Ansible と NEEDLEWORK による

ネットワーク自動化

[Ansible編]

2019/06/14 Interop Tokyo 2019

セイコーソリューションズ（株）様ブース

株式会社 エーピーコミュニケーションズ

横地 晃

APC
apcommunications

自己紹介

名前	横地 晃
会社	株式会社エーピーコミュニケーションズ （出展ブース 6T08：Security World）
業務	ネットワーク自動化関連の技術開発
コミュニティ	Ansible ユーザー会、JANOG

@akira6592

ブログ（てくなべ）
https://tekunabe.hatenablog.jp

過去発表資料
https://www.slideshare.net/akira6592/

Ansible の概要

自動化ツール Ansible の特徴

シンプル	• プログラミング不要 • 構成定義ファイル（Playbook）を利用
パワフル	• 多数のサーバー、クラウド、**ネットワーク**向けのモジュールを2800以上標準装備 • カスタムモジュールも自作可能
エージェントレス	• 操作対象機器側に専用ソフトはインストール不要

- 構成管理ツールとも呼ばれ、Chef や puppet などと比較されることが多い
- 本資料は Ansible 2.8.0 を前提

Ansible でネットワーク機器にできること

- **接続方式**
  - SSH、NETCONF、HTTP/HTTPS（API）などで接続

- **できることの例**
  - 参照（show）コマンド実行による情報取得
  - 設定コマンド実行による設定追加・変更・削除

Ansible を利用するメリット（ターミナルソフトのマクロとの比較）

1. Ansible の他の機能と連携しやすい

例えば

- コマンド出力結果を copy モジュールに渡して、ファイルに保存
- テンプレート機能を利用して、コンフィグを生成して投入
- 監視サーバーに登録されているホスト情報を接続に利用

2. ログインやモード変更の処理を簡略化できる

- 認証情報を定義しておくだけで自動でログイン、ログアウト
- 設定系モジュールは暗黙的にコンフィグレーションモードへ移行

3. コマンド投入エラーを標準で検出できる

- エラー検出処理はAnsible モジュール内に組み込み済み
- どのようなプロンプトが返ってきたら正常か、という指定が不要

50以上のネットワークプラットフォームに対応

- A10
- Aci
- Aireos
- Aos
- Aruba
- Asa
- Avi
- Bigswitch
- Checkpoint
- Cloudengine
- Cloudvision
- Cnos
- Cumulus
- Dellos10
- Dellos6
- Dellos9
- Edgeos
- Edgeswitch
- Enos
- Eos
- Exos
- F5
- Fortimanager
- Fortios
- Frr
- Ftd
- Illumos
- Ingate
- Ios
- Iosxr
- Ironware
- Itential
- Junos
- Meraki
- Netact
- Netconf
- Netscaler
- Netvisor
- Nos
- Nso
- Nuage
- Nxos
- Onyx
- Opx
- Ordnance
- Ovs
- Panos
- Radware
- Restconf
- Routeros
- Skydive
- Slxos
- Sros
- Voss
- Vyos

ネットワークモジュール一覧 https://docs.ansible.com/ansible/latest/modules/list_of_network_modules.html

サンプル1:
コンフィグバックアップ

サンプル1: コンフィグバックアップ（準備）

```
- hosts: fw
  gather_facts: no

  tasks:
    - name: show command test
      junos_command:
        commands:
          - show configuration
      register: result

    - name: save config to file
      copy:
        content: "{{ result.stdout[0] }}"
        dest: "show_config_{{ inventory_hostname }}.txt"
```

対象ホストグループ

実行したい show コマンド
（変更すれば他のshowコマンドでも対応可）

保存先ファイル名

※このほか、対象ホストの接続情報や、認証情報を定義するファイルを用意する

サンプル1: コンフィグバックアップ（実行）

Ansible 側

ansible-playbook コマンドを実行

```
$ ansible-playbook -i inventory show01.yml

PLAY [fw] **********************************************************************

TASK [show command test] *******************************************************

ok: [172.16.0.1]

TASK [save config to file] ***                                  ****************

changed: [172.16.0.1]

PLAY RECAP *********************************************************************
172.16.0.1         : ok=2    changed=1    unreachable=0    failed=0   skipped=0    rescued=0    ignored=0
```

コンフィグがファイルとして
新たに保存された旨のログ

サンプル2:
設定変更

サンプル2: 設定変更（準備）

```
- hosts: fw
  gather_facts: no

  tasks:
    - name: config test
      junos_config:
        lines:
          - set system ntp server 10.0.0.123
```

対象ホストグループ

実行したい設定コマンド
（変更すれば他の設定コマンドでも対応可）

※このほか、対象ホストの接続情報や、認証情報を定義するファイルを用意する

サンプル2: 設定変更（実行）

Ansible 側

ansible-playbook コマンドを実行

```
$ ansible-playbook -i inventory set01.yml

PLAY [fw] **********************************************************************

TASK [config test] *************************************************************
changed: [172.16.0.1]

PLAY RECAP *********************************************************************
172.16.0.1         : ok=1    changed=1    unreachable=0    failed=0   skipped=0    rescued=0    ignored=0
```

設定変更された旨のログ

ネットワーク機器側

```
root@vsrx1> show configuration system ntp | display set
set system ntp server 10.0.0.123
```

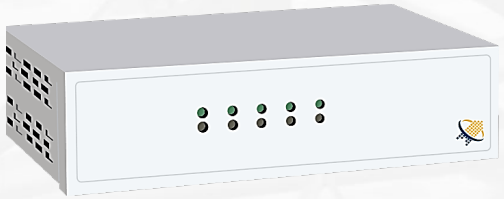
設定変更された

ところで、
こんな時はどうする？

こんな時には

- **IP到達性のない機器に Ansible を使うには？**
  - Ansible にも対応したコンソールサーバー「SmartCS」で
  - 詳細はセイコーソリューションズ様ブース（ココ）

- **テストを自動化するには？**
  - ネットワークテスト自動化にも対応した「NEEDLEWORK」
  - 詳細はこのあとのセッション後半で



まとめ

まとめ

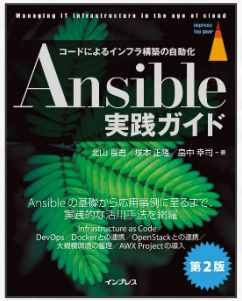
- **はじめやすい自動化ツール**
  - シンプル、パワフル、エージェントレス
- **50以上のネットワークプラットフォームに対応**
  - 参照や設定などができる
- **マクロにはないメリットも**
  - Ansible の他機能との連携
  - ログイン/ログアウトの簡略化
  - 組み込みのエラー検出、など

参考情報

- 公式ドキュメント
  - トップ https://docs.ansible.com/
  - Getting Started https://docs.ansible.com/ansible/latest/user_guide/intro_getting_started.html

- ブラウザだけで独習できる日本語コース
  - Ansible 101 by irixjp | Katacoda https://www.katacoda.com/irixjp/scenarios/ansible-101

- 書籍
  - Ansible実践ガイド 第2版
  - Ansible徹底入門



AnsibleとNEEDLEWORKによる
ネットワーク自動化

NEEDLEWORK

2019/06/14 @Interop セイコーソリューションズ（株）様ブース

（株）エーピーコミュニケーションズ
先進サービス開発事業部　國森　修

自己紹介

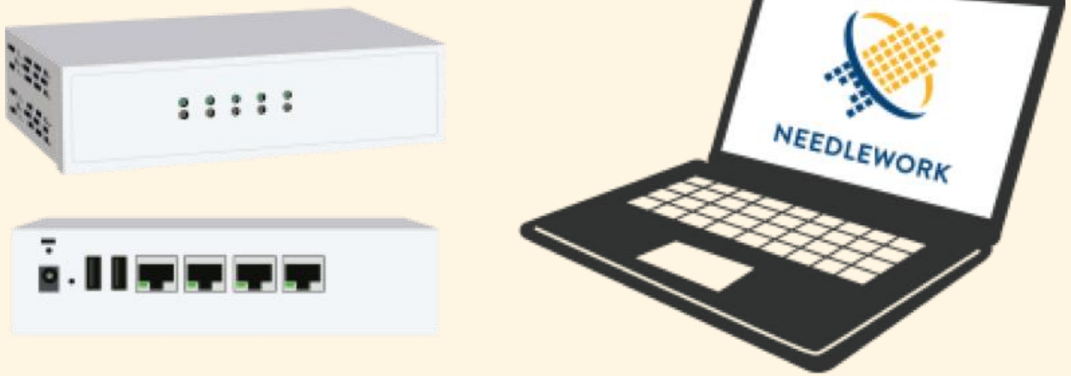
- 國森　修／Shu Kunimori

- 株式会社エーピーコミュニケーションズ
  ー 先進サービス開発事業部

- 現在は事業責任者
  ー ネットワーク／サーバ基盤エンジニア　12年
    ー 新規事業開発　3年

NEEDLEWORK（ニードルワーク）とは？

InteropTokyo Best of Show Award
［ セキュリティ部門 ］
ファイナリストにノミネートされました



NEEDLEWORKは2つのテスト作業を自動化できるアプライアンスです。

1. ファイアウォールのポリシーテスト作業を自動化します。
2. ネットワークの通信テスト作業を自動化します。

解決したい課題

●一般的な案件／作業パターン

時間軸 → 設計 → 構築 → テスト → 納品導入 → 運用

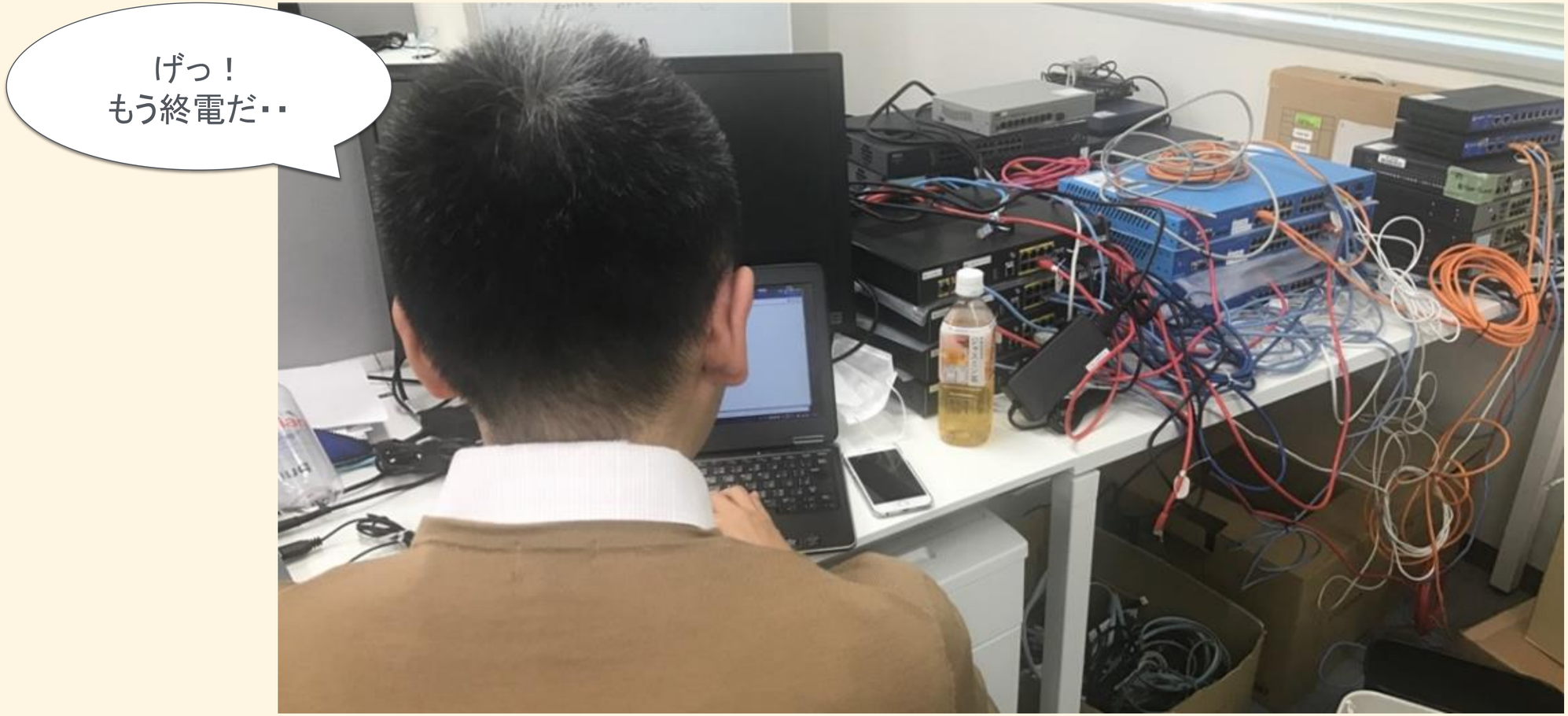
●炎上案件／作業のパターン

犠牲者多発

時間軸 → 設計（お客様／上長承認待ち） → 構築 → テ → 納品導入 → 運用

まぁまぁ決まらない設計／まぁまぁ時間のかかる承認

解決したい課題



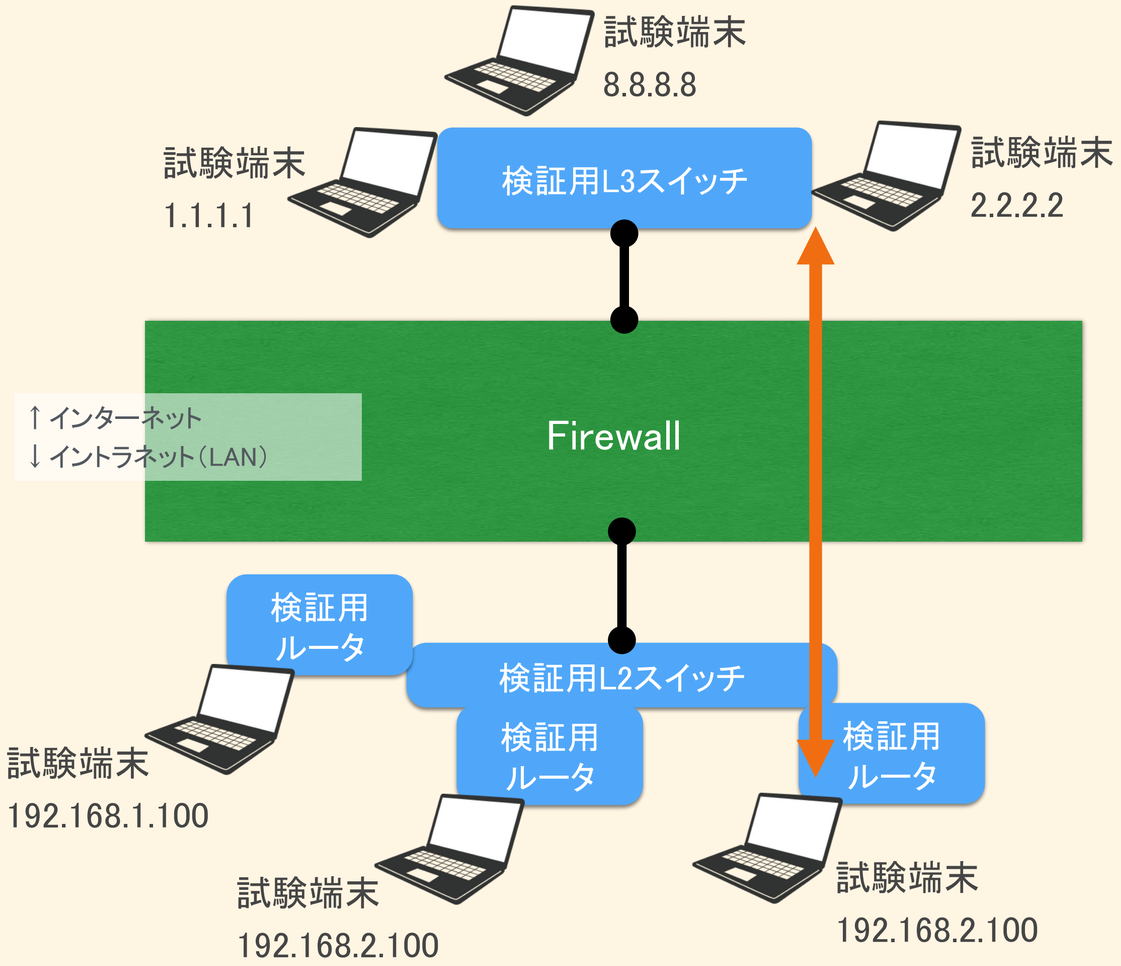
エンジニア早期帰宅の具体的な手段

NEEDLEWORK
FWポリシーテスト機能

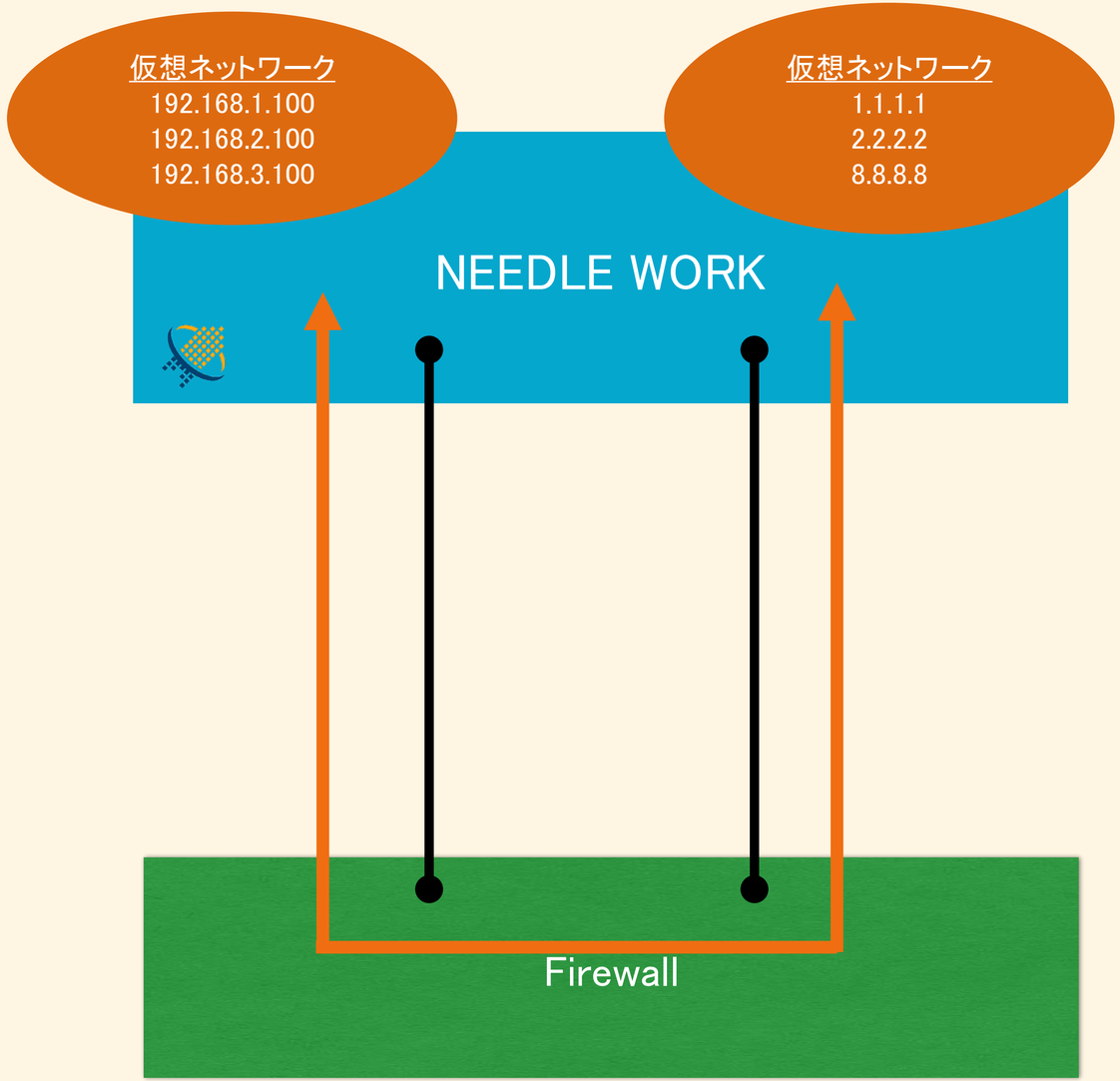
できることその１（機材が削減できます）

【従来のテスト構成】

多数の機材の調達、環境構築が必要



【NEEDLEWORKを使用したテスト構成】



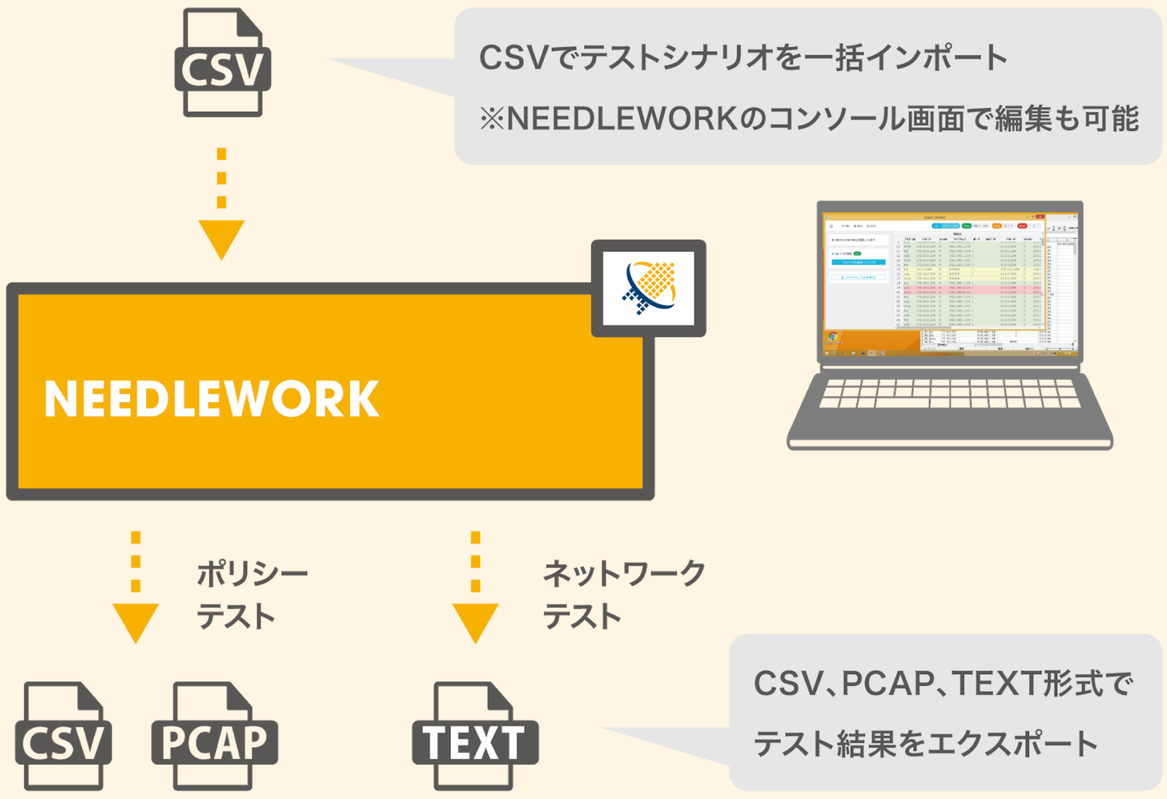
できることその2（ポリシーテストが超簡単）

1. FWとNEEDLEWORKを接続

2. 試験内容を定義したCSV（テストシナリオ）をインポート
   - ・送信元IP、宛先IP
   - ・通信の方向（ex. Trust -> Untrust）
   - ・プロトコル、ポート番号

3. ワンクリックで通信試験を実行

4. 試験結果をエクスポート（CSV）



できることその3（シンプルな試験方法）

プロトコル	アプリケーション	試験方法	備考
ICMP	–	ICMP Echo-Request / Replyによる疎通確認	
TCP	–	3ウェイハンドシェイク＋FINによる疎通確認	※3ウェイハンドシェイク確立後、 ダミーデータを宛先⇔送信元間で送受信します
	HTTP	HTTP GETによるコンテンツ取得	※AntiVirusテストの場合はTestVirus（Eicar）をGETします
	DNS	DNSパケットによる名前解決確認	※指定したドメインの名前解決を行います
UDP	–	UDPパケットの往復による疎通確認	※ダミーデータを宛先⇔送信元間で送受信します
	DNS	DNSパケットによる名前解決確認	※指定したドメインの名前解決を行います

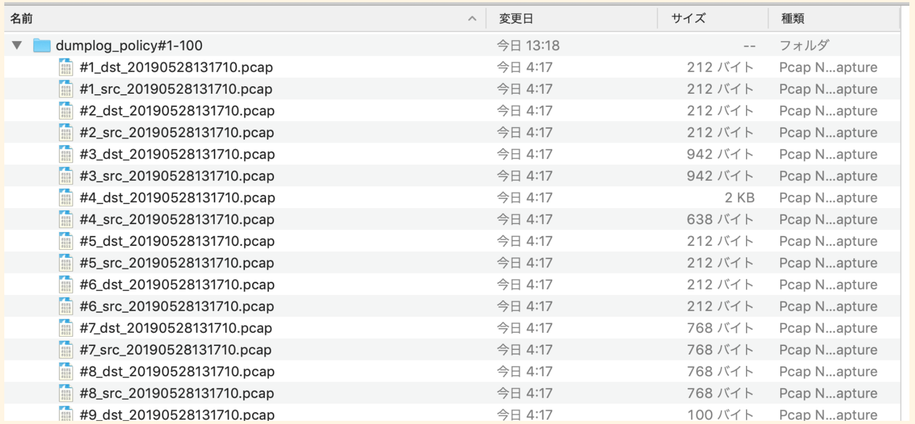
※HTTP、DNS以外はL3/L4レベル（TCP/IP）の試験となります

弊社テスト実績は以下の通り
- Cisco Systems ASA（＊）
- Juniper Networks SRX（＊）/ SSG / ISG
- Palo Alto Networks 次世代ファイアウォール（＊）
- Fortinet FortiGate（＊）
- Check Point Software Technologies Check Point（＊）

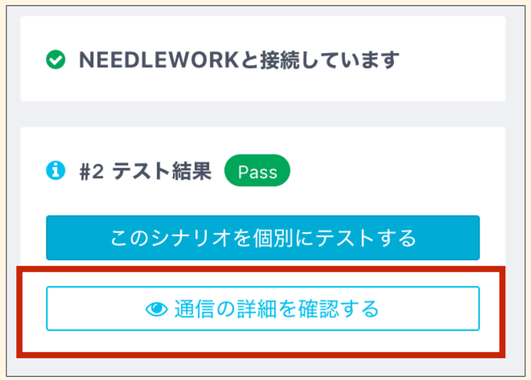
＊：UTM機能（URLフィルタリング、アンチウィルス）のテスト実績があるFW

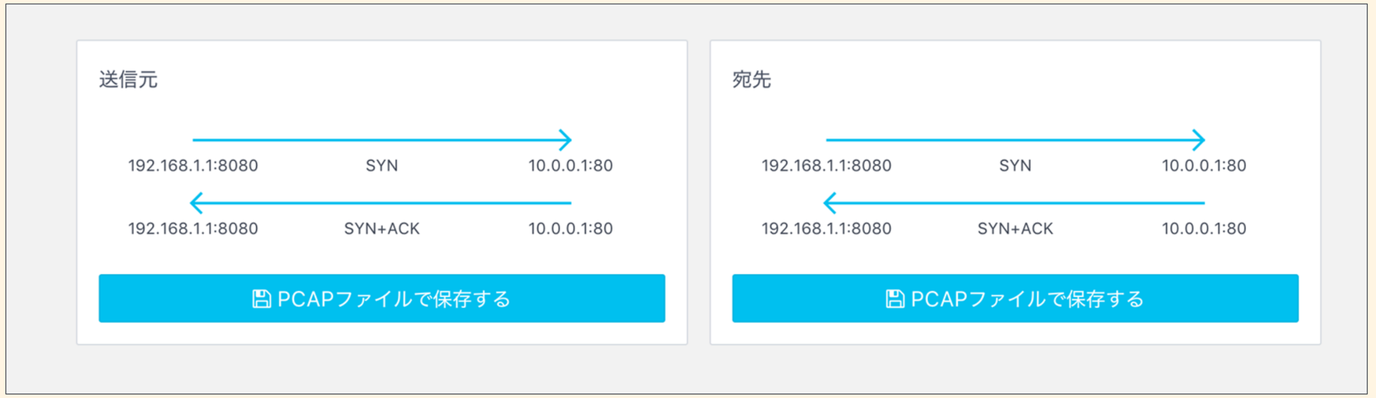
できることその4（エビデンス整理が超簡単）

試験時のパケットキャプチャデータをPCAPで一括ダウンロード可能です。
（PCAP形式）



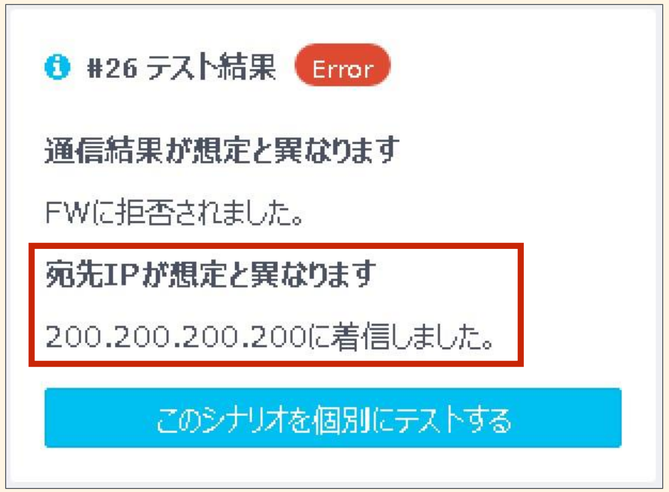
通信詳細を確認することも可能で、パケットのフローを追ってデバッグに活用いただけます。



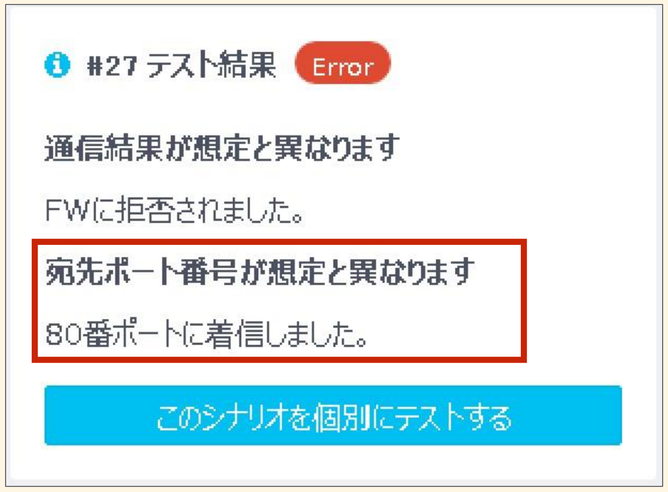


できること　その他（NAT/NAPT確認機能）

シナリオ記載の情報と異なる宛先IPアドレス、ポート番号に転送された場合に、
エラーとして表示されます。



ファイアウォールで宛先NATされ、
シナリオと異なるIPアドレスに転送された場合に、
エラーとして実際に転送されたIPアドレスを表示します。



ファイアウォールで宛先NATされ、
シナリオと異なるポート番号に転送された場合に、
エラーとして実際に転送されたポート番号を表示します。

できること　その他（UTMテスト機能）

以下のUTM機能のテストが可能です。

・URLフィルタ

シナリオに記載したURLを、宛先からHTTPでGETします。
ファイアウォールの挙動に応じて、PassかBlockで結果を表示します。

・アンチウィルス

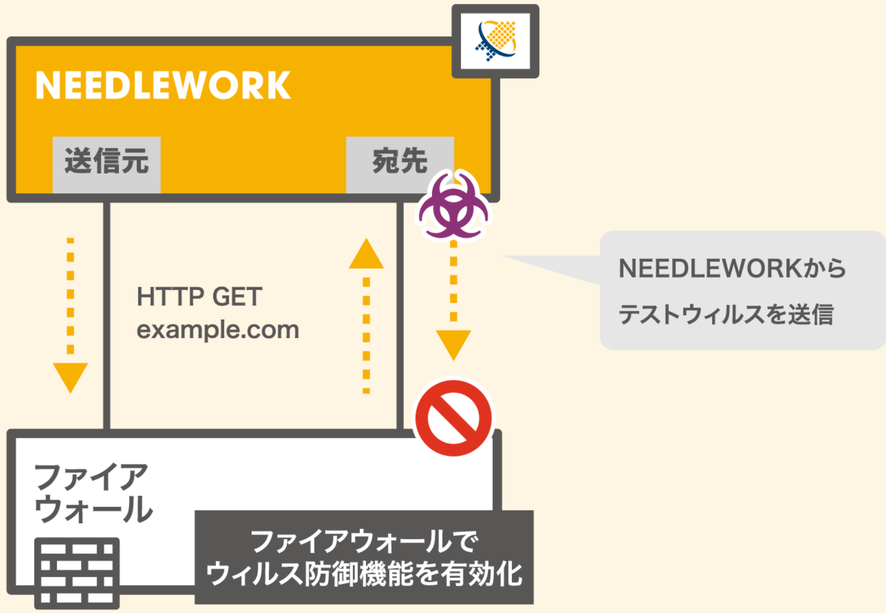
テストウィルス（Eicar）を、宛先からHTTPでGETします。
ファイアウォールの挙動に応じて、PassかBlockで結果を表示します。

・スパイウェア

DNSプロトコルでのテスト時に、
名前解決を行うドメインを自由に指定することが可能です。
マルウェアサイトのドメイン等、ファイアウォールのアンチスパイウェア機能で
ブロック想定のドメイン名を指定することで、アンチスパイウェア機能の確認が可能です。

UTM	
URL / ドメイン	アンチウイルス
www.ap-com.co.jp	
www.ap-com.co.jp	enable

【テストシナリオのURL/ドメイン指定イメージ】

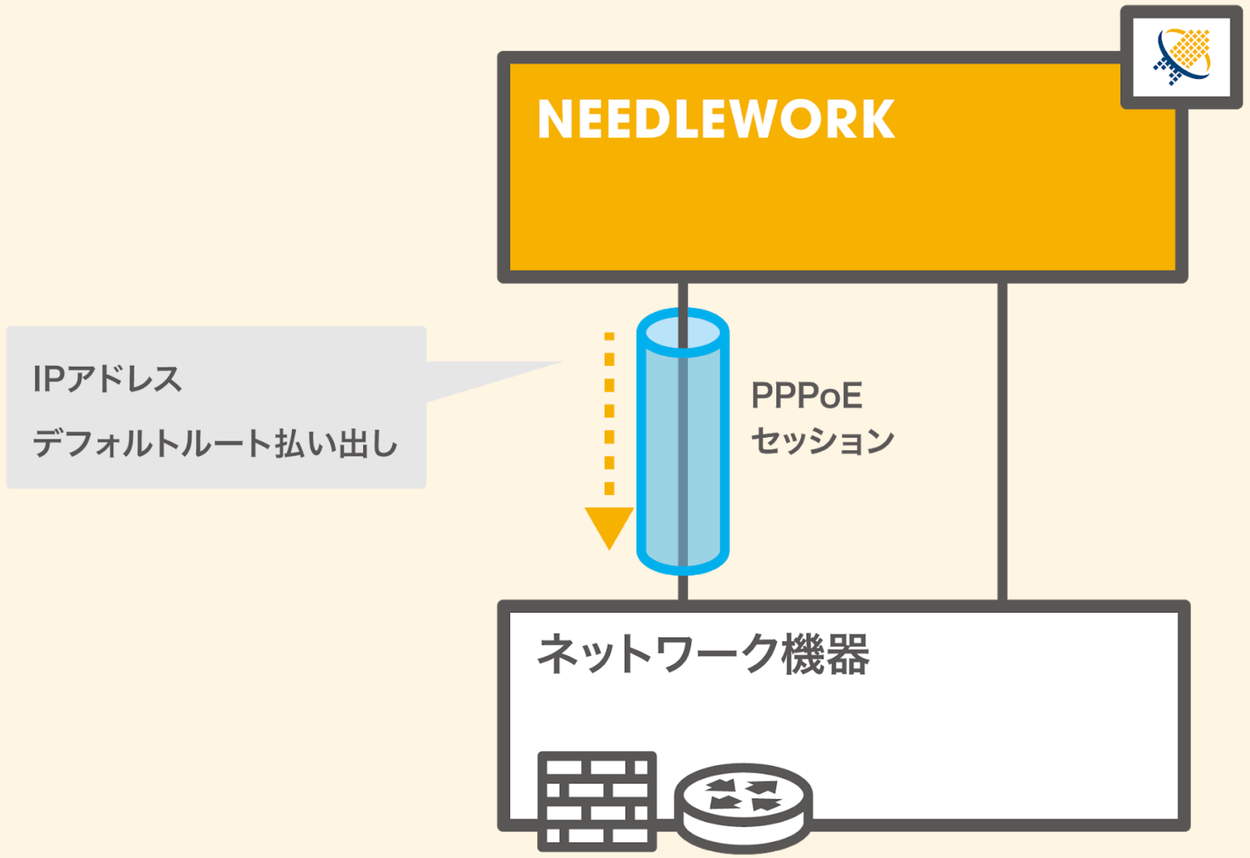


タイプ	名前	宛先ポート	アプリケーション	アクション	重大度
spyware	generic:www.modulepush.com	53	dns	reset-both	medium
spyware	generic:www.modulepush.com	53	dns	reset-both	medium
spyware	generic:www.modulepush.com	53	dns	reset-both	medium

【Palo Alto次世代ファイアウォールのスパイウェア検知イメージ】

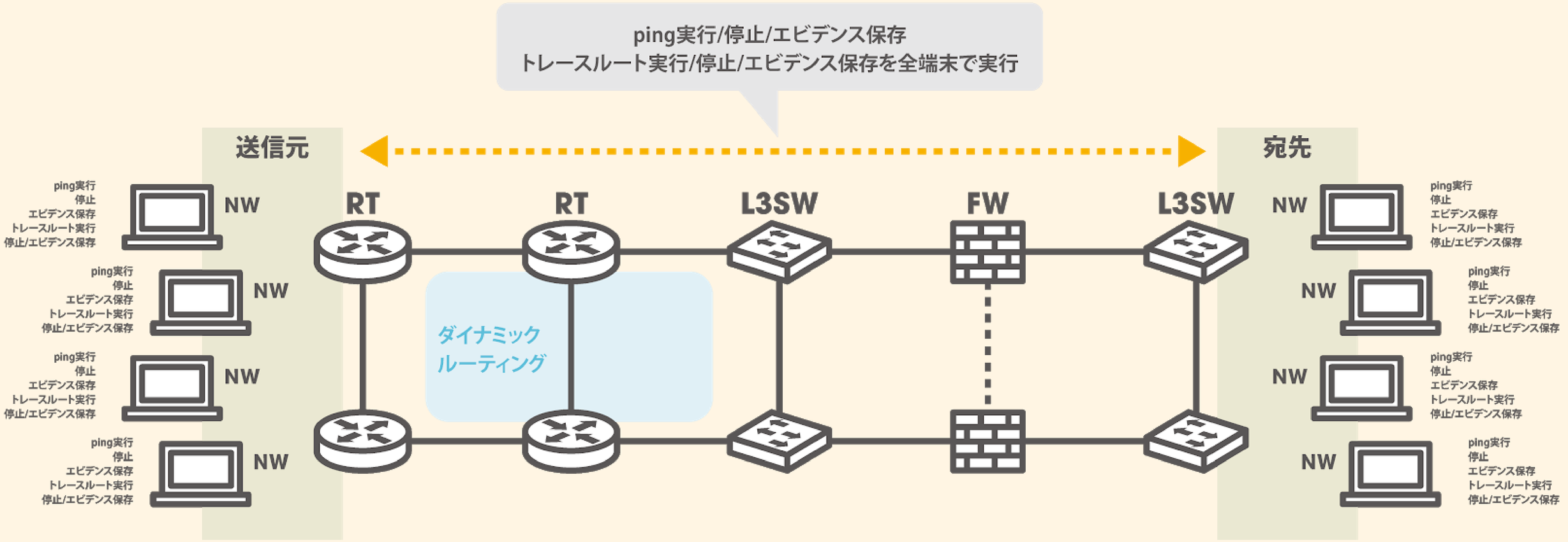
できること　その他（PPPoEサーバ機能）

NEEDLEWORKがPPPoEサーバとなり、
指定のIPアドレス、デフォルトルートをテスト対象機器に払い出すことが可能です。

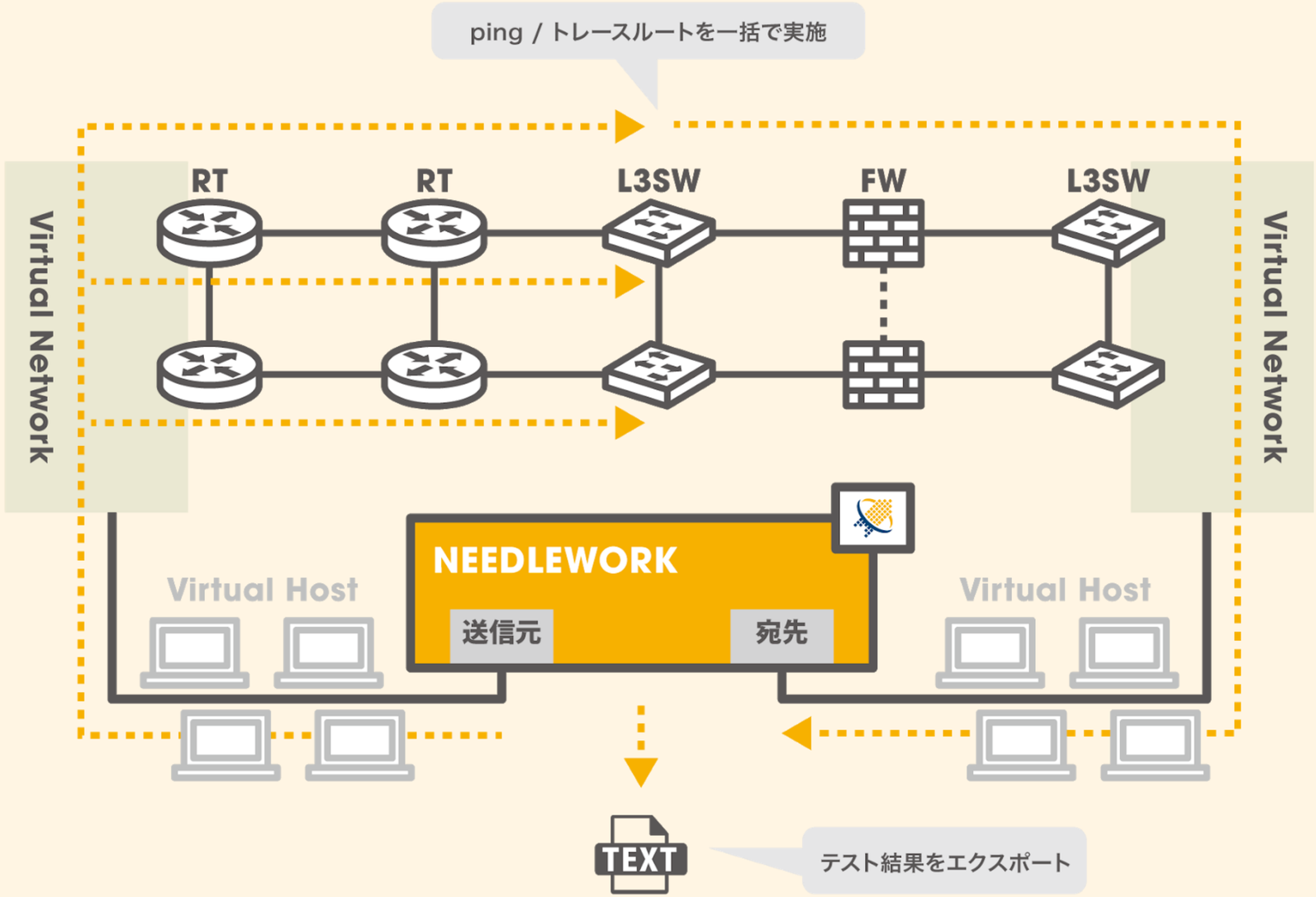


NEEDLEWORK
ネットワークテスト機能
（2019年6月下旬正式リリース予定）

ネットワークテストの構成（従来）



ネットワークテストの構成（NEEDLEWORK）



ネットワークテスト作業が超簡単に

①事前経路確認（トレースルート）

1. 全端末でトレースルート実行
2. 完了後に全端末でトレースルート結果を保存

②Ping送信（並列で送信）

1. 全端末でPing実行

③テスト実施（障害試験）

1. テスト実施後に全端末でPing停止
2. 全端末でPing結果を保存

④事後経路確認（トレースルート）

1. 全端末でトレースルート実行
2. 完了後に全端末でトレースルート結果を保存

①試験シナリオ作成

1. 事前トレースルートの有無を記載
2. Ping送信対象の記載
3. 事後トレースルートの有無を記載

②試験実行/停止

1. 実行ボタンをクリック
2. 障害発生オペレーション
3. 停止ボタンをクリック
4. 保存されたエビデンスを一括ダウンロード

半分以下に短縮

ネットワークテスト機能導入による削減効果

・SI案件（弊社の実績）
10,000千円　2案件
8,000千円　2案件
5,000千円　3案件
3,000千円　5案件
1,000千円 30案件

・フェーズ毎の工数割合
設計 40%
構築 10%
試験 30%
導入 20%

・適用案件の試験工程を50%削減できた場合の試算
10,000千円　2案件 x 30% x 50%=　3,000千円
8,000千円　2案件 x 30% x 50%=　2,400千円
5,000千円　3案件 x 30% x 50%=　2,250千円
3,000千円　5案件 x 30% x 50%=　2,250千円
1,000千円　30案件 x 30% x 50%=　4,500千円

Total　14,400千円

SI売上1億円規模で
1年　1,440万円
5年　7,200万円
削減できます。

導入実績のご紹介

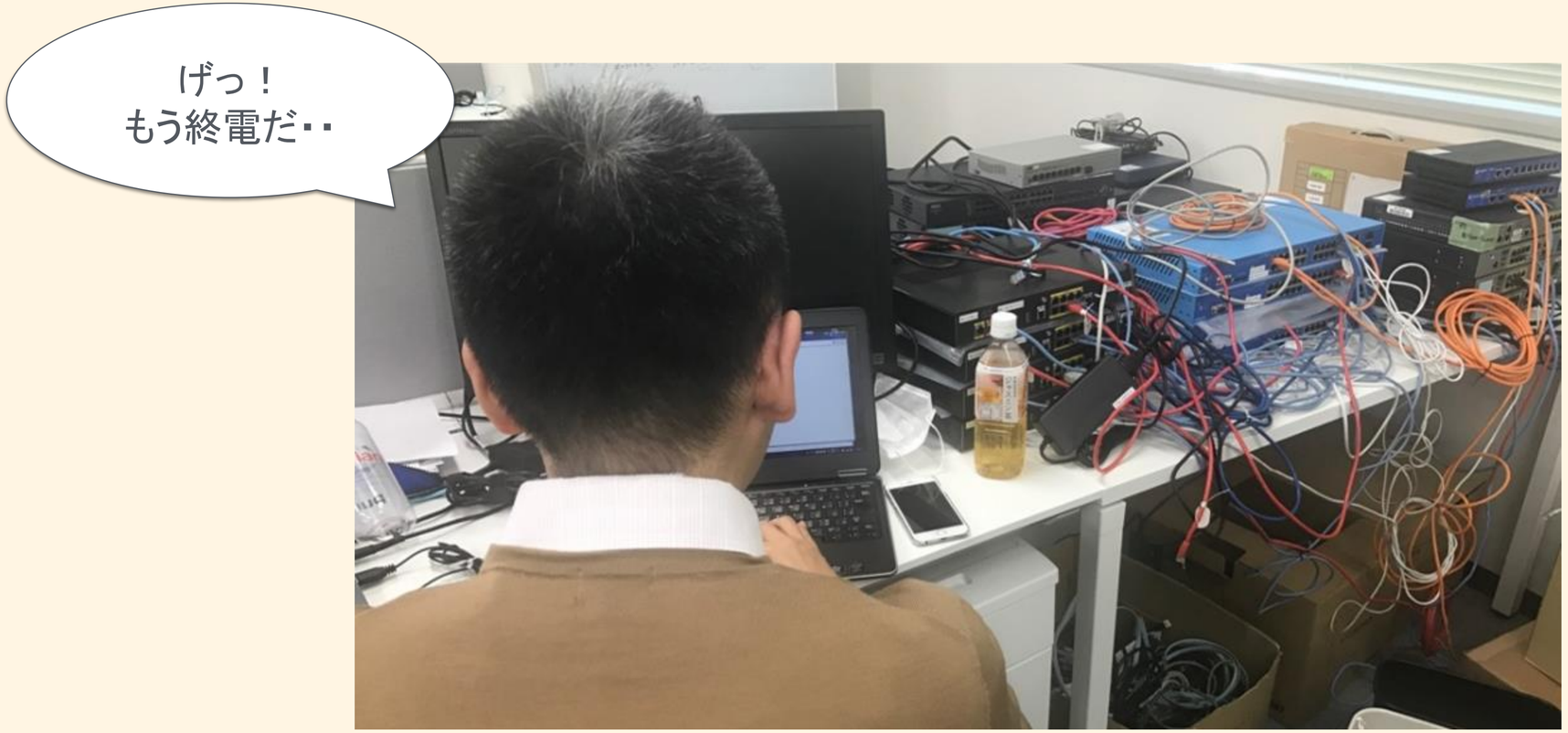
導入企業様

正式販売開始から約2年

導入済：29社
商談中：60社

NEEDLEWORKサービスサイト　ユーザ事例
https://www.ap-com.co.jp/ja/needlework/index.html#casestudy

解決したい課題

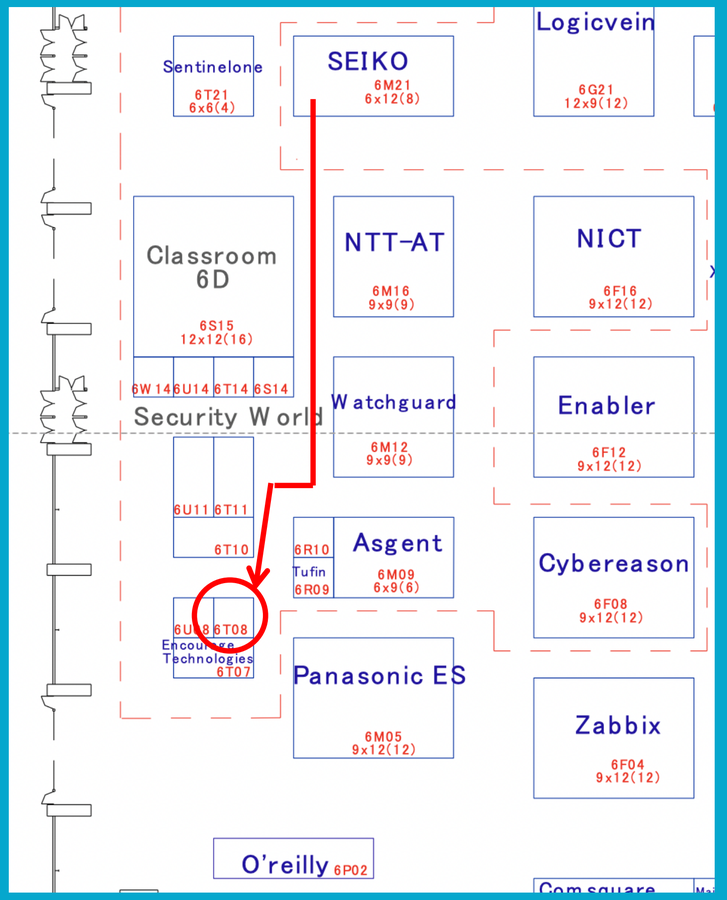


エンジニア早期帰宅の具体的な手段

弊社ブースにて詳しいご説明を行っております。残り時間少ないですがご興味がございましたら弊社ブースへお越しください。

・デモ
・活用事例
・価格
・今後のロードマップ

ご静聴ありがとうございました。



NEEDLEWORK