会計監査確認センター合同会社

Balance Gateway

インフラストラクチャー・セキュリティ FAQ

2024 年 8 月 31 日改訂

目次

本資料について

この「インフラストラクチャー・セキュリティ FAQ」は、Balance Gateway のインフラストラクチャーの概要および主要な情報セキュリティ対策を紹介するためのものです。

ドキュメントの想定利用者

- Balance Gateway を利用する監査チーム（監査人）
- Balance Gateway の利用を前提とした被監査会社（監査クライアント）
- Balance Gateway の利用を前提とした確認回答者

免責事項

本資料の内容は、別段の表示が無い限り、その作成時点の情報に基づき作成しています。将来、関連する制度やルールの改定や追加、その他の状況変化に応じて、本資料に記載された内容は、予告なしに変更されることがあります。

サーバー環境

1. Balance Gateway のホスティングおよびデータの処理と保管はどこで行われるのですか？

Balance Gateway のホスティングおよびデータ処理と保管は、日本国内のデータセンターおよび Microsoft Azure 上で行われています。日本国内の各機器は、施錠された専用のラックで管理されています。Azure のデータ保管は日本国内のリージョンを使用しています。

2. ホスティングされているデータセンターの運用主体はどこですか？

データセンターの運用主体については、セキュリティ上の理由のため非公開としています。

3. Balance Gateway のサーバー環境はどのように監視されていますか？

Balance Gateway サーバーはシステム監視ソフトウェアを使用して監視されています。何らかのサーバー機能障害が起きた場合には、このソフトウェアが会計監査確認センター合同会社のシステム管理者に通知します。具体的な監視ソフトウェア名称については非公開としています。

4. データセンターではネットワークとアクセスはどのように監視されていますか？

スイッチとルーターについては、誤作動、使用帯域、遅延、機能性が監視されています。

5. 必要なサービスパック、パッチの提供は適切なタイミングで行われるのですか？

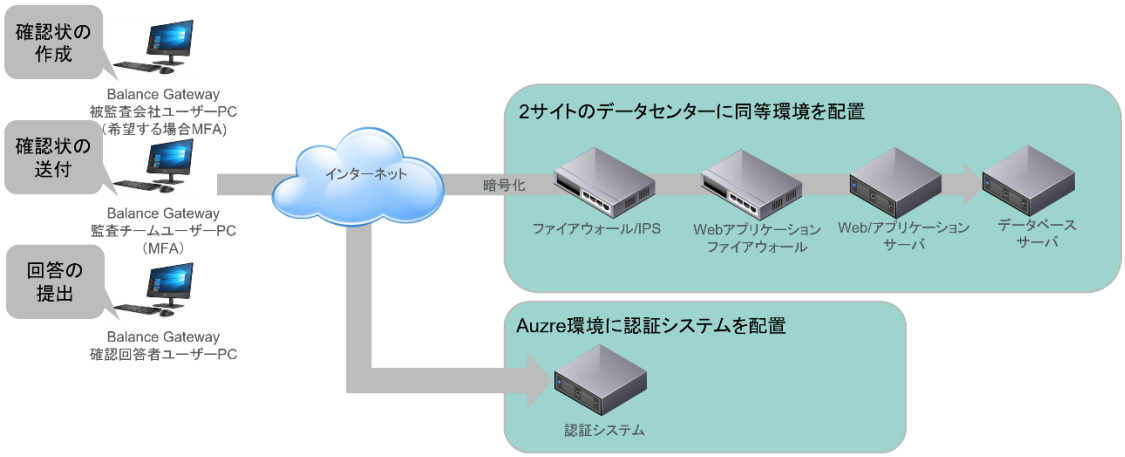
はい。セキュリティの問題を含めた重要なアップデートプログラムは優先的に適用されます。すべてのアップデートプログラムは本番環境に適用される以前に、検証環境で本番環境と同じプロセスに従ってテストされます。本番環境への適用は、テスト結果に基づき、システム責任者の承認を経て、実施されます。詳細は、後述する「開発とテスト」の項目をご覧ください。

6. OS、ミドルウェアのセキュリティ対策のパッチ適用頻度を教えてください。

最低月 1 回の頻度で影響の有無および度合いを確認し、適用しています。

7. Balance Gateway のシステム構成を教えてください。

システムの概要は、下図のとおりです。


確認状の
作成
Balance Gateway
被監査会社ユーザーPC
（希望する場合MFA）
確認状の
送付
Balance Gateway
監査チームユーザーPC
（MFA）
回答の
提出
Balance Gateway
確認回答者ユーザーPC
インターネット
暗号化
2サイトのデータセンターに同等環境を配置
ファイアウォール/IPS
Webアプリケーション
ファイアウォール
Web/アプリケーション
サーバ
データベース
サーバ
Auzre環境に認証システムを配置
認証システム

1

アクセス管理 — ユーザー

1. Balance Gateway には、どのような種類のユーザーの役割がありますか。各ユーザーの役割には、どのような違いがありますか？

Balance Gateway には、監査チーム、被監査会社（監査クライアント）、確認回答者の 3 種類のユーザーの役割が存在します。各役割は、更に、管理者および一般ユーザーの 2 種類に区分されます。例えば、監査チームの管理者および一般ユーザーは、プロジェクト内のすべてのドキュメントを閲覧できます。また、管理者は、プロジェクトへのメンバー追加、承認行為など、プロジェクト内の一定の管理権限を有することが、一般ユーザーとの違いです。

2. Balance Gateway へのアクセスはどのように許可されますか？

監査チームは、各監査事務所を通じた利用申請手続が完了すると、Balance Gateway へのアクセスが可能になります。被監査会社、確認回答者の各ユーザーのアクセスを許可するのは各管理者または監査チームです。いずれのユーザーの場合も、具体的なアクセス方法については、メールで通知されます。

3. Balance Gateway へのアクセスはスマートフォンでも許可されますか？

アクセスは可能ですが動作保証外となっています。

4. Balance Gateway へのアクセスが許可された場合の認証プロセスはどうなっていますか？

Balance Gateway は、ディレクトリサービスでユーザー情報を管理しています。各ユーザーはログイン画面からアカウント／パスワードにより認証されます。また、多要素認証（MFA）の利用も可能です。なお、各プロジェクトへアクセスする際には、初回アクセス時に、プロジェクトごとの初回認証コードの入力が必要となります。

5. Balance Gateway のユーザーの削除は、どのようなプロセスで行われますか？

各アカウントはプロジェクトに紐づいており、プロジェクトが完了するとそのプロジェクトにアクセスすることができなくなります。また、監査チーム、被監査会社、確認回答者のアカウントは、必要に応じて監査チームまたは被監査会社管理者によって削除されます。

6. 使用されているパスワード要件はどのようなものですか？

各ユーザー向けの「Balance Gateway 操作マニュアル」をご参照ください。

7. アカウントのパスワードのリセット手順はどのようなものですか？

ユーザー自身にて、ログイン画面の「パスワードを忘れた方はこちら」リンクからパスワードをリセットすることができます。

8. Balance Gateway のメール通知はどのように送られるのですか？

各ユーザーには、ユーザーID として使用されているメールアドレス宛に、必要な通知メールが個別に送られます。

9. Balance Gateway は、承認されていないユーザーがアプリケーション内のデータやその他の情報（コメントやアラートなど）へアクセスすることを防止するため、どのように設計されていますか？

Balance Gateway では、ユーザーは、監査チームから明確なアクセス権限を与えられたプロジェクトやその中の各確認状（確認回答者情報と回答）のデータだけにアクセスして閲覧できるように設計されています。

10. Balance Gateway は、アップロードされたドキュメントを承認されていないアクセスから守るために、どのように設計されていますか？

アップロードされたドキュメントは、所定の Balance Gateway プロジェクトやその中の各確認状（確認回答者情報と回答）にアクセス権限を与えられたユーザーのみが閲覧できるようになっています。Balance Gateway にアップロードされたファイルにアクセスするには、Balance Gateway の当該プロジェクトへのアクセス権が必要です。

アクセス管理 — システム管理者

1. Balance Gateway にシステム管理者としてアクセスできるのは誰ですか？

会計監査確認センター合同会社の運用管理チームメンバーだけが、システム管理者としての権限を保有します。システム管理者によるアクセスは定期的に確認され、アクセスが不要になったと判断された場合は取り消されます。アカウントは個人と紐づいておりユーザーごとにアクセス権が付与されます。

2. 内部不正に対して、対策を講じていますか？

入退室管理、データベースの暗号化、サーバーへのアクセス記録の管理を実施しています。

3. システム管理者はどのようにメンテナンスを実施しているのですか？

システム管理者は所定の端末からのみ Balance Gateway にアクセスすることが許可されています。

4. システム管理者の端末は盗難、紛失時の対策を実施していますか？

システム管理者の端末には BIOS ロック、ドライブ暗号を適用しています。

開発とテスト

1. 開発とテストのプロセスとはどのようなものですか？

Balance Gateway の本番サーバーに、アップグレードプログラムや修正コード、拡張機能がインストールされる前には、事前にテストが計画され、実施されます。このテストには、アプリケーション性能テスト、ペネトレーションテストなどが含まれます。Balance Gateway のソフトウェア、カスタムコード、またはオペレーティングシステムの変更は、すべてのテストが終了した段階で、承認プロセスを通じて本番環境に配備されます。

暗号化・データ転送・ウイルス対策

1. Balance Gateway を使用する際、データは暗号化されますか？

はい。データは保管中にも転送中にも暗号化されます。

2. Balance Gateway で採用されている暗号化通信はどのようなものを利用していますか？

具体的な暗号アルゴリズムは開示していませんが、暗号アルゴリズムについては適宜見直しを実施し、脆弱性が発見されたアルゴリズムについては無効化を実施しています。

3. 使用される通信プロトコルの種類に制約はありますか？

Balance Gateway では使用するプロトコルとして HTTPS だけを認めています。

4. Balance Gateway サーバーにおけるウイルスの検出と防御の方法を教えてください。

ウイルス検出は、すべてセンターコンソールから行われます。ファイルがアップロードされると、リアルタイムのオンアクセススキャンが実行されます。ウイルスチェックのパターンはベンダーから自動的にダウンロードされ、更新が反映されます。

5. Balance Gateway にアップロードされるファイルについてウイルス対策以外にセキュリティ対策を実施していますか？

ネットワーク伝送時に IPS によりネットワーク経路上で不正ファイルを検知・ブロックします。

6. Balance Gateway で送信するメールはウイルスチェックされますか？

Balance Gateway はあらかじめ定められた内容でメールを送信するため、ウイルスが混入することはありません。

セキュリティ — ネットワーク

1. データセンターのアプリケーション間で共有される機能はありますか？

Balance Gateway はデータセンターでホスティングされていますが、他のアプリケーションとの共有はございません。

2. Balance Gateway はインターネットからどのように保護されていますか？

Balance Gateway サーバーはファイアウォールを介してインターネットに接続しています。

3. Balance Gateway ではどのような侵入防御システムが使用されていますか？

Balance Gateway 環境の境界に侵入防御システム（IPS）、Web アプリケーションファイアウォール（WAF）を採用しています。IPS、ファイアウォール、VPN のログ情報はログアグリゲーターに送られ、ここで異常な動きや変則的な動作が検知された場合は、システム管理者に通知されます。ハードウェアとソフトウェアのチェックは自動化されたツールによって実行されます。ツールにはアラートレベルが定められており、システムに問題が発生したと判断するとシステム管理者に通知されます。

4. Balance Gateway では、どのようなセキュリティ脆弱性テストまたはペネトレーションテストが行われているのですか？

Balance Gateway アプリケーションだけでなく、社内外と接する Balance Gateway インフラストラクチャー（サーバーやネットワーク機器など）についても、所定のセキュリティ脆弱性テストを定期的に実施しています。テスト結果は Balance Gateway のシステム管理者が評価し、脆弱性が見つかった場合には、問題を調査し、軽減策を講じるか修正が行われます。

5. 直近のテストの報告書を開示することは可能ですか？

報告書の内容はシステム情報を含むため開示しておりません。

6. Balance Gateway ではデータのキャッシングは行われるのですか？

Balance Gateway でデータのキャッシングが行われることはありません。すべてのデータは、ユーザーからのリクエストに応じて、データセンターに設置された Balance Gateway サーバーから直接提供されます。

7. Balance Gateway のアクセスログはユーザーに提供されますか？

ユーザーにアクセスログは提供していません。

8. Balance Gateway のアクセスログの保持期間はどのくらいですか？

期間については開示しておりません。内部で定められた期間保持しています。

セキュリティ ― 施設

1. Balance Gateway がホスティングされているデータセンターでは、物理的アクセスのセキュリティはどのように担保されていますか？

データセンターに立ち入ることができるのは、制限されたエリアへの立ち入りを必要とする担当者に制限されています。データセンターの物理的セキュリティ対策として、警備員、出入り口での認証、監視カメラ、案内人の帯同による来訪者の入退室記録を採用しています。

2. 業務上の立ち入りを必要とする人材に対しては、どのような物理的なアクセスの制限を行っていますか？

ID カードの識別コードは、建物内の必要とされる領域だけに立ち入り権限を与えるように設定されています。

3. データセンター施設のロビーへの立ち入りはどのようになっていますか？ロビーのスタッフは来訪者の記録を維持していますか？

データセンターは、それを収容する施設のロビーとは直接つながっていません。データセンターに立ち入る際の ID カードを発行するのは施設の管理スタッフではなく、権限のあるデータセンター職員です。来訪者の記録は保管されます。

4. 臨時的なスタッフやコンサルタント、受託業者によるデータセンターへの立ち入りは認められていますか？

臨時的なスタッフやコンサルタント、受託業者によるデータセンターへの立ち入りは、データセンター施設内でのサービス提供が必要な場合にのみ、権限のあるデータセンター職員が限定的に許可します。一時的な立ち入りを許可された個人がデータセンター施設に立ち入る際は、ID カードが割り当てられ、システム管理者が付き添うことになっています。

5. データセンター施設は、外観からデータセンターであることが分かりますか？

施設の建物は、データセンターであるとは表示されていません。

6. 業務時間終了後のデータセンター施設への立ち入りはどのように管理されているのですか？

警備員が常駐しています。

7. 来訪者が建物に立ち入る際は ID カードの着用は義務付けられていますか？

はい。来訪者は ID カードの常時携帯が義務付けられています。

8. ID カードの付与履歴は保管されていますか？

はい。ID カード付与履歴は保管されています。

9. データセンターを含む運用施設を見学することはできますか？

他のお客さまとの機密保持の観点から見学を受け入れておりません。

運営と手続に関する情報

1. すべてのサーバーのオペレーティングシステムのインストールと保守は、データセンターの技術者が担当するのですか？

通常業務として、会計監査確認センター合同会社のシステム管理者がオペレーティングシステムのインストールとサポートを担当しています。

2. Balance Gateway のシステム導入と日常的な運用は誰が管理しているのですか？

会計監査確認センター合同会社の運用管理チームが管理しています。このチームは、運営とサポートを担当する事務センタースタッフ、アプリケーション開発チーム、ネットワークを含むインフラとセキュリティチームで構成されます。

3. 運用管理はすべて会計監査確認センター合同会社内で実施しているのですか？

いいえ。一部の業務は会計監査確認センター合同会社管理のもと外部委託しています。

4. どのような業務を委託しているのですか？

アプリケーションの開発・保守業務、インフラの開発・保守業務、リソース監視（24 時間監視）、セキュリティ監視（24 時間監視）を外部組織に委託しています。各組織とは機密保持契約を締結しています。各委託業務においては、必要な情報のみにアクセスが限定されています。また、委託先には、サーバーなど本番環境の操作権限は付与されていません。

5. 万が一データが漏れた場合、どのような対応を誰がとることになるのでしょうか？

情報漏洩があった場合は所定の緊急窓口へ報告後、専門チームが影響範囲や原因の特定、外部機関への報告等を行うなど対応を実施します。

6. インシデント対応した際の報告はどのように行われるのですか？

調査を行い影響範囲や原因が特定でき次第、影響があったユーザーに監査チームを通じて報告します。

7. 将来必要となるネットワーク容量、処理能力、ストレージ容量に関する予測は継続的に検討されているのですか？

はい。処理能力やストレージの追加が必要となる時期を予測し判断するため、それぞれの機器の利用状況をモニタリングしています。

8. Balance Gateway におけるワークスペースと個々のファイルのサイズ制約について教えてください。

Balance Gateway の全体的なディスクスペース使用量は毎日モニタリングされ、必要に応じて短期間で拡張できるようになっています。

バックアップとデータ保護

1. データのバックアップとリストアを実行する際の標準的な手順を教えてください。

Balance Gateway では日次でデータ更新分がバックアップされるほか、週次ですべてのデータがバックアップされます。データのバックアップはオンサイトとミラーサイトで 2 回繰り返されます。バックアップデータはセキュリティが確保された環境で保管しています。また、システム障害の発生などデータの欠損が確認された場合には、状況に応じてリストアを実施します。

2. 契約の途中や終了時にデータを移行できますか？

Balance Gateway 上で作成された帳票やアップロードされた各種データは、監査チームおよび被監査会社にてダウンロード可能です。

3. 契約が終了した後のデータの取り扱いを教えてください。

プロジェクトが終了したデータについては該当領域が削除されます。

4. Balance Gateway では災害復旧サイトを活用していますか？

はい。常時、複数拠点で運用されており、運営環境のフェイルオーバー（障害迂回）が可能になります。災害復旧計画は年 1 回以上見直され、テストされています。

第三者認証

1. Balance Gateway はどのような第三者認証を受けていますか？

米国公認会計士協会「セキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシーに関する Trust サービス規準」の日本公認会計士協会による翻訳のうち、セキュリティ、可用性、処理のインテグリティ及び機密保持の規準に基づいた第三者による評価を受けています。これには、金融情報システムセンター（FISC）の金融機関等コンピュータシステムの安全対策基準に関する評価も含まれています。

内部統制のデザインについて、SOC2 Type1 レポートを 2019 年 12 月に取得いたしました。また、内部統制のデザインに加えて運用状況も含めた SOC2 Type2 レポートは 2020 年 9 月に取得しており、年 2 回定期的に再取得しています。

問い合わせ先

1. Balance Gateway に関する質問の問い合わせ先はどこですか？

使用前のシステムに関するお問い合わせは、ご担当の監査チームにご連絡ください。

使用開始後のお問い合わせ窓口は、以下のとおりです。

会計監査確認センター合同会社　確認状事務センター

受付時間：午前 9 時 30 分から午後 5 時 30 分 ※土曜日・日曜日・祝日・当社休業日を除く

TEL: 043-369-4099

E-Mail: support@balancegateway.jp