

IoT時代のICT管理システムの在り方

林 経正



自己紹介と、ITRCとの関わり

- 日本電信電話株式会社にて、
 - 通信向けLSI構成法の研究開発、
映像配信系ネットワークサービスの開発、
IDS/IPS中心にネットワークセキュリティの研究開発、
 - 米国にてベンチャー企業立ち上げ、
 - 新規事業立ち上げに従事
- ベンチャー企業にて、
 - Webマーケティングサービスの開発・運用に従事
 - NTTグループに買収される経験
- 2012年2月に起業
 - 大手通信事業会社のネットワークプロビジョニングシステム、監視システムの開発
 - NFV関連の大型企業買収のデューデリジョン実施
 - 各省庁、自治体等から自社製品「SMART Gateway」製品名指定で公開調達
 - 仮想化、自動化、セキュリティ技術に軸をおいて事業展開
- ITRCとの関わり
 - 2016年5月にITRCにて講演
「SDNの事業展開とWhitebox技術の最前線」
 - **これをきっかけにKDDIグループへビジネス成立**
 - 今年には妻と子供を同伴
 - **講演活動の家庭内理解が深まる！？**

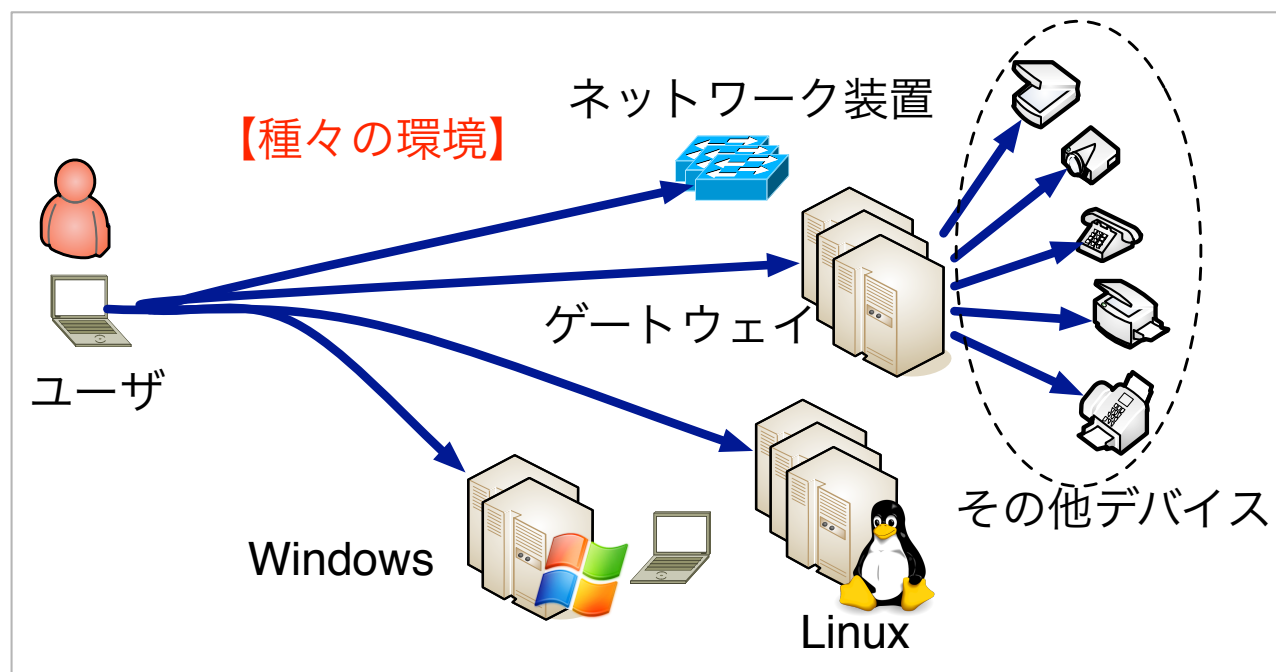
アジェンダ

- IoT時代のICT運用管理
- 過去の実績を振り返る
- 我々が目指すもの
- IoT時代のICT管理システムのデモ

① IoT時代のICT運用管理

IoT時代に求められるICTインフラ管理

- より多くのサービスが提供
- ヘテロなICTインフラに対して、より複雑なシステム管理が必要
- 巨大で複雑なICTインフラの運用コストの削減が重要
- どうやって低運用コストを実現？
- **単純で簡易な管理システム**



② 過去の実績を振り返る

SDNを利用した簡易化/自動化の成果

- 論理業務とハード設備調達業務の分離し、
論理業務に集中
 - ネットワークサービスの単純化と、
多量の客様オーダー処理の実現
 - ICT管理自動化を促進
- SDN化により、OPEXを50%削減（APNOMS 2014'
keynote speech）
- NTTコムはSDN自動化で成功
 - 300 顧客オーダー/月（2012年）
 - 1,300 顧客オーダー/日（2016年）

③ 我々が目指すもの

単純で簡易な管理システムの要件

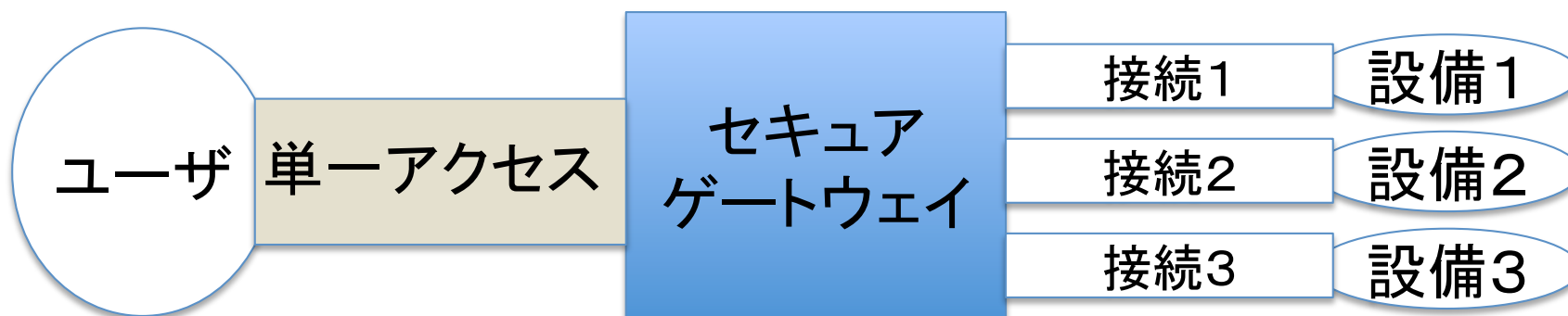
- ICTへのアクセス方法は画一化
- 管理オペレーションは、種々のICTインフラの仕様に非依存
 - 管理するICTインフラの装置、ミドルウェア、OSに非依存
- 特別なVPNアプリなどのインストールせず
- ICTインフラに手を入れず

期待する効果

- ① 新しいITインフラ設備、新しいOS、ミドルウェアに対応
 - 既存のITインフラ設備、サービスに影響を与えない
 - ITインフラ設備や、サービスの変更に影響されない
 - サイバーセキュリティコストを低減化
- ② よりシンプルで容易な管理が可能
 - ITインフラ管理が容易
 - より多くのITインフラ設備、サービスを運用可能
 - サービス運用コストを低減化
- ③ 操作の完全再現と、分析が容易
 - 危険な業務を速やかに検知可能
 - 有事の事態に完全に把握

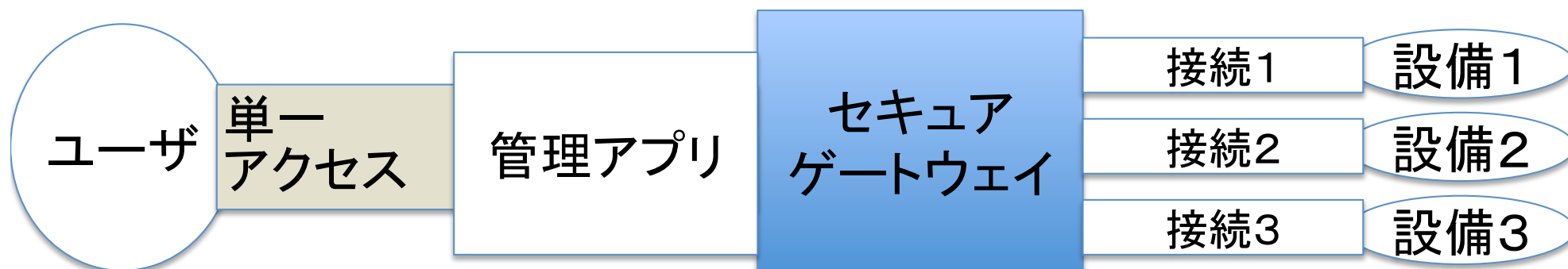
目指すべきシンプルで容易な運用とは

- IT資産へのアクセス方法が単一化
 - どんなサーバ、ネットワーク機器にでも同じ管理方法
 - OSが変わっても追加コストをかけずに対応
- 特別なクライアントソフトは必要なし
- 管理対象のIT資産の変更なし
 - 機能追加(エージェントのインストール含む)
 - コンフィグ変更なし



本日紹介するセキュアゲートウェイ

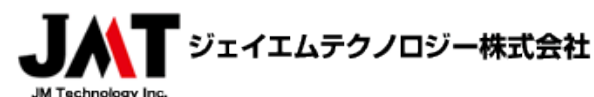
- 「**SMART Gateway**」というセキュアゲートウェイ
- 同時に複数のIT資産を操作可能
- 定型業務は自動処理が可能
- 実パスワードの隠蔽が可能
- 全てのコマンド業務を再現、分析可能
- 全機能を外部システムで制御可能



これまでの導入実績



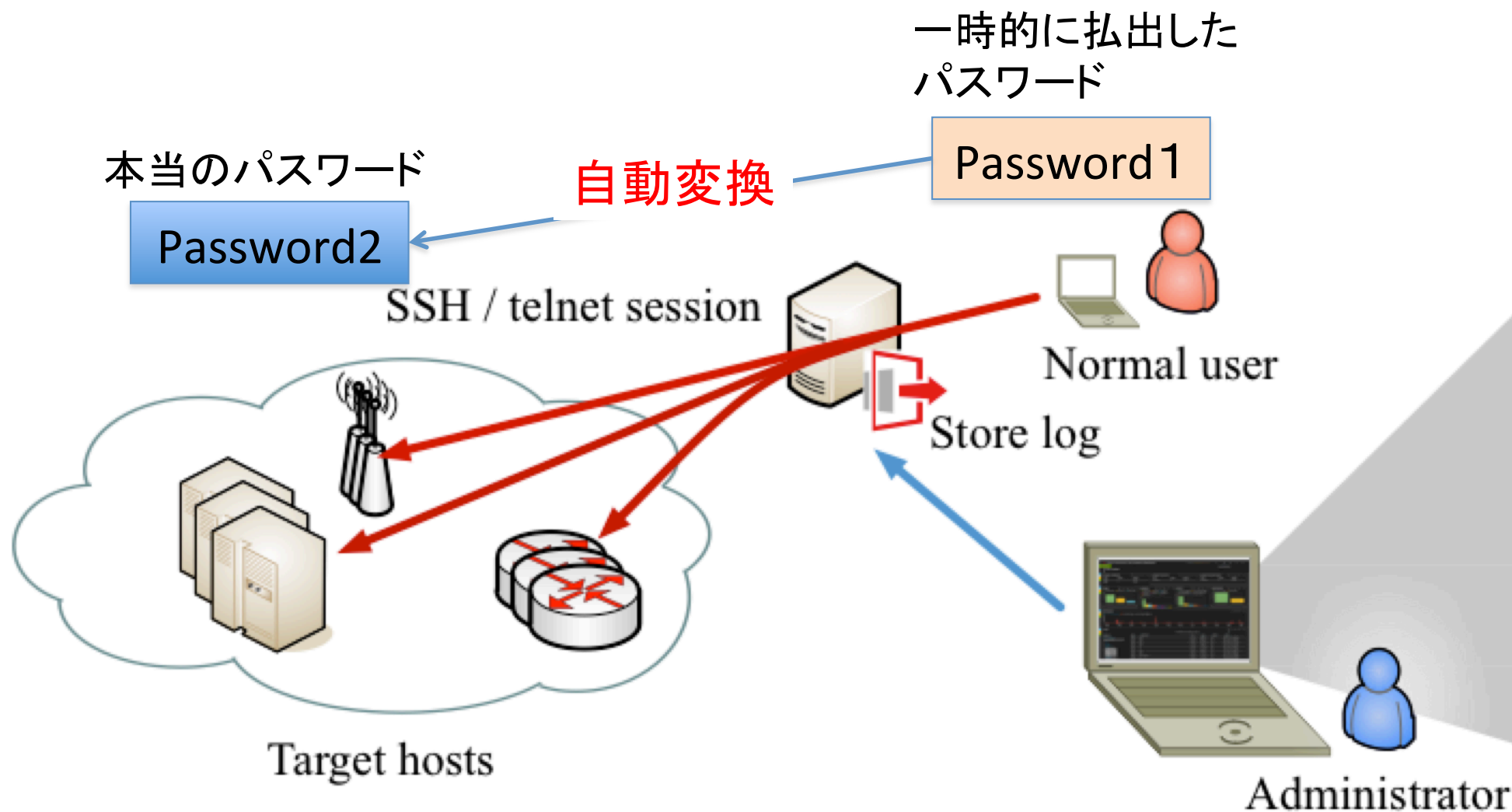
東洋ビジネスエンジニアリング株式会社



なぜ、SMART Gatewayが選ばれたか？

- 利用コマンド制限においては、管理対象は、OSや機器を選ばない【**世界唯一**】
 - 既存のIT資産運用に影響を与えず導入可能
- httpsを利用したセキュアで導入が楽なVPNを提供
 - ブラウザを介してファイル送受信が可能【**世界初**】
- 有事の事態に、実際に行われた操作を完全に再現し、容易に記録・分析可能【**他製品にない**】
 - インシデントが発生した場合でも、「私やっていません！」問題を排除
- IT資産の実パスワードを隠蔽でき、セキュアな運用が可能

IT資産の実パスワードを隠蔽



導入事例に見る典型的な課題

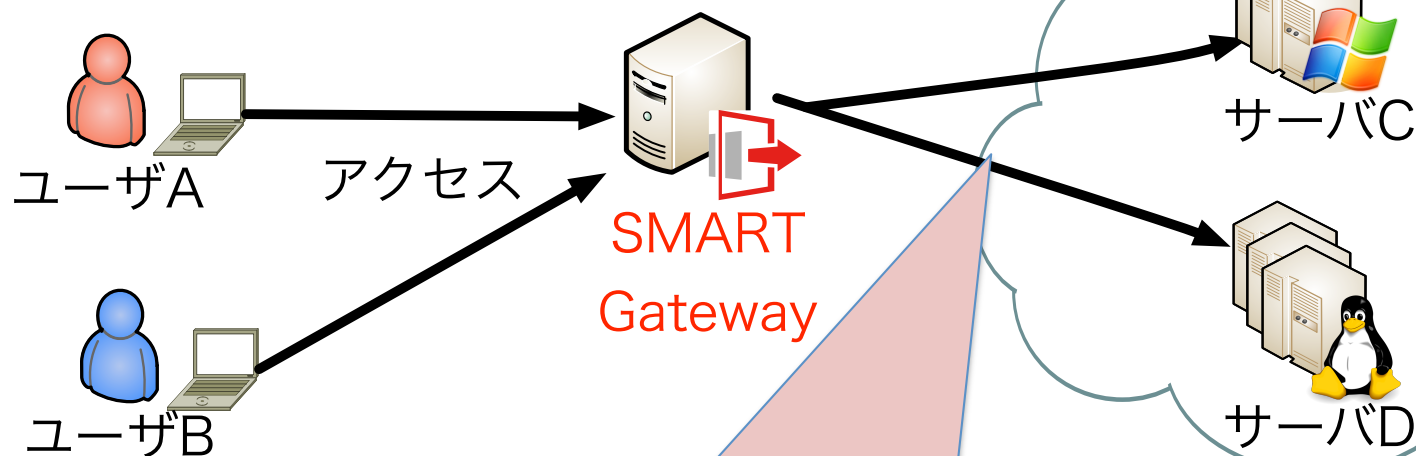
【課題3】

各ユーザ、各サーバ毎に投入
コマンドを制限する事が出来ない

【課題1】

各ユーザ、各サーバ毎の監査
証跡をまとめるコストが大きい

各ユーザが、各サーバで実施した業務が
問題ないことを毎月報告



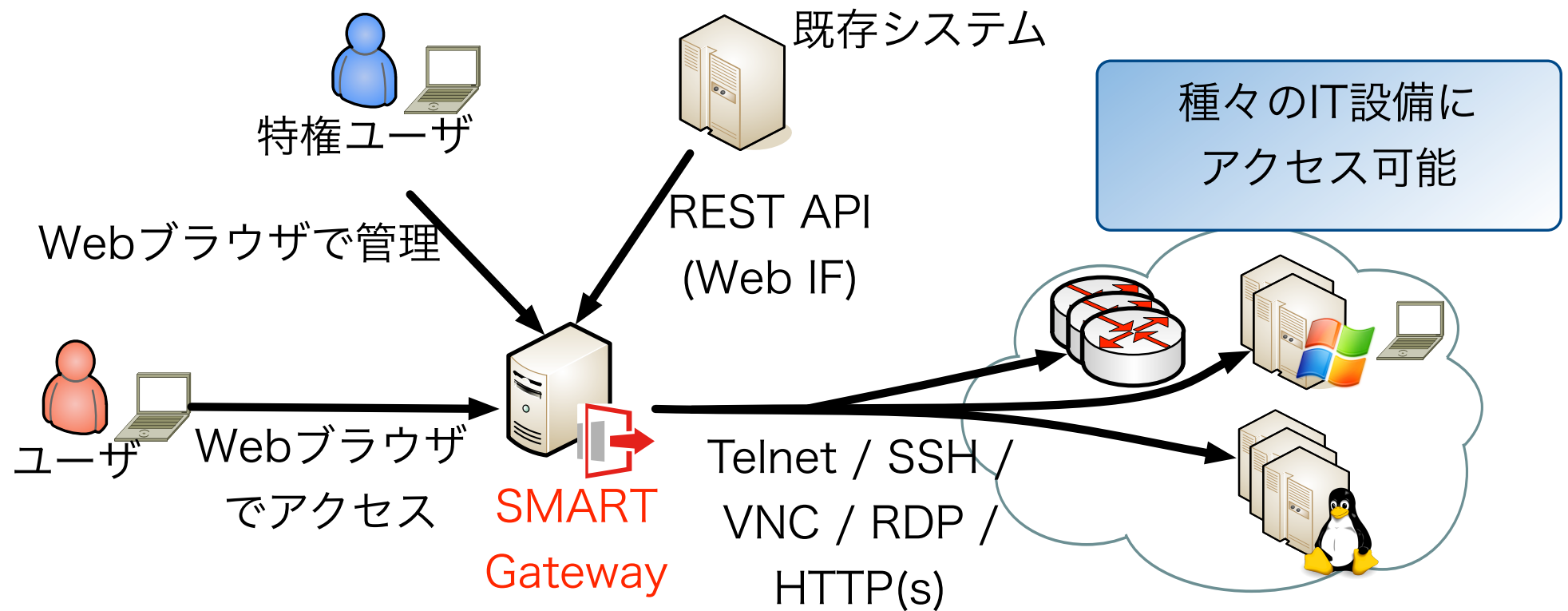
【課題2】

ログインIDやパスワードの使い回し

④ IoT時代のICT管理システムのデモ 【SMART Gatewayのデモ】

SMART Gateway のデモ環境

- 全ての設備はブラウザからアクセス可能
→ Web management of Things (WoT)



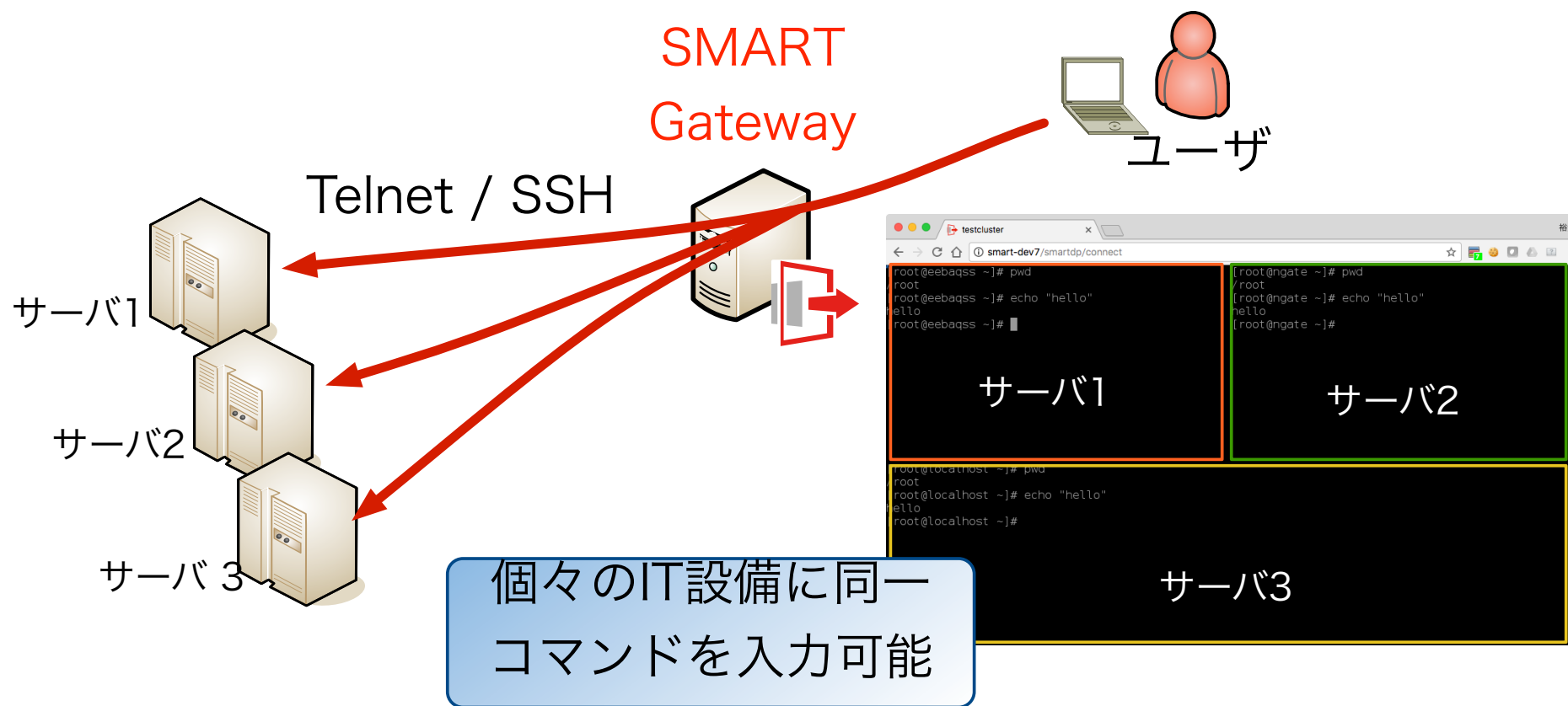
全ての制御はブラウザで

The image shows a web browser window with two tabs. The first tab, titled 'ssh', displays a terminal session with the following commands and output:

```
[root@ngate test]# touch script.sh
[root@ngate test]# chmod +x script.sh
[root@ngate test]# ls
script.sh
[root@ngate test]# pwd
/root/test
[root@ngate test]#
```

The second tab, titled 'Windows7', displays a Windows 7 desktop environment. A purple callout box is overlaid on the desktop with the text 'Windows (RDP) / Webブラウザ'. The desktop features the Windows 7 logo, a taskbar with icons for Start, Internet Explorer, File Explorer, and Google Chrome, and a system tray showing the time as 23:00 on 2017/09/23. The browser's address bar for both tabs shows 'smart-dev7/smartdp/connect'.

同時に複数のサーバを制御可能(1/2)



同時に複数のサーバを制御可能(2/2)

- 【例】ネットワーク状態を俯瞰することが可能、素早く障害機器を特定

```
[root@demo01 ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=63 time=4.83 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=63 time=4.71 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=63 time=4.48 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=63 time=4.82 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=63 time=4.84 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=63 time=4.61 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=63 time=5.75 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=63 time=4.01 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=63 time=3.86 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=63 time=3.83 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=63 time=3.97 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=63 time=3.88 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=63 time=4.24 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=63 time=3.82 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=63 time=4.19 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=63 time=4.08 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=63 time=3.77 ms
64 bytes from 8.8.8.8: icmp_seq=18 ttl=63 time=4.11 ms
```

サーバ1

```
[root@demo02 ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=63 time=3.70 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=63 time=3.79 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=63 time=3.77 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=63 time=4.18 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=63 time=3.57 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=63 time=3.29 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=63 time=5.78 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=63 time=4.95 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=63 time=5.00 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=63 time=4.53 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=63 time=4.68 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=63 time=4.66 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=63 time=3.38 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=63 time=5.12 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=63 time=5.25 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=63 time=5.24 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=63 time=4.90 ms
64 bytes from 8.8.8.8: icmp_seq=18 ttl=63 time=4.21 ms
```

サーバ2

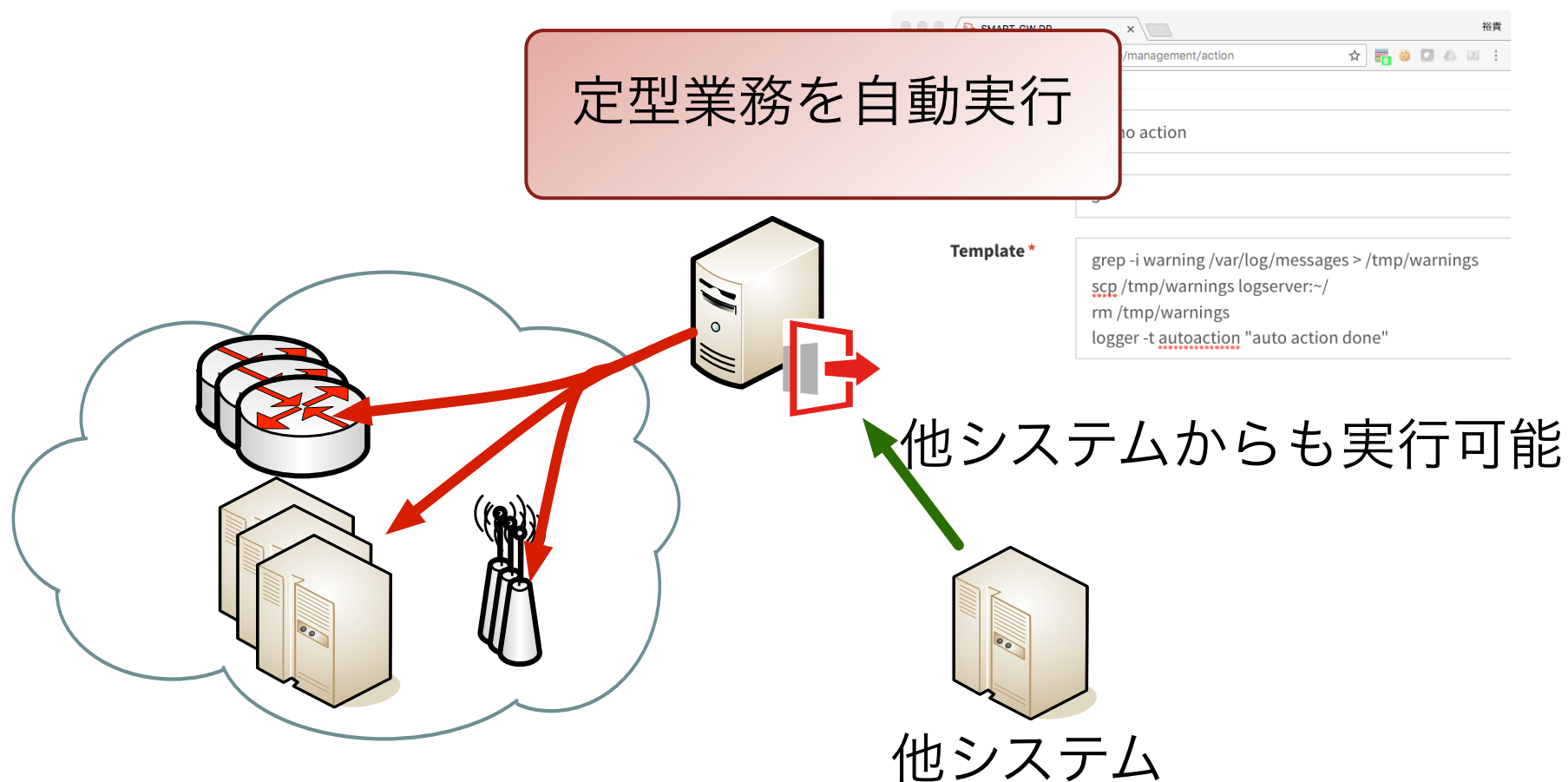
```
[root@demo03 ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=63 time=4.06 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=63 time=4.08 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=63 time=3.75 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=63 time=3.71 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=63 time=3.92 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=63 time=3.95 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=63 time=3.86 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=63 time=4.23 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=63 time=3.94 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=63 time=4.07 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=63 time=4.81 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=63 time=4.58 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=63 time=4.54 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=63 time=4.64 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=63 time=4.63 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=63 time=4.42 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=63 time=4.40 ms
64 bytes from 8.8.8.8: icmp_seq=18 ttl=63 time=5.11 ms
```

サーバ3

```
[root@demo04 ~]# ping 8.8.8.8
connect: Network is unreachable
[root@demo04 ~]#
```

サーバ04
ネットワーク障害有り

定型業務は自動処理(高効率化とミス防止)



全てのコマンド業務を完全再現、分析

- 特権ユーザのコマンド投入業務も制限・管理可能
- 業務の完全把握と、(テキスト)分析が容易！



```
root@uno2:~ — ssh uno2-tsune — 80x24
* updates: ftp.tsukuba.wide.ad.jp
base | 3.7 kB | 00:00
epel | 4.3 kB | 00:00
epel/primary_db | 5.9 MB | 00:00
extras | 3.4 kB | 00:00
updates | 3.4 kB | 00:00
updates/primary_db | 4.2 MB | 00:00
Resolving Dependencies
There are unfinished transactions remaining. You might consider running yum-comp
lete-transaction first to finish them.
--> Running transaction check
---> Package kernel.x86_64 0:2.6.32-696.10.3.el6 will be installed
---> Package kernel-devel.x86_64 0:2.6.32-696.10.3.el6 will be installed
---> Package kernel-firmware.noarch 0:2.6.32-696.10.2.el6 will be updated
---> Package kernel-firmware.noarch 0:2.6.32-696.10.3.el6 will be an update
---> Package kernel-headers.x86_64 0:2.6.32-696.10.2.el6 will be updated
---> Package kernel-headers.x86_64 0:2.6.32-696.10.3.el6 will be an update
---> Package perf.x86_64 0:2.6.32-696.10.2.el6 will be updated
---> Package perf.x86_64 0:2.6.32-696.10.3.el6 will be an update
--> Finished Dependency Resolution
--> Running transaction check
---> Package kernel.x86_64 0:2.6.32-696.3.1.el6 will be erased
---> Package kernel-devel.x86_64 0:2.6.32-696.3.1.el6 will be erased
□
```

パスワード一括自動変更 & 管理画面

Plug-in機能として「パスワード」一括管理機能を追加で組み込むPlug-in機能を提供

SMART DP

MAIN NAVIGATION

メインページ

MANAGEMENT

ユーザ

接続

権限

認証

アクション

パスワード

STATISTICS

セッション

パスワード管理

更新スキーム パスワードポリシー

更新スキーム一覧

更新日時: 2017/10/13 23:26:47

Column visibility Copy Excel CSV

検索:

10 件表示

	Name	Password Policy	Action	Connections
詳細 実行	update scheme	simple policy	auto password update (DO NOT CHANGE THIS)	eeba

1 件中 1 から 1

追加

複数の管理対象のPWとそれに対応するSMART-GWのBEPWを同時に変更

更新履歴一覧

更新日時: 2017/10/13 23:26:46

10 件表示

管理対象のPWと、SMART-GW上で管理しているPWを同時に変更し、履歴管理

Date Time	Update Scheme	Connection	Destination	Password	Update User	Status
2017/10/13 23:17:28	update scheme	eeba	192.168.50.236	testpassword09P@	admin	SUCCESS
2017/10/13 23:15:23	update scheme	eeba	192.168.50.236	fj&D-3"xY(	admin	SUCCESS
2017/10/13 22:23:53	update scheme	eeba	192.168.50.236	test12\$Lzxcv	admin	SUCCESS
2017/10/13 22:22:13	update scheme	eeba	192.168.50.236	'3G/f&u#<3	admin	SUCCESS
2017/10/13 22:10:05	update scheme	eeba	192.168.50.236	sc?>V5\$;	admin	SUCCESS
2017/10/13 22:09:15	update scheme	eeba	192.168.50.236	#X65zbKlgw	admin	FAILURE
2017/10/13 22:03:58	update scheme	eeba	192.168.50.236	asdf	admin	SUCCESS
2017/10/13 22:00:12	update scheme	eeba	192.168.50.236	test	admin	SUCCESS

8 件中 1 から 8 まで表示

前 1 次

実際のデモをご覧ください

