スーパーコンピュータ SQUID における多要素認証の運用

寺前 勇希 [1)], 木越 信一郎 [1)], 伊達 進 [2)]

1) 大阪大学 情報推進部 情報基盤課 研究系システム班
2) 大阪大学 サイバーメディアセンター 応用情報システム研究部門

teramae-y@cmc.osaka-u.ac.jp

Operation of Multi-Factor Authentication on SQUID

Yuki Teramae[1)], Shinichiro Kigoshi[1)], Susumu Date[2)]

1) Department of Information and Communications Technology Services, Osaka University
2) Applied Information Systems Research Division, Cybermedia Center, Osaka University

概要

大阪大学サイバーメディアセンターでは 2021 年 5 月よりスーパーコンピュータシステム SQUID を運用している。本システムは多要素認証を導入しており、従来のパスワード認証に加えて TOTP による認証を実施している。本稿では、本システムで導入した多要素認証の仕組みを紹介するとともに、導入後 2 年間の運用状況と今後の課題を記す。

1. はじめに

大阪大学サイバーメディアセンター（以下、本センター）では、2021 年 5 月よりスーパーコンピュータシステム SQUID（Supercomputer for Quest to Unsolved Interdisciplinary Datascience）の運用を開始した。SQUID は、汎用 CPU ノード群、GPU ノード群、ベクトルノード群、大容量ストレージから構成され、総理論演算性能 16.591 PFLOPS を有するスーパーコンピュータである[1]。

本センターをはじめ、全国共同利用施設のスーパーコンピュータを利用する場合は、外部からインターネットを通じて Secure Shell による接続 (以下、SSH 接続) を行うことが一般的である。SSH 接続の認証方式としては、公開鍵認証およびパスワード認証のいずれかを用いるケースが多く、当センターでは以前よりパスワード認証を採用している。これは公開鍵認証において、パスフレーズを設定しない利用者が一定数存在することに伴うセキュリティリスクを案じてのことである。しかしながらサイバー攻撃の巧妙化に伴い、強固なパスワードを使った認証においてもセキュリティは十分であるとは言い難い。スーパーコンピュータシステムに対する大規模な不正アクセスの事案も記憶に新しく[2]、本センターが全国の研究者に SQUID システムを提供する役割から、セキュリティの確保は不可欠である。そこで、SQUID においては、SSH 接続の認証方式として新たに多要素認証 (MFA: Multi-Factor Authentication) を導入し、セキュリティを強化することとした。

2. 多要素認証の導入検討

2-1. 多要素認証の方式について

本センターのように他機関の利用者に対して提供するスーパーコンピュータシステムにおいては、SSH 接続の認証にパスワードあるいは公開鍵を用いることが多い。SQUID ではシステム上の制約や構築期間等を鑑み、多要素認証として通常のパスワード認証に加えて、時間ベースワンタイムパスワード (以下、TOTP: Time-Based One-Time Password)による認証を行うこととした。

TOTP 認証は、RFC 6238 に準拠した、時刻に基づくワンタイムパスワードでの認証を提供するアルゴリズムである。基本的な動作は以下のとおりである。

A1. サーバとクライアントの間で、秘密鍵が生成され、共有される。
A2. サーバとクライアントで、同じタイムスタンプを取得する。
A3. 秘密鍵とタイムスタンプを組み合わせ、

ハッシュ関数で署名を行う。

A4. ハッシュ値から特定の桁数の数値を抽出し、ワンタイムパスワードとして出力する。

A5. クライアントから提供されたワンタイムパスワードとサーバで生成されたワンタイムパスワードが一致するか確認する。

2-2. 他機関が運用するシステムへの導入状況

スーパーコンピュータシステムを運用している他大学・他機関にて、多要素認証の導入状況を調査した。2023 年 6 月に発表された TOP500 [3] において、”Academic”カテゴリとして登録されている機関が運用するシステムのうち、インターネット上で接続方法が公開されていた上位 50 件を対象に、システムへの認証方法を集計したところ、表 1 のとおりとなった。

表 1：多要素認証の導入状況

多要素認証を導入していない	多要素認証を導入している	パスワード/公開鍵と組み合わせる認証方式			
		TOTP	Push	SMS	その他
32	18	10	8	8	3

多要素認証を導入しているシステムのうち半数以上は、TOTP による認証を取り入れている。次いで、利用者の端末に直接認証要求を行う Push 認証や利用者のスマートフォンに対して SMS や電話でワンタイムコードを送付する SMS 認証を取り入れたシステムが多い結果となった。Push 認証や SMS 認証は、セキュリティプラットフォームである Duo Security [4] を使ったシステムが大半を占めていた。また、SSH 接続自体に多要素認証を導入していないシステムであっても、アカウントのパスワードをリセットする際に多要素認証を使用しているものもあった。なお、調査対象のシステムの中には本センターのような共同利用に相当しないものもあり、多要素認証は導入していないものの、VPN 経由でのアクセスを必須にすることで、セキュリティを担保するシステムも見られた。

3. SQUID 多要素認証の概要

本節では、SQUID 利用者の視点で、多要素認証の具体的な挙動について紹介する。

3-1. 事前準備

TOTP 認証を使用するにあたり、利用者はあらかじめ、スマートフォンやタブレット等自身の端末を用意し、秘密鍵を保管するための Authenticator アプリをインストールする必要がある。一般に、Google Authenticator、Microsoft Authenticator といったアプリケーションが用いられる。

3-2. 初回ログイン

利用者が SQUID に対して任意のターミナルソフトで SSH 接続すると、パスワード認証の後で、画面に秘密鍵の QR コードおよび文字列が出力される (図 1) 。このいずれかを Authenticator アプリで読み取ることで、SQUID と利用者の端末間で、TOTP 認証用の秘密鍵が共有される。前述のとおり TOTP 認証ではこの秘密鍵を元に、現在の時刻を基準としたワンタイムパスワードを生成する。このパスワードは 30 秒ごとに変化し、再生成される仕組みである。なお、認証モジュールの仕組み上、再認証は発生せず、初回ログインではパスワードのみの認証となる。そのため、秘密鍵を生成した後、ターミナルを終了する仕組みとし、この段階では SQUID を利用することはできない。

図 1: 初回ログイン時 QR コード表示画面

3-3. 二回目以降のログイン

利用者が再度 SQUID に対して SSH 接続すると、自身がアカウントに設定したパスワードに加えて、ワンタイムパスワードの入力を促すメッセージが表示される。初回ログイン時に登録した、Authenticator アプリに表示される TOTP 認証用のワンタイムパスワードを入力することで、SQUID

へのログインおよび利用が可能となる。

4. 多要素認証の運用について

4-1. 運用開始前の準備について

認証方式の変更から、運用初期においては利用者の混乱が予想された。そのため、ログイン手順については特に詳細なドキュメントを作成することを意識し、以下のようなことを心がけた。作成したドキュメント [5] の一部を図 2 に示す。

- 画面キャプチャを多用すること。
- iPhone、Android それぞれで Authenticator アプリをインストールする段階から順を追って解説すること。
- 初回ログインのみの手順か、次回ログイン以降も必要な手順かを明記すること。
- 日本語と英語両方で出来る限り同じレベルの解説を行うこと。

また、初心者を対象とした講習会においては、ビデオを ON にして、講師のスマートフォンの画面を写し出し実際に QR コードを読み込んでワンタイムコードを取得することを実演する等、時間を十分にかけて、利用者の目線で説明することを重視した。

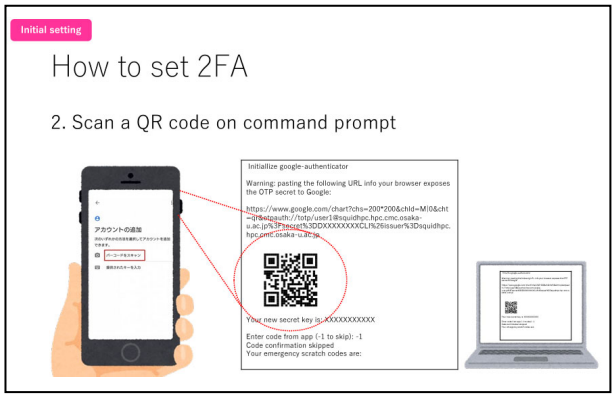

図 2:ログイン手順のドキュメント

4-2. 運用開始後の反響・問い合わせについて

運用当初は、多要素認証に慣れない利用者からいくつかの質問があったものの、大きな混乱は見られず、現在に至っている。運用開始月である 2021 年 5 月から 2022 年度末までの多要素認証に関わる問い合わせの件数を図 3 および図 4 に示す。

運用初期から現在にかけて、問い合わせの 90%以上は秘密鍵の登録 (QR コードの読み取り) を行わずに、うっかり画面を閉じてしまったケースや、秘密鍵を登録したスマートフォンの故障・機種変更等により秘密鍵の再登録が必要となるケースである。この場合は、システム管理者にて TOTP 認証の秘密鍵を削除することで設定をリセットし、対応している。

また運用初期は、画面サイズの都合で QR コードが崩れて表示される、という問い合わせも時折見られた。QR コードが崩れて表示される場合は、ターミナルの画面サイズを変更するか、あるいは QR コードとともに出力される秘密鍵の文字列を直接入力することで、Authenticator アプリに秘密鍵を登録可能である。この問題については、ドキュメントを整備する他、講習会などでも話題にふれることで、問い合わせの件数は減少傾向にあり、最近はあまり見られない。

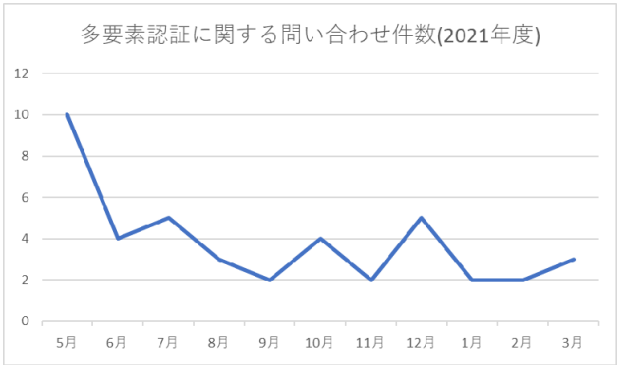

図 3: 多要素認証に関する問い合わせ件数 (2021 年度)

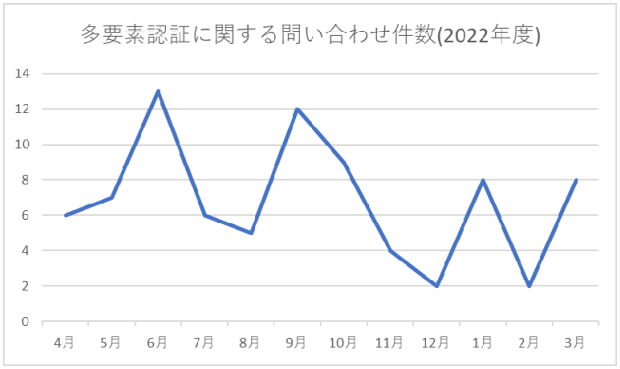

図 4:多要素認証に関する問い合わせ件数 (2022 年度)

4-3. TOTP 認証のリセットについて

TOTP 認証をリセットし秘密鍵を再登録する場合は、SQUID 上の既定のディレクトリに置かれた秘密鍵を削除する必要がある。この作業は、システム管理者が手作業で実施しており、次のようなフローで実施している。

B1. 利用者からシステム管理者宛にメールや WEB フォームを通して TOTP 認証をリセットすることの依頼がある。

B2. 身元確認として、依頼に書かれたメールアドレスとアカウントが、SQUID に登録されている利用者情報と合致していることを確認し、秘密鍵を削除する。
B3. アカウントに設定されているパスワードをリセットする。
B4. TOTP 認証 秘密鍵の再登録と、パスワードの再設定を利用者に依頼する。

アカウントを窃取した第三者による TOTP 認証リセットを防ぐため、アカウント所有者の身元確認として”B2”においてメールアドレスを確認することとしている。

4-4. その他の問題点について

発生件数は少ないが、利用者の操作により SQUID 上に秘密鍵が正常に生成されないケースがある。具体的には以下が該当する。

- 初回ログインの途中で、画面を削除するなどの操作を行い、ターミナルを強制終了した場合
- 秘密鍵を保管するディレクトリのあるファイルシステムにおいて、利用者の Quota が超過している状態で手続きをした場合

SQUID では、秘密鍵を登録するための QR コードを表示した後に、既定のディレクトリ配下に秘密鍵が生成される、といった処理順になっており、上記のケースでは利用者の Authenticator アプリには秘密鍵が登録された状態になっているものの、SQUID 側では秘密鍵が存在しない状態となってしまう。こうしたケースでは、WEB ミーティングで利用者の画面を見ながら問題を確認することで解決できたものの、時間を要した。

5. 今後の課題

5-1. 多要素認証に対応できないケース

一般的な利用の範疇では問題ないのだが、多要素認証に対応できないケースはまれに見受けられる。例えば、利用者のローカル PC 上に立ち上げた解析用アプリケーション (※一般的なターミナルソフトではなく、解析から可視化までを行うアプリケーションを指す) から、直接スーパーコンピュータに接続してジョブ投入を行うケースがある。このようなアプリケーションの多くはパスワード認証や公開鍵認証には対応しているものの、TOTP 認証に対応できていないことがあり、SQUID に対して利用できない。こうしたアプリケーションを利用している方から相談を受けた際は、研究の進捗へ影響や緊急性を考慮・審査し、問題ないと判断される場合は、誓約書を提出してもらうことで、期間限定の例外として多要素認証を限定的に解除する。ただし、誓約書には以下の内容を盛り込み、あくまで特例的な措置であることが明示的に示される。

- 多要素認証を除外することでセキュリティは、利用者自身で責任を持つこと。
- パスワードを強力なものにすること。他人と共有しないこと。
- 本センターの判断で多要素認証を再設定する可能性があること。

現状、あくまで例外として 1 グループでのみ、そのような対応を実施しているが、今後同様の相談が寄せられ、対応件数が増えた場合に根本的な解決策を検討する必要がある。

この他、講習会用に配布する無料のアカウントについては、同様に多要素認証の設定を解除している。アカウントの有効期間が 1 週間と限定的であること、認証に手間取ることで講習会の進行に影響する可能性があることを鑑み、このような運用としている。

5-2. TOTP 認証のリセット時の身元確認の厳密性

TOTP 認証をリセットする際は、リセットを依頼した者の身元確認が必要不可欠である。前述のとおり、本センターではメールアドレスのみで身元確認を行っている。一方、本センターと同様に TOTP 認証を取り入れたスーパーコンピュータシステムを運用するケンブリッジ大学においては、TOTP 認証のリセットを実施する際に、ビデオ通話を実施した上で公文書や教職員証の提示を求め、身元確認を実施しており、本センターと比べより厳密な運用を行っている [6] 。本センターでも同様の運用をとることは可能かもしれないが、サービスの利便性や迅速性、リセットに対応する人員数を鑑みると、現在よりも厳密な運用にすることは容易ではなく、今後もより良い方法を検討していく必要がある。

5-3. TOTP 認証用の秘密鍵の統一

ここまで、SQUID にログインする場合の多要

素認証について記述したが、SQUID の関連システムとして提供している利用状況を閲覧できる WEB ポータルや、SQUID 利用者が利用できるデータ集約基盤 ONION (Osaka university Next-generation Infrastructure for Open research and open InnovatioN) [7] の ONION-file (NextCloud) でも多要素認証を実施しており、同様の TOTP 認証を提供している。現状、サービスごとにそれぞれ TOTP 認証用の秘密鍵が存在している状態となっており、利用者は Authenticator アプリ上で、複数の秘密鍵を管理する必要があり、煩雑になる。これを共通化することで、より利便性が高まると考えられる。

また、これは Authenticator アプリ側への改善要望であるが、アプリ内において TOTP 認証用の秘密鍵(ワンタイムパスワード)をフォルダ管理・グループ管理できるようになれば、より使いやすくなると感じている。

6. おわりに

本稿では、SQUID への多要素認証の導入とその運用状況について詳細に記した。多要素認証は、セキュリティ強化のために一定の効果がある一方で、利用者にとってはメリットが見えづらく、むしろログインの度に端末を取り出す手間が増えていることで、不便に感じる方も多いと思われる。セキュリティ強化と利便性の間でどのようなバランスを取るべきか、今後も検討を続けていく必要がある。本稿が、他機関のスーパーコンピュータシステムにおける多要素認証の導入と運用の参考になると幸いである。

謝辞

本研究成果は、本センターのスーパーコンピュータ SQUID を利用して得られたものである。スーパーコンピュータ SQUID における多要素認証の構築・運用にあたり、日本電気株式会社の皆様には多大なる尽力を頂いた。ここに記して謝意を示す。

参考文献

[1] Susumu Date, Yoshiyuki Kido, Yuki Katsuura, Yuki Teramae & Shinichiro Kigoshi, “Supercomputer for Quest to Unsolved Interdisciplinary Datascience (SQUID) and its Five Challenges”, WSSP 2021: Sustained Simulation Performance 2021, pp 1-19, https://doi.org/10.1007/978-3-031-18046-0_1

[2] EGI CSIRT (2020), “Attacks on multiple HPC sites”, https://csirt.egi.eu/attacks-on-multiple-hpc-sites/

[3] TOP500, “June 2023”, https://www.top500.org/lists/top500/2023/06/

[4] Duo Security, https://duo.com/ja-jp

[5] 大阪大学サイバーメディアセンター 大規模計算機システム (2021), “Getting started guide for logging in SQUID”, http://www.hpc.cmc.osaka-u.ac.jp/wp-content/uploads/2021/07/how_to_login_SQUID_en.pdf

[6] University of Cambridge, “How do I reset my TOTP for SSH to CSD3?”, https://docs.hpc.cam.ac.uk/hpc/user-guide/mfa.html#how-do-i-reset-my-totp-for-ssh-to-csd3

[7] 伊達 進, 寺前 勇希, 勝浦 裕貴, 木越 信一郎, 木戸 善之, “ONION：大阪大学のデータ集約基盤”, 学術情報処理研究, 2022, 26 巻, 1 号, p.87-96 , https://doi.org/10.24669/jacn.26.1_87