大学・病院・企業の大規模サイト向け
ITインフラサービス

CYPOCHI CLOUD SERVICE

株式会社 サイポチ

〒102-0082　東京都千代田区一番町15-8 壱番館４階
TEL：03-6240-9841
https://www.cypochi.co.jp
https://www.cypochi.com

ISO / IEC 27001
情報セキュリティマネジメントシステム（ISMS）適合性評価制度
ISO / IEC 27001:2013　認定 - 認証登録番号 :11155

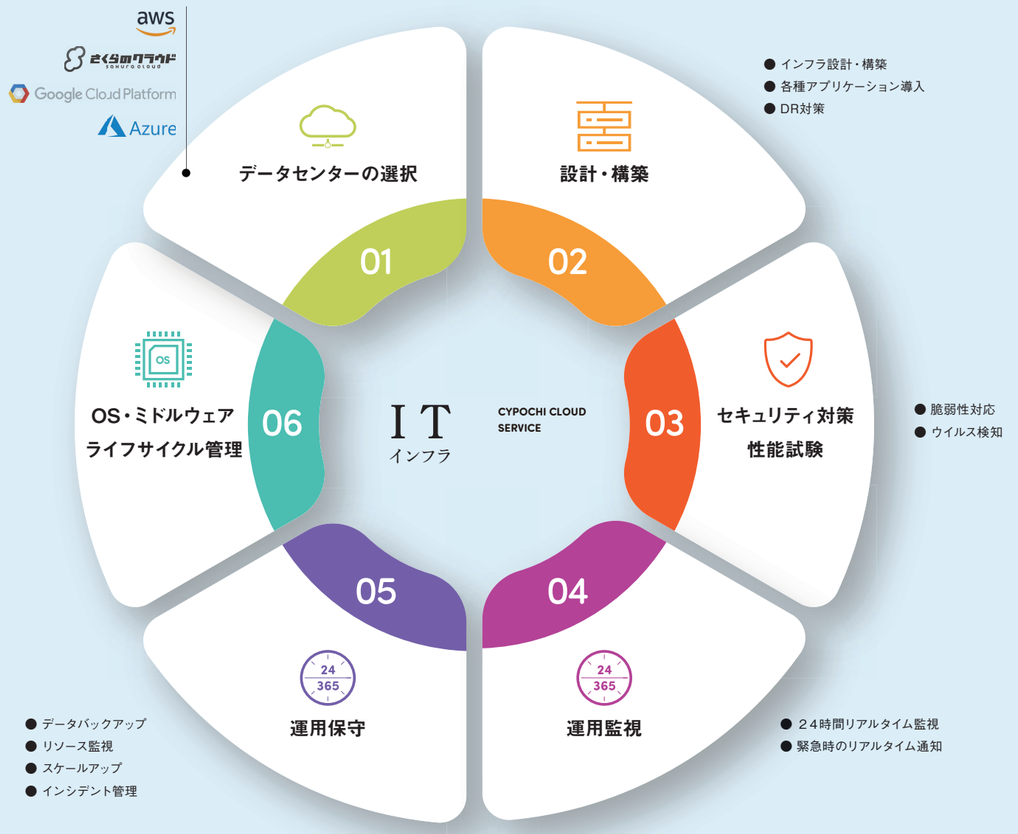
ISO27001:2013 認証取得

2022.02-1500

CYPOCHI

日々増大するインターネットの脅威から
お客様のITインフラを守り、
より安全・安心・快適な環境を提供します。

CYPOCHI CLOUD サービスは、海外・国内データセンターのクラウドサービスを利用して、大規模なITインフラの設計・構築・保守を行なっています。
これまで、情報システムご担当者様を悩ませてきた、セキュリティ対策、バージョン管理、アクセス集中時の対応、運用に応じた拡張、災害時の事業継続性等を低コストで解決し、「ゼロ情シス」を支援します。



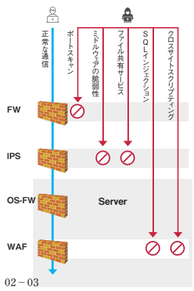
導入サービス　No.01 – No.12

01

インフラ設計・構築

運用に最適なインフラ設計・構築を行っていきます。ロードバランサ、サーバ、オートスケール、ストレージ、データベース、バックアップ、監視等、安定稼働を実現するプランをご提案させていただきます。

02 – 03



ファイアウォールの設定

OSに搭載されたファイアウォールで、攻撃によって意図しない動作を引き起こすリスクを最小化します。
お客様の要件に合わせて、最適なファイアウォール設定を実施します。

WAFの導入

WAFとは、WEBアプリケーションファイアウォールの略称で、リクエストが到達する前に、問題があればリクエストを拒否する仕組みのことです。これにより、一定の脆弱性を防御できます。

04

ウイルス対策

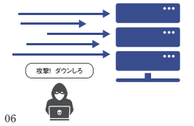
ウイルス対策ソフトを導入し、ウイルスやスパイウェアをリアルタイムに検出し、WEBサイト利用者のパソコンからの感染や、WEBサーバからWEBサイト利用者のパソコンへの被害拡大を防止します。

05

サーバ情報の隠ぺい

悪意のあるサイバー攻撃者は、使われているサーバのバージョン情報を基に、脆弱性を狙い、攻撃を仕掛けてきますので、万が一に備えバージョン情報を非表示にし、攻撃するチャンスを与えないようにします。

06



DoS・Brute Force攻撃対策

大量アクセスで、WEBサーバの機能低下を狙うDoS/DDoS攻撃、ログインパスワードを総当り攻撃してくるBrute Force攻撃に、サーバソフトウェアへのDoS・Brute Force対策モジュールを導入します。

07

各種アプリケーション導入

CMSやFORMなどの各種アプリケーション導入を行います。CYPOCHI AIRのアプリケーションをご利用される場合は、インフラもアプリも常に最新の環境が維持されます。

08

脆弱性試験

OS、ミドルウェア、アプリケーションの脆弱性に対する攻撃を考慮した上で各種対策を行います。サーバ構築とアプリ導入後に脆弱性試験を行い、問題が無いことを確認します。

09

サーバ監視と自動復旧

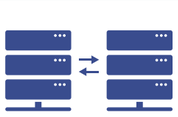
サーバが正常に稼動しているのか、24時間365日監視とサーバがダウンした際の自動復旧設定を行います。
また、運用前に監視や自動復旧が正しく動作するかの確認を行います。

10

インフラ性能テストと最適化

サーバへの負荷テストを行い、スループット、レスポンスタイム、リソース使用量の3つの評価を行います。平常時、ピーク時のアクセスに対応できるようにバランスよくチューニングを行います。

11



バックアップ試験

導入サービスの最後に、バックアップやウイルス検知が設定した周期で正常に実行されるかの確認とバックアップしたデータやアプリを復元し、正常に動作するかの試験を行います。

12

DR（ディザスタリカバリ）対策

自然災害、大火災などの緊急事態に遭遇した時に、WEBサイトの運営を継続させるインフラ対策です。
運用サーバと離れたエリアにバックアップを行い、災害発生時における復旧の手段や計画を整えます。

運用サービス　No.13 – No.18

13

モニタリング監視

サーバが正常に稼動しているか、24時間365日監視を行っていきます。サーバの異常を検知した際は、アラート通知で重要度を判定し、状態復旧まで素早く障害に対応していきます。

14

日々の脆弱性対応

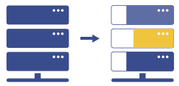
最新のセキュリティ情報を「JPCERT」、「RedHat Errata」、「JVN」等の専門機関から入手し、OS、ミドルウェア、WEBアプリケーションへの適切な脆弱性対策（バージョンアップ等）を行っていきます。

15

ウイルス検知

導入したウイルス対策ソフトによって毎日定期的にウイルスチェックを実行します。ウイルスやスパイウェアを迅速に検出します。

16



データバックアップ

万が一のデータ紛失や重大な障害が発生した際、速やかに障害復旧が行えるように、定期的にデータのバックアップを行います。サーバデータはバックアップ用の別ディスクに安全にバックアップされます。

17

リソース監視とスケールアップ

サーバのメモリ、CPU、ディスクの消費量に応じて、スケールアップのご案内をしています。
また、受験シーズンなど高負荷時の一時的なスケールアップ対応も行っています。

18

インシデント管理

運用への影響を最小限に抑え、迅速な障害対応を図る目的で、インシデントを一元管理していきます。インシデントを分類・レベルで分けて対応状況を可視化していきます。

障害発生時　No.19 – No.21

19

24/365レスキュー対応と自動復旧

24時間365日のレスキュー対応では、サーバ停止等を自動検知し、自動復旧を試みるシステムを設定しています。サービス停止時間を最小限に抑えることが可能です。

20

復旧作業

専任のエンジニアが、リモートで状況の把握と原因特定をして、障害の切り分けと対応にあたります。作業手順書に従い、復旧作業を進めていきます。

21

障害報告・復旧完了報告

障害発生時の報告、復旧作業での進捗報告、復旧完了報告など、適時必要な報告を行います。また、障害報告はインシデント管理にも記述していきます。

障害発生時の対応フロー