資料５－４

政府機関における自動翻訳システムの導入に向けた取組状況

令 和 ２ 年 ３ 月

総務省国際戦略局

検討の背景

＜政府機関へのクラウド型翻訳システムの本格導入に向けてさらにクリアすべき課題＞

課題① 適切なプライバシー・セキュリティの確保

・行政機関の窓口業務等において必要と想定される「プライバシー保護」、「セキュリティ」の確保（クラウドが満たすべき技術的保護要件等の整理）

課題② クラウド導入についての検討

・政府情報システムにおける「クラウド・バイ・デフォルト」の原則に沿った導入検討（個別府省毎に実施すると負担大）

2019年４月26日の第４回言語バリアフリー関係府省連絡会議において、
佐藤ゆかり総務副大臣（当時）から、以下について各府省に協力を要請

- **各府省のご協力の下、外国人対応業務を洗い出し、自動翻訳システムに入力されうる情報の整理・類型化を行う。**
- **総務省は、上記の類型化を踏まえ、政府機関向けクラウド型翻訳システムが具備すべき技術的保護要件等を整理する。**
- **政府機関へのクラウド型翻訳システムの導入に向けて、自動翻訳利活用府省により、府省横断的な「クラウド・バイ・デフォルト」の原則に沿った検討を実施する。**

政府機関によるクラウド型翻訳サービスの利用に関する課題

□ 民間企業が提供するクラウド型の翻訳サービスは多数存在しているところ、政府機関においては、要機密情報を約款による外部サービスを利用して取り扱うことが禁止されている。

【参考】

〇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日改定　サイバーセキュリティ戦略本部決定）

第三章 政府機関等の情報セキュリティ対策のための基本対策
（外部委託）
第十六条　機関等は、情報処理に係る業務を外部委託する場合には、必要な措置を定め、実施しなければならない。
2　機関等は、外部委託（約款による外部サービスの利用を除く。）を実施する場合は、委託先において情報漏えい対策や、委託内容に意図しない変更が加えられない管理を行うこと等の必要な情報セキュリティ対策が実施されることを選定条件とし、仕様内容にも含めなければならない。
3　機関等は、要機密情報を約款による外部サービスを利用して取り扱ってはならない。
4　（略）

〇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）
（平成30年7月25日　サイバーセキュリティ戦略本部）

第4部　外部委託
4.1　外部委託
4.1.2　約款による外部サービスの利用
遵守事項
（1）　約款による外部サービスの利用に係る規定の整備
（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。
以下（略）

各府省等における外国人対応業務の洗い出し結果①

□ 各府省等に対し、外国人対応に関わる業務と取扱い情報に関するアンケートを実施。

省庁・機関	本府省	地方支分部局等 ※警察庁・総務省消防庁においては都道府県警・各消防本部
内閣官房・内閣府	—	—
警察庁	・外国からの視察・研修の受入れ ・外国政府機関等とのやりとり、意見・情報交換	・相談事案対応　・運転免許申請等　・交通指導取締り ・留置管理業務　・110番通報
総務省	・情報公開や個人情報保護に関する相談 ・行政不服審査法に基づく不服申し立ての受付等 ・ITU等国際会議における海外からの寄与文書等の翻訳 ・外国政府とのやりとり	・国の行政等に関する苦情や意見・要望を受け付け ・救急現場における外国人傷病者の症状等の聴取　・119番通報の翻訳
法務省	・認証紛争解決事業者に関する問合せ・苦情等 ・外国人に対する法律援助（法律相談実施を含む。） ・記録の閲覧等の窓口業務	・人権相談　・矯正施設における検査業務の一部 ・帰国説得、送還具備設定
財務省	・外国政府とのやりとり	・滞納整理事務　・調査事務、行政指導、確定申告 ・日本に出入国する外国人旅客の輸出入通関業務
文部科学省	・大使館、外国政府、国際機関等とのやりとり ・国際会議の会議文書の確認　・外国人向け調査の翻訳	—
厚生労働省	・行政手続き等に関わる苦情や意見・要望・質問対応 ・外国企業との薬事規制等に関するやり取り ・申請手続き、照会・相談 ・大使館や関係機関とのやり取り等	・申請手続き・許可書交付 ・就職相談対応 ・国民年金の手続に関する相談
農林水産省	・問い合わせ（総合窓口、直通メールなど） ・各国との有機同等性協議（メール、テレビ会議）	・外国語広報資料、ホームページの作成、調査研究 ・指導監督
経済産業省	・外国人の申請受付　・外国政府とのやりとり	・輸出入手続きの申請及び相談 ・外国語で記載された輸出入契約書等の内容を確認
国土交通省	・外部の労働者等からの公益通報に関する対応 ・立入検査、職務質問、捜査（海上保安庁警備）	・在留外国人 公共交通における事故による被害者等に対する相談・要望・問い合せ・苦情対応
環境省	・外国人からの問合せ等　・外国政府とのやりとり	・外国人からの問合せ等
最高裁判所	—	・家裁事件手続等に関する案内

各省庁等における外国人対応業務の洗い出し結果②

外国人対応業務の内容

本府省		地方支分部局	
30.0%	受付、窓口対応、申請、苦情対応	46.6%	受付、窓口対応、申請、苦情対応
27.9%	外国政府等対外対応	46.6%	外国政府等対外対応
22.1%	業務対応・業務説明	2.9%	研修、視察
5.0%	会議	1.1%	業務対応・業務説明
5.0%	研修、視察	1.0%	会議
8.5%	その他	3.0%	その他

「申請、相談業務」「外国政府等対外対応」の割合が高い。

個人を特定する情報の有無

本府省		地方支分部局	
51.1%	あり	89.8%	あり
48.9%	なし	10.2%	なし

半数以上の業務で、
個人を特定する情報の取り扱いがある。

個人を特定する情報が会話に出てくる頻度

本府省		地方支分部局	
11.6%	きわめて高い	32.6%	きわめて高い
20.9%	多い	29.3%	多い
51.2%	時々	25.0%	時々
16.3%	ほとんどない	13.0%	ほとんどない

通訳者を介して会話をすると仮定し場合、どの程度の機微性＊があるか。

本府省		地方支分部局	
12.0%	職員	17.9%	職員
74.7%	守秘義務契約を結んだ通訳	69.0%	守秘義務契約を結んだ通訳
4.0%	通常契約を結んだ通訳	11.9%	通常契約を結んだ通訳
9.3%	誰でもいい	1.2%	誰でもいい

＊相手(他人)に知られたくない情報であるか

会話において、個人を特定する情報を扱うことがあり、
通訳者を介して会話をすると仮定した場合、
「職員」又は「守秘義務契約を結んだ通訳」で対応する必要がある。

政府機関の外国人対応に関わる業務でクラウド型の自動翻訳システムを活用する場合、適切なプライバシー・セキュリティを確保すべき情報を取り扱うことを想定した運用が必要。

各省庁等における自動翻訳システムの導入に向けた実証調査

□ 今年度（令和元年度）、アンケート協力省庁等のうち、以下の省庁等において実証調査を実施。

省庁等	担当課		実証場所	用途	利用サービス
総務省	行政評価局	行政相談企画課	行政相談センター	行政相談に使用	音声翻訳
法務省	矯正局	成人矯正課	千葉刑務所	収容者との会話に使用	音声翻訳
	出入国在留管理庁	政策課外国人施策推進室	本庁内 地方出入国在留管理局	案内・相談・調査業務等に使用	音声翻訳 文書翻訳
国土交通省	海事局	外航課	本省内	業務等に使用	文書翻訳
	気象庁	予報部予報課 地震火山部管理課	国際会議	出席者との議論等に使用	音声翻訳 文書翻訳
農林水産省	消費・安全局	植物防疫課	全国14箇所の空港	入国者との防疫業務に使用	音声翻訳 文書翻訳
		動物衛生課	全国30箇所の空港・港	入国者との検疫業務に使用	音声翻訳 文書翻訳
厚生労働省	職業安定局	外国人雇用対策課	茨城・東京・神奈川・愛知・福岡における管轄内のハローワーク	相談者からの相談内容把握等に使用	音声翻訳
環境省	地球環境局 自然環境局 環境再生・資源循環局	国際連携課／国際地球温暖化対策担当参事官室 国立公園課・地方環境事務所 総務課循環型社会推進室／リサイクル推進室／廃棄物規制課	本省内 地方環境事務所・国立公園	来園者への案内・説明や廃棄物の輸出入の審査業務等に使用	音声翻訳 文書翻訳
最高裁判所	事務総局	家庭局第1課 秘書課	最高裁判所	最高裁判所内の案内	音声翻訳 文書翻訳

政府機関における自動翻訳システムの導入のための参照技術要件集 － 検討体制

- 現行の政府機関等の情報セキュリティ対策のための統一基準群※（以下「統一基準群」という。）は、政府機関が（当該基準群の適用対象となる）情報システムとしてクラウド型翻訳システムを導入・利用する場合に満たすべき技術要件が明確になっていない。

※ ①政府機関等の情報セキュリティ対策のための統一規範、②政府機関等の情報セキュリティ対策の運用等に関する指針、③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）、④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）

- これを明確化するため、クラウド型の自動翻訳システムの提供者となる事業者及びセキュリティ（ISO27000シリーズ）の監査・認証機関で構成される「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」（事務局：日本総研）（以下「検討会」という。）を開催し、同システムの利用者となる各省庁・機関の協力のもと、検討を実施。

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

＜提供者（事業者）＞

NTT東日本、NTTコミュニーションズ、コニカミノルタ、凸版印刷、東芝デジタルソリューションズ、フェアリーデバイセズ、みらい翻訳

＜監査・認証機関＞

BSI、バリューアップジャパン

＜事務局＞

日本総研

協力

利用者（省庁・機関）

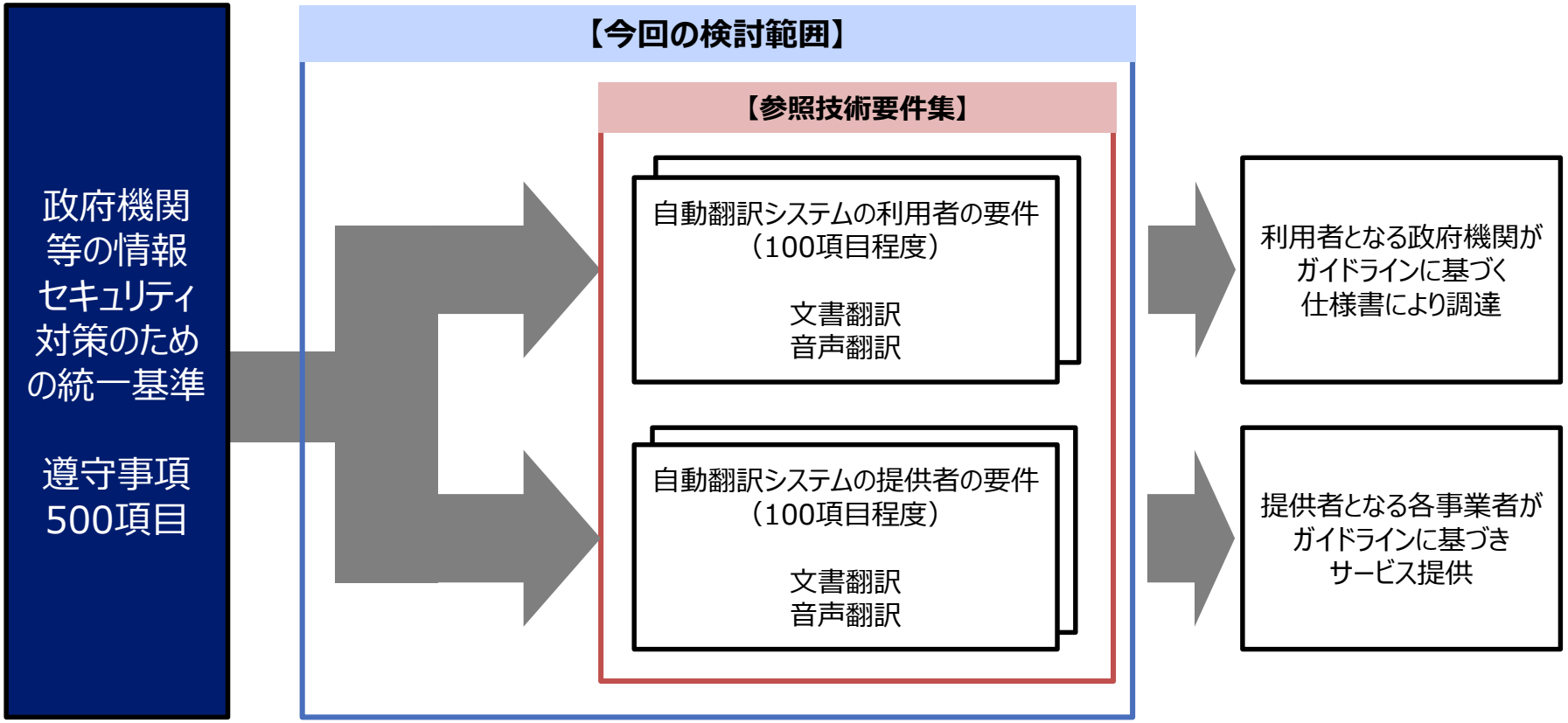
総務省
法務省
厚生労働省
農林水産省
国土交通省
環境省
最高裁判所

＊P4の実証調査の実施省庁・機関

政府機関における自動翻訳システムの導入のための参照技術要件集 － 全体フレーム

- 検討会において、統一基準群のうち「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/平成30年7月25日）に定められた対策項目に基づき、クラウド型の自動翻訳システムの利用者・提供者それぞれが遵守すべき要件を整理。

※　クラウド型ではない自動翻訳システム（オンプレミス型）や統一基準群の適用対象となる情報システムに該当しないサービスについては、本要件の対象外と考える。



参照技術要件集の対象範囲

自動翻訳システムのサービス提供形態		クラウド形態	情報管理	
			取り扱う情報	情報管理 ※操作ログ、翻訳データ
本要件集の対象範囲				
運用委託型	✓ 提供者の組織でのみ利用可能なクラウドサービス ✓ 提供者の組織でリソースを確保、外部との分離あるいは、制御対象 ✓ 委託による運用も可能	SaaS（主にプライベートクラウド）	要機密情報（機密性2情報）	提供者が利用者の求めに応じてログ管理や情報の取扱制限（例：持出禁止、暗号化、消去）を行うことが可能
購入・利用規約型	✓ 任意組織で利用可能なクラウドサービス ✓ リソースはクラウドサービス事業者が制御 ✓ 端末・アプリの購入や利用規約によるサービス利用	SaaS（主にパブリッククラウド）	公開情報（機密性1情報）	提供者が利用者の求めに応じてログ管理や情報の取扱制限を行うことが条件次第で可能
				提供者が利用者の求めに応じてログ管理や情報の取扱制限を一般的に行ってない
購入	✓ 任意組織で利用可能なオフラインサービス ✓ 端末の購入による利用	オフライン		提供者がログ管理や情報の取扱制限を行うことが不可能

参照技術要件集の概要 － 全体像

■ 検討会において、クラウド型の自動翻訳システムの導入に当たり、同システムの利用者と提供者のそれぞれが遵守すべき要件を整理。

政府機関等の情報セキュリティ対策のための統一基準				利用者が遵守すべき要件	提供者が遵守すべき要件
部	章	節	主な遵守事項		
1	総則		略	－	－
2	情報セキュリティ対策の基本的枠組み		○情報セキュリティ対策に関わる責任者の設置及び必要となる組織・体制整備 ・各種情報セキュリティ責任者及び委員会、監査責任者の設置 ・情報セキュリティ対策推進体制の整備、対策基準・対策推進計画の策定 ・教育体制の整備・教育実施計画の策定 ・情報セキュリティインシデントに備えた事前準備（報告手順、再発防止、対処手順など） ・自己点検計画の策定・手順の準備、実施、評価・改善 ・独立性を有する者による情報セキュリティ対策の監査の実施（計画、実施、対処）	・セキュリティ体制の整備 ・インシデントに関わる報告手順 ・自己点検計画の策定、実施 ・情報セキュリティ監査実施方法 ・監査結果報告	・セキュリティ体制の整備 ・インシデントに関わる報告手順 ・自己点検計画の策定、実施 ・情報セキュリティ監査実施方法 ・監査結果報告
2	2.1	導入・計画			
2	2.2	運用			
2	2.3	点検			
2	2.4	見直し			
3	情報の取扱い		○業務遂行における情報の利用等（作成、入手、利用、保存、提供、運搬、送信、消去等）に関わる情報のセキュリティの確保 ・情報の格付や取扱制限の決定・明示等 ・情報の目的外での利用等の禁止 ・情報を取り扱う区域の管理	・情報の取扱いに関する規定の整備 ・情報作成時等における格付や取扱制限の決定・明示等 ・要管理対策区域の範囲決定、入退管理対策	・情報の取扱いに関する規定の整備 ・情報作成時等における格付や取扱制限の決定・明示等 ・要管理対策区域の範囲決定、入退管理対策
3	3.1	情報の取扱い			
3	3.2	情報を取り扱う区域の管理			
4	外部委託		○外部委託に係る規定の整備 ・調達仕様書における情報セキュリティ要求事項の確認 ・約款による外部サービスの利用に係る規定の整備 ○クラウドサービス利用に関わる対策 ・委託先へのガバナンスの有効性や利用の際のセキュリティ確保のために必要な事項整理	・外部委託基準として国内法令の適用 ・情報セキュリティ水準の評価方法 ・情報の委託先における目的外利用の禁止 ・実施場所、インシデント対処（責任分界、体制整備） ・契約履行の確認方法 ・約款による外部サービス利用適用 ・アクセスログ等の管理	・外部委託基準として国内法令の適用 ・情報セキュリティ水準の評価方法 ・情報の委託先における目的外利用の禁止 ・実施場所、インシデント対処（責任分界、体制整備） ・契約履行の確認方法 ・約款による外部サービス利用適用 ・アクセスログ等の管理
4	4.1	外部委託			
5	情報システムのライフサイクル		○情報セキュリティ水準の維持に向けた情報セキュリティインシデントの対処対策 ・情報システムに関わる文書等の整備 ・情報システムのセキュリティ要件の策定、調達、構築、運用、保守 ・情報システムの運用継続	・情報システムのセキュリティ要件の策定 ・情報システムの運用・保守	・情報システムのセキュリティ要件の策定 ・情報システムの運用・保守
5	5.1	情報システムに係る文書等の整備			
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	5.3	情報システムの運用継続計画			
6	情報システムのセキュリティ要件		○情報システムのセキュリティ機能の整備 ・認証機能、アクセス制御、権限の管理、ログの取得・管理、暗号化 ○情報セキュリティの脅威への対策 ・情報システムを構成するサーバ装置、端末及び通信回線装置のソフトウェアの脆弱性への適切な対処 ・情報システムの破壊、情報の外部漏えい等の脅威を想定、事態の未然防止に向けた不正プログラムへの対策 ・標的型攻撃対策 ○アプリケーション・コンテンツの提供時の対策 ・なりすまし対策	・アクセス管理（主体認証、アクセス制御、権限） ・内部の不正操作防止 ・ログの取得、管理 ・情報漏えい対策（暗号化） ・特権的な利用者（例：管理者）における管理 ・第三者の侵入（情報窃取、破壊）防止 ・サービス不能攻撃（可用性の維持） ・標的型攻撃	・アクセス管理（主体認証、アクセス制御、権限） ・内部の不正操作防止 ・ログの取得、管理 ・情報漏えい対策（暗号化） ・特権的な利用者（例：管理者）における管理 ・第三者の侵入（情報窃取、破壊）防止 ・サービス不能攻撃（可用性の維持） ・標的型攻撃
6	6.1	情報システムのセキュリティ機能			
6	6.2	情報セキュリティの脅威への対策			
6	6.3	アプリケーション・コンテンツの作成・提供			
7	情報システムの構成要素		○情報システムの構成要素 ・端末利用への対策：外的要因（不正プログラム感染や不正侵入等）、内的要因（職員等の不適切な利用や過失等による不正プログラム感染等の情報セキュリティインシデント） ・機関等支給以外の端末に対する対策 ・サーバ、特定用途機器 ・電子メール、ウエブ ・通信回線の導入時対策	・端末、サーバ装置、通信回線の導入・運用・終了時の対策 ・端末からの不正プログラム感染、侵入（情報漏えい）防止 ・要機密情報を取り扱う端末の導入及び利用時の対策 ・無線LAN 環境導入時の対策	・端末、サーバ装置、通信回線の導入・運用・終了時の対策 ・端末からの不正プログラム感染、侵入（情報漏えい）防止 ・要機密情報を取り扱う端末の導入及び利用時の対策 ・無線LAN 環境導入時の対策
7	7.1	端末・サーバ装置等			
7	7.2	電子メール・ウェブ等			
7	7.3	通信回線			
8	情報システムの利用		略	－	－

参照技術要件集の抜粋 － ①クラウドサービスの利用

政府機関等の情報セキュリティ対策のための統一基準	遵守事項	利用者が遵守すべき要件	遵守要件の解説
第4部 外部委託			
4.1 外部委託			
4.1.4 クラウドサービスの利用			
4.1.4 (1) クラウドサービスの利用における対策	(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。
	(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。	
	(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。	
	(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。
	(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。

参照技術要件集の抜粋 － ②ログの取得・管理

政府機関等の情報セキュリティ対策のための統一基準		利用者が遵守すべき要件	
	遵守事項		遵守要件の解説
第6部 情報システムのセキュリティ要件			
6.1 情報システムのセキュリティ機能			
6.1.4 ログの取得・管理			
6.1.4 (1) ログの取得・管理	(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
	(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
	(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

参照技術要件集の抜粋 － ③端末の導入及び利用時の対策

政府機関等の情報セキュリティ対策のための統一基準	遵守事項	利用者が遵守すべき要件	遵守要件の解説
第7部 情報システムの構成要素			
7.1 端末・サーバ装置等			
7.1.1 端末			
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	(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。	
	(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
	(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
	(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。	
	(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。 (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） (イ) 端末管理責任者 機関等支給以外の端末	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。	
	(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。	
	(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。	

今後について

○　今般の「参照技術要件集」は、政府機関における自動翻訳システムの導入促進の観点から、各府省において令和２年度以降に実施するクラウド型の自動翻訳システムの調達手続等に資するよう第１版が作成されたもの。

○　クラウド型の自動翻訳システムの提供事業者においては、本要件集及び関連情報を踏まえ、令和２年度から順次、サービス提供が開始されることが想定される。

○　その上で、クラウドサービス全体に係る政府調達に関しては、政府全体での安全性評価制度等に関する検討が進められており※、今後その関連基準等の具体化が図られていくことが見込まれる。

○　このため、「参照技術要件集」についても、上記の状況と連動・整合させながら運用されていく必要があり、今後、必要に応じて見直し等を図っていきたい。

※関連情報
- 「クラウドサービスの安全性評価に関する検討会　とりまとめ」の公表（令和2年1月30日 総務省・経済産業省）
- 政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて（令和2年1月30日 サイバーセキュリティ戦略本部決定 ）