



イチから体験!

NGINX ハンズオントレーニング

～ NGINX App Protect WAF編 ～

東京エレクトロン デバイス株式会社

2025年4月24日

※本資料に掲載されている会社名・製品・サービス名・ロゴは各社の商標または登録商標です。
また、写真・ロゴマーク・その他の著作物に関する著作権はそれぞれの権利を有する各社に帰属します。

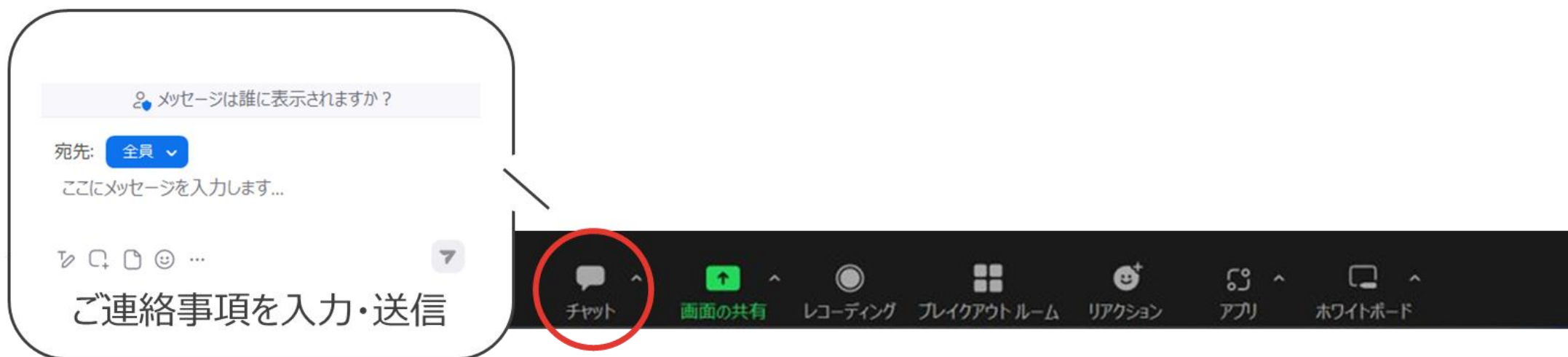


セミナーについて

配信中のご質問・ご連絡について

Webinar画面

【配信・運営やセッション内容のご質問】
「チャット」よりご連絡ください。



今後のより充実したセミナー開催のため アンケートへのご協力をお願いいたします。

配布資料は、セミナー終了後 お送りするメールにてご案内いたします。





イチから体験!

NGINX ハンズオントレーニング

～ NGINX App Protect WAF編 ～

東京エレクトロン デバイス株式会社

2025年4月24日

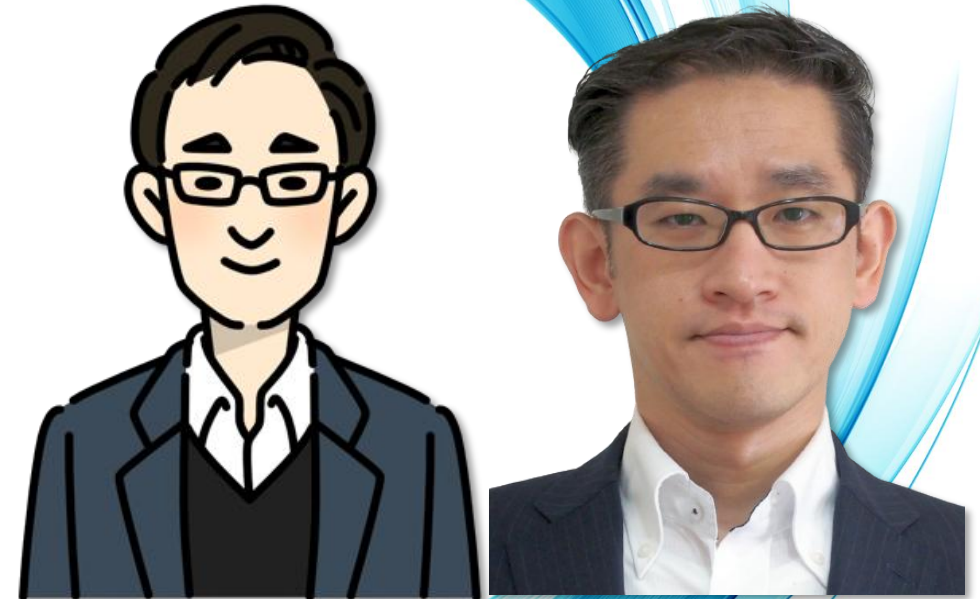
※本資料に掲載されている会社名・製品・サービス名・ロゴは各社の商標または登録商標です。
また、写真・ロゴマーク・その他の著作物に関する著作権はそれぞれの権利を有する各社に帰属します。



自己紹介

本日の講師：長岡 圭一

- 東京エレクトロン デバイス株式会社
 - CN BU プロダクト第一技術部
 - F5製品のサポートエンジニア 
 - 主な担当は F5 NGINX 
- F5製品以外にもXMLセキュリティ・メールセキュリティ・データセキュリティといった製品にも携わってきました
- Pythonを駆使して業務の自動化・効率化にも取り組んでいます
- 弊社TED-CNブログにて NGINXに関する技術情報を発信しています
 - URL → <https://cn.teldevice.co.jp/blog/>



東京エレクトロンデバイスについて

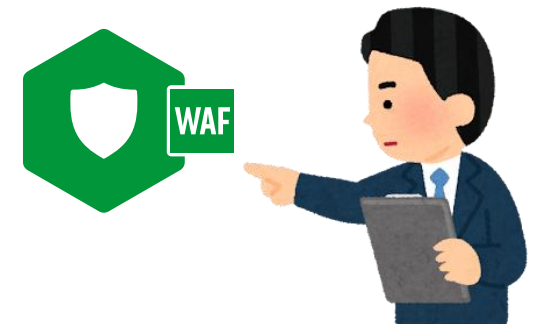
- F5の日本法人が出来る前からの代理店 (1999年～)
- 幅広い取り扱いラインナップ
 - **F5 BIG-IP**
 - **F5 NGINX**
 - **F5 Distributed Cloud Services (F5 XC)**
- F5国内販売額 9年連続No.1の一次代理店 (2023年度実績)
- 自社検証環境を利用した技術支援(デモ/ハンズオンのご提供)
- 保守契約ユーザー向けの会員制サイト(FAQ/ドキュメント等)
- F5製品の重要情報をPush型でメール配信(脆弱性、既知の重大不具合及び改修情報、リリース情報等)



- ハンズオン環境の準備
- NGINX App Protect WAFについて
- ハンズオン
 1. シンプルなWAFの設定
 2. 通信のブロック
 3. 特定Signatureの除外設定
 4. Custom Blocking Page
 5. Sensitive Parameter
 6. 特定パラメータの制御
 7. Bot Clientの確認
 8. IPアドレスによる制御

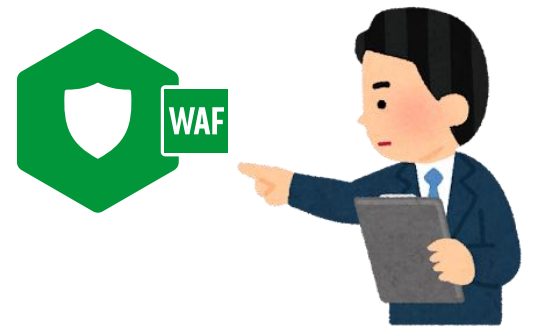
- NGINX One のご紹介

- 時間の都合により、上記のできるところまで実施とさせていただきます。ご了承くださいませようお願い申し上げます。



本日のゴール

1. WAFを用いて外部からの悪意あるリクエストを検知・拒否する方法を理解する
2. NGINXの WAFモジュールの設定 について理解する





ハンズオン環境の準備

ハンズオン環境の準備：ハンズオンガイドURLのご案内

- ハンズオンガイド：

- F5 Labs - Index — NGINX Plus Lab Security documentation

<https://f5j-nginx-plus-lab2-security.readthedocs.io/en/latest/>

Zoomのチャット
にて、本URLを
貼ります。

🏠 NGINX Plus Lab Security
latest

Search docs

LAB CONTENTS:

- 環境
- NGINX LAB
- NGINX App Protect WAF (NAP WAF)
- NGINX App Protect Dos (NAP Dos)
- (参考) バックエンドのアプリケーション&ELKのデプロイ手順

▶ Version 3.1
✓ PR #379
✗ PR #378

📖 Read the Docs v: latest ▼

🏠 / F5 Labs - Index Edit on GitHub

F5 Labs - Index

ようこそ！

ようこそ！ NGINX Labへ！
実際にNGINXを触って試していただくための手順をまとめています。
ラボ環境にアクセス可能な方は手順に従って操作をしてください。
事前に資料をご覧になりたい方は座学資料を御覧ください。

座学資料

このラボはNGINX Plusのインストールから各種設定を行っていただけます。

NGINX Plusの基本的な動作や仕様について紹介しております。

ハンズオン環境の準備：ハンズオン環境の起動

- UDF (Unified Demonstration Framework) コンポーネントへの接続準備

招待されているトレーニング・セッションを選択して、“LAUNCH”をクリック

The screenshot shows the UDF interface. On the left, under 'COURSE SESSIONS', there is a table with the following data:

Date & Time	Course	Location	Instructors
Fri 01 May 3:00 PM - 5:00 PM JST Duration: 2 hours	BIG-IP LTM hands-on in Tokyo	https://f5networks.zoom.us/j/6126548210	Tetsuya TSUJI

Below the table, there are buttons for 'UNREGISTER' and 'LAUNCH'. The 'LAUNCH' button is circled in blue. A blue arrow points from this button to the 'Join' button in the lobby on the right.

The lobby on the right is titled 'BIG-IP LTM hands-on in Tokyo' and shows the session duration 'Ends in 2 hours' and the same Zoom link. The 'Join' button is circled in blue. A blue arrow points from the text 'Joinをクリック' to this button.

Below the 'Join' button, there is a 'Course Overview' section and an 'Instructors' section listing Tetsuya TSUJI as F5, Solutions Engineer III.

ハンズオン環境の準備：ハンズオン環境の起動（２）

- 左上にある「 DEPLOYMENT 」をクリック

The screenshot shows a web interface for managing a deployment. At the top, there are tabs for 'DOCUMENTATION' and 'DEPLOYMENT', with 'DEPLOYMENT' being the active tab. On the left, a sidebar indicates 'Ends in 11 hours' and a 'Leave Session' button. The main content area is titled 'Your Deployment' and features a green play button icon. Below this, there are three sections: 'F5 Products', 'Subnets', and 'Systems'. The 'Subnets' section shows a 'Management' subnet with IP 10.1.1.0/24 and a 'DETAILS' link. The 'Systems' section lists five systems: 'docker_host' (CentOS 7), 'ubuntu_web' (Ubuntu 20.04 LTS), 'ubuntu01' (Ubuntu 20.04 LTS), 'ubuntu02' (Ubuntu 20.04 LTS), and 'Windows2019_JumpBox' (Windows Server 2019 Base). Each system has 'ACCESS' and 'DETAILS' links. A blue-bordered box in the lower-left corner contains a legend: a green play button icon followed by ': システムの起動が完了した' and a refresh icon followed by ': デプロイ中'.

DOCUMENTATION DEPLOYMENT

Ends in 11 hours
Leave Session

Your Deployment

F5 Products

Subnets

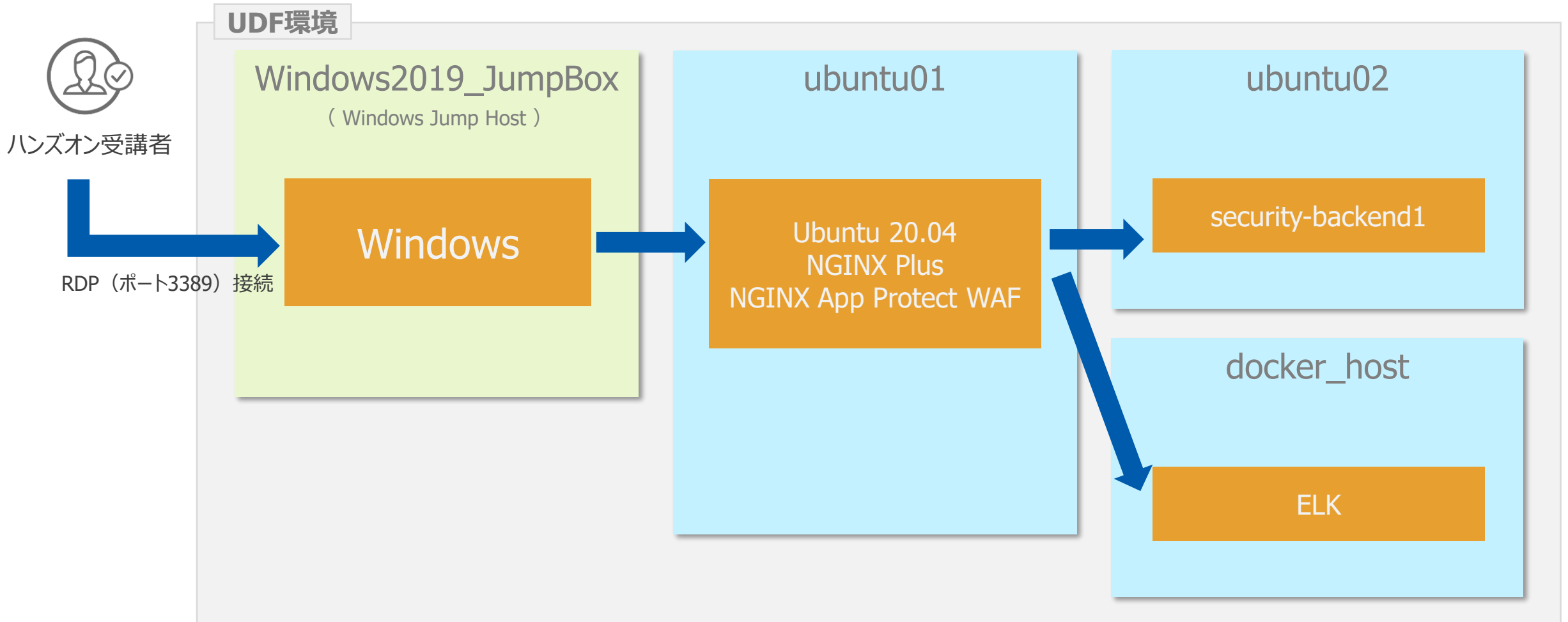
- Management 10.1.1.0/24
DETAILS

Systems

- docker_host CentOS 7
ACCESS DETAILS
- ubuntu_web Ubuntu 20.04 LTS
ACCESS DETAILS
- ubuntu01 Ubuntu 20.04 LTS
ACCESS DETAILS
- ubuntu02 Ubuntu 20.04 LTS
ACCESS DETAILS
- Windows2019_JumpBox Windows Server 2019 Base
ACCESS DETAILS

▶ : システムの起動が完了した
🔄 : デプロイ中

ハンズオン環境の準備 : ハンズオン環境について



ハンズオン環境の準備 : ハンズオン環境にRDP接続

ubuntu01
Ubuntu 20.04 LTS

ubuntu02
Ubuntu 20.04 LTS

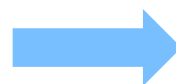
Windows2019
Windows Server 2019

RDP

1920x1080
1600x1200
1440x900
1366x768
1280x1024
1280x800
800x600
640x480

ACCESS DETAILS

Window2019_JumpBox の「 ACCESS 」をクリック



Windows セキュリティ

資格情報を入力してください

これらの資格情報は、
6f0242f2-00c8-41e5-9dac-5852dd453ffe.access.udf.f5.com への接
続に使用されます。

user

●●●●

ドメイン:
パスワードのリセット/ロック解除

☐ このアカウントを記憶する

その他

Administrator
65-60769¥Administrator

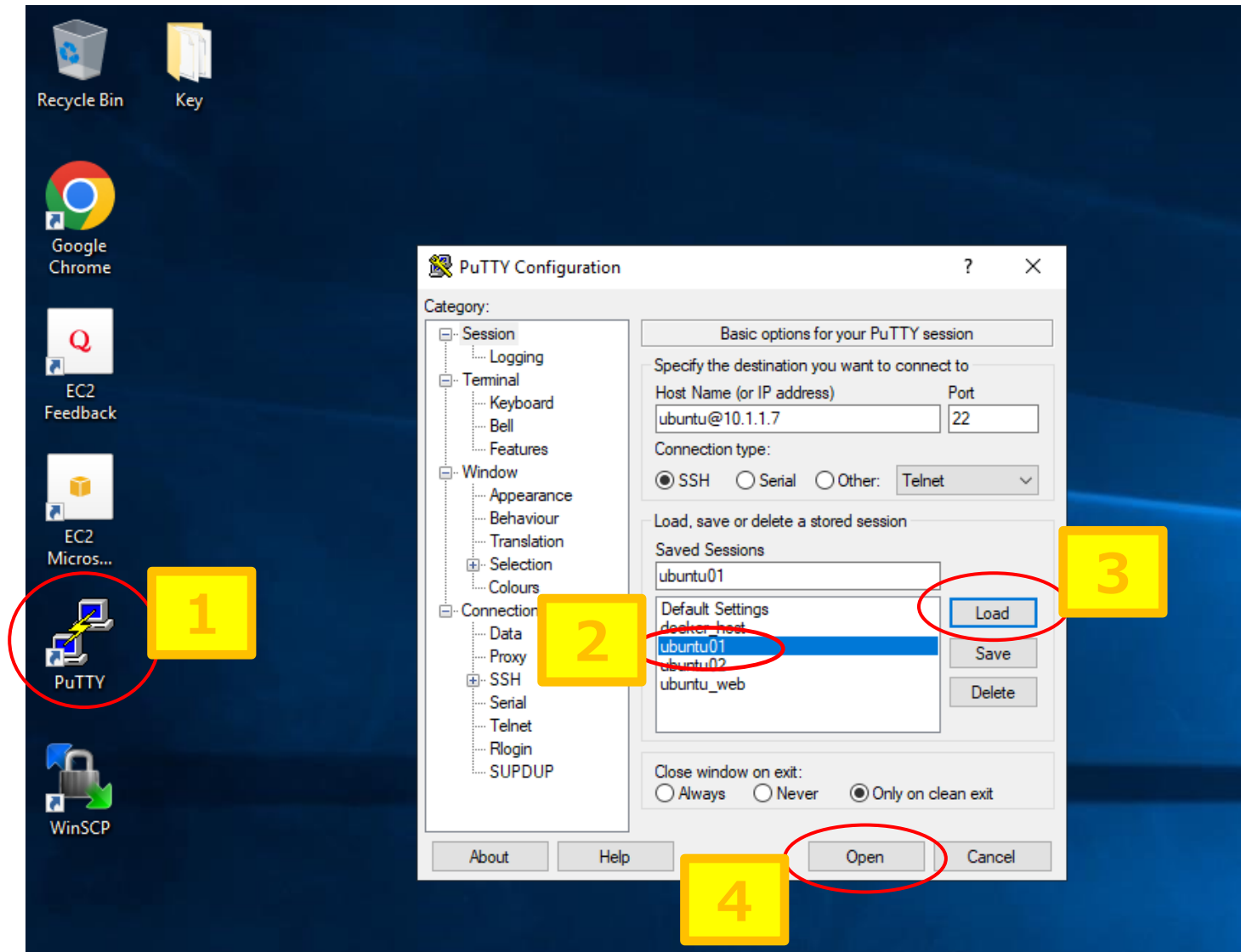
別のアカウントを使用する

パスワードのリセット/ロック解除

OK キャンセル

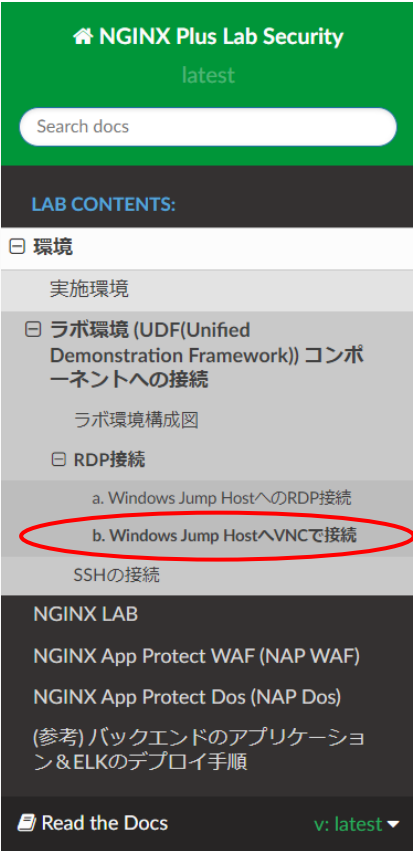
アカウント名 : user
パスワード : user

ハンズオン環境の準備 : Windowsから「ubuntu01」へのSSH接続



補足： RDPクライアントによる接続が出来ない場合の手順

- 端末のセキュリティ設定等により、RDPクライアントによる接続が出来ない場合、 [b. Windows Jump HostへVNCで接続](https://f5j-nginx-plus-lab2-security.readthedocs.io/en/latest/class1/module01/module01.html#b-windows-jump-hostvnc) を参照してください → <https://f5j-nginx-plus-lab2-security.readthedocs.io/en/latest/class1/module01/module01.html#b-windows-jump-hostvnc>



NGINX Plus Lab Security
latest

Search docs

LAB CONTENTS:

環境

実施環境

ラボ環境 (UDF(Unified Demonstration Framework)) コンポーネントへの接続

ラボ環境構成図

RDP接続

a. Windows Jump HostへのRDP接続

b. Windows Jump HostへVNCで接続

SSHの接続

NGINX LAB

NGINX App Protect WAF (NAP WAF)

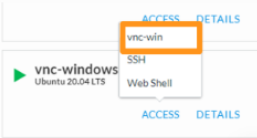
NGINX App Protect Dos (NAP Dos)

(参考) バックエンドのアプリケーション&ELKのデプロイ手順

Read the Docs v: latest

b. Windows Jump HostへVNCで接続

vnc-windowsの **vnc-win** をクリックしてください



接続 をクリックしてください



パスワードが求められます。 **admin** と入力してください





NGINX App Protect WAFについて

- 読み方：エンジンエックス アップ プロテクト ワフ

NGINXソリューション

● ラインナップ

Overview			
Open Source		NGINX OSS	Dev/Opsに最適な、超軽量・高速・多機能なAll-In-One Software
		NGINX Plus	NGINX OSSをベースに、さらなるエンタープライズユースに対応したソフトウェア (LBメソッド・冗長機能・JWT制御・API制御 に加え、各種セキュリティモジュールの利用が可能)
All-In-One SW		NGINX Instance Manager	NGINX OSS、NGINX Plusの統合管理。ヒストリカルなAPM機能、コンフィグ・証明書管理、管理対象の NGINX OSS / NGINX Plusに対するAPI制御機能を提供
		NGINX App Protect WAF	F5が提供する、ミッションクリティカル環境に最適な高速な高品質なWAF
Security		NGINX App Protect DoS	従来のツールでは検知できないレイヤー7のDoS脅威から高度な保護を提供
		NGINX Ingress Controller	Kubernetesの高度な通信制御を提供。NGINX機能をIngressリソースを通じて管理可能
Container		NGINX Gateway Fabric	Gateway API v1に準拠したRed Hat OpenShiftを始めとした様々なKubernetes環境で利用可能
		NGINX One Console	NGINXインスタンスを監視および管理するためのSaaS型管理コンソール
SaaS		NGINXaaS for Azure	NGINX PlusをAzureからSaaS環境として提供、コンフィグを貼り付けるだけで活用が可能





● ラインナップ

Overview		
Open Source		NGINX OSS
		Dev/Opsに最適な、超軽量・高速・多機能なAll-In-One Software
All-In-One SW		NGINX Plus
		NGINX Instance Manager
Security		NGINX OSSをベースに、さらなるエンタープライズユースに対応したソフトウェア (LBメソッド・冗長機能・JWT制御・API制御 に加え、各種セキュリティモジュールの利用が可能)
		NGINX OSS、NGINX Plusの統合管理。ヒストリカルなAPM機能、コンフィグ・証明書管理、管理対象の NGINX OSS / NGINX Plusに対するAPI制御機能を提供
Security		NGINX App Protect WAF
		NGINX App Protect DoS
Container		F5が提供する、ミッションクリティカル環境に最適な高速な高品質なWAF
		従来のツールでは検知できないレイヤー7のDoS脅威から高度な保護を提供
Container		NGINX Ingress Controller
		NGINX Gateway Fabric
SaaS		Kubernetesの高度な通信制御を提供。NGINX機能をIngressリソースを通じて管理可能
		Gateway API v1に準拠したRed Hat OpenShiftを始めとした様々なKubernetes環境で利用可能
SaaS		NGINX One Console
		NGINXaaS for Azure
		NGINX インスタンスを監視および管理するためのSaaS型管理コンソール
		NGINX PlusをAzureからSaaS環境として提供、コンフィグを貼り付けるだけで活用が可能



NGINX App Protect

- APIやアプリケーションを保護するための軽量で高性能なソフトウェアセキュリティソリューション

- **特徴**

- ワールドワイドで実績豊富なF5 BIG-IP Advanced WAF（AWAF）の機能を移植
- 柔軟なデプロイを実現 → プラットフォームに依存せず、クラウド・オンプレ・コンテナに展開
- DevOpsツールとの統合も容易で、CI/CDパイプラインにも適応可能
- WAF、L7 DoS保護、ボット保護、APIセキュリティ、脅威インテリジェンスサービスを提供
- 高度なセキュリティ機能 → OWASP Top 10の主要なWebアプリケーション攻撃を防御
- NGINX Plusにアドオンすることで、NGINXのリバースプロキシ機能やロードバランシング機能と連携
- シンプルな管理 → NGINXの設定ファイルに統合されており、数行の追加でNGINXにWAF機能を有効化

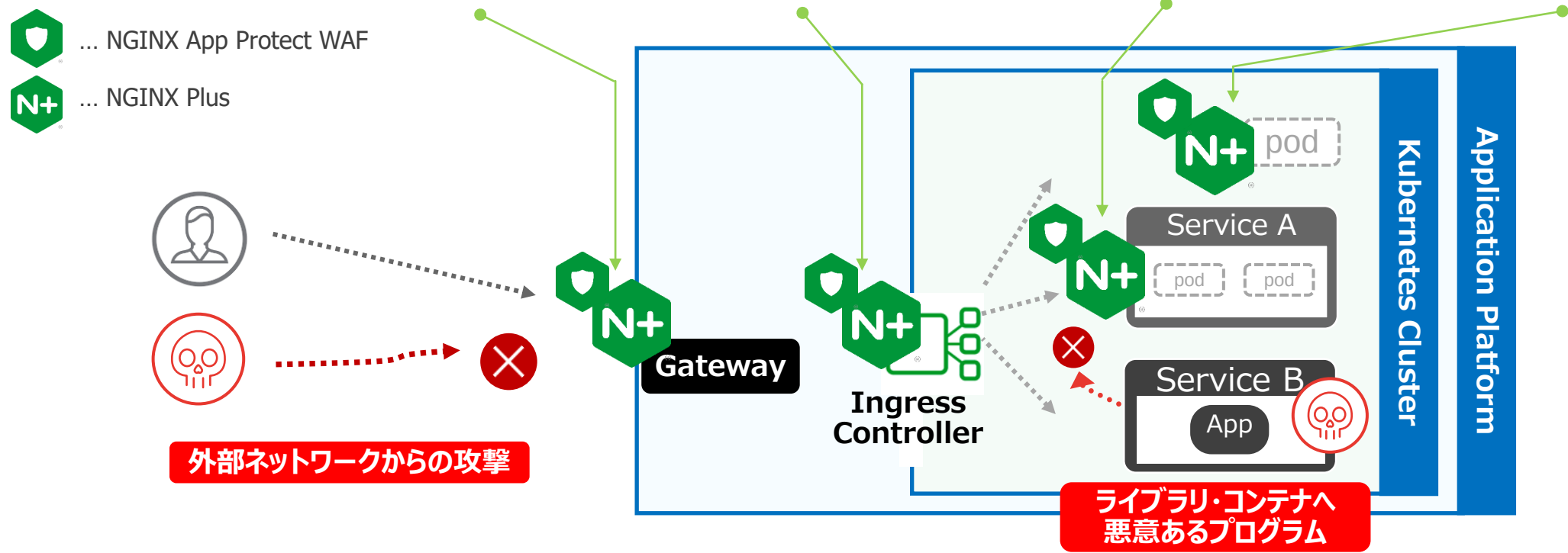


NGINX
App Protect

NGINX App Protect WAF
NGINX App Protect DoS

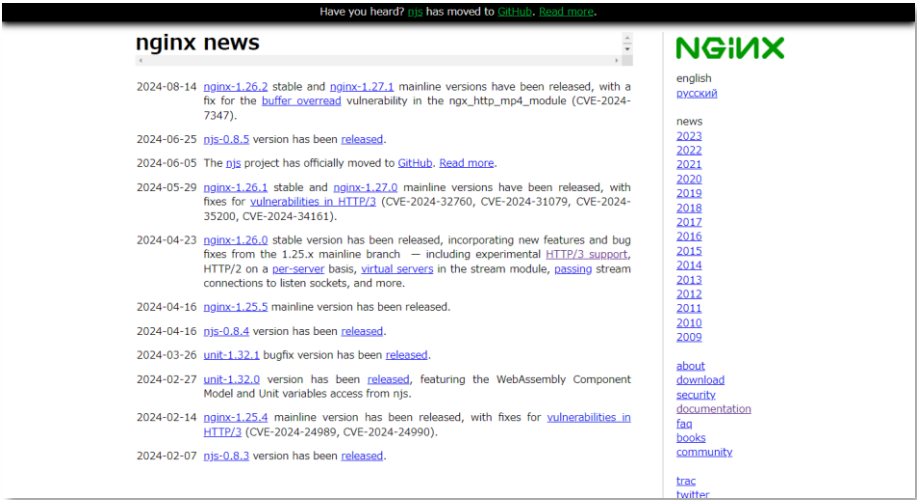
NGINX App Protect WAFのデプロイ構成

	Gateway / At Edge	Ingress Controller	Per-Service Proxy	Per-Pod Proxy
担当者	NeOps/SecOps /DevSecOps	NetOps/SecOps /DevSecOps	DevSecOps	DevOps
スコープ	サービス全体	サービス毎・URI毎	サービス毎	Endpoint毎
コスト・効率性	高/統合によるメリット	高/統合によるメリット	中	細かな設定
設定管理方法	nginx.conf	K8s API	nginx.conf	nginx.conf



NGINX App Protect WAFの新バージョン

- NGINX App Protect WAF **V5** がリリース（2024/03/19 リリース）
 - [NGINX Open Source Software（OSS）へのアドオンが可能](#)
 - 対象は Nginx.orgの手順でインストールできるNGINX OSS
 - 現在の最新バージョンは 2025/04/01 リリースの 5.6（[*URL](#)）
 - NGINX Open Source 1.27.4 に対応



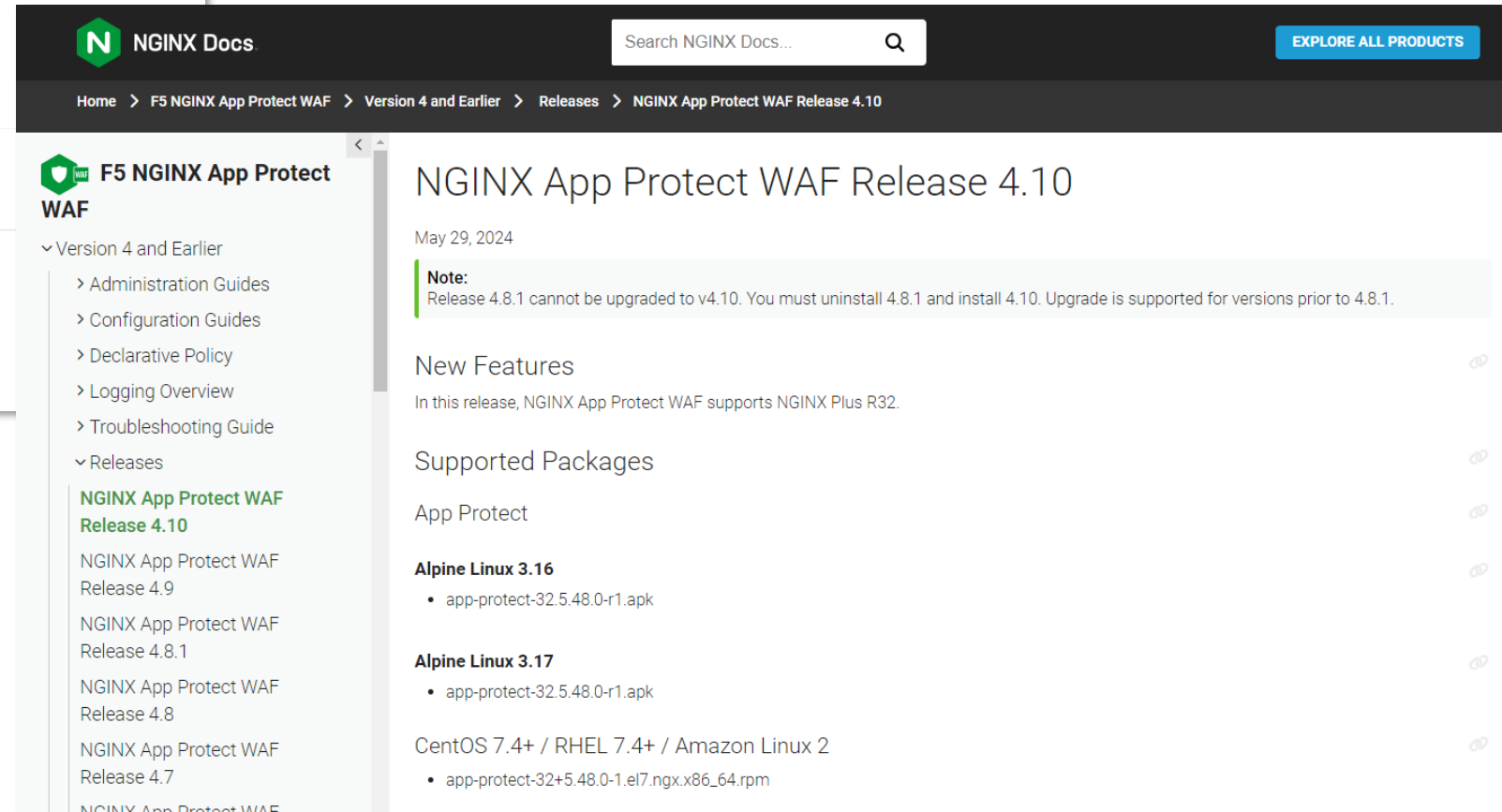
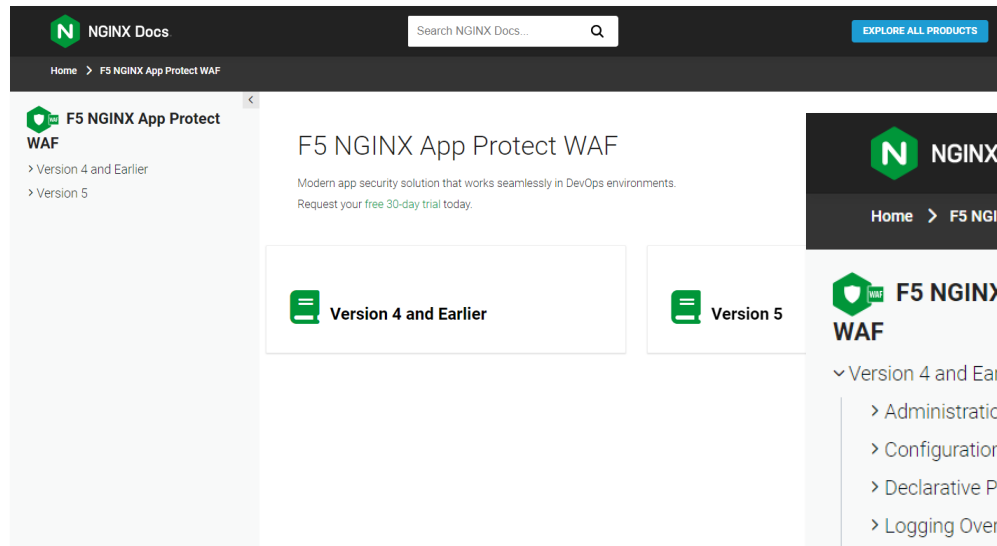
<https://nginx.org/>

- V4との主な違い

	V4	V5
デプロイメント環境	ベア／VM／コンテナ	コンテナ
サポートするデータプレーン	NGINX Plus	NGINX OSS／NGINX Plus
提供方法	パッケージ	コンテナイメージ
NGINX Ingress Controllerへのデプロイ	可	対応予定

インストール

- F5 NGINX App Protect WAF → <https://docs.nginx.com/nginx-app-protect-waf/>

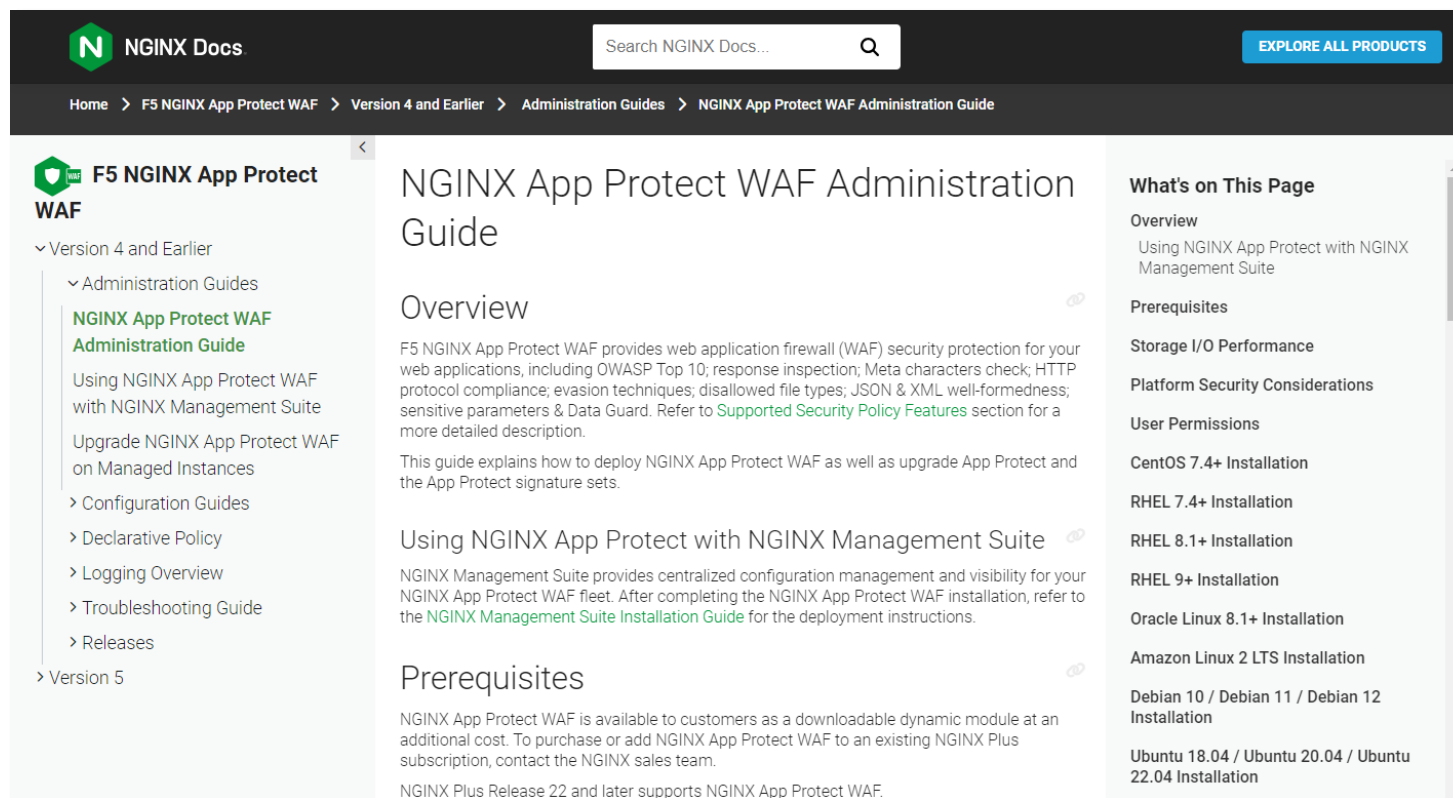


本日利用予定のパッケージの情報

Ubuntu 20.04

- `app-protect_32+5.48.0-1~focal_amd64.deb`

- OSサポート情報、必要ストレージ、などの条件 → <https://docs.nginx.com/nginx-app-protect-waf/v4/admin-guide/install/>



- NGINX
 - NGINX Plus Release 22 and later
- OS
 - CentOS/RHEL 7.4.x and above
 - RHEL 8.1.x and above
 - RHEL 9 and above
 - Oracle Linux 8.1.x and above
 - Amazon Linux 2
 - Debian 10 (Buster) - (NGINX Plus R28から非推奨)
 - Debian 11 (Bullseye)
 - Debian 12 (Bookworm)
 - Ubuntu 18.04 (Bionic) - (NGINX Plus R30から非推奨)
 - Ubuntu 20.04 (Focal)
 - Ubuntu 22.04 (Jammy)
 - Alpine 3.16
 - Alpine 3.17
- その他 : Dockerデプロイ
 - 各種OSをベースとしたDockerfileのサンプルの提供

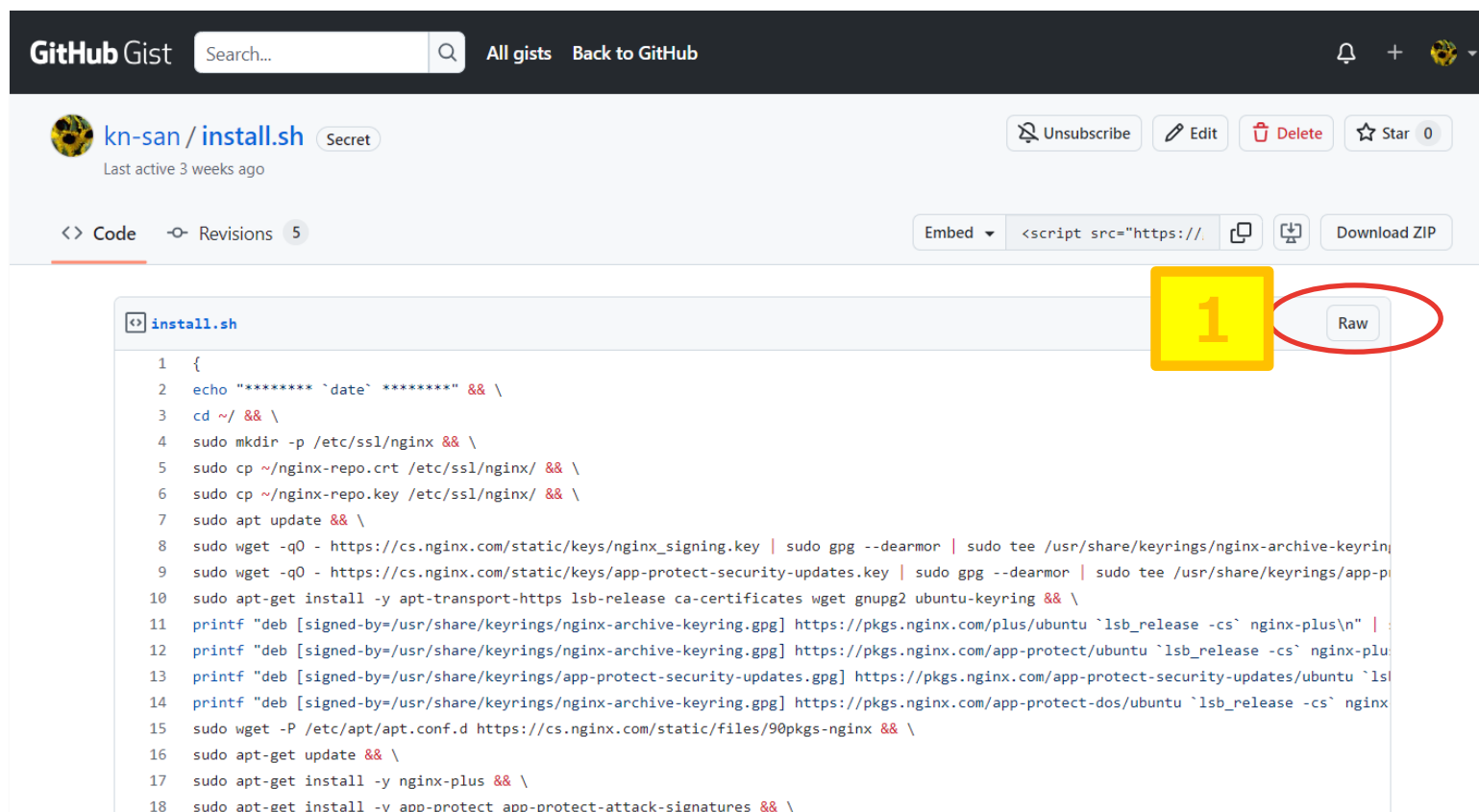
インストール (NGINX App Protect V4)

- *PuTTY*にて「ubuntu01」にアクセスした後、NGINX App Protect V4 をインストールします。

→ **install.sh**

<https://gist.github.com/kn-san/0486e297e175ac0a7f62db02dfc17792>

Zoomのチャット
にて、本URLを
貼ります。



```
1 {
2 echo "***** `date` *****" && \
3 cd ~/ && \
4 sudo mkdir -p /etc/ssl/nginx/ && \
5 sudo cp ~/nginx-repo.crt /etc/ssl/nginx/ && \
6 sudo cp ~/nginx-repo.key /etc/ssl/nginx/ && \
7 sudo apt update && \
8 sudo wget -qO - https://cs.nginx.com/static/keys/nginx_signing.key | sudo gpg --dearmor | sudo tee /usr/share/keyrings/nginx-archive-keyring
9 sudo wget -qO - https://cs.nginx.com/static/keys/app-protect-security-updates.key | sudo gpg --dearmor | sudo tee /usr/share/keyrings/app-p
10 sudo apt-get install -y apt-transport-https lsb-release ca-certificates wget gnupg2 ubuntu-keyring && \
11 printf "deb [signed-by=/usr/share/keyrings/nginx-archive-keyring.gpg] https://pkgs.nginx.com/plus/ubuntu `lsb_release -cs` nginx-plus\n" |
12 printf "deb [signed-by=/usr/share/keyrings/nginx-archive-keyring.gpg] https://pkgs.nginx.com/app-protect/ubuntu `lsb_release -cs` nginx-plu
13 printf "deb [signed-by=/usr/share/keyrings/app-protect-security-updates.gpg] https://pkgs.nginx.com/app-protect-security-updates/ubuntu `ls
14 printf "deb [signed-by=/usr/share/keyrings/nginx-archive-keyring.gpg] https://pkgs.nginx.com/app-protect-dos/ubuntu `lsb_release -cs` nginx
15 sudo wget -P /etc/apt/apt.conf.d https://cs.nginx.com/static/files/90pkgs-nginx && \
16 sudo apt-get update && \
17 sudo apt-get install -y nginx-plus && \
18 sudo apt-get install -y app-protect app-protect-attack-signatures && \
```

1. URLにアクセス後、「Raw」をクリック
2. 表示された内容をコピーを実施
3. ターミナルソフト上で、ペーストを実施
4. ペーストされた内容をENTERキーを押下することで実行

- 5分ほどでインストールが完了します

補足：PuTTYターミナルソフトのクリップボードのペースト（ショートカットキー）は、「SHIFT + Insert」です。

NGINX App Protect WAF設定例

NGINX App Protect WAF設定例：基本設定

1. NGINX Plusをインストールしたホストで NGINX App Protect をインストール
2. NGINX App Protectモジュールをロードし WAF / セキュリティログに関する設定を実施

```
load_module modules/nginx_http_app_protect_module.so;

http {
    server {
        listen      80;
        app_protect_enable on;
        app_protect_security_log_enable on;
        app_protect_security_log "/etc/nginx/log-default.json" syslog:server=elk:5144;

        location /application01 {
            root /usr/share/nginx/html;
            app_protect_policy_file "/etc/nginx/security-policy.json";
            index index.html index.htm;
        }
    }
}
```

NGINX App Protect WAF設定例：基本設定

1. NGINX Plusをインストールしたホストで NGINX App Protect をインストール
2. NGINX App Protectモジュールをロードし WAF / セキュリティログに関する設定を実施

① `load_module modules/nginx_http_app_protect_module.so;`

NGINX App Protect WAF用のモジュールのロード

```
http {  
    server {  
        listen 80;
```

NGINX App Protect WAFの有効化

② `app_protect_enable on;`

セキュリティログ出力の有効化

③ `app_protect_security_log_enable on;`

④ `app_protect_security_log "/etc/nginx/log-default.json" syslog:server=elk:5144;`

セキュリティログ出力フォーマットの指定と出力先の設定

```
    location /application01 {  
        root /usr/share/nginx/html;
```

⑤ `app_protect_policy_file "/etc/nginx/security-policy.json";`

セキュリティポリシーファイルの設定

```
        index index.html index.htm;  
    }  
}
```

- locationディレクティブに WAF のポリシーファイル を指定することで、location毎に異なるポリシーを適用できます。
- locationディレクティブ毎に WAFのON/OFFなどの設定も可能です。

1. セキュリティポリシーファイル：/etc/app_protect/conf/NginxDefaultPolicy.json をベースにカスタマイズ

```
{
  "policy" : {
    "name": "app_protect_default_policy",
    "template": { "name": "POLICY_TEMPLATE_NGINX_BASE" }
  }
}
```

- NGINXの設定ファイル（conf）で“app_protect_policy_file”を指定しなかった場合には、/etc/app_protect/conf/NginxDefaultPolicy.json が自動で適用されます。
- “policy” > “name” は、システム内でユニークな名称である必要があります。
- ファイルのPathは、任意の場所を指定できます。

例)
/etc/nginx/conf.d/sec_policy.json

1. セキュリティポリシーファイル：/etc/app_protect/conf/NginxDefaultPolicy.json をベースにカスタマイズ

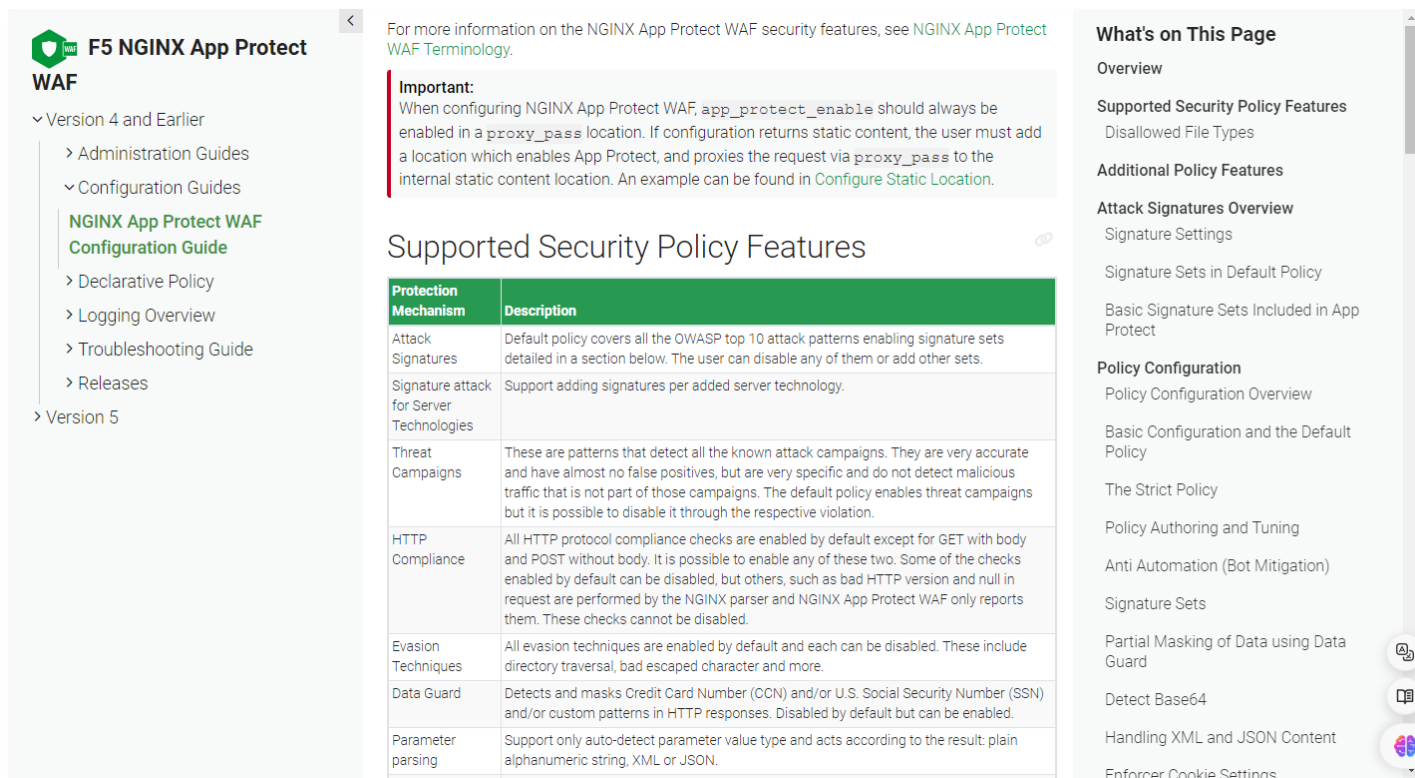
```
{
  "policy" : {
    "name": "custom_policy",
    "template": { "name": "POLICY_TEMPLATE_NGINX_BASE" },
    "applicationLanguage": "utf-8",
    "enforcementMode": "blocking",
    "signatures": [
      {
        "signatureId": 200002147,
        "enabled": false
      }
    ]
  }
}
```

- NGINXの設定ファイル（conf）で“app_protect_policy_file”を指定しなかった場合には、/etc/app_protect/conf/NginxDefaultPolicy.json が自動で適用されます。
- “policy” > “name” は、システム内でユニークな名称である必要があります。
- ファイルのPathは、任意の場所を指定できます。

例)
/etc/nginx/conf.d/sec_policy.json

- JSON形式のポリシーの記述
- 記述方法：NGINX App Protect WAF Declarative Policy
 - <https://docs.nginx.com/nginx-app-protect-waf/v4/declarative-policy/policy/>

- NGINX Docs : <https://docs.nginx.com/nginx-app-protect-waf/v4/configuration-guide/configuration/>



For more information on the NGINX App Protect WAF security features, see [NGINX App Protect WAF Terminology](#).

Important:
When configuring NGINX App Protect WAF, `app_protect_enable` should always be enabled in a `proxy_pass` location. If configuration returns static content, the user must add a location which enables App Protect, and proxies the request via `proxy_pass` to the internal static content location. An example can be found in [Configure Static Location](#).

Supported Security Policy Features

Protection Mechanism	Description
Attack Signatures	Default policy covers all the OWASP top 10 attack patterns enabling signature sets detailed in a section below. The user can disable any of them or add other sets.
Signature attack for Server Technologies	Support adding signatures per added server technology.
Threat Campaigns	These are patterns that detect all the known attack campaigns. They are very accurate and have almost no false positives, but are very specific and do not detect malicious traffic that is not part of those campaigns. The default policy enables threat campaigns but it is possible to disable it through the respective violation.
HTTP Compliance	All HTTP protocol compliance checks are enabled by default except for GET with body and POST without body. It is possible to enable any of these two. Some of the checks enabled by default can be disabled, but others, such as bad HTTP version and null in request are performed by the NGINX parser and NGINX App Protect WAF only reports them. These checks cannot be disabled.
Evasion Techniques	All evasion techniques are enabled by default and each can be disabled. These include directory traversal, bad escaped character and more.
Data Guard	Detects and masks Credit Card Number (CCN) and/or U.S. Social Security Number (SSN) and/or custom patterns in HTTP responses. Disabled by default but can be enabled.
Parameter parsing	Support only auto-detect parameter value type and acts according to the result: plain alphanumeric string, XML or JSON.

What's on This Page

- Overview
- Supported Security Policy Features
 - Disallowed File Types
- Additional Policy Features
- Attack Signatures Overview
 - Signature Settings
 - Signature Sets in Default Policy
- Basic Signature Sets Included in App Protect
- Policy Configuration
 - Policy Configuration Overview
 - Basic Configuration and the Default Policy
 - The Strict Policy
 - Policy Authoring and Tuning
- Anti Automation (Bot Mitigation)
- Signature Sets
- Partial Masking of Data using Data Guard
- Detect Base64
- Handling XML and JSON Content
- Enforcer Cookie Settings

- 保護メカニズム
 - 攻撃シグネチャ
 - サーバーテクノロジーのシグネチャ攻撃
 - 脅迫キャンペーン
 - HTTP コンプライアンス
 - 回避テクニック
 - データガード
 - パラメータ解析
 - 使用できないメタ文字
 - 許可されていないファイルタイプの拡張子
 - クッキーの適用
 - 敏感なパラメータ
 - JSONコンテンツ
 - XMLコンテンツ
 - 許可される方法
 - IP リストの拒否と許可
 - XFFヘッダーを信頼する
 - gRPC コンテンツ
 - 大規模なリクエストのブロック



ハンズオン

- ハンズオンガイド：
 - F5 Labs - Index — NGINX Plus Lab Security documentation
<https://f5j-nginx-plus-lab2-security.readthedocs.io/en/latest/>



🏠 / F5 Labs - Index

🔗 Edit on GitHub

F5 Labs - Index

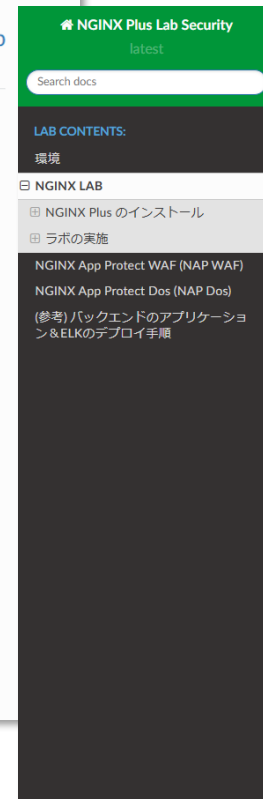
ようこそ！

ようこそ！ NGINX Labへ！
実際にNGINXを触って試していただくための手順をまとめています。
ラボ環境にアクセス可能な方は手順に従って操作をしてください。
事前に資料をご覧になりたい方は座学資料を御覧ください。

座学資料

このラボはNGINX Plusのインストールから各種設定を行っていただけます。

NGINX Plusの基本的な動作や仕様について紹介しております。



🏠 / NGINX LAB

🔗 Edit on GitHub

NGINX LAB

NGINX Plus のインストール

1. NGINX Plus、アドオンモジュールのインストール (15min)

こちらの手順「[NGINX Plusのインストール \(15min\)](#)」を参考に、NGINX Plus、アドオンモジュールをインストールしてください

手順の内容に加えて、必要となるモジュールをインストールしてください

```
sudo apt-get install nginx-plus-module-njs
```

インストールしたパッケージの情報を確認いただけます

```
# dpkg-query -f='${Package} ${Version} ${Architecture}\n' -W nginx-plus-module-njs
```

Package	Version	Architecture
nginx-plus-module-njs	25+0.7.0-1-focal	amd64

ラボの実施

1. 必要なパッケージの取得

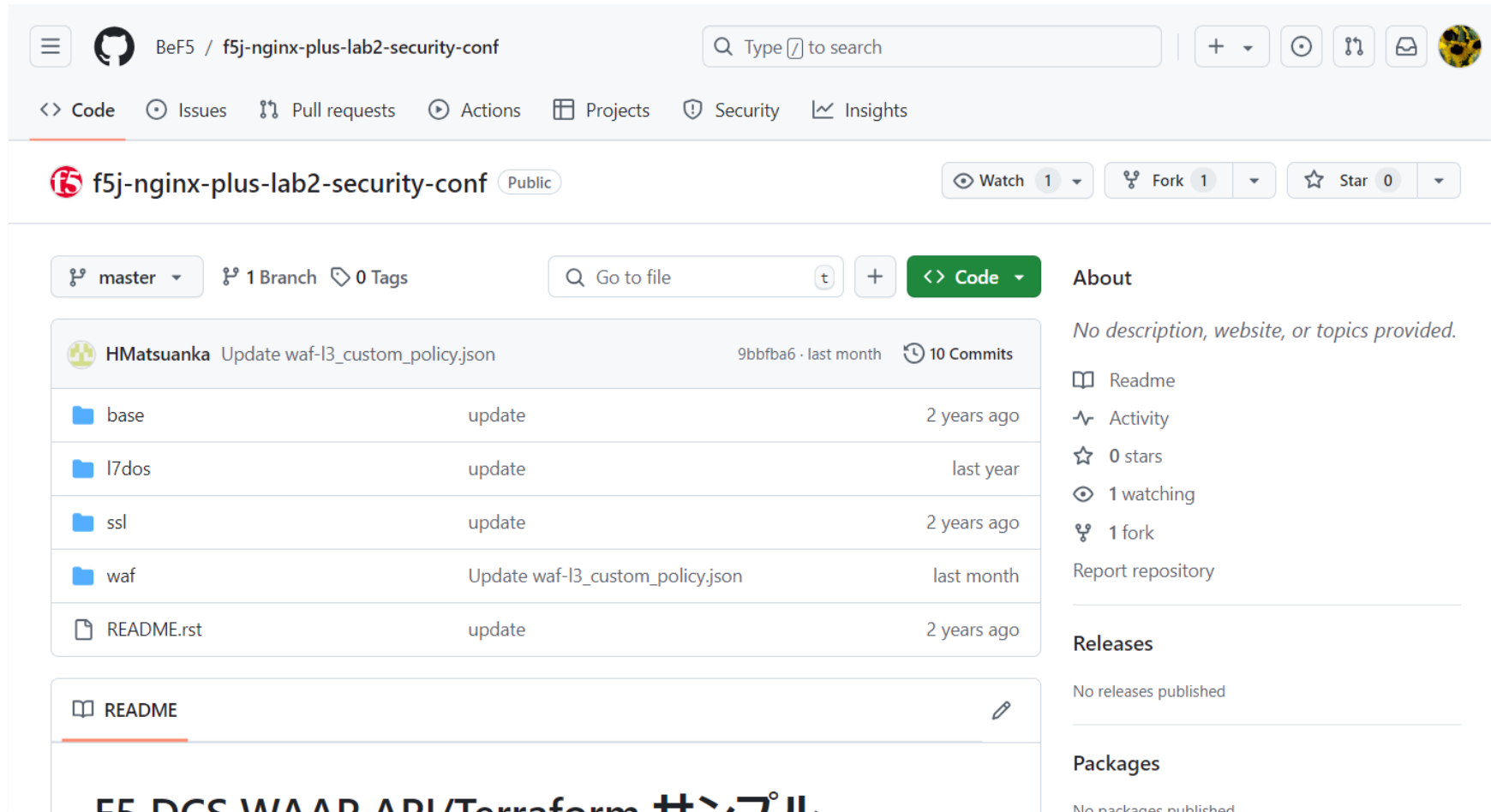
```
sudo su
cd ~/
git clone https://github.com/Bef5/f5j-nginx-plus-lab2-security-conf.git
```

2. インストールしたNGINX Plusに必要な設定を追加

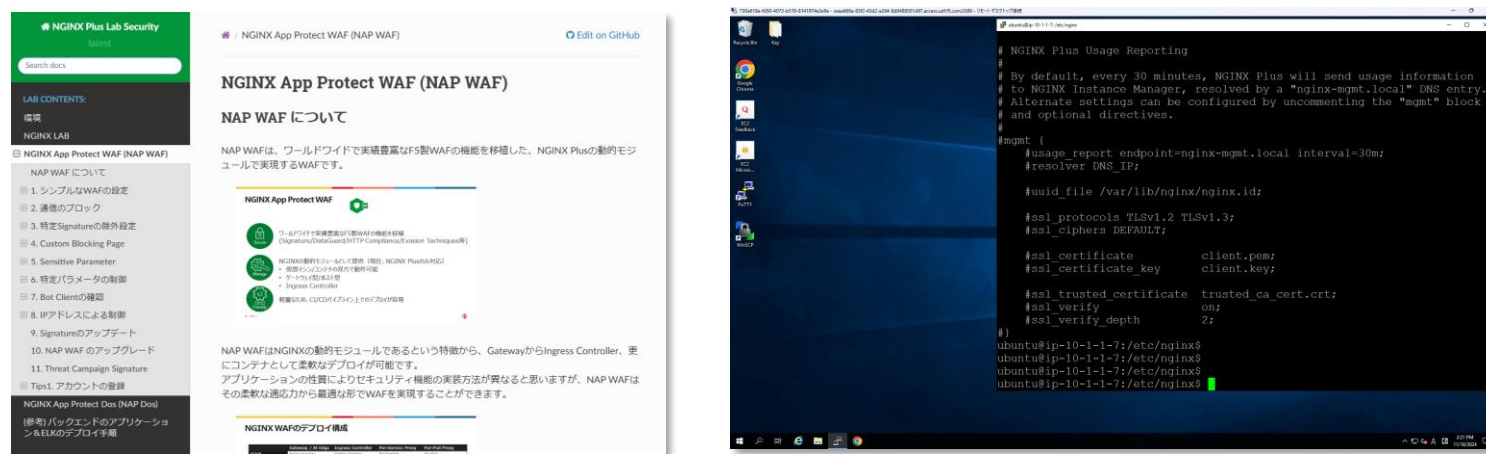
GitHub : BeF5/f5j-nginx-plus-lab2-security-conf

- 本ハンズオンセミナーで利用する各種設定ファイル

<https://github.com/BeF5/f5j-nginx-plus-lab2-security-conf.git>



※ ハンズオンは、ハンズオンガイドのサイト と リモートデスクトップ環境 を使って進めていきます。





NGINX One Console のご紹介

NGINX One Console は、複数の NGINX インスタスを一元的に管理・監視するためのSaaS型統合管理ツールです。

ダッシュボード機能

インスタスの死活監視

バージョンの可視化

NGINX CVE情報

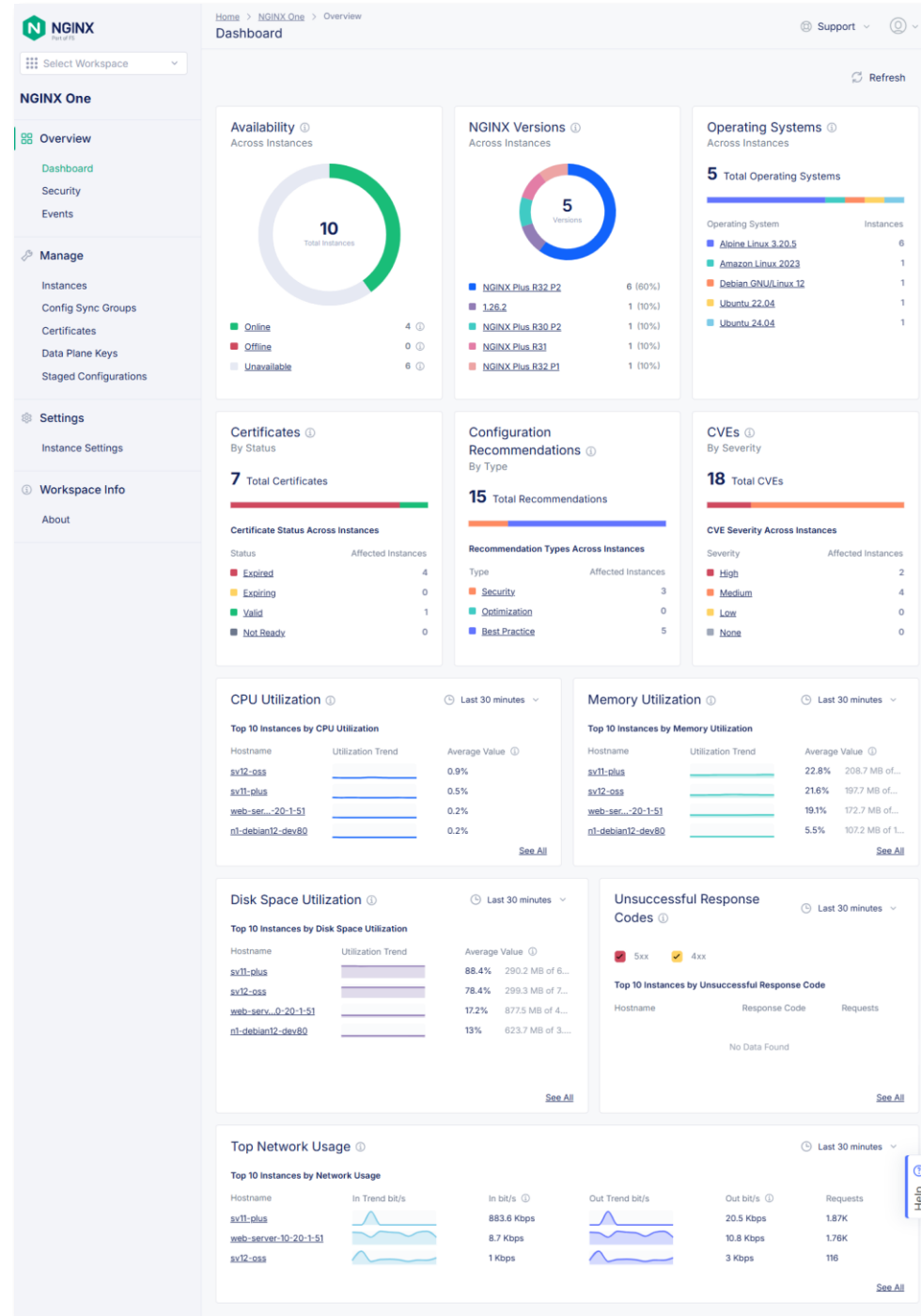
サーバー証明書管理

設定推奨リコメンデーション機能

AIアシスタント機能

テレメトリクスの収集

CPU/メモリの各使用率



The screenshot displays the NGINX One management console. The left sidebar contains navigation menus for 'NGINX One' (Overview, Dashboard, Security, Events) and 'Manage' (Instances, Config Sync Groups, Certificates, Data Plane Keys, Staged Configurations, Settings). The main area shows the 'Configuration' tab for instance 'sv11-plus'. It displays a configuration file path and its contents, including a 'server' block with 'listen 443 ssl http2;'. A 'Show Recommendations' toggle is active. Below the configuration, a message states: 'Modify the NGINX configuration files directly on your instance to apply the desired recommendations: 1 recommendation found for /etc/nginx/conf.d/sv11pro.naga1.dev.tedlab.net.conf'. A specific recommendation is highlighted: 'Best Practice - Warning: default_server parameter is not set for the listen directive on line 2'. An 'AI Assistant' chat window is open, showing a user query in Japanese and a detailed response explaining the benefits of HTTP/2 and the need to set 'default_server'.

表示・設定変更

AIアシスタント機能

デプロイ&リロード

推奨設定の提示（リコメンデーション機能）

AIアシスタント機能

複数インスタンスへの同時デプロイ&リロード

変更履歴表示 & 差分比較

リコメンデーション機能

Home > NGINX One > Manage

Certificates

+ Add Certificate Refresh

Certificate Status

Total	Valid (31+ days)	Expires Soon (<31 days)	Expired	Not Ready
9	2	0	7	0

Management Status ⓘ

Managed	Unmanaged
3	6

Managed Certificates or CA Bundles 3 items

Managed Unmanaged Export (3) Search

+ Add Filter

☐	Name	Type	Subject Name	Status	Start Date	Expiration Date	Actions
☐	deb01-ussl	SSL Certificate	deb01.n...lab.net	Expired	2024/12/13, 10:0...	2025/3/13, 10:09...	...
☐	dev02-ussl	SSL Certificate	dev02.n...lab.net	Expired	2024/12/13, 10:0...	2025/3/13, 10:09...	...
☐	n-server01	SSL Certificate	singatur...rai..lab	Valid	2016/1/22, 17:29...	2026/1/19, 17:29...	...

Help

ステータス表示

有効期限表示

30日間前警告表示

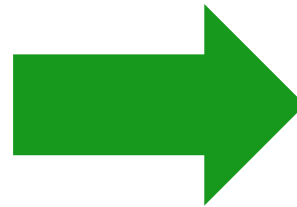
証明書と鍵のアップロード

インスタンスへの適用



まとめ

- NGINXのWAF = NGINX App Protect WAFについて
- いくつかの設定をハンズオン
 - シンプルなWAFの設定
 - 通信のブロック
 - 特定Signatureの除外設定
 - Custom Blocking Page
 - Sensitive Parameter
 - 特定パラメータの制御
 - Bot Clientの確認
 - IPアドレスによる制御



1. WAFを用いて外部からの悪意あるリクエストを検知・拒否する方法を理解する
2. NGINXのWAFモジュールの設定について理解する





東京エレクトロンデバイスからのお知らせ

各編 企業毎の
個別開催
実施可能！

冗長

イチから体験！ NGINXハンズオントレーニング ～冗長構成～

* 不定期開催 → 詳しく弊社ホームページにて！

<https://cn.teldevice.co.jp/seminar/>

イチから体験！ NGINXハンズオントレーニング ～認証～

* 不定期開催 → 詳しく弊社ホームページにて！

<https://cn.teldevice.co.jp/seminar/>

認証

WAF

イチから体験！ NGINXハンズオントレーニング ～NGINX App Protect WAF編～

* 不定期開催 → 詳しく弊社ホームページにて！

<https://cn.teldevice.co.jp/seminar/>

NGINXがまるっと分かる！ブログ更新中！

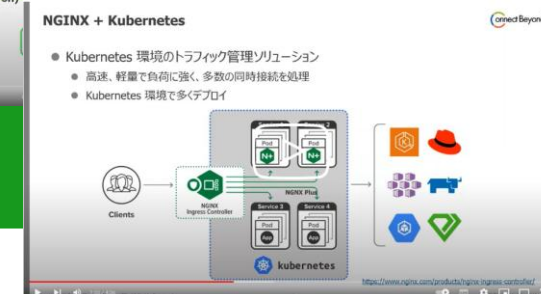
<https://cn.teldevice.co.jp/blog/search/?q=NGINX>

ブログ

YouTube

NGINXを簡単解説！

F5 NGINX - YouTube



無料トライアルライセンスのご案内（30日間有効の機能制限なし）



- 東京エレクトロンデバイスのF5 NGINX製品のページより
ページ中段の「**無料トライアルライセンス申し込み**」をクリックください

- URL :

<https://cn.teldevice.co.jp/product/f5-nginx/>



- 発行可能なライセンス種類

- NGINX Plus
- NGINX App Protect WAF
- NGINX App Protect DoS



**今後のより充実したセミナー開催のため
アンケートへのご協力をお願いいたします。**

**配布資料は、セミナー終了後にお送りするメールにて
ご案内いたします。**



ありがとうございました

東京エレクトロン デバイス株式会社