２０２６年３月１０日

ＡＩの社会実装において、障害となる又は不十分な効果をもたらす規制・制度についての情報提供募集に対する BSA の回答

（情報提供フォームにて回答）

事例１：地方自治体におけるネットワーク分離（総務省ガイドライン）の壁

Q2. ＡＩの活用を検討している分野について教えてください。（必須）（複数回答可）

分野については、次の日本標準産業分類の大項目単位のどれに当てはまるか、厳密でなくても差し支えありませんので、該当する分野を選択し:てください。

A 農業、林業
B 漁業
C 鉱業、採石業，砂利採取業
D 建設業
E 製造業
F 電気・ガス・熱供給・水道業
G 情報通信業
H 運輸業、郵便業
I 卸売業、小売業
J 金融業、保険業
K 不動産業、物品賃貸業
L 学術研究、専門・技術サービス業
M 宿泊業、飲食サービス業
N 生活関連サービス業、娯楽業
O 教育、学習支援業
P 医療、福祉

22F Shibuya Mark City West　1-12-1 Dogenzaka, Shibuyaku, Tokyo 150-0043
+81 3 4360 5474　www.bsa.org

Q 複合サービス事業 R サービス業（他に分類されないもの） S 公務（他に分類されるものを除く） T 分類不能の産業
A2. S 公務（他に分類されるものを除く）
Q3. ＡＩを利用するどのようなサービス・製品を、開発、提供又は利用しようと、検討しているのか、教えてください。（必須） どのような課題やニーズに対して、ＡＩをどのように活用し、それによりどのような付加価値を得ることを検討しているのかを具体的に御記入ください。可能な限り、５Ｗ１Ｈが分かるように御記入願います。
A3. 地方自治体（特に福祉部門や児童相談所など）において、住民とのオンライン相談や会議の際、SaaS 型 AI サービス（ミーティング要約機能）を利用して音声を自動でテキスト化・要約し、相談記録や議事録作成の業務効率化と付加価値の向上を図りたい。
Q4. 3. で御記入いただいた内容について、現行制度が原因となっている、又は原因となっていると思われるお困りごとを具体的に御記入してください。 また、ＡＩを導入することで既存の業務の効率化や新事業の創出を図ることが可能であるものの、既存の規制や制度のために十分な効果を上げられないもの、現行制度においてＡＩを導入することを想定しておらずどうしてよいか分からないものなどがあれば、併せてこちらに御記入ください。 以上のほか、問題の原因となっている具体的な法令（法律、政令、省令など）やガイドライン、通達の名称と、条項や該当箇所を特定できるように、詳細に御記入ください。複数ある場合には、分かる範囲で全て御記入ください。専門家等の第三者に指摘され、自分たちでは分からない場合や法令等に抵触すると漠然と認識されている場合には、その旨を御記入ください。 可能な限り、５Ｗ１Ｈが分かるように御記入願います。
A4. 総務省「地方公共団体における情報セキュリティ政策に関するガイドライン」、特にその中の「三層の分離（特に α’モデル）」の制約が AI サービス利用において障壁となっている。 福祉相談などにおいて、マイナンバーを扱う「個人番号利用事務系」や、機密情報を扱う「LGWAN 接続系」から、インターネット経由で提供される SaaS 型 AI サービス（LLM）へのデータ転送が厳しく制限されている。AI の学習にデ

ータが利用されない設定であっても、微機微情報を含むデータが海外サーバー（リージョン）を通過すること自体がセキュリティポリシー違反と解釈されることが多い。また、α'モデル等を用いて LGWAN 側に情報を持っていくための無害化処理を行うと、効率化の観点から AI の十分な効果を得られない。結果として AI 機能の導入を断念し、一律で機能をオフにして運用せざるを得ない状況にある。デジタル庁等が AI 活用を推進する一方で、総務省のガイドラインが旧来のネットワーク分離を前提としているため、現場に自己矛盾と混乱が生じている。
Q5. 4.**で記入した困っている状況等に対して、改善する具体的な提案があれば、自由に御提案ください。（任意）** これまで御回答いただきました困っている状況等について、それを改善するための具体的な提案があれば、御自由に御記入ください。
A5. 総務省のガイドラインを改定し、LGWAN 環境等からでも、一定のセキュリティ条件（AI 学習へのデータ不利用など）を満たしたクラウドベースの AI サービス（SaaS）を、過度な無害化処理なしに安全に利用できるような明確な基準と特例措置を設けていただきたい。省庁間の AI 活用に関する方針のダブルスタンダードを解消してほしい。
Q6. 本フォームについて、改善すべき点（広報の在り方、選択肢の種類、質問の内容等全般について）があれば、御自由に御記入ください。（任意）
A6.特になし

事例２：地方自治体における公文書管理と情報公開制度の壁

Q2. ＡＩの活用を検討している分野について教えてください。（必須）
A2. S 公務（他に分類されるものを除く）
Q3. ＡＩを利用するどのようなサービス・製品を、開発、提供又は利用しようと、検討しているのか、教えてください。（必須）
A3: 地方自治体において、SaaS 型 AI サービス（ミーティング要約機能・録画機能）を活用し、庁内会議や外部との協議における議事録作成を自動化し、職員の膨大な事務負担を削減したい。
Q4. 3. で御記入いただいた内容について、現行制度が原因となっている、又は原因となっていると思われるお困りごとを具体的に御記入してください。

A4. 公文書管理法および各自治体の公文書管理条例、情報公開制度の運用が AI サービス提供・利用の障壁となっている。AI による要約を利用するには会議の「録音・録画」が前提となるが、生成された音声・動画データも「公文書」に該当する。しかし、これらマルチモーダルなデータを適切に保存・検索・管理するための国からの明確な指針が存在しない。自治体は、将来的にこれらのデータに対して情報公開請求があった際、音声や動画から個人情報等を特定して保護（マスキング・黒塗り）する作業負担が膨大になることを予見し、このリスク回避のために「録音・録画」自体を禁止せざるを得なくなっている。結果として AI 要約機能が使えず、旧態依然とした手書きや記憶に頼った議事録作成が続いており、業務効率化の機会が完全に失われている。
Q5. 4.　で記入した困っている状況等に対して、改善する具体的な提案があれば、自由に御提案ください。（任意）
A5. テキスト（紙ベース）を前提とした現在の公文書管理の仕組みを現代化し、AI 処理の過程で生成される中間データ（録音・録画データ）の保存・廃棄ルールや、情報公開請求時のマルチモーダルデータに対する合理的な開示基準（あるいは AI を活用したマスキングの指針等）を国として明確に示していただきたい。
Q6. 本フォームについて、改善すべき点（広報の在り方、選択肢の種類、質問の内容等全般について）があれば、御自由に御記入ください。（任意）
A6. 特になし

事例３：医療機関におけるクラウド利用制限（ガイドラインと現場ポリシーの乖離）

Q2. ＡＩの活用を検討している分野について教えてください。（必須）（2/6）（複数回答可）
A2. P 医療，福祉
Q3. ＡＩを利用するどのようなサービス・製品を、開発、提供又は利用しようと、検討しているのか、教えてください。（必須）
A3. 病院などの医療機関において、AI 機能が付帯するクラウド型電話（通話録音）や SaaS 型 AI サービス（通話文字起こし、要約機能）を利用し、患者との通話記録や診療録の作成業務を自動化・効率化したい。

Q4. 3. で御記入いただいた内容について、現行制度が原因となっている、又は原因となっていると思われるお困りごとを具体的に御記入してください。
A4. 厚生労働省が示す「医療情報システムの安全管理に関するガイドライン」の現場での解釈の乖離と、病院内部の古いセキュリティポリシーが障壁となっている。 同ガイドライン上では、一定の要件を満たせばクラウド環境へのデータ保存が認められている。しかし、長年クローズド環境を前提としてきた現場の多くの病院では、「患者情報（診療録など）を含むデータは院内オンプレミスサーバーでのみ保存」「院外サーバー（クラウド）利用不可」という旧来の内部ポリシーが維持されている。そのため、クラウドベースの SaaS 型 AI サービスの導入が事実上不可能となっている。メガバンク等とは異なり、単一の病院や医療法人でオンプレミス型の AI（億単位の費用）を導入することは現実的ではなく、結果として AI のトライアルや PoC すら断念せざるを得ない状況が多発している。
Q5: 4.で記入した困っている状況等に対して、改善する具体的な提案があれば、自由に御提案ください。（任意）
A5: 厚労省から医療機関に対し、クラウドベースの AI 利用を推進する旨の強力なメッセージを発信していただきたい。具体的には、旧来の内部ポリシーを見直すための指示や、クラウドを安全に利用する場合の具体的な「ポリシー改定案（サンプル）」の提示、さらにはポリシー改定・システム移行を後押しする補助金制度などの支援策を要望する。 AI の社会実装を加速する上では、単に法的障壁を取り除くだけではなく、法の解釈、技術の活用、そして信頼形成が重要であることが認識されるべき。たとえ法的に寛容な環境であっても、政策目標を現実世界での導入につなげるには、積極的な指針、教育・啓発、そしてエコシステム構築への取組みが不可欠である。
Q6. 本フォームについて、改善すべき点（広報の在り方、選択肢の種類、質問の内容等全般について）があれば、御自由に御記入ください。（任意）
A6. 特になし

事例４：透明性措置におけるサイバーセキュリティ・国家安全保障の保護の課題

Q2. ＡＩの活用を検討している分野について教えてください。（必須）（2/6）（複数回答可）

A2. S 公務（他に分類されるものを除く）
Q3. ＡＩを利用するどのようなサービス・製品を、開発、提供又は利用しようと、検討しているのか、教えてください。（必須）
A3. 政府機関において、政府情報システムをサイバー攻撃から保護するため、AI を活用したサイバーセキュリティソリューションを導入。
Q4. 3. で御記入いただいた内容について、現行制度が原因となっている、又は原因となっていると思われるお困りごとを具体的に御記入してください。
A4. 知的財産戦略本部（知財戦略本部）から提案されている「生成 AI の適切な利活用等に向けた知的財産の保護及び透明性に関するプリンシプル・コード（仮称）（案）」（以下「コード案」）は、現行案のまま実施された場合、サイバーセキュリティソリューションを含む AI 活用サービスの提供・利用の障壁となり、国家安全保障上のリスクにつながる可能性がある。コード案は、AI 事業者に対し、「モデルの学習プロセスの詳細」や「パラメータ設定」など、企業が営業秘密とみなす情報を公開することを期待している。コード案の原則 1 にある情報開示は、サイバーセキュリティ強化を目的とした AI に適用された場合、重大なリスクを伴う。このような詳細情報は、攻撃者に防御アーキテクチャの「設計図」を提供する結果となる可能性がある。さらに、原則 2 では、AI 事業者に対し、法的措置のためのデータアクセスを提供することを期待している。「法的手続の準備をしている」という理由だけでデータへのアクセスを認めることは、機微なセキュリテインテリジェンスへのアクセスを狙う悪意ある主体による濫用的な、情報漁りを招くおそれがある。このような機微なデータへのアクセスついては、より厳格な法的要件が課されるべきである。同様に、学習データの URL の提供を AI 事業者に求める原則 3 についても、重大なセキュリティ上の懸念が生じる。サイバーセキュリティ企業は、ウェブフィルターやファイアウォールを学習させるために大量の URL データを使用している。特定の URL が学習に使用されたかどうかを開示することは、当該インフラがセキュリティシステムによって検知されていることを、意図せずして悪意ある主体に示す結果となり、防御を回避できるようインフラを変更する手がかりを、そのような主体に与えてしまう可能性がある。
Q5. 4. **で記入した困っている状況等に対して、改善する具体的な提案があれば、自由に御提案ください。（任意）**
A5. 知的財産戦略本部は、原則 1 を改訂し、透明性に関する措置が概要レベルの、非機密情報に限定されることを明確 にし、営業秘密や契約上の機密情報、または機密

性の高い事業・技術情報の開示は求められないこ とを明示すべきである。また、知財戦略本部は、関係当事者の一方に有利または不利となり得る追加的な開示権限や手続きをコード案において新たに設けることを避けるべきである。特定の生成結果を、一つの情報源や URL に遡ることは技術的に不可能であるため、原則 2 と 3 は削除すべきである。AI モデルは学習データの複製を保存または取得するのではなく、学習データのコーパス全体にわたってパターンを学習し、特徴を一般化している。濫用を防止する観点から、特にセキュリティシステムに関連する学習データ へのアクセスについては、裁判所命令等、より高い基準を設けることを奨める。
Q6. 本フォームについて、改善すべき点（広報の在り方、選択肢の種類、質問の内容等全般について）があれば、御自由に御記入ください。（任意）
A6. 回答者が複数の事例を提出する場合、本フォームでは事例ごとに情報を個別入力する必要があり、複数回にわたって回答者が連絡先情報等を再入力することとなる。このような重複作業を回避するよう、フォームを改善することを奨める。