情報セキュリティ対策基本方針

株式会社ネットコムBB

No	対策内容	概要
1.データセンター自体のセキュリティ対策		
1.1 物理的対策		
1	データセンターへの侵入対策	データセンターへの侵入を防止するため、建物の入り口は有人監視、生体認証を始めとした高度な認証の実施、入退室ログの取得・管理などを行っている。
2	サーバルームへの侵入対策	サーバルームへの侵入を防止するため、各区画のセキュリティレベルに応じた、生体認証を始めとした高度な認証の実施、入退室ログの取得・管理などを行っている。
3	機器、外部媒体などの盗難対策	ストレージなどの機器やバックアップメディアなどの外部媒体などが盗難されないよう、建物の入り口で有人による入退室監視を実施している。
4	災害対策	地震、火災、水害、停電などの災害対策のため、ロケーションや設備に十分配慮したデータセンターが使用されている。
5	機器の障害対策	機器の冗長化やデータセンターの分散などにより、機器に障害が発生した場合でもサービスへの影響を最小限に抑える対策を行っている。
1.2 人的対策		
6	信頼できる運用者のアサイン	システムの運用者は、正規の社員のみとし、開発者のみサーバへアクセス可としている。
7	運用者のアクセス権管理	運用者は必要最低限のメンバーのみとし、DBへのアクセス、コンテンツ（HTML）のみのアクセス等で制限を行っている。
8	運用者による不正の監視・検出	運用者による不正を監視・検出するため、運用時の操作は全て記録する、複数の運用者で作業する、などの対策を行っている。
9	セキュリティ教育	業務内でセキュリティに関する講習を定期的に行っている。
2.構築システムの技術的対策		
2.1 ネットワーク		
10	通信ネットワークの強固な暗号化	全ての通信をTLS1.0以上のHTTPS通信としている。よって、送受信データを漏えいや改ざんから保護する機能を提供している。
11	通信ネットワークの信頼性と通信品質の確保	専用線により複数IXや、複数トランジットへの接続などを行うことにより、高い信頼性や通信品質を確保している。
12	DoS攻撃対応	随時アクセス過多に対してIPをブロックしている。
13	ARP Spoofing対策	静的ARPエントリ使用、ネットワークの監視、対策機能付きスイッチの利用、VLANの利用などにより、同一ネットワークへ接続できる機器は制限するなどの対策を行っている。
2.2 マルチテナント		
14	仮想化による情報隔離	OSの仮想化により、利用者間の情報を分離している。
15	マルチテナント間での攻撃対策	随時アクセス過多に対してIPをブロックしている。
16	シングルテナント対応	利用者の要求に応じて、物理的にサーバを占有するサービスを提供している。
2.3 サーバ		
17	サーバ要塞化	ホストOSやゲストOSにおいて、不必要なデーモンの停止やサービスアカウントの無効化を行うなどにより特定のサービスのみ稼働させ、アクセス制限も実施している。
2.4 アプリケーション		
18	柔軟なパスワードポリシーの設定	一定の文字数以上で、英大文字・小文字・数字を組み合わせたパスワードの設定が必要なよう、アプリケーションで制限している。
2.5 データ		
19	データの強固な暗号化	重要なデータを格納する場合は、伝送経路、ストレージ、データベースについて適切かつ強固な暗号化を実施している。さらに、ログインパスワードはDB格納時に暗号化（不可逆性）されるように対策を施している。
20	データ復元の防止	ストレージを別の利用者に割り当てる前に、無意味なデータで上書きして完全に消去している。
21	データ格納場所の確認	自社データセンターを含む国内のデータセンターを利用している。
2.6 ログ管理		
22	ログの収集と保管	ホストOS、ゲストOS、サーバ、ネットワーク機器、Webアプリケーションなどのログを収集し、重要度に応じてログの保管を実施している。
23	ログの定期的な監視、攻撃状況の検知	収集したログを定期的に監視し、不正なアクセスや処理等を迅速に検出している。
24	時刻同期	データセンター内の全ての機器やサーバを正確な時間（ntpサーバを設置）と同期させている。
2.7 脆弱性対策		
25	脆弱性診断の実施	ホストOS、ゲストOS、サーバ、ネットワーク機器、Webアプリケーションなどに対し、自社開発の脆弱性診断ツールによる脆弱性診断を実施している。
26	最新の脆弱性情報の入手と対策	最新の脆弱性情報を迅速に入手できる仕組みを構築し、自社開発の脆弱性診断ツールに、最新の脆弱性に対する更新を都度実施している。
27	ウイルス対策の実施	サーバへアップするファイルについては、事前にウイルス感染のチェックを行っている。
3.運用的対策		
3.1 セキュリティポリシー		
28	セキュリティポリシーの開示	プライバシーポリシーを公表し、対策の内容を明確にしている。
3.2 インシデント対応		
29	インシデント発生時の利用者への迅速な連絡体制確立	情報漏えいや破壊・改ざん等のインシデントが発生した場合に、利用者へ迅速に連絡する手順や体制を確立している。また、当番制で24時間365日の対応を実施している。
30	利用側インシデント対応者へのログの提供	インシデントが発生した場合、該当するログを利用者に提供している。