

情報セキュリティチェックシート

株式会社エヌ・ティ・ティ・シー・コミュニケーションズでは、法令及びその他の規範を遵守し、情報セキュリティへの取組みを行っております。本チェックシートは、当社ならびに当社のサービスについて、そのセキュリティ対策を記載したものです。

なお、記載事項は運用や改善のために変更する場合があります。

対象サービス：SuiteX、メールホスティング、SuitePRO

クラウド事業者名：株式会社エヌ・ティ・ティ・シー・コミュニケーションズ

最終更新日：2021年08月26日

	確認項目	回答	詳細
サービス概要	クラウドのサービス名称	WebARENA	
	クラウドのサービス開始年月日（年は西暦で記載）	SuiteX 2008年2月 メールホスティング 2012年3月 SuitePRO 2015年6月	
	クラウドサービスの内容・特徴	WebARENAは、NTTPCコミュニケーションズが提供するレンタルサーバーとデータセンターのサービスブランドです。 1997年のハウジングサービス開始以降、ホスティングサービス、メールサーバー、VPS、データセンターサービスを提供してきました。 またドメイン取得サービスやネットワークサービスとも連携し、お客様のビジネスの効率化、拡大をサポートします。	
	ISMS認証を取得している	○	ISO27001認証 認証番号：IS 89520 初回登録日：2005年2月10日
	過去2年間でセキュリティに関する事件・事故を起こしていない	○	
契約内容	サポート体制、受付/対応時間	日本語/10:30-16:30 有人チャット※SuitePRO技術サポート除く (年末年始・土日・祝祭日を除く) 24時間365日Webフォーム、チャットボット	
	故障通知のプロセスがある	○	Web掲載 https://support.nttpc.info/webarena/arenaall/ 連絡先メールアドレスへの通知
	故障検知後、指定された連絡先に通知するまでの時間が定められている	○	以下通知時間目安を設けております。 ・Web掲載 弊社検知後30分以内 ・連絡先メールアドレスへの通知 60分以内
	メンテナンス等の一時的サービス停止時の事前告知利用者への通知を実施している	○	工事実施日の約2週間前を目安としております。 Web掲載 https://support.nttpc.info/webarena/arenaall/ ただし、緊急やむを得ないときはこの限りではありません。
	サービス提供終了時の予定通知がなされるか、事前通知を実施している	○	基本サービスの重要な変更又は終了のときは、書面その他の方法をもって該当する基本サービスの契約者に対し、変更又は終了する3か月前までに通知します。 ※詳細はWebARENA共通利用規約「第1章 第6条（サービスの終了）」を参照願います。 https://web.arena.ne.jp/pdf/CommonAgreement.pdf
	個人情報を定められた目的以外で収集・利用・提供・開示することを禁止している	○	個人情報保護方針（プライバシーポリシー） https://www.nttpc.co.jp/company/effort/privacy.html
	サービス契約終了後、バックアップを含めたデータ削除の期間が明確になっている	○	契約終了時、サーバー上のデータは消去されます。 ※WebARENA共通利用規約「第7章 第4.1条（データの消去）」 https://web.arena.ne.jp/pdf/CommonAgreement.pdf お客様にてご用意されたWebコンテンツ、メールデータなどは、お客様までの管理となりますので、ローカル環境へのバックアップなどを、お客様にて実施していただく必要があります。
サービスの利用終了後、データ削除作業に対する廃棄証明の発行をしている	×	廃棄証明書の発行は行っていません。	
環境セキュリティ	データセンターの所在地はどちらですか	東京都内	
	Tierレベルはいくつですか	Tier3相当の設計をしております。	
	免震構造、制震構造、または耐震構造等の地震対策がされている	○	免震構造の建物内にて運用しています。
	直撃雷、または誘導雷対策等の避雷対策が実施されている建物である	○	
	入退室の権限付与を必要最小限にしている	○	
	機器の盗難対策を実施している	○	
	外部記憶媒体の接続制御（書き出しなど制御）を実施している	○	
	入退室履歴を記録している	○	
	入退室記録のチェックを実施している	○	
	機器操作を記録している	○	
	機器操作記録のチェックを実施している	○	
書類や記録媒体を内蔵している装置の廃棄手順を定めて、適切に処分している	○		

技術的セキュリティ	機密情報へのアクセス権限は、ID・パスワードその他の方法により適切に管理されている	○	
	機密情報へのアクセス記録を取得している	○	
	機密情報へのアクセス権限付与を必要最小限にしている	○	
	コンピュータウイルス対策は適切なルールに沿って実施されている	○	
	ファイアウォールによる外部からの不正アクセス防止など、機密情報の管理区分の設定及びアクセス制御を実施している	○	
	従業員と非開示契約を締結または秘密保持誓約書を取得している	○	入社時ならびに退職時に守秘義務を盛り込んだ誓約書の提出を義務付けています。
コンプライアンス	就業規則等において機密情報の取扱いに関する規程等に違反した場合の懲戒処分が定められている	○	
	情報セキュリティに関する基本方針・規程・マニュアル等の整備している	○	情報セキュリティ基本方針 (ISO27001認証) https://www.nttpc.co.jp/company/effort/security.html
	従業員に対するセキュリティ教育を定期的に行っている	○	
	情報セキュリティに関する組織体制を設置している	○	
	情報セキュリティ事故が発生した場合の連絡体制がある	○	
	個人情報の取扱いに関する規程が定められている	○	個人情報保護方針 (プライバシーポリシー) https://www.nttpc.co.jp/company/effort/privacy.html