SONAR ATSサービス

ホワイトペーパー

For ISO27017

Thinkings株式会社

2020 年 8 月 1 日

目的

このホワイトペーパーは、ISO/IEC 27017:2015(情報-セキュリティ技術-ISO27002に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範）に準拠したISMS（情報セキュリティマネジメントシステム）で求められている要求事項の実現のために、当社がお客様に対し提供しているセキュリティ仕様について明確にするものです。

適用範囲

当社のISO27017の適用範囲は、以下のサービス内容に対するものです。

・採用業務支援サービス（SONAR ATS）

・SONAR ATSの運用

SONAR ATSサービス

1. SONAR ATSサービスについて

SONAR ATSサービスとは、企業の新卒・中途採用等あらゆる採用ニーズに対応し、統合的に応募者管理ができる採用管理クラウドサービスであり、以下のメニューを含みます。

採用担当者向け機能	求人作成機能、応募者管理機能、採用フロー管理機能、イベント・選考スケジュール管理機能、面接アサイン機能（アドオン）、エントリーページ作成機能、メール・メッセージ機能、フォローアクション・通知機能、マイページ管理機能、マイページCMS機能（アドオン）、分析機能、シミュレーション機能、サーベイ作成機能、ユーザー管理機能、マスタ管理機能、ファイル出力（アドオン）、PDFファイル取込み（アドオン）
面接官向け機能	面接評価入力機能（アドオン）、面接スケジュール管理機能（アドオン）
応募者向け機能	ジョブボード、マイページ、モバイルチェックイン（アドオン）、ファイル提出（アドオン）
人材紹介会社（エージェント）向け機能	求人情報・推薦機能、推薦者管理機能

2. 責任について

SONAR ATSサービスについての責任は、サービスにおいての通常の運用におけるデータの消失、漏えい等の責任は当社に在するものとしますが、お客様側で行われる作業についての責任については、お客様側に在するものとします。

また、当社のサービスはMicrosoft Azureを使用しており、Microsoft側の責任については、以下のサイトに公開されています。

https://docs.microsoft.com/ja-jp/azure/security/fundamentals/shared-responsibility

クラウドサービスにおけるセキュリティについて

1. クラウドサービスプロバイダの地理的所在地

東京日本橋オフィス	東京都中央区日本橋本町4-8-16 KDX新日本橋駅前ビル5階
東京半蔵門オフィス	東京都千代田区一番町4-6 一番町中央ビル2F
徳島サテライトオフィス	徳島県徳島市東大工町1丁目9-1 徳島ファーストビル6階

2. クラウドサービスデータを保存する可能性のある国(ISO27017:6.1.3)

クラウドサービスデータの保存場所は日本国内になります。

3. 教育(ISO27017:7.2.2)

当社は、クラウドサービス派生データを適切に取り扱うために、従業員に、意識向上、教育及び訓練を提供し、委託先等にも同様の教育訓練の実施を要求します。

4. 資産目録(ISO27017:8.1.1)

当社は、資産目録の管理を行うにあたり、クラウドサービスカスタマデータ及びクラウドサービス派生データの識別を行います

5. 資産の除去(ISO27017:CLD 8.1.5)

サービスの利用終了時には、即時リソースの削除を行います。

バックアップの有効期限は35日間となりますので、35日間を経過するとリソースの復旧は出来なくなります。

6. 利用者登録及び削除(ISO27017:9.2.1)

SONARサービスの利用者登録及び削除は、システム上でお客様が直接実施可能です。

サポートサイト上に登録、削除手順をご提供しております。

7. 利用者アクセスの提供(ISO27017:9.2.2 9.2.3)

セキュリティに配慮したログオン手順（例：アカウントのロックアウト）や、良質なパスワード（例：セキュリティ強度を高める文字種別や文字数）の利用を確実にする仕組み等を整備しております。

また、IPアドレスフィルタリング機能により、特定のIPアドレスからのアクセスに制限できるようになっております。

8. 利用者の秘密認証情報の管理（ISO27017:9.2.4）

パスワード管理の安全性を高めるために以下について実施している。

・長いパスワード（最長100文字）

・システムで表示可能な記号や空白の仕様を許可

・推測されやすい予約語の使用を禁止

・連続で認証失敗した場合に強制的にアカウントをロック（オプション設定）

・パスワードの有効期限を強制しない（オプション設定）

・シングルサインオンによる外部の認証基盤との連携（アドオン）

9. 特権(ISO27017:9.2.3,9.4.4)

特権については、原則お客様側に1アカウントご提供しています。

特権ユーザが発行した一般アカウントについては、特権ユーザにて権限の付与が可能となっています。

また、特権ユーザの操作ログは全て当社側で取得しています。

10. 情報へのアクセス制限(ISO27017:9.4.1)

SONARサービスのアクセス制限は、特権アカウントにより設定可能です。

11. 仮想コンピューティング環境における分離(ISO27017:CLD 9.5.1)

サービスレイヤでの認証プロセス・アクセス元IPアドレス制限により、テナント間のアクセスは制御しています。

12. 仮想マシンの要塞化(ISO27017:CLD9.5.2)

仮想マシンは、要塞化として次のセキュリティ対策を実施しています。

- ポートの制限
- ファイアウォールの設置
- マルウェア対策
- 監視

13. 暗号による管理策の利用方針(ISO27017:10.1.1)

SONAR ATSサービス上の情報は、暗号化しております。

TDEによりデータベース内のすべてのデータファイルおよびログファイルが暗号化されております。

暗号化管理制御等の詳細については、以下のリンクをご参照ください。

https://docs.microsoft.com/ja-jp/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-2017

伝送中のデータの暗号化については以下の通りです。

Database:

Port 1433

Protocol TDS

Storage:

Port 443

Protocol https

※暗号TLSの設定はウェブサーバの設定と等しい

個人情報を含むデータとファイルを格納するストレージおよびデータベースは鍵長256bitのAESで透過的に暗号化しております。

14. 装置のセキュリティを保った処分又は再利用(ISO27017:11.2.7)

当社では直接装置の処分を行うことはありません。

Microsoft Azureの施設、建物、および物理上のセキュリティに基づきます。

https://docs.microsoft.com/ja-jp/azure/security/fundamentals/physical-security

15. 変更管理

SONARへのシステム変更等を行う場合は、約1ヵ月前にサービス内インフォメーションにて告知します。

16. 容量・能力の管理(ISO27017:12.1.3)

容量・能力についてはサービスを提供するのに十分な容量・能力を確保しております。

不足することが予測される場合、適宜増強等を行います。

17. 実務管理者の運用のセキュリティ(ISO27017:CLD12.1.5)

重要データを取扱う情報システムや情報等へアクセスする利用者とそのアクセス権を適切に管理するため、利用者及びアクセス権の登録・変更・削除の正式なプロセスに係る申請ルート、承認者、作業者等を明確化するとともに、運用中においては利用者アクセス権の定期的なレビューを実施しております。

情報システムへの特権的アクセス権の割当及び利用は特に厳重に管理しております。

最小権限および職務の分離の原則を踏まえて、重要インフラサービスの提供に係る情報システムや情報へのアクセス（リモートアクセスを含む）を制限しております。

18. クラウドサービスの監視(ISO27017:CLD12.1.5)

SONARサービスは常時監視しております。

不正アクセスの可能性、システム停止、リソースについてはお客様に影響がある場合は個別にお知らせします。

19. 情報のバックアップ(ISO27017:12.3.1)

SONARサービスのバックアップ体制は、東日本リージョンをメインとし、サブとして西日本リージョンを利用しており、必要に応じて相互復旧が可能です。

また、バックアップデータは全てAzure内のストレージに自動的に保管されており、年2回復旧テストも行っております。

20. クラウドサービスの監視(ISO27017:CLD12.4.5)

SONARサービスは、自動化された侵入検知プラットフォームを使用して、常に監視しております。

21. 仮想及び物理ネットワークのセキュリティ管理の整合(ISO27017:CLD13.1.4)

当社の内部規定を策定し、文書化しています。また、変更管理プロセスにより、物理と仮想での整合が取れなくなるような変更作業を行えないようコントロールを実施しています。

22. 情報セキュリティ要求事項の分析及び仕様化(ISO27017:14.1.1)

当社のクラウドサービスにおけるセキュリティ要求事項及び仕様は、SLA及びセキュリティ対策説明資料に記載しております。

23. セキュリティに配慮した開発のための方針(ISO27017:14.2.1)

当社のクラウドサービスについては、リリース前および、定期的なぜい弱性診断の実施や、定期的なネットワーク診断を行うことを方針として定めています。

24. 供給者との合意におけるセキュリティの取扱い(ISO27017:15.1.2)

当社がお客様に対し提供する情報セキュリティ対策については、次の通りになります。

- 監視
- ID,パスワード発行
- ぜい弱性管理と対策
- バックアップ
- データ暗号化

25. ICT サプライチェーン(ISO27017:15.1.3)

当社のクラウドサービスは、Microsoft Azureをピアクラウドサービスプロバイダとして運用しております。

Microsoft Azureのセキュリティ等に関する事項については、こちらをご参照ください。

https://docs.microsoft.com/ja-jp/azure/security/

26. 責任及び手順(ISO27017:16.1.1, 16.1.2)

当社で確認した次のインシデントについては、SONARシステムサポートにて対応のご案内をしております。

- サービスの中断、停止を伴うインシデント
- 情報漏えいの可能性（お客様が該当する場合）

インシデントが発生した場合、検出から1時間以内に該当するお客様にご案内いたします。

お客様でのご対応が必要となる場合は、その旨を個別のお客様にご案内いたします。

お客様からの問い合わせや報告は、SONARサポートサイトにて承ります。

また、お問い合わせ及び対応の履歴は追跡可能となっております。

27. 証拠の収集(ISO27017:16.1.7)

インシデントの対応結果については、SONARシステムサポートサイト上に掲載いたします。

当社のクラウドサービスにおけるログ等は、ご依頼をいただければ開示します。

28. 適用法令及び契約上の要求事項の特定(ISO27017:18.1.1)

当社のクラウドサービスにおける準拠法は日本法と定めています。

また、当社においての法的準拠については、コンプライアンス担当を設定し、管理を行っております。

29. 知的財産権(ISO27017:18.1.2)

知的財産権に関する苦情・相談等があった場合は、SONARサポートサイトでお問い合わせください。

30. 情報セキュリティの独立したレビュー(ISO27017:18.2.1)

情報セキュリティに関する独立したレビューとして、第三者審査機関による審査を受けてまいります。

サイトのぜい弱性等に対する対応は外部の監査サービスを使用して定期的に検査をしております。

*本文書に記載のISO27017に関連する項目は、お客様に公表すべき事項に限定しており、当社の認証にかかわるすべての項目を網羅しているわけではありません。