情報セキュリティ基礎

第8回　ネットワークトラブル解決の実践

藤本 章宏

これまでの振り返り

様々なレベルで送信元の偽装（なりすまし）

例：偽のWebサイトにアクセスさせられた

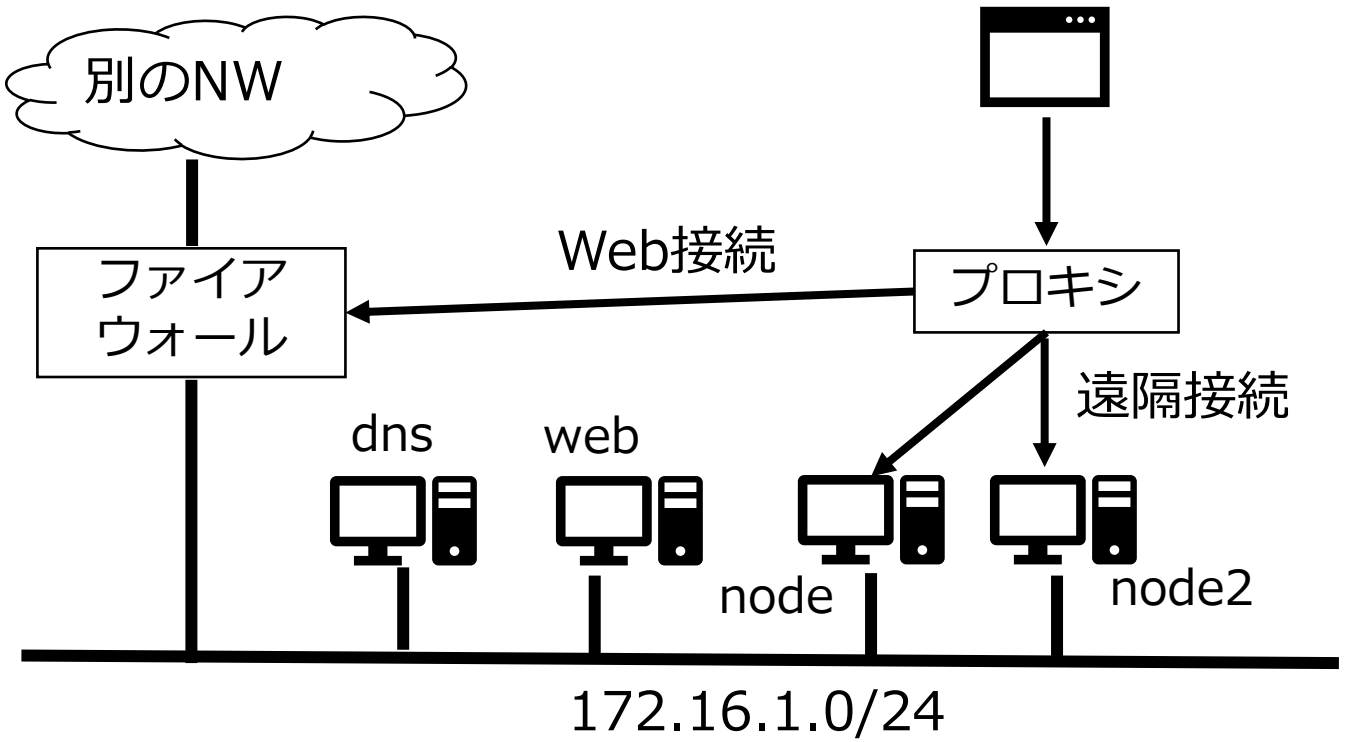
- URLがまぎらわしいものだった？
- 偽のDNSサーバにより、DNSキャッシュサーバが汚染された？
- IPアドレスは正しいけど、別のサーバに誘導された？

何が起こっているのかを見極め、
トラブルの原因を切り分けることが重要

演習環境

演習環境にアクセス

今回は**final01**内にある
f01_node と f01_node2 を使用



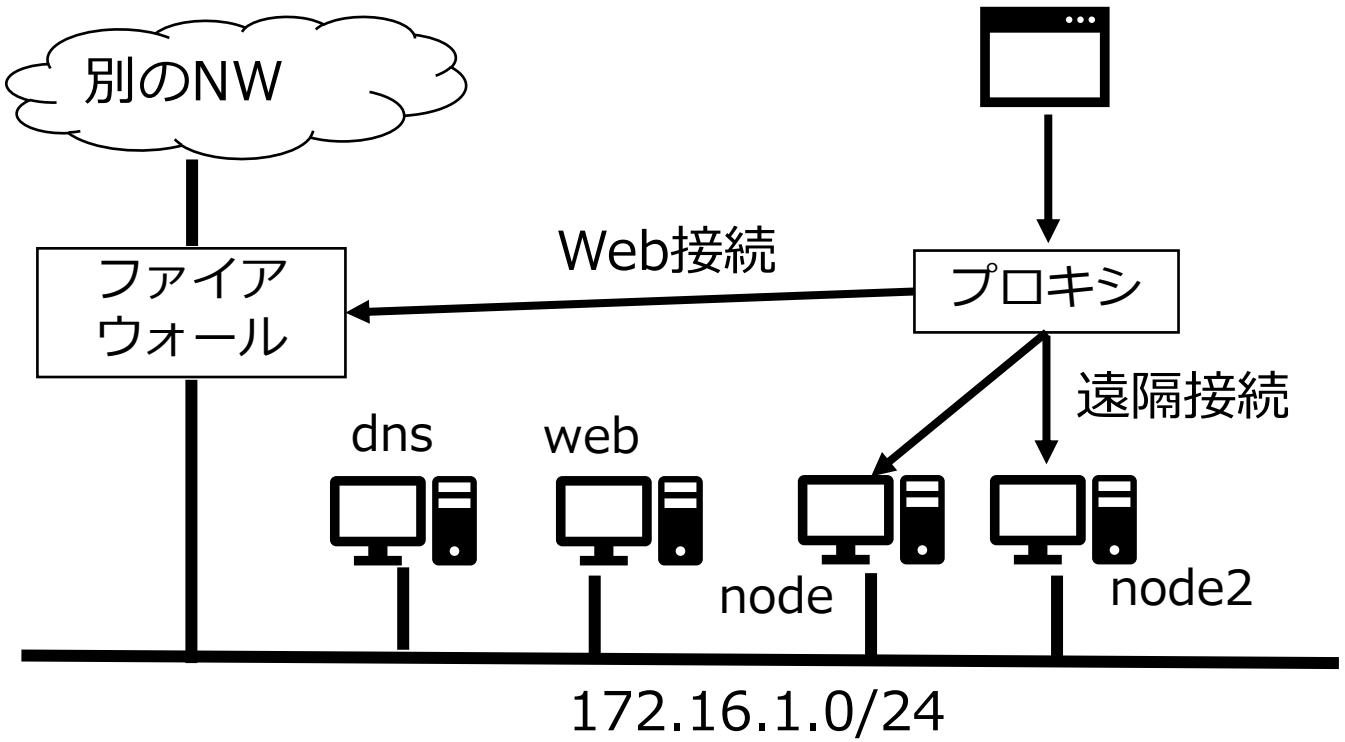
node.enshuは10秒間隔で
http://web.enshu/ にデータをPOST
(センサデータを送信するイメージ)

ホスト名	IPアドレス
node.enshu	172.16.1.1
node2.enshu	172.16.1.100
dns.enshu	172.16.1.53
web.enshu	172.16.1.80
ファイアウォール	172.16.1.254
	192.168.100.4

演習 1

演習環境にアクセス

今回は**final01**内にある
f01_node と f01_node2 を使用



node.enshu から送信されているデータが
見知らぬWebサーバで公開されているという
通報を受けました

データ掲載先: https://**********

1. node.enshuに遠隔接続して，データの
   送信先のIPアドレスを特定してください

2. ファイアウォールにアクセスして，
   1.で特定したIPアドレス宛の通信を
   ブロックしてください

※ 掲載先を再読み込みしても新しいデータが
追加されていなければ成功

node.enshuは10秒間隔で
http://web.enshu/ にデータをPOST
（センサデータを送信するイメージ）

外向きパケットの遮断


ロビー
レポート
システム
インタフェース
ファイアウォール
エイリアス
Automation
カテゴリー
グループ
NAT
ルール
フローティング
LAN
LANBRIDGE
OPT1
WAN
ループバック
Shaper
設定
ログファイル
診断
VPN
サービス
電源
ヘルプ
ファイアウォール: ルール: WAN
Inspect
プロトコル
送信元
ポート
送信先
ポート
ゲートウェイ
スケジュール
説明
Automatically generated rules
IPv4 *
許可
許可 (無効)
拒否
拒否 (無効)
拒絶
拒絶 (無効)
ログ
ログ (無効)
IN
OUT
最初に一致
最後に一致
Active/Inactive Schedule (click to view/edit)
エイリアス (クリックして表示 / 編集)
WAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.
② ＋ボタンを選択して、遮断ルールを作成
①「ファイアウォール」＞「ルール」＞「WAN」を選択

外向きパケットの遮断


root@OPNsense.localdomain
ロビー
レポート
システム
インタフェース
ファイアウォール
エイリアス
Automation
カテゴリー
グループ
NAT
ルール
フローティング
LAN
LANBRIDGE
OPT1
WAN
ループバック
Shaper
設定
ログファイル
診断
VPN
サービス
電源
ヘルプ
ファイアウォール: ルール: WAN
ファイアウォールルールの編集
全てのヘルプ
動作
拒否
無効
このルールを無効
クイック
一致したら、すぐに動作を適用します。
インタフェース
WAN
方向
out
TCP/IP バージョン
IPv4
プロトコル
TCP
送信元 / 反転
このオプションを使用すると、一致する意味が逆になります。
送信元
任意
送信元
詳細設定
送信先 / 反転
このオプションを使用すると、一致する意味が逆になります。
送信先
単一ホストもしくはネットワーク
ブロックしたいIPアドレス
24
送信先ポート範囲
from:
to:
任意
任意
③ 動作を「拒否」に設定
④ 方向を「out」に設定
⑤ 送信先を
「単一ホストもしくはネットワーク」
「遮断したいIPアドレス」
「32」

演習 2

なぜ，外部のIPアドレスにデータが
送信されていたのかを調査してください

また，どうすればその原因を取り除けるか
考えてください

今回は**final01**内にある
f01_node と f01_node2 を使用