White Paper

ソナーサービス

第 1.2 版

ユーソナー株式会社

制定日：2022/4/1
改定日：2024/10/11

はじめに

White Paper の目的

ソナーサービスは、当社が構築している企業情報データベース(LBC と呼ぶ)を用いて、取引先企業情報や名刺に関わる一連の作業の自動化･効率化、情報の一元化を実現する当社のクラウドサービスです。

本ドキュメントは、ソナーサービスの提供において基盤として利用するクラウドサービスにおけるセキュリティに関する方針、並びにプロセスの概要をご理解いただくとともに、ISMS クラウドセキュリティ認証である ISO/IEC 27017 及び PII プロセッサのパブリッククラウドにおける個人識別情報(PII)の保護の認証である ISO/IEC 27018 の要求に従う公表を行うことを目的とします。

White Paper の対象

ソナーサービスの導入を検討中の方
ソナーサービスを利用中の方

クラウドコンピューティングのための情報セキュリティ方針

当社では、クラウドコンピューティングに関する情報セキュリティの方針を定め、お客様に満足いただける機能的でセキュアなサービスの提供を目指しています。

> **クラウドコンピューティングに関する情報セキュリティ方針**
> 当社は、クラウドコンピューティング環境におけるお客様の情報資産を情報セキュリティ上の脅威から保護するための措置を講じ、お客様が安心してご利用いただけるセキュアなサービスを提供します。

当社の「情報セキュリティ方針」は以下の URL からご確認頂けます。
https://usonar.co.jp/privacy/isms.html

情報セキュリティ組織

当社では、情報セキュリティに関する統括責任者として取締役の「置田　富士夫」を任命し、情報セキュリティに関する統括責任と権限を与えています。また、情報セキュリティ委員会を設置し、情報セキュリティのマネジメントシステムの運用と継続的改善に取り組んでいます。

地理的所在地

当社の所在地、並びに当社がお客様のデータを保存する国は日本国となります。当社が基盤として利用するクラウドサービスにおいて、日本国以外のリージョンにお客様のデータを保存する必要性が生じた場合、お客様に事前に通知したうえで行います。

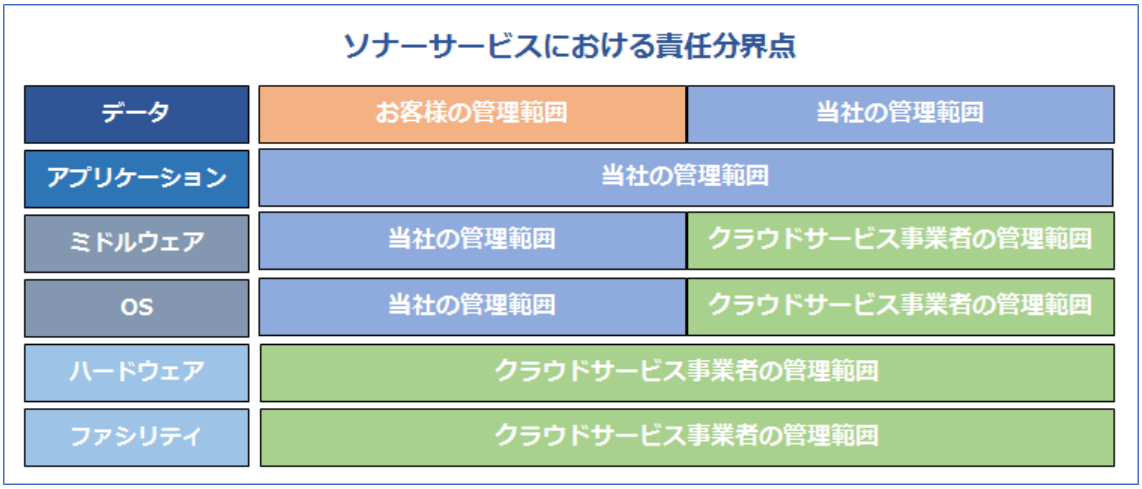
外部クラウドサービス

ソナーサービスにおいて、以下の機能を実現するために外部のクラウドサービスを利用しています。

サービス	機能	運営会社
アマゾンウェブサービス	インフラ構築，運用など	アマゾンウェブサービスジャパン株式会社

責任範囲

仮想レイヤーや施設におけるコンポーネントなど、サービスを実行するインフラストラクチャ、及びマネージドサービスについては、当社が基盤として利用するクラウドサービス事業者によって管理されます。当社は、事業者に対する購買管理規程に従い、調達時のセキュリティ審査、及びパフォーマンスのモニタリングによりクラウドサービス事業者を選定します。当社は、基盤上に構築したアプリケーション、及びアプリケーション上のデータに対して責任を負います。



当社の責任

・ソナーサービスの運用管理（ウイルス対策、脆弱性の管理、バックアップ、障害発生時の対応、可用性の維持）
・お客様がソナーサービスにアップロードした情報(以下「使用者コンテンツ」)の保護
・ソナーサービスに保管された秘密認証情報の管理
・お客様が取り扱うデータ保護のための暗号化、バックアップ、解約時のデータ削除
・ミドルウェア及び OS（マネージドサービスを除く）の脆弱性の管理

お客様の責任
・お客様によるソナーサービスの使用方法に起因して発生した問題
・お客様によるソナーサービスの使用方法に起因して、使用者コンテンツについて生じた損害
・お客様が利用されるアカウントの管理（登録、無効、権限設定）

当社とクラウドサービス事業者間における責任範囲
・アマゾンウェブサービス社が展開している責任共有モデルで定められた責任範囲に従っています。(https://aws.amazon.com/jp/compliance/shared-responsibility-model/)

情報セキュリティの意識向上，教育及び訓練
当社は、全従業員に対する入社時、及び年 1 回以上の情報セキュリティ教育を実施し、情報セキュリティに対する意識向上に努めています。

情報セキュリティのパフォーマンス評価
当社では、定期的（最低でも年に一回）に 情報セキュリティに関する内部監査を実施しています。定期的な内部監査以外に、組織、施設、技術、プロセス等の重大な変化に応じて随時監査を行っています。また、ソナーサービスの開発プロセスにおいて、第三者によるサービス脆弱性診断を実施しています。

インシデント対応プロセス
当社では、ISO/IEC27001 に準拠した標準化された情報セキュリティインシデント対応プロセスを整備しています。情報セキュリティインシデントに関する報告、エスカレーションに関する全ての手順を文書化しています。お客様に影響が及ぶインシデントは全てトップマネジメントまでエスカレーションされ、トップマネジメントの指示に従い、お客様への通知、及び管理・対処・評価を実施しています。

開発/調達

開発プロセス
当社のクラウドサービスの開発は、機能性とユーザビリティの確保はもちろんのこと、情報セキュリティについても配慮することを方針として行われます。開発は非機能要件としてのセキュリティ要件を定義し、厳格な承認プロセスを得たうえで実施されます。
セキュリティ機能に関するソースコードはレビューされ、テストプロセスを経たうえでビルドされます。

また、リリース前のみならず、リリース後も定期的な脆弱性診断を行っています。
サプライチェーン
当社のクラウドサービスの提供に関連するサプライヤー、及びサプライチェーンは以下の手段により管理することを方針としています。
・情報セキュリティ水準を当社と同等又はそれ以上に保つことを事前の審査により確実にする
・契約により秘密保持の確保を担保する
・サプライヤーがサプライチェーンを形成しサービス提供している場合、サプライヤーのサプライチェーンメンバーに対するセキュリティ管理の能力について審査する

アプリケーションのセキュリティ機能

情報セキュリティ機能

主にお客様が検討される情報セキュリティ機能として、本ホワイトペーパーは以下を記述しています。

機能（ISO/IEC27017 または 27018 の管理策）	本ホワイトペーパーの記述
A.9.2.1 利用者登録及び登録削除	利用者アクセスの管理
A.9.2.2 利用者アクセスの提供	利用者アクセスの管理
A.9.2.3 特権的アクセス権の管理	認証情報の管理
A.9.2.4 利用者の秘密認証情報の管理	認証情報の管理
A.9.4.1 情報へのアクセス制限	利用者アクセスの管理
A.10.1.1 暗号による管理策の利用方針	暗号化
A.12.3.1 情報のバックアップ	バックアップ
A.12.4.1 イベントログ取得	ログ
CLD.12.4.5 クラウドサービスの監視	クラウドサービスの監視

情報のラベル付け

ソナーサービスでは、名刺データの管理におけるタグ機能を提供し、お客様が登録された担当者情報の分類をサポートします。使用方法の詳細は、mソナーマニュアルをご参照ください。

利用者アクセスの管理

ソナーサービスは、お客様が安全に利用者アクセスの管理を行うためのユーザインターフェイスと機能を提供します。

お客様は管理者画面よりアカウント登録及び無効化を行い、またユーザに対する権限の割り当てを行うことが出来ます。
使用方法の詳細は、管理ソナーマニュアルをご参照ください。

認証情報の管理

アカウント管理の詳細は、管理ソナーマニュアルをご参照ください。
パスワードの設定はお客様のセキュリティポリシーにもとづいて実施してください。
管理者権限はお客様のセキュリティポリシーに従い厳重に管理することをお願いします。

ユーティリティプログラム

ソナーサービスは、ユーティリティプログラムを提供しておりません。

暗号化

データベースに保管されるお客様のデータは、AES-256 暗号化アルゴリズムを使用して暗号化を実施し、適切なアクセス権のもとで保管されます。
ソナーサービスとお客様との間での通信は、TLS 1.2 以上で暗号化し、情報の盗聴等のリスクに対処しています。

運用

変更

お客様に影響を与えるソナーサービスの変更は、お客様の通知先メールアドレス宛に事前通知します。

管理者用手順

各種マニュアルの提供に加え、ソナーサービスの FAQ サイト、チャットボットを提供しています。

バックアップ

ソナーサービスにおけるバックアップは、システムが日次で 2 世代分、お客様のデータが日次で 8 世代分をバックアップしています。
ただし、お客様からのバックアップデータの復元等に関するご要望には対応していません。

ログ

ソナーサービスの維持管理に必要となる適切なログを取得しています。
ログに含まれる項目の詳細はソナーサービスの「FAQ サイト」をご参照ください。
お客様が必要となる場合は、当社のサポート窓口までご相談ください。
ログは、取得後最低 3 年間保持します。

ソナーサービスは、基盤として利用するクラウドサービス事業者が提供する時刻同期サービスを利用し時刻同期を行っています。

クラウドサービスの監視

当社は、ソナーサービスが正常に提供され、他社を攻撃する基盤として使用される等に不正に使用されていないこと、データの漏洩が発生していないか等の監視を行っています。
監視結果をお客様に公開できるサービス機能は有しておりません。
情報漏洩が発生した際には速やかにお客様へご報告いたします。

技術的脆弱性の管理

脆弱性情報の収集は以下の手段により行います。
・JPCERT コーディネーションセンターから公開される脆弱性情報
・当社関係者による検知
・お客様、基盤を提供するクラウドサービス事業者等の外部からの情報提供

検出した脆弱性については、速やかに影響調査を行い、必要な対策を講じます。

ネットワーク

ソナーサービス専用の仮想ネットワークを構築し、入口への侵入を IDS/ IPS により監視することによりセキュリティを確保しています。
ソナーサービスは、お客様ごとにユニーク ID を割り振り、データベースのテーブル内で論理的に分離を行っています。

容量・能力の管理

当社は、サーバリソースの監視を行っています。リソースの増減は、クラウドサービス事業者が提供する管理コンソールを利用して実行します。
サーバリソースの不足は、スケールアップによる対応を原則としていますが、将来的なニーズに照らして、必要があればスケールアウトによる対応も行います。

負荷分散/冗長化

ソナーサービスは基盤を提供するクラウドサービス事業者のマネジメントサービスを使用し、複数の仮想サーバに処理を振り分ける、ロードバランシングを採用しています。
また、アプリケーションの構成はマシンイメージとして保存し、即時に複製が可能な状態を整えています。

インシデント対応

ソナーサービスに関連した情報セキュリティインシデントを検出した場合、以下の内容で速やかに通知します。

項目	内容
報告する範囲	データの消失、長時間のシステム停止等のお客様に大きな影響を及ぼす可能性のある情報セキィリティインシデント
対応の開示レベル	当社に起因する情報セキュリティインシデントでお客様に影響があるものは、すべて同等のレベルで対処します。
通知を行う目標時間	検知から 30 分以内を目標に通知します。
通知手順	ご登録頂いたメールアドレス宛 （必要に応じて電話等の手段を使用する場合もあります。）
復旧の目標時間	検知から 4 時間以内を目標に復旧対応します。
問合せ窓口	ユーソナー株式会社 サポート窓口
適用可能な対処	当社に起因する情報セキュリティインシデントでお客様に影響があるものは、あらゆる手段を講じて対処します。

また、お客様において情報セキュリティインシデントを検出された場合、またはその疑いをもたれた場合は、当社のサポート窓口までご連絡ください。

サービス利用停止後のデータの扱い

ソナーサービスでお客様が作成・保存したお客様のデータの除去に関しては、10 営業日以内に完全に消去いたします。バックアップデータは、バックアップ方針に従い保管した後に消去されます。お客様の情報が含まれるログデータに関しては、ログの保管期間に従い最長で 3 年半以内に消去されます。

装置のセキュリティを保った処分又は再利用

当社は、情報システム管理者に装置の処分又は再利用に関する役割を集中し、従業員による個別対応を排除することで、セキュア且つ確実な装置の処分又は再利用を実現しています。

一時的ファイルの削除

ソナーサービスの運用に伴い作成した一時的ファイルは、作成後 10 営業日以内に削除します。

その他

証拠の収集

当社は、デジタル証拠となり得るログデータを収集しています。
ログの情報をお客様に公開できるサービス機能は有しておりませんが、有事における調査を目的に情報提供を行うことができます。情報提供の範囲と方法については、ご相談のもと当社で決定いたします。

法令また権限のある官公庁からの要求によりソナーサービス上にあるデータ等の情報を、当該官公庁またはその指定先に開示もしくは提出することがあります。
詳細については「LBC 利用規約 8 条 1 項」に記載しています。

適用法令及び契約上の要求事項

利用契約に関する準拠法は日本法とし、本規約に起因し又は関連する一切の紛争については、東京地方裁判所を第一審の専属的合意管轄裁判所とします。

知的財産権

本サービスを構成する有形または無形の構成物（プログラム、データベース、画像、マニュアル等の関連ドキュメントを含むがこれらに限られない）に関する著作権を含む一切の知的財産権その他の権利は当社に帰属します。

記録の保護

当社は、アプリケーションにおけるデータ操作等のログ、及び仮想ネットワークへのアクセスに関するログ、サービスのバージョンアップに関する内部要員による作業ログは最低 1 ヶ月間保持します。

暗号化機能に対する規制

ソナーサービスにおいて暗号化の規制対象になる地域にはサービスを提供していません。

個人識別情報（PII）の利用目的

ソナーサービスにおいてお客様よりお預かりする個人識別情報(PII)は、ソナーサービスをお客様に提供するためのみに使用します。当社は、目的の達成に必要な範囲を超えた個人識別情報(PII)の取扱いを行わないための措置を講じます。

個人識別情報（PII）の第三者提供

ソナーサービスにおいてお客様よりお預かりする個人識別情報(PII)を第三者に提供することはありません。（個人情報保護に関する法律（個人情報保護法）第 23 条第 1 項の各号に掲げる場合を除く）

第3者認証

ISO/IEC27001

当社は、本社及びデータセンターを認証範囲として 2018 年 9 月 25 日に
ISMS（Information Security Management System）の国際規格である ISO/IEC27001 を取得しています。

ISO/IEC27017

当社は、ソナーサービスの提供に係るクラウドサービスプロバイダとしてのシステム構築・運用、及びアマゾンウェブサービスのクラウドサービスカスタマとしての利用に係る ISMS クラウドセキュリティマネジメントシステムを認証範囲として 2020 年 11 月 4 日に ISMS クラウドセキュリティ - ISO/IEC27017 を取得しています。

ISO/IEC27018

当社は、クラウド型名刺情報管理システムのサービス提供・運用を適用範囲として
2020 年 11 月 4 日に MANAGEMENT SYSTEM FOR PROTECTION OF PII IN PUBLIC CLOUD ACTING AS PII PROCESSORS - ISO/IEC27018 を取得しています。

ソナーサービスに関するお問い合わせ

ユーソナー株式会社 サポート窓口
TEL：0120-00-9000
メール：usonar-support@usonar.co.jp

改定履歴

版数	日付	改定内容
第 1.0 版	2022/4/1	初版発行
第 1.1 版	2022/7/19	社名変更、サポート窓口メールのドメイン変更、 通知を行う目標時間の短縮
第 1.2 版	2024/10/11	責任範囲(当社の責任・お客様の責任)の変更、 パフォーマンス評価の追記、暗号化記述の変更、 マニュアル表記の変更、ログ保管期間の変更、 バックアップデータ消去方針の追記