SECURITY GUIDE

安全なサービスであるために

セキュリティ& 運用基盤

Sciseed

クラウドサービスを安全に使うために重要な７つの対策

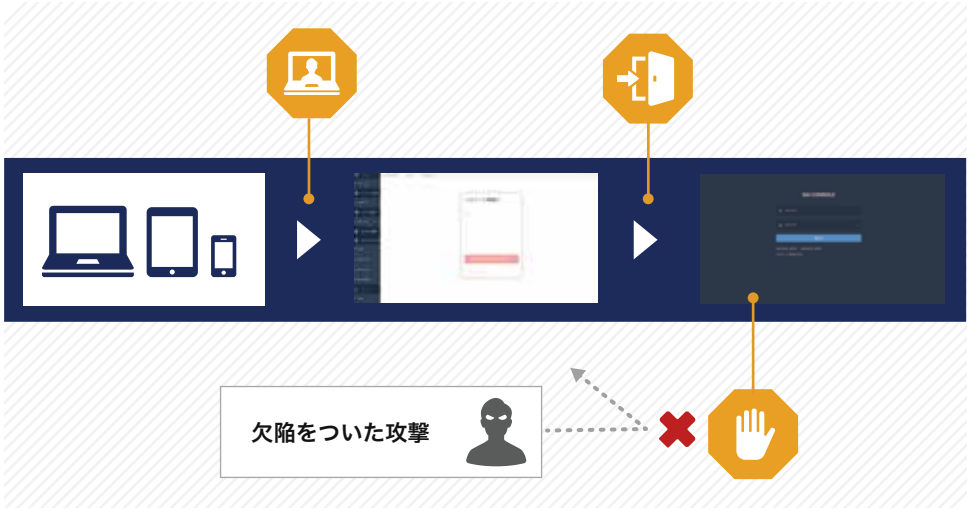
SECURITY セキュリティ

01 不正アクセス対策

サービスを利用するためのログイン画面に、許可されてない第三者がアクセスできないようにします。

02 不正ログイン対策

第三者がログイン画面にアクセスできてしまった場合でも、不正にログインできないような設定が可能です。



03 脆弱性対策

コンピュータや OS を持つ脆弱性など、セキュリティ上の欠陥をついた攻撃を未然に防ぐための体制を作り上げています。

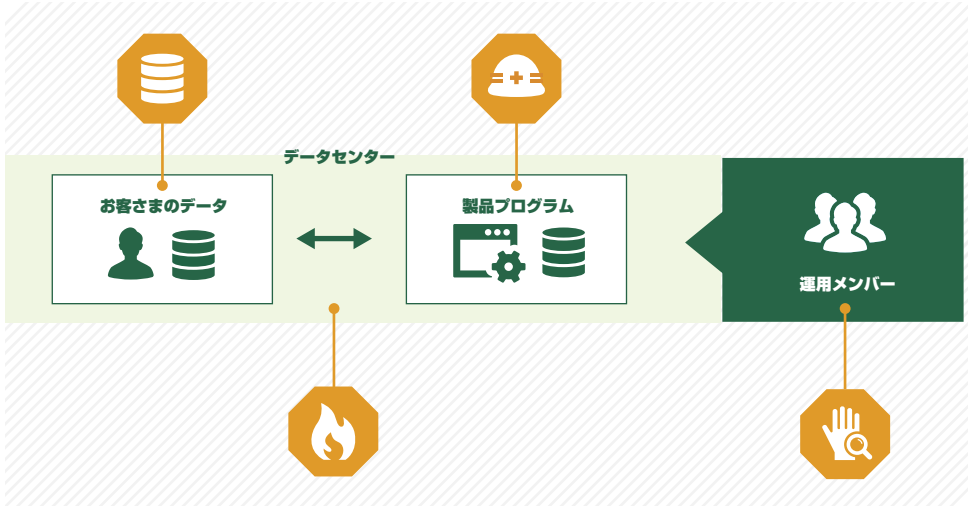
OPERATION BASE 運用基盤

04 データー消失対策

何重もの対策で、お客様のデータ保護を最優先に運営しています。

05 障害検知・復旧対策

ハードウェアなどに障害が発生した場合でも、できる限り早く復旧できる環境・体制を作っています。

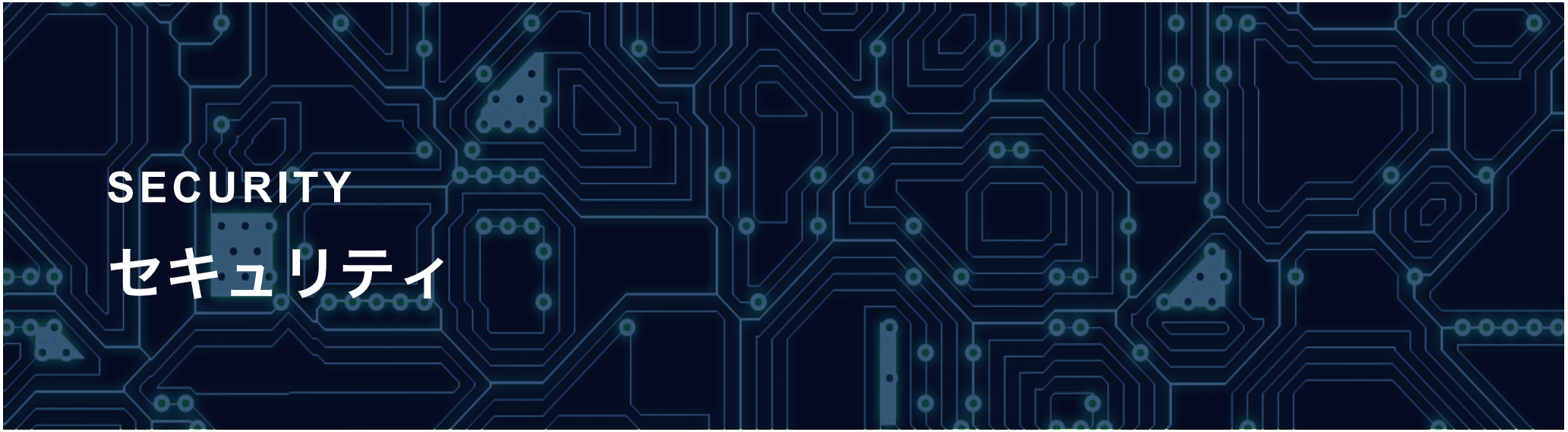


06 災害対策

災害や停電などが発生した場合でも、業務を止めることなくサービスを使い続けることが可能です。

07 ヒューマンエラー対策

人による不注意やプログラムの設定漏れなど、ミスが発生しにくい体制で運用を行ってます。



SECURITY
セキュリティ

お客様のポリシーに応じて設定できるよう、さまざまなセキュリティに関する機能を提供しています。

セキュリティインシデント対応専門のチームを設置し、セキュリティインシデントに迅速に対応します。

不正アクセス対策

複数のユーザー認証プロセスでセキュリティを強化

不正ログイン対策

複数のユーザー認証プロセスでセキュリティを強化

脆弱性対策

製品のセキュリティを強化するための取り組み

複数のユーザー認証プロセスで
セキュリティを強化

不正アクセス対策　不正ログイン対策

Basic 認証

通常のログイン画面に、さらにアクセス制限を加えることができます。Basic 認証設定を行うと、Basic 認証のログイン名・パスワードを知っている人のみ「弊社が提供する sAI Search もしくは sAI Chat の管理画面」のログイン画面にアクセス可能となります。

各サービスの URL へアクセス

Basic 認証のログイン名・パスワードを入力

ログイン名・パスワードを入力

二重のログイン認証を経てサービスを利用できる

IP アドレス制限

アクセスできる IP アドレスを限定し、想定外のアクセスをシャットアウトできます。

独自サブドメイン

個別のサブドメインを発行することで、企業ごとに異なるログイン URL でアクセスできます。

監視ログの通知

ログインやファイルのダウンロードなどの操作や監査ログの閲覧 / ダウンロードできます。また監査ログは重要度（レベル）に応じて、指定したメールアドレスに通知メールを送信できます。

日時	接続元	ユーザー	サービス	モジュール	アクション	結果
2019-04-22:14:49:05	XX.XXX.XXX.XXX	ando	sAISearch	Basic system	login	SUCCESS
2019-04-22:13:37:45	XX.XXX.XXX.XXX	ando	sAISearch	Basic system	login	SUCCESS
2019-04-22:12:37:41	XX.XXX.XXX.XXX	ando	sAISearch	Messages		FAILED
2019-04-22:12:37:06	XX.XXX.XXX.XXX	ando	sAISearch	Basic system	login	SUCCESS
2019-04-22:12:32:08	XX.XXX.XXX.XXX	ando	sAISearch	To-Do List	modify	SUCCESS
2019-04-22:10:41:20	XX.XXX.XXX.XXX	ando	sAISearch	BulletinBoard	create	SUCCESS

情報資産の暗号化

個人情報に該当する情報は暗号化して保存しています。

個人・機密情報の漏洩防止策

FW 及びサーバー側のアクセス制御機能を用いて外部からのアクセスを遮断し、重要データは表領域単位で暗号化しています。

パスワードポリシー

パスワードの文字数は 8 文字以上、アルファベットと数字を含めるという比較的厳しい基準を設定しております。

BLOCK!

悪意のあるサイトによる情報集出を防ぐ機能

クリックジャッキングからの保護

悪意のあるサイトからサービスが呼びだされ、ユーザーが意図しない動作をさせる「クリックジャッキング」からの保護機能を搭載しています。

ログイン画面の画像設定機能

ログイン画面の画像を独自に設定できることで、フィッシング (なりすまし) サイトによるログイン情報の流出を予防できます。

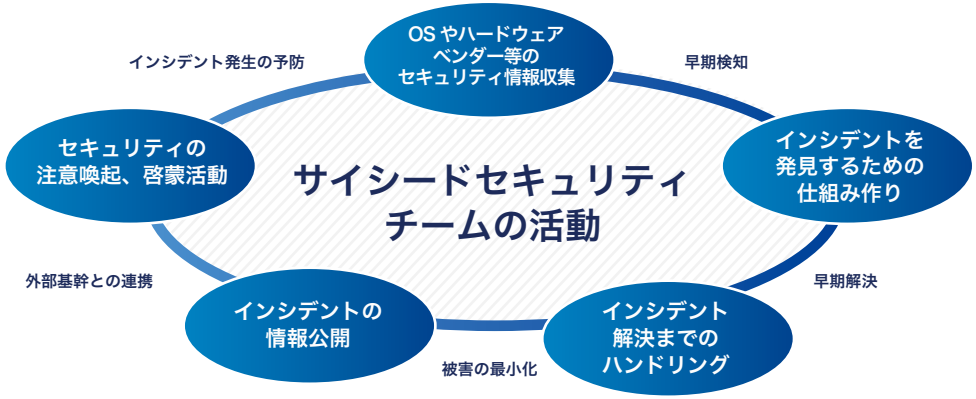
製品セキュリティを強化するための取り組み

脆弱性対策

近年、脆弱性と呼ばれるコンピュータのオペレーティングシステム (OS) や各種ソフトウェアにおけるセキュリティ上の欠陥を利用した不正アクセス等が問題になっています。
サイシードの製品および、利用している OS や他社のソフトウェアの脆弱性による被害を防止するため、サイシードでは様々な取り組みを行っています。

セキュリティインシデント対応専門チームの設置

社内外の様々なセキュリティインシデントに対応するチームを社内に設置しています。社外の組織、専門家とも協力し、インシデント発生の予防、早期検知、早期解決、被害が発生した場合の最小化を目的とした活動を行っています。



サイシード製品の脆弱性への取り組み

サイシード製品は、お客様への提供前に品質保証チームにおいて脆弱性検証を行っています。製品の内部仕様を知っている社内での検証が全ての脆弱性対応のベースになります。さらに信頼性を高めるために、外部の調査機関による監査、有識者による脆弱性発見の取り組みを行っています。

製品開発チーム
セキュアに開発するためのトレーニングなど

インフラ運用チーム
脆弱性対策へ即時に対応できる体制作り

品質保証チーム
・各製品の脆弱性診断
・外部機関と連携した脆弱性の早期発見対策

Sciseed サイシード

調査機関
第三者機関によるセキュリティ監査

外部の有識者
・脆弱性検証環境の提供
・脆弱性報奨金制度

外部機関

コンピューターの OS や他社ソフトウェア等の脆弱性への取り組み

OS や他社のソフトウェアなどの脆弱性についても、随時情報収集を行い必要に応じて対策を行います。また近年、ソフトウェアの脆弱性が発見された際、開発元による修正プログラムが提供される前に脆弱性を悪用した攻撃が開始される「ゼロデイ脆弱性」が増えています。「サイシード」では、開発元による修正プログラムの提供が遅れている場合は、自社で修正プログラムの開発を行い対処を行うこともあります。

他社のセキュリティ情報
・専門機関の情報
・各ベンダーの情報

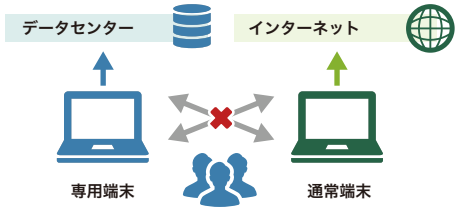
Sciseed サイシード
セキュリティチーム ⟷ 運用・開発チーム
・日々脆弱性情報を監視
・脆弱性対応のハンドリング
・脆弱性の影響を調査
・脆弱性への対応

開発中製品の試験等に用いる環境と、お客様のデータを預かる運用環境を分離しております。運用環境は一般社員はもちろん開発者もアクセスすることはできません。

社内の運用体制

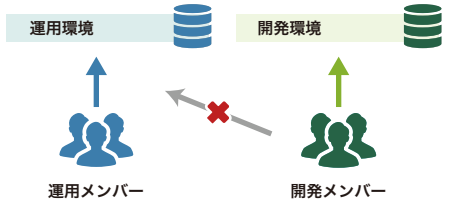
POINT 1 **データセンター接続は専用端末を利用**

運用メンバーがデータセンターに接続する際は、通常業務とは異なる、専用の端末からのみアクセスします。専用端末はインターネットに接続しておらず、インターネット経由の進入やウイルス混入のリスクがありません。



POINT 2 **開発用環境と運用環境の分離**

開発中製品の試験等に用いる環境と、お客様のデータを預かる運用環境を分離しております。運用環境は一般社員はもちろん開発者もアクセスすることはできません。



弊社では脆弱性の観点から、IE を非推奨ブラウザとしています。

脆弱性対策

各種ウェブブラウザのうち、特に Internet Explorer（IE）については、各企業や政府から脆弱性に関する多くの勧告が出されているため、
サイシードでは IE を非推奨ブラウザとしています。

Microsoft による Internet Explorer の使用停止勧告

Microsoft は、旧式のウェブブラウザである Internet Explorer（IE）の使用には危険が伴うとして、IE の使用停止を勧告すると同時に、最新ブラウザへの移行を推奨しています。この使用停止勧告の背景として、IE に関する下記のようなバグや脆弱性がこれまでに報告されています。

・2004 年 4 月：Windows ソース・コードの一部が流出

・2006 年 3 月：セキュリティホールを悪用するコードがウェブ上で公開

・2010 年 2 月：権限のない第三者に、古い OS 上の情報が閲覧可能となる脆弱性

・2012 年 10 月：IE に解放済みのメモリ領域を使用してしまうゼロデイの脆弱性

・2018 年 3 月：IE のアドレスバーに入力した全ての情報を攻撃者が閲覧できるバグ

アップデート版が提供されない業務用ウェブアプリケーションを使用する企業や団体などは、現在でも IE を使用する場合があります。しかし、Chirs Jackson 氏（Microsoft 社サイバーセキュリティアーキテクト）は、IE を使い続けるメリットは短期的な移行の手間を省くのみに止まり、長期的にみて最適の選択ではない、と述べています。

バグの発生が多いことや、これらのもたらすセキュリティ被害が比較的大きいものであることから、Microsoft は 2015 年に後継ブラウザーである「Microsoft Edge」の提供を開始しています。
これに伴い、IE7–10 のサポートは 2016 年に打ち切られています。また、2018 年 12 月には異なるエンジンが乱立する「断片化」を防ぐため、Chromium ベースへ移行すると発表し、2019 年 6 月にそれをリリースしました。

このような事実を踏まえ、現状では、多くのウェブアプリケーション開発者は IE の表示互換性を考慮していません。そのため、IE でのみ使用可能な業務用・産業向けのウェブアプリケーションを使う場合を除き、モダンブラウザーへの移行がセキュリティ面でもコスト面でもより良い選択であると考えられています。

McAfee による Internet Explorer の脆弱性に関する報告

セキュリティ企業の McAfee は、Google が過去に受けた組織的なサイバー攻撃に関して、Microsoft の Internet Explorer（IE）に存在する新たな脆弱性が利用されていたことが分かったと報告しました。
McAfee は被害に遭った組織や捜査当局と連携してこの事件について調べており、攻撃側が複数の悪質コードを使って標的とする組織に侵入しようとしていたことを確認しました。このコードを分析したところ、IE の一般には知られていない脆弱性を突いたものが 1 つ見つかったとしています。この脆弱性は Windows 7 を含む Microsoft の主要 OS すべてに影響するといい、McAfee は Microsoft にこの情報を提供しました。

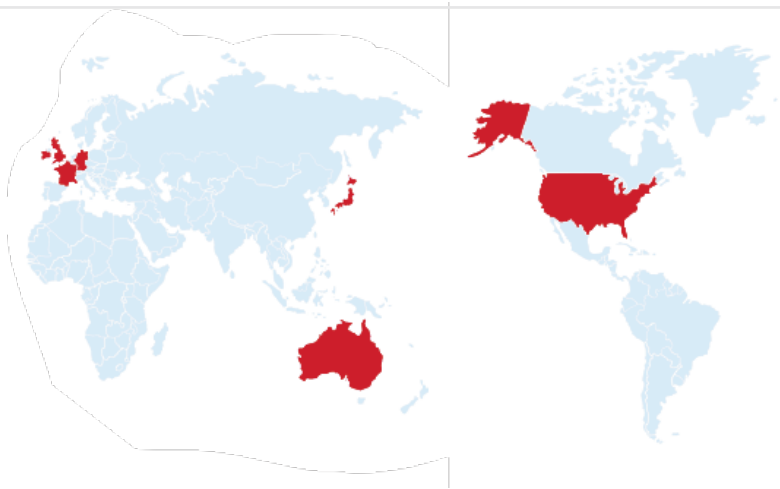
McAfee によると、今回のような標的を絞った攻撃のほとんどは、標的とする組織の中の特定の個人を狙ってファイルやリンクを送りつけ、信頼できる相手から届いたものと思わせてクリックさせる手口が使われる傾向にあります。今回の場合もこの方法で、IE の脆弱性を悪用し不正侵入を試みたと見ています。

各国政府による Internet Explorer の使用注意・停止勧告

アメリカ・イギリス・オーストラリア
2014 年に、アメリカ国土安全保障省（US-CERT）は Microsoft 製ブラウザ「Internet Explorer（IE）」でセキュリティ上の脆弱性が見つかったとして、不具合が改善されるまで使用を控えるよう勧告すると同時に、別のブラウザを使用するよう推奨しました。
イギリスのナショナル・コンピュータ緊急対応チーム（CERT-UK）や、オーストラリア政府のサイバーセキュリティ情報を提供するウェブサイト「ステイ・スマート・オンライン」も、US-CERT と同様の勧告を発表し、ユーザーに注意を呼びかけました。

フランス・ドイツ
2010 年に起きた Google へのサイバー攻撃事件時に、フランスの政府機関 CERTA は、Microsoft が修正プログラムを公開するまで IE の使用を控えるよう、国民に警告を発しました。
フランス政府同様、ドイツ政府におけるコンピュータ・通信のセキュリティ担当部門である「BSI（Bundesamt für Sicherheit in der Informationstechnik）」は、公式に発表したプレスリリース内で IE の脆弱性について触れ、高度なセキュリティを確保維持するためにはこの脆弱性が修正されるまで IE を使わない方が安全であると IE 以外のブラウザへの一時的な乗り換えを推奨しました。

日本
2014 年に、経産省所管の情報処理推進機構は、PC の情報搾取や遠隔操作、組織システムへのウイルス侵入・感染に繋がるような脆弱性が IE で見つかったとして、IE の使用に関する注意喚起を発表しました。



OPERATION BASE
運用基盤

機械は壊れる、人はミスをする、
ソフトウェアにはバグがある

クラウドサービスで最も大切なことは、お預かりしたデータの管理体制にあるとサイシードは考えています。
障害で万が一の事故が起こっても、お客様のデータを守り、安心してご利用いただくために「サイシード」はハードウェアやオペレーションなど様々な面で安全を確保しています。

データ消失対策
お客様のデータを守るためのバックアップ体制

災害対策
高い信頼性のデータセンターで災害時のリスクを低減

障害検知・復旧対策
もしもの障害も自動で検知、防止

ヒューマンエラー対策
ヒューマンエラーを防止する運用体制

お客様のデータを守るためのバックアップ体制

データ消失対策　災害対策

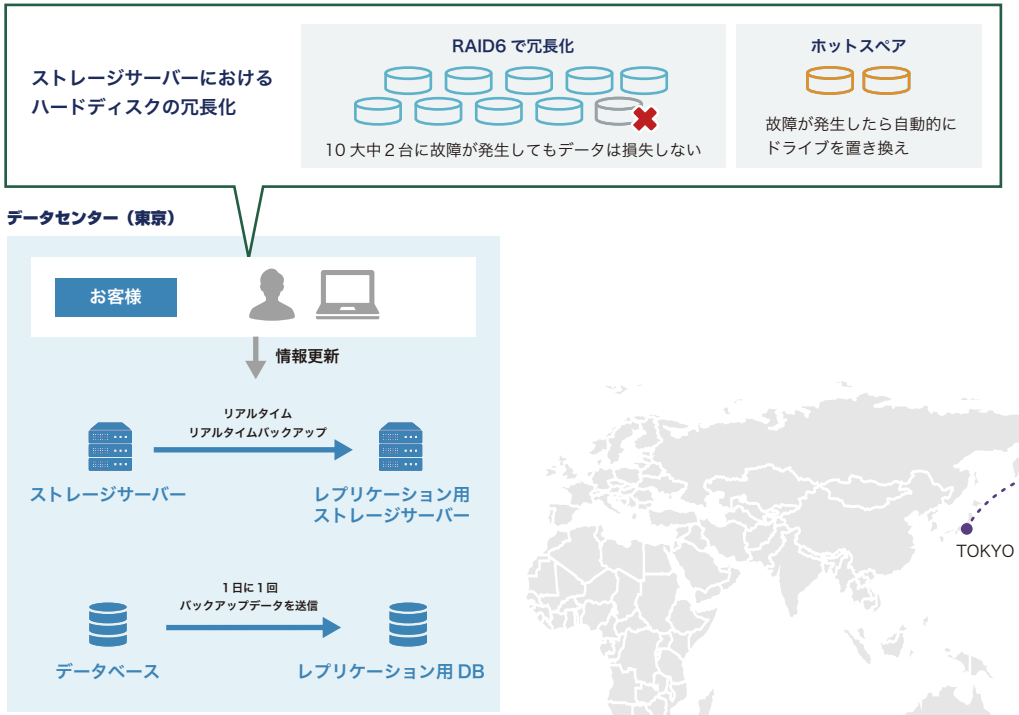
弊社は AWS のデータベースを利用しているため、データを守るためのバックアップ体制も AWS のセキュアなガイドラインに準じております。
AWS が利用するデータセンターの拠点は、環境評価および地理的評価を実施し、洪水・異常気象・地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。
弊社は「東京リージョン」と「オレゴン」もしくは「オハイオ」を併用しております。

ハードディスクの冗長化（RAID6）

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。
重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに充分な能力が存在することになります。

バックアップ専用サーバーによる 14 日分の差分バックアップ

データセンターには、お客様が普段使うストレージサーバーと冗長化のためのレプリケーション用ストレージサーバーだけでなく、バックアップ専用のストレージサーバーが用意されています。1 日 1 回それぞれのサーバーからデータを受け取っており、過去 14 日分のバックアップデータが保管されています。バックアップ専用のストレージサーバーがあることで、他のストレージサーバーのデータがすべて破損した場合でも、前日までの環境を復元させることが可能です。毎日復元のための試験を実施しており、きちんと復元できるよう日々の運用でもチェックしています。



ISO/IEC 27001:2013、27017:2015、および 27018:2014 への準拠の認定

AWS はセキュリティ管理のベストプラクティスと包括的なセキュリティ制御を規定したセキュリティ管理標準である「ISO/IEC 27001:2013 は、ISO/IEC 27002」への準拠の認定を受けています
この認証の基礎は強固なセキュリティプログラムの開発と実装であり、これには、AWS がどのようにしてセキュリティを全体的で包括的な方法で永続的に管理するかを定義する、情報セキュリティ管理システム (ISMS) の開発と実装が含まれます。

高い信頼性のデータセンターで災害時のリスクを低減

災害対策

AWS の事業継続計画は、災害時のサービス障害の回避および軽減措置について記載されています。それには、災害が起こる前、災害の最中、および災害後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

設備のメンテナンス

AWS は電気および機械に関連する設備をモニタリングし、予防的なメンテナンスを実施して、AWS データセンター内のシステムの継続的な運用性を維持しています。機器のメンテナンス手順は資格を持っている担当者が実行し、文書化されたメンテナンススケジュールに従って完了されます。

パンデミックへの対応

AWS は、感染症の爆発的な流行の脅威に対して迅速に対応するための準備として、パンデミック対応ポリシーと手順を災害復旧計画に組み込んでいます。関連したリスクに関する軽減のためのストラテジーには、重要なプロセスをリージョン外のリソースに移動するために、どのようにスタッフを配置するかという代替モデルと、重要なビジネス業務をサポートするための危機管理の発動計画が含まれます。パンデミック計画は、国際的な健康関連機関や規制に従っていますが、国際的な関連機関との連絡窓口等も含まれています。

ハードディスクは物理的に破壊

ユーザーデータの保存に使用されるメディアストレージデバイスは AWS によって「クリティカル」と分類され、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。
AWS では、デバイスの設置、修理、および破棄 (最終的に不要になった場合) の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄します。
ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制から除外されることはありません。

お客様のデータを守るための バックアップ体制

BACK UP 1

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。
そうした重要なシステムコンポーネントは、アベイラビリティーゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティーゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。
アベイラビリティーゾーンはお互いに接続されているため、アベイラビリティーゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。
これにより、高いレジリエンシーと、サービスの可用性がもたらされることになりますが、それは自ずとシステムデザインの一部として機能することになります。アベイラビリティーゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

BACK UP 2

従業員によるデータセンターへのアクセス

AWS は、権限を持つ担当者のみにデータセンターへの物理的なアクセスを許可しています。データセンターへのアクセスを必要とするすべての担当者は、まずアクセスを申請し、業務上の正当性を詳しく説明する必要があります。これらの申請は最少権限の原則に基づき許可されますが、個人がアクセスを必要とするデータセンターのレイヤーを指定する必要があり、アクセスの期限が設定されます。申請は権限を持つ人物のみが審査して承認し、請求した期限が過ぎた後は、アクセスが取り消されます。入場を許可された担当者は、その権限で指定されたエリアのみに入場が制限されます。

BACK UP 3

キャパシティの計画

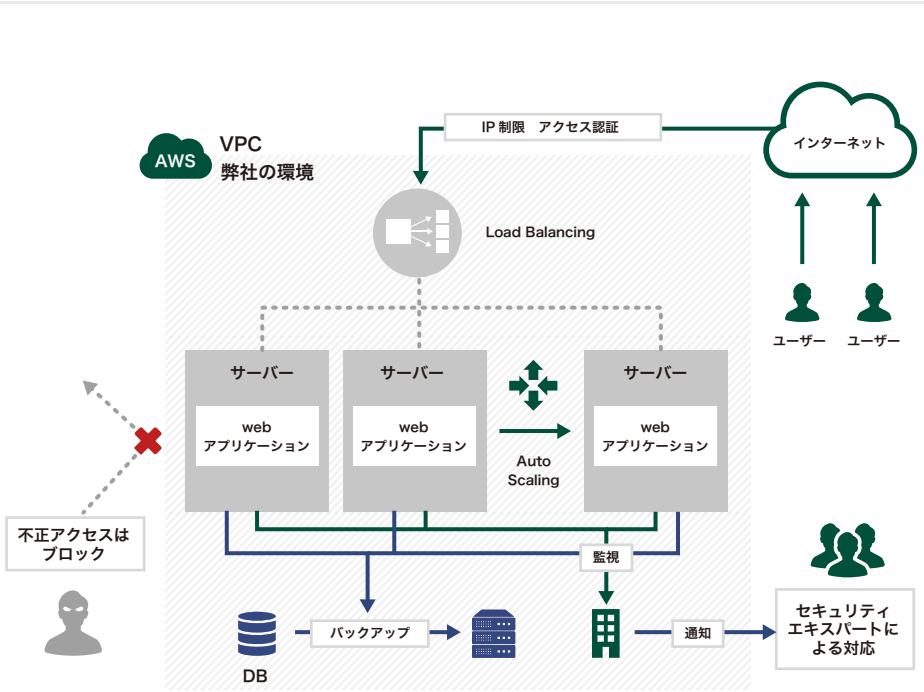
AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティーに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティープランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

BACK UP 4

データセンターへのアクセスの監視

AWS ではグローバルセキュリティオペレーションセンターを使用してデータセンターを監視しています。このグローバル・セキュリティ・オペレーションセンターは、モニタリング、対処優先順位の決定、および決定された処理を実施について責任をもっています。データセンターのアクセスを管理、モニタリングし、ローカルのチームと関連サポートチームと協力し、対処優先順位の決定、コンサルティング、分析、送信を行い、24 時間 365 日グローバルレベルのサポートを提供しています。

システム概略図

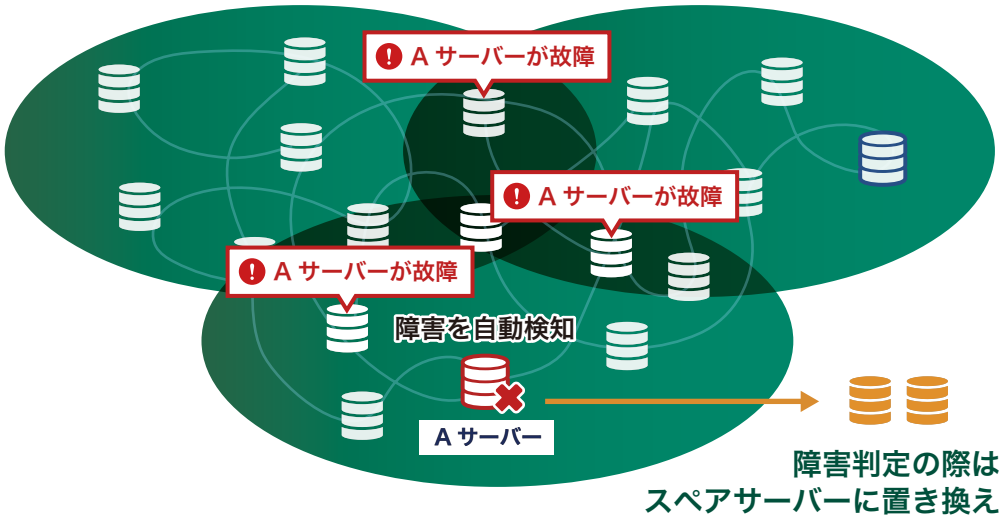


もしもの障害も
自動で検知、防止

障害検知・復旧対策

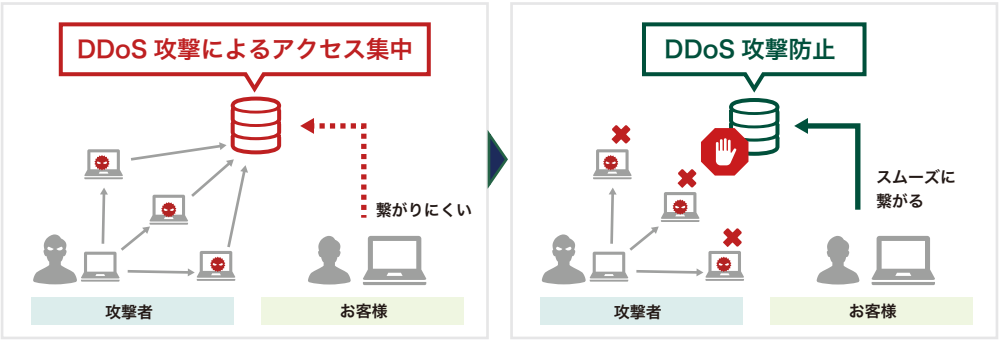
自動障害検知・回復システム

「サイシード」では、各種サービスのプログラムや Web サーバーが稼動している仮想サーバーの障害に備えて、「自律分散エージェントシステム」を構築しています。異常検知を素早く行うためにサーバー同士が相互に監視し合い、万一の時には合議の上で障害か否かを判断します。障害として判断された場合は、速やかにスペアサーバーに置き換わる自動復旧プロセスが開始され、通常であれば 5 分以内に回復する仕組みになっています。また、ネットワーク障害などで短時間に多数のサーバーが異常を起こした際には、連鎖障害を防止するモードに移行します。



DoS 攻撃、DDoS 攻撃の防止

特定のサブドメイン (URL) に対して短時間にアクセスが集中した場合は、自動的に該当するサブドメインを停止し、他の環境へ影響が及ばないようにする仕組みを採用しています。また、そのほか自動死活監視システム、自動侵入検知・防止システムも備えています。

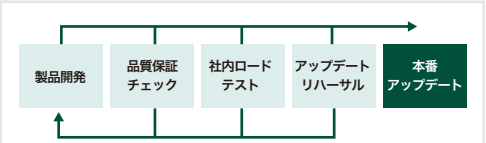


ヒューマンエラーを
防止する運用体制

ヒューマンエラー対策

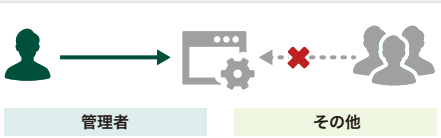
サービスアップデートまでの体制

サービスのアップデートをする際は複数回のテストを実施し、合格したもののみお客様の環境に適用しています。



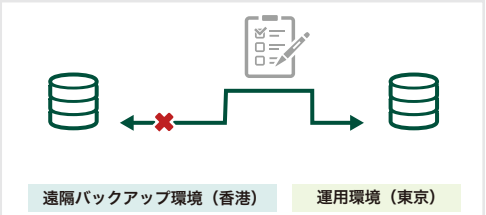
機密情報へのアクセス権限者を限定

弊社内に厳重に保管された専用 PC から、一部の管理者権限を持ったシステムアドミニストレータのみがアクセス可能



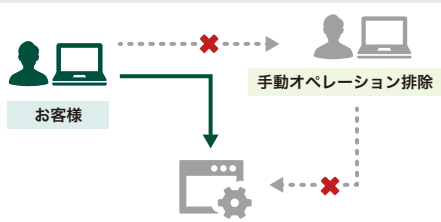
遠隔バックアップデータの分離

運用環境と遠隔バックアップ環境を「同時に」操作することができないようシステムを分離しています。そのためデータ消去に関するプログラムが万が一予期せぬ動作をした際も、遠隔バックアップデータが同時に削除されることはありません。



自動化で人による操作を低減

「サイシード」では、人的操作による手動オペレーションを可能な限り排除し、自動化しています。例えば、お客様環境の作成、サービスの追加、解約等はシステムで自動化しています。

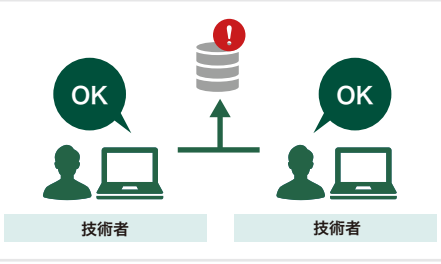


手順書の遵守とログの自動記録

手動オペレーションによる操作は、すべて手順書を整備しており、手順書に従って実施することを徹底しています。また、全ての操作はログを自動記録しており、ルールが守られているかチェックできる体制となっています。

緊急時も単独での操作禁止

例外として、障害発生時等緊急時には手順書を伴わない手動オペレーションを許可しています。ただし、どのような場合も技術者単独の操作を認めておらず、2 人以上の技術者が確認の上で操作を行っています。



運用環境

サービスレベル目標（SLO）

「サイシード」で提供されるサービスは、お客様に安心して快適にご利用頂けるよう下記のサービスレベルを目標に定め、運用しています。

- **稼働率：**99%
- **障害復旧時間：**60 分以内
- **アクセスログ保存期間：**オンラインで 1 年間

セキュリティ

● データ暗号化

伝送データについては全て暗号化しています。

● 脆弱性対応

第三者機関による脆弱性試験を定期的に実施しています。

可視性および信頼性

● サービス提供時間

24 時間 365 日 (定期メンテナンス等の計画停止を除く)
なお、「サイシード」は日本時間の毎月第 1 月曜日午前 10 時～午後 3 時の間に定期メンテナンスを実施いたします。(定期メンテナンス中もサービスはご利用いただけます。)

● 計画停止

1 週間前にログイン後のトップページにて通知します。

● 冗長化

全てのサーバー、ネットワーク、ストレージ、データについて冗長化を実施しています。

障害時の対応

障害通知のシステム監視を常時実施し、障害発生時には運用マニュアルに沿って対応します。

バージョンアップ

サービスのバージョンアップは全テナント一斉に実施します。

データ管理

● データセンター所在地

「サイシード」は AWS の東京リージョンで運用し、シンガポールリージョンのデータセンターにもバックアップデータを保管しています。

● バックアップ

お客様のデータは毎日無停止でバックアップを作成しています。

● データの消去

解約の翌日から 30 日後にデータを消去します。バックアップデータはデータの消去から 2 週間程度で完全消去いたします。

● 管理者の扱い

弊社内情報セキュリティポリシーで定めた管理体制に沿って、データにアクセスできる管理者を制限しております。

● お客様の保存データの取扱い

サービス上に登録されたお客様の「保存データ」はお客様ご自身により管理されるものであり、サイシードは許諾された範囲を除き一切の権利を有しません。

サポート

● 提供時間

平日 午前 9 時～午後 6 時
※年末年始を除く

● 提供手段

電話・E メール

運用責任者

株式会社サイシード

CTO **西田圭嗣**

東北大学工学部卒業、スイス連邦工科大学ローザンヌ校修士課程修了。人工知能、自然言語処理を専門とする。AI 関連商品全体のエンジニアリングを統括。

Sciseed　株式会社サイシード

※ 製品に関するお問い合わせはホームページへ ⇒ https://saichat.jp
※ sAI Search、sAI Chat、sAI Builder 及びサイシードのロゴマークは株式会社サイシードの登録商標です。
※ 記載された商品名、各製品名は各社の登録商標または商標です。
　また、当社製品には他社の著作物が含まれていることがあります。
　個別の商標・著作物に関する注記については、こちらをご参照ください ⇒ http://saichat.jp/

本カタログの記載事項は変更になる場合がございます。

2019 年 10 月現在（第三版）