MRB操作マニュアル

ログ確認

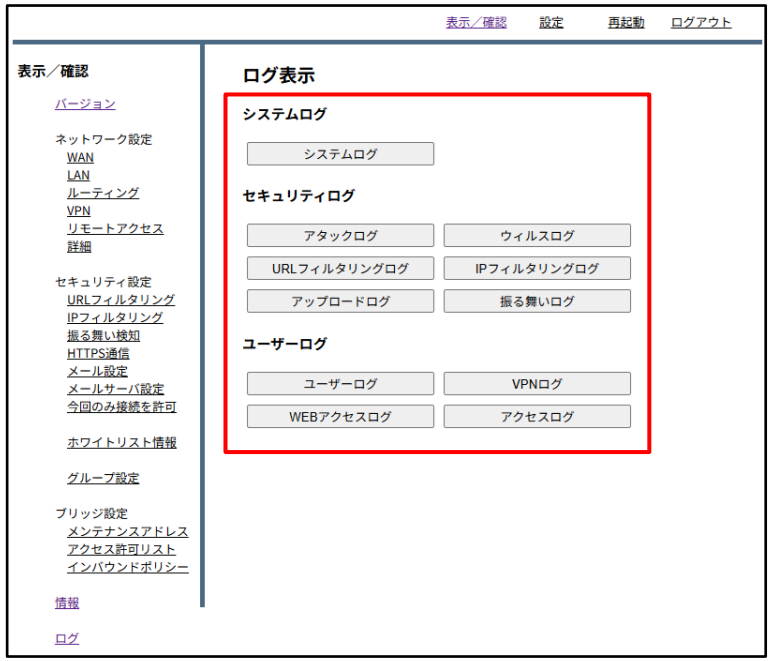
目次

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

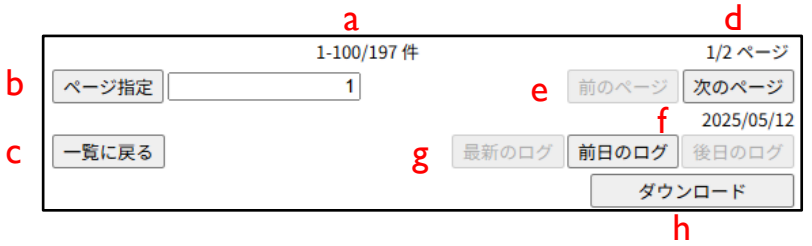
①　ローカル管理画面にログイン後、左の「ログ」をクリックします

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 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 mrb51 kernel: [xxxxxxxx] attack denied : IN=eth0 OUT= MAC=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 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
PROTP=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 例）2025/06/30 09:00:00
ログコード	ログの種類が表示されます V001：ウイルス判定 M001：ウイルス判定メール 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 100：デフォルトグループ 1：グループ1 2：グループ2 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 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 例）2025/06/30 09:00:00
ログコード	ログの種類が表示されます 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 100：デフォルトグループ 1：グループ1 2：グループ2 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 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 IP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** **例）2025/06/30 09:00:00**
ログコード	**ログの種類が表示されます** **1001：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** **100：デフォルトグループ** **1：グループ1** **2：グループ2** **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**
IPに紐づくURL	**アクセス先IP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 例）2025/06/30 09:00:00
ログコード	ログの種類が表示されます 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 100：デフォルトグループ 1：グループ1 2：グループ2 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 例）2025/06/30 09:00:00
ログコード	ログの種類が表示されます 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 100：デフォルトグループ 1：グループ1 2：グループ2 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 1：ICMP 6：TCP 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 例）2025/06/30 09:00:00
ログコード	ログの種類が表示されます 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 例）SETUP_WAN 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 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 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 例）2025/06/30 09:00:00
ログコード	ログの種類が表示されます 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 100：デフォルトグループ 1：グループ1 2：グループ2 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 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**

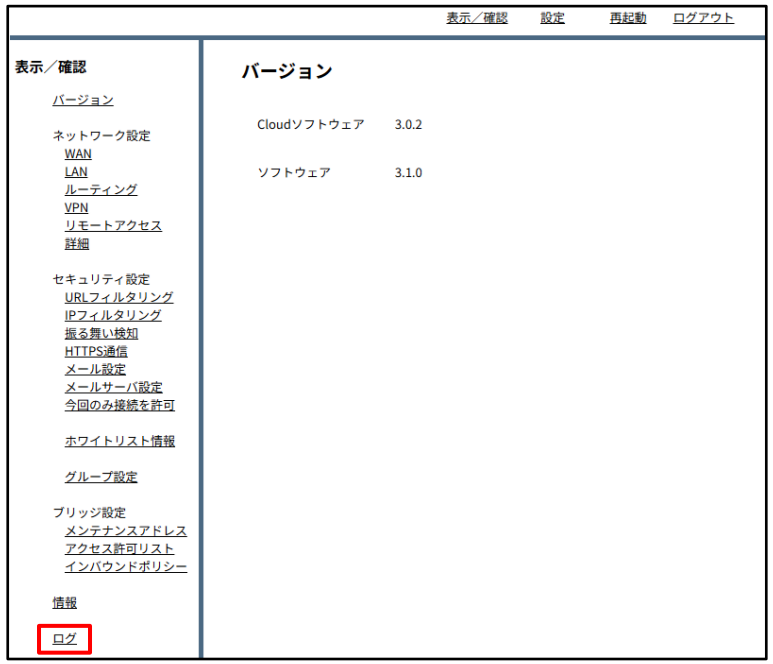
yyyy/mm/dd hh:mm:ss	**ログが出力された日時が表示されます** **例）**2025/06/30 09:00:00
通信状態	**通信状態が表示されます** 1：**通信成功** -1：**通信失敗**
グループ番号	**クライアント端末が所属するグループが表示されます** 100：**デフォルトグループ** 1：**グループ1** 2：**グループ2** 3：**グループ3**
通信領域	**通信領域が表示されます** 6：**ローカルネットワーク内の通信** 17：**外部ネットワークへの通信**
クライアント端末IPアドレス	**ログ対象のクライアント端末IPアドレス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

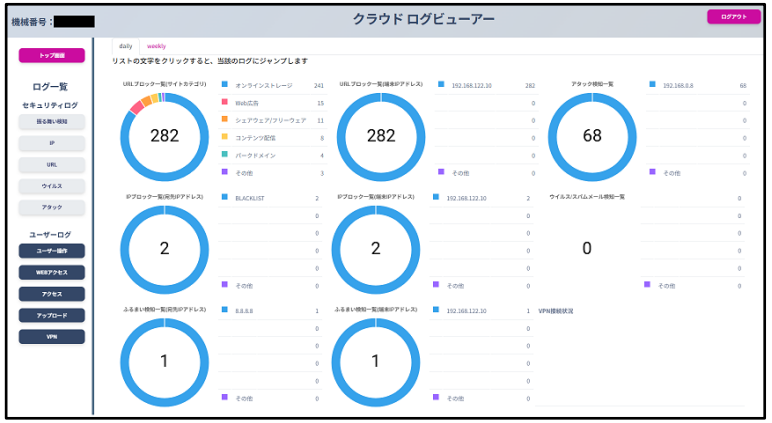
3.クラウド管理画面でのログ閲覧

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

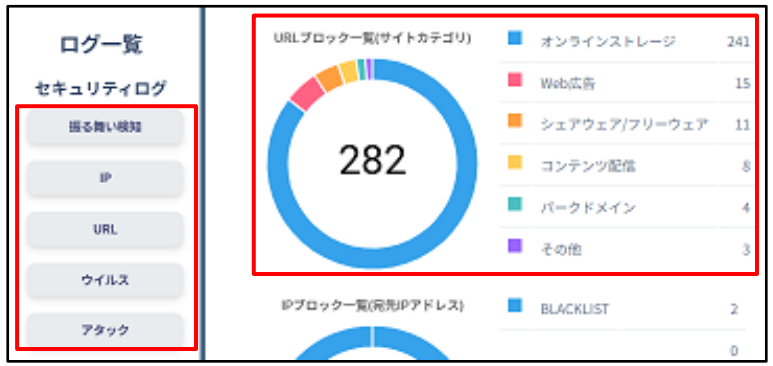
① クラウド管理画面にログイン後、左の「ログ」をクリックします

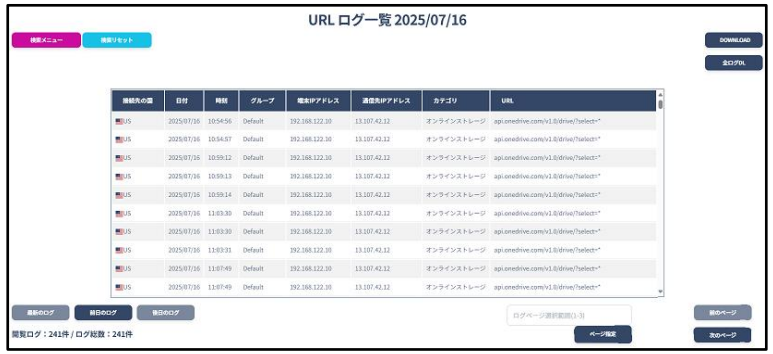


② ログ一覧と検知されたログのグラフが表示されます

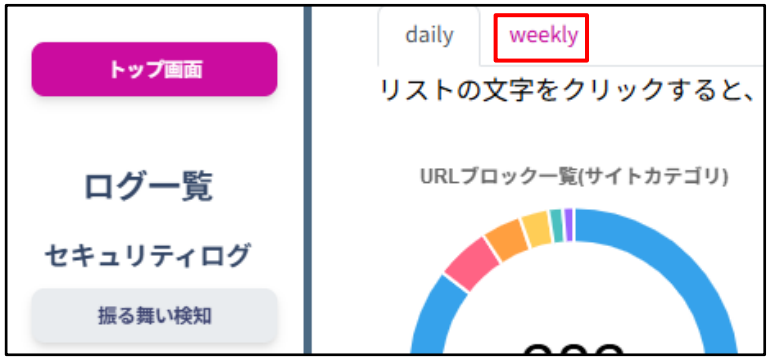


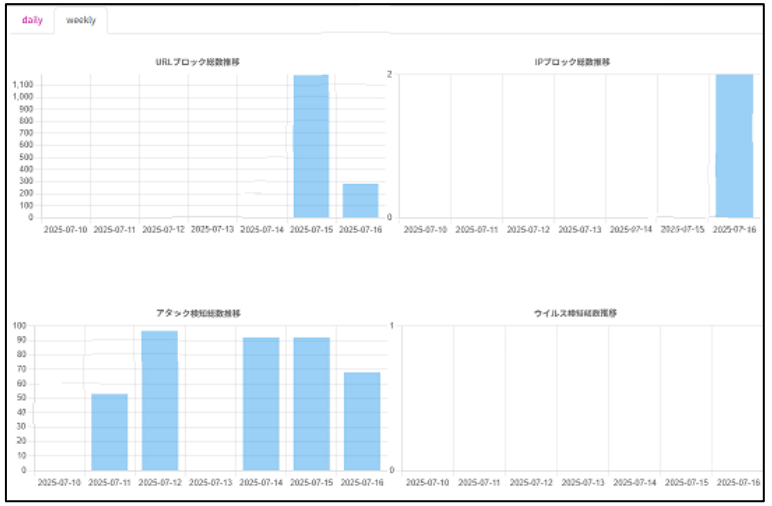
③ 閲覧したいログまたはグラフをクリックするとログの詳細が表示されます





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

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