SAPPHIRE

セキュリティホワイトペーパー

ver 1.0

Miletos Inc.

0. はじめに

目的

SAPPHIRE ホワイトペーパー（以下、「本書」といいます。）は、クラウドセキュリティの国際規格（ISO/IEC 27017 : 2015）で求められる要求事項に対して、Miletos株式会社（以下、「当社」といいます。）が実施する管理策をご確認いただき、安心して当社のクラウドサービスをご利用いただくことを目的としています。

適用範囲

本書の適用範囲は、当社提供の次のクラウドサービスとなります。

- SAPPHIRE for Enterprise (以下、「SAPPHIRE」といいます。

適用範囲

本書で使用する用語の意義は、それぞれ次のとおりとします。

- クラウドサービスユーザー
  - SAPPHIRE導入企業様で実際に経費精算業務を担当されるアプリケーションのユーザー様
- クラウドサービスカスタマーデータ
  - SAPPHIREでの処理に資する目的でクラウドサービスカスタマーが提供するマスタデータ
  - SAPPHIREの利用においてクラウドサービスユーザーが実際に入力した、経費精算データおよび承認の有無などのメタ情報

1. クラウドサービスカスタマーとの責任分界点

当社の責任

当社は、SAPPHIREの提供にあたり以下の事項を実施いたします。

- SAPPHIREのセキュリティ対策（インフラのセキュリティ対策など）
- SAPPHIREに保管されたクラウドサービスカスタマーデータの保護

クラウドサービスカスタマーの責任

クラウドサービスカスタマーは、SAPPHIREの利用にあたり、以下のセキュリティ対策を実施する必要があります。

- 各クラウドサービスユーザーに付与されたパスワードの適切な管理
- クラウドサービスユーザーアカウントの適切な管理（登録、削除等）

2. データ保管場所

クラウドサービスカスタマーデータは、国内を中心にGoogle Cloudの以下リージョンにて保管されます。

- asia
- US

3. 情報資産の管理

- クラウドサービスカスタマーデータ（保存データ）とSAPPHIREが管理運用するための情報資産は明確に分離しています。なお、SAPPHIRE上にクラウドサービスユーザーが作成・保存する情報資産は、クラウドサービスカスタマーの管理範囲となります。
- クラウドサービスカスタマー間の保存データは論理的に分離されています。

4. データの削除

- SAPPHIREの利用終了時、クラウドサービスカスタマーは当社に対してデータの削除を申請することが可能です。当該申請があった場合、当社は申請日から1ヶ月以内にすべてのデータについて削除を行います。
- クラウドサービスカスタマーは、当社に対して、バックアップデータの削除を申請することができません。保管期間等についての詳細は、「14．バックアップの状況」にて後述します。
- クラウドサービスカスタマーは、当社に対して、ログの削除を申請することができません。保管期間等についての詳細は、「15．ログに関する情報」にて後述します。

5. システムを構成する通信装置のセキュリティを保った処分または再利用

- SAPPHIREの提供において使用されるサーバー、ネットワーク機器等の装置は、Google Cloudによって管理されています。装置の処分・再利用におけるセキュリティに関しては、Google Cloudに直接お問い合わせください。

6. 容量・能力の管理

- SAPPHIREを構成するサーバー等のリソースは24 時間監視されています。リソースの状態が逼迫していると当社が判断した場合、追加を実施することがあります。

7. ラベル付け機能

- クラウドサービスカスタマーは、経費に関するメタ情報を独自に設定することによって、情報および関連資産を分類し、整頓することが可能です。

8. 利用者登録および削除

- SAPPHIREではクラウドサービスカスタマーの利用するIdP をクラウドサービスの認証に使用するため、クラウドサービスカスタマーは自身のIdPで適切なユーザー管理をする必要があります。

9. アクセス権の管理

- クラウドサービスカスタマーからの申請があった場合は、当社はクラウドサービスカスタマーが管理するために用いる特権アカウントを提供します。

- 特権アカウントは、クラウドサービスカスタマーが管理するすべてのクラウドサービスユーザーになりかわってログインすることができるほか、ユーザーの作成・経費申請フォームの構成を変更する機能を有します。特権アカウントは、クラウドサービスカスタマー側IdPから提供されるアカウント（クラウドサービスユーザー）やアカウントのグループに紐付けられます。
- クラウドサービスカスタマーは、サービスの提供する機能でアカウントに権限の付与ならびに剥奪を行うことができます。
- クラウドサービスカスタマーは利用中のIdPの設定によって特権アカウントに二段階認証を要求することができます。

10. パスワードの配布方法

- SAPPHIREでは、クラウドサービスカスタマーのIdPを認証に使用するため、ユーザーの初期パスワードの割当て方法およびアカウント再発行時のパスワード変更手順はクラウドサービスカスタマーのアカウント運用方針に依拠するものとします。

11. 暗号化の状況

- SAPPHIRE上の情報は、AES-256によってディスクレベルで暗号化され、保護されます。
- SAPPHIREとクラウドサービスユーザー間の通信は、SSL/TLS通信によって暗号化されます。
- 上記暗号方式以外をご希望される場合でも、別の暗号方式はご利用いただけません。
- クラウドサービスカスタマーは、暗号鍵を自ら指定してディスクレベルでの暗号化を実施することができません。

12. 変更管理

- 当社は、SAPPHIREの可用性等に悪影響を与える可能性のある変更について、クラウドサービスカスタマーに次の情報を提供しています
    - 不具合修正、機能追加その他変更種別
    - SAPPHIREおよびその基礎にあるシステムの変更についての技術的な説明
    - 変更予定日および予定時刻
- 当社は、すべてのSAPPHIREのご利用において認証を必須としているため、クラウドサービスカスタマーのIdPが提供するセキュリティ手順を迂回して、各種サービス機能を利用する機能（ユーティリティプログラム）をご用意していません。

- 当社は、電子メールやSlack等のコミュニケーションツールにてクラウドサービスカスタマーへのサポートを提供しています。最新のSAPPHIREの変更内容および変更の適用状況については、これらのツールを介して情報の共有をいたします。

13. バックアップの状況

- システムおよびユーザーデータは、毎日バックアップを取っており、7世代分を常に保持しております。
- バックアップの手法は、増分バックアップとなります。
- バックアップのロケーションは、Google Cloudのasiaとなります。
- SAPPHIREは、クラウドサービスカスタマーがご自身でバックアップ／リストアする機能を提供していません。なお、弊社スタッフもクラウドサービスカスタマーデータにアクセスしない運用を原則としているため、クラウドサービスカスタマーから申請があった場合でも、その要望に合わせユーザーデータを復旧する対応等はいたしません。
- 障害対応等でのリストア作業については、当社にて実施します。なお、リストア作業を行う前に、クラウドサービスカスタマーにその旨事前に連絡または周知いたします。

14. ログに関する情報

イベントログの取得および保護

- クラウドサービスカスタマーは、SAPPHIREの経費メタ情報であるアクションログを確認することで、経費申請から承認にかけてのイベントログを閲覧することができます。
- 当社は、障害対応等のトラブルシュートや障害検知のため各種システム監査ログを取得しておりますが、クラウドサービスカスタマーにその内容の一部または全部の提出を求められた際、これに応じる義務を負いません。

クラウドサービスの監視

- 当社は、クラウドサービスカスタマー向けのSAPPHIRE監視機能を提供していません。
- 当社は、各種インスタンスのCPU使用率・ストレージ利用容量・通信量・バッチ処理等の監視を行っています。

クロックの同期

- SAPPHIREのアクションログで提供されるログは内部的にはUTCで保存されており、場所によって、自動的に時差が補正されて表示されます。
- サービス内で内部的に利用されるログの時間は、Google Cloud内部のNTPサーバーと同期しています。

15. 脆弱性管理に関する情報

セキュリティパッチのタイミング

- 当社は、SAPPHIREで利用しているインフラ・ミドルウェア・ライブラリに関する脆弱性情報を定期的に収集し、当社で適用する必要があるか確認しています。認識された脆弱性のうち対処が必要なものに関しては、セキュリティパッチを随時適用していきます。

ウイルス対策ソフトウェアの導入

- SAPPHIREのアプリケーションは、Google Cloud上のプライベートネット空間でコンテナ化・要塞化（「ネットワークやサーバーについての遵守事項」にて後述）された状態で実行されます。そのため、当社独自のウイルス対策は行っていません。Google Cloudのウイルス対策の実施状況については、Google Cloudに直接お問い合わせください。

第三者による脆弱性診断

- 3ヶ月に1度、経済産業省が定める「情報セキュリティサービス基準」に適合した脆弱性診断ツールによる診断を実施しています。

サーバーの適切な分離

- Webサーバー、データベースおよびバッチ処理システムは分離しています。

技術的脆弱性の監視状況

- 各種パッケージの脆弱性を随時確認することで、社内の脆弱性監視体制（リソース監視体制）としています。

- 当社のSLOを超えたシステム停止、不正アクセス／情報漏えいを引き起こす可能性があると当社が認識した脆弱性は、テスト環境で検証したのち、速やかにパッチを適用しています。

ネットワークやサーバについての遵守事項

- コンテナを設定する際に、適切な側面からの要塞化（不要なポートを閉めることおよび利用するプロトコルの制限）を実施しています。
- 上記、要塞化を実施しているためIDS、IPSの導入は行っておりませんが、アプリケーションレイヤーにおける防御はWAFによって強化しています。
- コンテナの動作は、各種ログを取得し・監視しています。
- アプリケーションやバッチ実行のインスタンスとDBサーバー、オブジェクトストレージ等は、すべて分離して各種ログを取得し、監視しています。

当社のセキュリティ研修等

- 新しく入社する社員に対しては、都度情報セキュリティに関する教育を実施しています。また、社員全員に対して、年に1回以上情報セキュリティに関する教育を実施しています。いずれもテスト問題を用意しており、合格するまで受講するルールとしています。
- 社内内部監査、マネジメントレビュー、年度リスクアセスメントの実施に加え、ISO/IEC 27001およびISO/IEC27017 の ISMS 認証取得において第三者による審査を受けることで、常によりセキュアなサービスを提供するよう取り組んでいます。

16. 適用法令

- SAPPHIREの利用に関する契約書その他の文書は、日本国内の各種法令に準拠して解釈されます。

17. 資産の取り扱いに関する情報

- 当社は、クラウドサービスカスタマーデータをデータセンターのみに保管します。
- 裁判所からの開示請求など、日本法に基づいた正当な情報開示請求が行われた場合、クラウドサービスカスタマーの事前の同意なく、クラウドサービスカスタマーデータを第三者に開示することがあります。

18. 開発におけるセキュリティ情報

- アプリケーションのプログラミングについては、社内で定められたコーディング規約に従って実施されています。

19. インシデント発生時の対応

- 当社は、電子メールやSlack等のコミュニケーションツールにてクラウドサービスカスタマーをサポートしております。セキュリティインシデント等が検知された際には、これらのツールを介して当社にご連絡ください。
- インシデントが発生した場合に、当社がクラウドサービスカスタマーに対して報告する範囲は次のとおりです。
    - 当社がクラウドサービスカスタマーに報告する情報セキュリティインシデントの範囲
        - SLOを超えたシステム停止
        - 不正アクセス／情報漏洩
        - 当社が更新等可能な、上記を引き起こしうる重大なセキュリティ脆弱性
    - 当社がクラウドサービスカスタマーに報告しない情報セキュリティインシデントの範囲
        - 当社が制御できないAWSやGoogle Cloudなどの外部クラウドサービスのセキュリティ脆弱性の対応状況
- インシデントを検知する手段およびクラウドサービスカスタマーに開示する情報については、次のとおりです。
    - SLOを超えたシステム停止：第三者の通知システムによって検知し停止時間および復旧状況についての情報
    - 不正アクセス／情報漏洩：WAFおよびDBへのアクセスログから検知し、影響する顧客範囲およびデータ範囲についての情報
    - 当社が更新等可能な、上記を引き起こしうる重大なセキュリティ脆弱性：定期的なレビューによって検知し、対応予定および対応状況についての情報
- インシデントに関する通知を行う目標時間について当社は以下のように定めます。
    - SLOを超えたシステム停止：停止を検知した後SLOを超え次第に通知を行い、また復旧が完了した際にも通知することを目標といたします。
    - 不正アクセス／情報漏洩／アカウント乗っ取り（なりすまし）／迷惑メール送信：事象を検知したのち影響範囲が判明したら速やかに通知を行うことを目標といたします。
    - 当社が更新等可能な、上記を引き起こしうる重大なセキュリティ脆弱性：事象を検知した後、5営業日以内の通知を目標といたします。また対応が完了し次第に通知を行うことを目標といたします。

- 上記の他、天災等によるシステム停止に関して非災害地域でバックアップから復旧を行う場合があります。

20. 認証

- 当社は、情報マネジメントシステム認定センター(ISMS-AC)が運営する、ISMS適合性評価制度におけるISMS認証およびISMSクラウドセキュリティ認証を取得しています。
- SAPPHIREは、脆弱性の診断についても3ヶ月に1回審査を受けています。クラウドサービスカスタマからご要望があった場合、開示可能な範囲で情報を提供します。

21. 外部クラウドサービスの利用

- 当社では、ピアクラウドサービスとして、次の外部クラウドサービスを利用しています。
  - AWS
  - Google Cloud

22. サービスに関するお問い合わせ

- 当社は、メールやslack等コミュニケーションツールにてクラウドサービスカスタマーをサポートいたしています。サービスや知的財産権に関するお問い合わせ、当社情報セキュリティ責任者へのお問い合わせも、これらのコミュニケーションツールからご連絡いただくことになっております。

22. 契約内容と本書との関係

- クラウドサービスカスタマーと当社間で締結した契約内容と本書の内容が矛盾抵触した場合には、その部分について当該契約内容が優先して適用されるものとします。

24. 当セキュリティホワイトペーパーの改定

- 本書の記載内容に変更があった場合は、速やかにクラウドサービスカスタマーに電子メール等の手段にて当該内容を通知いたします。

改訂履歴

版	改訂年月日	改訂内容 (概要)
1.0	2021/08/01	初版