システムセキュリティ責任者は、本サービス利用に関する通信回線において、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。	要件を満たすため、以下の事項を実施することが望ましい。 ・IPアドレスを制限 ・MACアドレスを制限	サービス事業者は、端末のアクセス制御を行う機能を提供すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・IPアドレスを制限 ・端末ID等で制限	A.13.1.1 ネットワーク管理策 A.13.1.2 ネットワークサービスのセキュリティ	13.1.1 ネットワーク管理策 13.1.2 ネットワークサービスのセキュリティ	追加要求事項なし	追加要求事項なし
7	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。	情報システムセキュリティ責任者は、本サービス利用に関する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。	要件を満たすため、以下の事項を実施することが望ましい。 ・通信は、SSL/TLS、IPSec等を用いた保護	サービス事業者は、VPNやHTTPSなどの暗号化通信プロトコルによるサービス提供できること。		A.10.1.1 暗号による管理策 A.13.1.1 ネットワーク管理策 A.13.1.2 ネットワークサービスのセキュリティ	10.1.1 暗号による管理策 13.1.1 ネットワーク管理策 13.1.2 ネットワークサービスのセキュリティ	10.1.1 暗号による管理策	10.1.1 暗号による管理策
7	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。	情報システムセキュリティ責任者は、本サービス利用に関するサービス利用者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の措置を講ずること。	要件を満たすため、以下の事項を実施することが望ましい。 ・MACアドレスを制限 ・接続する端末を管理簿などにより管理	本サービスに該当しない。		A.13.1.1 ネットワーク管理策 A.13.1.2 ネットワークサービスのセキュリティ	13.1.1 ネットワーク管理策 13.1.2 ネットワークサービスのセキュリティ	追加要求事項なし	追加要求事項なし
7	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。	情報システムセキュリティ責任者は、サービス事業者に対し、本サービスの設置環境を管理している場合、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されていることを確認すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・本サービスにおける設置環境の管理について、サービス事業者が外部の事業者（IaaS)を採用している場合、別途、管理運用規定に即し必要な措置が講じられていることを確認する	サービス事業者は、本サービスの設置環境を管理している場合は、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。	要件を満たすため、以下の事項を実施することが望ましい。 ・本サービスにおける設置環境の管理について、サービス事業者が外部の事業者（IaaS)を採用している場合、別途、管理運用規定に即し必要な措置が講じられていることを確認する	A.11.2.1 装置の設置及び保護	11.2.1 装置の設置及び保護	追加要求事項なし	追加要求事項なし
7	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。	サービス利用者は、本サービスの可用性が確保されていることをサービス事業者に確認すること。	本サービスにおいては、原則、要安定情報を扱わないことを踏まえ、適宜サービス利用者がサービス事業者に確認することが望ましい。	本サービスに該当しない。		A.17.2.1 情報処理施設の可用性	17.2.1 情報処理施設の可用性	追加要求事項なし	追加要求事項なし

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
7	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。	情報システムセキュリティ責任者は、本サービスの設置環境において、運用・保守等によるメンテナンス作業でアクセスするための通信回線が限定されていることを確認すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・サービス利用者がアクセスする接続先と、サービス事業者がメンテナンスでアクセスする接続先とが分離されていることを確認する ・サービス事業者がメンテナンスでアクセスする回線は、サービス事業者内に閉じた回線又は、専用線であること ・インターネット回線を用いる場合、7.3.1(1)(j)の対策が実施されていることを確認する	サービス事業者は、本サービスの設置環境において運用・保守等によるメンテナンス作業でアクセスするための通信回線を限定すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・サービス利用者がアクセスする接続先と、サービス事業者がメンテナンスでアクセスする接続先を分離する ・サービス事業者がメンテナンスでアクセスする回線は、サービス事業者内に閉じた回線又は、専用線であること ・インターネット回線を利用して本サービスの設置環境へアクセスする場合、7.3.1(1)(j)の対策を実施する	A.13.1.3 ネットワークの分離 A.13.1.1 ネットワーク管理策	13.1.3 ネットワークの分離	13.1.3 ネットワークの分離	13.1.3 ネットワークの分離
7	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。	情報システムセキュリティ責任者は、サービス事業者が本サービスの設置環境へ運用・保守などによるメンテナンス作業でアクセスするための通信回線について、事業者回線と本サービス設置環境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じていることを確認すること。	暗号化通信を行っている場合は、通信回線で送受信されるデータの監視だけでは不十分であるため、以下の事項が実施されていることが望ましい。 ・本サービス設置環境の操作ログの記録 ・本サービス設置環境での作業内容の記録	サービス事業者は、本サービスの設置環境へ運用・保守などによるメンテナンス作業でアクセスするための通信回線について、事業者回線と本サービス設置環境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。	暗号化通信を行っている場合は、通信回線で送受信されるデータの監視だけでは不十分であるため、以下の事項を実施することが望ましい。 ・本サービス設置環境の操作ログの記録 ・本サービス設置環境での作業内容の記録	A.13.1.1 ネットワーク管理策	13.1.1 ネットワーク管理策	追加要求事項なし	追加要求事項なし
7	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。	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が整備されていることを確認すること。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を利用している場合は、この限りでない。	要件を満たすため、以下の事項を実施することが望ましい。 ・本サービスにおける設置環境の管理について、サービス事業者が外部の事業者（IaaS)を採用している場合、別途、管理運用規定に即し必要な措置が講じられていることを確認する	サービス事業者は、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を利用している場合は、この限りでない。	要件を満たすため、以下の事項を実施することが望ましい。 ・本サービスにおける設置環境の管理について、サービス事業者が外部の事業者（IaaS)を採用している場合、別途、管理運用規定に即し必要な措置が講じられていることを確認する	A.12.6.2 ソフトウェアのインストールの制限	12.6.2 ソフトウェアのインストールの制限	追加要求事項なし	追加要求事項なし
7	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が確保されているか確認すること。	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が確保されていることを確認すること。	要件を満たすため、以下の事項が実施されていることが望ましい。 ・VPNやSSHなど暗号化通信の利用 ・IPアドレス制限などによる接続元の限定 ・踏み台サーバなどを経由した設置環境への接続 ・踏み台サーバへのファイアウォールやウィルス対策ソフトウェア、IDS/IPSの導入	サービス事業者は、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。	要件を満たすため、以下の事項を実施していることが望ましい。 ・VPNやSSHなど暗号化通信の利用 ・IPアドレス制限などによる接続元の限定 ・踏み台サーバなどを経由した設置環境への接続 ・踏み台サーバへのファイアウォールやウィルス対策ソフトウェア、IDS/IPSの導入	A.9.1.2 ネットワーク及びネットワークサービスへのアクセス	9.1.2 ネットワーク及びネットワークサービスへのアクセス	9.1.2 ネットワーク及びネットワークサービスへのアクセス	追加要求事項なし
7	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。	本サービスに該当しない。		本サービスに該当しない。		A.15.1.3 ICTサプライチェーン	15.1.3 ICTサプライチェーン	追加要求事項なし	15.1.3 ICTサプライチェーン
7	7.3	7.3.1	(2)	通信回線の運用時の対策									
7	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。	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が講じられていることを確認すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・本サービスにおける設置環境の管理について、サービス事業者が外部の事業者（IaaS)を採用している場合、別途、管理運用規定に即し必要な措置が講じられていることを確認する。	サービス事業者が本サービスの設置環境を管理している場合、サービス事業者は、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。	要件を満たすため、以下の事項を実施することが望ましい。 ・本サービスにおける設置環境の管理について、サービス事業者が外部の事業者（IaaS)を採用している場合、別途、管理運用規定に即し必要な措置が講じられていることを確認する。	A.13.1.1 ネットワーク管理策	13.1.1 ネットワーク管理策	追加要求事項なし	追加要求事項なし
7	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。	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が行われていることを確認すること。		サービス事業者は、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。	要件を満たすため、以下の事項を実施することが望ましい。 ・各ネットワークの境界の明確化 ・ネットワーク構成情報の管理 ・ネットワーク構成情報の最新化	A.13.1.1 ネットワーク管理策	13.1.1 ネットワーク管理策	追加要求事項なし	追加要求事項なし
7	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。	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が定期的に調査され、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、改善が図られていることを確認すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・本サービスにおける設置環境の管理について、サービス事業者が外部の事業者（IaaS)を採用している場合、定期的な調査とともに、別途、管理運用規定に即し必要な措置が講じられていることを確認する	サービス事業者は、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。	要件を満たすため、以下の事項を実施することが望ましい。 ・本サービスにおける設置環境の管理について、サービス事業者が外部の事業者（IaaS)を採用している場合、定期的な調査とともに、別途、管理運用規定に即し必要な措置が講じられていることを確認する	A.12.6.2 ソフトウェアのインストールの制限	12.6.2 ソフトウェアのインストールの制限	追加要求事項なし	追加要求事項なし
7	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。	本サービスに該当しない。		サービス事業者は、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。		A.13.1.3 ネットワークの分離	13.1.3 ネットワークの分離	13.1.3 ネットワークの分離	13.1.3 ネットワークの分離

A.政府機関の情報セキュリティ対策のための統一基準						B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
										①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
												利用者（政府機関）	事業者
7	7.3	7.3.1	(3)		通信回線の運用終了時の対策								
7	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。	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が講じられているか確認すること。	要件を満たすため、以下の事項を実施することが望ましい。 ・本サービスにおける設置環境の管理について、サービス事業者が外部の事業者（IaaS)を採用している場合、別途、管理運用規定に即し必要な措置が講じられていることを確認する	サービス事業者は、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。	要件を満たすため、以下の事項を実施することが望ましい。 ・本サービスにおける設置環境の管理について、サービス事業者が外部の事業者（IaaS)を採用している場合、別途、管理運用規定に即し必要な措置が講じられていることを確認する	A.11.2.7 装置のセキュリティを保った処分又は再利用	11.2.7 装置のセキュリティを保った処分又は再利用	11.2.7 装置のセキュリティを保った処分又は再利用	11.2.7 装置のセキュリティを保った処分又は再利用
7	7.3	7.3.1	(4)		リモートアクセス環境導入時の対策								
7	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。	本サービスにおいては、リモートアクセスを前提に通信回線および情報システムの情報セキュリティを確保すること。		本サービスにおいては、リモートアクセスを前提に通信回線および情報システムの情報セキュリティを確保すること。		A.9.1.2 ネットワーク及びネットワークサービスへのアクセス	9.1.2 ネットワーク及びネットワークサービスへのアクセス	9.1.2 ネットワーク及びネットワークサービスへのアクセス	追加要求事項なし
7	7.3	7.3.1	(5)		無線LAN 環境導入時の対策								
7	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。	情報システムセキュリティ責任者は、本サービス利用に関する無線 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。	無線LANに接続して本サービスを利用する場合、以下の事項を実施することが望ましい。 ・機関等内通信回線と分離し、無線LANからインターネット回線への接続に限定する ・無線LANに接続する端末を限定する ・無線LANのセキュリティ／暗号化方式は十分に強度が方式を採用する	サービス事業者は、社内で無線LANを利用する場合、本サービスに影響を及ぼさないよう、情報セキュリティ確保のための必要な措置を講じること		A.9.1.2 ネットワーク及びネットワークサービスへのアクセス A.10.1.1 暗号による管理策の利用方針	9.1.2 ネットワーク及びネットワークサービスへのアクセス 10.1.1 暗号による管理策の利用方針	9.1.2 ネットワーク及びネットワークサービスへのアクセス 10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針
7	7.3	7.3.2			IPv6 通信回線								
7	7.3	7.3.2	(1)		IPv6 通信を行う情報システムに係る対策								
7	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。	本サービスに該当しない。		本サービスに該当しない。		※該当要件なし	※該当要件なし	※該当要件なし	※該当要件なし
7	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。	本サービスに該当しない。		本サービスに該当しない。		※該当要件なし	※該当要件なし	※該当要件なし	※該当要件なし
7	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	本サービスに該当しない。		本サービスに該当しない。		※該当要件なし	※該当要件なし	※該当要件なし	※該当要件なし
7	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	本サービスに該当しない。		本サービスに該当しない。		※該当要件なし	※該当要件なし	※該当要件なし	※該当要件なし
7	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	本サービスに該当しない。		本サービスに該当しない。		※該当要件なし	※該当要件なし	※該当要件なし	※該当要件なし
7	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	本サービスに該当しない。		本サービスに該当しない。		※該当要件なし	※該当要件なし	※該当要件なし	※該当要件なし
7	7.3	7.3.2	(2)		意図しないIPv6 通信の抑止・監視								
7	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。	本サービスに該当しない。		本サービスに該当しない。		※該当要件なし	※該当要件なし	※該当要件なし	※該当要件なし

A.政府機関の情報セキュリティ対策のための統一基準					B.多言語自動翻訳サービス利用者（要件） 政府統一基準に基づいた遵守すべき要件	B1.サービス利用者の遵守すべき 要件に対する解説	C.多言語自動翻訳サービス事業者（要件） 政府統一基準に基づいた遵守すべき要件	C1.サービス事業者の遵守すべき 要件に対する解説	D.ISO/IEC27001、27002、27017との照合			
									①ISO/IEC27001	②ISO/IEC27002	③ISO/IEC27017	
											利用者（政府機関）	事業者
8	情報システムの利用											
8	8.1	情報システムの利用										
8	8.1	1	情報システムの利用									
8	8.1	8.1.1	(1)	情報システムの利用に係る規定の整備	組織における当該規定を遵守		本サービスに該当しない。		A.14.1.1 情報セキュリティ要求事項の分析及び仕様化	14.1.1 情報セキュリティ要求事項の分析及び仕様化	14.1.1 情報セキュリティ要求事項の分析及び仕様化	14.1.1 情報セキュリティ要求事項の分析及び仕様化
8	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	同上		本サービスに該当しない。		A.7.2.2 情報セキュリティの意識向上，教育及び訓練	7.2.2 情報セキュリティの意識向上，教育及び訓練	7.2.2 情報セキュリティの意識向上，教育及び訓練	7.2.2 情報セキュリティの意識向上，教育及び訓練
8	8.1	8.1.1	(3)	情報システムの利用時の基本的対策	同上		本サービスに該当しない。		A.7.2.2 情報セキュリティの意識向上，教育及び訓練	7.2.2 情報セキュリティの意識向上，教育及び訓練	7.2.2 情報セキュリティの意識向上，教育及び訓練	7.2.2 情報セキュリティの意識向上，教育及び訓練
8	8.1	8.1.1	(4)	電子メール・ウェブの利用時の対策	同上		本サービスに該当しない。		A.7.2.2 情報セキュリティの意識向上，教育及び訓練 A.13.2.3 電子的メッセージ通信	7.2.2 情報セキュリティの意識向上，教育及び訓練 13.2.3 電子的メッセージ通信	7.2.2 情報セキュリティの意識向上，教育及び訓練	7.2.2 情報セキュリティの意識向上，教育及び訓練
8	8.1	8.1.1	(5)	識別コード・主体認証情報の取り扱い	同上		本サービスに該当しない。		A.9.3.1 秘密認証情報の利用	9.3.1 秘密認証情報の利用	追加要求事項なし	追加要求事項なし
8	8.1	8.1.1	(6)	暗号・電子署名の利用時の対策	同上		本サービスに該当しない。		A.10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針	10.1.1 暗号による管理策の利用方針
8	8.1	8.1.1	(7)	不正プログラム感染防止	同上		本サービスに該当しない。		A.12.2.1 マルウェアに対する管理策	12.2.1 マルウェアに対する管理策	追加要求事項なし	追加要求事項なし
8	8.2	機関等支給以外の端末の利用										
8	8.2	8.2.1	機関等支給以外の端末の利用									
8	8.2	8.2.1	(1)	機関等支給以外の端末の利用可否の判断	原則として本サービスでは扱わないものとし、扱う場合は別途扱いを定めること。		本サービスに該当しない。		A.11.1.5 セキュリティを保つべき領域での作業	11.1.5 セキュリティを保つべき領域での作業	追加要求事項なし	追加要求事項なし
8	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	同上		本サービスに該当しない。		A.11.1.5 セキュリティを保つべき領域での作業	11.1.5 セキュリティを保つべき領域での作業	追加要求事項なし	追加要求事項なし
8	8.2	8.2.1	(3)	機関等支給以外の端末の利用時の対策	同上		本サービスに該当しない。		A.12.2.1 マルウェアに対する管理策	12.2.1 マルウェアに対する管理策	追加要求事項なし	追加要求事項なし

政府機関等に向けた多言語自動翻訳システム利活用ガイドライン検討会
構成員

（順不同）
・NTTコミュニケーションズ株式会社
・NTT東日本株式会社
・コニカミノルタ株式会社
・凸版印刷株式会社
・株式会社バリューアップジャパン
・BSIジャパン株式会社
・フェアリーデバイセズ株式会社
・東芝デジタルソリューションズ株式会社
・株式会社みらい翻訳
・（事務局）株式会社日本総合研究所

※ 総務省（研究推進室、情報流通振興課）、NICTもオブザーバ参加