bellFace セキュリティホワイトペーパー

2.5版

2025年10月

目次

1. はじめに

セキュリティホワイトペーパーの目的

本文書(以下、セキュリティホワイトペーパー)では、ベルフェイス株式会社のセキュリティへの取組みを説明するとともに、Software as a Serivce として提供している bellFace を安全に利用するための考慮ポイントについて紹介しております。

セキュリティホワイトペーパーの対象者

セキュリティホワイトペーパーでは、以下の方を対象として記述されております。

- bellFace をご利用の方
- bellFace の契約をご検討中の方

bellFace とは

bellFace は電話面談システムです。スクリプト機能や資料共有機能などの商談、説明に特化した機能が特長となります。詳細については、以下のサービスサイトをご確認ください。

https://bell-face.com/

2. 情報セキュリティのための方針群

2.1. 情報セキュリティのための方針群 （ISO/IEC27017 項番：5.1.1）

bellFace サービス運営では以下の方針を定めております。弊社の情報セキュリティ基本方針(https://peers.jp/informationsecurity)に従い、サービス運営を行います。セキュリティに関して、極めて重要な事項として取り扱います。

また、bellFace では弊社運用担当者がお客様情報資産(お客様にて保存されるデータ)へのアクセスは、弊社情報セキュリティ規程群に基づき運用を行っており、bellFace サービス運用上、お客様情報資産にアクセスしなければいけない事象が発生した場合は、特定の運用担当者のみしかアクセスできないよう厳格な状態にて運用を行っております。

3. 情報セキュリティのための組織

3.1. 情報セキュリティの役割および責任 （ISO/IEC27017 項番：6.1.1）

bellFace サービス利用規約(https://bell-face.com/terms/id/) にてサービス内容を定義し、サービス提供を実施しております。

なお、弊社およびお客様の責任分界点は以下のように定義しております。

ベルフェイス株式会社の責任

bellFace は、以下のセキュリティ対策を実施します。

- bellFace のセキュリティ対策
- bellFace に保管されたお客様データの保護

- bellFace を構成するシステムのセキュリティ対策

お客様の責任

お客様は、以下のセキュリティ対策を実施する必要があります。

- 各利用者に付与されたパスワードの適切な管理
- bellFace アカウントの適切な管理（登録、停止、管理者権限の付与など）
- bellFace サービスのご利用の過程でアップロード、生成されたデータの適切な管理（お客様資料、商談メモなど）

パブリッククラウドベンダーの責任

基盤となるインフラストラクチャのセキュリティはパブリッククラウドベンダーが確保

※ bellFace はシステムの基盤としてパブリッククラウドベンダーである AWS を利用し構築しております。

AWS のホワイトペーパーに関しては、以下の URL をご参照ください。

AWS ホワイトペーパーとガイド
https://aws.amazon.com/jp/whitepapers/

3.2. 関係当局との連絡 （ISO/IEC27017 項番：6.1.3）

弊社の所在地等に関しては、以下のページをご確認ください。

ベルフェイスシステム株式会社
https://bell-face.com/

bellFace サービスに保存いただくデータの所在は日本国内となります。

3.3. クラウドコンピューティング環境における役割及び責任の共有及び分担 （ISO/IEC27017 項番：CLD 6.1.3）

適切な権限を持つ従業員が開発および運用を業務フローに則り、開発および運用を行っております。イレギュラー発生時(手順書以外の処理)の対応ルールとして、エスカレーションプロセスに基づくエスカレーションを実施し、責任者の判断によって業務の続行、中止を行っております。

クラウドサービスの開発・運用の継続に必要な仕様書のドキュメントを整備し、適宜修正を行っており、開発・運用を継続するための体制維持にも努めております。

4. 人的資源のセキュリティ

4.1. 情報セキュリティの意識向上、教育及び訓練 (ISO/IEC27017 項番:7.2.2)

弊社では、情報セキュリティの意識向上を目的として、入社時、および年に1回以上情報セキュリティ教育を実施しております。

教育の記録、教育参加者の記録、およびテスト結果の記録、再テストが必要な方への連絡等を行い、従業員すべてに対して教育を行っているかどうか弊社内で確認を行っております。

4.2. 資産目録 (ISO/IEC27017 項番:8.1.1)

お客様の情報資産(お客様にて保存されるデータ)と弊社がサービスを運営する為の情報は、明確に分離しております。

4.3. クラウドサービスカスタマの資産の除去 (ISO/IEC27017 項番:CLD 8.1.5)

bellFace の利用契約が終了した場合、解約完了から 1 週間経過した後、システム上にあるデータベースにあるお客様データを削除します。

システム上からの削除完了を示す削除証明の発行は弊社では対応いたしません。
bellFace で利用しているパブリッククラウドベンダーでのデータの削除については、下記 URL をご参照ください。

クラウドにおける安全なデータの廃棄
https://aws.amazon.com/jp/blogs/news/data_disposal/

4.4. 情報のラベル付け (ISO/IEC27017 項番:8.2.2)

お客様が bellFace 上で格納された情報は、お客様が入力した情報がそのままラベル付けとしての機能を果たします。必要に応じて、格納頂いた情報の分類分けをお客様で実施頂けます。また、その情報はお客様のみ変更が可能です。弊社でお客様の情報に対しての変更等は行うことはありません。

5. アクセス制御

5.1. 利用者登録及び登録解除 (ISO/IEC27017 項番:9.2.1)

bellFace では、管理者メニュー上で利用者の招待および利用者の停止を行うことが可能となります。そのため、管理者のみしか利用者の招待および停止を行うことができません。一般ユーザーでは行うことができません。

ユーザー管理
https://help.bell-face.com/categories/676933af8286f848e87a5110/

5.2. 利用者アクセスの提供 (ISO/IEC27017 項番:9.2.2)

お客様は、登録されたユーザーの権限を、自由に切り替えることが出来ます。適切な権限グループを設定することで、閲覧・編集を細かく制御することが可能です。

管理者ユーザーができること
https://help.bell-face.com/categories/675bee0d449dc408d527b71b/

認証の種類

項目	値
認証手段	ID、パスワードによる認証
シングルサインオン(SSO)の利用	SAML2.0 に準拠している場合利用可能(※)

(※) シングルサインオンの利用については、弊社営業担当にご確認ください。

アカウントロック条件

誤ったパスワードを3回入力するとロックがかかります。

パスワードの長さ、文字種

https://help.bell-face.com/faqs/676e6acd2931069c1f87f703/

パスワードの再発行

https://help.bell-face.com/faqs/67692de38286f848e87a3f5b/

5.3. 特権的アクセス権の管理 （ISO/IEC27017 項番：9.2.3）

管理者認証に関しては、ID とパスワードの認証に加え、アクセス元 IP アドレスによる制限を設定する事が可能となっております。ただし、アクセス元 IP アドレスによる制限は、一般ユーザーも同様に適用されます。

5.4. 利用者秘密情報の管理 （ISO/IEC27017 項番：9.2.4）

管理者が、新規利用者を招待したと同時に、招待者のメールアドレスに、招待の受諾用のURL情報が含まれたメールが送信されます。

新規利用者は、その URL にアクセスし、メールアドレス・パスワードを入力・設定した後に、招待を受諾することで、サービスの利用を開始できます。

5.5. 情報へのアクセス制限 （ISO/IEC27017 項番：9.4.1）

bellFace をご利用頂く際のアクセス制御に関しては、利用者として登録されたお客様のみアクセスできる手段を用いております。また、サービス内での情報で共有設定が存在している場合、共有者以外が情報に対して閲覧できないようになっております。

5.6. 特権的なユーティリティプログラムの使用 （ISO/IEC27017 項番：9.4.4）

bellFace では、セキュリティ手順を回避し各種サービス機能の利用を可能とするユーティリティプログラムの提供は行っておりません。

5.7. 仮想コンピューティング環境における分離 （ISO/IEC27017 項番：CLD 9.5.1）

bellFace でお客様が生成したデータについては、論理的に分割されており、制御されております。そのため、お客様が生成したデータを他のお客様が閲覧するという事象は発生しません。

5.8. 仮想マシンの要塞化 （ISO/IEC27017 項番：CLD 9.5.2）

bellFace をご契約いただいた初期状態は初期に登録された管理者および利用者が利用可能な状態でご提供いたします。そのため、ID の管理についてはお客様の管理範囲となります。

bellFace のシステムでは、悪意のある攻撃や脆弱性の特定のための不必要な情報については公開せず、また、必要なポートのみ開放することで、要塞化を行っております。

6. 暗号

6.1. 暗号による管理策の利用方針 (ISO/IEC27017 項番:10.1.1)

bellFace では、お客様に安心して bellFace を通じた商談を実施することを目的として、通信や生成されたデータ等に関して暗号化を実施しております。暗号化については、CRYPTREC 暗号リスト(電子政府推奨暗号リスト) に基づいた暗号化を使用しております。

自社内で独自に作成した暗号化などは脆弱性を誘発するため、一切使用しておりません。

電子政府における調達のために参照すべき暗号のリスト
(CRYPTREC 暗号リスト)
https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022.pdf

ネットワーク

TLS のバージョンは TLS1.2 以上を使用しております。

データベース

データベースに保管されるお客様の各種基本情報(氏名、メールアドレス、各機能で利用するデータなど)はデータベース自体の暗号化を行い、適切なアクセス権のもとで保管しております。

お客様のパスワードに関しては、不可逆暗号化(ハッシュ化)された状態で、データベースに保管しております。また、商談メモなど一部の重要な情報については可逆暗号化された状態でデータベースに保管しております。暗号化方式としては、AWS の機能を用いております。

ストレージ

ストレージ領域における暗号化方式としては、AWS の機能を用いております。

6.2. 鍵管理 (ISO/IEC27017 項番:10.1.2)

bellFace では、お客様データを適切に管理するため、社内情報セキュリティ規程群に基づいた鍵管理手順に沿って鍵管理を実施しております。また、パブリッククラウドベンダーの鍵管理を用い、適切に運用および管理できるようにしております。

7. 物理的及び環境的セキュリティ

7.1. 装置のセキュリティを保った処分又は再利用 (ISO/IEC27017 項番：11.2.7)

bellFace 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物理装置の処分については責任共有モデルに基づき、全てパブリッククラウドベンダーが対応いたします。また、弊社では社内システムにおいても物理装置を用いたシステム構成を行わず、すべて パブリッククラウドベンダーを利用した構成となっているため、物理装置の処分は行っておりません。

社内の他の物理装置等(業務用途貸与 PC 等)は、社内規則に基づき処分もしくは再利用を行っております。

8. 運用のセキュリティ

8.1. 変更管理 (ISO/IEC27017 項番：12.1.2)

サービス内容を変更する場合、影響のあるお客様に対し変更内容をメール、bellFace 内、その他 bellFace 関連サイトのいずれかにてご連絡いたします。また、メンテナンスを実施する際、サービス停止等お客様に影響のある場合も同様の方法にてご連絡しております。

弊社では、Web アプリケーションにおいてバージョン管理を実施し、過去の変更を管理しております。リリース前には、開発者およびテスト担当によるテストを実施し、責任者による承認を経て Web アプリケーションをリリースしております。

8.2. 容量・能力の管理 (ISO/IEC27017 項番：12.1.3)

bellFace では、スケーラビリティを考え設計されており、その設計をもとに bellFace を構築しております。運用時においてリソースの監視を実施しており、容量および能力が必要であれば、必要に応じてリソース拡張を実施しております。

サービス運用上必要な作業は、お客様への影響を配慮し実施しておりますが、お客様に対してサービス中断等の影響が発生する場合は、メンテナンス連絡を通じてお客様にご連絡いたします。

8.3. 情報のバックアップ (ISO/IEC27017 項番：12.3.1)

設備障害、およびシステム障害等によりお客様および弊社データの欠損および消失が発生しないよう、bellFace ではバックアップを実施しております。バックアップの方法については下表のとおりとなります。

バックアップは bellFace の安全な稼働を目的として取得しているため、お客様自身の故意によるデータの消失等に対して復元等の実施はいたしません。

項目	値
バックアップ保管先	日本国内
バックアップ保管世代	日次 × 14 世代
バックアップ保管期間	2週間
バックアップ操作権限	システム運用業務に従事する一部の従業員のみ

8.4. イベントログの取得 (ISO/IEC27017 項番:12.4.1)

お客様にて取得可能なイベントログは以下のとおりとなります。イベントログは CSV 形式でダウンロード可能です。

各種ログのダウンロード

https://help.bell-face.com/faqs/677fd19a1131bf14e25ec75d/

ユーザー管理

https://help.bell-face.com/categories/676933af8286f848e87a5110/

商談記録

https://help.bell-face.com/categories/6769330618ecfdf7b05554dc/

8.5. 実務管理者及び運用担当者の作業ログ (ISO/IEC27017 項番:12.4.3)

bellFace ではインシデントの検知、記録、原因究明のため、ならびに運用の正当性の裏付けを目的として、システム上で各種ログを取得しております。ログの閲覧については、不正なアクセスや改ざんを防ぐため、弊社の一部の従業員しかアクセスが行えないように限られた権限のもとで保管および閲覧可能としています。

当該目的のためにシステムに取得したログについては13ヶ月の保管を実施しております。

8.6. クロックの同期 (ISO/IEC27017 項番:12.4.4)

bellFace で表示される時刻およびログとして記録される時刻は、日本標準時(JST) となっております。時刻は正確な時刻が表示されるよう、システム上で AWS の機能や、パブリックな NTP サービスを参照し、正確な時刻同期を実施しております。

8.7. 技術的脆弱性の管理 (ISO/IEC27017 項番:12.6.1)

弊社では、脆弱性情報を常時収集しております。収集した情報を元に、サービス設備への影響を評価し、弊社の責任範囲において影響がある場合については、速やかに対応しております。

また、お客様に影響しうるインシデントについても、「8.1. 変更管理」に基づく連絡方法をもってお客様にご連絡いたします。

8.8. 実務管理者の運用のセキュリティ (ISO/IEC27017 項番:CLD 12.1.5)

お客様の bellFace の利用手順書は以下のページをご利用ください。

https://help.bell-face.com/

8.9. クラウドサービスの監視 (ISO/IEC27017 項番:CLD 12.4.5)

bellFaceはサービスの提供に必要なシステムおよびログの監視を行っています。また、「8.4 イベントログの取得」の通り、お客様のユーザーの利用状況を確認する機能を提供しております。

9. システムの取得、開発及び保守

9.1. 情報セキュリティ要求事項の分析及び仕様化 (ISO/IEC27017 項番:14.1.1)

「5. アクセス制御」に記載のとおりとなりますのでご確認ください。

9.2. 情報セキュリティに配慮した開発のための方針 (ISO/IEC27017 項番:14.2.1)

情報システムを正確かつ安全に運用するため、開発フロードキュメント群を整備しております。

bellFace サービスを提供する Web アプリケーションのセキュリティに関しては、公的機関発行のガイドラインに準拠して開発を行っております。

10. 供給者関係

10.1. 供給者関係のための情報セキュリティの方針 (ISO/IEC27017 項番:15.1.1)

弊社は、bellFace サービスの開発業務の一部を外部に委託することがございます。委託にあたり、情報セキュリティ規程群にもとづき、事前にセキュリティ上の確認を実施するとともに、情報の取り扱いなどに関する契約を締結しております。
また、契約を継続する委託先においては定期的にセキュリティ上の確認を行っており、終了時にも情報・機器等の返却について確認しております。

10.2. 供給者関係との合意におけるセキュリティの取り扱い (ISO/IEC27017 項番:15.1.2)

bellFace はサービス区分としては SaaS(Software as a Service) となります。責任範囲については「3.1. 情報セキュリティの役割及び責任」をご参照下さい。また、情報セキュリティ対策についても、「3.1. 情報セキュリティの役割及び責任」における範囲において必要なセキュリティ対策を実施しております。

10.3. ICT サプライチェーン (ISO/IEC27017 項番:15.1.3)

bellFace の提供にあたり、一部外部のサービスを利用しております。

外部サービス起因による bellFace の機能の一部の提供が行われない状態を抑止するため、上述のセキュリティ上の確認と合わせ、クラウドサービスレベルチェックシートにより契約時、および年に1度以上リスク管理および評価をしております。

11. 情報セキュリティインシデント管理

11.1. 責任及び手順 (ISO/IEC27017 項番:16.1.1)

弊社の責任範囲に関する情報セキュリティインシデントが発生した場合、お客様には「8.1. 変更管理」に基づいてご連絡いたします。

並行し、弊社では弊社に関連する各官公庁(総務省、個人情報保護委員会)に対しても報告をいたします。なお、責任範囲については「3.1. 情報セキュリティの役割及び責任」をご参照下さい。

11.2. 情報セキュリティ事象の報告 (ISO/IEC27017 項番:16.1.2)

お客様に影響しうる情報セキュリティ事故が発生した場合、弊社の情報セキュリティインシデント基準に基づき、弊社が障害と認定後 、速やかにお客様専用のポータルサイトやメール等にて報告いたします。報告方法については「8.1 変更管理」に基づいた連絡を実施いたします。

11.3. 証拠の収集 (ISO/IEC27017 項番:16.1.7)

情報セキュリティまたは個人情報保護法上のインシデント発生時、可能な範囲で弊社から必要なデータをお客様に提供いたします。各官公庁よりお客様に対して通達があり、ベルフェイスに対しても情報提供の必要がある場合も同様にデータ提供をいたします。

12. 遵守

12.1. 適応法令及び契約上の要求事項の特定 (ISO/IEC27017 項番:18.1.1)

bellFace システムの基盤は日本国内に設置しております。
利用規約を含む本契約の効力、解釈及び履行に関する準拠法は日本法とします。
bellFace サービス利用規約(https://bell-face.com/terms/id/) に記載しておりますので、ご参照ください。

12.2. 知的財産権 (ISO/IEC27017 項番:18.1.2)

利用者データに起因する知財権侵害に関する報告窓口として、以下をご利用ください。

お問い合わせ窓口
03-6811-2211

12.3. 記録の保護 (ISO/IEC27017 項番:18.1.3)

bellFace ではインシデントの検知、記録、原因究明のため、ならびに運用の正当性の裏付けを目的として、システム上で各種ログを取得しております。ログの閲覧については、不正なアクセスや改ざんを防ぐため、弊社の一部の従業員しかアクセスが行えないように限られた権限のもとで保管および閲覧可能としています。

当該目的のためにシステムに取得したログについては13ヶ月の保管を実施しております。

12.4. 暗号化機能に対する規制 (ISO/IEC27017 項番:18.1.5)

bellFace では、お客様に安心して bellFace を通じた商談を実施することを目的として、通信や生成されたデータ等に関して暗号化を実施しております。暗号化については、CRYPTREC 暗号リストに基づいた暗号化を使用しております。

電子政府における調達のために参照すべき暗号のリスト
(CRYPTREC 暗号リスト)
https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022.pdf

改定履歴

版	改定日	改定内容
1.0	2019/07/01	初版発行
1.1	2020/02/05	3.9 暗号化の項について一部改定
1.2	2020/06/11	ISMS 認定情報更新・参照URL更新・4.1利用者管理手法更新
2.0	2022/06/15	ISO27017 セキュリティ要求に基づいた表記方法へ変更
2.1	2022/10/27	新規ユーザー登録を招待制に変更、ISO27017認証情報の追記
2.2	2023/03/01	「8.3 情報のバックアップ」バックアップ世代数の誤記を修正（7世代から14世代）
2.3	2024/7/01	「CRYPTREC 暗号リスト」の最新版への対応
2.4	2024/12/2	ISO 27001:2022 認定への移行に伴う変更
2.5	2025/10/01	新設分割に伴う変更