

# Brounie Hound

## 操作ガイド

CT4B 3班

# 目次

使用前の準備

---

メール設定

---

ルールグループの設定方法

---

キャプチャ・検知機能

---

この資料で使用している画面は開発中のもので、実際に使用される画面とは異なる場合があります。

[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キヤフ・チャ・検知機能](#)

# 使用前の準備

## WireSharkの導入方法

[目次に戻る](#)

[使用前の準備](#)

[メール設定](#)

[ルールグループの設定方法](#)

[キャプチャ・検知機能](#)

BrownieHoundを使用いただく前に、  
WireSharkを導入する必要があります。  
下記のリンクもしくはアイコンからWireSharkの  
ダウンロードページに飛んでください。



<https://www.wireshark.org/download.html>

# WireSharkの導入方法

[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キャプチャ・検知機能](#)

We're now a non-profit! Support open source packet analysis by making a donation.

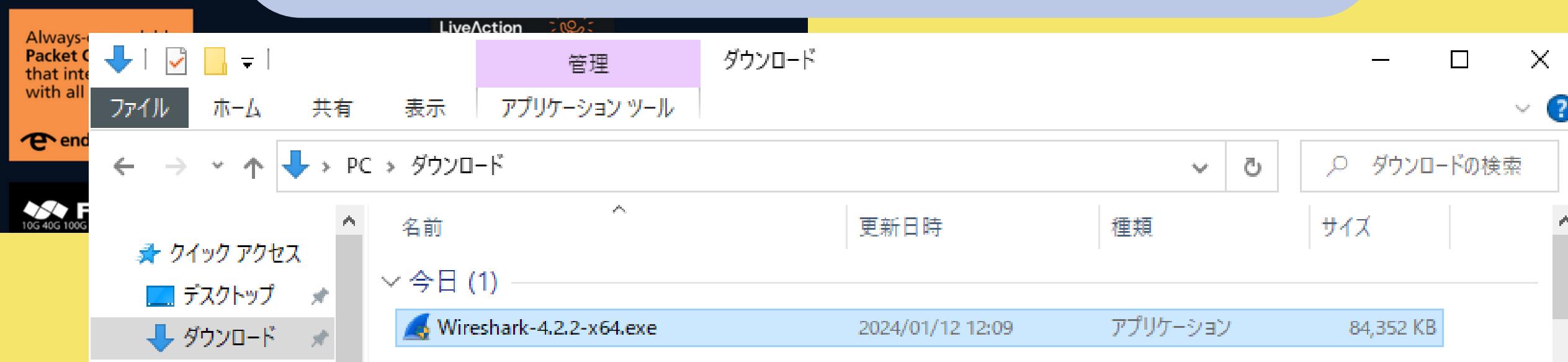
News Learn SharkFest Get Acquainted ▾ Get Help ▾ Develop ▾ Shop Members

## Download Wireshark

The current stable release of Wireshark is 4.2.2. It supersedes all previous releases.

- ▼ Stable Release: 4.2.2
  - Windows x64 Installer
  - Windows Arm64 Installer
  - Windows x64 PortableApps®
  - macOS Arm Disk Image
  - macOS Intel Disk Image
  - </> Source Code
- ▶ Old Stable Release: 4.0.12
- ▶ Documentation

こちらの画面からお使いのバージョンに合わせたものをダウンロードしていただき、ダウンロードした Wireshark-〇〇.exeを起動して、指示通りに導入を進めてください。



[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キヤフ・チャ・検知機能](#)

# メール設定

[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キャプチャ・検知機能](#)

## メール設定画面の表示方法



[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キャプチャ・検知機能](#)

## メール設定画面の操作方法



ユーザーネームを入力してください  
認証メールに使用します。

ユーザーネーム

ここでメール送信をオンにできます  
(初期状態ではオフになっています)

送信スパン

BrownieHound



10 分毎 10

メールの送信間隔を設定できます  
お好みの時間を設定してください

送信先メールアドレス

BrownieHound2024@gmail.com

※「Browniehound」  
認識されている場  
すがご確認いただけ

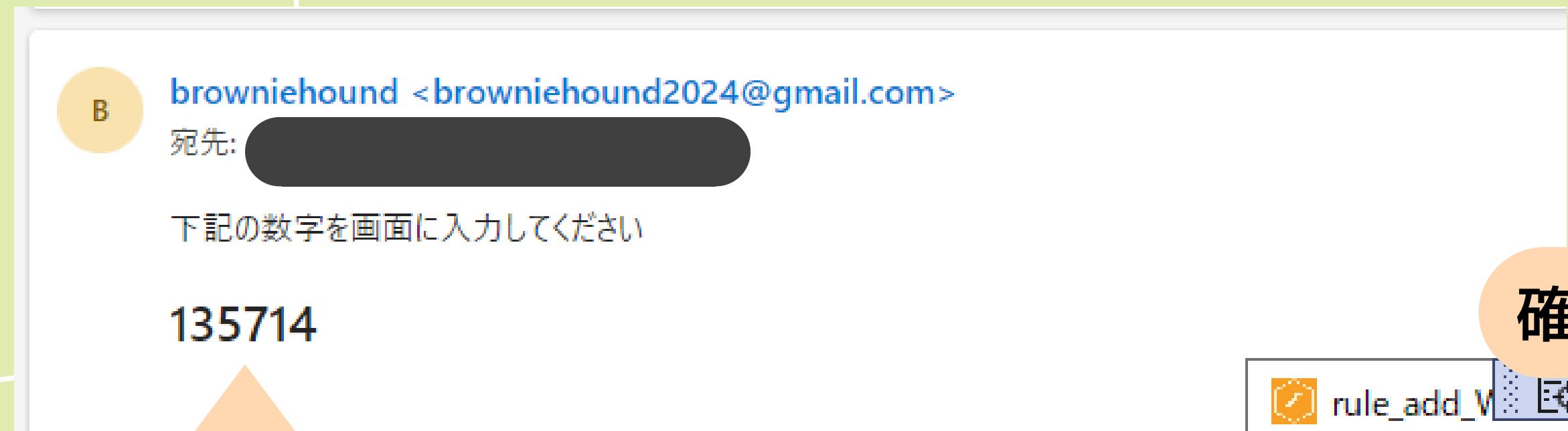
お使いのメールアドレスを入れてください

戻る

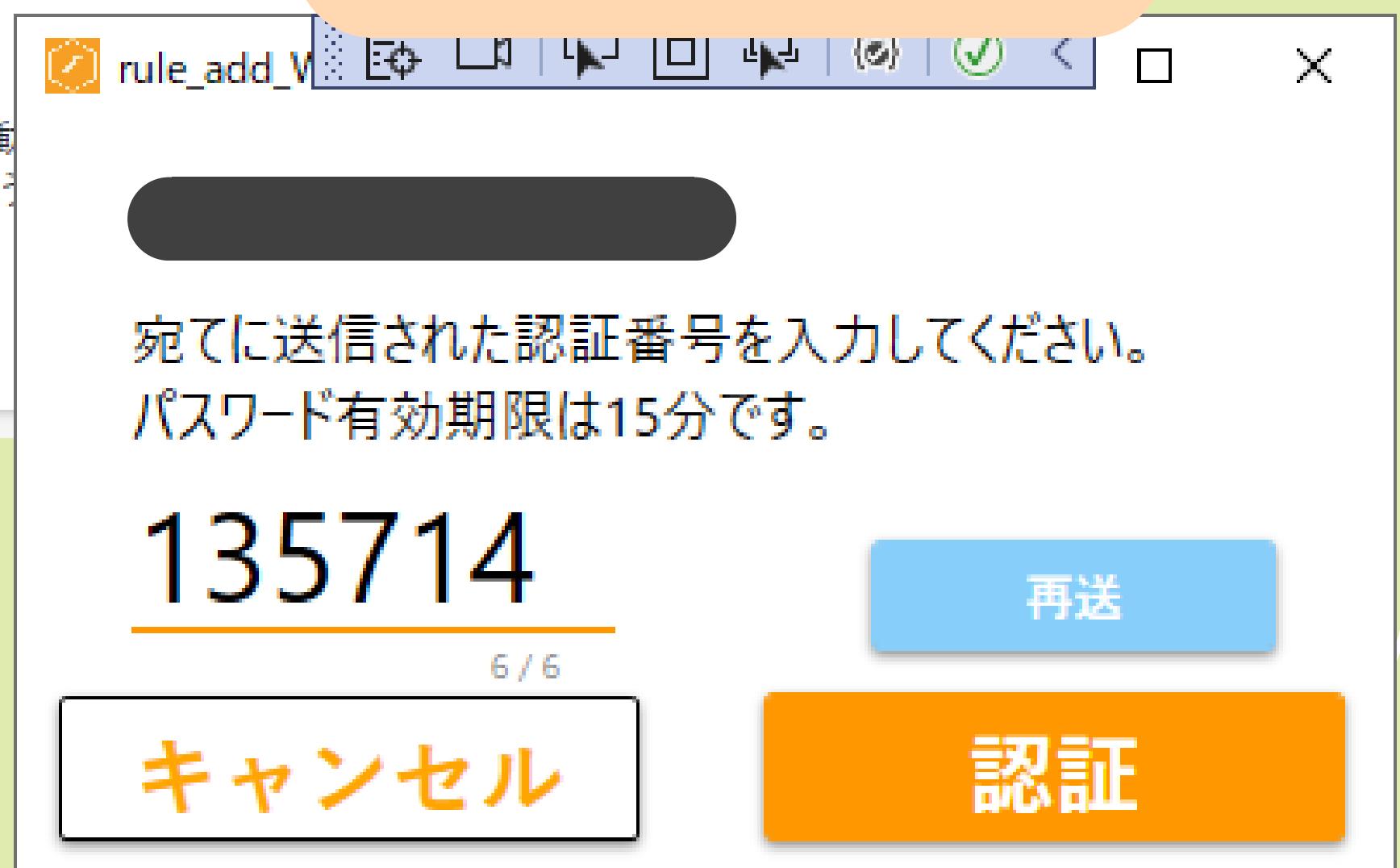
確定

## メール設定画面の操作方法

[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キャプチャ・検知機能](#)



入力されたアドレスにメールが送られるので  
この数字をBrownieHoundに  
15分以内に入力してください。



確定したら認証は完了です

## メール設定画面の操作方法

[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キャプチャ・検知機能](#)

A screenshot of an email client interface. The subject is "の定期検知メール-0". The message body contains a table titled "Link Rule" and "New\_rule". A large orange callout bubble points to the table with the text "このようなメールが届きます".

browniehound  
宛先: [REDACTED]

2024/01/22 (月) 14:51

の定期検知メール-0

こののようなメールが届きます

時間：2024/01/22 14:50:49  
総キャプチャ数：81501

Link Rule

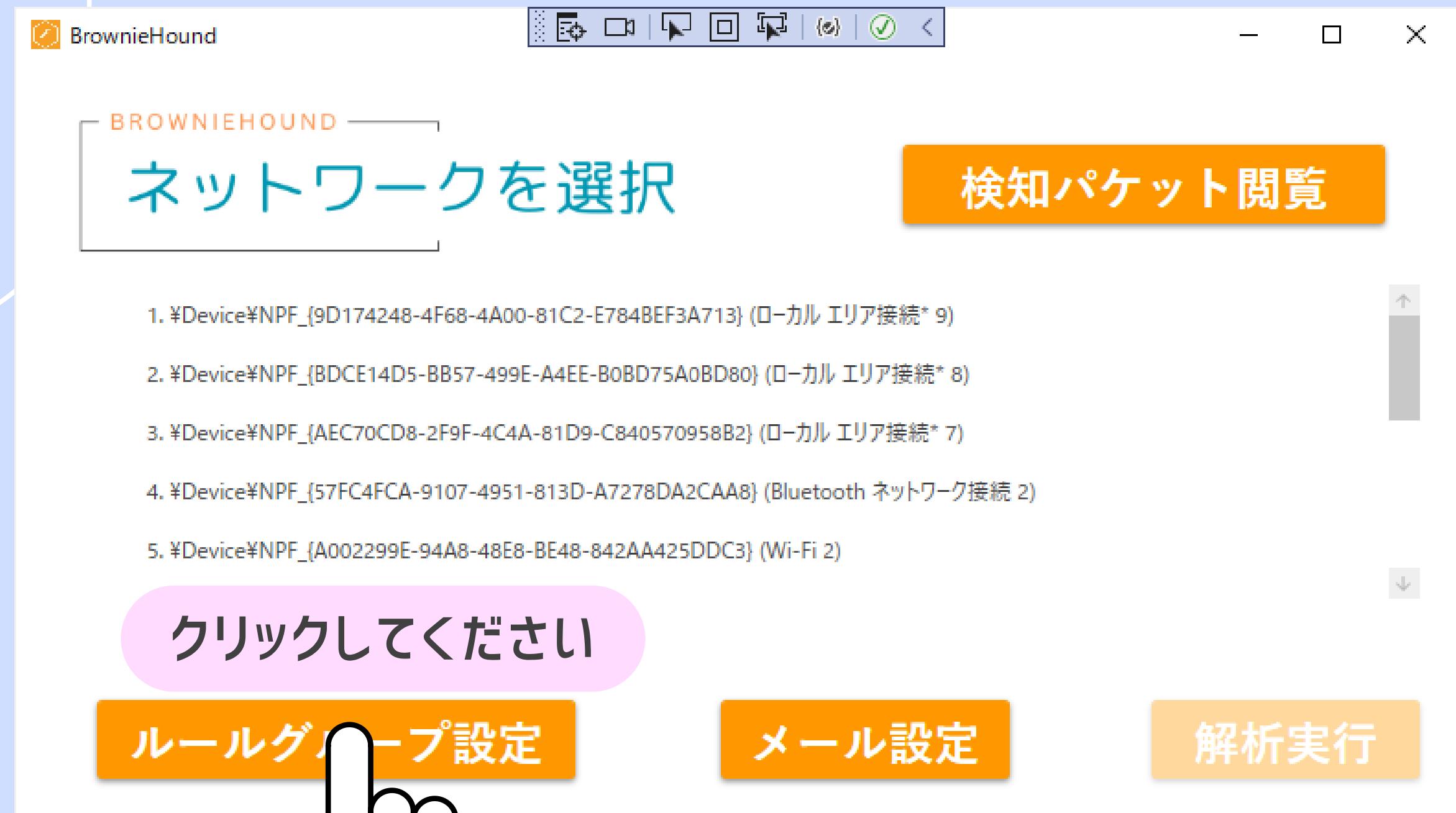
New\_rule

No	Category	Time	間隔(s)	頻度	Source	Destination	Protocol	sourcePort	destPort	Length
0	black	0	10	20	all	192.168.194.32	all	all	all	100
1	white	0	1	1	all	all	UDP	all	all	none
4		2024-01-22 14:40:50.0338			192.168.194.130	192.168.194.32	DNS	53	52446	338
5		2024-01-22 14:40:50.061823			192.168.194.130	192.168.194.32	DNS	53	63153	197
6		2024-01-22 14:40:50.061823			192.168.194.130	192.168.194.32	DNS	53	52047	242
33		2024-01-22 14:40:50.258937			192.168.194.130	192.168.194.32	DNS	53	61685	212
34		2024-01-22 14:40:50.26492			192.168.194.130	192.168.194.32	DNS	53	63304	167
35		2024-01-22 14:40:50.26492			192.168.194.130	192.168.194.32	DNS	53	63068	212
69		2024-01-22 14:40:50.396338			192.168.194.130	192.168.194.32	DNS	53	58683	283

[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キヤフ・チャ・検知機能](#)

# ルールグループの設定方法

## ルールグループ設定画面の表示方法



[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キャプチャ・検知機能](#)

## ルールグループの追加・編集

BrownieHound

BROWNIEHOUND

### ルールグループの設定

<input type="checkbox"/> すべて選択	No	Name	ruleItems
--------------------------------	----	------	-----------

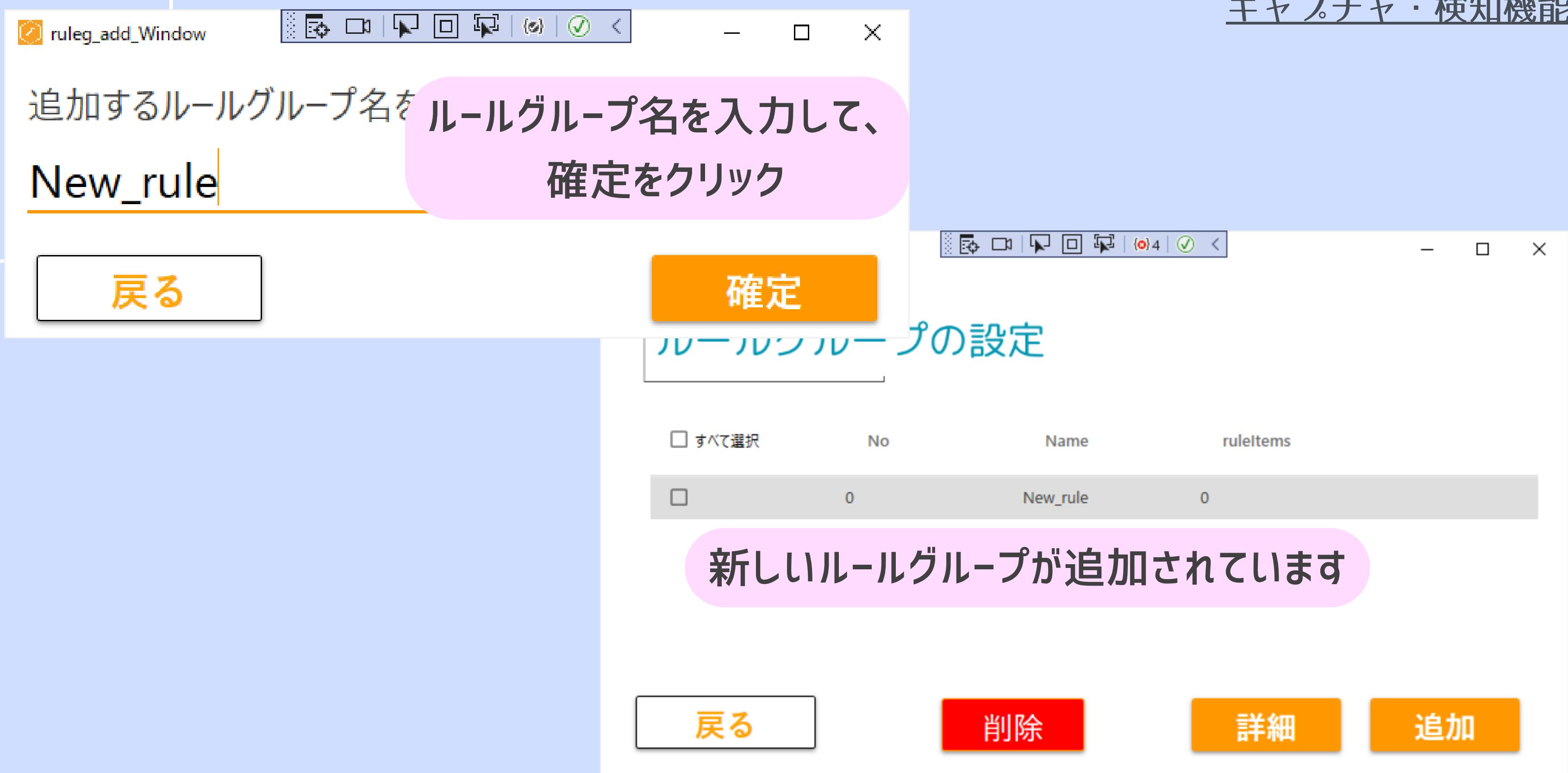
戻る 削除 詳細 追加



[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キャプチャ・検知機能](#)

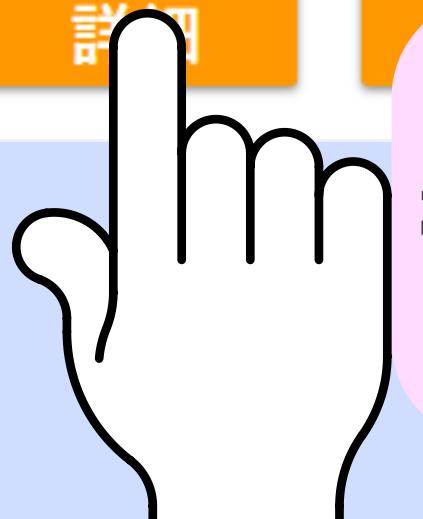
## ルールグループの追加・編集

[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キャプチャ・検知機能](#)



## ルールグループの追加・編集

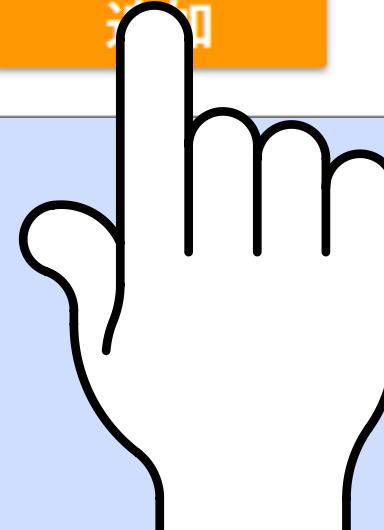
[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キャプチャ・検知機能](#)



追加したルールグループの編集をするときは、編集するルールグループを選んで詳細をクリック

[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キャプチャ・検知機能](#)

## ルールグループの追加・編集



[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キャプチャ・検知機能](#)

## ルールグループの追加・編集

検知方式を設定します

検出>通信を検知した場合

否検出>検知されなかった場合

プロトコルを設定します

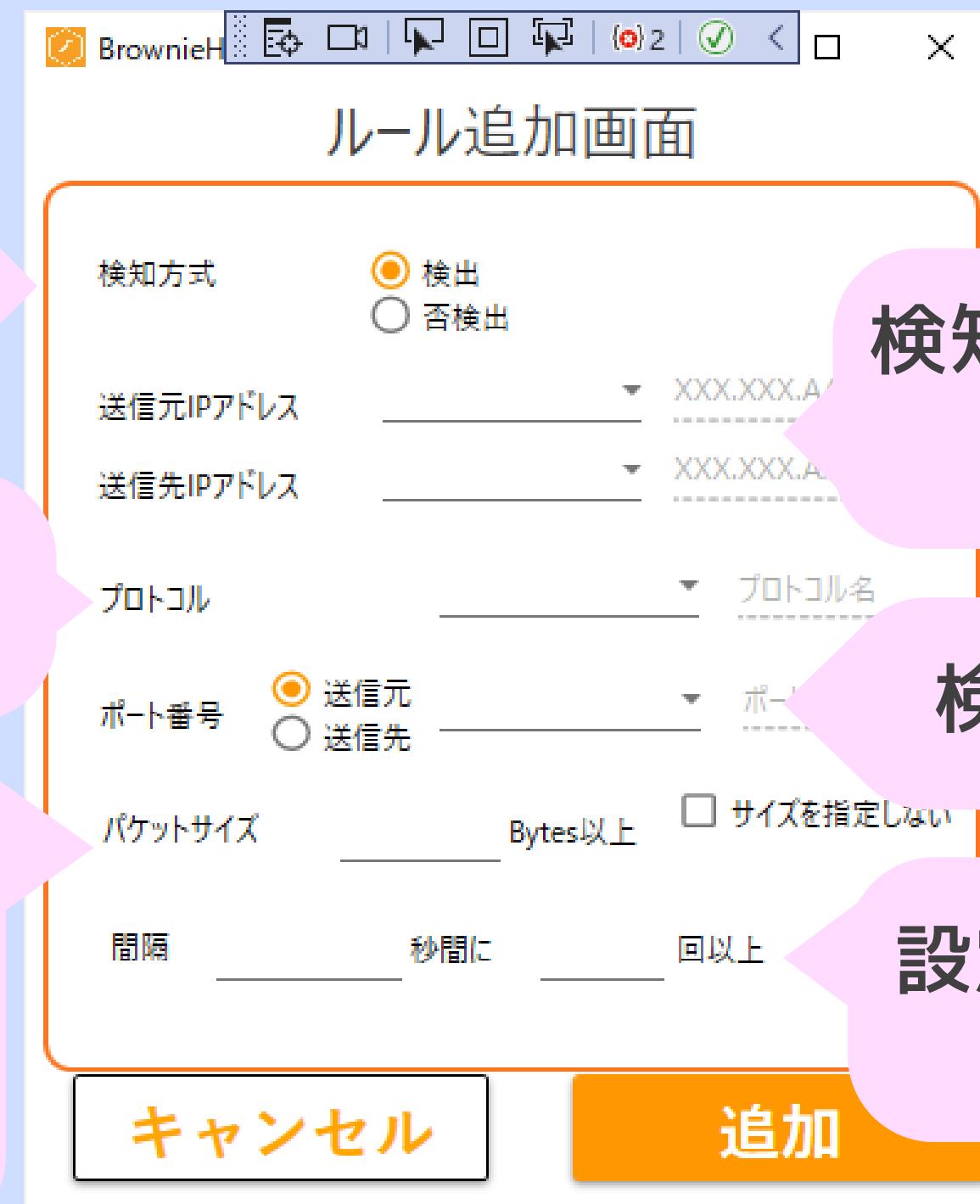
HTTP,SSH等

検知する通信のパケットサイズ

(1~9999までの数値)

もしくは指定なし)

と通信間隔を設定してください



検知したい通信の送信元、送信先の  
IPアドレスを設定してください

検知するポート番号を設定します

設定が終わったら追加を押して  
確定してください

[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キャプチャ・検知機能](#)

## ルールグループの追加・編集



ルールを修正したい場合はルールを選択して  
編集を、削除する場合は削除をクリック

[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キャプチャ・検知機能](#)

## ルールグループの追加・編集

複数のルールを設定した場合、ルールのグループ化にチェックを入れることで、全てのルールの条件を満たした場合のみ検知するようにできます。

ルール詳細 New\_rule

すべて選択  ルールのグループ化

番号	検出可否	送信元IP	送信先IP	プロトコル	送信元ポート番号	送信先ポート番号	検知時間(s)	検知回数	サイズ
1	検出	all	myAddress	all	all	all	10	20	100
2	否検出	all	all	UDP	all	all	1	1	none

**名前の修正**

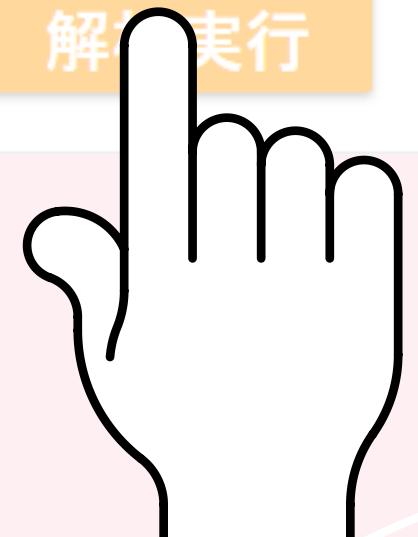
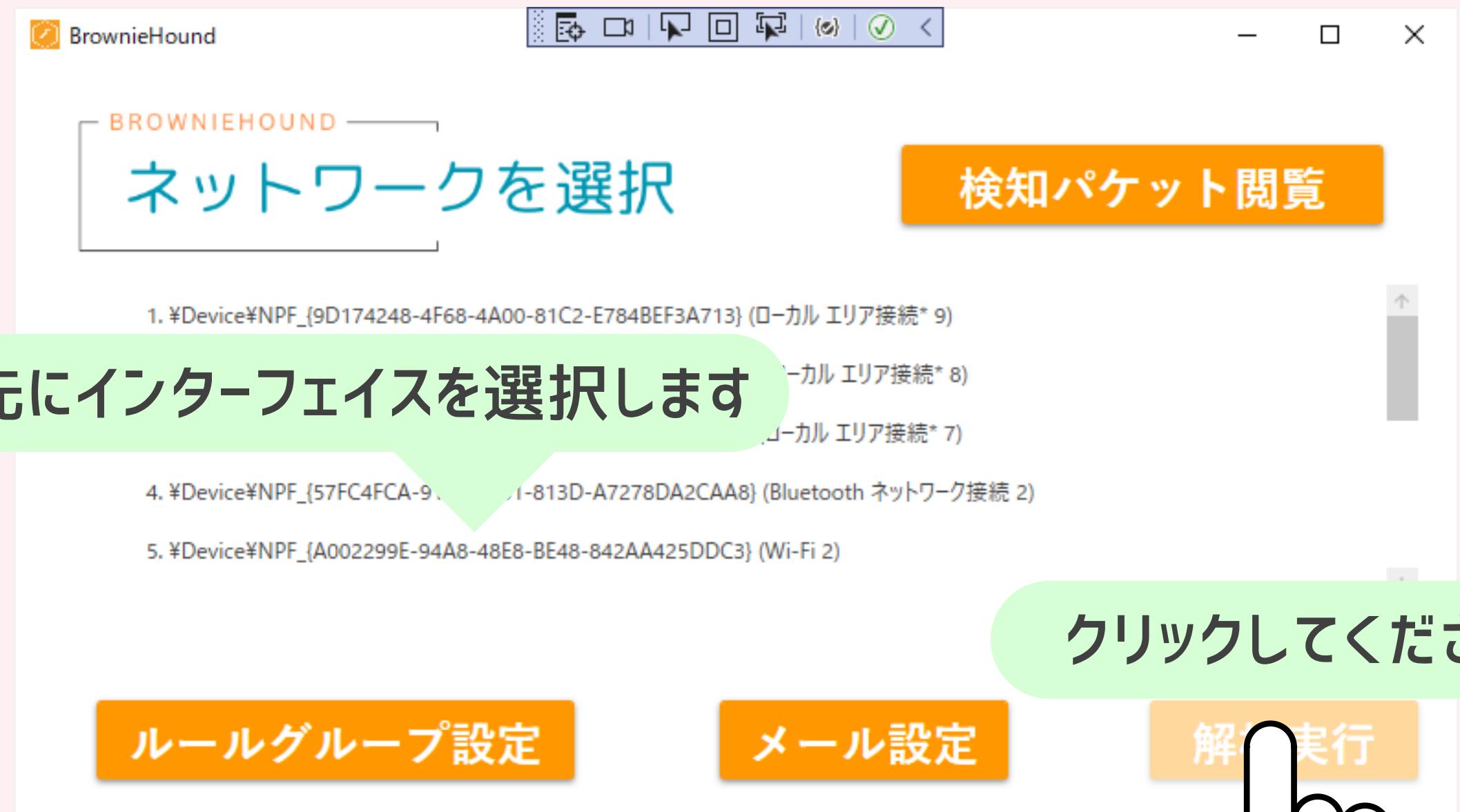
**戻る** **削除** **編集** **追加**

[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キャプチャ・検知機能](#)

# キャプチャ・検知機能

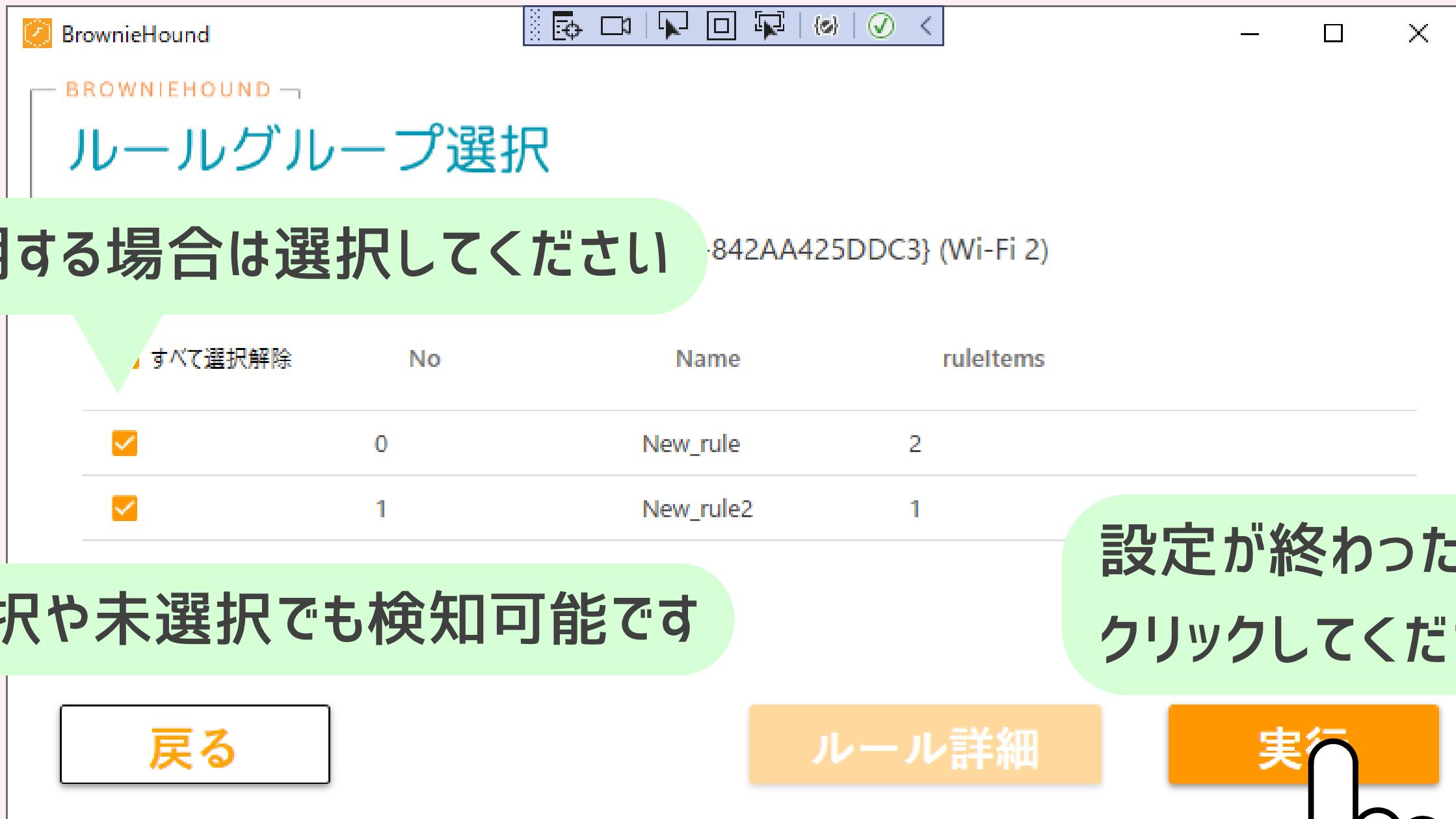
[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キャプチャ・検知機能](#)

## キャプチャ画面の表示方法



[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キャプチャ・検知機能](#)

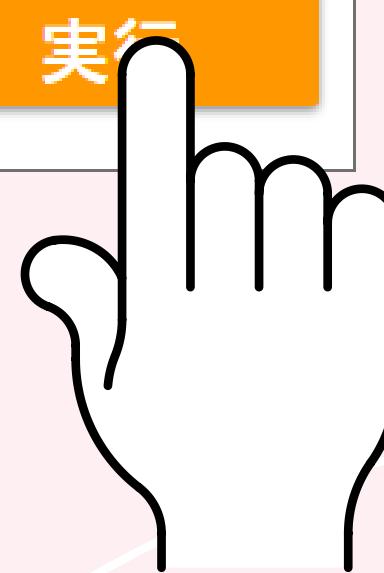
## キャプチャ画面の表示方法



The screenshot shows the BrownieHound application window titled "BrownieHound". The main content area is titled "ルールグループ選択" (Rule Group Selection). A message at the top right says "ルールを適用する場合は選択してください" (Please select if you want to apply rules). Below this, a table lists two rule groups:

No	Name	ruleItems
0	New_rule	2
1	New_rule2	1

A green callout bubble points to the first row with the text "ルールは複数選択や未選択でも検知可能です" (Rules can be selected multiple times or not selected, and detection is possible). Another green callout bubble points to the "実行" (Execute) button with the text "設定が終わったらクリックしてください" (Click after settings are completed). At the bottom, there are three buttons: "戻る" (Back), "ルール詳細" (Rule Details), and the highlighted "実行" (Execute) button.



## キャプチャ画面の使用方法

[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キャプチャ・検知機能](#)

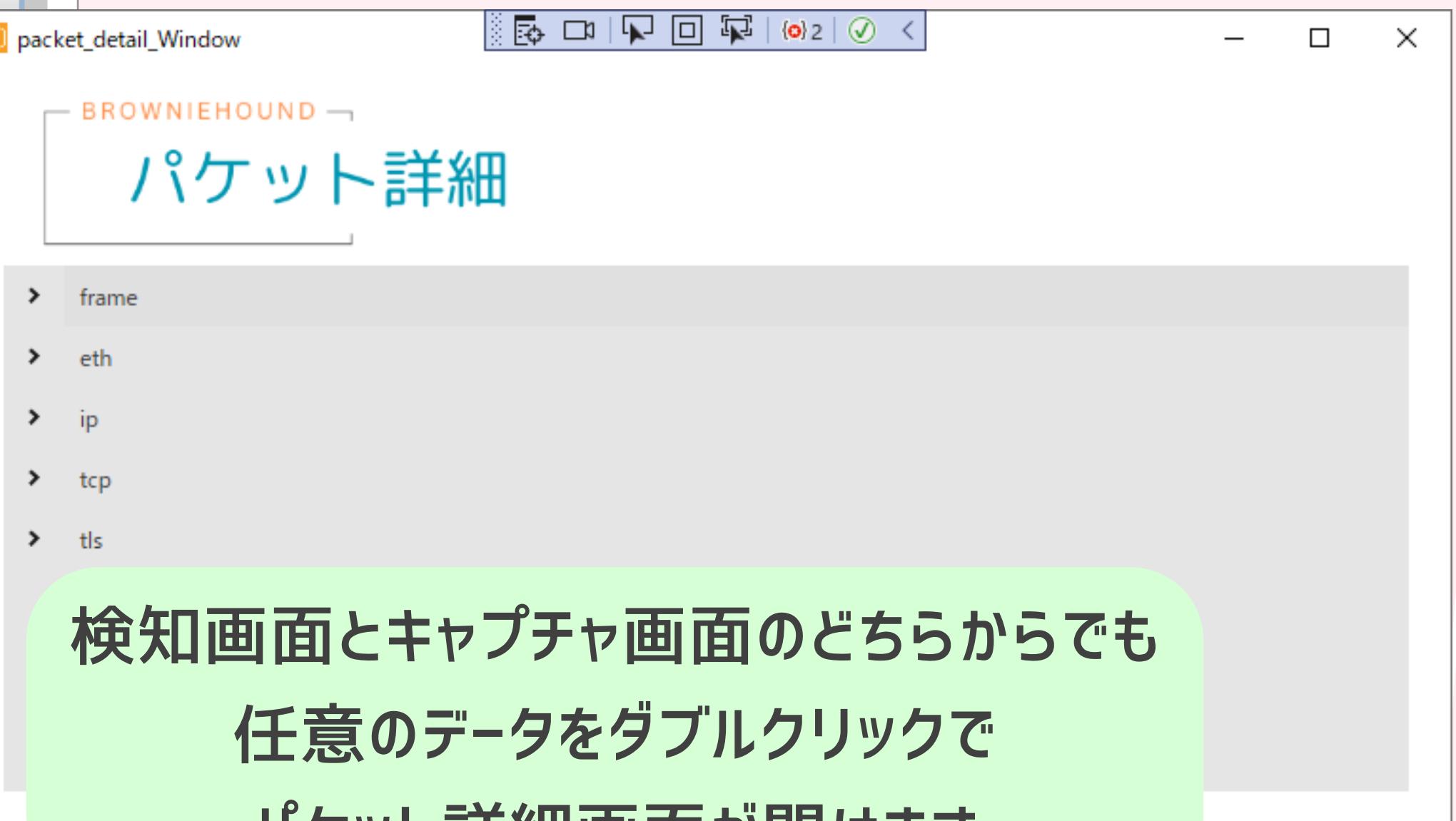
The screenshot shows the BrownieHound application interface. At the top left is the title bar "BrownieHound". Below it is a toolbar with icons for zoom, search, and file operations. The main window has a header "BROWNIIEHOUND 検知パケット". A large orange button labeled "保存" (Save) is positioned in the center. On the left, there is a tree view under the heading "LinkRuleGroup:New\_rule" showing two rules: "rule1" and "rule2". Rule 1 is expanded, showing its details: "0:[category:black][interval:10][count:20][source:all][destination:10.18.24.107][protocol:all][sourceport:all][destport:all][length:100]" and "1:[category:white][interval:1][count:1][source:all][destination:all][protocol:UDP][sourceport:all][de...". A green callout bubble points to this expanded rule area with the text "ここを展開することで検知ルールに引っかかった通信が表示されます" (By expanding here, the communication that triggered the detection rule will be displayed). On the right side of the interface, there is another window titled "BROWNIIEHOUND キャプチャ" showing a list of captured network packets. The table has columns: time, Source, Destination, Protocol, and Length. The first four rows of the table are:

time	Source	Destination	Protocol	Length
308	10.18.24.104	224.0.0.251	MDNS	128
309	fe80::186d:382f:9a73:d099	ff02::fb	MDNS	148
310	00:00:cd:37:00:01	ff:ff:ff:ff:ff:ff	ARP	56

At the bottom of the interface are several buttons: "終了" (Exit), "停止" (Stop), "閲覧切替" (View Switch), and another "停止" (Stop) button.

[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キャプチャ・検知機能](#)

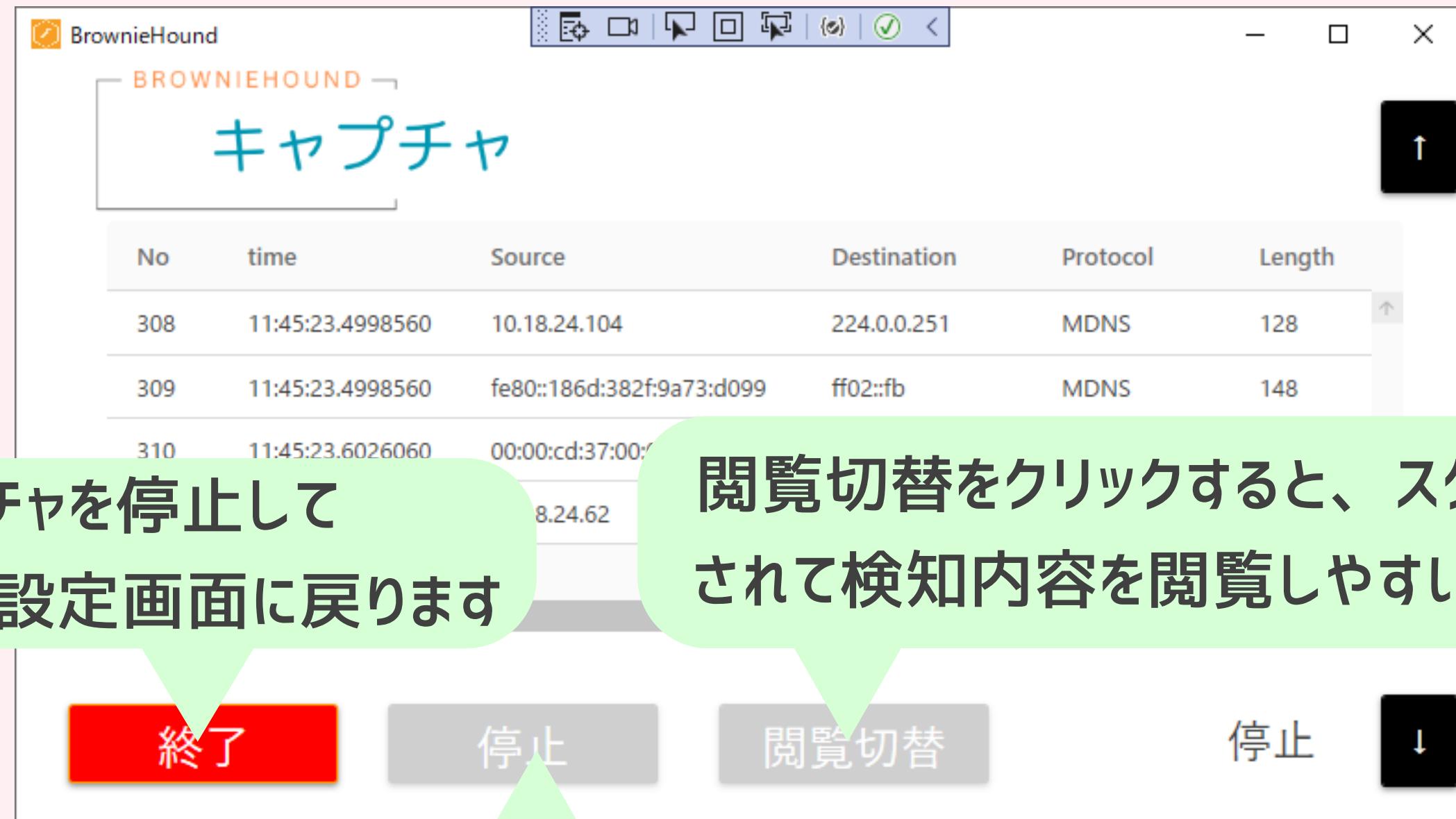
## キャプチャ画面の使用方法



検知画面とキャプチャ画面のどちらからでも  
任意のデータをダブルクリックで  
パケット詳細画面が開けます

[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キャプチャ・検知機能](#)

## キャプチャ画面の使用方法



キャプチャを停止して  
ルールグループ設定画面に戻ります

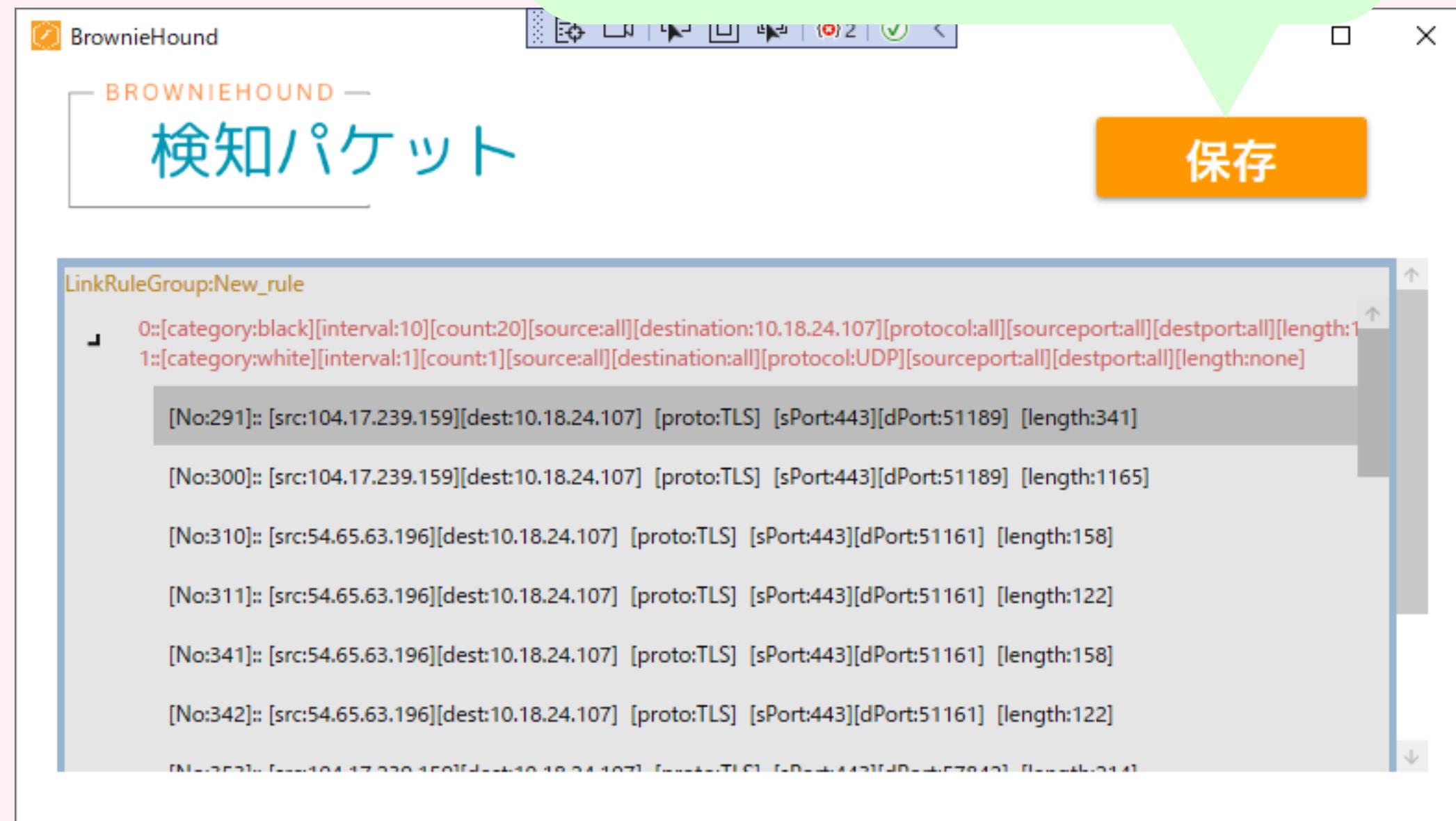
閲覧切替をクリックすると、スクロールが停止  
されて検知内容を閲覧しやすいようになります

停止をクリックすると、キャプチャが停止されます

[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キャプチャ・検知機能](#)

## キャプチャ画面の使用方法

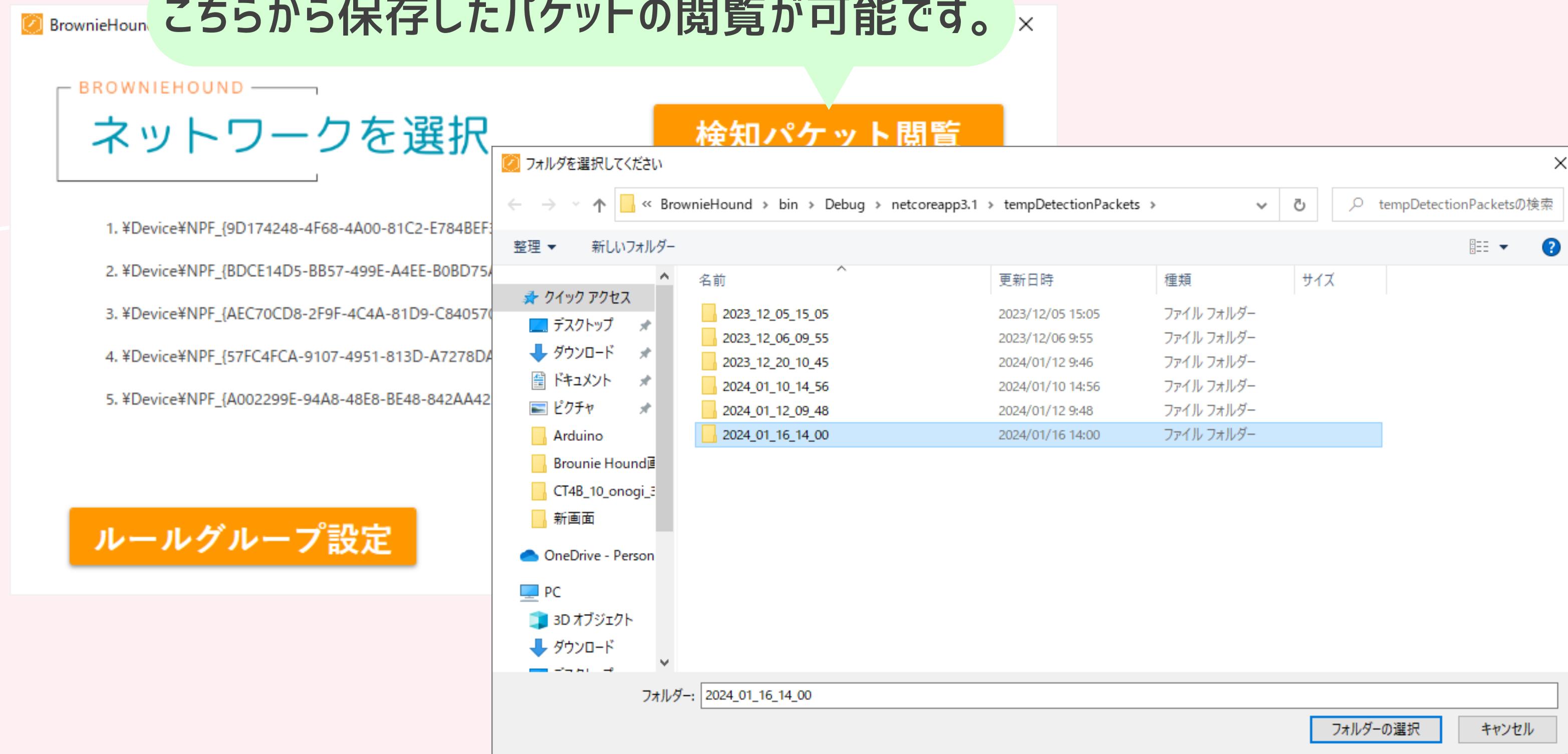
保存をクリックすると、検知した  
パケットの情報が保存されます。



[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キャプチャ・検知機能](#)

## キャプチャ画面の使用方法

こちらから保存したパケットの閲覧が可能です。



[目次に戻る](#)  
[使用前の準備](#)  
[メール設定](#)  
[ルールグループの設定方法](#)  
[キャプチャ・検知機能](#)

## キャプチャ画面の使用方法

複数のルールを設定していた場合は、こちらから  
別のルールの閲覧に切り替えることができます。

