SSH トンネリングとプロキシ

```
% GIT_TRACE=1 GIT_CURL_VERBOSE=1 git push
21:32:14.216308 exec-cmd.c:139          trace: デバッグ出力: /Applications/Xcode.app/Contents/Developer/usr/b
21:32:14.216594 exec-cmd.c:238          trace: 実行可能なディレクトリを解決しました: /Applications/Xcode.app
21:32:14.216949 git.c:460               trace: ビルドイン: git push
21:32:14.218655 run-command.c:655       trace: コマンド実行: unset GIT_PREFIX; ssh git@github.com 'git-receiv
```

すべて最新です

GIT_PUSH 操作が遅く、特に `ssh git@github.com` フェーズで遅延が発生しました。この問題を解決するために、SSH

SSH トンネルに `corkscrew` を使用するには、まずインストールする必要があります。macOS では、Homebrew を使用

`~/.ssh/config`:

```bash
Host *
    UseKeychain yes
    AddKeysToAgent yes
    IdentityFile ~/.ssh/id_rsa
    ProxyCommand corkscrew localhost 7890 %h %p
```

ログ:

“‘bash % ssh root@138.201.174.0 -vvv ⛒ **プロキシ設定を検出しました:** - HTTP_PROXY: http://127.0.0.1:7890 - HTTPS_PROXY: http://127.0.0.1:7890

OpenSSH_9.8p1, LibreSSL 3.3.6 debug1: 読み取り構成データ /Users/lzwjava/.ssh/config debug1: /Users/lzwjava/.ssh/config 行 1: * に対するオプションを適用中 debug1: 読み取り構成データ /etc/ssh/ssh_config debug1: /etc/ssh/ssh_config 行 21: /etc/ssh/ssh_config.d/* にマッチするファイルはありません debug1: /etc/ssh/ssh_config 行 54: * に対するオプションを適用中 debug2: resolve_canonicalize: 138.201.174.0 はアドレスです debug3: 拡張ユーザー識別ファイル ‘~/.ssh/known_hosts’-> ‘/Users/lzwjava/.ssh/known_hosts’debug3: 拡張ユーザー識別ファイル ‘~/.ssh/known_hosts2’-> ‘/Users/lzwjava/.ssh/known_hosts2’debug1: 認証プロバイダーの $SSH_SK_PROVIDER は解決しなかったため、無効にします debug3: channel_clear_timeouts: クリア中 debug1: プロキシコマンドの実行: exec corkscrew localhost 7890 138.201.174.0 22 debug1: 秘密鍵ファイル /Users/lzwjava/.ssh/id_rsa タイプ 0 debug1: 秘密鍵ファイル /Users/lzwjava/.ssh/id_rsa-cert タイプ -1 debug1: ローカルバージョン文字列 SSH-2.0-OpenSSH_9.8 debug1: リモートプロトコルバージョン 2.0、リモートソフトウェアバージョン OpenSSH_9.6p1 Ubuntu-3ubuntu13.5 debug1: compat_banner: マッチ OpenSSH_9.6p1 Ubuntu-3ubuntu13.5 pat OpenSSH* compat 0x04000000 debug2: fd 5 の設定 O_NONBLOCK debug2: fd 4 の設定 O_NONBLOCK debug1: 138.201.174.0:22 に‘root’として認証中 debug3: record_hostkey: ファイル /Users/lzwjava/.ssh/known_hosts:164 に ED25519 キータイプを見つけました debug3: record_hostkey: ファイル /Users/lzwjava/.ssh/known_hosts:165 に RSA キータイプを見つけました debug3: record_hostkey: フ

ァイル /Users/lzwjava/.ssh/known_hosts:166 に ECDSA キータイプを見つけました debug3: load_hostkeys_file: 138.201.174.0 から 3 つのキーを読み込みました debug1: fopen /Users/lzwjava/.ssh/known_hosts2: そのようなファイルやディレクトリはありません debug1: fopen /etc/ssh/ssh_known_hosts: そのようなファイルやディレクトリはありません debug1: fopen /etc/ssh/ssh_known_hosts2: そのようなファイルやディレクトリはありません debug3: order_hostkeyalgs: ssh-ed25519-cert-v01@openssh.com マッチング最適な優先順序キータイプがあるため、HostkeyAlgorithms をそのまま使用 debug3: パケット送信: タイプ 20 debug1: SSH2_MSG_KEXINIT を送信 debug3: パケット受信: タイプ 20 debug1: SSH2_MSG_KEXINIT を受信 debug2: ローカルクライアント KEXINIT 提案 debug2: KEX アルゴリズム: sntrup761x25519-sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,ext-info-c,kex-strict-c-v00@openssh.com debug2: ホストキーアルゴリズム: ssh-ed25519-cert-v01@openssh.com,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,sk-ssh-ed25519-cert-v01@openssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com,rsa-sha2-512-cert-v01@openssh.com,rsa-sha2-256-cert-v01@openssh.com,ssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,sk-ssh-ed25519@openssh.com,sk-ecdsa-sha2-nistp256@openssh.com,rsa-sha2-512,rsa-sha2-256 debug2: Ciphers ctos: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com debug2: Ciphers stoc: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com debug2: MACs ctos: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1 debug2: MACs stoc: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1 debug2: 圧縮 ctos: none,zlib@openssh.com,zlib debug2: 圧縮 stoc: none,zlib@openssh.com,zlib debug2: 言語 ctos: debug2: 言語 stoc: debug2: first_kex_follows 0 debug2: 予約 0 debug2: 対向サーバーの KEXINIT 提案 debug2: KEX アルゴリズム: sntrup761x25519-sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,ext-info-s,kex-strict-s-v00@openssh.com debug2: ホストキーアルゴリズム: rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519 debug2: Ciphers ctos: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com debug2: Ciphers stoc: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com debug2: MACs ctos: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1 debug2: MACs stoc: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1 debug2: 圧縮 ctos: none,zlib@openssh.com debug2: 圧縮 stoc: none,zlib@openssh.com debug2: 言語 ctos: debug2: 言語 stoc: debug2: first_kex_follows 0 debug2: 予約 0 debug3: kex_choose_conf: 厳格な KEX 順序を使用 debug1: kex: アルゴリズム: sntrup761x25519-sha512@openssh.com debug1: kex: ホストキーアルゴリズム: ssh-ed25519 debug1: kex: サーバー -> クライアント暗号: chacha20-poly1305@openssh.com MAC: 隠蔽されています 圧縮: なし debug1:

kex: クライアント -> サーバー暗号: chacha20-poly1305@openssh.com MAC: 隠蔽されています 圧縮: なし debug3: パケット送信: タイプ 30 debug1: SSH2_MSG_KEX_ECDH_REPLY を期待 debug3: パケット受信: タイプ 31 debug1: SSH2_MSG_KEX_ECDH_REPLY を受信 debug1: サーバーホストキー: ssh-ed25519 SHA256:+5SaMkJXG9yZrsYjXgxFfRZpvb6qjc/arFG2Nk4Vv48 debug3: record_hostkey: ファイル /Users/lzwjava/.ssh/known_hosts:164 に ED25519 キータイプを見つけました debug3: record_hostkey: ファイル /Users/lzwjava/.ssh/known_hosts:165 に RSA キータイプを見つけました debug3: record_hostkey: ファイル /Users/lzwjava/.ssh/known_hosts:166 に ECDSA キータイプを見つけました debug3: load_hostkeys_file: 138.201.174.0 から 3 つのキーを読み込みました debug1: fopen /Users/lzwjava/.ssh/known_hosts2: そのようなファイルやディレクトリはありません debug1: fopen /etc/ssh/ssh_known_hosts: そのようなファイルやディレクトリはありません debug1: fopen /etc/ssh/ssh_known_hosts2: そのようなファイルやディレクトリはありません debug1: ホスト'138.201.174.0'は ED25519 ホストキーと一致します。debug1: ファイル /Users/lzwjava/.ssh/known_hosts:164 にキーを見つけました debug3: パケット送信: タイプ 21 debug1: ssh_packet_send2_wrapped: 再設定送信シークエンス番号 3 debug2: ssh_set_newkeys: モード 1 debug1: 134217728 ブロック後に再暗号化 debug1: SSH2_MSG_NEWKEYS を送信 debug1: SSH2_MSG_EXT_INFO を送信 debug3: パケット送信: タイプ 7 debug1: SSH2_MSG_NEWKEYS を期待 debug3: パケット受信: タイプ 21 debug1: ssh_packet_read_poll2: 再設定読み取りシークエンス番号 3 debug1: SSH2_MSG_NEWKEYS を受信 debug2: ssh_set_newkeys: モード 0 debug1: 134217728 ブロック後に再暗号化 debug2: KEX アルゴリズム: sntrup761x25519-sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,ext-info-c,kex-strict-c-v00@openssh.com debug2: ホストキーアルゴリズム: ssh-ed25519-cert-v01@openssh.com,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,sk-ssh-ed25519-cert-v01@openssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com,rsa-sha2-512-cert-v01@openssh.com,rsa-sha2-256-cert-v01@openssh.com,ssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,sk-ssh-ed25519@openssh.com,sk-ecdsa-sha2-nistp256@openssh.com,rsa-sha2-512,rsa-sha2-256 debug2: Ciphers ctos: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com debug2: Ciphers stoc: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com debug2: MACs ctos: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1 debug2: MACs stoc: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1 debug2: 圧縮 ctos: none,zlib@openssh.com,zlib debug2: 圧縮 stoc: none,zlib@openssh.com,zlib debug2: 言語 ctos: debug2: 言語 stoc: debug2: first_kex_follows 0 debug2: 予約 0 debug3: パケット送信: タイプ 5 debug3: パケット受信: タイプ 7 debug1: SSH2_MSG_EXT_INFO を受信 debug3: kex_input_ext_info: 拡張子 server-sig-algs debug1: kex_ext_info_client_parse: server-sig-algs=<ssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,sk-ssh-ed25519@openssh.com,sk-ecdsa-sha2-nistp256@openssh.com,rsa-sha2-512,rsa-sha2-256> debug3: kex_input_ext_info: 拡張子 publickey-hostbound@openssh.com debug1: kex_ext_info_check_ver: publickey-hostbound@openssh.com=<0> debug3: kex_input_ext_info: 拡張子 ping@openssh.com debug1: kex_ext_info_check_ver: ping@openssh.com=<0> de-

bug3: パケット受信: タイプ 6 debug2: service_accept: ssh-userauth debug1: SSH2_MSG_SERVICE_ACCEPT を受信 debug3: パケット送信: タイプ 50 debug3: パケット受信: タイプ 7 debug1: SSH2_MSG_EXT_INFO を受信 debug3: kex_input_ext_info: 拡張子 server-sig-algs debug1: kex_ext_info_client_parse: server-sig-algs=<ssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,sk-ssh-ed25519@openssh.com,sk-ecdsa-sha2-nistp256@openssh.com,rsa-sha2-512,rsa-sha2-256> debug3: パケット受信: タイプ 51 debug1: 認証を継続できるもの: publickey,password debug3: 異なるリスト publickey,password で再開 debug3: 好まれる順序: publickey,keyboard-interactive,password debug3: authmethod_lookup publickey debug3: 残りの好まれる順序: keyboard-interactive,password debug3: authmethod_is_enabled publickey debug1: 次の認証方法: publickey debug3: ssh_get_authentication_socket_path: パス '/private/tmp/com.apple.launchd.cTjjogIh4V/Listeners' debug1: get_agent_identities: エージェントをホストキーにバインド debug1: get_agent_identities: エージェントから 3 つのキーを返しました debug1: /Users/lzwjava/.ssh/id_rsa RSA SHA256:bF6g9+hPW6crim36xewb/0Pvl/Y34 明示的なエージェントを試行 debug1: lzwjava@Zhiweis-MacBook-Air.local RSA SHA256:ibpUGVDyOYKOQArPUs5ZSnp0oECaZJWSF エージェントを試行 debug1: /Users/lzwjava/Downloads/LightsailDefaultKey-ap-northeast-1.pem RSA SHA256:AQCwUpsEP8cawJtCQNidQq0poQgAgkUuFYQMjxw8evI エージェントを試行 debug2: pubkey_prepare: 完了 debug1: 提示公共鍵: /Users/lzwjava/.ssh/id_rsa RSA SHA256:bF6g9+hPW6crim36xewb/0Pvl/Y34 明示的なエージェント debug3: パケット送信: タイプ 50 debug2: 公開鍵パケットを送信し、応答を待機 debug3: パケット受信: タイプ 60 debug1: サーバーがキーを受け入れました: /Users/lzwjava/.ssh/id_rsa RSA SHA256:bF6g9+hPW6crim36xewb/0Pvl/Y34 明示的なエージェント debug3: sign_and_send_pubkey: publickey-hostbound-v00@openssh.com を使用して RSA SHA256:bF6g9+hPW6crim36xewb/0Pvl/Y34 を署名 debug3: sign_and_send_pubkey: rsa-sha2-512 SHA256:bF6g9+hPW6crim36xewb/0Pvl/Y34 を使用して署名 debug3: パケット送信: タイプ 50 debug3: パケット受信: タイプ 52 認証に成功しました 138.201.174.0 (プロキシを介して) を使用して"publickey"。debug1: チャネル 0: 新しいセッション [client-session] (非アクティブタイムアウト: 0) debug3: ssh_session2_open: チャネル新規: 0 debug2: チャネル 0: send open debug3: パケット送信: タイプ 90 debug1: no-more-sessions@openssh.com をリクエスト debug3: パケット送信: タイプ 80 debug1: 対話型セッションに入