「安否確認サービス」セキュリティ対策のご紹介

2014 年 3 月 26 日
サイボウズスタートアップス株式会社

1　はじめに

「安否確認サービス」（以下「本サービス」）は、お客様の BCP（Business Continuity Plan）をお手伝いさせていただくサービスです。このために本サービスでは災害や事故などの影響を排除してサービスを継続提供できるだけのセキュリティがきちんと実現されている必要があります。

本サービスを提供させていただく上で、私どもサイボウズスタートアップス（以下「弊社」）は様々なセキュリティ対策を検証し、実施しております。このドキュメントはそうしたセキュリティ対策のご説明をさせていただくものです。

2　「安否確認サービス」に求められていること

本サービスではお客様のお名前、生活しておられる地域、メールアドレスなどの個人情報をお預かりしております。弊社はこの個人情報がお客様にとってどれだけ重要な情報であるかを認識しており、本サービスのご提供にあたってお預かりしている情報の漏洩や第三者による不正使用などの事故が発生しない様に強く求められていることも認識しております。

また、本サービスには重大災害や事故、事件などの発生によって各種の社会的インフラに大規模な障害が発生した状況下であっても、その影響を最小限度に抑えて確実にサービスの継続ができる対策も求められています。

以上、本サービスに求められております上記のセキュリティ要求

『情報を漏らさない、サービスを止めない』

につきまして、本サービスと弊社はどの様に考えて対処をしておりますかを、ご説明させていただきます。

3 「安否確認サービス」とセキュリティ対策

3.1 安否確認サービスの機密性対策

3.1.1 通信経路の暗号化

本サービスではお客様とのすべての通信を SSL（Secure Socket Layer）によって暗号化しています。この暗号化に使われている暗号技術は継続的に安全性の検証が行われており、インターネット接続でのオンラインバンキングをはじめとして広く使用実績があるものです。

本サービスをご利用中の通信を傍受・盗聴されるような事態が発生しても、お客様の情報は漏洩や第三者による不正使用から守られています[1]。

3.1.2 アカウント認証情報の管理

本サービスでは、アカウント認証のパスワード（パスフレーズ）およびプライベートメールアドレスを暗号化して保管しております。このために万一保管していた暗号化データが漏洩した場合でも、第三者がこれを不正使用するのは困難です。

3.1.3 認証に基づく認可（アプリケーションとデータの利用）

本サービスでは、お客様の管理者アカウントを初期登録する毎に、お客様専用のアプリケーションを個別に作成します。

これによって、本サービスが取り扱うすべてのお客様に共通している情報を除き、本サービスでお客様が扱っておられるアプリケーションや情報に他のお客様がアクセスをすることはできません。

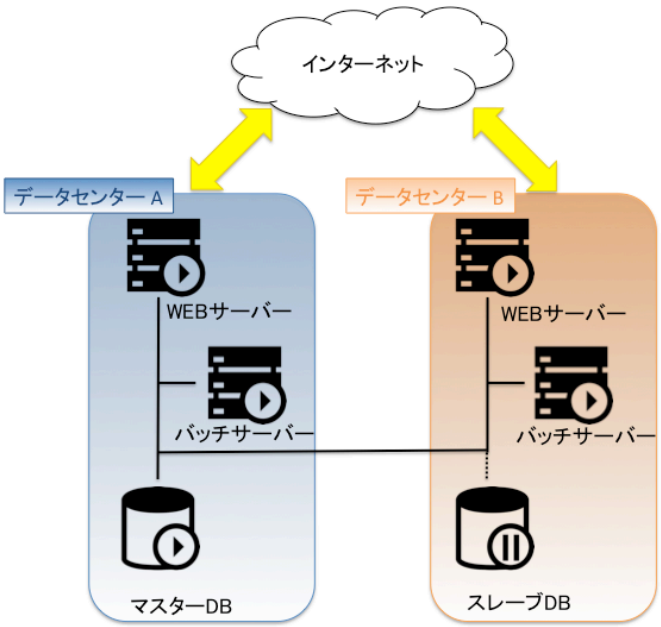
---

[1] 通信の暗号化は、通信端末からサーバまでの通信経路が対象です。通信端末側に「キー・ロガー」などのような盗聴プログラムが仕掛けられている場合には、この暗号化通信技術ではお客様の重要情報を守ることはできません。

3.2　安否確認サービスのシステム構成とセキュリティ

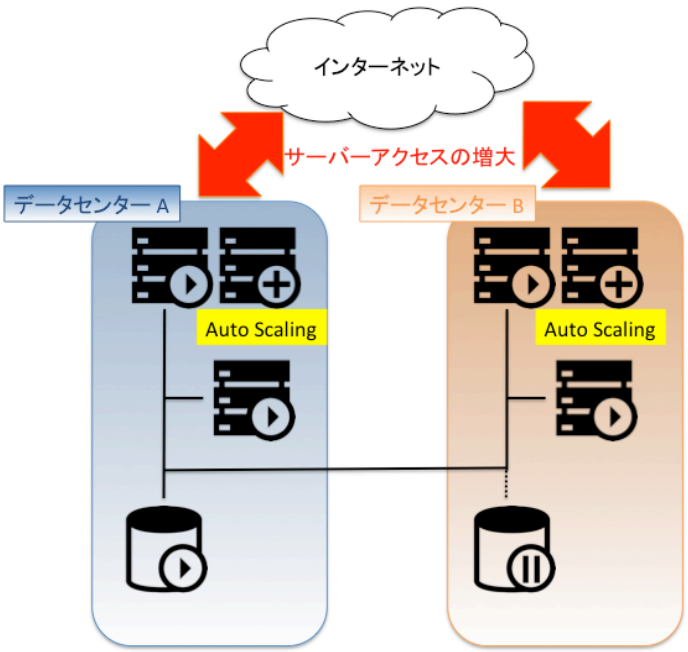
3.2.1 クラウドコンピューティングによる世界規模での地域分散配置

本サービスでは、ひとつのデータセンターに設置したサーバではなく、下図の様に２つの地域に分散配置されているデータセンターA,B を利用した クラウドコンピューティングサービスを連携させたシステムで、サービスを提供しています。



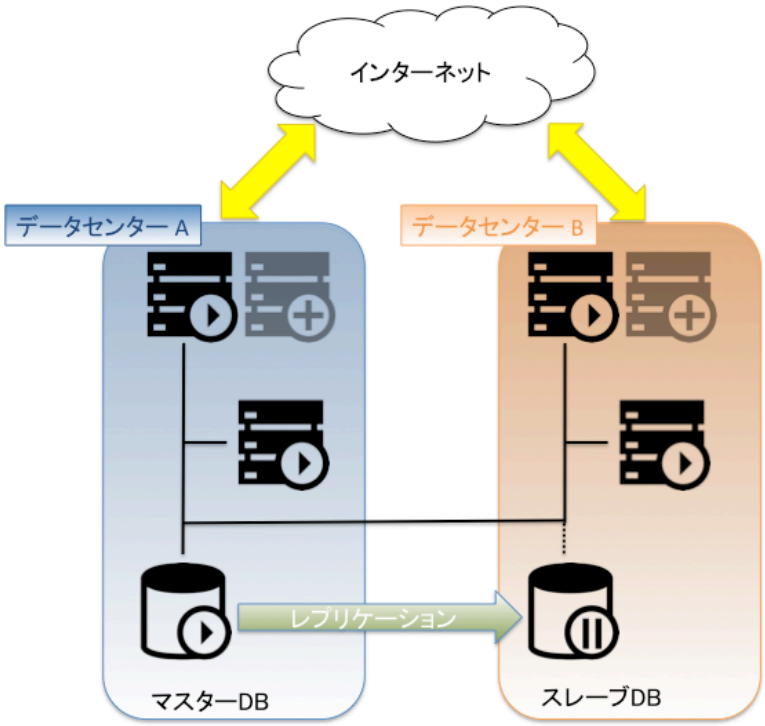
3.2.2 AutoScaling によるトラフィック増への対応

クラウドコンピューティングサービスの特性を利用し、非常時のトラフィックの急増に備え自動的にサーバーを増やす AutoScaling 構成を採用しており、トラフィック増によるサーバーダウンを回避しています。



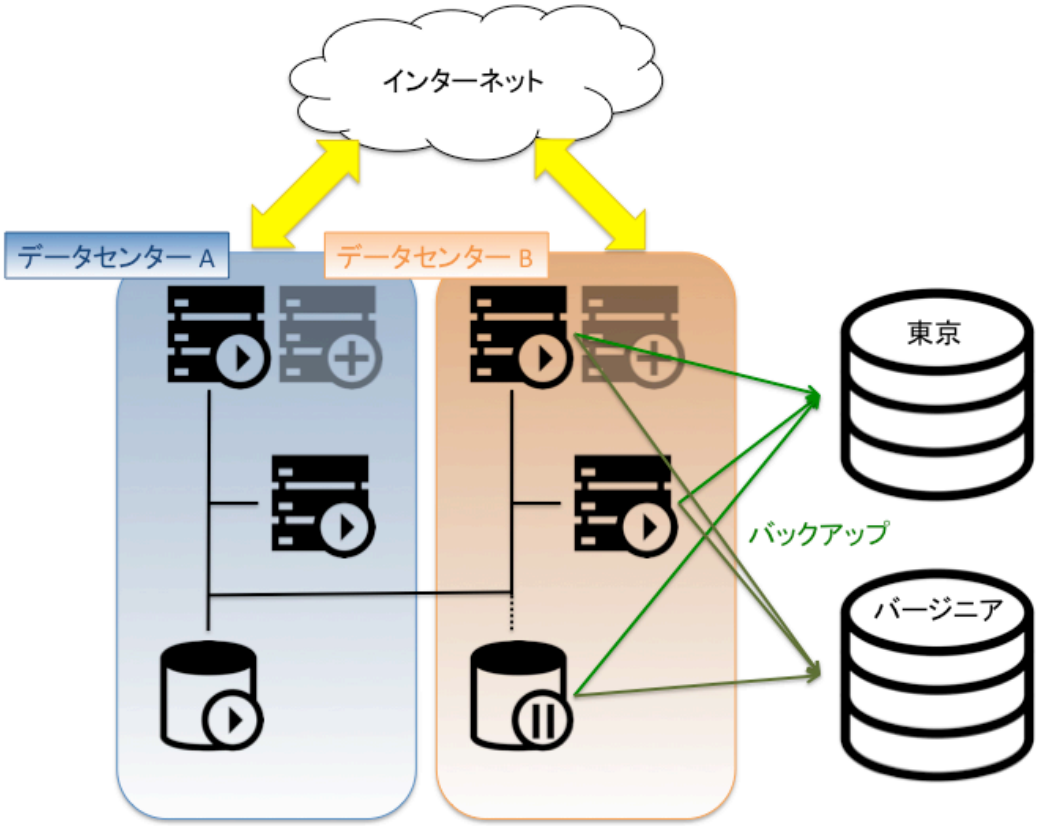
3.2.3 レプリケーションによるデータ同期とフェイルオーバ

本サービスは、データセンターA にあるデータベースをレプリケーションのマスターDB として、データセンターB にあるスレーブ DB のデータベースとリアルタイムにデータの同期を行っています。**データセンターA** 側で なんらかの障害が発生してサービスが出来ない状態になったとしても、このデータ同期によってスレーブ DB にフェイルオーバをすることができるため、本サービスのダウンタイムは最小限に抑えることができます。またこのフェイルオーバは自動で行われます。



3.2.4 国をまたぐバックアップ体制

データセンターA,B は シンガポール内の異なる地域に配置され 冗長化されていますが、更にクラウドコンピューティングサービスの特性を利用し、国境をまたぐバックアップ体制を採っています。これによりシンガポール全域で障害が発生した場合にも、日本(東京)、もしくはアメリカ(バージニア)にて サービスを継続することが可能となっています。



3.2.5 データベースバックアップとシステムバックアップについて

本システムのデータベースのバックアップは、１日２回完全なバックアップが５世代まで作成され、さらにトランザクションログを保持する事により任意時点(障害発生時点)の 5 分前までの復元を可能にしています。

システムバックアップは、1 日 2 回、10 世代までおこなわれております。

4　安否確認サービスが利用しているクラウドサービスについて

本サービスがクラウドサービスを利用するにあたり、クラウドサービスの提供事業者が開示している以下のセキュリティ要件を評価検討した結果、同サービスの利用を決定いたしました。

4.1　各種認証と認可の取得

本サービスが利用しているクラウドサービスは、SAS 70 (the Statement on Auditing Standards 70) の認証を取得しており、業務の受託に対してこの認証に基づいて受託した業務に対する内部統制の有効性を報告することができます。その他には、PCI DSS (Payment Card Industry Data Security Standard), ISMS (Information Security Management System), FISMA (Federal Information Security Management Act) の認証や許可を取得しています。

4.2　セキュアデザインの原則

本サービスが利用しているクラウドサービスは、セキュアソフトウェアベストプラクティスに基づいて開発がされています。これにはセキュリティチームによる公式なデザインレビュー、脅威モデリング、継続的なリスクアセスメントの実施、ソースコード診断、外部専門家による脆弱性診断が含まれています。

4.3　データセンターの物理的セキュリティ

本サービスは、以下のセキュリティ要件に基づいて運用されているデータセンターのクラウドサービスを利用しています。

- 外部からはデータセンターであることが判らない建物にサーバを収納
- 入退出は監視カメラや各種の電子的侵入検知システムなどで監視
- 入館には最低でも二種類の異なった認証を二回受ける
- 入館者は記録署名の上で、入館証を提示して担当者の立ち会いの下で行動
- 入館ができる業者は業務的必要性が認められる場合だけに限定
- 正規従業員であっても業務的な必然性が無ければ入館はできない
- 従業員のデータセンターへのアクセスはすべて記録され監査をされている

以上の対策により、部外者がクラウドサービスの運用されているデータセンターを見いだし、その内に立ち入る様なことはきわめて困難なものとなっています。

4.4　ネットワークセキュリティ

本サービスが利用しているクラウドコンピューティングサービスでは、以下のネットワークセキュリティ対策が実施されています。

- 世界最大のオンラインストア運用の知見に基づく DDoS 緩和対策
- ファイアウォールではソース IP と MAC アドレスの整合性をチェック
- ポートスキャン（使用規約違反）の監視と排除
- ARP キャッシュポイゾニング対策による「なりすまし」の防止

以上の対策により、本サービスが利用しているクラウドコンピューティングサービスのネットワーク環境の下で、他の利用者からの盗聴や妨害を受ける可能性はほとんどありません。

4.5　仮想環境のセキュリティ

本サービスが利用しているクラウドコンピューティングサービスでは、以下の仮想環境のセキュリティ対策が実施されています。

- クラウドサービス提供者は仮想環境にアクセスすることができない
- ファイアウォールが設定されており、仮想環境内からの設定変更は不可
- 仮想環境の設定変更には証明書などによる認証が必要

以上の対策により、本サービスが利用しているクラウドコンピューティングサービスの仮想環境は、従来のデータセンターに収容されている物理的なサーバに匹敵する独立性が確保されており、悪意を持った攻撃者による侵入を受けた場合でも二次的な被害の拡大は最小限度に抑えられる対策が取られています。

5　サイボウズスタートアップスのセキュリティスタンダード

本サービスをお客様にご利用いただきますにあたり、弊社は弊社が規定しているセキュリティポリシに基づき、本サービスの運用管理に以下の様なセキュリティスタンダードを適用しております。

5.1　セキュリティリスク顕在化の予防

5.1.1 ハードウェアの管理

弊社では、本サービスの運用管理に使用している PC、ハードディスク、ネットワーク装置などについて、正常な稼働状態が維持されていることを確認の後に運用管理作業を実施しています。

5.1.2 ソフトウェアの管理

本サービスの運用と運用管理に使用しているオペレーティングシステムとソフトウェア、フレームワークについては、デベロッパやベンダーより提供されているセキュリティパッチを迅速に適用しています。

アンチウィルスソフトを使用して、常時最新のパターンファイルが適用されている状態を維持しています。

5.1.3 ネットワークポリシの遵守

本サービスの運用管理では、暗号化されているリモート接続のみを使用しております。また、本サービスのサーバには https, ssh 以外のプロトコルでの接続が出来ない様にファイアウォールが設定されています。

さらに ssh については予め設定されているソースアドレス以外からの接続は遮断される設定となっています。

5.1.4 セキュリティ情報の共有

グループウェアを使用し、本サービスの関係者全員が参加している掲示板にセキュリティ情報を掲載して情報の共有をしています。また、運用中に発生した事故やトラブルについての情報も共有し、再発の防止に努めています。

5.1.5 暗号技術危殆化への対応

本サービスが通信暗号化やアカウント認証で使用している各種暗号技術について、デベロッパと研究機関から提供される検証情報を継続的に収集し、適切なタイミングで暗号技術の変更を行います。

5.1.6 アカウントとパスワードの管理

本サービスのアカウントの認証には公開鍵での認証か、充分な文字数と数字や記号が含まれる品質の良いパスフレーズを使用しています。

本サービスの関係者が、本サービスの運用などから離脱する場合には、直ちに使用していたアカウントのパスワードをアカウント管理者が変更し、一ヶ月の猶予期間経過の後にアカウントを削除します。

5.2　セキュリティリスク顕在化の検知

5.2.1 多様な手段によるシステム監視

本サービスでは複数の監視サーバを運用することで、システム稼働状態を自動監視しています。また、クラウド運用コンソールと、サーバシステムログ、アプリケーションログによってもシステムの稼働状況を監視しており、これらのサマリーが運用関係者に送付されるようになっています。

5.2.2 脆弱性公開情報への対応

本サービスの関係者は JVN (Japan Vulnerability Notes), JPCERT/CC (Japan Computer Emergency Response Coordination Center), IPA (Information-technology Promotion Agency) などのセキュリティポータルサイトを巡回購読し、新たに公開された脆弱性情報が本サービスに当該するものであるかどうかを定期的にチェックしています。本サービスに当該している脆弱性が公開された場合には、直ちにセキュリティ勧告に従った対策を実施します。

5.3　セキュリティリスク顕在化への対応

5.3.1 リスク顕在化の状況掌握

本サービスの運用でセキュリティリスクが顕在化した場合には、ただちにサービスの運用を停止して、リスク顕在化の進捗を抑止することに努めます。また、リスク顕在化の影響範囲を特定するための作業を最優先として実施いたします。

5.3.2 タスクフォースの発動

セキュリティリスクの顕在化が明確となった時点で、弊社は CEO を長とするリスク顕在化対応タスクフォースを発動します。タスクフォースは本サービスの関係者から横断的にスタッフを選び、情報収集担当、対応作業担当、広報担当によって構成されます。

リスク顕在化対応タスクフォースは本サービスを利用しているお客様に対してセキュリティリスクが顕在化したことを第一報として迅速に通知し、二次被害の発生を防止することに努めます。また 5.3.1 で掌握できているリスクの顕在化に関する情報とタスクフォースの活動状況をお客様に対して広報します。

5.3.3 脆弱性の排除

セキュリティタスクフォースは、リスク顕在化の原因となった脆弱性を特定し、これを除去または無効化します。脆弱性を特定することができない場合には、セキュリティベンダへの支援を要請します。

5.3.4 原状復帰計画の策定

脆弱性の除去または無効化がなされたことを確認の後、セキュリティタスクフォースは本サービスの原状復帰計画を策定します。計画の策定が完了したところで、お客様へサービスの復帰計画を広報します。

5.3.5 収束宣言と広報資料の作成

本サービスの原状復帰が確認され、事態の収束も確認されたところでリスク顕在化対応の収束宣言を行い、タスクフォースを解散します。タスクフォースの解散にあたっては、5.3.1 から 5.3.5 に到るまでの経緯を記録した広報資料を作成し、本サービスをご利用いただいているお客様へ開示します。

5.3.6 再発防止策の策定

セキュリティリスクが顕在化するまでの経緯を分析し、同様なリスク顕在化の再発防止が可能であるかを検討します。充分に有効な防止策が策定できない場合には、防止策による対応ではなくシステム設計や運用設計などの見直しも検討します。

以上