



The Admissions Office

Offering the choice of colleges from the world map

White Paper

第 7 版 2023.11.1 作成
株式会社 TAO

目次

1	はじめに	3
1.1	The Admissions Office (TAO) とは	
1.2	責任共有モデル	
1.3	システム開発と運用	
1.4	本ホワイトペーパーについて	
2	事業概要とセキュリティへの取り組み	4
2.1	事業概要	
2.2	セキュリティへの取り組み	
2.3	認証取得への取り組み	
3	セキュリティ体制	5
3.1	当社における情報セキュリティマネジメント	
3.2	正規スタッフによる運用業務の遂行	
3.3	建物・部屋のセキュリティ	
3.4	業務ネットワークのセキュリティ	
3.5	The Admissions Office (TAO) システムのセキュリティ	
3.6	情報セキュリティインシデント対応	
4	The Admissions Office (TAO)システム情報	15
4.1	クロック	
4.2	AWS リージョン情報	
4.3	バックアップ	
5	The Admissions Office (TAO)サポートデスク	15
5.1	The Admissions Office (TAO) サポートデスクの特色	
5.2	The Admissions Office (TAO) サポートデスクの運用体制	

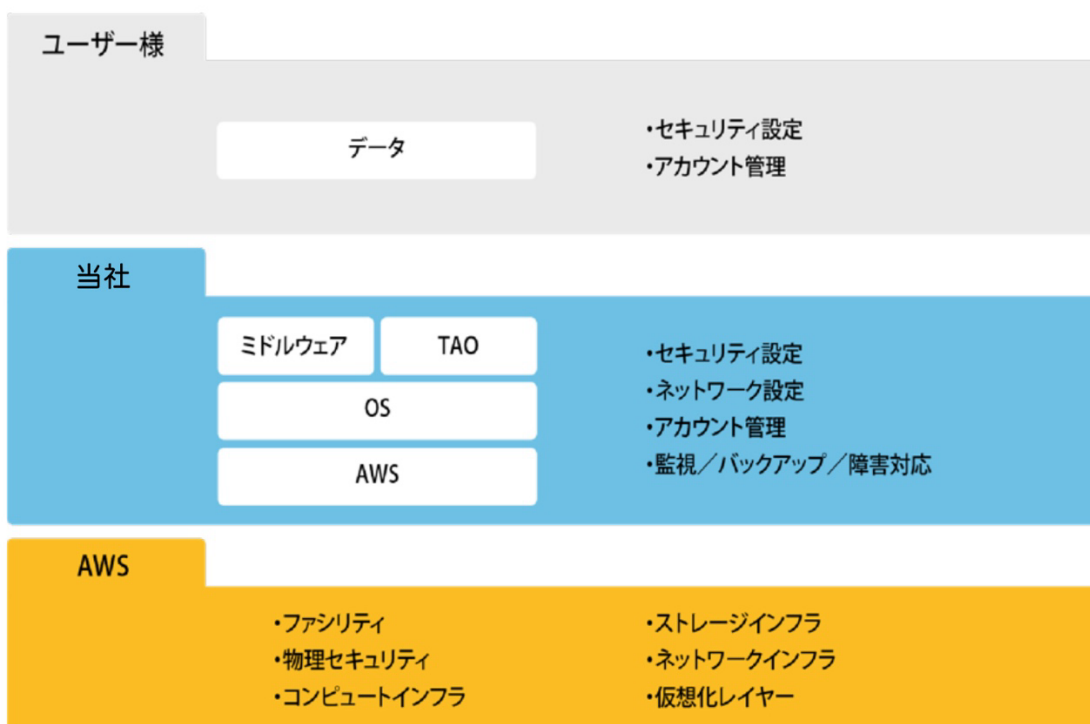
1. はじめに

1.1 The Admissions Office (TAO) とは

株式会社 TAO（以下当社）によって提供される The Admissions Office（以下 TAO）は、学生がひとつのフォームで複数の大学に出願できる Web 入試コンソーシアムサービスです。

1.2 責任共有モデル

AWS が提示する「責任共有モデル」(Shared Responsibility Model) は、クラウド運用の発展から生まれてきた考え方の一つです。当社は AWS クラウドインフラストラクチャを基盤に TAO システムを構築し、ユーザー様は TAO アプリケーションを運用することになりますので、セキュリティ上の責任はユーザー様と当社と AWS の三者による分担となります。



ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティにおけるさまざまなコンポーネントの操作、管理、コントロールは、AWS によって行われ、AWS インフラストラクチャ上に構築した TAO システムにおけるセキュリティは当社が保護いたします。TAO システム上で運用されるデータのセキュリティについてはユーザー様ご自身で保護していただく必要があります。

1.3 システム開発と運用

AWS は、クラウドシステムの長い運用経験から数多くのベストプラクティスを蓄積し公表しています。このことから、AWS が TAO のプラットフォームとして適切であると判断して利用を決定しました。そして TAO システムは、当社及び信頼のおけるビジネスパートナーのもつ技術力と経験に従って開発・運用されています。このことは、TAO ご利用のユーザー様が安心して TAO 上にデータの蓄積をしていただければ良いことを意味します。このように、システム構築、セキュリティについて、ユーザー様、当社、AWS がそれぞれに役割と責任を分担することで、TAO システムは運用されています。

1.4 本ホワイトペーパーについて

本ホワイトペーパーは、前述の「責任共有モデル」の考え方に基づき、当社が提供する TAO サービス基盤におけるセキュリティの取り組み、およびユーザー様にご利用いただけるセキュリティサービスについてご理解を深めていただくために提供するものです。

対象読者:

TAO 利用中の方

TAO 導入をご検討中の方

2. 事業概要とセキュリティへの取り組み

2.1 事業概要

TAO は、学生がひとつのフォームで複数の大学に出願できるシステムを提供する事業です。

【主な機能】

複数の出願書類の提出を必要とする募集を大学等が作成する

出願者が募集に対して出願書類の入力を行う

出願者が受験料の支払いを行う

出願者と大学等がメッセージでやりとりを行う

大学等が合否結果を出願者に伝える

2.2 セキュリティへの取り組み

ユーザーの皆様安心して TAO のサービスをご利用いただくために、第三者機関による認証を含む実効性の高いセキュリティ施策を実施し、情報セキュリティに対して万全の体制で取り組んでいます。

2.3 認証取得への取り組み

○情報セキュリティマネジメントシステム (ISO/IEC27001, ISO/IEC27017)

TAO を運営する当社が属するサマデイグループは、2016 年 12 月に情報セキュリティマネジメントシステム (ISMS: Information Security Management System) の国際規格である ISO/IEC27001 の認証を取得いたしました。国際規格 ISO/IEC27001/日本工業規格 JISQ27001「情報セキュリティマネジメントシステム－要求事項」を基準として、TAO が保有する情報資産を機密性、完全性、可用性の観点から維持改善するために、事業内におけるセキュリティルールを確立し、継続的に運用、監視、見直しを行っています。また、TAO は 2020 年 12 月に ISMS クラウドセキュリティ認証 (ISMS-CS) の認証を取得いたしました。

○ソフトウェア脆弱性情報に関する取り組み 近年、インターネット基盤ソフトウェアで新たな脆弱性が多く発見されていることから、当社では、ソフトウェア脆弱性への対応を強化するため、脆弱性情報収集を行う TAO サポートデスクを設置しています。定常的に脆弱性情報の収集を行い、実際にソフトウェア脆弱性が発見された場合には、速やかにその影響の有無および緊急度について判断し、ユーザー様のシステムを防護するために適切な対応を行います。また、セキュリティを専門とする企業による脆弱性診断テストを実施しています。

3. セキュリティ体制

3.1 当社における情報セキュリティマネジメント

3.1.1 情報セキュリティマネジメントシステム (ISMS)

当社の情報セキュリティマネジメントは、当社が属するサマデイグループの情報セキュリティマネジメントシステムポリシー (以下「ISMS ポリシー」) に基づき、以下の体制で行っています。

○情報セキュリティ委員会

当社の情報セキュリティ推進に関する事案を審議し、組織内への周知活動を行っています。情報セキュリティ管理責任者、情報セキュリティ推進事務局、情報セキュリティ教育責任者、情報システム管理責任者、各部門の情報セキュリティ部門責任者から構成されており、月例で会議を開催しています。

○情報セキュリティ管理責任者

グループ代表の命を受けたグループ内の常勤役員がこの任にあたり、情報セキュリティの全社的な実施及び運用に関する責任と権限をもちます。

○情報セキュリティ推進事務局

情報セキュリティ推進事務局は、情報セキュリティの推進を行う責任と権限をもちます。

○情報セキュリティ部門責任者

情報セキュリティ部門責任者は、各部門の情報セキュリティの統括責任者です。

○内部監査責任者

内部監査責任者は、グループ代表が任命します。公平かつ客観的な立場で、グループ内の情報セキュリティ運用・遵守状況の監査に関する責任と権限を持ちます。

○情報セキュリティ教育責任者

適用範囲内の全従業員に対して、情報セキュリティ方針の遵守、ISMSの運用についての教育を計画し、実施し、報告する責任を有します。情報セキュリティ管理責任者により任命されます。

○情報システム管理責任者

適用範囲内の情報システムに関する情報セキュリティの管理・運用に対して責任を有します。

3.1.2 情報資産管理

当社は、ISMSポリシーに基づき、すべての情報資産に対して適切な管理方法を定めるための台帳を作成し、当社の定める機密レベルに応じたアクセス権設定および情報の取り扱い方法を行っています。また、各情報資産に対するリスクを、推定される損害、脅威、脆弱

性の観点から定量的に評価し、必要に応じて適切な管理策を適用することでリスク低減を図ることも定期的に行っています。ユーザー様情報を含む社内情報の取り扱いについては、当社の定める手順に従って適切な保護および利用を行い、その文書・記録媒体については、保管期間を定め、必要な保護および定期的な検査の実施、保管期間を経過した記録の適切な廃棄を行っています。

3.1.3 日常業務におけるセキュリティ運用の実践

当社では、全社員に対して当社の個人情報保護方針、情報セキュリティ基本方針、情報セキュリティに関する関連法令および契約事項について、その内容の理解および周知徹底を図っています。社員が業務上知り得た社外秘以上の秘密情報および個人情報は、期限なくこれを秘密に保持し、関係者外への開示を禁止しています。また、社外に業務を委託する場合は、外部委託先評価を年1回以上行い、秘密保持契約ならびに個人情報取り扱いに関する覚書を締結しています。

3.1.4 教育

当社では、教育研修規程の定めに従い、中期教育計画を作成し、下記のセキュリティ教育を実施しています。

○全社における情報セキュリティ教育 当社では、全従業員を対象に情報セキュリティに関する教育および理解度チェックを年1回以上実施し、当社の業務に関わる全スタッフのセキュリティへの理解を継続的に強化しています。

○TAOにおけるセキュリティスキルの向上 当社では、TAO業務に従事する全スタッフに対して、AWSサービスおよびセキュリティに関連したトレーニングの受講および認定資格の取得を奨励し、セキュリティ知識およびスキルの向上に努めています。

○最新セキュリティ情報の共有

当社では、セキュリティに関する最新情報を社内に共有する体制を確立しています。

3.1.5 監査

当社では、ISMSポリシーに従い、下記の通りセキュリティ監査を実施しています。

○ISMS 監査

ISO27001、ISMS 規定文書および当社で定めた手順書類、関連法令または規制条項を監査基準とした定期内部監査を年1回実施しています。

○臨時監査

情報セキュリティ委員会が必要と認めた場合には臨時監査を実施することを社内規定で定めています。

3.2 正規スタッフによる運用業務の遂行

TAOにおいては、その運用業務に携わるスタッフ（以下「TAO スタッフ」）について正社員雇用契約を締結し、内部からの攻撃リスクを最小限に抑えています。また、TAO スタッフの雇用に際しては、ISMS ポリシーに従い、過去の職歴や経歴などを可能な範囲（地域法の制約内）で調査し、TAO における職務を理解しその役割に適材な人物により運用業務を遂行しています。

3.3 建物・部屋のセキュリティ

3.3.1 安全な建物・部屋の選定

当社では、事業に関連する情報資産の物理的な保護を図るために、当社の定める手順に基づき、その事業の用に供する建物や部屋について、堅牢性、遮蔽性、防犯性など当社の定めるセキュリティ条件による審査および選定を実施しています。

3.3.2 利用中の建物・部屋のセキュリティレベル

当社では、業務上アクセスする必要のある情報資産の重要度に応じて、現用中の建物や部屋に対して、情報セキュリティポリシーに従い、建物や部屋に下記のセキュリティ区画を設定し、入退室管理および監視を行っています。

○セキュリティレベル 1

玄関、通路、階段、トイレなどのパブリックなエリアです。

○セキュリティレベル 2

当社従業員が訪問者の対応を行なうエリアです。入室は許可されたものに限定されています。

○セキュリティレベル 3

当社従業員が業務を行うセキュリティエリアです。入室は許可されたものに限定されています。

○セキュリティレベル4

当社従業員がセキュリティ要求がより高い業務を行う高セキュリティエリアです。情報セキュリティ管理責任者に入室許可され、尚且つ教育を受けた専任の TAO スタッフのみ入室可能としています。外部訪問者の入室は禁止としています。ルーム内での補修工事など特別な理由により情報セキュリティ管理責任者が許可した場合は、訪問者には常に入室権限のある TAO スタッフが同行し、作業内容の記録および ISMS 管理責任者への報告を行います。

3.3.3 建物・部屋の防犯および入退室管理

当社においては、事業に関連して保有する情報資産を保護するために、特にセキュリティ保護が必要な領域において、防犯カメラまたは入室ログ収集システムを導入し、その領域へのアクセスについて監視およびログ収集を行っています。防犯カメラの録画映像および入室ログについては、情報セキュリティポリシーにより3ヶ月以上保管しています。退職・休職により TAO スタッフの異動があった場合は、速やかに交付されたアクセス権を回収し、部外者の物理的な侵入を防止できる体制を実現しています。

3.3.4 建物・部屋の物理的なネットワークの保護

当社においては、社内ネットワーク上の情報資産を保護するために、当社で管理する建物・部屋に敷設された物理的なネットワークに対して、下記の保護策を行っています。

- 最低限必要な権限者のみがネットワークに接続できるように、物理的な保護を行っています。
- サーバールックは常時施錠し、鍵は情報セキュリティ管理責任者が厳重に管理しています。
- 通信回線への物理アクセスを可能とする機器（ワイヤレスアクセスポイント、ゲートウェイ、ハンドヘルドデバイス、ネットワーク/通信ハードウェア）については、事前に情報セキュリティ管理責任者が認めたものを除き、セキュリティエリア3への持ち込みを禁止しています。
- 外部からの訪問者に関しては、特別に情報セキュリティ管理責任者の明示的な承認がある場合を除いて、セキュリティエリア2および3における物理ネットワークへの接続を禁止および遮断しています。また、物理ネットワークの保護策について実効性を確保するため、当社で管理する物理ネットワークの変更作業についても、情報セキュリティポリシーにより下記のように変更ルールを定めています。
- サーバーやネットワークの変更などネットワーク機器に関して設定変更の必要がある場合は、承認フローに従い、情報セキュリティ管理責任者に承認を得た上で実施し、作業

終了後、作業内容および変更した設定の内容について、情報セキュリティ管理責任者に報告し記録しています。

- 機器の保守などで業務上、やむを得ずネットワーク機器を持ち込む場合には事前に情報セキュリティ責任者の承認を必要としています。

3.4 業務ネットワークのセキュリティ

当社においては、事業に関連する情報資産を保護するため、当社の他事業と独立した社内ネットワークを構築しています。さらに、各種閉域ネットワークサービスを活用し、認証情報を外部から隔離された場所で一元管理することにより、極めてセキュリティ強度の高い業務ネットワークおよび認証システムを導入し、運用業務の基盤として利用しています。また TAO システムも他要素認証で外部からの侵入を防ぎ、ログ機能によってシステムの不正利用がないか監視する事が可能です。

3.4.1 ネットワークのセキュリティレベル

当社において利用する業務ネットワークについては、セキュリティレベルに応じて2つのネットワークに分割することにより、利用者の区分に従った適切なアクセス制御を行っています。

○セキュリティネットワーク 1 (ゲストネットワーク)

訪問者など部外者向けのネットワークです。無線（暗号化通信）による接続のみ提供しています。当社の他のネットワークと接続されておらず、当社の持つ情報資産へのアクセス経路はありません。

○セキュリティネットワーク 2 (オフィスネットワーク)

当社において通常の運用業務に利用するネットワークです。予め許可された業務端末のみが接続可能です。無線（暗号化通信）および有線による接続を行っています。

3.4.2 認証情報の一元管理

TAO 業務ネットワークでは、TAO スタッフの認証情報を一元管理しています。これにより、退職・休職によるスタッフの異動があった場合や、万が一認証情報が漏えいした場合にも速やかに当該アカウントを無効化することにより、TAO 業務ネットワーク上の情報資産へのアクセスを完全に遮断できる体制を実現しています。

3.4.3 サーバ監視

TAO 業務ネットワークでは、情報セキュリティポリシーに従い、ネットワークリソースへのアクセスを追跡および監視し、その記録を事後に変更できないように保護した上でアクセスログとして保存しています。さらに、監視システムによる常時監視を行っています。

3.4.4 運用業務端末のセキュリティ

TAO 業務ネットワークへの接続は、運用専用端末のみ可能としています。これら運用業務を行う端末（以下、「運用業務端末」）については、事前に承認を受けた TAO スタッフ以外の利用は禁止しています。運用業務端末については、以下のセキュリティポリシーを適用し、その操作について常に監視および操作ログの保存を行っています。

- ウィルス対策ソフト、プログラムについては常に最新を維持する。
- ベンダーが提供する OS や業務用ソフトウェアの修正プログラムは、自動更新に設定する。
- 事前に認められたプログラム以外はインストールしない。
- USB メモリーなどの外部デバイス利用を禁止する。
- インターネットへの接続については、業務上必要な場合のみ利用することとし、適切な URL フィルタリングの導入により意図しない不正サイトへの接続をブロックする。
- クライアント操作ログを取得する。

リモート運用端末については、セキュリティについて技能および経験に裏打ちされたスキルを持つと認定された TAO スタッフのうち、特に必要があると認められた者だけが所持できるものとします。

3.4.5 業務ネットワークの定期的な検査

TAO 業務ネットワークにおいては、情報セキュリティポリシーに従い、定期的に以下のネットワーク検査およびテストを実施することで、セキュリティの強度を適切なレベルに維持しています。

- 不正なネットワーク機器の検出
- ネットワークの脆弱性検査
- インフラストラクチャの内部および外部ペネトレーションテスト

3.5 TAO システムのセキュリティ

TAO システムは強度の高いポリシーによるパスワード運用、また他要素認証で外部からの侵入を防ぎ、ログ機能によってシステムの不正利用がないか監視する事が可能です。

3.5.1 複数の認証システム

TAO では、以下の 2 つの認証システムを併用することで、多重に本人確認を行い、万が一パスワード情報が漏えいした場合であっても、TAO システムへの侵入を防御するための高度なセキュリティ運用を行っています。

○ユーザー認証

ログインするユーザーが TAO ユーザーであることを認証します。

○2 段階認証

ログインするユーザーのメールアドレスを利用した認証を行います。

3.5.2 パスワードポリシー

TAO においては、本人以外による不正利用を防止するために、情報セキュリティポリシーに従い、認証システム上でのパスワード管理について強度の高いポリシーで運用しています。パスワードは暗号化してデータベースに格納しています。

3.5.3 暗号化の種類

TAO の全ての通信は SSL/TLS 通信を利用して暗号化されます。また、全ての情報は暗号化されストレージに保管されています。

3.5.4 ログ機能

TAO システムの管理画面には操作履歴が確認できる、ログ機能が実装されており、不正な利用がないか監視することが可能です。

3.5.5 情報の公開範囲設定

TAO システムに投稿された情報は、予め公開範囲を設定することにより、情報の機密区分に応じた分類が可能です。

3.5.6 アカウントの停止

TAO ご解約の場合は、解約日に TAO 法人アカウントの解約手続きを行います。該当の法人アカウントと法人アカウントに関連するすべてのアカウントのログインが不可能となり、不正なアクセスを防止します。再契約の際には該当の法人アカウントと法人アカウントに関連するすべてのアカウントのログインが可能となります。

3.5.7 サーバ監視

TAO システムは監視システムによる常時監視を行っています。万が一 TAO のセキュリティに対して影響のある事象が発生した場合には、24 時間即応可能な TAO スタッフが、当社の定めるインシデント対応手順書に従い、迅速かつ効果的に対応する体制を確立しています。

3.5.8 仮想ネットワーク・仮想マシン

TAO システムを構成する AWS 上の仮想ネットワークは、本ホワイトペーパーにおける 3.4.2,3.4.3,3.4.4,3.4.5 に定める当社の情報セキュリティポリシーに従い設定され、VPC(仮想プライベートネットワーク)によるネットワークアドレス分離、及び IAM(ロール権限)での制御、またアクセスキー・シークレットキーでのアクセス保護を行っております。

また仮想マシンについては以下の対策を実施しております。

[Web サーバ用途の仮想マシン(ECS)]

- 関係各社のオフィス IP からのみアクセスできるよう制御

[本番環境で利用しているロードバランサ(ELB)]

- 80, 443 ポートのみアクセスできるよう設定

また、本番環境の Web サーバに関しては監視アプリケーションによる下記対策を実施する

- 不正プログラム対策
- 侵入防御検知(既知の脆弱性含む)
- ファイル改ざん検知
- セキュリティログ監視

3.5.9 セキュリティ診断

TAO システムに対して以下の Web アプリケーション診断を適宜行っております。

- 外部の専門企業によるアプリケーションの脆弱性診断

- プラットフォーム診断

3.5.10 開発体制

TAO システム開発時にはソースコードの静的解析による OWASP TOP10 ベースのセキュリティチェックを実施し、加えてコーディングルールのチェックを実施しております。そしてレビューをしたプログラムソースのみを本番環境に反映するルールを設けております。また、開発用 WEB サーバは関係各社の指定 IP からのみアクセスできるよう制御しております。既存の TAO システムに対する定期的な変更、緊急の変更、および設定の変更は、類似するシステムの業界基準に従って、許可、記録、テスト、承認、および文書化されます。TAO システムを更新するにあたり、お客様とお客様によるサービスの使用に対する影響は最小限に抑えられます。サービスが悪影響を受ける可能性がある場合、TAO のお知らせ機能を利用して顧客に通知します。

※OWASP Top10 とは： ウェブアプリケーションセキュリティをとりまく課題を解決することを目的とする、国際的なオープンなコミュニティが、ウェブアプリケーションにおける重要な脆弱性やその脆弱性を作りこまないようにする方法などを示した成果物。

3.6 情報セキュリティインシデント対応

TAO システムを提供するために用いるリソース、またはユーザが管理しているリソースにセキュリティインシデント（不正侵入、DoS 攻撃、情報漏えいなど）が発生した場合の対応について、TAO のお知らせ機能を利用して以下の内容を告知いたします。（インシデントのレベルに応じて、TAO に登録されているメールアドレスにもメールで通知いたします）

- 発生内容
- 日時
- 影響範囲
- 復旧見込み

※以下情報は状況によって告知する場合があります。

- 原因
- 当面の対応策
- 再発防止策
- 問い合わせ窓口（事故に関する連絡先）

4. TAO システム情報

4.1 クロック

システムで使用しているクラウドサービスのクロックは NTP サーバを利用しております。

4.2 AWS リージョン情報

TAO システムは AWS の東京リージョン及びシンガポールリージョンを利用して構築されております。バックアップ(DB スナップショットや出願されたファイルデータ)は東京リージョン及びシンガポールリージョンで保存されています。AWS に適用される法域については米国ワシントン州法準拠、ワシントン州キング郡の州裁判所か連邦裁判所です（東京リージョンも適用内）。

4.3 バックアップ

TAO システムは日次でデータバックアップを取得しております。またお客様向けバックアップ機能として、管理画面の各種データ CSV ダウンロード機能、書類のダウンロード機能が実装されています。

5. TAO サポートデスク

TAO サポートデスクは、TAO をご利用いただいているお客様に対してサポートサービスをご提供する窓口です。お客様からのご依頼やご相談を承るだけでなく、万が一お客様のシステムについて障害が発生した場合のご連絡窓口となります。TAO は、TAO サポートデスクを通じて、お客様のシステムの効率的で安定した運用を実現いたします。

5.1 TAO サポートデスクの特色

TAO サポートデスクは、以下のような特色を持っています。

高度なクラウド技術を有する外部パートナースタッフ

TAO サポートデスクは、AWS プラットフォームで稼働するアプリケーションやインフラストラクチャの設計・導入・運用に必要なスキルと技術知識を有するエンジニアが多数所属する外部パートナーと提携しており、日々お客様のシステムの安定稼働に必要な活動を行っています。

クラウド運用を支援する TAO 開発チーム

TAO では、クラウドシステムに精通したエンジニアによる開発チームが、認証基盤や自動化基盤および運用基盤など TAO を支える多彩なシステムの開発を行い、日々改善を重ねています。

TAO サポートデスクは、TAO 開発チームと密接に連携することで、高度で迅速なクラウド運用を実現しています。

5.2 TAO サポートデスクの運用体制

TAO サポートデスクは、以下のような運用体制により、TAO システムを運用いたします。

・お客様

TAO システムの運営に関する責任を有し、判断決定を行います。

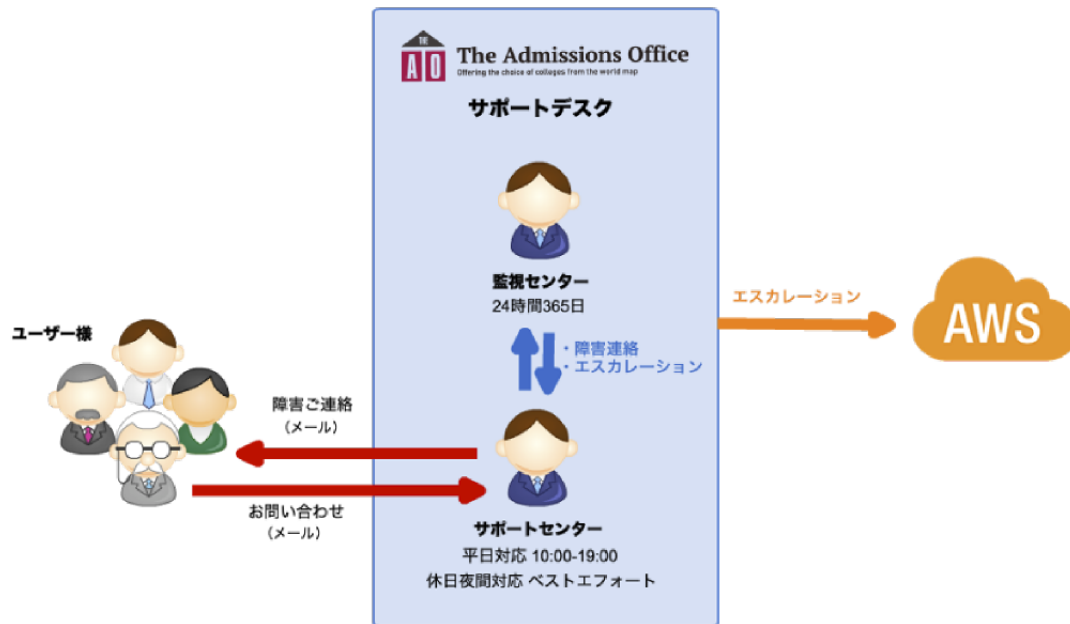
・監視センター

平常時の監視および障害発生時に一次切り分けおよび復旧作業を行います。監視センターで解決できない場合は、専門の担当(開発チーム)に対してエスカレーションを行います。監視センターは、24 時間 365 日対応をカバーする外部パートナーに属するエンジニアにより組織されます。

・サポートセンター

TAO に関わる障害や仕様などに関する問い合わせに対応し、障害検出後、お客様へ提供しているサービスに影響を及ぼす障害のみ、2 営業日内にご連絡をいたします。サポートセンターで解決できない問題がある場合は、専門の担当(開発チーム/監視センター)に対してエスカレーションを行います。また、技術的せい弱性に関する情報を必要に応じてお客様にお伝えいたします。

【TAO サポートデスク運用体制】



TAO サポートデスク連絡先

support@admissions-office.net