SSHプロトコル

2001. 10. 25

鬼塚　優

SSHとは

- ssh (Secure Shell) はネットワークを介してコンピュータにログインするプログラムで、遠隔地のマシンでコマンドを実行したり他のマシンへファイルを移したりするために使われる。
- ssh は強力な認証と安全ではない経路を通じての安全な通信を提供する。
- ssh は rlogin(リモートログイン), rsh(リモートシェル), そして rcp(リモートファイルコピー) の代わるものとして意図されている。

SSHを使用する理由

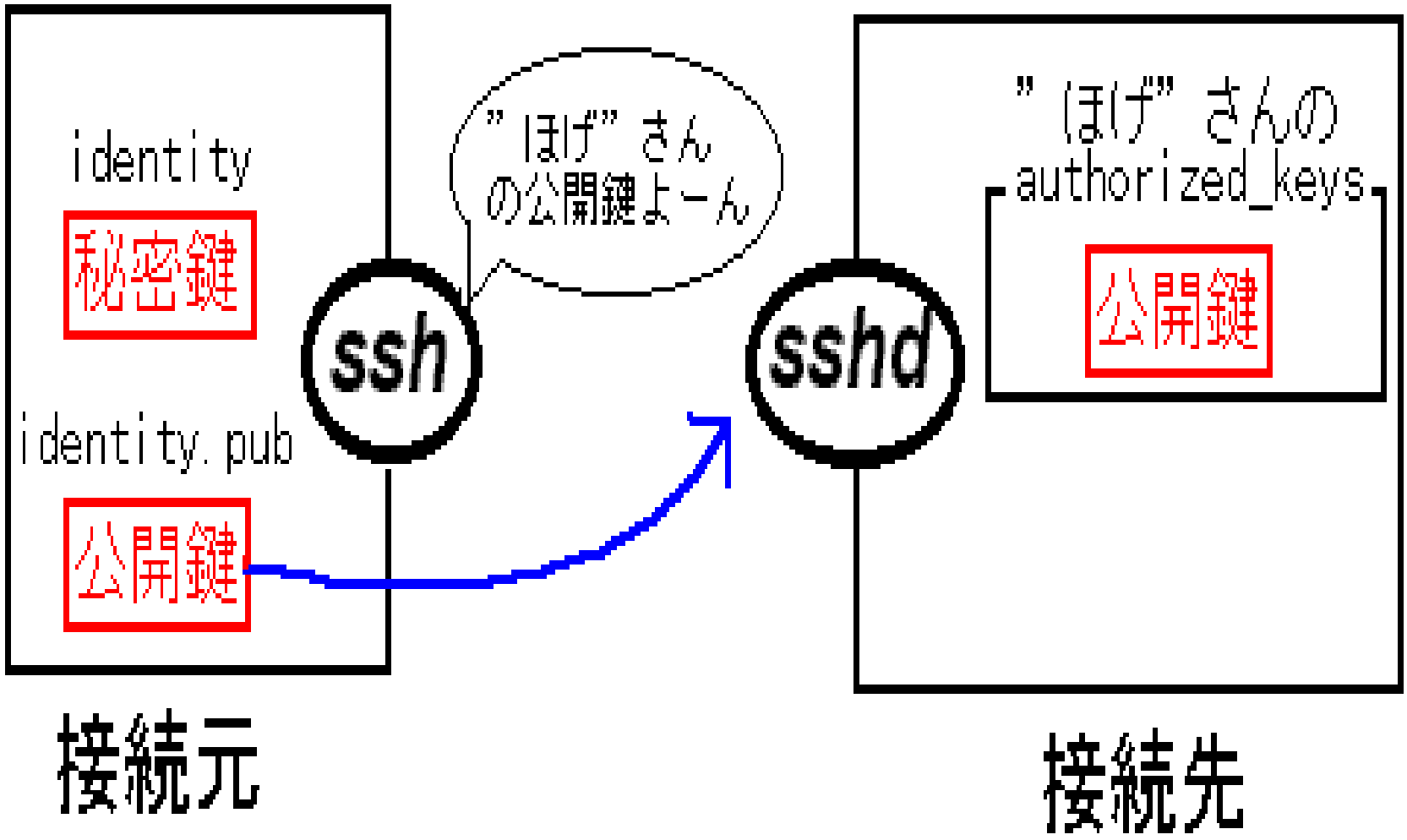
- 昔からあるBSDの「‘r’ - コマンド」(rsh, rlogin, rcp)は何種類もの異なる攻撃に対して無防備で、ネットワークを介してマシンに root でアクセスすることは、システムへの多数の方法での無権限アクセスを招くおそれがある。
- X Window System もまた幾つかの深刻な脆弱さを抱えているが、ssh によって、安全な遠隔地からのX接続をユーザーには透明なままで実現できる。

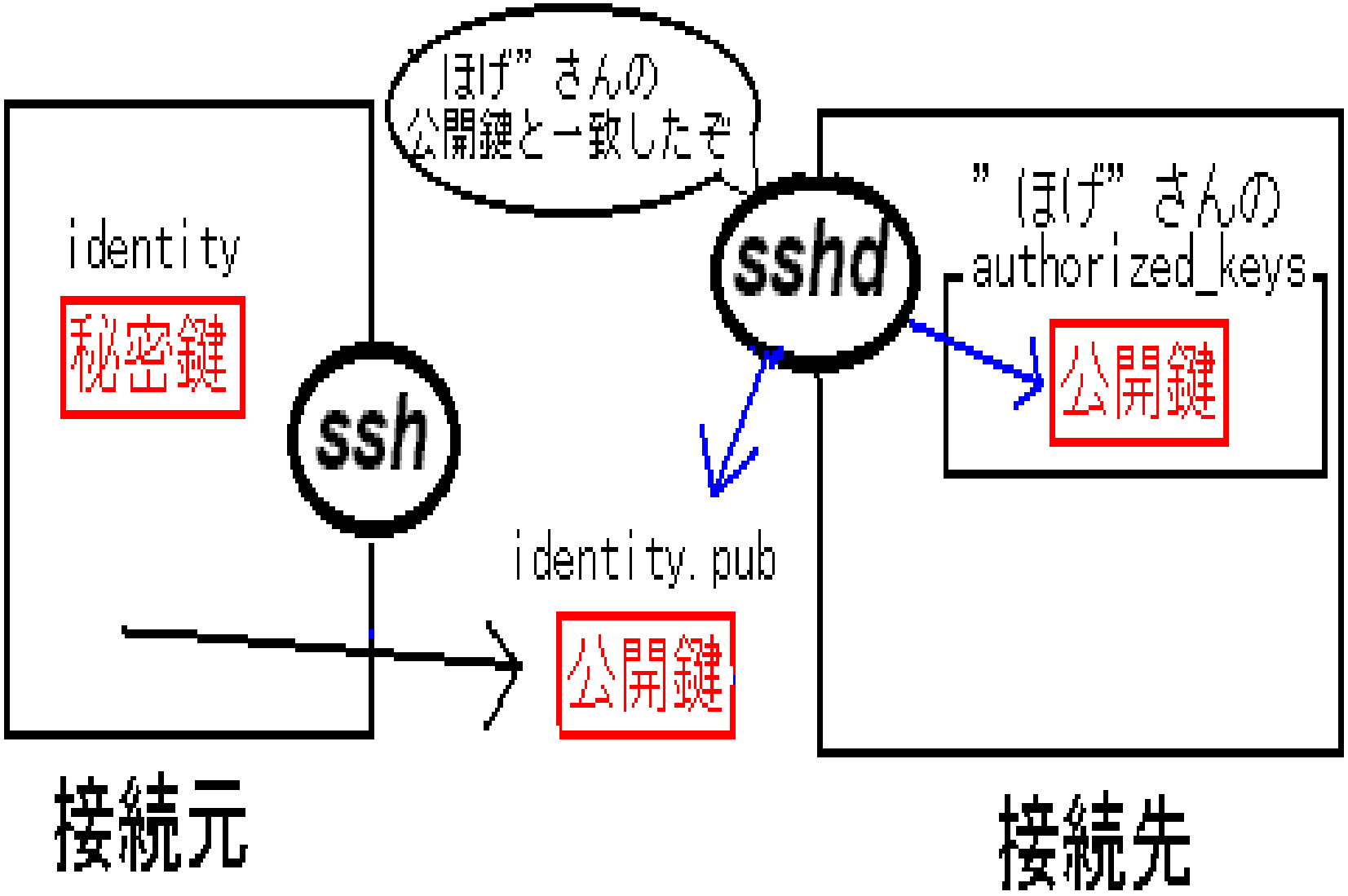
SSHでは、次の保護手段が取られている

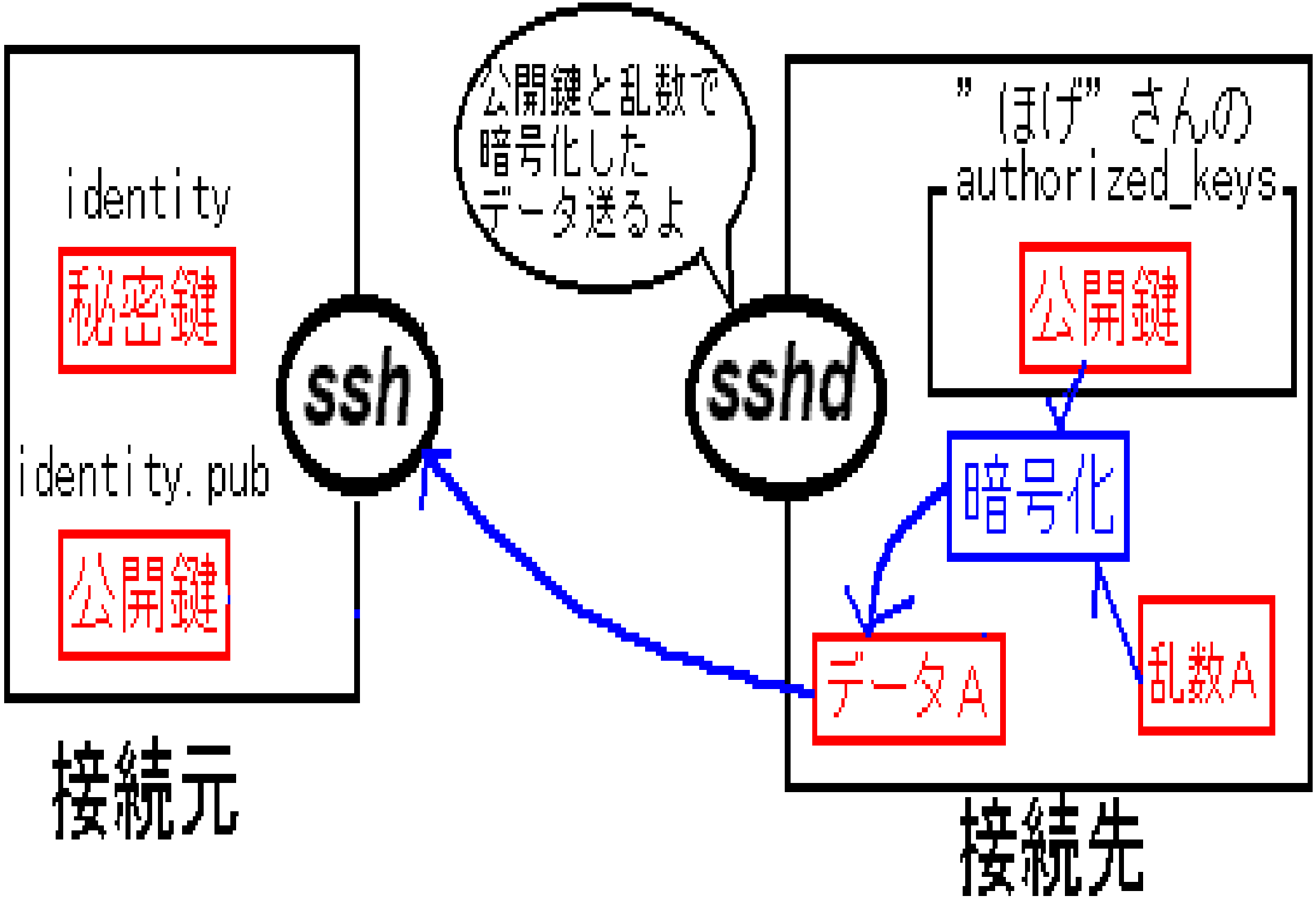
- 初期接続後のセッションで、クライアントは初期接続のときと同じサーバーに接続していることを確認できる。
- クライアントは、サーバーに対し、ユーザー名やパスワードなどの認証情報を暗号化形式で転送できる。
- 接続時に送受信したデータはすべて強力な暗号化を用いて転送されるので、解読は非常に難しくなる。
- クライアントは、シェルプロンプトから起動したX11アプリケーションを使用することができる。この方法では、安全なグラフィカルインターフェイスが提供される。

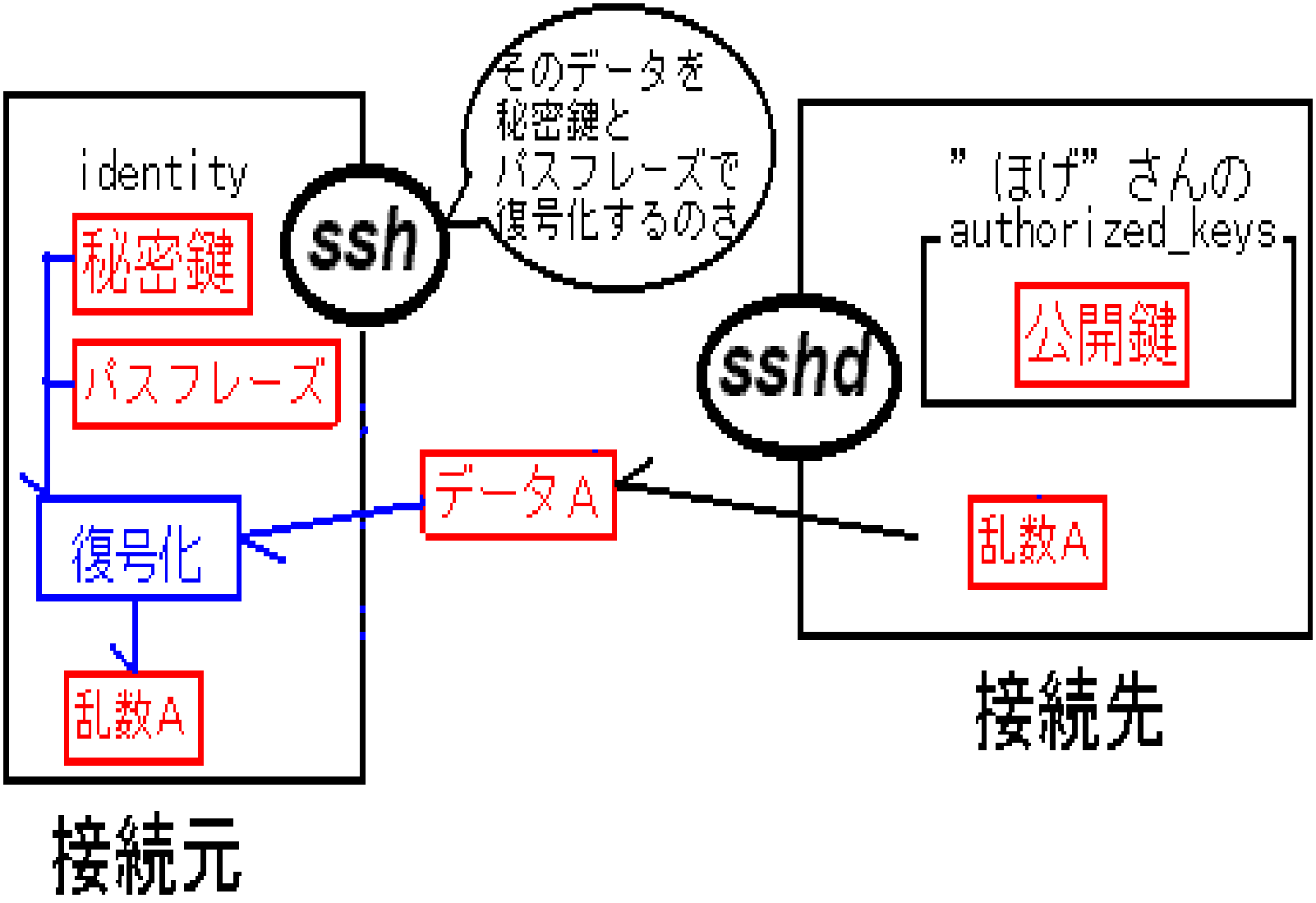
SSHにはいくつかのクライアント認証方式があります。

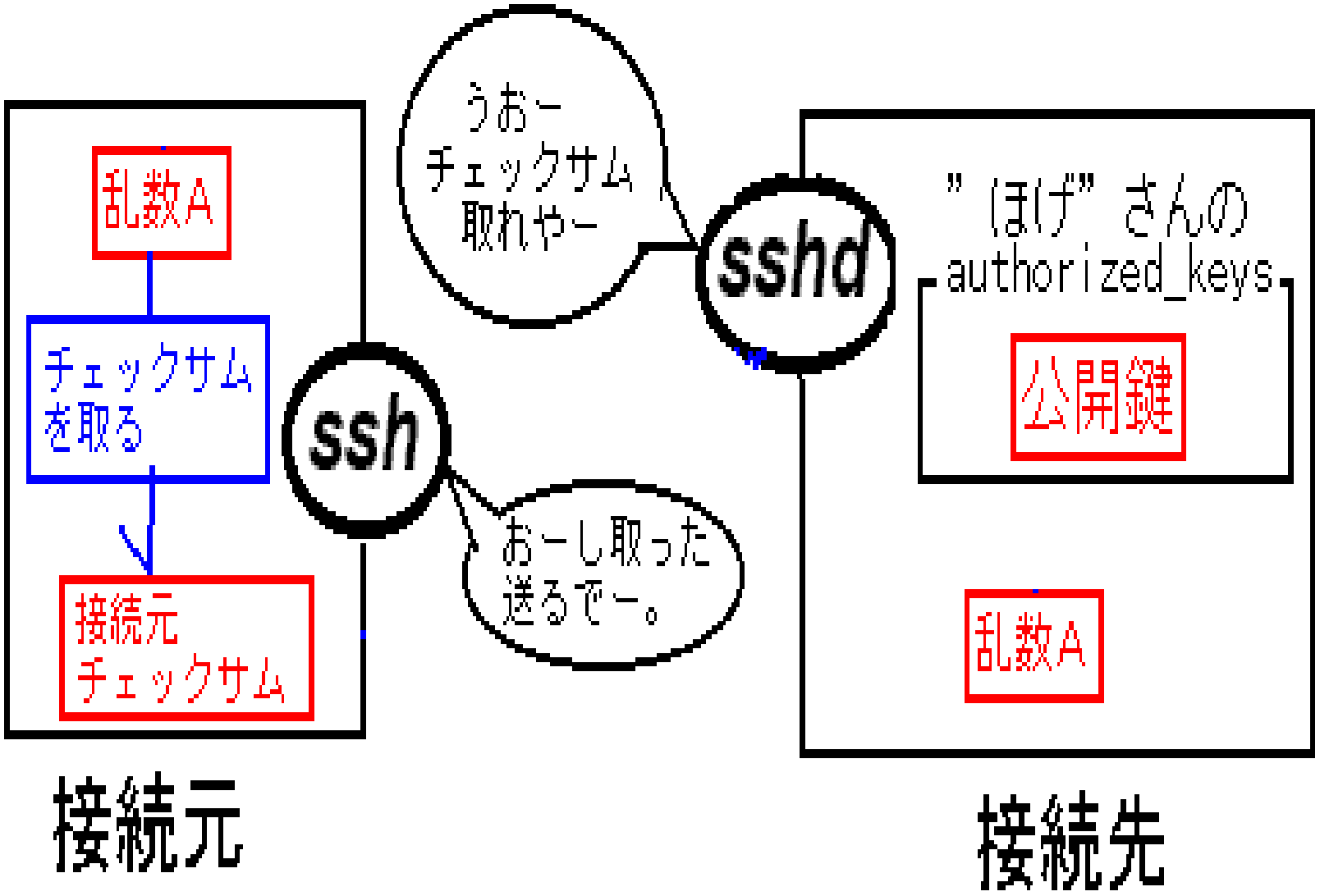
- ホストベースのRSA認証
- ユーザーベースのRSA認証
- パスワード認証

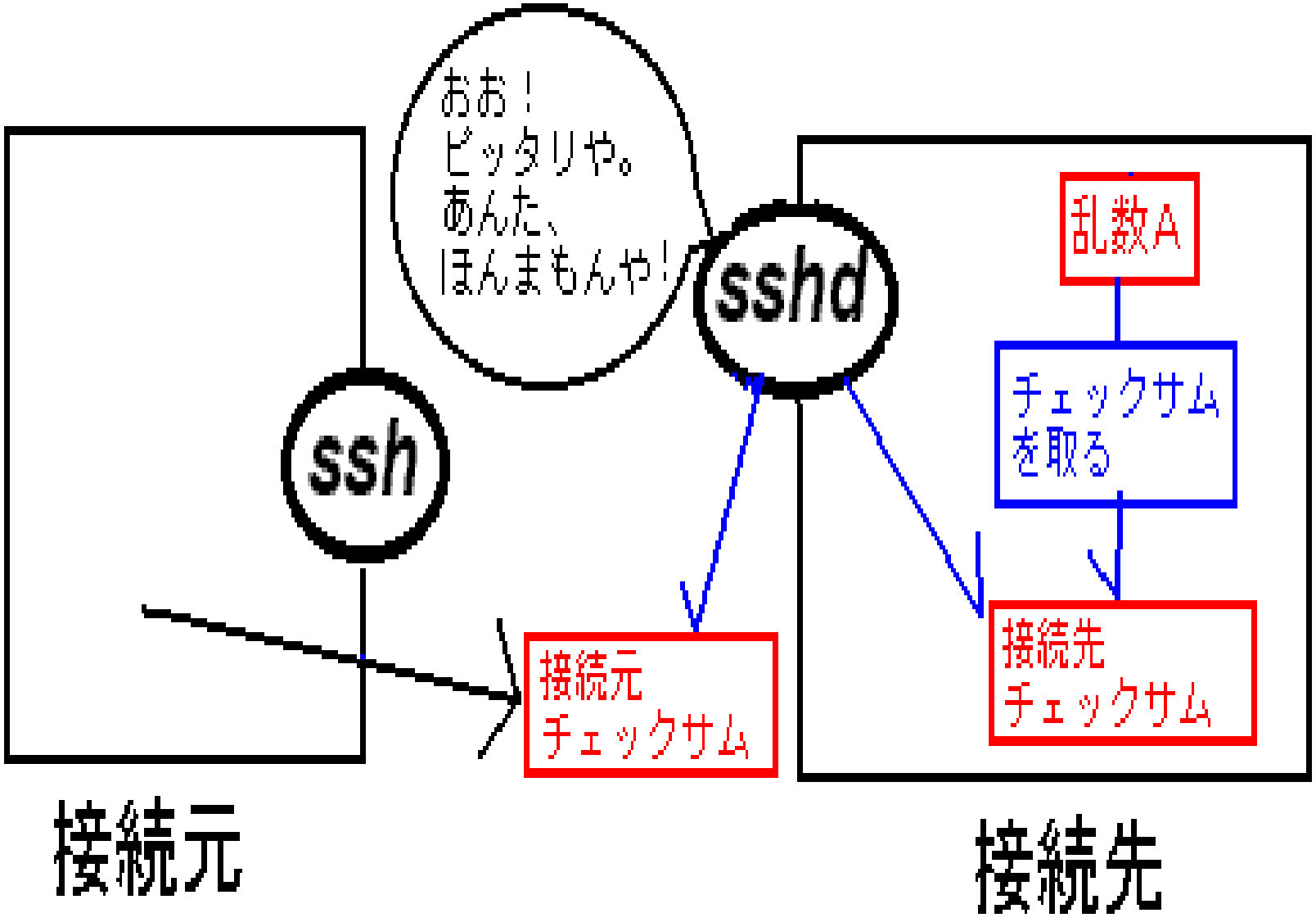

identity
秘密鍵
identity.pub
公開鍵
”ほげ”さん
の公開鍵よーん
ssh
sshd
”ほげ”さんの
authorized_keys
公開鍵
接続元
接続先


ほげ”さんの
公開鍵と一致したぞ
identity
秘密鍵
ssh
sshd
”ほげ”さんの
authorized_keys
公開鍵
identity.pub
公開鍵
接続元
接続先


identity
秘密鍵
identity.pub
公開鍵
ssh
公開鍵と乱数で
暗号化した
データ送るよ
sshd
”ほげ”さんの
authorized_keys
公開鍵
暗号化
データA
乱数A
接続元
接続先


そのデータを
秘密鍵と
パスフレーズで
復号化するのさ
identity
ssh
秘密鍵
パスフレーズ
復号化
乱数A
データA
sshd
”ほげ”さんの
authorized_keys
公開鍵
乱数A
接続先
接続元


うおー
チェックサム
取れやー
sshd
”ほげ”さんの
authorized_keys
公開鍵
乱数A
チェックサム
を取る
ssh
おーし取った
送るでー。
接続元
チェックサム
乱数A
接続元
接続先


おお！
ピッタリや。
あんた、
ほんまもんや！
sshd
ssh
乱数A
チェックサム
を取る
接続元
チェックサム
接続先
チェックサム
接続元
接続先

- パスワード認証

---ユーザ名とパスワードを提示し、ユーザとして認証されればサーバにログインできる。このとき、トランスポート層プロトコルを用いてすでに通信路を暗号化しているので、ネットワーク上をパスワードがそのまま流れるわけではない。

- ホストベース認証

---.rhostファイルや/etc/hosts.equivファイルに、クライアントのホスト名が記載されている場合、パスワードなどの認証を経ずにログインできる仕組み