Snowflake パスワードによる単一要素認証ブロックに伴う FreeWay のご案内

2025/2/17

Snowflake パスワードによる単一要素認証ブロックについて

平素は弊社製品　WebQuery/Excellent/FreeWay をご利用いただきまして誠にありがとうございます。

Snowflake 社より、2025 年 11 月をもってパスワードによる単一要素認証のサインインをブロックする旨（※1）が発表されました。

また、段階的なアプローチとして、Snowflake では以下のような仕様変更があります。

フェーズ	時期	内容
1	2025 年 4 月	人間ユーザー(※2)のパスワード認証時に MFA(多要素認証)を必須とする認証ポリシーがデフォルトで有効となる。
2	2025 年 8 月	カスタム認証ポリシーの設定に関わらず、すべての人間ユーザーのパスワード認証時に MFA が必須となる。
3	2025 年 11 月	サービスユーザーのパスワードによる単一要素認証が廃止される。

※1. 参考記事
https://www.snowflake.com/ja/blog/blocking-single-factor-password-authentification/

※2. ユーザーの種類に関しては※1.参考記事を参照ください。

フェーズ 1 では、今までパスワードによる単一認証で接続できていた人間ユーザーを対象に MFA の登録が必須となります。ただし、カスタム認証ポリシーを設定済みの場合はこの限りではありません。同時に、ユーザータイプ:LEGACY_SERVICE のユーザーの Snowsight へのアクセスもブロックします。

フェーズ 2 では、フェーズ 1 で対象から外れていたカスタム認証ポリシーを設定済みの場合でも、パスワード認証する時は MFA の使用が必須となります。

フェーズ 3 では、すべてのユーザーでパスワード認証する時は MFA の使用が必須となり、ユーザータイプ:LEGACY_SERVICE のユーザーはユーザータイプ:SERVICE へと完全移行されます。

シングルサインオンやキーペア認証を使用している場合は、これらが適応されません。

以上は Snowflake 社による 2024 年 12 月時点のアナウンス内容です。
内容は変更される可能性があります。

FreeWay での影響

FreeWay では、ODBC ドライバーを使用して Snowflake へ接続をしています。
その際の認証方式はパスワード認証を採用していました。
そのため、今回のパスワードによる単一要素認証ブロックの対象となり、
FreeWay から Snowflake への接続するお客様には以下のような影響があります。

(1) カスタム認証ポリシーを未設定でパスワード認証を使用している場合

2025 年 4 月より FreeWay から人間ユーザーのみ Snowflake への接続ができなくなる。

(2) カスタム認証ポリシーを設定済みでパスワード認証を使用している場合

2025 年 8 月より FreeWay から人間ユーザーのみ Snowflake への接続ができなくなる。

(3) ユーザータイプ:LEGACY_SERVICE のユーザーでパスワード認証を使用している場合

2025 年 11 月より FreeWay から Snowflake への接続ができなくなる。

FreeWay の方針と設定方法

Snowflake へ認証方式としては、以下 4 つがあります。

・SAML 認証
・パスワード認証（多要素認証）
・外部 OAuth 認証
・キーペア認証

このうち、FreeWay では Snowflake へ接続する際の認証方式として、
キーペア認証をサポート/ご案内いたします。

パスワード認証かつ多要素認証の設定は可能ですが、WebQuery/Excellent から Snowflake に接続するごとに別端末での認証が必要になり、操作パフォーマンスが落ちてしまいます。

また、キーペア認証のサポートにより、
ユーザータイプ:SERVICE のユーザーでの接続も可能になります。

キーペア認証の設定は従来の FreeWay のセットアップ手順と異なるため、
設定手順を以下に示します。

1. 秘密キー、公開キーを生成する

例では openssl を使用して秘密キー、公開キーを生成する。

秘密キーの生成コマンド）

```
openssl genrsa 2048 | openssl pkcs8 -topk8 -inform PEM -out rsa_key.p8 -nocrypt
```

公開キーの生成コマンド）

```
openssl rsa -in rsa_key.p8 -pubout -out rsa_key.pub
```

※ファイル名 rsa_key.p8,rsa_key.pub は任意のファイル名

※秘密キーは暗号化して生成することも可能。暗号化する場合は
-nocrypt オプションを省略し、パスコードの指定をする。

※生成した秘密キーファイルは
FreeWay 導入サーバーの任意のパスに配置すること。

2. Snowflake のユーザーに公開キーを割り当てる

Snowflake へ管理権限ユーザーでログインし以下の SQL を実行する。

SQL）ALTER USER <ユーザー名> SET RSA_PUBLIC_KEY = '<公開キー>' ;

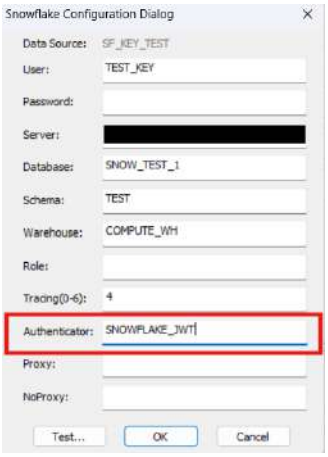
※手順 1.で作成された公開キーファイルを開き、
記載から改行コードを削除したものが公開キーとなる。

※DESCRIBE USER コマンドでユーザーの公開キー割り当てを確認できる。

3. FreeWay 導入サーバーの ODBC データソースにキーペア認証の設定をする

[FreeWay 導入サーバーが Windows の場合]

・ODBC データソース アドミニストレーターで
データソースを作成または編集する際に
Authenticator : SNOWFLAKE_JWT にする。



・レジストリエディタより
¥HKEY_LOCAL_MACHINE¥SOFTWARE¥ODBC¥ODBC.INI¥<対象のデータソース名>以下に
PRIV_KEY_FILE キーを追加し、値に <秘密キーファイル配置フォルダ>/rsa_key.p8
を入力する。

※秘密キーを暗号化している場合、PRIV_KEY_FILE_PWD キーを追加し、
値に秘密キーファイルをデコードするパスコードを入力する。

[FreeWay 導入サーバーが Linux の場合]

・odbc.ini ファイルの対象のデータソースに以下の設定を追加する。
AUTHENTICATOR = SNOWFLAKE_JWT
PRIV_KEY_FILE = <秘密キーファイル配置フォルダ>/rsa_key.p8

※秘密キーを暗号化している場合、以下も追加する。
PRIV_KEY_FILE_PWD = <秘密キーファイルをデコードするパスコード>

4. FreeWay のロケーション（接続先 DB）設定をする

対象のロケーション（接続先 DB）設定にて、通常通りの設定をする。
ただし、DB ユーザーのパスワード欄は入力しても無視される。

以上が FreeWay から Snowflake へ接続するための設定手順になります。

参考サイト

https://docs.snowflake.com/ja/user-guide/key-pair-auth#generate-the-private-key

https://docs.snowflake.com/ja/developer-guide/odbc/odbc-parameters#label-odbc-key-pair-authentication

また、**DB の接続解除機能**をご利用のお客様に関しては以下の設定も必要となります。

ロケーション（接続先 DB）の設定、FreeWay セットアップのデータベース接続解除
もしくはセッションモニターから接続解除する時の DB ユーザーについて
以下のいずれかの条件を満たしていること。

・ACCOUNTADMIN ロールかつ
　ODBC データソースに紐づけた秘密キーに対応した公開キーが紐づけられている

・ロケーションに記載した DB ユーザーと同じ

以上