VSN

Linux Professional Institute Japan LPI-JAPAN

LPICレベル1技術解説セミナー

2013/10/20

株式会社 VSN
小口 尊士

自己紹介

- 会社概要
  - 株式会社 VSN
    - IT・情報システム、メカトロニクス・エレクトロニクス、バイオ・ケミストリー分野におけるエンジニア派遣事業、開発請負、および有料職業紹介事業。
      - http://www.vsn.co.jp
  - 関係会社（Adeccoグループ：Japan）
    - 株式会社VSNビジネスサポート
    - 株式会社VSNマイスト
    - Adecco株式会社
  - 講師
    - 某大手電機メーカーに派遣し、主にUNIXやLinuxを使用したインターネットサーバシステムのプラットフォーム設計、構築、運用業務やツール作成に従事。

株式会社VSN
天王洲トレーニングセンター

アジェンダ

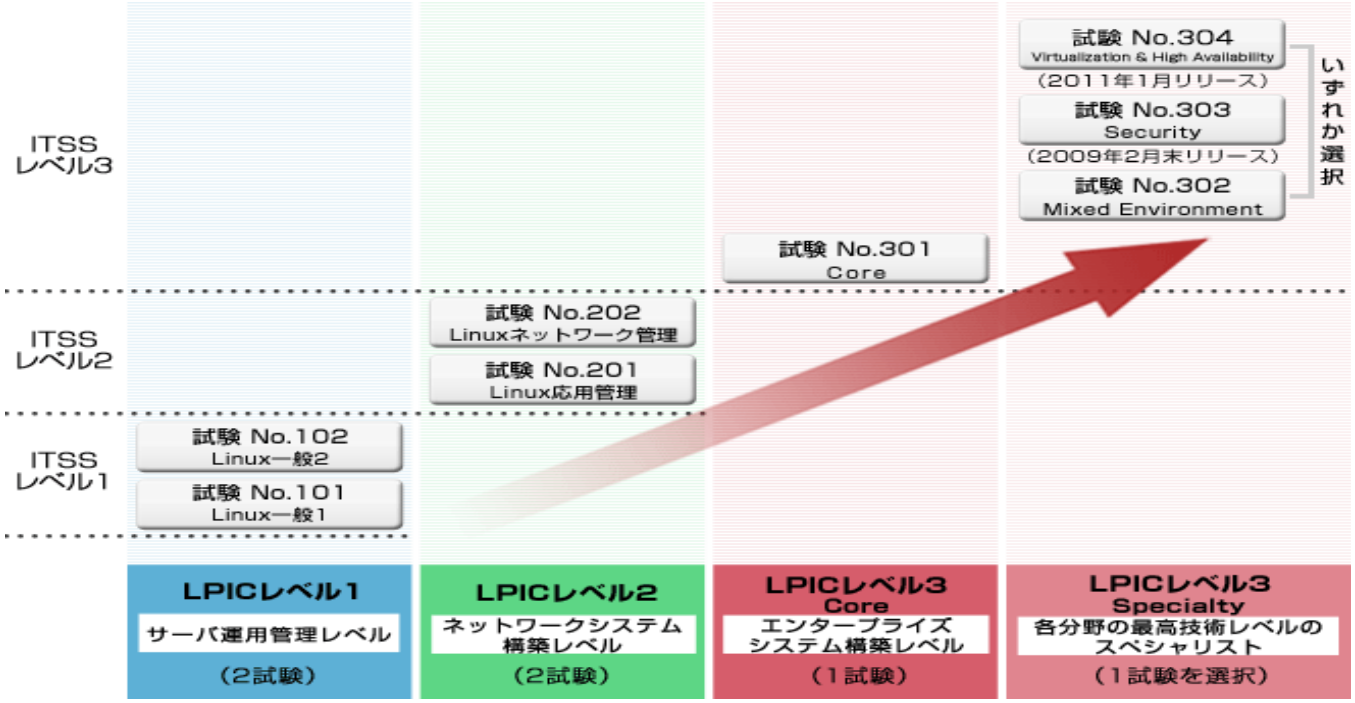
- LPIC 特徴
  - LPIC 特徴
  - LPIC レベル1試験概要
- LPIC レベル1 出題範囲
  - LPIC レベル1 101試験
  - LPIC レベル1 102試験
- 技術解説
  - 主題108　重要なシステムサービス
    - システム時刻を維持する
      - システムクロックとハードウェアクロック
      - NTP（Network Time Protocol）
  - 主題110　セキュリティ
    - 暗号化によるデータの保護
      - OpenSSH（ホスト認証）
      - OpenSSH（公開鍵認証）

Linux Professional Institute

LPIC 特徴

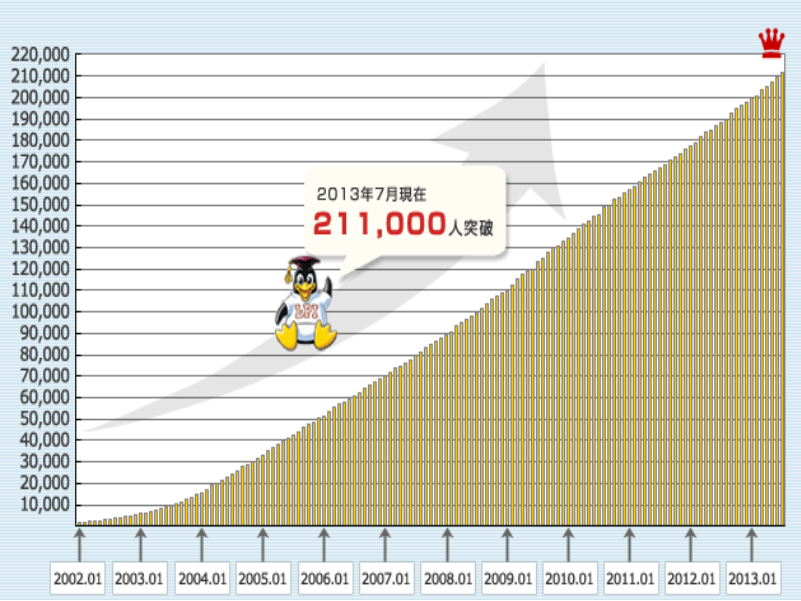
LPIC 特徴

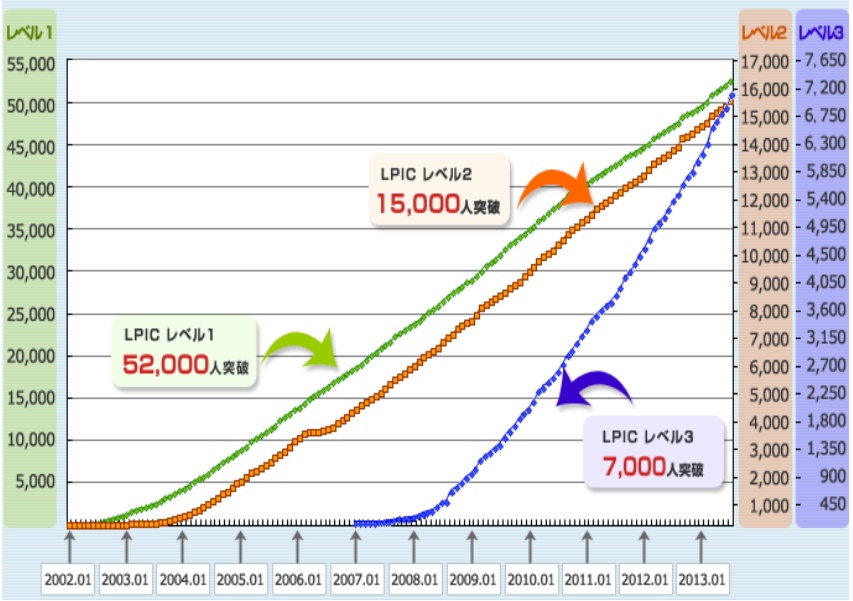
- 上位レベルの受験には下位レベルの認定が必要です。
- 2014年1月1日以降の試験から下記の点が変更されます。
  - LPICレベル2 試験範囲
  - LPICレベル3 資格体系



LPIC 特徴

- 国内累計受験者数 **211,000人** 以上（2013年7月時点）
- 国内各レベル認定者数 **75,000人** 以上（2013年7月時点）





LPIC 試験概要

受験方法　　：CBT
試験時間　　：90分
合否通知　　：スコアレポート
合否タイミング：試験終了後即時
平均勉強時間(※注1)：138.1時間
　　：101試験 81.6時間
　　：102試験 56.5時間

※ 注1 ・・・弊社エンジニアの平均取得時間です。
※ 注2・・・右記例題はサンプルであり、本番試験内容とは一切関係ありません。
その他詳細は、下記LPI-Japan　HPをご参照ください。
http://www.lpi.or.jp/examination/level1.shtml

多肢選択式問題（※注2）

■ 例題

ログインユーザーの一覧を出力するコマンドとして適切なものを選びなさい。

- who
- whoami
- whoareyou
- ldd

コマンド穴埋め問題（※注2）

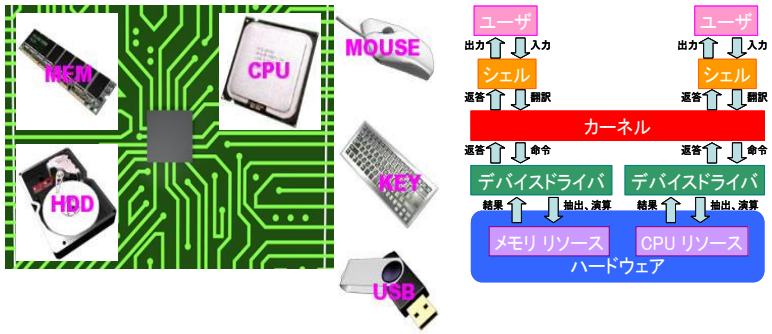
■ 例題

カレントディレクトリの一覧を出力するコマンドを記述しなさい。

LPIC レベル1 出題範囲

LPIC レベル1 101試験

主題101 : システムアーキテクチャ



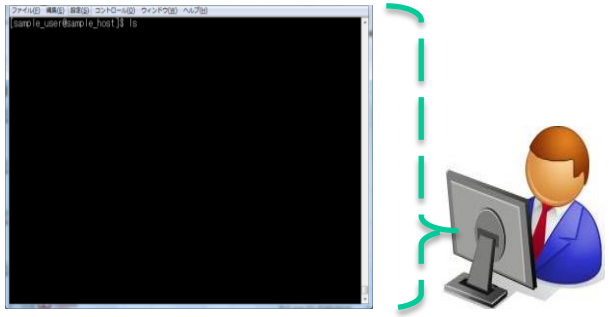
1 ハードウェア設定の決定と構成
2 システムのブート
3 ランレベルの変更とシステムのシャットダウンまたはリブート

主題102 : Linuxのインストールとシステム管理

1 ハードウェアディスクのレイアウト設計
2 ブートマネージャのインストール
3 共有ライブラリを管理する
4 Debianパッケージ管理を使用する
5 RPMおよびYUMパッケージ管理を使用する

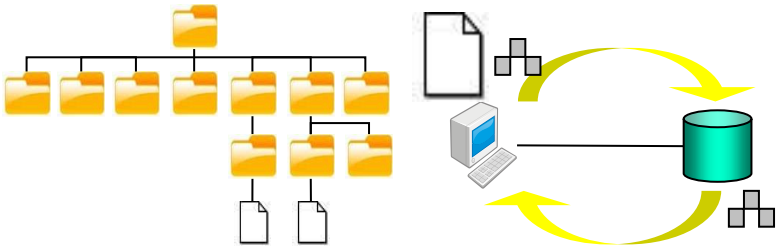
LPIC レベル1 101試験

主題103 : GNUとUnixのコマンド



1 コマンド行で操作する
2 フィルタを使ってテキストストリームを処理する
3 基本的なファイル管理を行う
4 ストリーム、パイプ、リダイレクトを使う
5 プロセスを生成、監視、終了する
6 プロセスの実行優先度を変更する
7 正規表現を使用してテイストファイルを検索する
8 vi を使って基本的なファイル編集を行う

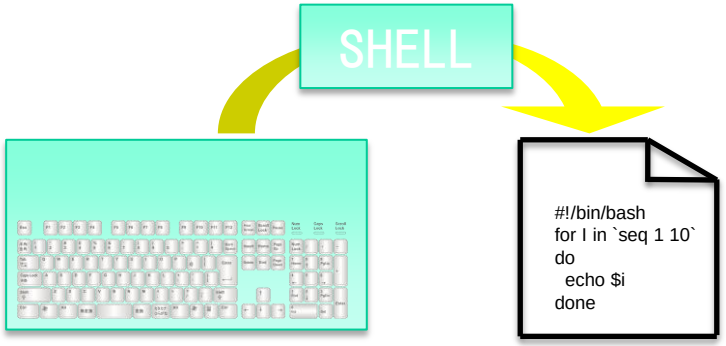
主題104 : デバイス、Linuxファイルシステム、ファイルシステム階層標準



1 パーティションとファイルシステムの作成
2 ファイルシステムの整合性を保持する
3 ファイルシステムのマウントとアンマウントをコントロールする
4 ディスククォータ
5 ファイルのパーミッションと所有者を管理する
6 ハードリンクとシンボリックリンクを作成・変更する
7 システムファイルを見つける、適切な位置にファイルを配置する

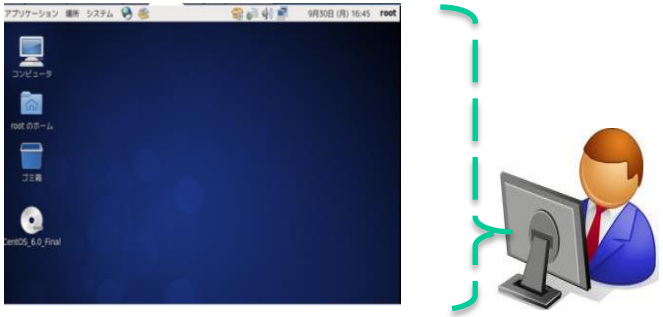
LPIC レベル1 102試験

主題105 :シェル、スクリプト、およびデータ管理



1 シェル環境のカスタマイズと使用
2 簡単なスクリプトをカスタマイズまたは作成する
3 SQLデータ管理

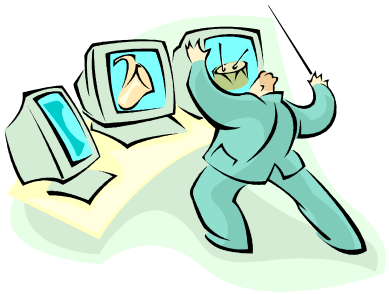
主題106 :ユーザインターフェースとデスクトップ



1 X11のインストールと設定
2 ディスプレイマネージャの設定
3 アクセシビリティ

LPIC レベル1 102試験

主題107 : 管理業務



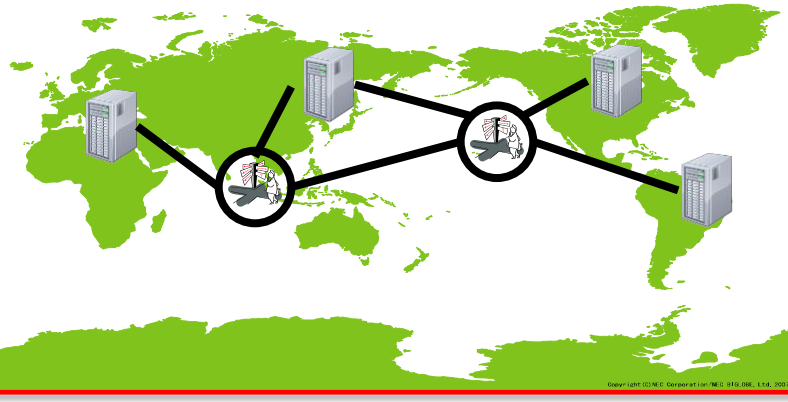
1 ユーザーアカウント、グループアカウント、および関連するシステムファイルを管理する
2 ジョブスケジューリングによるシステム管理業務の自動化
3 ローカライゼーションと国際化

主題108 : 重要なシステムサービス

1 システム時刻を維持する
2 システムのログ
3 メール転送エージェント(MTA)の基本
4 プリンタと印刷を管理する

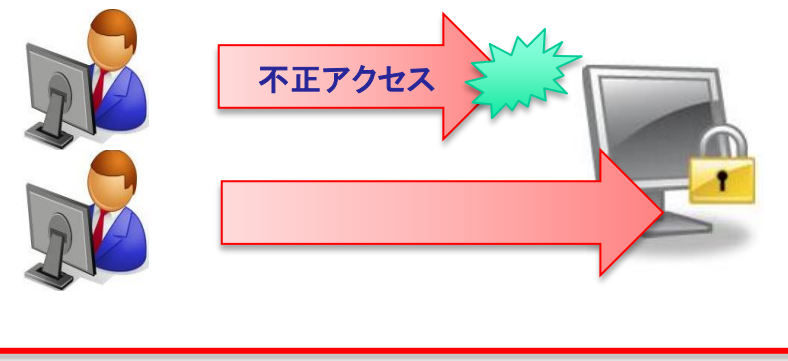
LPIC レベル1 102試験

主題109 : ネットワークの基礎



1 インターネットプロトコルの基礎
2 基本的なネットワーク構成
3 基本的なネットワークの問題解決
4 クライアント側のDNS設定

主題110 :セキュリティ



1 セキュリティ管理業務を実施する
2 ホストのセキュリティ設定
3 暗号化によるデータの保護

技術解説

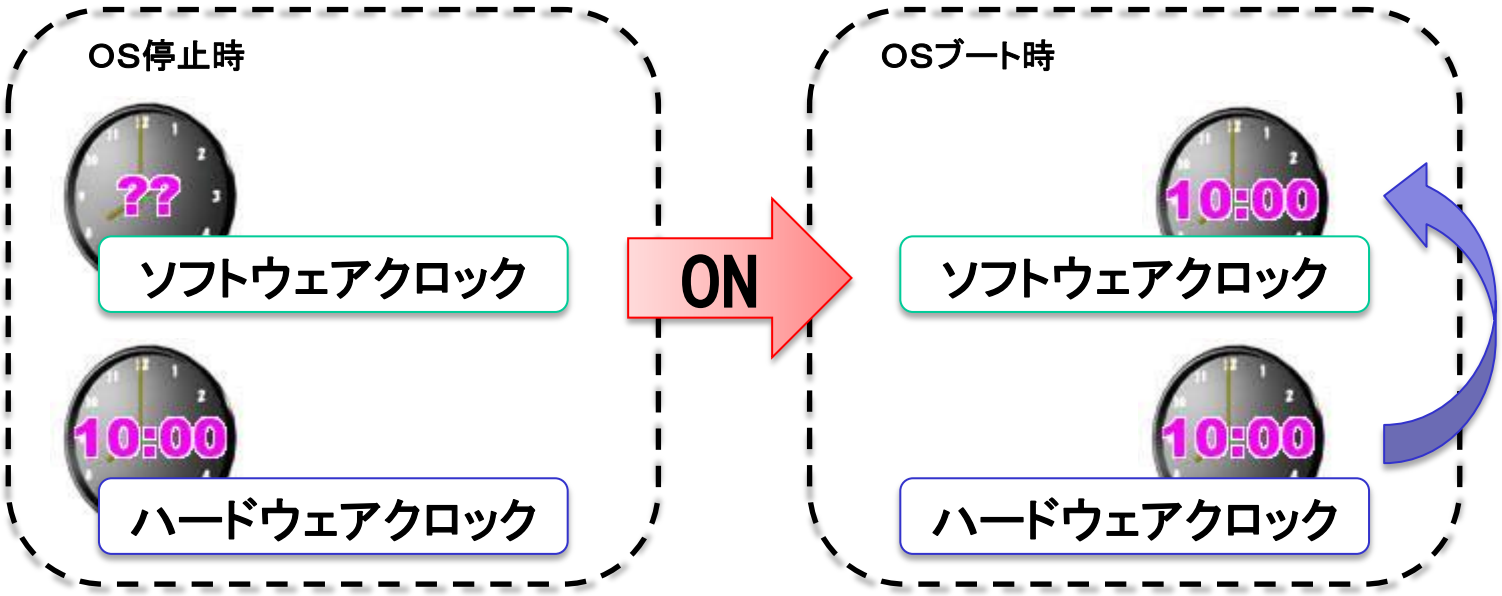
主題108　重要なシステムサービス

- システムクロックとハードウェアクロック
  - Linuxカーネルが保持する時計（システムクロック）とマザーボードが保持する時計（ハードウェアクロック）の時計を合わせることは地味ですが非常に重要です。
  - 時計が合っていないことで、スケジューリングされたジョブの実行時刻、ログの出力時刻に差異が発生し、Serverの管理に支障が出ます。
- コマンド
  - Client 側　　：date［ **オプション**］
    ：hwclock［ **オプション** ］　※ 注1

※ 注1
[ ] はオプションですので、実行時に省略することも可能です。

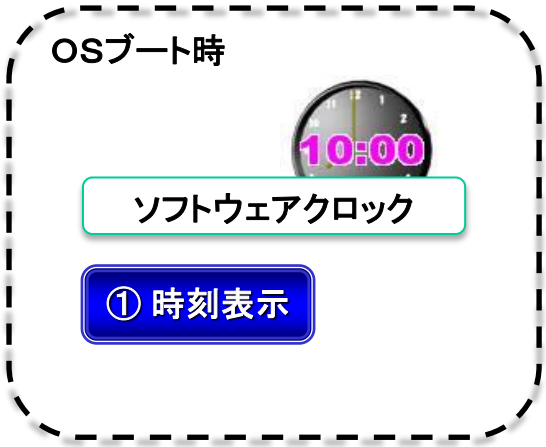
主題108　重要なシステムサービス

時刻同期（Server内部）



主題108　重要なシステムサービス

- ハードウェアクロックとシステムクロック（動作解説）

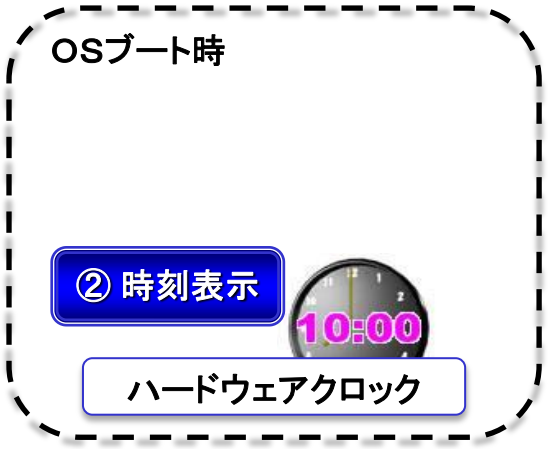



```
$ date   ―①
Sun Oct  20 14:30:00 JST 2013   ※注1
```

※注1
設定した環境変数LANGの値によって出力される言語が異なりますので、ご注意ください。

主題108　重要なシステムサービス

- ハードウェアクロックとシステムクロック（動作解説）

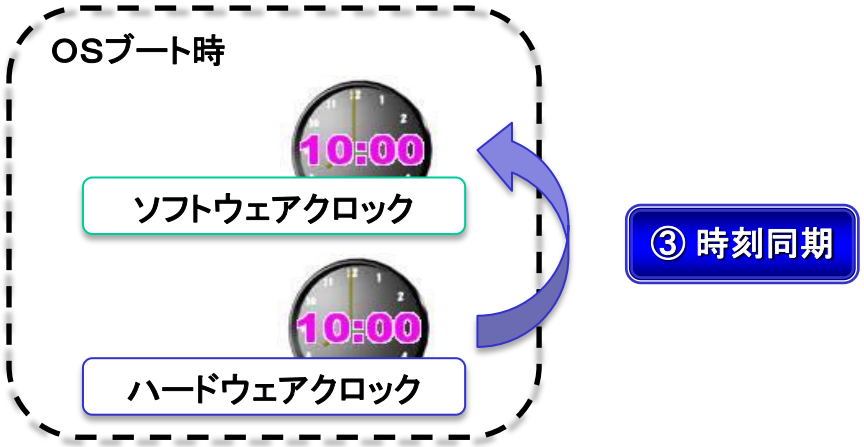



```
$ su -   ※注1
# hwclock  -r   ー②
Sun Oct  20 14:30:00 2013  -0.200798 seconds
```

※注1
ハードウェアクロックの表示はスーパーユーザしか実行できませんので、ご注意ください。

主題108　重要なシステムサービス

- ハードウェアクロックとシステムクロック（動作解説）




```
$ su -   ※注1
# hwclock  -s   ー③
```

※注1
時刻同期はスーパーユーザしか実行できませんので、ご注意ください。

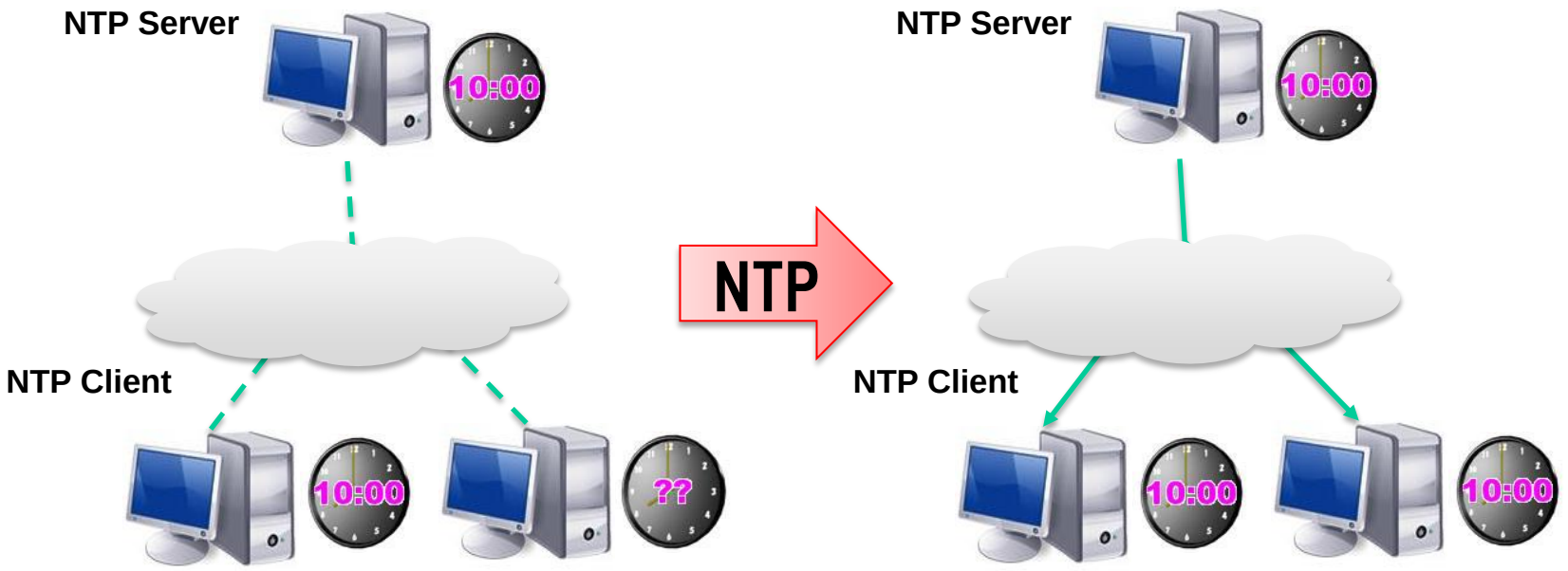
主題108　重要なシステムサービス

- NTP（Network Time Protocol）
  - システムクロックやハードウェアクロックによる時刻同期は精度が低く、信頼性に欠ける点があり、またシステム間での時刻同期には適していません。
  - システム間の時刻同期はNTPを使用します。
- ファイル
  - NTP Client 側　　：/etc/ntp.conf
  - NTP Server 側　　：/etc/ntp.conf
- コマンド
  - NTP Client 側　　：ntpdate［ **オプション** ］**ホスト名** or **IPアドレス**　※ 注1

※ 注1
[ ] はオプションですので、実行時に省略することも可能です。
ホスト名を使用する場合は、Domain Name Systemや/etc/hostsを利用した名前解決ができる必要があります。

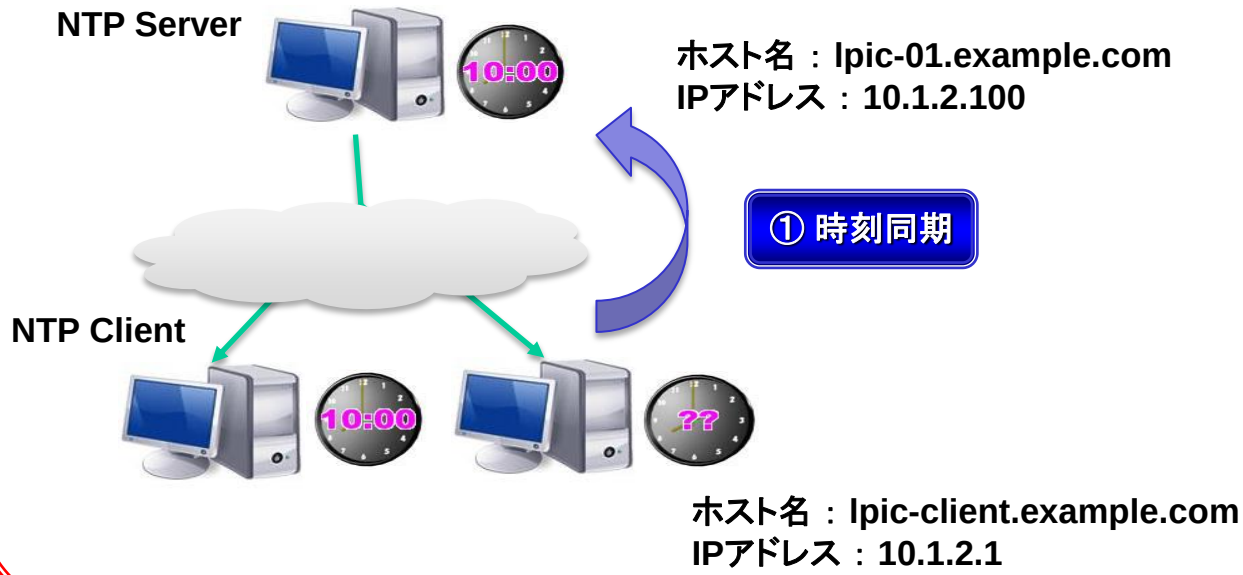
主題108　重要なシステムサービス

時刻同期（システム間）



主題108　重要なシステムサービス

- NTP（Network Time Protocol 動作解説）




```
# ntpdate 10.1.2.100  ―①
20 Oct 14:30:00 ntpdate[29658]: step time server 10.1.2.100 offset 800.828809 sec
```

主題108　重要なシステムサービス

- NTP（Network Time Protocol 動作解説）

コマンド名	オプション	意味
date	MMDDhhmm	システムクロックを「MMDDhhmm」で設定
	+%Y%m%d	システムクロックを %Y(西暦)、%m(月)、%d(日)で表示

コマンド名	オプション	意味
hwclock	-w	システムクロックをハードウェアクロックに反映
	-s	ハードウェアクロックをシステムクロックに反映

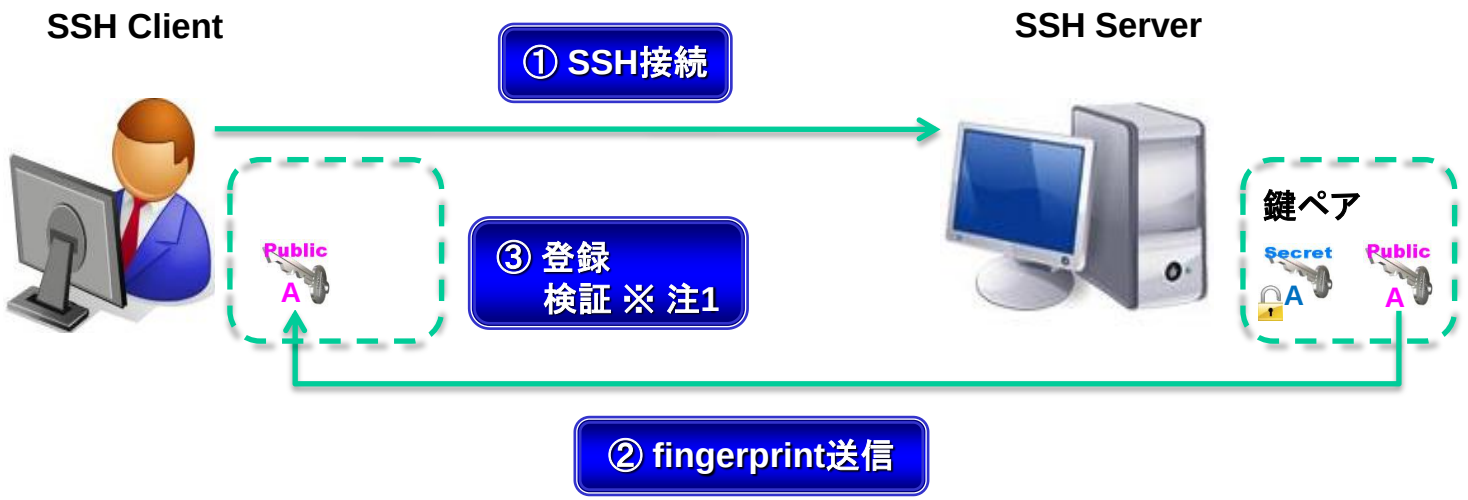
主題110　暗号化によるデータの保護

- OenSSH（ホスト認証）
  - ホスト認証は“偽装されたServerへの誤ったログイン”を防止するための仕組み。
- ファイル
  - SSH Client 側　　：${HOME}/.ssh/known_hosts（**接続Serverの公開鍵リスト**）
  - SSH Server 側　　：/etc/ssh/ssh_host_rsa_key（**ホスト公開鍵**）
  - 　　：/etc/ssh/ssh_host_rsa_key.pub（ホスト秘密鍵）
- コマンド
  - SSH Client 側　　：ssh ［ **オプション** ］ **ホスト名** or IP**アドレス**　※ 注1

※ 注1
[ ] はオプションですので、実行時に省略することも可能です。
ホスト名を使用する場合は、Domain Name Systemや/etc/hostsを利用した名前解決ができる必要があります。

主題110　暗号化によるデータの保護

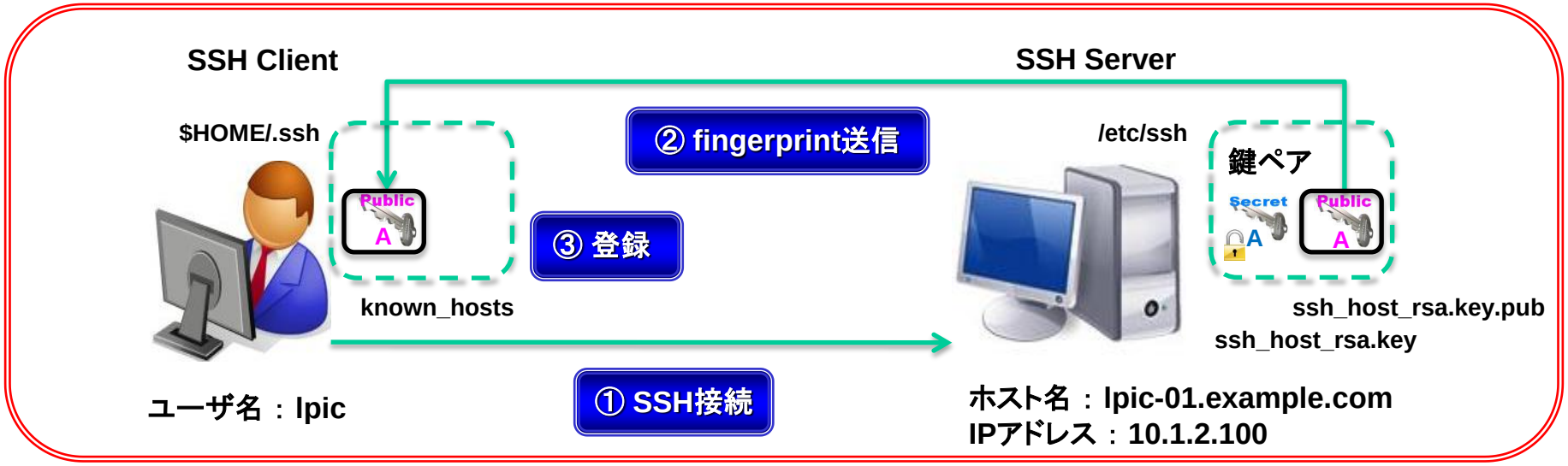
OpenSSH（ホスト認証）



※ 注1
初回接続時、SSH Client側にSSH Serverの公開鍵を登録した場合、次回以降は「登録」ではなく、「検証」を実施します。

主題110　暗号化によるデータの保護

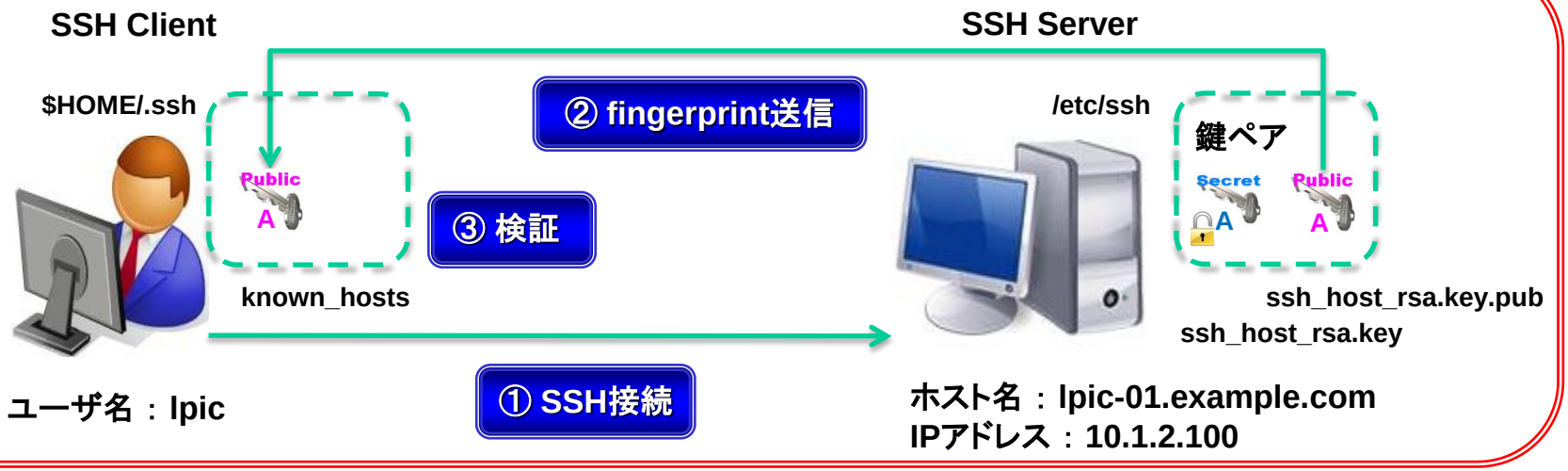
- OenSSH（ホスト認証動作解説）初回接続時




```
$ ssh  -l lpic 10.1.2.100   ―①
The authenticity of host '10.1.2.100 (10.1.2.100)' can't be established.
RSA key fingerprint is 03:71:6d:ce:ef:41:91:d8:9f:a4:c9:8f:be:b1:24:f8.   ―②
Are you sure you want to continue connecting (yes/no)?  yes   ―③
Warning: Permanently added '10.1.2.100' (RSA) to the list of known hosts.
```

主題110　暗号化によるデータの保護

- OenSSH（ホスト認証動作解説）登録以降（正常）

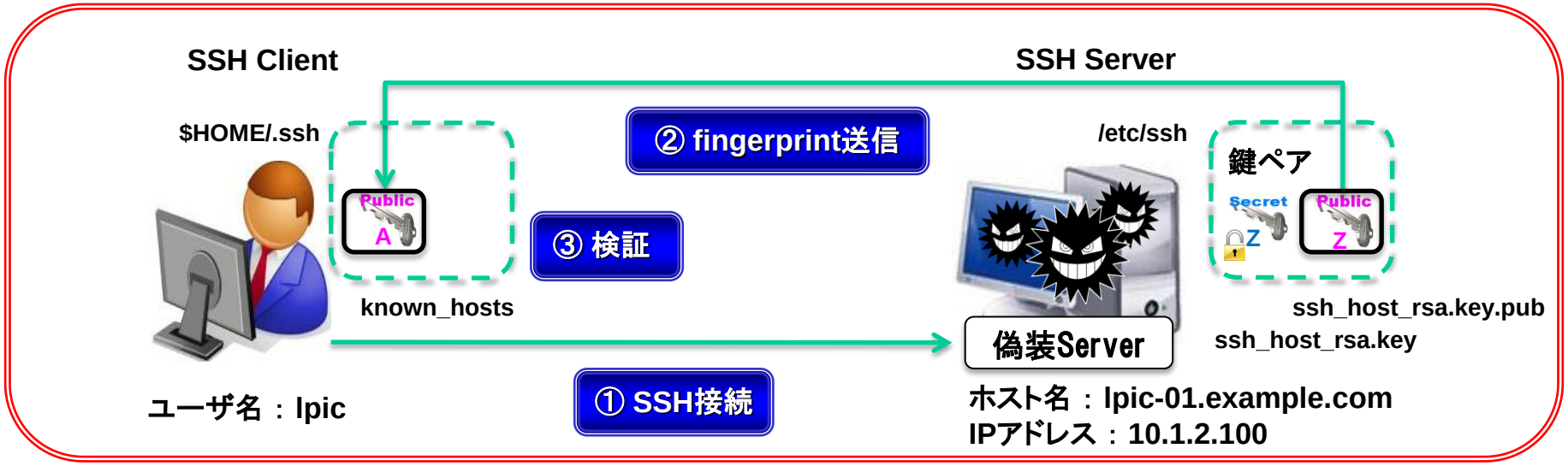


$ *ssh -l lpic 10.1.2.100*　ー①
lpic@10.1.2.100's password：***xxxxxxxx*** ※ 注1

※ 注1
上記はパスワード認証を実施した場合の出力内容であり、公開鍵認証による応答は次節にてご紹介いたします。
②、③番の内容はモニターには明示的に表示されませんので、ご注意ください。

主題110　暗号化によるデータの保護

- OenSSH（ホスト認証動作解説）登録以降（偽装Serverへ誘導された場合）




```
$ ssh  -l lpic 10.1.2.100   ー①
```

- 主題110　暗号化によるデータの保護
  - OenSSH（ホスト認証動作解説）登録以降（偽装Serverへ誘導された場合）

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!         @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!

Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
16:86:ae:64:03:a3:91:51:a9:94:10:44:5a:cb:bf:49.
Please contact your system administrator.
Add correct host key in /root/.ssh/known_hosts to get rid of this message.
Offending key in /lpic/.ssh/known_hosts:7
RSA host key for 10.1.2.100 has changed and you have requested strict checking.
Host key verification failed. ー③
```

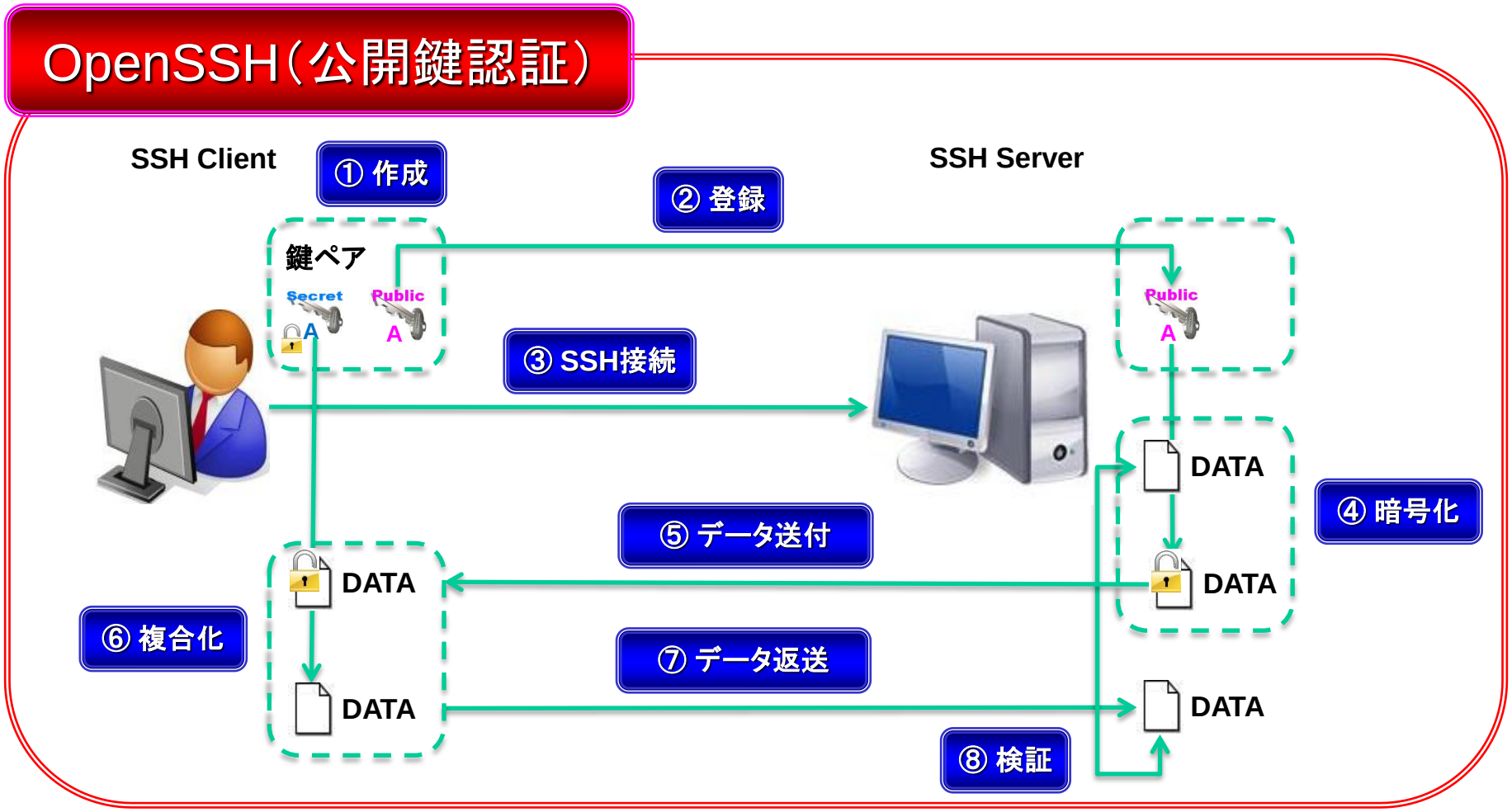
※ 読みやすくするために若干出力内容を整形しておりますので、ご注意ください。

主題110　暗号化によるデータの保護

- OenSSH（公開鍵認証）
  - 公開鍵認証はネットワーク上にユーザパスワードを送信せずに、リモートログインするための仕組み。
- ファイル
  - SSH Client 側　：${HOME}/.ssh/id_rsa.pub（**ユーザ公開鍵**）
    ：${HOME}/.ssh/id_rsa（**ユーザ秘密鍵**）
  - SSH Server 側　：${HOME}/.ssh/authorized_keys（**ユーザ公開鍵リスト**）
- コマンド
  - SSH Client 側　：ssh-keygen［ **オプション** ］※注1
    ：scp **コピー元**File名 **コピー先ホスト名:コピー先** File名
    ：ssh-agent［ **オプション** ］
    ：ssh-add［ **オプション** ］

※ 注1
[ ] はオプションですので、実行時に省略することも可能です。

主題110　暗号化によるデータの保護



主題110　暗号化によるデータの保護

- OenSSH（公開鍵認証動作解説）

$ *ssh-keygen　-t　rsa*　ー①
Enter file in which to save the key (/lpic/.ssh/id_rsa): ***xxxx***　※ 注1
Enter passphrase (empty for no passphrase): ***xxxxxxxx***
Enter same passphrase again: ***xxxxxxxx***
※ 注1
出力内容を整形してますので、ご注意ください。鍵ペアを既定のまま作成する場合は、未入力でEnterを押してください。
鍵をパスワードで保護したい場合は、同じパスワードを2回入力してください。またパスワードを設定しないことも可能です。

主題110　暗号化によるデータの保護

- OenSSH（公開鍵認証動作解説）


```
$ scp $HOME/.ssh/id_rsa.pub lpic@10.1.2.100:lpic_key.pub  ―②  ※ 注1
lpic@10.1.2.100's password: xxxxxxxx  ※注2
lpic_key.pub                                  100%  410     0.4KB/s   00:00
```

※ 注1　コピー先file名（lpic_key.pub）は任意のファイル名設定します。
※ 注2　パスワードはモニターには明示的に表示はされませんので、ご注意ください。

主題110　暗号化によるデータの保護

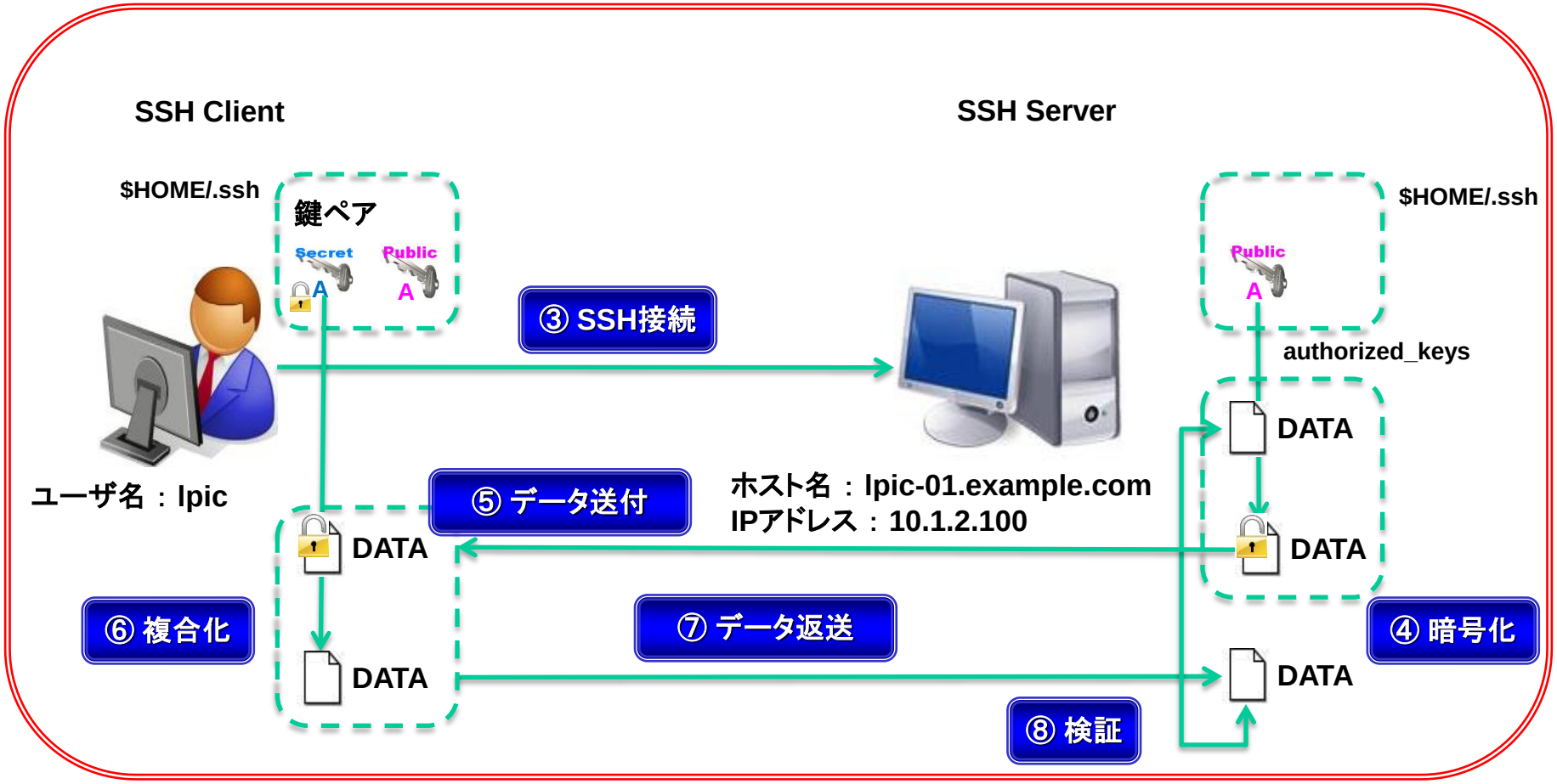
- OenSSH（公開鍵認証動作解説）


```
$ ssh -l lpic@10.1.2.100　－②
lpic@10.1.2.100's password: xxxxxxxx　※注1
$ mkdir $HOME/.ssh
$ cat $HOME/lpic_key.pub >> $HOME/.ssh/authorized_keys
$ chmod 600 $HOME/.ssh/authori zed_keys
```

※ 注1　パスワードはモニターには明示的に表示はされませんので、ご注意ください。

主題110　暗号化によるデータの保護

- OenSSH（公開鍵認証動作解説）



- 主題110　暗号化によるデータの保護
  - OenSSH（公開鍵認証動作解説）

```
$ exit
$ ssh -l lpic@10.1.2.100   ー③
Enter passphrase for key '/lpic/.ssh/id_rsa': xxxxxxxx   ー⑥ ※注1
Last login: days Mon  day MM:DD:SS YYYY from SSH ClientのIPアドレス
$
```

※ 注1　パスワードはモニターには明示的に表示はされず、また④、⑤、⑦、⑧番内容はモニターには明示的に表示されませんので、ご注意ください。

- 主題110　暗号化によるデータの保護
  - OenSSH（公開鍵認証）の問題点
    - パスワード入力
      - sshコマンドを使ったリモートログインでは、パスワード認証、公開鍵認証ともにリモートホストへのログイン時にパスワードの入力が必要です。
      - ユーザ秘密鍵にパスワードを設定しない場合は例外ですが、セキュリティ上適切ではありません。

＜パスワード認証の場合＞
$ *ssh -l lpic@10.1.2.100*
lpic@10.1.2.100's password: ***xxxxxxxx***　※注1

＜公開鍵認証の場合＞
$ *ssh -l lpic@10.1.2.100*
Enter passphrase for key '/lpic/.ssh/id_rsa': ***xxxxxxxx***　※注1

※ 注1　パスワードはモニターには明示的に表示はされので、ご注意ください。

- 主題110　暗号化によるデータの保護
  - OenSSH（公開鍵認証）の解決策
    - ユーザ秘密鍵をメモリに記憶する
      - ssh-agent
        - » ssh-add

```
$ ssh-agent  bash
$ ps aux | grep ssh-agent
lpic    26260  0.0  0.0  54916   808 ?        Ss   10:43   0:00 ssh-agent bash
$ ssh-add
Enter passphrase for key '/lpic/.ssh/id_rsa': xxxxxxxx   ※注1
$ ssh-add -l
2048 c1:6c:68:e0:1a:bc:35:e3:9a:8d:02:f0:c9:6b:68:ec /lpic/.ssh/id_rsa (RSA)
$ ssh -l lpic@10.1.2.100
Last login: days Mon  day MM:DD:SS YYYY from SSH ClientのIPアドレス
$

※ 注1　パスワードはモニターには明示的に表示はされので、ご注意ください。
```

主題110　暗号化によるデータの保護

- OenSSH（公開鍵認証コマンド解説）

コマンド名	オプション	意味
ssh-keygen	-t　rsa	RSA暗号での鍵ペア作成
	-t　dsa	DSA暗号での鍵ペア作成
	-p	パスワード変更

コマンド名	オプション	意味
scp	-p	コピー元Fileの属性情報を保持したまま、リモートコピー
	-r	再帰的コピー

コマンド名	オプション	意味
ssh-agent	-l	保持パスワードのリスト