Datamanegy HR

セキュリティガイド

Charlotte Datamanegy HR
HRデータ統合プラットフォーム

2024年7月1日現在（ver.1.0）

Datamanegy HR セキュリティガイド

2024年7月1日現在

データセンター		
建屋等		
1	データセンターの所在地はどこですか？	日本(関東、関西リージョン)
2	データセンター専用建物ですか？ (耐震・免震構造など)	データセンター専用建物となっております。
3	給電ルートは冗長化されていますか？	複数系統の電力ルートを持ち、自家発電及びUPSがあります。
4	無停電電源(UPS)や、非常用電源の用意はありますか？	有
5	火災感知・報知システムはありますか？	有
6	不正侵入対策はされていますか？	有
マシンルーム等		
7	サーバーマシンルームとオペレーションルームは分離されて いますか？	分離されております。
8	入退室管理はされていますか？	有
9	入退室記録は保存されていますか？保管期間は？	有(保管期間は非公開)
10	社員証やバッチなどにより、構内従業者と訪問者の区別は 外見から行えるような措置が取られていますか？	有
11	サーバールーム内を監視するカメラ設備はありますか？	有
12	十分な空調設備は備わっていますか？	有
13	サーバルーム内消火設備はありますか？	有
その他		
14	第三者セキュリティ認証は何を取得していますか？	FISC、PCI-DSS、HIPAA、ISMAP、SOC1、SOC2
15	ユーザ企業の監査の受け入れは可能ですか？	データセンターの監査は、いかなる理由があっても禁止されております。

Charlotte及び周辺サービスは、『Oracle Cloud Infrastructure』上で稼働しております。
Oracle Cloudのデータセンターに関する情報は、下記公開資料や日本オラクル株式会社様へ個別にヒアリングした結果を元に作成しております。
より詳細な情報確認は下記情報をご参照ください。

『Oracle Cloud Infrastructure Security Architecture』
https://docs.oracle.com/cd/F34086_01/oci_security_jp.pdf

安全管理措置		
サーバー		
16	サーバーに対するウィルス対策や不正アクセスなどに対する 対策は施されていますか？	ウィルス対策ソフト及びWAF及びIPS/IDSを導入しており、定期的なウィルススキャン、 アップロードファイルへのリアルタイムスキャンを実施しております。
17	OSのセキュリティパッチの適用を実施していますか？	新バージョンリリース後、下記の手順にて30日以内に本番環境への適用を実施しております。 ①適用要否を検討する。 ②適用が必要な場合、テスト環境にて無影響確認を実施する。 ③影響がないことが確認できた場合、本番環境へ適用する。
18	ソフトウェアのセキュリティパッチの適用を実施していますか？	セキュリティパッチは1日1回以上自動適用しております。

安全管理措置		
サーバー		
19	不正アクセスに対する防御および監視を実施していますか？	IPS/IDSのログを監視システムにて常時監視しております。
20	各種脆弱性攻撃への対策は行っていますか？	IPAで設定されているセキュリティ基準に基づき、各種対策を実施しております。
21	脆弱性診断を実施していますか？	月2回の内部脆弱性診断、年1回の外部脆弱性診断を実施しております。
22	インターネットとの境界にファイアウォールが設置されていますか？	有
23	必要な通信ポートのみに制限されていますか？	不要な通信ポートは閉塞しております。
24	ファイアウォールの設定内容や設定ファイルは定期的に確認管理されていますか？	定期的に設定ポリシー管理を実施しております。
25	DMZは設置されていますか？	DMZを設置しております。
ネットワーク		
26	通信の安全性は実装されていますか？	Charlotteへの通信は全てTLS1.2による暗号化を行っております。
27	なりすまし対策はされていますか？	EV SSL証明書を適用しております。
データ保管		
28	データの暗号化は実施されていますか？	データは全て暗号化保存されています。
29	バックアップは取得されていますか？ またその取得周期、世代数、保管場所は？	バックアップを取得しております。 ・周期：毎日夜間 ・世代数：30世代 ・保管場所：データセンターと別筐体
30	遠隔バックアップは取得されていますか？ またその取得周期、世代数、保管場所は？	遠隔バックアップを取得しております。 ・周期：週次 ・世代数：5年間 ・保管場所：バックアップ筐体と別筐体
31	解約後、復元不可能な状態で環境の削除を行っていますか？ 行っている場合、削除までの期間は？	復元不可能な状態で環境を削除しております。 削除までの期間は解約後5営業日以内です。
障害対策		
32	障害を監視していますか？	監視システムにてサーバ死活、リソース、アプリケーションログを常時監視しております。
33	どのようなログを取得していますか？またその保管期間は？	ログ種類：操作ログ、アクセスログ、エラーログ、保護システム（ウイルス対策システム、侵入検知システム、改ざん検知システム）のイベントログ 保管期間：それぞれ5年間
34	ログの正当性を担保するため、時刻の同期をしていますか？	NTPサーバとクロック同期しております。
その他		
35	ID/PW以外に、ログインに必要なものはありますか？	ID/PWの知識認証以外にCharlotteキー（※）という独自のキーファイルによる多段階認証が必要です。 ※特許取得済：特許第7015030号 また、オプションでSSO認証によるログインを必須とすることも可能です。
36	株式会社ユー・エス・イー（Charlotte推進室）として取得している認証はありますか？	Pマーク、ISMS、ASPIC