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

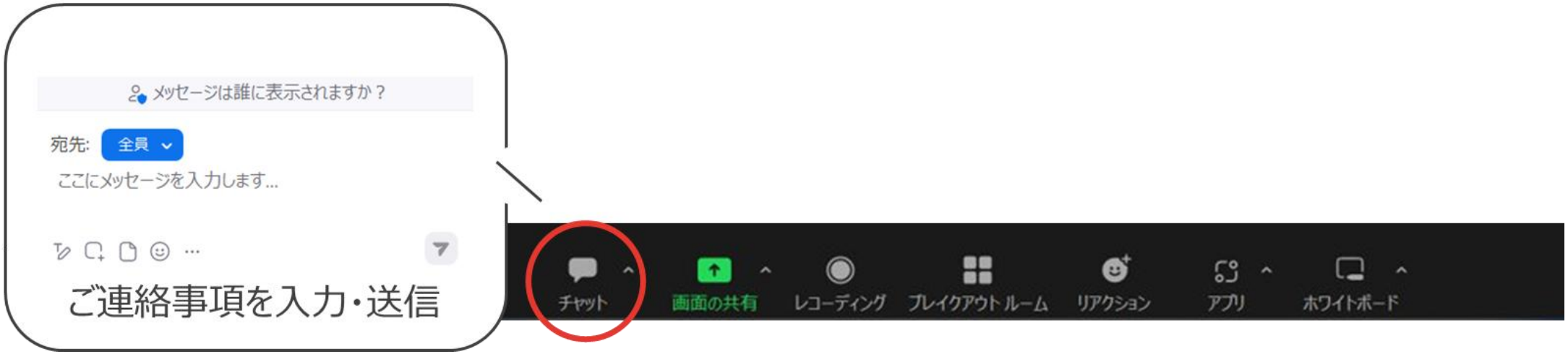
2024年11月28日

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。



配布資料/アンケートについて

Connect Beyond

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。

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

2024年11月28日

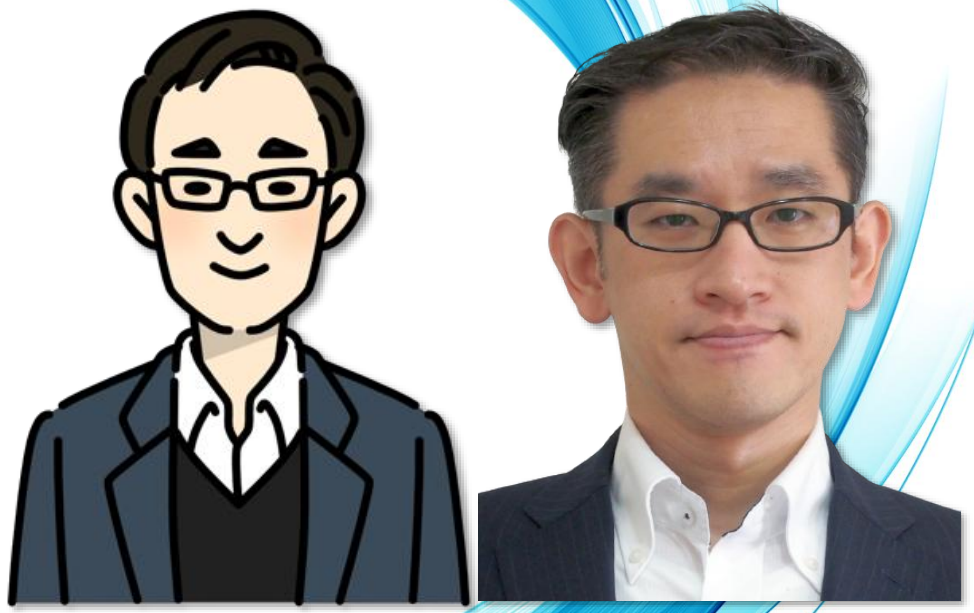
自己紹介

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/

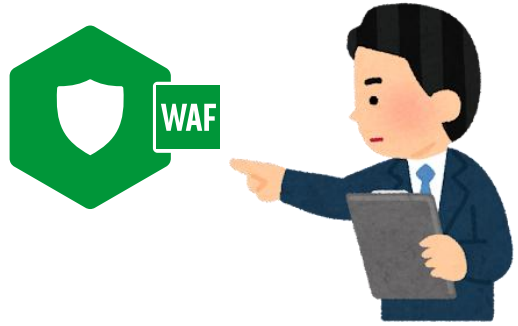


東京エレクトロンデバイスについて

- 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10年連続No.1の一次代理店（2024年実績）
- 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)

アジェンダ

- 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

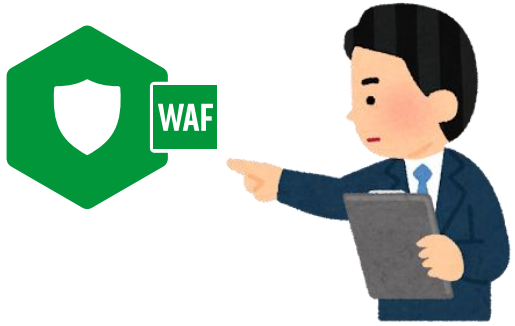


- 時間の都合により、上記のできるところまで実施とさせていただきます。ご了承くださいますようお願い申し上げます。

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

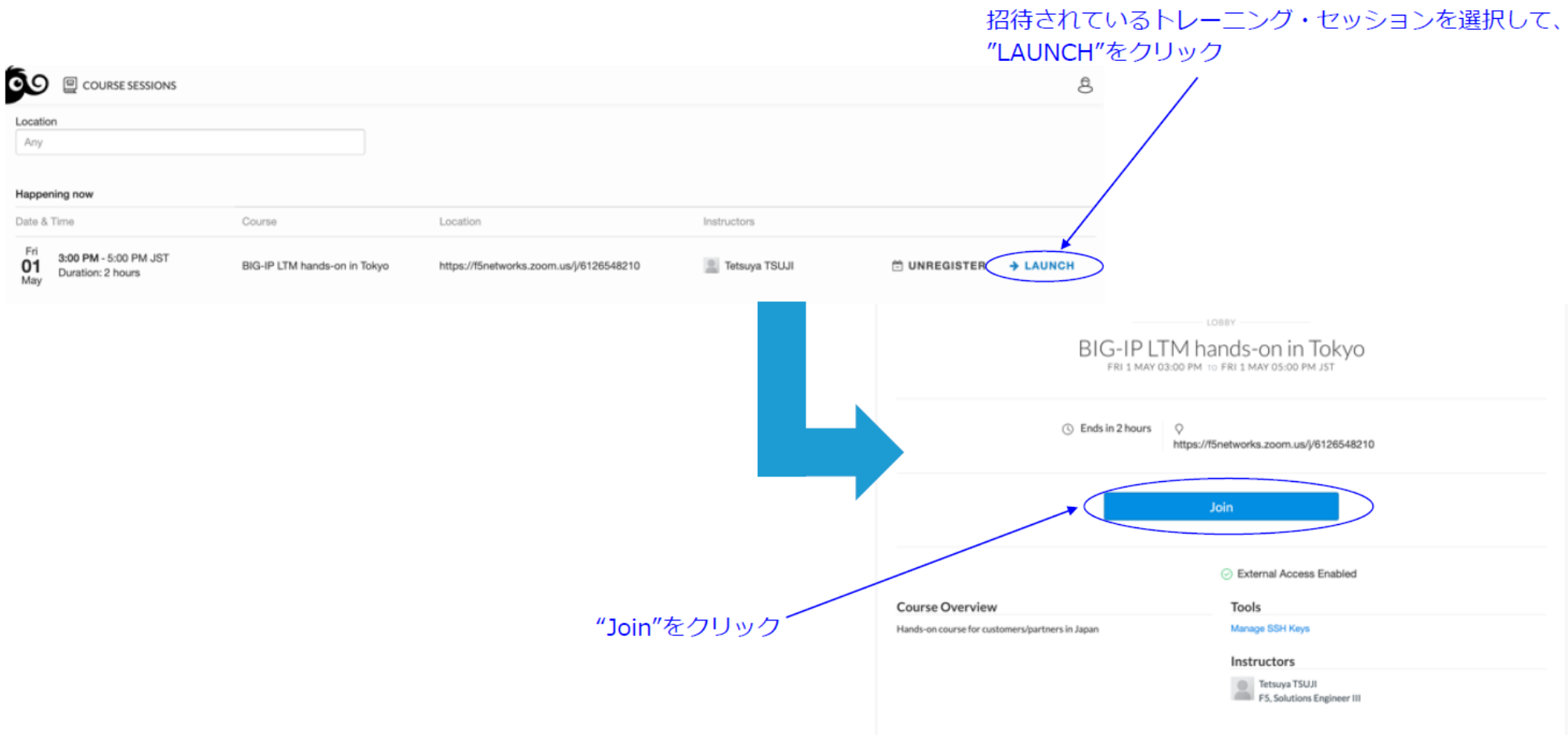
ハンズオン環境の準備：ハンズオンガイドURLのご案内

- 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。

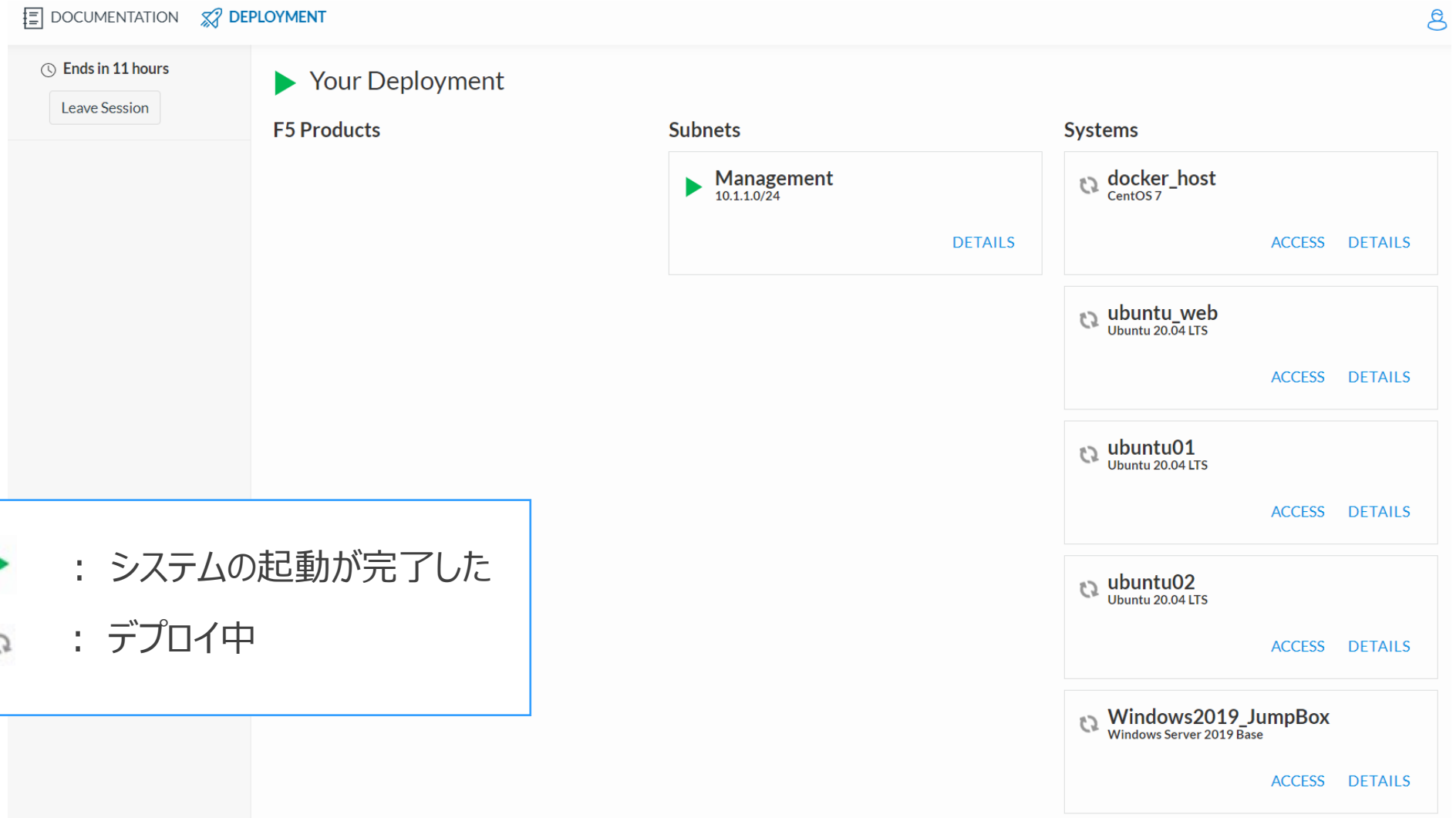
ハンズオン環境の準備：ハンズオン環境の起動

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



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

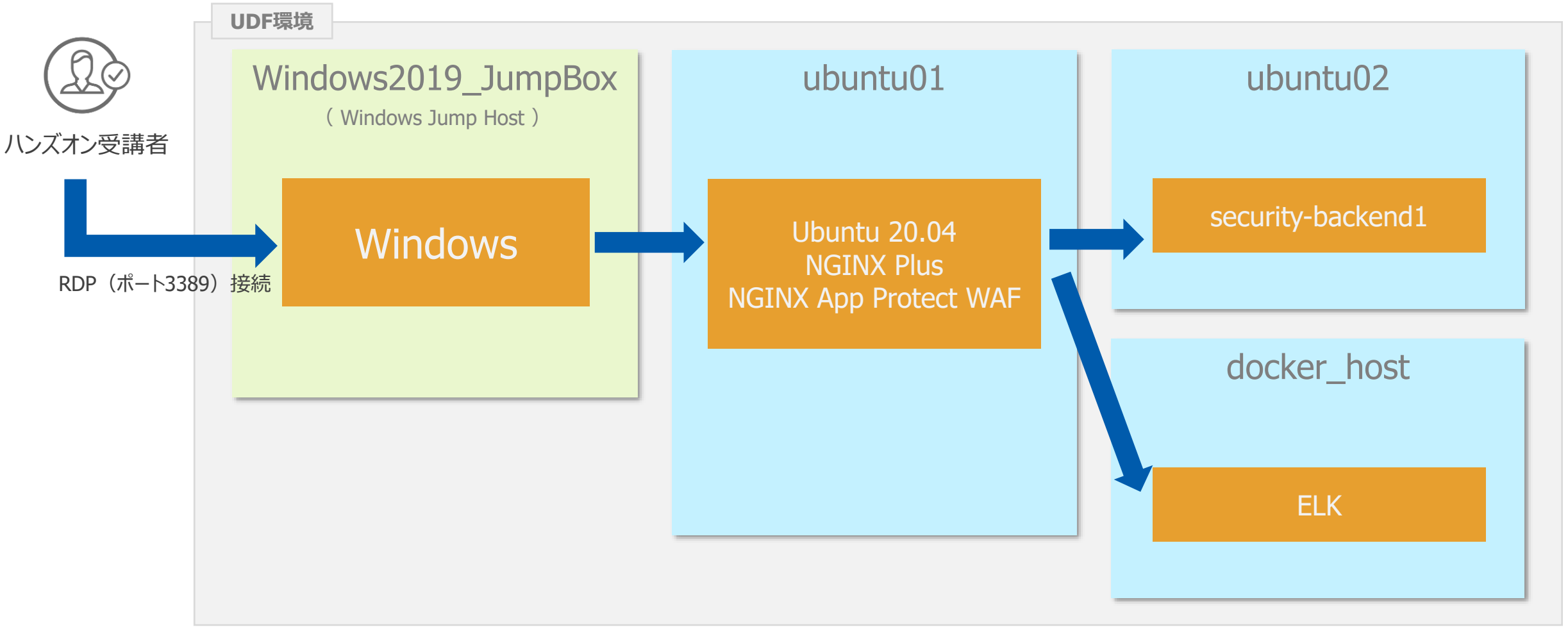


：システムの起動が完了した

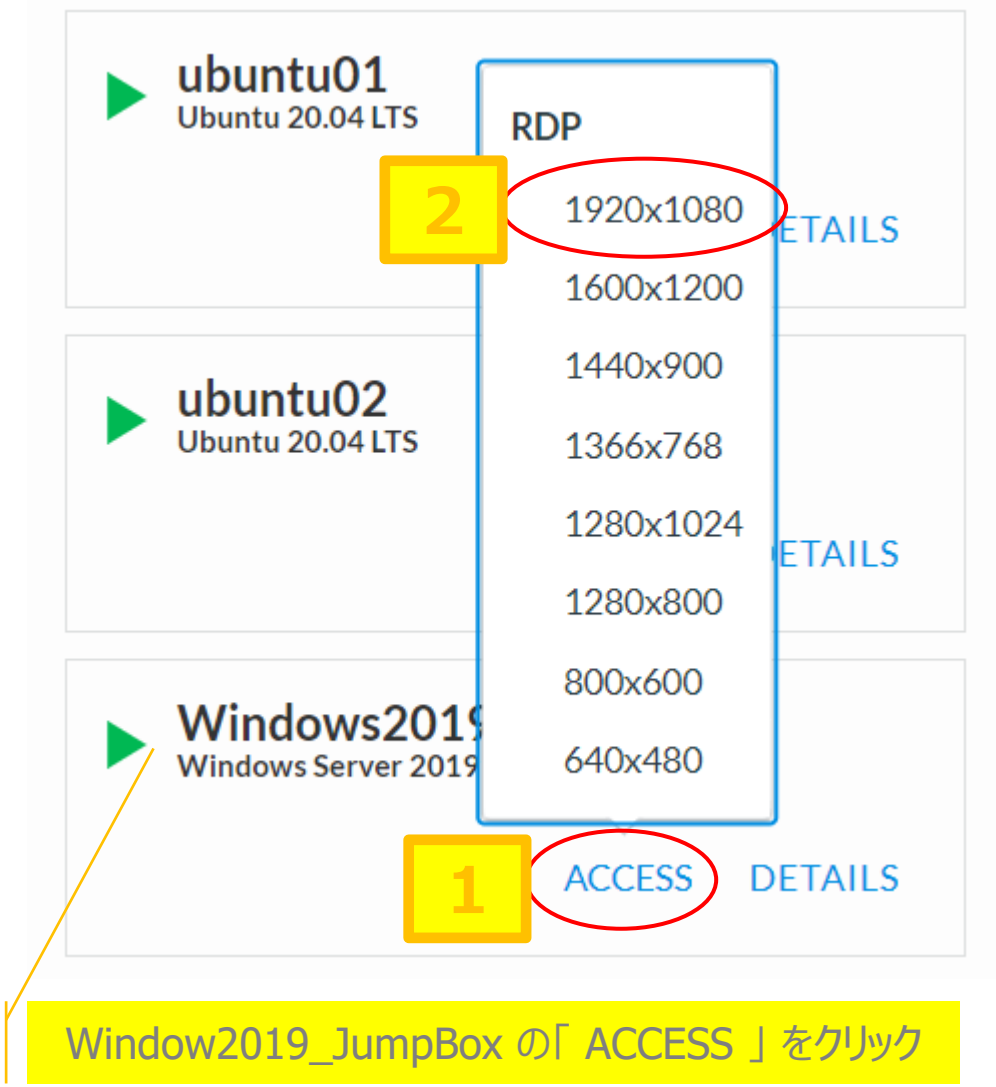
：デプロイ中

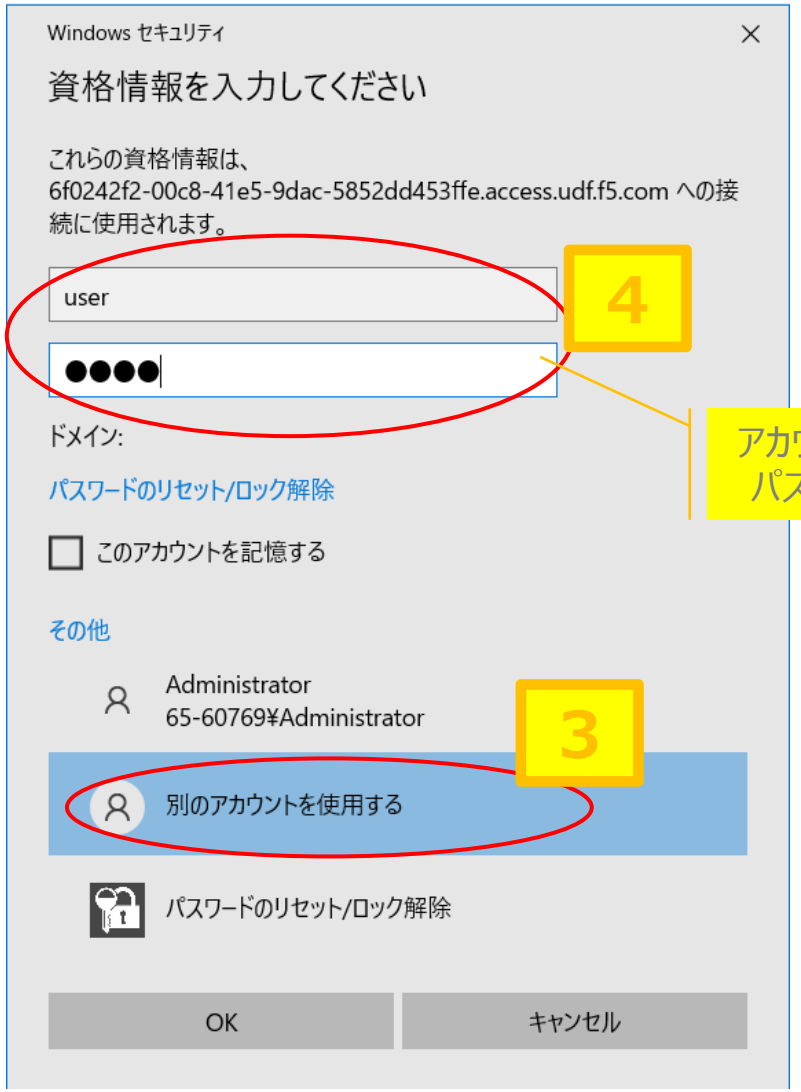
東京エレクトロン デバイス

ハンズオン環境の準備：ハンズオン環境について

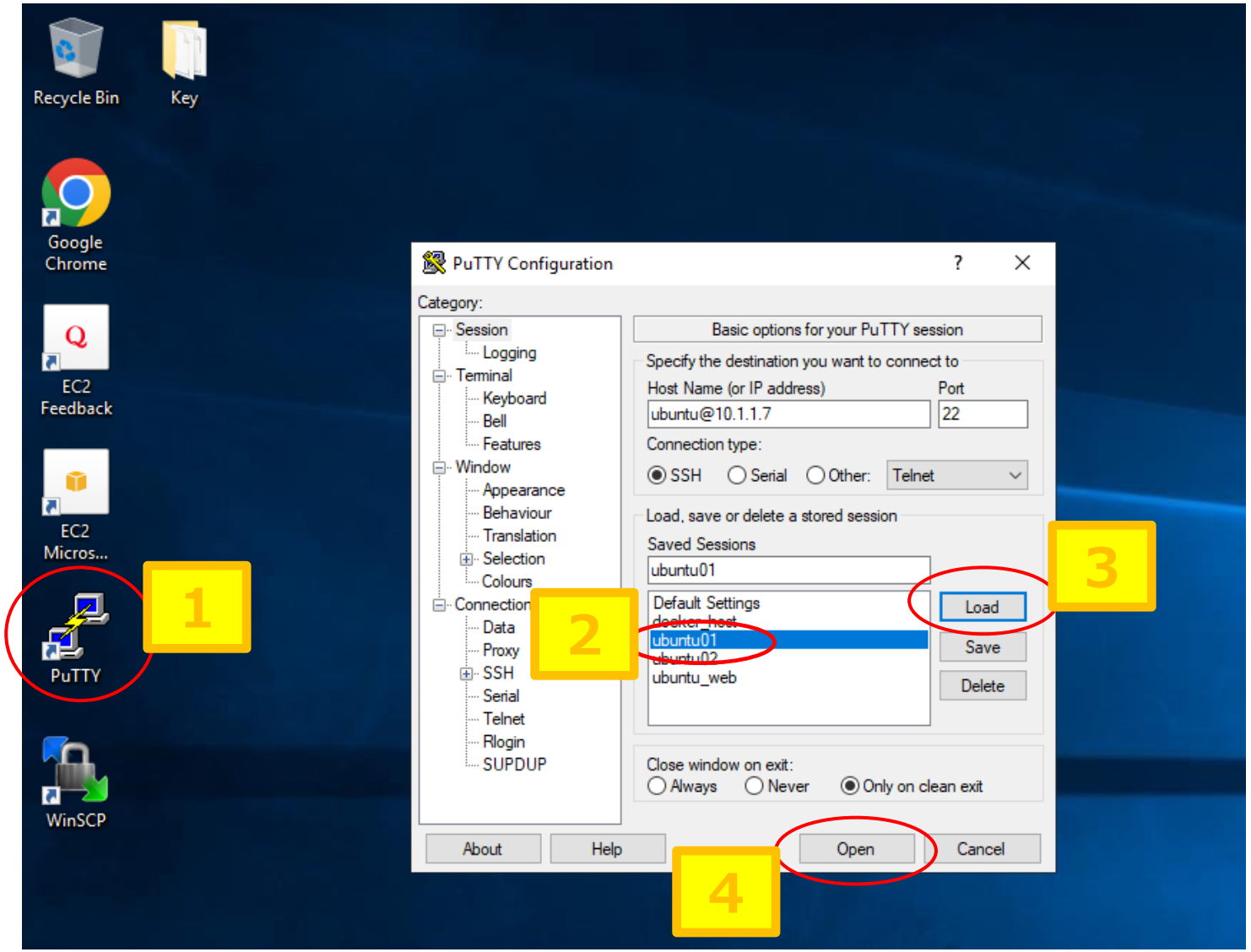


ハンズオン環境の準備：ハンズオン環境にRDP接続





ハンズオン環境の準備：Windowsから「ubuntu01」へのSSH接続



1. デスクトップの PuTTYアイコンをクリック
2. Session内の「ubuntu01」をクリック
3. 「Load」ボタンをクリック
4. 画面下の「Open」ボタンをクリック

- ターミナル画面に表示されるポップアップ画面にて、「Accept」をクリック

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 App Protect WAFについて

NGINXソリューション

NGINXソリューション

- NGINXが提供するソフトウェア

	概要
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）
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
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
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
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

NGINXソリューション

- NGINXが提供するソフトウェア

	概要
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）
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
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
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
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

NGINX App Protect

F5 NGINX App Protect → 通称：NAP（ナップ）

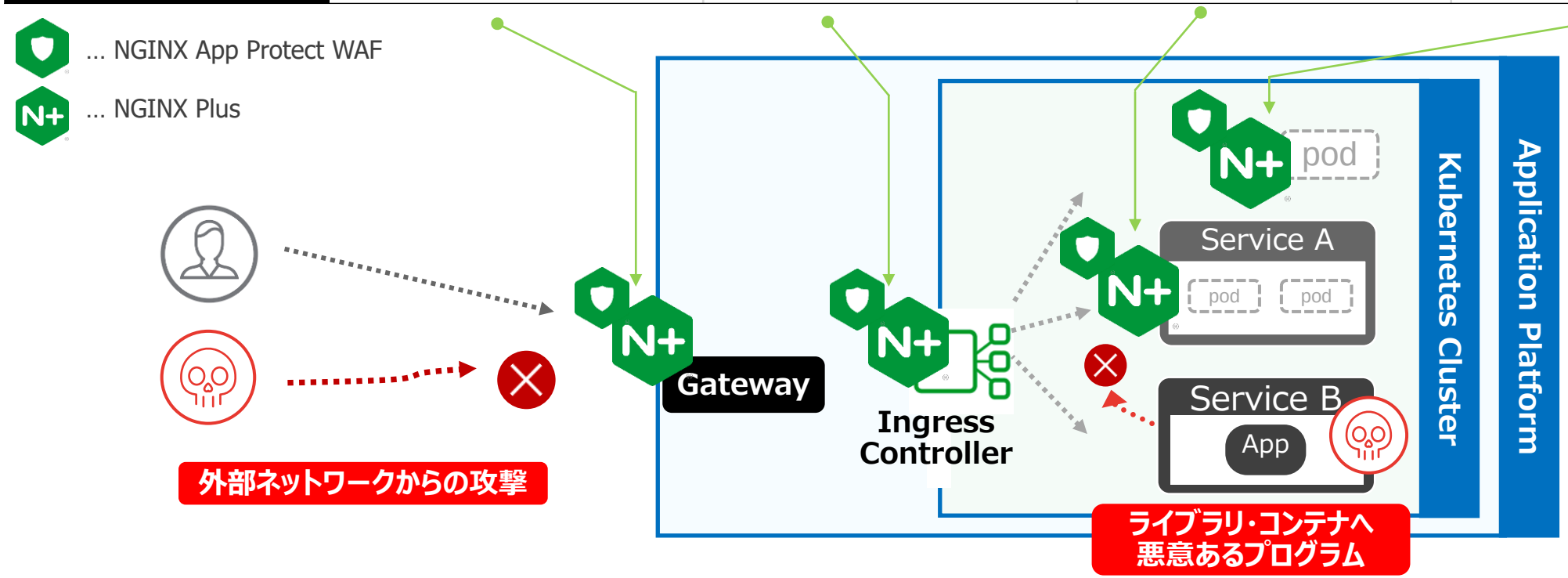
- APIやアプリケーションを保護するための軽量で高性能なソフトウェアセキュリティソリューション
  - **特徴**
    - ワールドワイドで実績豊富なF5 BIG-IP Advanced WAF（AWAF）の機能を移植
    - 柔軟なデプロイを実現 → プラットフォームに依存せず、クラウド・オンプレ・コンテナに展開
    - DevOpsツールとの統合も容易で、CI/CDパイプラインにも適応可能
    - WAF、L7 DoS保護、ボット保護、APIセキュリティ、脅威インテリジェンスサービスを提供
    - 高度なセキュリティ機能 → OWASP Top 10の主要なWebア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

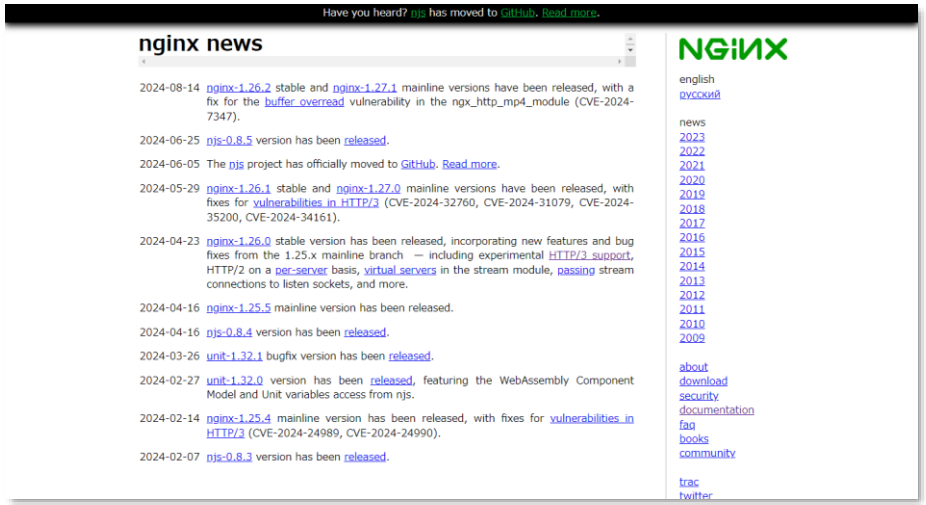
NGINX App Protect WAFのデプロイ構成

	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 2024/05/29 リリースの 5.2（*URL）
    - NGINX Open Source 1.25.4 and 1.25.5 に対応



https://nginx.org/

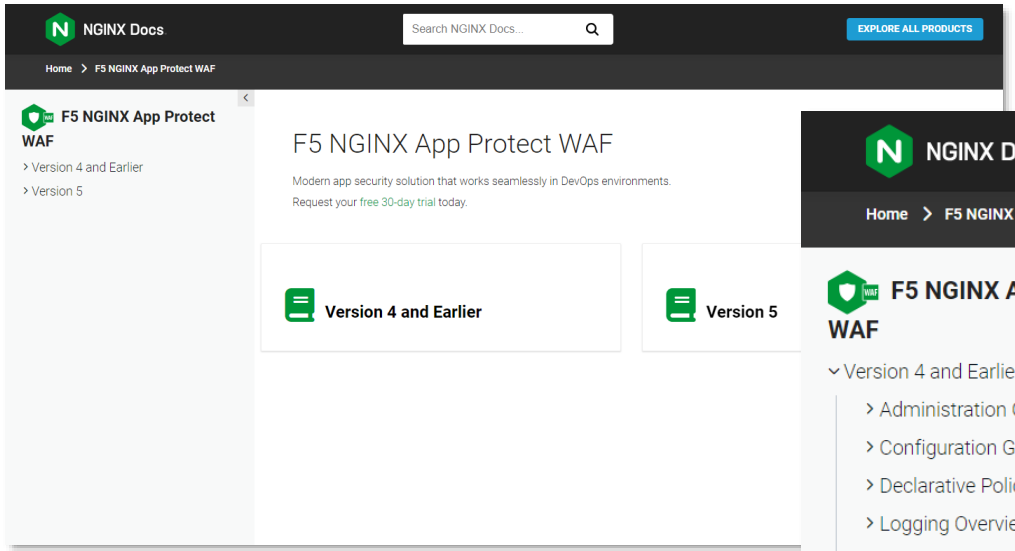
- V4との主な違い

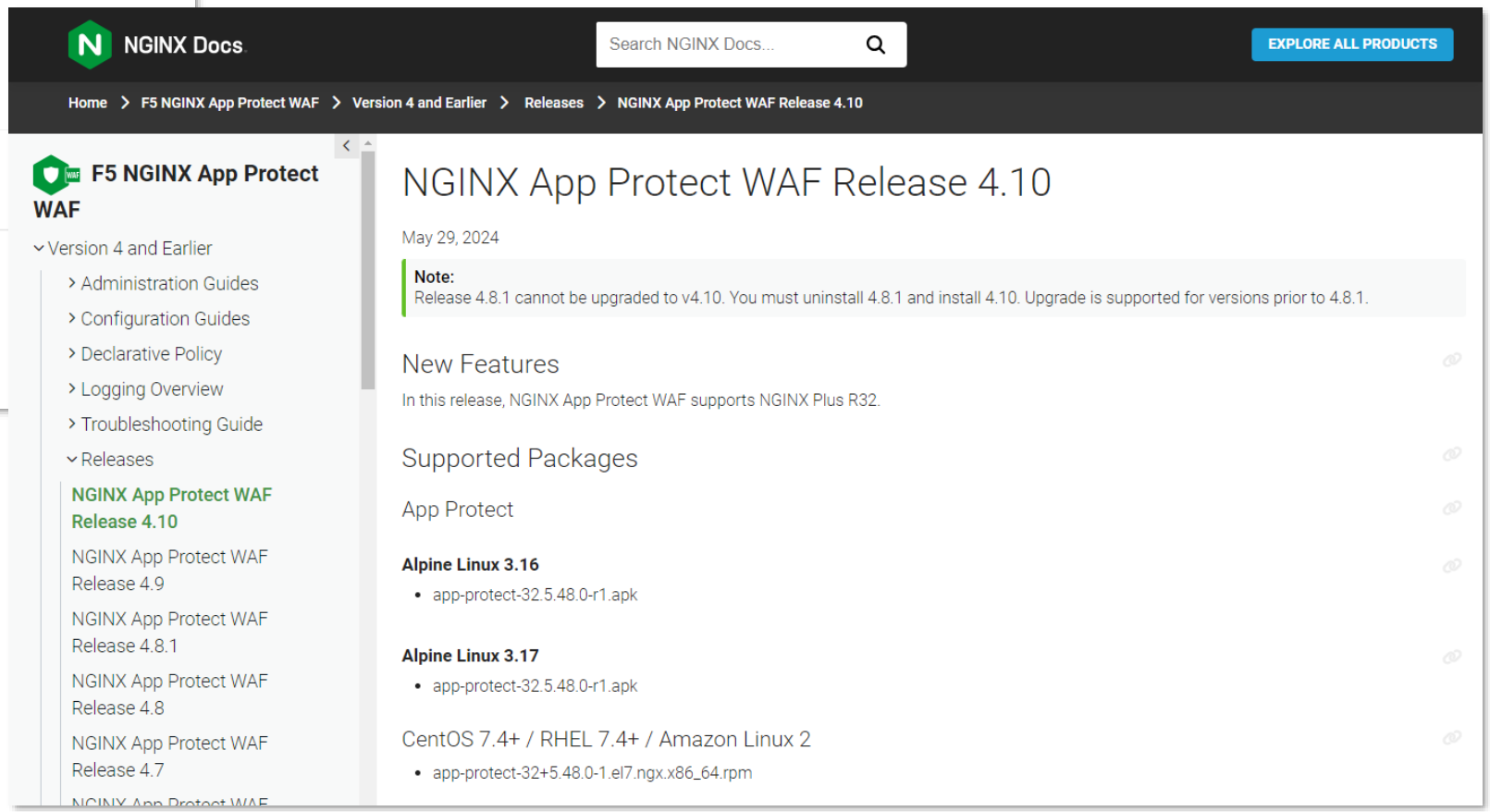
	V4	V5
デプロイメント環境	ベア／VM／コンテナ	コンテナ
サポートするデータプレーン	NGINX Plus	NGINX OSS/NGINX Plus
提供方法	パッケージ	コンテナイメージ
NGINX Ingress Controllerへのデプロイ	可	対応予定

インストール

NGINX Docs：オンラインマニュアル（NGINX Product Documentation）

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





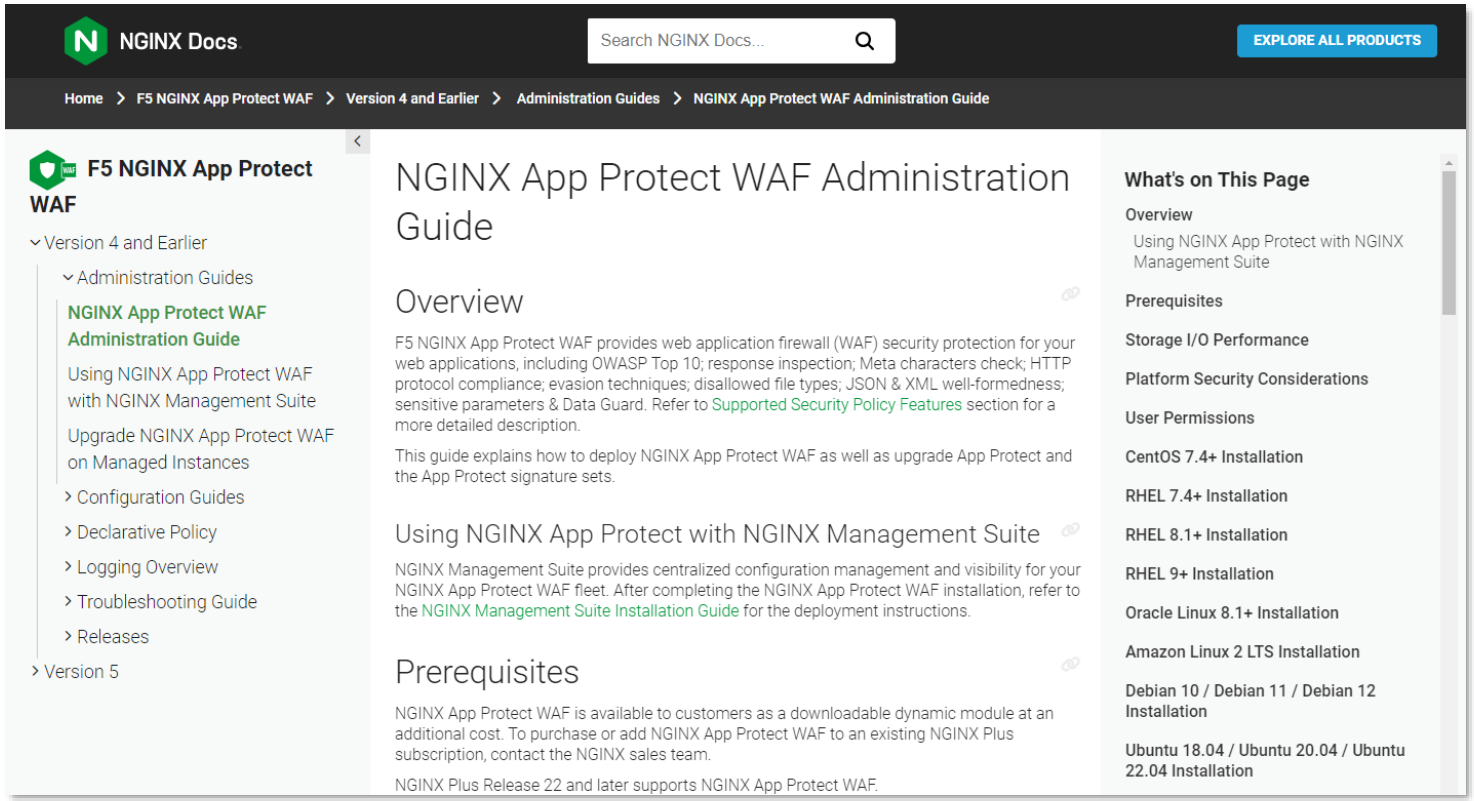
本日利用予定のパッケージの情報

Ubuntu 20.04

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

NGINX Docs：インストール前提条件（V4）

- 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

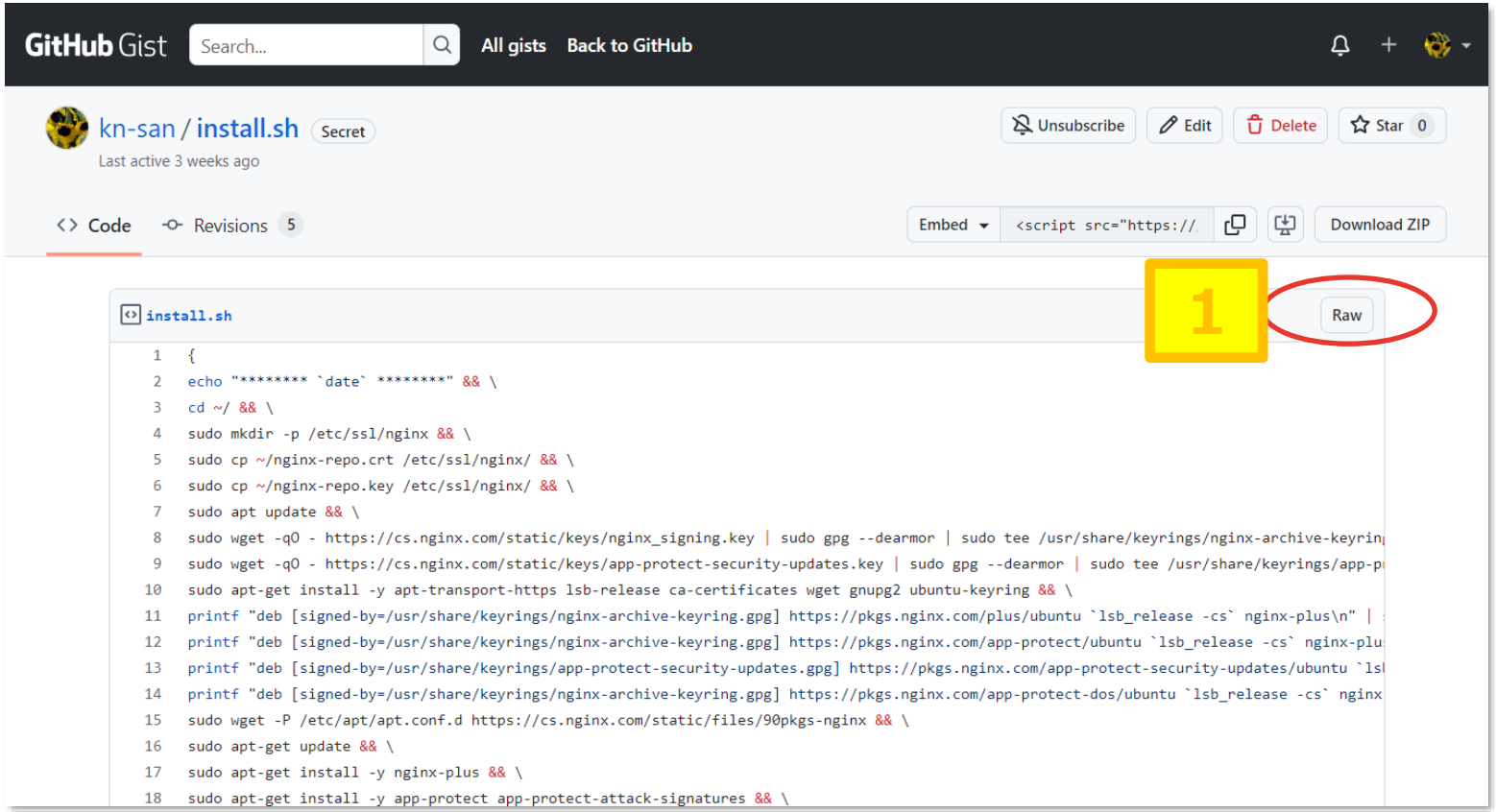
インストール（NGINX App Protect V4）

- *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. 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/ngx_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/ngx_http_app_protect_module.so;

http {
    server {
        listen       80;
②       app_protect_enable on;
③       app_protect_security_log_enable on;
④       app_protect_security_log "/etc/nginx/log-default.json" syslog:server=elk:5144;

        location /application01 {
            root   /usr/share/nginx/html;
⑤           app_protect_policy_file "/etc/nginx/security-policy.json";
            index  index.html index.htm;
        }
    }
}
```

NGINX App Protect WAF用のモジュールのロード

NGINX App Protect WAFの有効化

セキュリティログ出力の有効化

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

セキュリティポリシーファイルの設定

- 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。

NGINX App Protect WAF設定例：セキュリティポリシー（１）

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

NGINX App Protect WAF設定例：セキュリティポリシー（２）

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
         }
      ]
   }
}
```

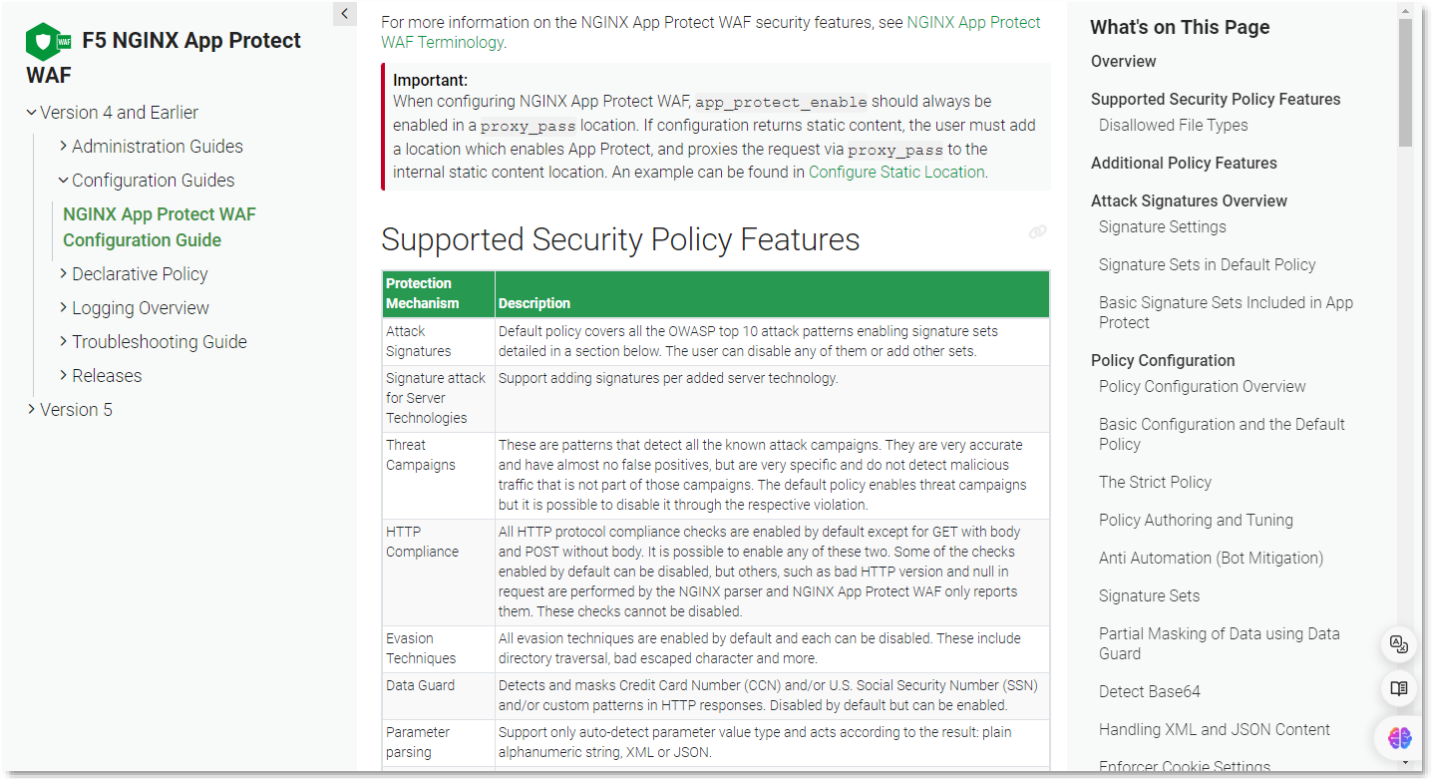
- NGINXの設定ファイル（conf）で“app_protect_policy_file”を指定しなかった場合には、/etc/app_protect/conf/NginxDefaultPolicy.json が自動で適用されます。
- “policy” > “name” は、システム内でユニークな名称である必要があります。
- ファイルのPathは、任意の場所を指定できます。

  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/

サポートされているセキュリティポリシー機能

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



F5 NGINX App Protect WAF

- Version 4 and Earlier
  - Administration Guides
  - Configuration Guides
    - NGINX App Protect WAF Configuration Guide
  - Declarative Policy
  - Logging Overview
  - Troubleshooting Guide
  - Releases
- Version 5

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

onnect Beyond

ハンズオン

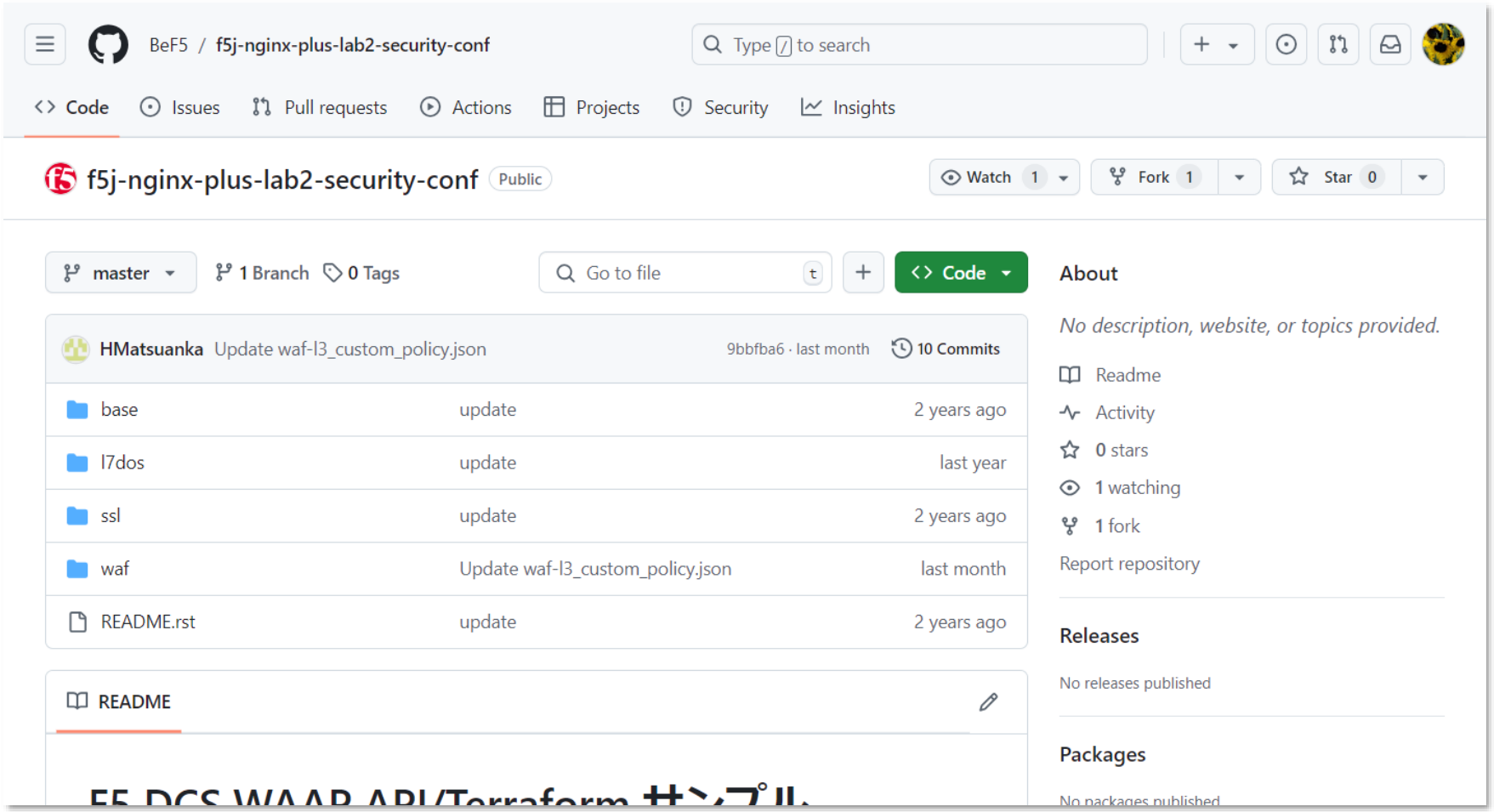
ハンズオンガイド（再掲）

- 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/

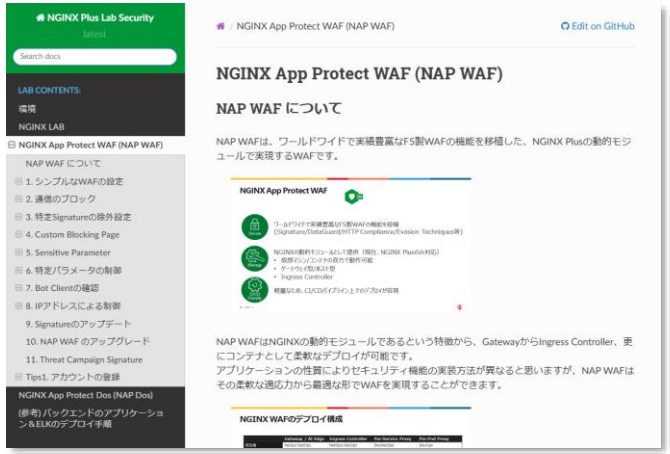
GitHub：BeF5/f5j-nginx-plus-lab2-security-conf

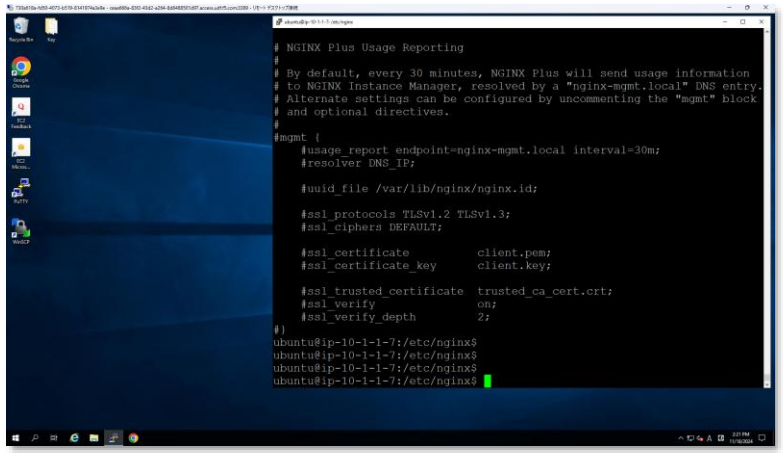
- 本ハンズオンセミナーで利用する各種設定ファイル

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



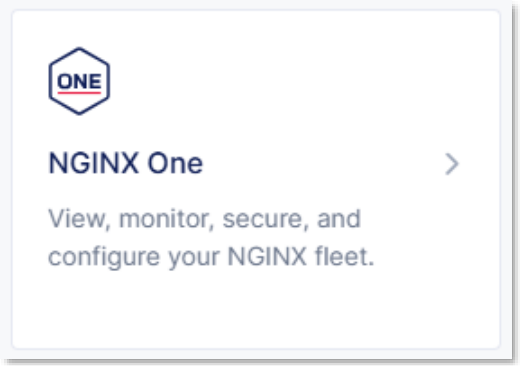
※ ハンズオンは、ハンズオンガイドのサイト と リモートデスクトップ環境 を使って進めていきます。





NGINX One Console のご紹介

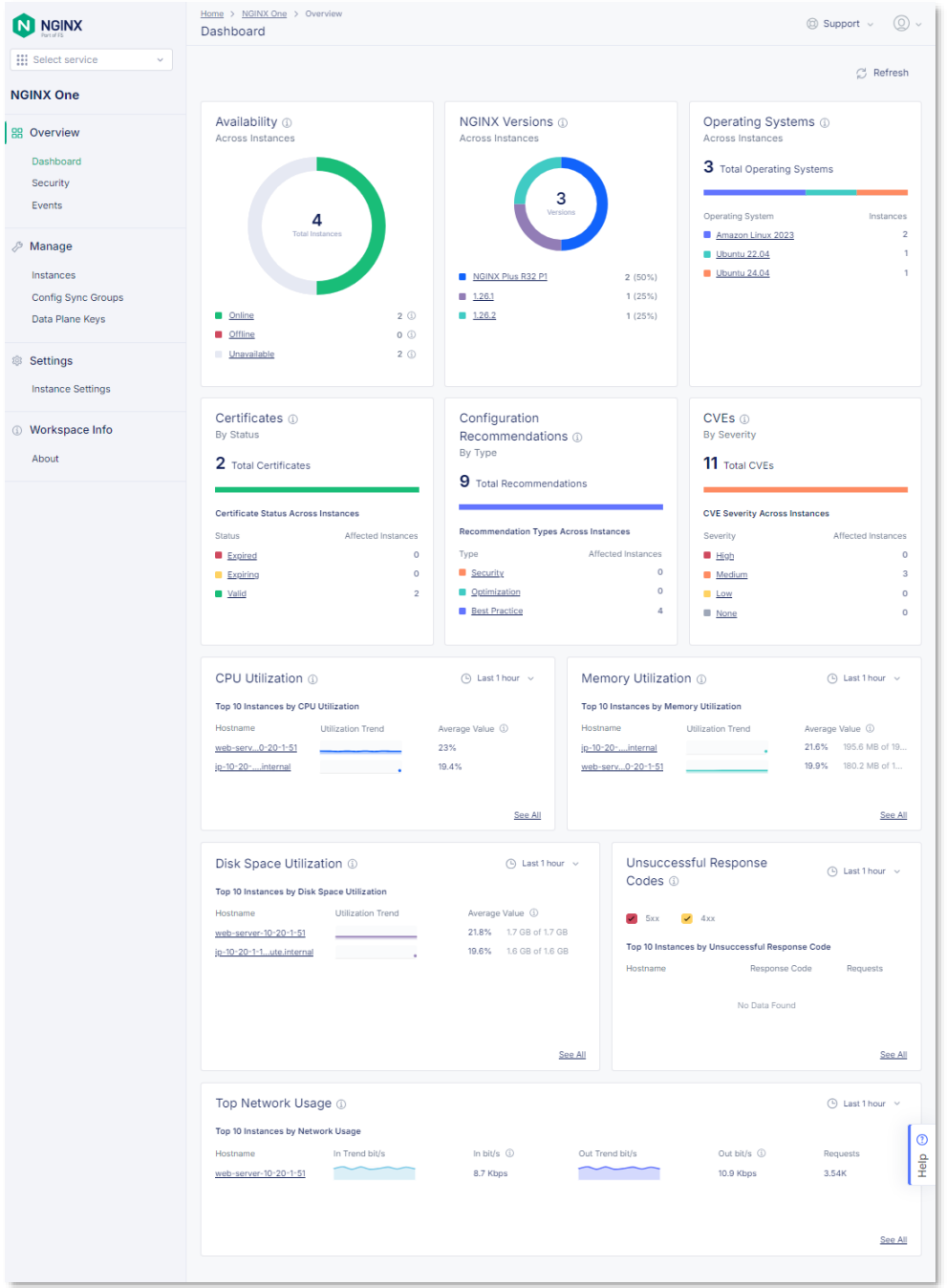
NGINX One Console（ 2024年9月GA！ ）



- NGINX One Console

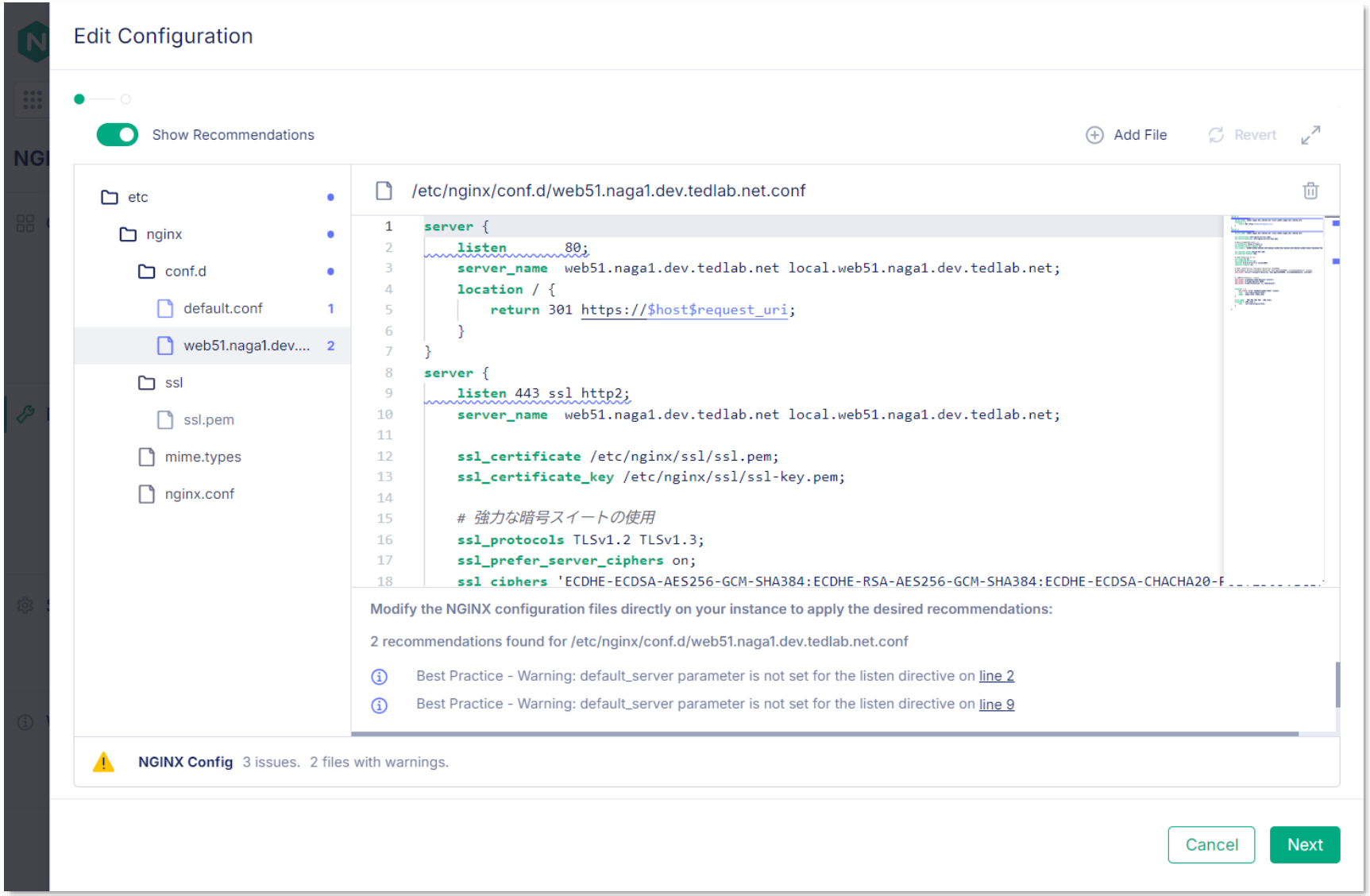
SaaS型で複数の NGINX Plus と NGINX Open Source インスタンスを単一のコンソールで管理する

- 設定の確認
- パフォーマンスメトリクスの追跡
- セキュリティ脆弱性（CVE）の特定
- SSL証明書の管理
- F5 Distributed Cloud Services（F5 XC）統合
- など



東京エレクトロン デバイス

NGINX One > Edit Configuration



- Edit Configuration

設定されたconfファイルの内容の参照・編集ができ、設定内容に関するリコメンデーションを提案するVS Codeライクなエディターを装備

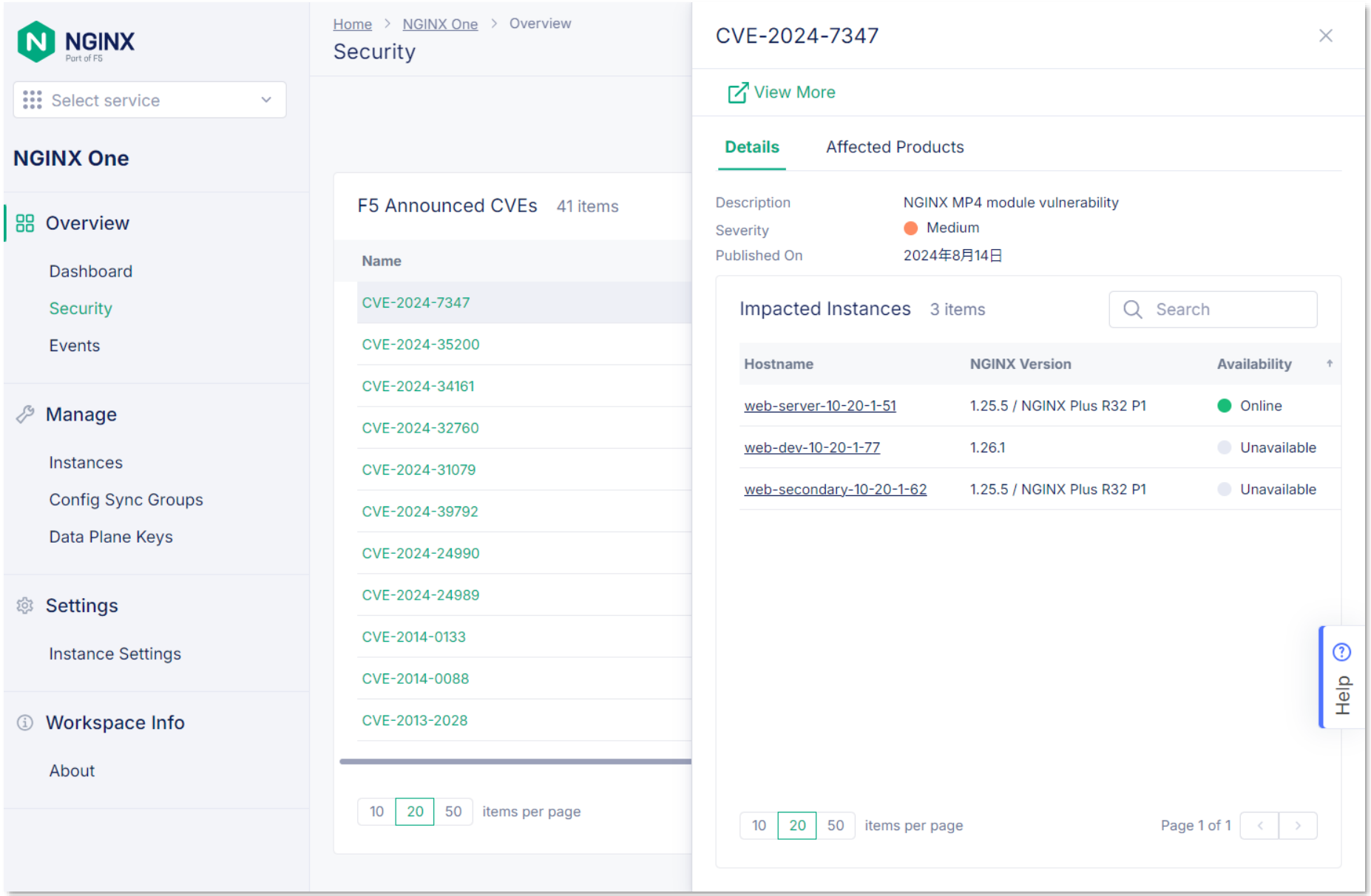
  - 編集後の設定内容のデプロイも可能（ファイルのアップロードと設定内容の読み込みの実行）
  - 変更箇所の差分表示

NGINX One > セキュリティ脆弱性（CVE）の特定

- Security

NGINXインスタンスに存在するCVEを特定

  - 各CVEに該当するインスタンスの表示
  - CVE情報
  - など



まとめ

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

無料！ハンズオントレーニング概要概要（Zoomオンラインセミナー）

各編 企業毎の
個別開催
実施可能！

基礎

イチから体験！ NGINXハンズオントレーニング
～基礎編～

＊ 毎月開催予定 → 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
～応用編～

応用

＊ 隔月にて開催予定 → 詳しく弊社ホームページにて！
https://cn.teldevice.co.jp/seminar/

WAF

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

＊ 隔月にて開催予定 → 詳しく弊社ホームページにて！
https://cn.teldevice.co.jp/seminar/

東京エレクトロン デバイス

NGINXの情報発信しています！

NGINXがまるっと分かる！ブログ更新中！

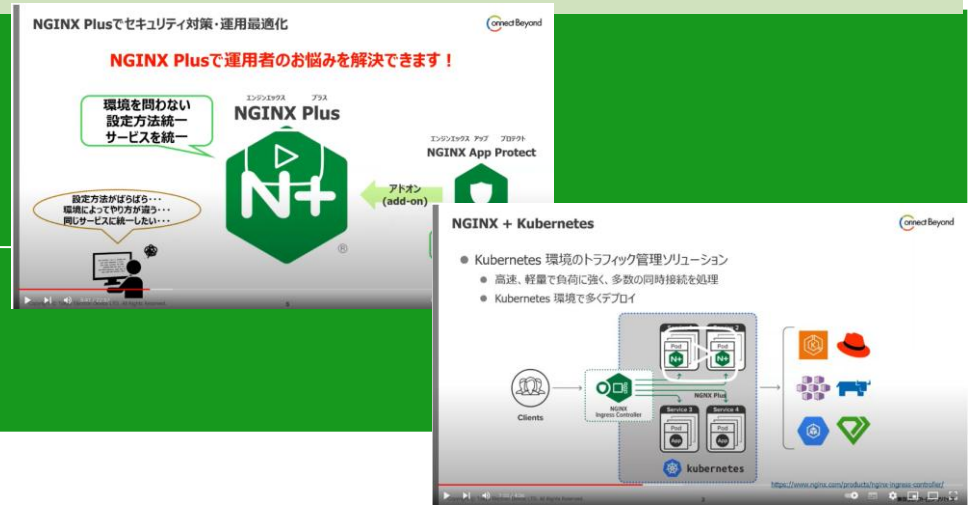
https://cn.teldevice.co.jp/blog/search/?q=NGINX

ブログ

YouTube

NGINXを簡単解説！

F5 NGINX - YouTube



東京エレクトロン デバイス

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

セッション資料/アンケートについて

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