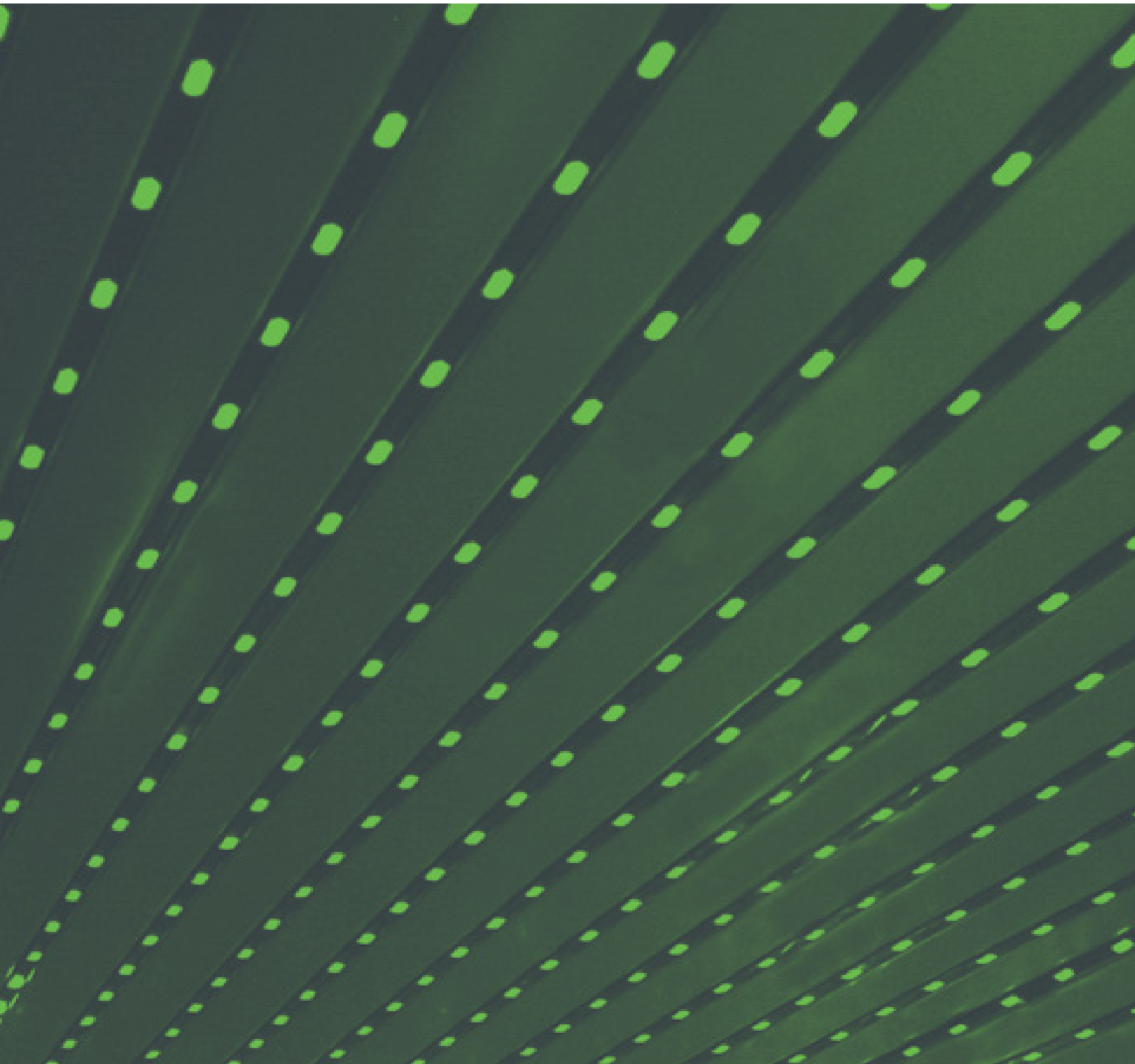
ガイド

ビジネス継続性への対応

バージョン 3.0 2022 年 8 月 16 日公開



目次

概要

このガイドはなぜ必要ですか。

堅牢に設計したソリューションでも、サービス障害が発生することがあります。Duo は、4 年以上にわたって 99.99% を超える稼働時間を維持していますが、それでも Duo のサービスが私用できなくなることがあります。

サービス障害は、従業員の生産性に影響し、一時的にセキュリティ態勢が脆弱になる可能性があります。Duo は、信頼できるアクセスプロバイダーとして、顧客が起こりうるすべての状況に備え、潜在的な障害に対応するための計画を立てられるようにします。

Duo のサービスの詳細と、クラウドアーキテクチャと製品開発プロセスが高可用性を確保するためにどのように設計されているかについては、当社のサービスの信頼性のホワイトペーパーを参照してください。

サービス障害と環境について

Duo サービスが利用できない場合、Duo で保護されたアプリケーションと IT 組織の対応方法について検討する必要があります。

潜在的な障害のシナリオを考慮することにより、最終的に Duo のエクスペリエンスが向上します。

このガイドは、以下の点で役に立ちます。

- サービス障害の 2 つのカテゴリを理解する
- Duo の障害モードと、fail safe と fail secure のいずれかを選択する方法を理解する
- アプリケーションが障害の種類によってどのように動作するかを理解する
- 障害発生時のユーザへのメッセージ

成功を実現するためのプラン

このガイドを読み、サービス障害のシナリオとアプリケーションの障害モードの動作を理解し、アプリケーション固有のディザスタリカバリ（DR）計画を作成することを強くお勧めします。この計画には以下が含まれています。

- 障害モードが想定どおりに動作しない場合 Duo のクラウドサービスをブロックまたはバイパスするために必要なプロセスを理解する。
- **保護された各アプリケーション**の認証ワークフローから Duo を削除する手順。

設定の決定

各アプリケーション（使用可能な場合）にどの障害モード設定（Fail safe または Fail secure）を使用する必要があるかを慎重に検討してください。* 選択は次の要素に依存する可能性があります。

- ポリシーとコンプライアンスの要因
- 保護されたアプリケーション内に含まれるデータのタイプ
    - 健康記録、財務、個人識別情報（PII）、知的財産（IP）など
- さまざまなレベルのアクセス権を持つユーザのグループ
- セキュリティと使いやすさのバランスの必要性

*Duo.com/docs から特定のアプリケーションのマニュアルを参照して、設定可能な障害モードが機能しているかどうかを確認します。

サービスが低下した場合の障害モード設定とアクションプランに関しては、一般に、組織のアプリケーションが該当する主なカテゴリは 3 つあります。

制限レベル	到達不能（障害モードが作動）	品質低下（障害モードは作動しない）
最も制限の厳しいカテゴリ 保護されたアプリケーション内に含まれる契約、法律、ポリシー、またはデータの機密性には、**例外なく二要素認証が必要**とされます。	Fail secure	ユーザとグループを「バイパス」ステータスに切り替えないでください。これにより、二要素認証がスキップされます。
制限的 一部のユーザのサブセットは、例外なく、常に二要素認証にパスする必要があります。	Fail secure	例外なく二要素認証にパスする必要があるユーザとグループは「バイパス」ステータスに切り替えないでください。これにより、二要素認証がスキップされます。 二要素を使用せずに該当アプリケーションにアクセスを許容できるユーザおよびグループにおいては、二要素認証をスキップできるように「バイパス」に切り替えることができます。
制限の少ないカテゴリ 保護されたアプリケーション内に含まれる契約、法律、ポリシー、またはデータの機密性には、**あらゆる状況での二要素認証の使用が義務付けられていません。**	Fail safe	二要素を使用せずに該当アプリケーションにアクセスを許容できるユーザおよびグループにおいては、二要素認証をスキップできるように「バイパス」に切り替えることができます。

* ユーザのグループが複数のアプリケーションにアクセスできる場合は考慮してください。ユーザを「バイパス」に設定すると、アクセスできるすべてのアプリケーションの二要素認証がスキップされます。グループが別のアプリケーションにアクセスするためにこれを行う必要がある場合は、そのグループの該当アプリケーションへのアクセスを最初に削除する必要があります。

サービス障害の種類

Duo サービス障害は、通常、Duo サービスが**到達不能**な場合、または、Duo サービスの**品質低下**が発生した場合の 2 つに分けられます。

Duo が到達不能であることおよびサービスの品質低下との違いを理解することは、Duo で保護されたアプリケーションの動作、そして最終的にはエンドユーザのエクスペリエンスに影響を与えるため、重要です。

Duo サービスに到達不能

(障害モードが作動)

- Duo サービスが一時的に使用できない
  - Duo サービスが、Duo プロンプトの表示に失敗するか、180 秒以内に AUTH API 要求への応答に失敗する
- ネットワーク接続の問題により、顧客のアプリケーションが Duo サービスへ到達できない。これらは通常、顧客のローカルネットワークで発生しますが、地域レベルまたはグローバルレベルで発生することもあります。
  - 建設会社が光ファイバを切断してしまう
  - ファイアウォールまたは DNS の問題
  - ISP への接続またはルーティングの問題
- アプリケーション/インテグレーションの問題
  - Duo で保護されたアプリケーションの設定ミス

Duo サービスの品質低下

(障害モードは作動しない)

- 二要素方式の障害
  - Duo のテレフォニープロバイダー（SMS/コール）によるサービス障害
  - APNS（Apple プッシュ通知サービス）がユーザの iPhones にプッシュ通知を配信できない*
- 認証が完了しない
  - Duo により不正なコードがプッシュされたため、ユーザは正常にログインできない
  - Duo 認証の遅延と障害は増加するが、サービスの一部は利用可能

*ユーザが電話での通知を許可することを忘れることはよくあります。これは Duo サービスの品質低下とは見なされません。ユーザが Duo モバイルアプリを起動すると、保留中の認証要求が表示されます。その他のエンドユーザのトラブルシューティングについては、『iOS』または『Android』のガイドを参照してください。

サービス障害がいつ発生したかを知るにはどうすればよいですか。

サービス障害が疑われる問題がユーザまたはユーザの顧客に発生している場合、まず、status.duo.com から、可能性がある障害に関する情報を確認してください。サービス障害に起因しないサービス停止または技術的な問題が発生していると思われる場合は、Duo サポートにお問い合わせください。

Duo のクラウドサービスをモニタリングするための他のオプションについては、こちらのナレッジベースの記事を参照してください。

Duo 障害モード：Duo サービスに到達不能

障害モード（「failmode」とも呼ばれる）は、Duo サービスが到達不能、または重大な問題が検出された場合に作動します。a Duo には、検出されたエラーに基づいて障害モードが作動するエラー検出メカニズムがあります。

Duo サービスに継続的にアクセスできるように、お客様は、すべての Duo の IP 範囲への通信を許可する必要があります。こちらの記事では、追加の考慮事項を含む IP 範囲のリストを参照できます。

場合によっては、他の原因によりサービスが中断される可能性があります。たとえば、Duo サービスは到達可能ですが、他の理由で認証が失敗している可能性があります。この詳細については、Duo サービスの品質低下までスクロールダウンしてください。

障害モードは、2 つの方法のいずれかで動作するように設定できます。

1. **Fail safe**（「フェールオープン」とも呼ばれます）：Duo サービスに到達できない場合、ユーザはプライマリ認証にパスすると、Duo で保護されたアプリケーションへのアクセスが**許可**されます。
    - これにより、二要素認証が一時的にバイパスされるため、セキュリティ態勢が弱くなります。
    - ユーザへの負担は少なく、ワークフローが中断されることはありません。従業員は引き続きログインして作業できます。
    - たとえば、authproxy cfg ファイルには、以下の構文がサーバーセクションに表示されます。Authentication Proxy 設定の詳細については、こちらをクリックしてください。

```
failmode=safe
```

2. **Fail secure**（「フェールクローズ」とも呼ばれます）：Duo サービスに到達できない場合、ユーザはプライマリ認証にパスし ても、Duo で保護されたアプリケーションへのアクセスが**拒否**されます。
    - これは最も安全なオプションです。
    - アプリケーションへのユーザアクセスが拒否されるため、日々の業務が中断される可能性があります。
    - たとえば、authproxy.cfg ファイルには、以下の構文がサーバーセクションに表示されます。

```
failmode=secure
```

Fail safe モードまたは Fail secure モードを有効にするかについては、以下の「設定の決定」の項を参照してください。

Duo 障害モード：Duo サービス品質低下

この場合、Duo Authentication Proxy、Duo Access Gateway、またはその他の Duo で保護されたアプリケーションは、Duo サービスに到達できますが、認証は完了できません。障害モードは動作しません。

考えられるシナリオ

- 認証が完了できない
    - 実際の例：Duo が送信したコードが古いバージョンの Duo Prompt を使用している顧客の認証を阻んでしまった。ユーザは、プライマリ認証にパスし、セカンダリ認証リクエストを承認した後、ログインに失敗しました。

- 複数の認証方式の失敗
    - 実際の例：Duo の SMS サービスは、ユーザにテキストメッセージを正常に配信できず、ユーザは認証できませんでした。

解決策

一部の解決策は、すべてのシナリオにおいて、すべての顧客に実行可能ではない場合があります。たとえば、ファイアウォールルールの変更は、ユーザにメッセージを送るよりも負担が大きい場合があります。お客様の組織に最適な解決策を検討してください。品質低下の問題は、通常、30 分以内に解決されます。次のいずれかの解決策を採用する場合は、**問題の解決後に変更内容を元に戻してください。**

- サービスの品質低下が続く状態で、認証ポリシーを適用し、二要素認証をバイパスします。Duo の有料版をお持ちのお客様は、認証ポリシーを利用できます。この解決策は、Duo サービスが到達不能である場合にも使用できます。
    - 方法：アプリケーションレベルの認証ポリシーを作成し、一時的に適用します。
    - 実行内容：ユーザは二要素認証を完了せずに特定のアプリケーションにアクセスできるようになります。ユーザのグループメンバーシップに基づいて、アクセスを制限したり有効にしたりすることができます。

- status.duo.com に回避策が掲載されている場合は、サービス停止の旨と回避策をユーザに案内します。
    - 方法：以下の「エンドユーザ メッセージング テンプレート」の項を参照してください。[Status.duo.com] に移動して、Duo が一時的な回避策を識別しているかを確認します。
    - 実行内容：お客様の組織と Duo の双方が問題を認識し、解決に取り組んでいることをユーザに保証します。

- すべてまたは一部のユーザを「バイパス」ステータスに設定されたグループに移動します。
    - 方法：ユーザがまだグループに属していない場合、手動または一括でユーザをグループに移動します。そのグループは、1) 保護されたアプリケーションへのアクセスと、2) 「バイパス」ステータスへの設定を必要とします。
    - 実行内容：これにより、グループ内のすべてのユーザに対する二要素認証はバイパスされます。

- Duo が動作しないよう、アプリケーションの設定/プロファイルを元に戻します。
    - 方法： duo.com/docs から特定のアプリケーションのマニュアルを参照してください。
    - 実行内容：一連の認証から二要素認証を削除します。

- Duo Authentication Proxy を使用するアプリケーションの場合は、プライマリ専用モード機能を使用します。
    - 方法：この機能は Authentication Proxy バージョン 2.14.0 で導入され、プロキシサーバーでコマンドを実行することによって有効になります。
    - 実行内容：これにより（デフォルトは 1 時間、最大 4 時間）デフォルトの「Fail safe」を使用する RADIUS または LDAP アプリケーションのすべてのログインに対して、Duo 認証を一時的にスキップします。

- ファイアウォールルールを使用して手動で Duo のサービスをブロックし、到達不能な状況をつくる。
    - 方法：TCP ポート 443 で *.duo.com および *.duosecurity.com をブロックします。
    - 実行内容：これにより、障害モードが動作します。Fail safe が設定されている場合、アプリケーションへのアクセスは二要素認証なしで許可されます。Fail secure が設定されている場合、アクセスがブロックされます。status.duo.com を頻繁にモニタし、変更を元に戻すタイミングを確認します。

アプリケーションの障害モードの動作について

サービス障害の際、障害モードの設定オプションと動作は、Duo が保護しているアプリケーションによって異なる場合があります。この項では、Duo によって開発されたアプリケーション、Duo の WebSDK、および主なサードパーティによって開発されたアプリケーションに関する重要な違いと詳細を調べ、Duo で保護されたアプリケーションがサービス障害によってどのように影響を受けるかを理解できるようにします。

障害モード制御を提供する Duo 開発のアプリケーション

次の表は、障害モード制御を提供する Duo が開発およびサポートしているアプリケーションの一覧と、さまざまなサービス障害シナリオで障害モードが動作する方法としない方法の詳細を示しています。すべての機能とセキュリティの改善を確実に行うために、常に最新バージョンに更新することをお勧めします。

- Duo Authentication Proxy
- Duo Access Gateway（DAG）
- Windows ログオン/RDP 用の Duo
- Duo Unix
- AD FS 2.X
- AD FS 3/4
- OWA
- RD Web/ゲートウェイ
- Oracle Access Manager

障害モード制御を提供しない Duo 開発のアプリケーション

- Duo Network Gateway（DNG）
- Microsoft Azure Active Directory (Conditional Access)
- Duo Single Sign-On

WebSDKv2

Duo の WebSDKv2 には、障害モードを作動したり、WebSDK アプリケーションから Duo サービスにアクセスできるかを自動的に検証したりするための組み込みメカニズムがありません。Duo のクラウドサービスにアクセスできなくなった場合、WebSDK だけでは、二要素認証を正常に完了せずにユーザを認証することはできません。

意図せず 2FA がバイパスされる状況を防ぐために、アプリケーションが Fail safe（オープン）になる条件を注意深くプログラムすることが非常に重要です。サービスをモニタするには、Duo の Auth API ping エンドポイントを使用して、Duo サービスの疎通チェック（Duo のインテグレーション情報は不要）を実装し、次に Auth API チェックエンドポイント（推奨）を使用してインテグレーション情報と署名を確認します。詳細については、こちらのドキュメントを参照してください。

カスタムの Fail safe 動作を開発する場合は、障害モード動作を呼び出す条件を十分にテストするようにしてください。常に、Fail secure（クローズ）はすべてのシナリオで最も安全なオプションです。

WebSDKv4

Duo の WebSDKv4 には、Duo のサーバーがアクセス可能であり 2FA 要求を受け入れることができるかどうかを判断するための組み込み関数が含まれています。この関数の呼び出しに関するドキュメントは、こちらから入手できます。WebSDKv2 と同様に、アプリケーション開発者は、Duo 関数がエラー（Fail safe または Fail secure）を返した場合にアプリケーションをどのように処理するかについてのロジックをアプリケーションに組み込んでおく必要があります。アプリケーションに Duo のサービスや障害の処理方法を決定するロジックへのチェック機能が含まれていない場合、デフォルトで Fail secure（クローズ）になります。

常に、Fail secure（クローズ）はすべてのシナリオで最も安全なオプションです。

サードパーティによる開発

Duo はできる限り多数のサードパーティと連携し、インテグレーションがベストプラクティスに沿っている確認しますが、サードパーティが審査用に開発したインテグレーションを提出したり、当社に通知したりすることは要請していません。そのため、Duo はすべてのサードパーティのインテグレーションと、それらがどのように障害モードの制御を提供できるかを必ずしも認識しているわけではありません。

次に、一般的なサードパーティにより開発された Duo インテグレーションのリストと、それらが障害モードをサポートしているかどうかを示します。

- LastPass
  - 設定可能な障害モードはありません。
  - ユーザはデバイスを信頼することができ、一定期間 MFA を再度実行する必要はありません。
  - DR のシナリオでは、管理者は LastPass にログインし、認証ワークフローから Duo を削除する必要があります。

- 1Password
  - 設定可能な障害モードはありません。
  - オフラインアクセスまたはスタンドアロン vault の MFA は必要ありません。

- Okta
  - 設定可能な障害モードはありません。
  - DR のシナリオでは、管理者はログインし、認証ワークフローから Duo を削除する必要があります。
- OneLogin
  - 設定可能な障害モードはありません。
  - DR のシナリオでは、管理者はログインし、認証ワークフローから Duo を削除する必要があります。
- Ping Federate
  - 設定可能な障害モードを提供します。マニュアルは こちらをご覧ください。
- CAS
  - 設定可能な障害モードを提供します。マニュアルはこちらをご覧ください。

重要：すべてのインテグレーションが障害モードの動作を制御するメカニズムを提供するわけではありません。

- Authentication Proxy または Duo Access Gateway を使用したインテグレーションには、障害モードを指定する**オプションがあります。**
- Duo が開発したインテグレーションのほとんどは、インストール中に障害モードの設定を行うことができます。たとえば、Windows ログオンおよび RDP 用の Duo 認証の障害モードは、インストーラで設定できます。ほとんどの Duo アプリケーションパッケージでは、インストール後の障害モードの設定（たとえば、Duo Unix や Windows ログオンなど）を変更する方法も提供されています。
- Thycotic、Ping Federate、LastPass などのサードパーティによって作成された Duo のインテグレーションは、障害モードを制御する方法を提供できず、デフォルトで Fail secure になる可能性があります。障害もノードが設定可能かを確認するには、ベンダーのドキュメントを参照してください。
- WebSDKv2 統合には、障害モードをチェックするロジックが含まれません。詳細については、「アプリケーションが障害の種類によってどのように動作するかを理解する」の項を参照してください。
- Azure 条件付きアクセス（CA）は、Azure のクラウドサービスが Duo のクラウドサービスに到達できない場合、フェールクローズします。
  - サービス停止が長期間になる場合、ユーザが 2FA なしでアプリにアクセスできるようにするために、お客様は Duo 2FA 要件を CA ポリシーから削除することを検討しなければならない場合があります。
- Duo Network Gateway（DNG）は、Duo のクラウドサービスに到達できない場合、フェールクローズします。
- ユーザは、Duo SSO と連携するアプリケーションでの認証を受けられなくなります。
  - Duo SSO はプライマリ認証とセカンダリ認証の両方を処理するため、ユーザはサービスに直接アクセスできる必要があります。
  - 停止が長期間になる場合、お客様は、Duo SSO とアプリケーションの連携を手動で解除し、別の認証ソースを使用するようにアプリケーションを設定することを検討しなければならない可能性があります。この設定は、多くのアプリケーションでは煩雑で非実用的な変更になることが多く、あくまでも最後の手段として検討する必要があります。

エンドユーザ メッセージング テンプレート

インシデントの発生時に組織がエンドユーザにメッセージを送信するタイミングを考慮してください。ユーザが問題を報告した後すぐ、Duo が status.duo.com に通知を投稿した後だがユーザがまだ問題を報告する前、またはインシデントが 20 分以上未解決のままである場合などに行う可能性があります。

時刻

- 平日の午前 11 時にインシデントが発生した場合は、即時にユーザへ知らせる必要があります。
- 週末の午後 11 時にインシデントが発生した場合は、ユーザへの伝達はすぐには必要ないかもしれません。

四半期の時期

- 四半期の最終週にインシデントが発生した場合は、時刻に関係なく、即時にユーザに知らせる必要性があります。

アクセスの重要度

- 重要なアプリケーションへのアクセスに影響を与えるインシデントが発生した場合は、時刻、日付、またはその他の要因に関係なく、速やかな連絡が必要になります。

Duo サービスが到達不能または品質低下

Duo が到達不能になったときに Fail safe を使用している場合、またはサービスの品質低下が生じたときに手動で障害モードを作動させる場合：

件名： 認証に関する問題が発生しています

本文： Duo は、サービス障害を報告しています。一時的な回避策として、当社は、Duo 二要素認証の要件を引き上げています。問題が解決された後、二要素認証が再開されます。

Fail secure を使用している場合：

件名： 認証に関する問題が発生しています

本文： Duo 二要素認証の問題が発生しています。<アプリケーション> に含まれるデータの性質により、この問題が解決されるまでアクセスは拒否されます。

認証方式固有の問題

件名： 認証に関する問題が発生しています

本文： Duo は、<push/SMS/phone> サービスに関する問題を報告しています。一時的な回避策として、<SMS/push/phone のコールバック> を使用してください。問題が解決し次第、アップデートがあります。

よくある質問（FAQ）

障害モード作動時に通知を受けることはできますか。

障害モードは、Duo Authentication Proxy または Duo で保護されたアプリケーションでローカルに設定され起動されます。モニタリングツールまたは SIEM ソリューションを使用して、障害モードの発生を監視することをお勧めします。

Authentication Proxy のログを調べることによって、障害モードが作動したかどうかを確認できます。ログを保存するデフォルトのディレクトリは、64 ビット Windows マシンでは C:\Program Files (x86)\Duo Security Authentication Proxy\log、32 ビット Windows マシンでは C:\Program Files\Duo Security Authentication Proxy\log です。

次に、障害モードが呼び出されたときに表示される、2 つの Duo Authentication Proxy ログの例を示します。

1. **Fail safe** ログの例

```
!! Auth Proxy versions 2.11.0 and later

2018-11-09 16:53:57-0500 [-] (('10.0.1.99', 54698), 146): Failmode Safe - Allowed Duo login on
preauth failure
2018-11-09 16:53:57-0500 [-] (('10.0.1.99', 54698), 146): Returning response code 2: AccessAccept
2018-11-09 16:53:57-0500 [-] (('10.0.1.99', 54698), 146): Sending response


!! Auth Proxy versions 2.10.1 and earlier

2016-03-22 16:52:22-0400 [-] (('10.2.4.121', 43031), 170): Allowed Duo login on unexpected failure
2016-03-22 16:52:22-0400 [-] (('10.2.4.121', 43031), 170): Returning response code 2:
AccessAccept
2016-03-22 16:52:22-0400 [-] (('10.2.4.121', 43031), 170): Sending response
```

2. **Fail secure** ログの例

```
!! Auth Proxy versions 2.11.0 and later


2018-11-09T16:57:51-0500 [-] (('10.0.1.99', 43674), 63): Failmode Secure - Denied Duo login on
preauth failure
2018-11-09T16:57:51-0500 [-] (('10.0.1.99', 43674), 63): Returning response code 3: AccessReject
2018-11-09T16:57:51-0500 [-] (('10.0.1.99', 43674), 63): Sending response


!! Auth Proxy versions 2.10.1 and earlier


2016-03-22 16:54:38-0400 [-] (('10.2.4.121', 53573), 109): Denied Duo login on unexpected failure
2016-03-22 16:54:38-0400 [-] (('10.2.4.121', 53573), 109): Returning response code 3: AccessReject
2016-03-22 16:54:38-0400 [-] (('10.2.4.121', 53573), 109): Sending response
```

以下は、SIEM 対応の authevents.log からの出力です。

1. **Fail safe** ログの例

```
!! Auth Proxy versions 2.11.0 and later

{"username": "testuser1", "status": "Allow", "client_ip": null, "server_section":
"radius_server_auto", "timestamp": "2018-11-09T21:53:57.950000Z", "auth_stage": "Secondary
authentication", "factor": null, "msg": "Failmode Safe - Allowed Duo login on preauth failure"}

!! Auth Proxy versions 2.10.1 and earlier

{"username": "testuser1", "status": "Allow", "client_ip": null, "server_section":
"radius_server_auto", "msg": "Allowed Duo login on unexpected failure", "timestamp": "2018-04-
17T21:39:13.416000Z", "auth_stage": "Secondary authentication"}
```

2. **Fail secure** ログの例

```
!! Auth Proxy versions 2.11.0 and later

{"username": "testuser1", "status": "Reject", "client_ip": null, "server_section":
"radius_server_auto", "timestamp": "2018-11-09T21:57:51.326000Z", "auth_stage": "Secondary
authentication", "factor": null, "msg": "Failmode Secure - Denied Duo login on preauth failure"}

!! Auth Proxy versions 2.10.1 and earlier

{"username": "testuser1", "status": "Reject", "client_ip": null, "server_section":
"radius_server_auto", "msg": "Denied Duo login on unexpected failure", "timestamp": "2018-04-
17T21:38:11.822000Z", "auth_stage": "Secondary authentication"}
```

Duo の導入は、高可用性を備えて構築されていますか。それとも「アクティブ/アクティブ」として設計されていますか。

はい。Duo の導入を、単一の端末で考えることはできません。Duo は、多数の独立したクラスタまたは顧客の成長をサポートするための「導入環境」を備えており、1 つの導入環境における障害の影響を最小限に抑えます。これらの各導入の基盤となるインフラストラクチャ コンポーネントは、Amazon Web Services（AWS）の可用性ゾーンを構成する複数の物理データセンター間のリアルタイム レプリケーションによってサポートされています。また、Duo は、個々の導入ごとに、リアルタイムで少なくとも 1 つの追加 AWS リージョンに顧客データを複製します。

Duo は DDoS 攻撃から導入環境をどのように保護しますか。

AWS は、独自の AWS Shield DDoS 防止テクノロジーを利用して、Duo のインフラストラクチャに対する DDoS 攻撃を透過的に緩和するための対策を講じています。AWS または Duo 独自の強化されたインフラストラクチャによって自動的に緩和されない Duo サービスに対する攻撃が発生した場合、Duo の担当者に問題がすぐに通知され、必要に応じて対策が実行されます。この対策には、特定の IP アドレス/ネットブロックの体系的なブラックホール化、または影響を受けていないインフラストラクチャや IP アドレスへの顧客トラフィックの再配置などが含まれています。

サービスの停止が発生した場合、自分のアカウントを別の導入環境に移動できますか。

導入環境間で顧客を移動するために使用されるテクノロジーは、導入元と導入先の両方の環境への影響を最小限に抑えるように設計されており、バックグラウンドで実行されるため、多くの場合比較的長いプロセスになります。このプロセスは、障害シナリオの一部として実行するのには適していません。さらに、場合によっては、顧客のワークロードを代替インフラストラクチャに移動しても、根本的な問題が解決されず、サービス停止の影響が増大することさえあります。一部の停止シナリオでは、該当する顧客アカウントを異なる導入環境に移動すると、根本的な問題が発生し、サービス停止時間が長くなる可能性があります。

サービス障害の影響を受けています。別の導入環境に移行できますか。

すべての Duo 導入環境は同様に作成され、優れた稼働時間を実現するために同じ高可用性プロパティと履歴を共有します。これらの理由により、現在の導入環境から移行しても、サービ障害のリスクレベルが本質的に低下することはありません。