

# MRB操作マニュアル

ログ確認

# 目次

1. ローカル管理画面でのログ閲覧
2. ログの種類と見方
3. クラウド管理画面でのログ閲覧

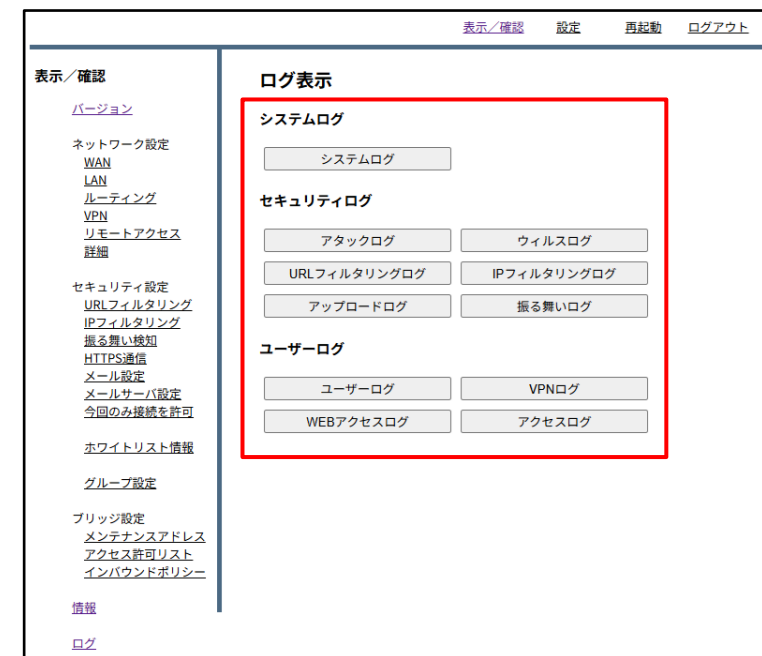
# I. ローカル管理画面でのログ閲覧

ローカル管理画面でのログ閲覧手順とログの種類について説明します

- ① ローカル管理画面にログイン後、左の「ログ」をクリックします



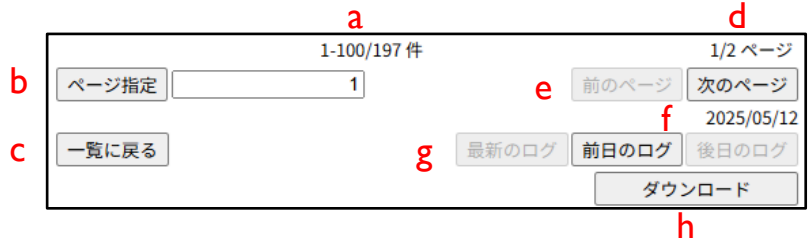
- ② 閲覧するログをクリックします



③ クリックしたボタンに対応するログが表示されます



④ 閲覧ログ操作は以下の通りです



- a...現在閲覧しているログ件数/すべてのログ件数です
- b...閲覧するログページを指定できます
- c...ログ一覧に戻ります
- d...現在閲覧しているログページ/すべてのログページです
- e...ログページの遷移ができます
- f...閲覧しているログの日付です
- g...閲覧するログの日付を変更できます
- h...閲覧している日付のログをダウンロードします

## 2. ログの種類と見方

ログの種類と見方について説明します

① 各ログの内容については以下の通りです

| ログ種別         | 内容                                                                         |
|--------------|----------------------------------------------------------------------------|
| アタックログ       | 外部からアタックされた場合に記録されます                                                       |
| ウイルスログ       | ダウンロードしようとしたファイルがウイルス判定された場合に記録されます<br>また、ウイルス判定メール、スパム判定メール受信時にもログが記録されます |
| URLフィルタリングログ | URLフィルタリングにて通信をブロックした場合に記録されます                                             |
| IPフィルタリングログ  | IPフィルタリングにて通信をブロックした場合に記録されます                                              |
| アップロードログ     | データを外部にアップロードした際に記録されます                                                    |
| 振る舞いログ       | Webアクセス以外の通信をブロックした際に記録されます                                                |
| ユーザーログ       | ユーザがMRB管理画面にて行った操作が記録されます                                                  |
| VPNログ        | VPN接続が記録されます                                                               |
| Webアクセスログ    | アクセスしたWebサイトが記録されます                                                        |
| アクセスログ       | Webサイト以外のアクセスが記録されます                                                       |

② ログの見方は以下の通りです

【アタックログ】

mmm dd hh:mm:ss mrb5l kernel: [xxxxxxxx] attack denied : IN=eth0 OUT= MAC=xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xxSRC=IPアドレス  
DST=IPアドレス LEN=xx TOS=0x00 PREC=0x00 TTL=xx ID=xxxx PROTO=xxx SPT=xxxx DPT=xxxx WINDOW=xxxx RES=0x00 SYN URGP=0

|                       |                                        |
|-----------------------|----------------------------------------|
| mmm dd hh:mm:ss       | ログが出力された日時が表示されます<br>例) Jun 1 09:00:00 |
| kernel:[xxxxxxxx]     | カーネル時間が表示されます                          |
| attack denied         | アタックを防御した意味を示します                       |
| IN=eth0               | インバウンド通信のIN側のNICが表示されます                |
| OUT= MACxx:xx:xx:~:xx | インバウンド通信のアウト側のMACアドレスが表示されます           |
| SRC=IPアドレス            | アタックしている相手のIPアドレスが表示されます               |
| DST=IPアドレス            | アタック対象のIPアドレスが表示されます                   |
| LEN=xx                | パケットの長さが表示されます                         |
| TOS=0x00              | パケットの優先度が表示されます                        |

|             |                        |
|-------------|------------------------|
| PREC=0x00   | パケットの優先度が表示されます        |
| TTL=xx      | パケットが破棄されるまでの時間が表示されます |
| ID=xxxx     | ヘッダの識別番号が表示されます        |
| PROTO=xxx   | 通信のプロトコルが表示されます        |
| SPT=xxxx    | 送信元のポート番号が表示されます       |
| DPT=xxxx    | 送信先のポート番号が表示されます       |
| WINDOW=xxxx | ウィンドウサイズが表示されます        |
| RES=0x00    | TCPヘッダの予約領域が表示されます     |
| SYN URGP=0  | コントロールフラグの状態を示します      |

次のページに続きます↓

## 【ウイルスログ】

yyyy/mm/dd hh:mm:ss ログコード グループ番号 クライアント端末IPアドレス->グローバルIPアドレス カテゴリコード URL/メールアドレス

|                     |                                                                            |
|---------------------|----------------------------------------------------------------------------|
| yyyy/mm/dd hh:mm:ss | ログが出力された日時が表示されます<br>例) 2025/06/30 09:00:00                                |
| ログコード               | ログの種類が表示されます<br>V001：ウイルス判定<br>M001：ウイルス判定メール<br>M002：スパム判定メール             |
| グループ番号              | クライアント端末が所属するグループが表示されます<br>100：デフォルトグループ<br>1：グループ1<br>2：グループ2<br>3：グループ3 |
| クライアント端末IPアドレス      | ログ対象のクライアント端末IPアドレスが表示されます                                                 |
| グローバルIPアドレス         | ウイルス判定、スパム判定されたグローバルIPアドレスが表示されます                                          |
| カテゴリコード             | 検知したカテゴリコードが表示されます<br>1~82：カテゴリ番号 ※詳細はカテゴリコード一覧をご参照ください                    |
| URL/メールアドレス         | ウイルス判定、スパム判定されたURL/メールアドレスが表示されます                                          |

次のページに続きます↓

## 【URLフィルタリングログ】

yyyy/mm/dd hh:mm:ss ログコード グループ番号 クライアント端末IPアドレス>グローバルIPアドレス カテゴリコード URL

|                     |                                                                                    |
|---------------------|------------------------------------------------------------------------------------|
| yyyy/mm/dd hh:mm:ss | ログが出力された日時が表示されます<br>例) 2025/06/30 09:00:00                                        |
| ログコード               | ログの種類が表示されます<br>U001 : URLフィルタリングによるブロック                                           |
| グループ番号              | クライアント端末が所属するグループが表示されます<br>100 : デフォルトグループ<br>1 : グループ1<br>2 : グループ2<br>3 : グループ3 |
| クライアント端末IPアドレス      | ログ対象のクライアント端末IPアドレスが表示されます                                                         |
| グローバルIPアドレス         | ブロックされたアクセス先のグローバルIPアドレスが表示されます                                                    |
| カテゴリコード             | 検知したカテゴリコードが表示されます<br>1~82 : カテゴリ番号 ※詳細はカテゴリコード一覧をご参照ください                          |
| URL                 | アクセス先のURLが表示されます                                                                   |

次のページに続きます↓



【IPフィルタリング】

yyyy/mm/dd hh:mm:ss ログコード グループ番号 クライアント端末IPアドレス>グローバルIPアドレス 脅威カテゴリ IPIに紐づくURL

|                     |                                                                                    |
|---------------------|------------------------------------------------------------------------------------|
| yyyy/mm/dd hh:mm:ss | ログが出力された日時が表示されます<br>例) 2025/06/30 09:00:00                                        |
| ログコード               | ログの種類が表示されます<br>I00I : IPフィルタリングによるブロック                                            |
| グループ番号              | クライアント端末が所属するグループが表示されます<br>100 : デフォルトグループ<br>1 : グループ1<br>2 : グループ2<br>3 : グループ3 |
| クライアント端末IPアドレス      | ログ対象のクライアント端末IPアドレスが表示されます                                                         |
| グローバルIPアドレス         | ブロックされたアクセス先のグローバルIPアドレスが表示されます                                                    |
| 脅威カテゴリ              | 検知した脅威カテゴリが表示されます                                                                  |
| IPIに紐づくURL          | アクセス先IPIに紐づくURLが表示されます                                                             |

脅威カテゴリは以下の通りです

|             |                  |          |
|-------------|------------------|----------|
| Spam Source | Proxy            | BotNets  |
| Scanners    | Windows Exploits | Phishing |

次のページに続きます↓

## 【アップロードログ】

yyyy/mm/dd, hh:mm:ss, ログコード, グループ番号, クライアント端末IPアドレス, グローバルIPアドレス, セッション番号, パケットサイズ, URL

|                     |                                                                                |
|---------------------|--------------------------------------------------------------------------------|
| yyyy/mm/dd hh:mm:ss | ログが出力された日時が表示されます<br>例) 2025/06/30 09:00:00                                    |
| ログコード               | ログの種類が表示されます<br>0: 通常ログ                                                        |
| グループ番号              | クライアント端末が所属するグループが表示されます<br>100: デフォルトグループ<br>1: グループ1<br>2: グループ2<br>3: グループ3 |
| クライアント端末IPアドレス      | ログ対象のクライアント端末IPアドレスが表示されます                                                     |
| グローバルIPアドレス         | アウトバウンド通信先のIPアドレスが表示されます                                                       |
| セッション番号             | アウトバウンド通信のセッション番号が表示されます                                                       |
| パケットサイズ             | アウトバウンド通信のパケットサイズが表示されます                                                       |
| URL                 | アウトバウンド通信先のURLが表示されます                                                          |

次のページに続きます↓

## 【振る舞いログ】

yyyy/mm/dd, hh:mm:ss, ログコード, グループ番号, プロトコル識別コード, クライアント端末IPアドレス:SRCポート番号,  
グローバルIPアドレス:DSTポート番号

|                     |                                                                                |
|---------------------|--------------------------------------------------------------------------------|
| yyyy/mm/dd hh:mm:ss | ログが出力された日時が表示されます<br>例) 2025/06/30 09:00:00                                    |
| ログコード               | ログの種類が表示されます<br>0: 通常ログ                                                        |
| グループ番号              | クライアント端末が所属するグループが表示されます<br>100: デフォルトグループ<br>1: グループ1<br>2: グループ2<br>3: グループ3 |
| プロトコル識別コード          | 通信プロトコルが表示されます<br>1: ICMP<br>6: TCP<br>17: UDP                                 |
| クライアント端末IPアドレス      | ログ対象のクライアント端末IPアドレスが表示されます                                                     |
| SRCポート番号            | 送信元のポート番号が表示されます                                                               |
| グローバルIPアドレス         | アウトバウンド通信先のIPアドレスが表示されます                                                       |
| DSTポート番号            | 送信先のポート番号が表示されます                                                               |

次のページに続きます↓

## 【ユーザーログ】

yyyy/mm//dd hh:mm:ss ログコード 操作内容

|                     |                                                 |
|---------------------|-------------------------------------------------|
| yyyy/mm/dd hh:mm:ss | ログが出力された日時が表示されます<br>例) 2025/06/30 09:00:00     |
| ログコード               | ログの種類が表示されます<br>C001：設定変更を行ったログ                 |
| 操作内容                | ユーザー行った操作内容が表示されます<br>例) SETUP_WAN<br>SETUP_LAN |

次のページに続きます↓

## 【VPNログ】

yyyy/mm/dd hh:mm:ss VPN番号 ネット数 ステータス クライアント端末IPアドレス-グローバルIPアドレス  
(ネットワークアドレス1-ネットワークアドレス2) トンネル番号

|                     |                                               |
|---------------------|-----------------------------------------------|
| yyyy/mm/dd hh:mm:ss | ログが出力された日時が表示されます<br>例) 2025/06/30 09:00:00   |
| VPN番号               | VPN番号が表示されます                                  |
| ネット数                | リモートネットワーク数が表示されます                            |
| ステータス               | VPNのステータスが表示されます<br>例) connected、disconnected |
| クライアント端末IPアドレス      | クライアント端末IPアドレスが表示されます                         |
| グローバルIPアドレス         | VPN接続先のグローバルIPアドレスが表示されます                     |
| ネットワークアドレス1         | 自身のLAN側ネットワークアドレスが表示されます                      |
| ネットワークアドレス2         | VPN接続先のLAN側ネットワークアドレスが表示されます                  |
| トンネル番号              | VPN接続で使用しているトンネル番号が表示されます                     |

次のページに続きます↓

## 【WEBアクセスログ】

yyyy/mm/dd hh:mm:ss, ログコード, グループ番号, クライアント端末IPアドレス, グローバルIPアドレス, シーケンス番号, データ転送量, HTTPメソッド, URL

|                     |                                                                                |
|---------------------|--------------------------------------------------------------------------------|
| yyyy/mm/dd hh:mm:ss | ログが出力された日時が表示されます<br>例) 2025/06/30 09:00:00                                    |
| ログコード               | ログの種類が表示されます<br>0: 通常ログ                                                        |
| グループ番号              | クライアント端末が所属するグループが表示されます<br>100: デフォルトグループ<br>1: グループ1<br>2: グループ2<br>3: グループ3 |
| クライアント端末IPアドレス      | ログ対象のクライアント端末IPアドレスが表示されます                                                     |
| グローバルIPアドレス         | WEBアクセス先のIPアドレスが表示されます                                                         |
| シーケンス番号             | シーケンス番号が表示されます                                                                 |
| データ転送量              | データ転送量が表示されます                                                                  |
| HTTPメソッド            | HTTPメソッドが表示されます<br>例) GET、POST                                                 |
| URL                 | アクセス先のURLが表示されます                                                               |

次のページに続きます↓

## 【アクセスログ】

yyyy/mm/dd hh:mm:ss, 通信状態, グループ番号, 通信領域, クライアント端末IPアドレス:ポート番号1, グローバルIPアドレス:ポート番号2

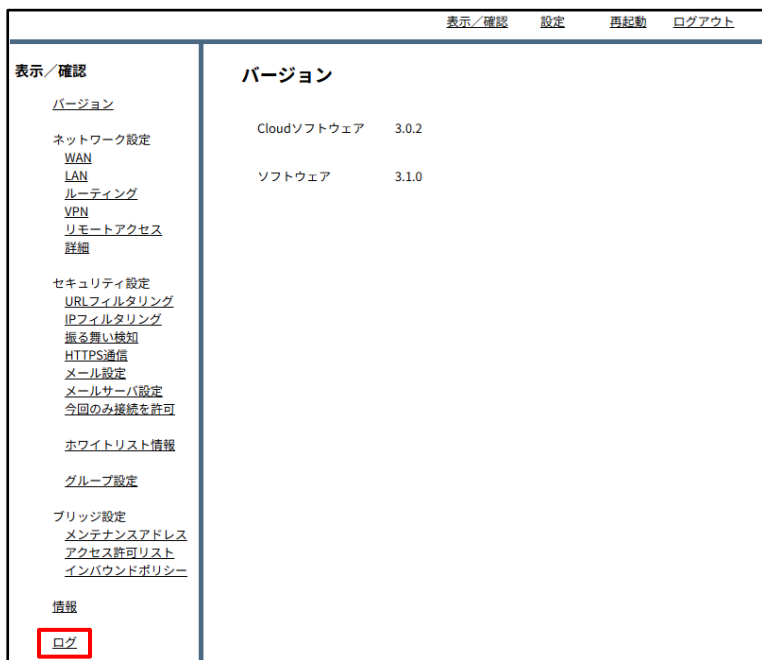
|                     |                                                                                |
|---------------------|--------------------------------------------------------------------------------|
| yyyy/mm/dd hh:mm:ss | ログが出力された日時が表示されます<br>例) 2025/06/30 09:00:00                                    |
| 通信状態                | 通信状態が表示されます<br>1: 通信成功<br>-1: 通信失敗                                             |
| グループ番号              | クライアント端末が所属するグループが表示されます<br>100: デフォルトグループ<br>1: グループ1<br>2: グループ2<br>3: グループ3 |
| 通信領域                | 通信領域が表示されます<br>6: ローカルネットワーク内の通信<br>17: 外部ネットワークへの通信                           |
| クライアント端末IPアドレス      | ログ対象のクライアント端末IPアドレスが表示されます                                                     |
| ポート番号1              | クライアント端末のポート番号が表示されます                                                          |
| グローバルIPアドレス         | アクセス先のIPアドレスが表示されます                                                            |
| ポート番号2              | アクセス先のポート番号が表示されます                                                             |

ログの見方の説明は以上になります

### 3.クラウド管理画面でのログ閲覧

クラウド管理画面でのログ閲覧手順について説明します

- ① クラウド管理画面にログイン後、左の「ログ」をクリックします

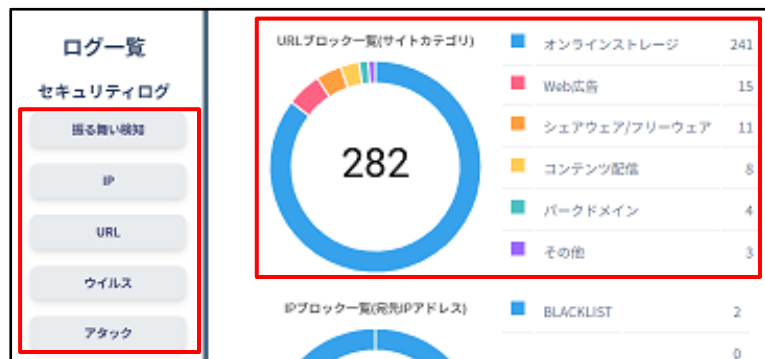


- ② ログ一覧と検知されたログのグラフが表示されます





- ③ 閲覧したいログまたはグラフをクリックするとログの詳細が表示されます

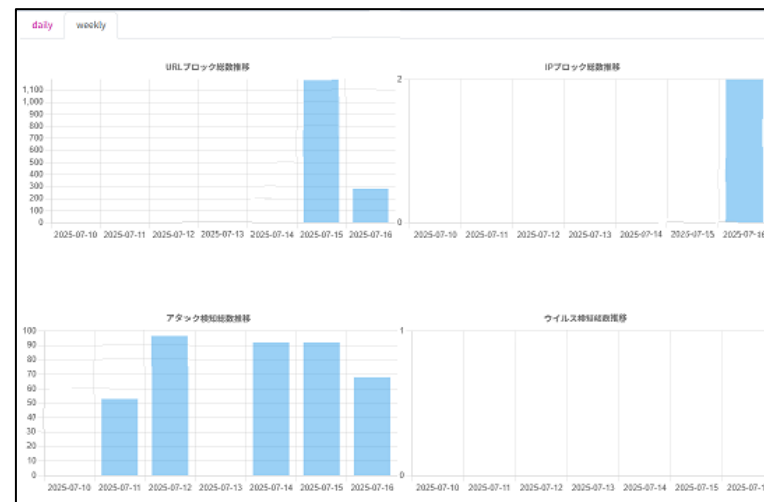


URL ログ一覧 2025/07/16

| 検出内容   | 日時                  | 検出      | グループ    | 検出IPアドレス       | 検出URLアドレス    | カテゴリ       | URL                                 |
|--------|---------------------|---------|---------|----------------|--------------|------------|-------------------------------------|
| 振り舞い検知 | 2025/07/16 10:54:56 | Default | Default | 192.168.122.10 | 13.107.42.12 | オンラインストレージ | api.orelive.com/v1.0/drive/select** |
| 振り舞い検知 | 2025/07/16 10:54:57 | Default | Default | 192.168.122.10 | 13.107.42.12 | オンラインストレージ | api.orelive.com/v1.0/drive/select** |
| 振り舞い検知 | 2025/07/16 10:59:12 | Default | Default | 192.168.122.10 | 13.107.42.12 | オンラインストレージ | api.orelive.com/v1.0/drive/select** |
| 振り舞い検知 | 2025/07/16 10:59:13 | Default | Default | 192.168.122.10 | 13.107.42.12 | オンラインストレージ | api.orelive.com/v1.0/drive/select** |
| 振り舞い検知 | 2025/07/16 10:59:14 | Default | Default | 192.168.122.10 | 13.107.42.12 | オンラインストレージ | api.orelive.com/v1.0/drive/select** |
| 振り舞い検知 | 2025/07/16 11:03:30 | Default | Default | 192.168.122.10 | 13.107.42.12 | オンラインストレージ | api.orelive.com/v1.0/drive/select** |
| 振り舞い検知 | 2025/07/16 11:03:30 | Default | Default | 192.168.122.10 | 13.107.42.12 | オンラインストレージ | api.orelive.com/v1.0/drive/select** |
| 振り舞い検知 | 2025/07/16 11:03:31 | Default | Default | 192.168.122.10 | 13.107.42.12 | オンラインストレージ | api.orelive.com/v1.0/drive/select** |
| 振り舞い検知 | 2025/07/16 11:03:31 | Default | Default | 192.168.122.10 | 13.107.42.12 | オンラインストレージ | api.orelive.com/v1.0/drive/select** |
| 振り舞い検知 | 2025/07/16 11:07:48 | Default | Default | 192.168.122.10 | 13.107.42.12 | オンラインストレージ | api.orelive.com/v1.0/drive/select** |
| 振り舞い検知 | 2025/07/16 11:07:49 | Default | Default | 192.168.122.10 | 13.107.42.12 | オンラインストレージ | api.orelive.com/v1.0/drive/select** |

検索ログ: 241件 / ログ総数: 241件

- ④ 「weekly」をクリックすると直近一週間のログが表示されます



※グラフをクリックするとログの詳細が表示されます

## ⑤ 閲覧ログ操作は以下の通りです

WEBアクセス ログ一覧 2025/05/12

検索メニュー C 検索リセット

DOWNLOAD F  
全ログDL

| 接続先の国 | 日付         | 時刻       | グループ    | 端末IPアドレス       | 通信先IPアドレス       | URL                                                                         |
|-------|------------|----------|---------|----------------|-----------------|-----------------------------------------------------------------------------|
| US    | 2025/05/12 | 00:41:59 | Default | 192.168.123.12 | 23.46.155.220   | http://ctldl.windowsupdate.com/msdownload/update/v3/static/trusted/en/pi... |
| US    | 2025/05/12 | 00:42:08 | Default | 192.168.123.12 | 23.46.155.220   | http://ctldl.windowsupdate.com/msdownload/update/v3/static/trusted/en/di... |
| US    | 2025/05/12 | 00:44:22 | Default | 192.168.123.12 | 104.93.9.35     | http://x1.c.lencr.org                                                       |
| US    | 2025/05/12 | 00:48:38 | Default | 192.168.123.12 | 23.46.155.220   | http://download.windowsupdate.com/d/msdownload/update/others/2025/05/...    |
| GB    | 2025/05/12 | 00:49:04 | Default | 192.168.123.12 | 130.33.125.141  | http://130.33.125.141/d/msdownload/update/software/defu/2025/05/am_delt...  |
| US    | 2025/05/12 | 01:44:03 | Default | 192.168.123.12 | 23.46.155.202   | http://ctldl.windowsupdate.com/msdownload/update/v3/static/trusted/en/di... |
| US    | 2025/05/12 | 01:44:22 | Default | 192.168.123.12 | 151.101.110.172 | http://ctldl.windowsupdate.com/msdownload/update/v3/static/trusted/en/di... |
| US    | 2025/05/12 | 01:44:23 | Default | 192.168.123.12 | 23.221.141.54   | http://x1.c.lencr.org                                                       |
| US    | 2025/05/12 | 02:10:48 | Default | 192.168.123.12 | 150.171.28.11   | http://edge.microsoft.com/browsenetworktime/time/1/current?cup2key=2~V...   |
| US    | 2025/05/12 | 02:51:03 | Default | 192.168.123.12 | 151.101.110.172 | http://ctldl.windowsupdate.com/msdownload/update/v3/static/trusted/en/di... |

最新のログ B 前日のログ 後日のログ

閲覧ログ: 1-100件 / ログ総数: 194件 A

ログページ選択範囲(1-2) D ページ指定

前のページ E 次のページ

a...現在閲覧しているログの件数/すべてのログ件数です

b...閲覧するログの日付を変更できます

c...検索メニューを表示し、時刻・キーワードでログを検索できます

d...閲覧するログページを指定できます

e...ログページの遷移ができます

f...閲覧しているログをダウンロードできます

## 検索メニュー

検索メニュー 検索リセット

時刻検索: 時間検索の場合、こちらを入力: フリーワード検索

hh:mm:ss, hh:mm hh:mm:ss, hh:mm

検索