



본 문서는 MBUSTER V2.0의 제품 설치 후 ㈜에스티씨랩으로부터 본 제품의 운용을 위해 지침에 따라 교육 받은 관리자(최상위 관리자)에게 주어지는 문서입니다.

또한 MBUSTER V2.0의 제품에 포함된 모든 프로그램과 자료 파일, 사용 설명서, 문서 내용 등은 저작권법과 컴퓨터 프로그램 보호법에 의하여 보호받고 있습니다.

MBUSTER V2.0제품에 포함된 모든 프로그램과 자료, 문서 내용 등은 어떤 목적으로도 변형하거나 재가공하여 재판매 할 수 없습니다.

이 설명서의 내용은 ㈜에스티씨랩의 사전 예고 없이 변경될 수 있습니다.

이 기능 설명서에서 언급하는 모든 회사명과 제품명은 개발사의 등록 상표입니다.

Copyright STCLab Inc. All rights reserved.

본사: 서울 강남구 봉은사로 37길 5 캠프지 2층

Tel: +82-2-3453-1424

Homepage : http://www.stclab.com

**<차 례>**

**1. 개요** **5**

1.1 제품의 용도 5

**2. MBUSTER 메인화면** **6**

2.1 MBUSTER MANAGER 6

2.2 사용 가이드 7

**3. 대시보드** **8**

**4. 접속자 관리** **10**

4.1 접속자 리스트 10

**5 매크로 관리** **12**

5.1 매크로 리스트 12

5.2 차단 증적 자료 14

**6. 통계 관리** **15**

6.1 유형별 접속 통계 15

6.2 매크로 통계 17

6.3 국가별 통계 19

**7. 아이피 상세 정보** **21**

**8. MBUSTER 관리** **24**

8.1 도메인 생성 24

8.2 도메인 관리 25

8.3 정책 설정 30

8.4 예외처리 관리 33

8.5 감사로그 34

8.6 BOT 리스트 35

**9. 보고서** **36**

**10. 데이터 저장 및 복구** **37**

**11. 기술지원 문의** **38**

**12. MBUSTER MANAGER 가이드** **39**

**13. 용어정의** 40

**1. 개요**

**1.1 제품의 용도**

MBUSTER는 매크로 차단 솔루션으로서, 아래와 같은 용도로 개발되었습니다.

- 정상적인 사용자들에게는 매크로 사용자들로 인해 정상적인 사용자의 예약 기회가 제한되는 현상을 막기 위함

- 매크로 사용자들을 차단함으로써 서버 부하를 줄여 더 양질의 서비스를 제공

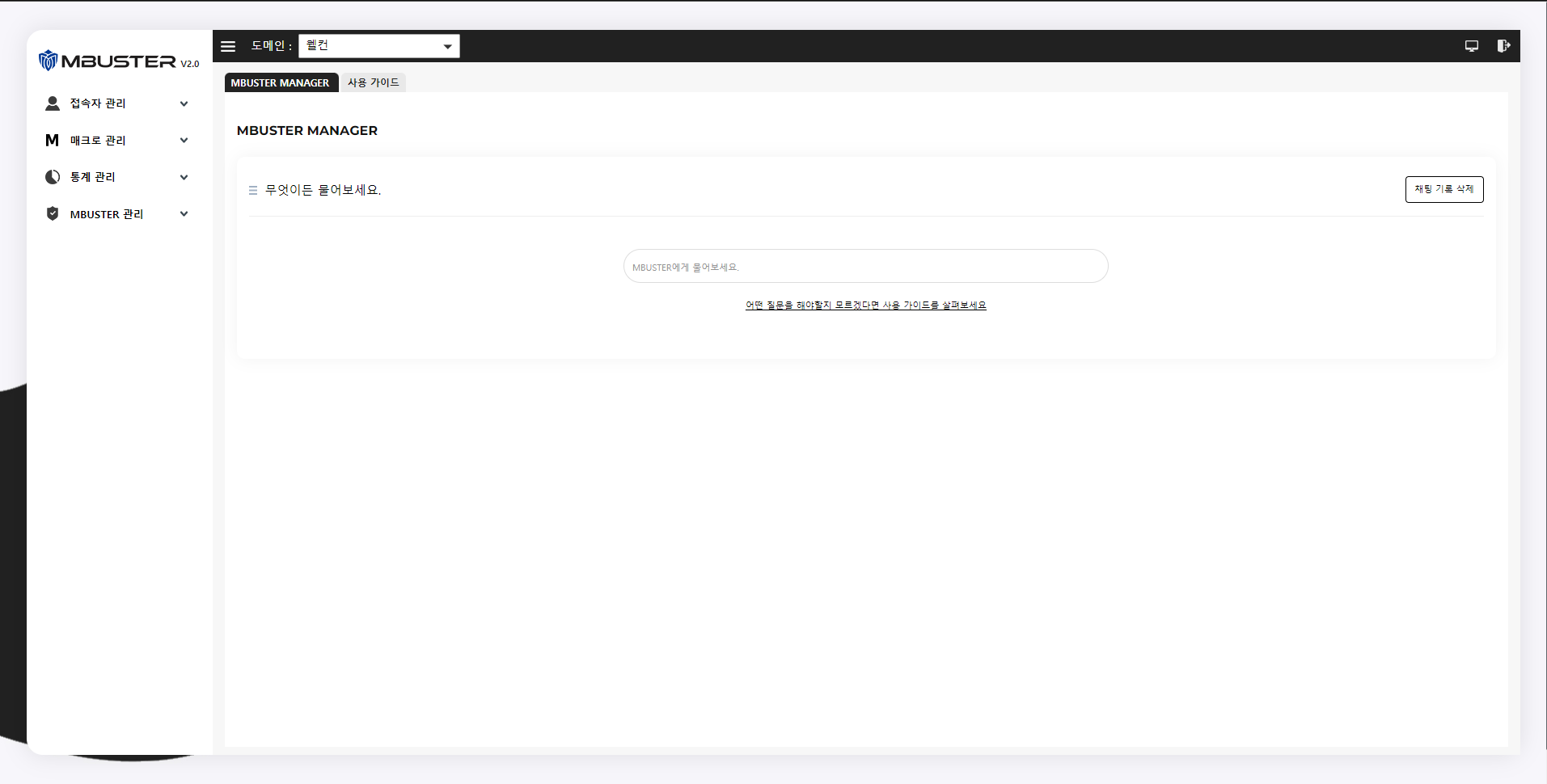
- 채팅형 관리자 화면을 제공하여 원하는 정보를 쉽고 빠르게 조회 가능

**2. MBUSTER 메인화면**

**2.1 MBUSTER MANAGER**

MBUSTER V2.0 로그인 후 진입할 수 있는 메인화면입니다.

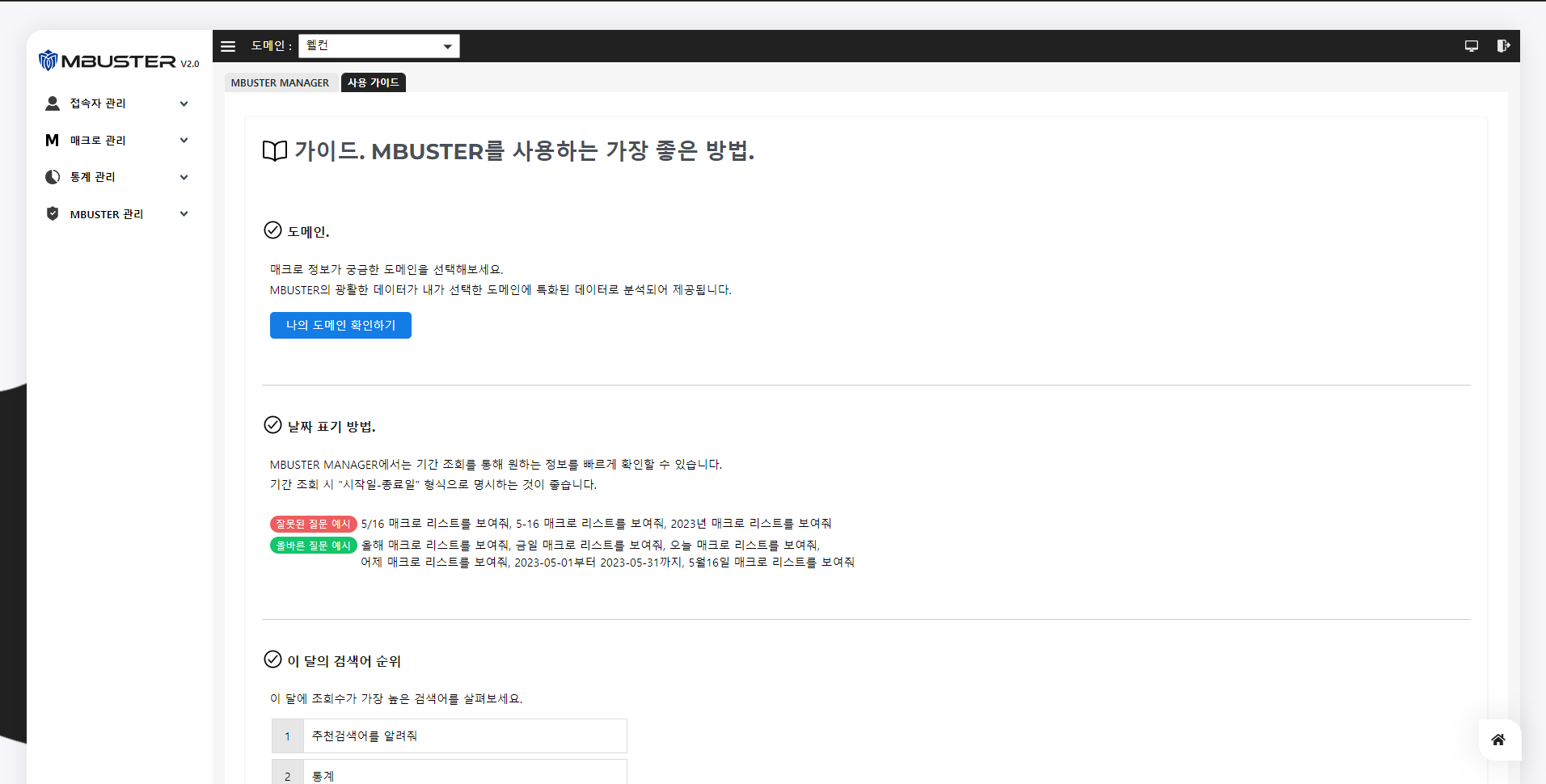
MBUSTER MANAGER는 채팅을 통해 관리하는 도메인의 정보를 질문하고 답변 받을 수 있는 페이지입니다.



<MBUSTER MANAGER>

|  |  |
| --- | --- |
| **항목** | **설명** |
| **검색어 입력창** | MBUSTER에게 궁금한 점을 질문하고 엔터를 누릅니다. |
| **채팅 기록 삭제** | 쌓여있는 채팅 기록을 지웁니다. |

**2.2 사용가이드**



<사용 가이드>

|  |  |
| --- | --- |
| **항목** | **설명** |
| **사용 가이드** | MBUSTER 및 MBUSTER MANAGER를 사용하는 방법에 대해 가이드합니다. |

**3. 대시보드**



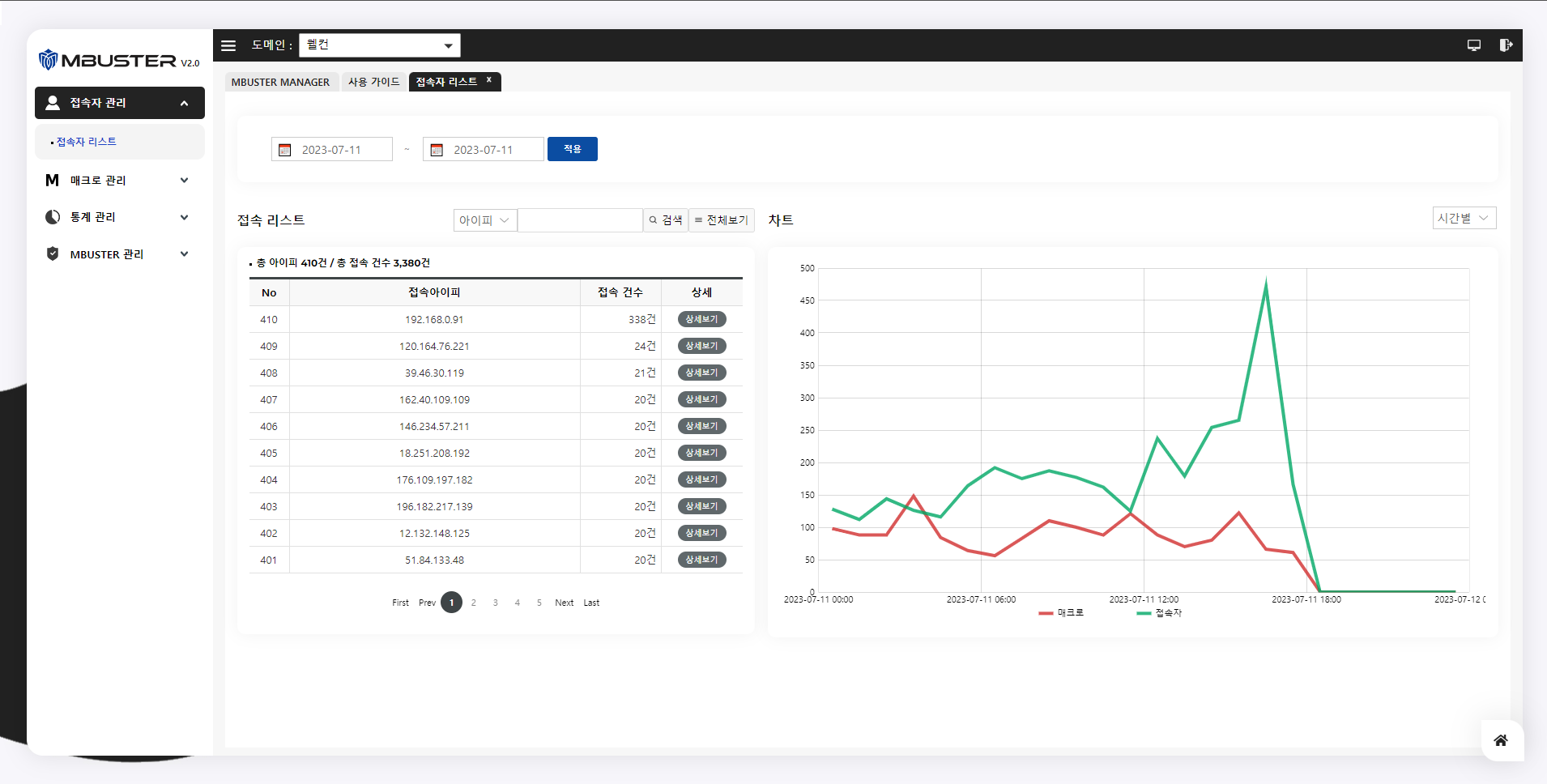
<대시보드>

|  |  |  |
| --- | --- | --- |
| **No** | **항목** | **설명** |
| 1 | **금일 접속/차단 건수 및 차단율** | 금일 총 접속 건수와 접속자/매크로 건수, 그리고 차단율을 보여줍니다. |
| 2 | **매크로 접속 현황** | 정적 분석/동적 분석의 각 엔진마다 몇 건의 매크로를 차단했는지 차트를 통해 시각적으로 보여줍니다. |
| 3 | **정적분석** | [Header 분석을 통한 차단]  웹 사이트에 접속하는 사용자의 요청 헤더값에 의해 차단된 매크로 건수를 보여줍니다.  [아이피 관리를 통한 차단]  MBUSTER가 관리하는 BOT　IP 및 차단 설정된 IP에 의해 차단된 매크로 건수를 보여줍니다.  [접속통계분석을 통한 차단]  접속통계분석에 의해 차단된 매크로 건수를 보여줍니다. |
| 4 | **동적분석** | [해외 접속자 차단]  해외 접속에 의해 차단된 매크로 건수를 보여줍니다.  [행위분석 캡챠 차단]  행위분석과 2차 검증 수단인 캡챠를 통과하지 못해 차단된 매크로 건수를 보여줍니다.  [행위분석 브라우저 챌린지 차단]  행위분석과 2차 검증 수단인 브라우저 챌린지를 통과하지 못해 차단된 매크로 건수를 보여줍니다.  [행위분석 차단]  행위분석에 의해 즉시 차단된 매크로 건수를 보여줍니다. |
| 5 | **최근 매크로 이력** | 차단된 매크로의 최근 접속 시도 이력을 보여줍니다. |

**4. 접속자 관리**

**4.1 접속자 리스트**

접속자 리스트는 웹 서비스에 접속한 사용자를 리스트와 차트로 볼 수 있는 화면입니다.



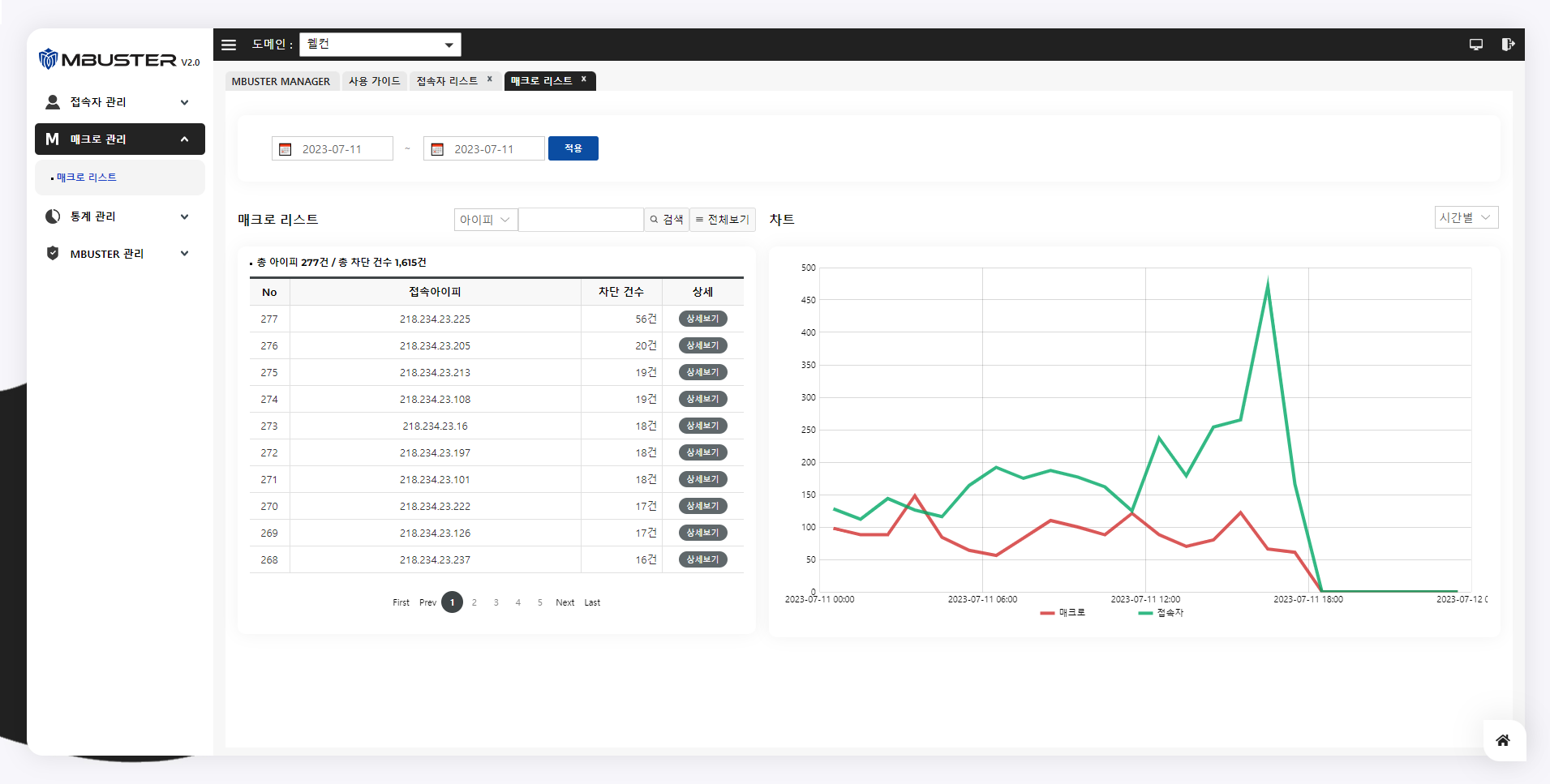
<접속자 리스트>

|  |  |
| --- | --- |
| **항목** | **설명** |
| **도메인** | 조회하고자 하는 도메인을 선택합니다. |
| **기간 검색** | 조회하고자 하는 기간을 선택합니다. |
| **아이피 검색** | 검색한 아이피를 기준으로 리스트와 차트를 조회할 수 있습니다. |
| **접속 리스트** | 웹 서비스에 접속한 접속자를 보여줍니다.   |  |  | | --- | --- | | No | 리스트 순번 | | 접속 아이피 | 웹 서비스에 접속한 아이피를 보여줍니다. | | 접속 건수 | 해당 아이피가 접속한 건수를 보여줍니다. | | 상세 | 해당 아이피의 상세정보 페이지로 이동합니다. | |
| **차트 유형** | 월별, 주별. 일별, 시간별 중 하나를 선택해 차트를 조회할 수 있습니다. |
| **차트** | 차트 유형에 따른 접속자 건수를 보여줍니다. 월별 차트 클릭 시 주별 차트를 확인할 수 있습니다.  주별 차트 클릭 시 일별 차트를 확인할 수 있습니다.  일별 차트 클릭 시 시간별 차트를 확인할 수 있습니다.  시간별 차트를 좌우로 드래그하여 해당 시간에 대한 데이터만 조회 가능합니다. |

**5. 매크로 관리**

**5.1 매크로 리스트**

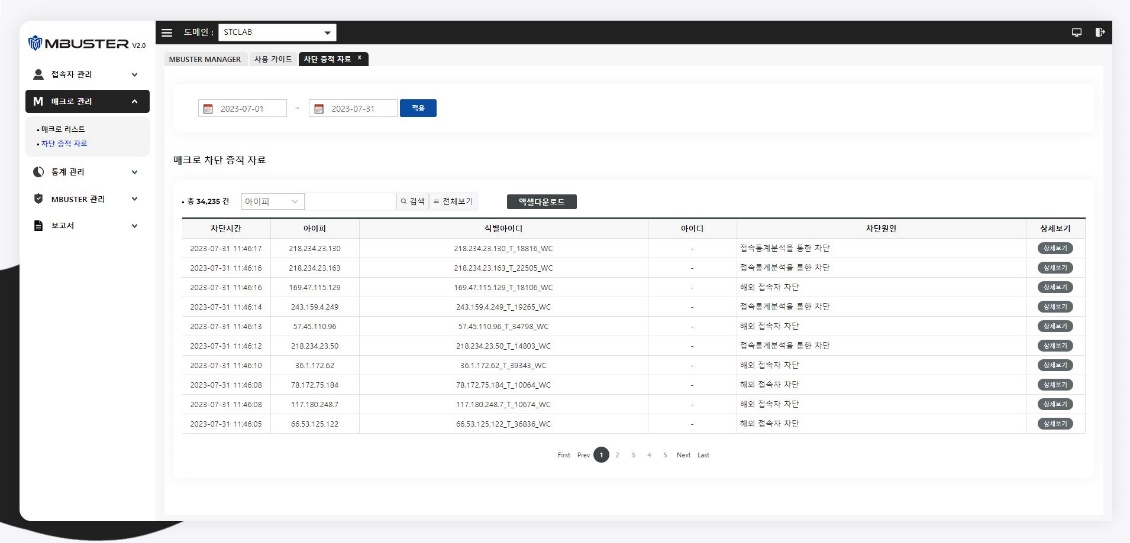
매크로 리스트는 웹 서비스에 접속하지 못한 차단된 매크로를 리스트와 차트로 볼 수 있는 화면입니다.



<매크로 리스트>

|  |  |
| --- | --- |
| **항목** | **설명** |
| **도메인** | 조회하고자 하는 도메인을 선택합니다. |
| **기간 검색** | 조회하고자 하는 기간을 선택합니다. |
| **아이피 검색** | 검색한 아이피를 기준으로 리스트와 차트를 조회할 수 있습니다. |
| **매크로 리스트** | 웹 서비스에 접속하지 못하고 차단된 매크로를 보여줍니다.   |  |  | | --- | --- | | No | 리스트 순번 | | 접속 아이피 | 웹 서비스에서 차단된 아이피를 보여줍니다. | | 차단 건수 | 해당 아이피가 차단된 건수를 보여줍니다. | | 상세 | 해당 아이피의 상세정보 페이지로 이동합니다. | |
| **차트 유형** | 월별, 주별. 일별, 시간별 중 하나를 선택해 차트를 조회할 수 있습니다. |
| **차트** | 차트 유형에 따른 접속자 건수를 보여줍니다. 월별 차트 클릭 시 주별 차트를 확인할 수 있습니다.  주별 차트 클릭 시 일별 차트를 확인할 수 있습니다.  일별 차트 클릭 시 시간별 차트를 확인할 수 있습니다.  시간별 차트를 좌우로 드래그하여 해당 시간에 대한 데이터만 조회 가능합니다. |

**5.2 차단 증적 자료**

차단 증적 자료는 사용자가 어떤 이유로 차단되었는지 확인하고 증적 자료를 엑셀로 다운받을 수 있는 페이지입니다.

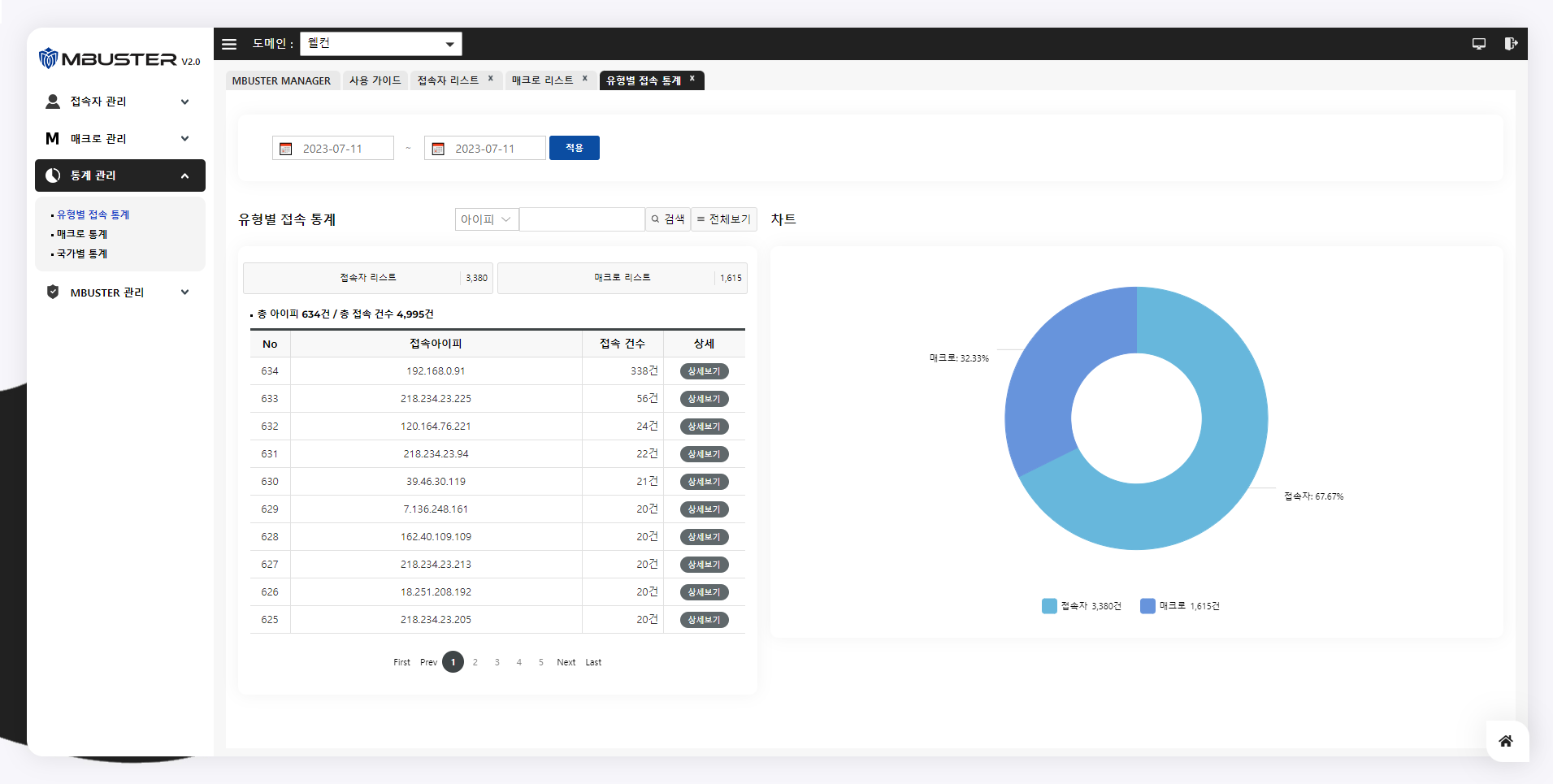
<차단 증적 자료>

|  |  |
| --- | --- |
| **항목** | **설명** |
| **엑셀 다운로드** | 차단 증적 자료를 엑셀로 다운로드 할 수 있습니다. |
| **차단 시간** | 매크로가 차단된 시간을 보여줍니다. |
| **아이피** | 차단된 매크로의 아이피를 보여줍니다. |
| **식별아이디** | 사용자를 구분하는 값입니다. |
| **아이디** | 로그인에 사용한 아이디를 보여줍니다. |
| **차단원인** | 매크로의 차단 원인을 확인할 수 있습니다. |

**6. 통계 관리**

**6.1 유형별 접속 통계**

유형별 접속 통계는 전체 접속자 중 실제 접속자와 접속하지 못하고 차단된 매크로를 한눈에 비교해 볼 수 있도록 통계 정보를 제공하는 페이지입니다.



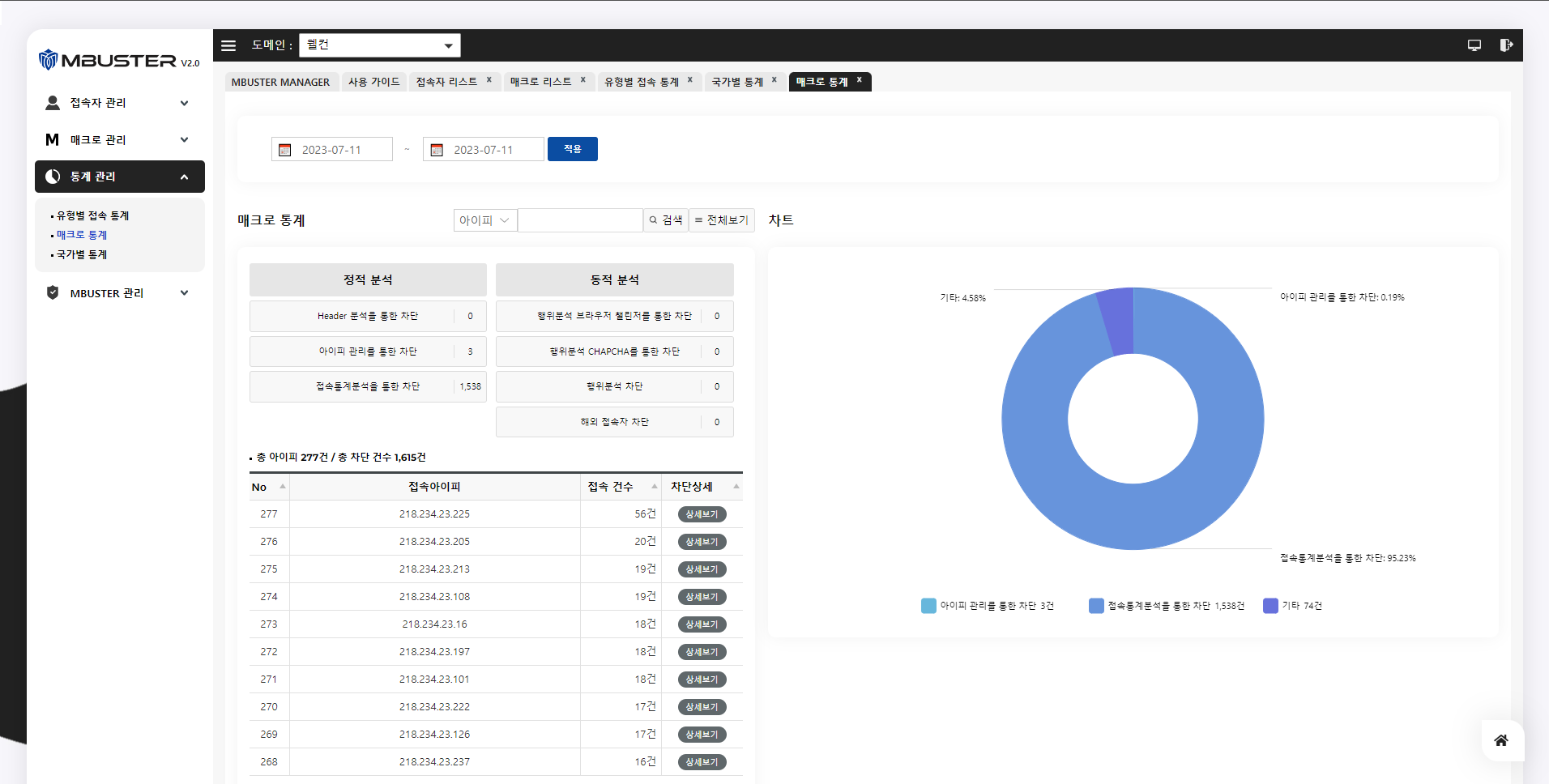
<유형별 접속 통계>

|  |  |
| --- | --- |
| **항목** | **설명** |
| **도메인** | 조회하고자 하는 도메인을 선택합니다. |
| **기간 검색** | 조회하고자 하는 기간을 선택합니다. |
| **아이피 검색** | 검색한 아이피를 기준으로 리스트와 차트를 조회할 수 있습니다. |
| **유형별 접속 리스트** | 접속자 리스트와 매크로 리스트 각 탭에 총 몇 건의 접속이 있었는지 보여주며, 탭을 클릭할 경우 탭의 내용에 맞게 리스트와 차트 데이터가 변경됩니다.   |  |  | | --- | --- | | No | 리스트 순번 | | 접속 아이피 | 웹 서비스에서 접속한/차단된 아이피를 보여줍니다. | | 접속/차단 건수 | 해당 아이피가 접속한/차단된 건수를 보여줍니다. | | 상세 | 해당 아이피의 상세정보 페이지로 이동합니다. | |
| **유형별 접속 통계** | 매크로와 접속자의 비율을 보여줍니다.  차트 클릭시 옆의 리스트에서도 해당 정보를 볼 수 있습니다. |

**6.2 매크로 통계**

매크로 통계는 MBUSTER의 어떤 매크로 차단 엔진에 의해 매크로가 차단되었는지 보여주는 통계 페이지입니다.

데이터 조회의 경우 응답시간 10초 이내에 응답하며, CPU 30%. Memory50% 이내 사용합니다.



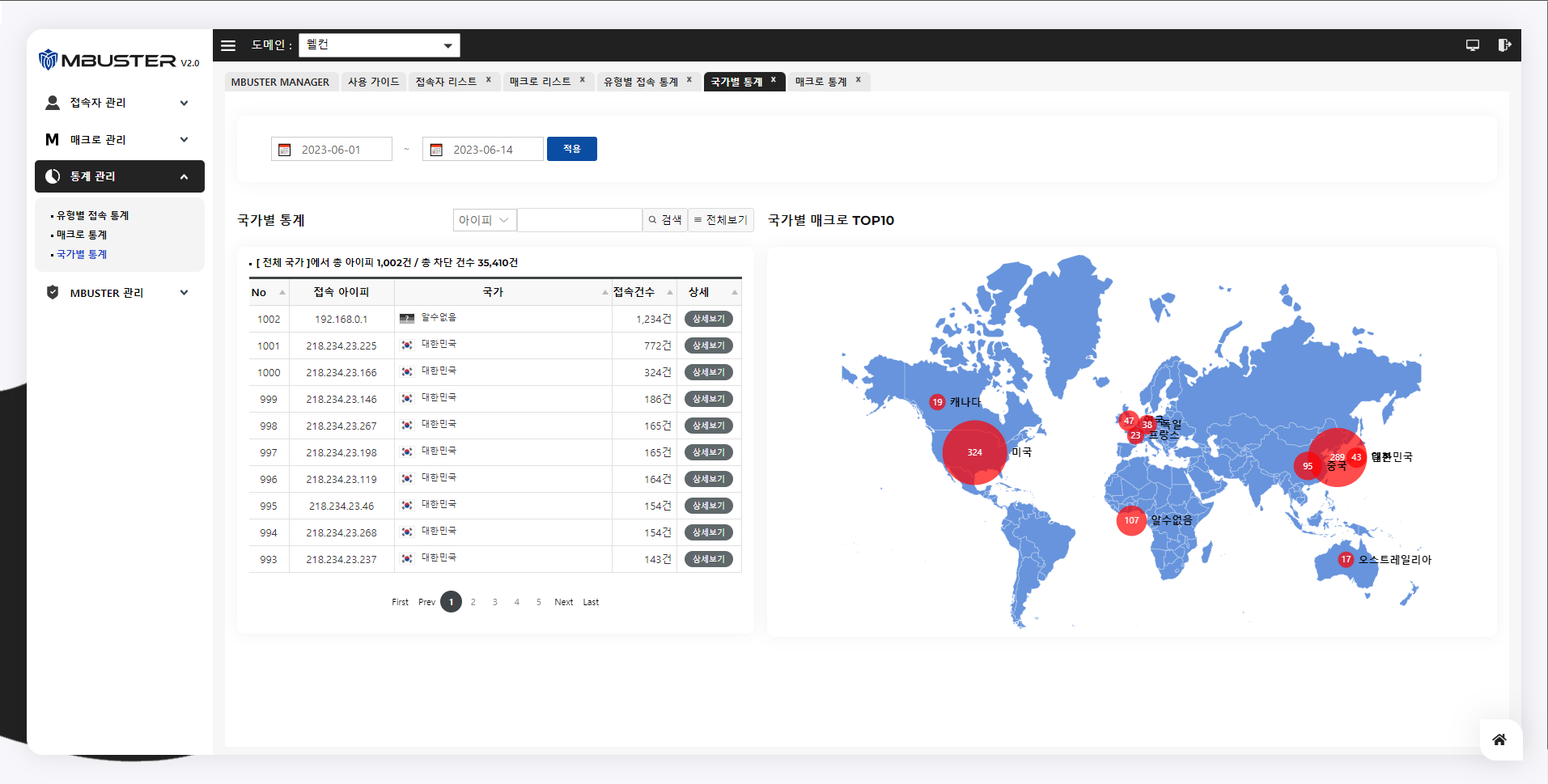
<매크로 통계>

|  |  |
| --- | --- |
| **항목** | **설명** |
| **도메인** | 조회하고자 하는 도메인을 선택합니다. |
| **기간 검색** | 조회하고자 하는 기간을 선택합니다. |
| **아이피 검색** | 검색한 아이피를 기준으로 리스트와 차트를 조회할 수 있습니다. |
| **매크로 통계** | MBUSTER가 정의하는 정적분석/동적분석 엔진을 구분하여 보여주고, 어떤 엔진으로 매크로가 차단되었는지 분석할 수 있도록 리스트를 제공합니다. 각 탭을 클릭할 경우 탭의 내용에 맞게 리스트와 차트 데이터가 변경됩니다.   |  |  | | --- | --- | | No | 리스트 순번 | | 접속 아이피 | 웹 서비스에서 차단된 아이피를 보여줍니다. | | 차단 건수 | 해당 아이피가 차단된 건수를 보여줍니다. | | 차단 상세 | 해당 아이피의 상세정보 페이지로 이동합니다. | |
| **차트** | 매크로 차단 엔진별 수량과 비율을 나타냅니다.  차트 클릭시 옆의 리스트에서도 해당 정보를 볼 수 있습니다. |

**6.3 국가별 통계**

국가별 통계는 매크로가 어느 국가에서 들어왔는지 지도에 표시하여 한눈에 볼 수 있게끔 통계 정보를 제공합니다.

데이터 조회의 경우 응답시간 10초 이내에 응답하며, CPU 30%. Memory50% 이내 사용합니다.

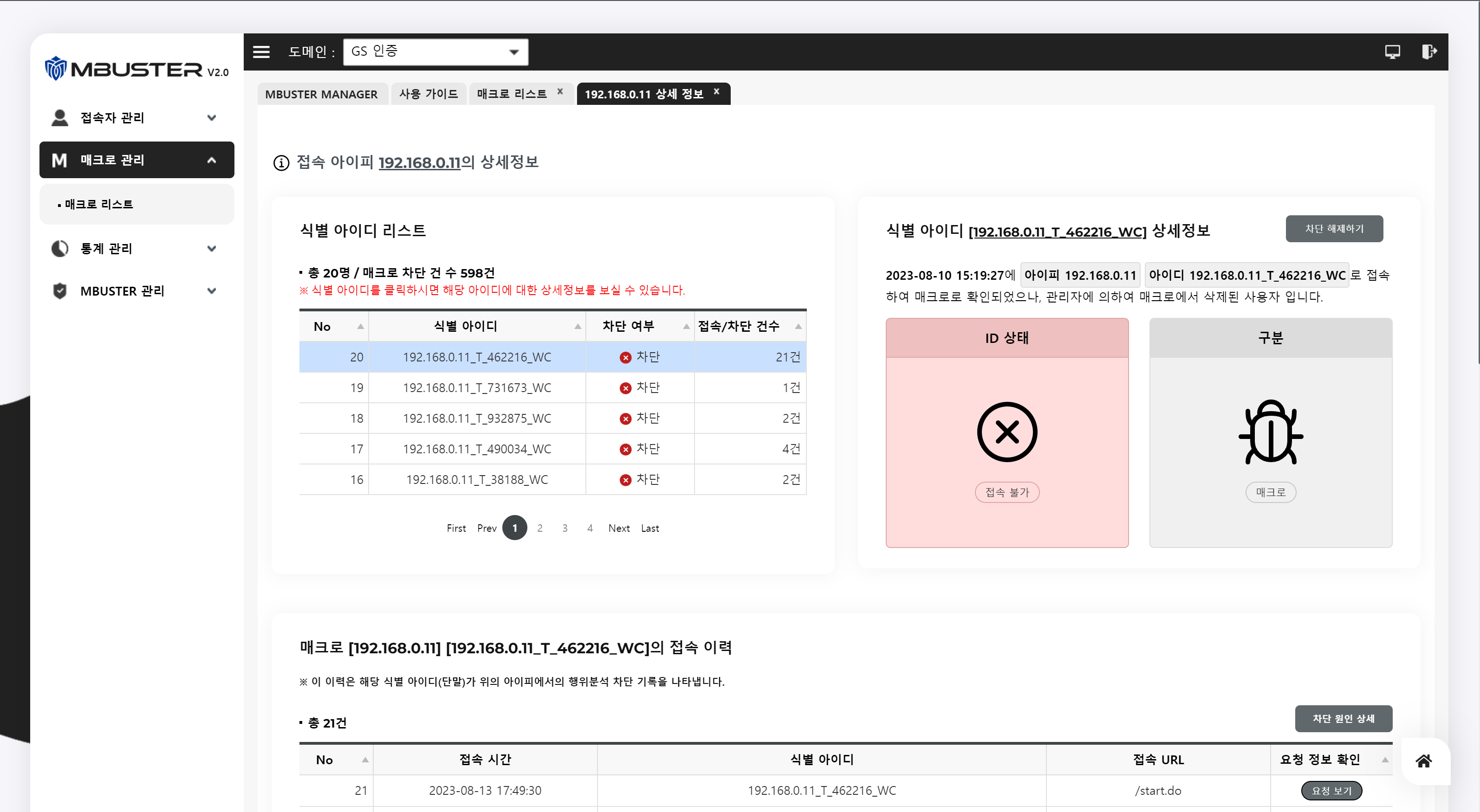


<국가별 통계>

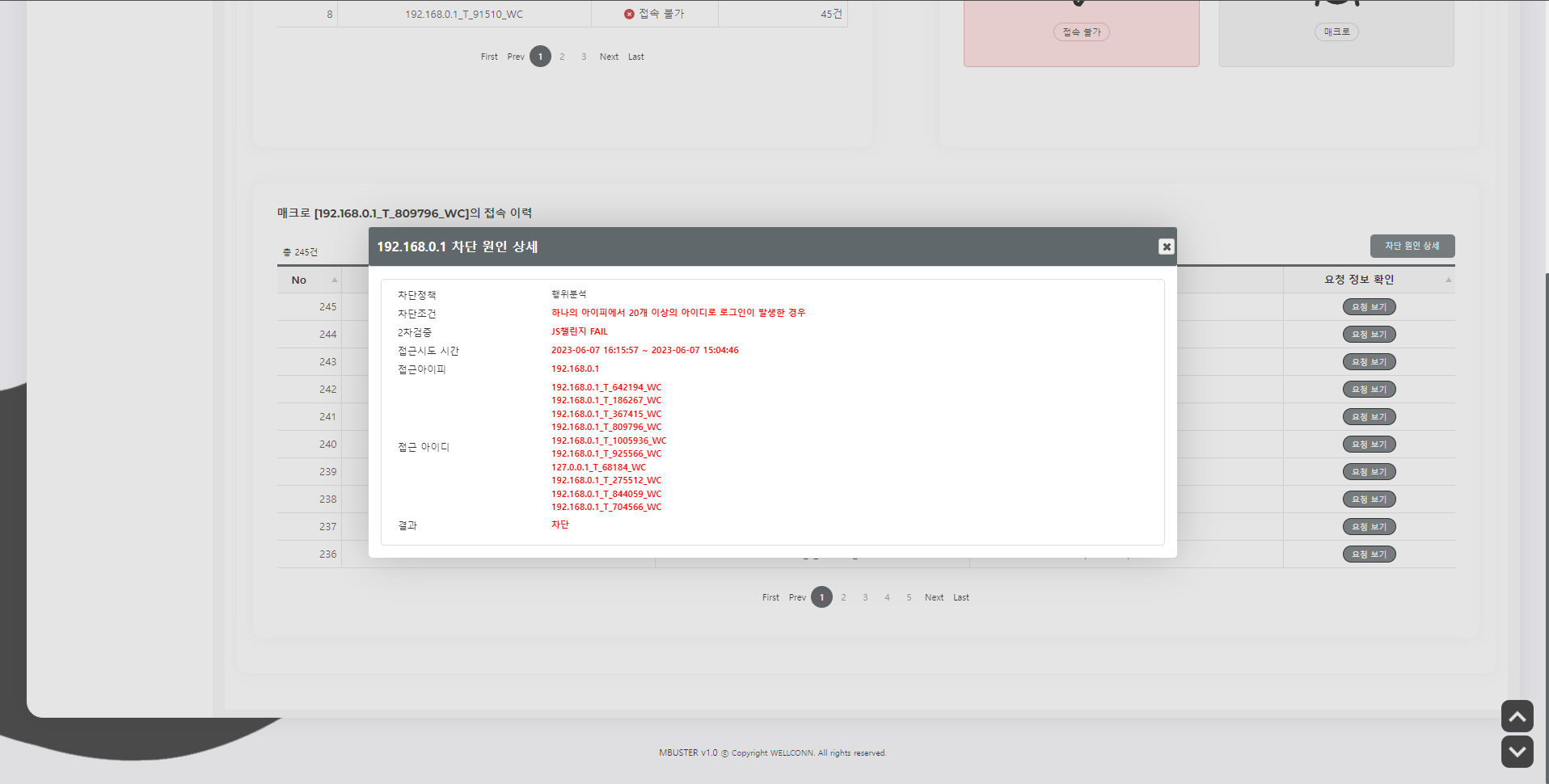
|  |  |
| --- | --- |
| **항목** | **설명** |
| **도메인** | 조회하고자 하는 도메인을 선택합니다. |
| **기간 검색** | 조회하고자 하는 기간을 선택합니다. |
| **아이피 검색** | 검색한 아이피를 기준으로 리스트와 차트를 조회할 수 있습니다. |
| **매크로 통계** | 매크로가 많은 국가 10곳을 리스트업하여 해당 국가에서 접속한 매크로 리스트를 국가 정보와 함께 보여줍니다.   |  |  | | --- | --- | | No | 리스트 순번 | | 접속 아이피 | 웹 서비스에서 차단된 아이피를 보여줍니다. | | 국가 | 해당 아이피의 국가 정보를 보여줍니다. | | 차단 건수 | 해당 아이피가 차단된 건수를 보여줍니다. | | 차단 상세 | 해당 아이피의 상세정보 페이지로 이동합니다. | |
| **국가별 매크로 TOP10** | 매크로가 많은 국가 10곳을 지도에 표시하여 보여줍니다. |

**7. 아이피 상세 정보**

아이피 상세정보는 해당 아이피로 접속한 사용자들을 식별 아이디로 구분하여 각 사용자의 접속상태와 접속 이력을 보여주는 페이지입니다.

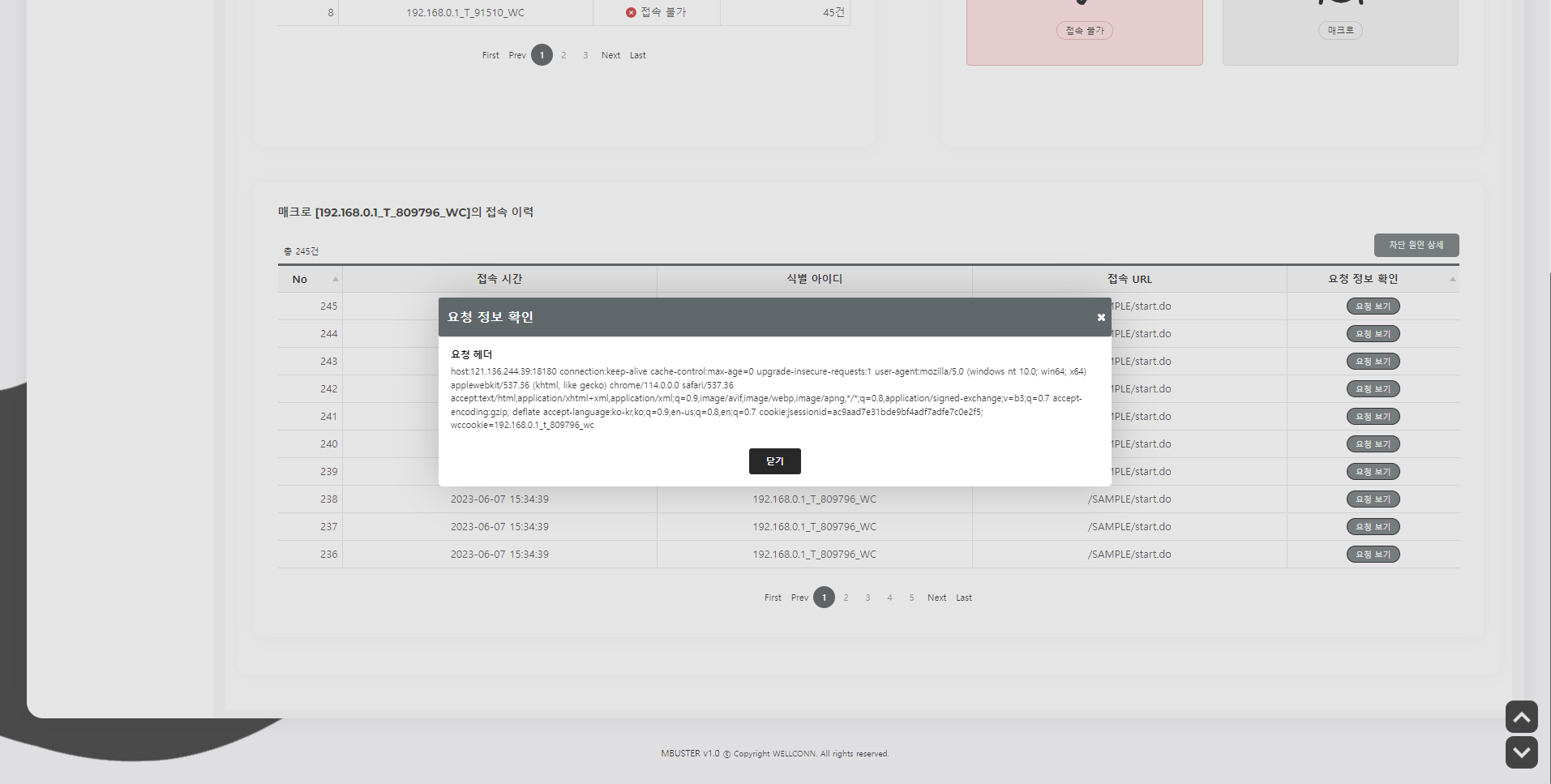


<아이피 상세 정보>



<차단 원인 상세 예시>

|  |  |
| --- | --- |
| **항목** | **설명** |
| **식별 아이디 리스트** | 해당 아이피로 접속한 사용자들을 식별 아이디로 구분하여 접속 가능 상태와 접속 건수를 알려줍니다.   |  |  | | --- | --- | | No | 리스트 순번 | | 식별 아이디 | 사용자를 구분하는 값 | | 차단 여부 | 사용자가 접속했었는지 차단되었는지에 대한 당시 상태를 보여줍니다. | | 접속/차단 건수 | 사용자의 접속/차단 건수를 보여줍니다.  \* 유형별 접속 통계처럼 차단여부가 접속/차단자가 함께 표기되는 경우가 있어 ‘접속/차단 건수’로 표기 | |
| **식별 아이디 상세정보** | 해당 ID와 현재 상태와 구분을 시각적으로 보여줍니다.  해당 ID에 대한 차단 및 차단해제를 할 수 있습니다.  ‘차단하기’로 차단한 경우 해당 아이디가 차단 목록에 들어가 있음을 [MBUSTER 관리>정책 설정>정적 분석>아이피 관리를 통한 차단] 에서도 확인할 수 있습니다.  ID상태: 접속 가능/접속 불가  구분: 일반유저/매크로  \* 개인 식별 아이디 부여방법  - 개인 식별 아이디는 최초 접속시 (개인 식별 아이디가 없는 경우) 현재 접속한 아이피 기준으로 생성됩니다.  - 이후 요청에서는 앞에서 발급된 개인식별아이디를 사용합니다  - 아이피가 변경되어 접속을 하더라도 개인 식별 아이디는 변경되지 않습니다 |
| **차단 원인 상세** | 사용자가 ‘매크로’일 경우 차단 원인을 보여줍니다. |
| **사용자/매크로 [아이피] [식별 아이디]의 접속 이력** | 해당 아이피와 식별 아이디를 가진 사용자가 접속한/차단유형별 차단된 이력을 보여줍니다.   |  |  | | --- | --- | | No | 리스트 순번 | | 접속 시간 | 사용자가 접속한 시간 | | 식별 아이디 | 사용자를 구분하는 값 | | 접속 URL | 사용자가 접속한 URL 정보 | | 요청 정보 확인 | 요청 보기 버튼을 클릭하면 해당 요청에 대한 헤더 정보 값을 확인할 수 있습니다 | |
| **사용자/매크로 [아이피] [식별 아이디]의 접속 이력** | 해당 식별 아이디를 가진 사용자가 접속한 모든 이력을 보여줍니다.   |  |  | | --- | --- | | No | 리스트 순번 | | 접속 시간 | 사용자가 접속한 시간 | | 식별 아이피 | 사용자의 IP | | 식별 아이디 | 사용자를 구분하는 값 | | 접속 URL | 사용자가 접속한 URL 정보 | | 요청 정보 확인 | 요청 보기 버튼을 클릭하면 해당 요청에 대한 헤더 정보 값을 확인할 수 있습니다 | |



<요청 정보 확인 예시>

**8. MBUSTER 관리**

**8.1 도메인 생성**

매크로 차단을 수행할 사이트의 도메인을 등록하는 페이지입니다.



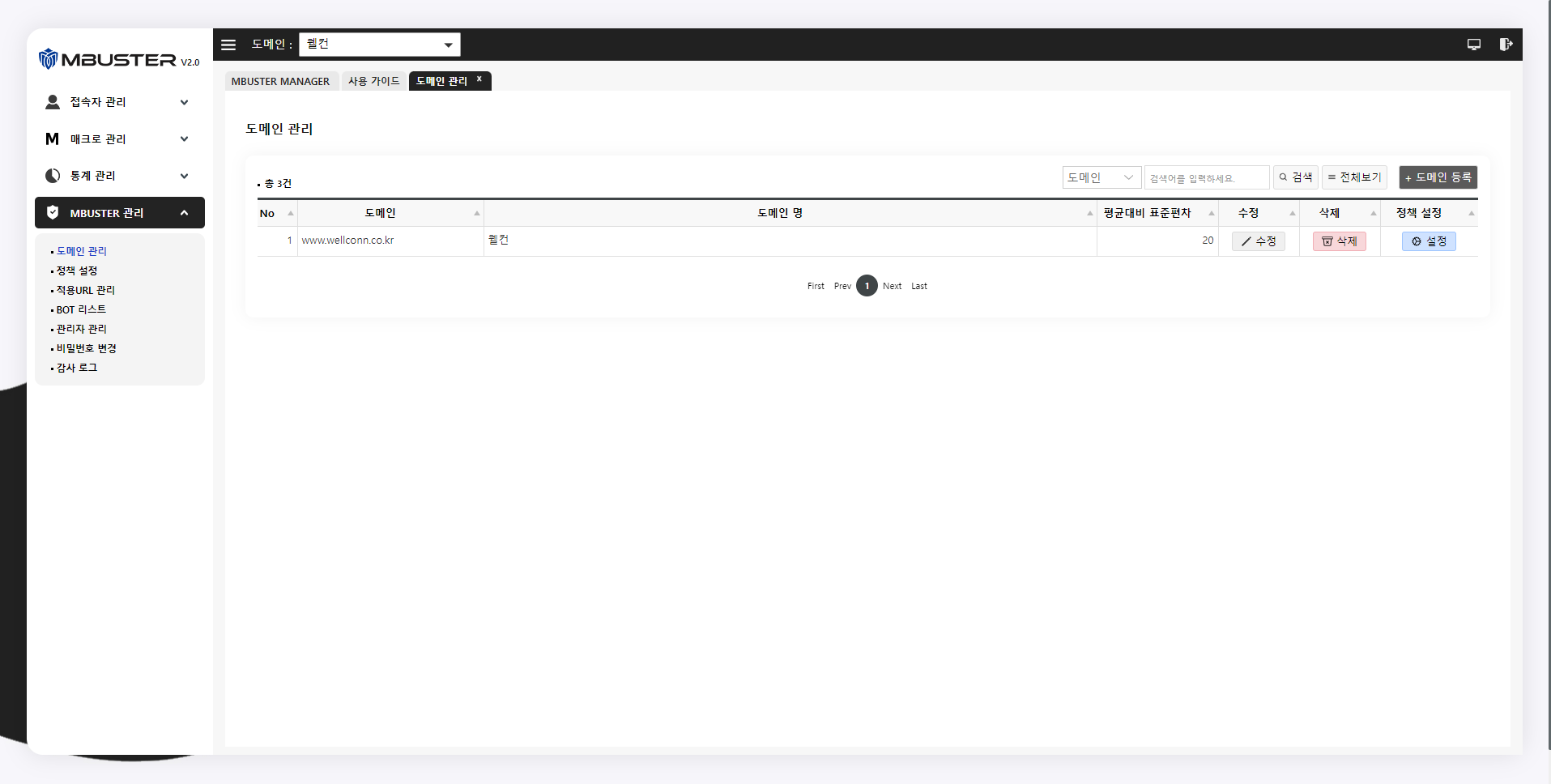
<도메인 생성>

|  |  |
| --- | --- |
| **항목** | **설명** |
| **도메인 별칭** | 도메인을 구별할 수 있는 별칭 등록 |
| **도메인** | 실제 매크로 차단을 수행할 사이트의 도메인을 입력 |

**8.2 도메인 관리**

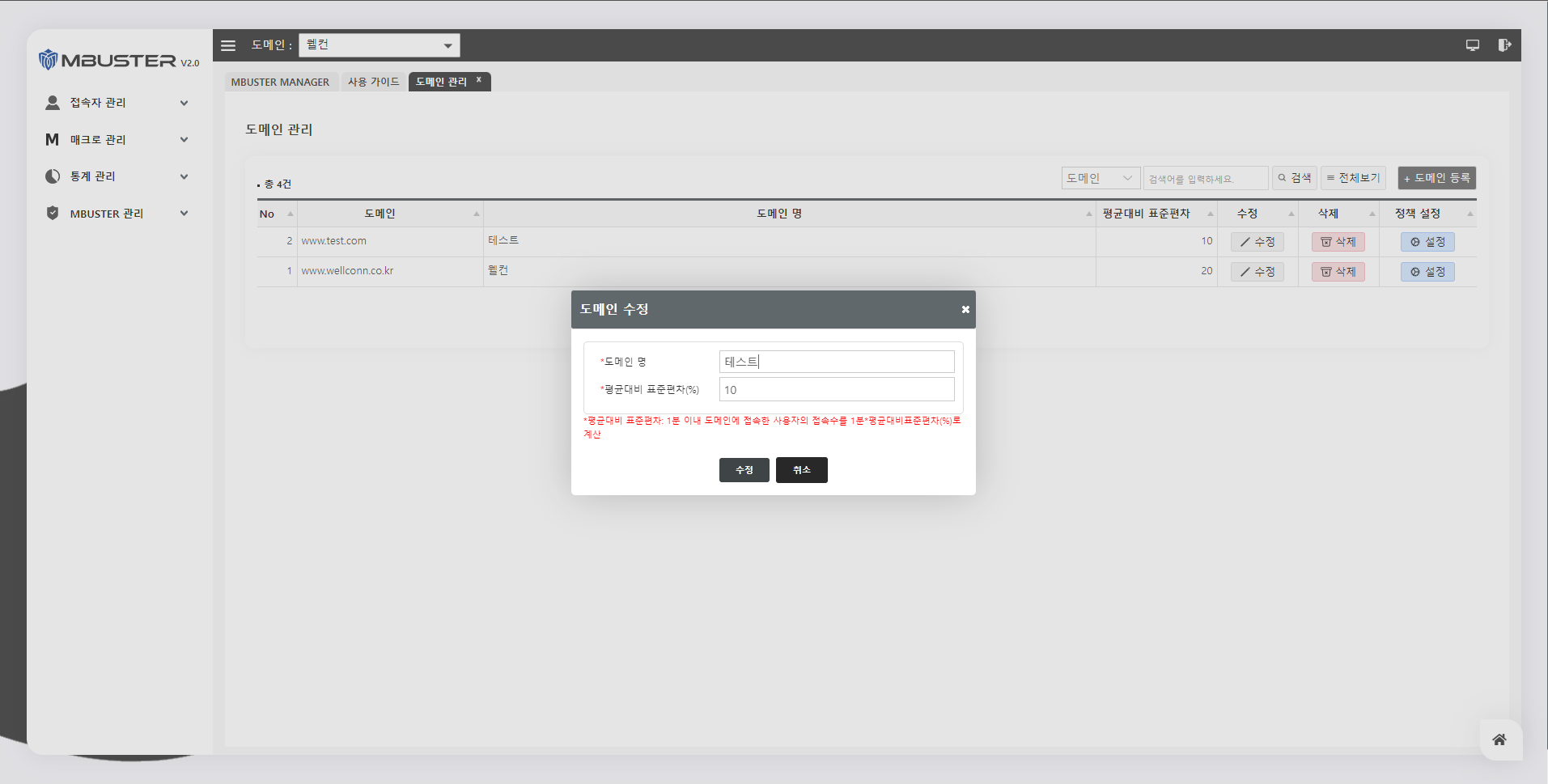
도메인 관리는 매크로 차단을 적용할 도메인을 수정/삭제하는 페이지입니다.

도메인 등록은 도메인 생성 메뉴에서 하실 수 있습니다.



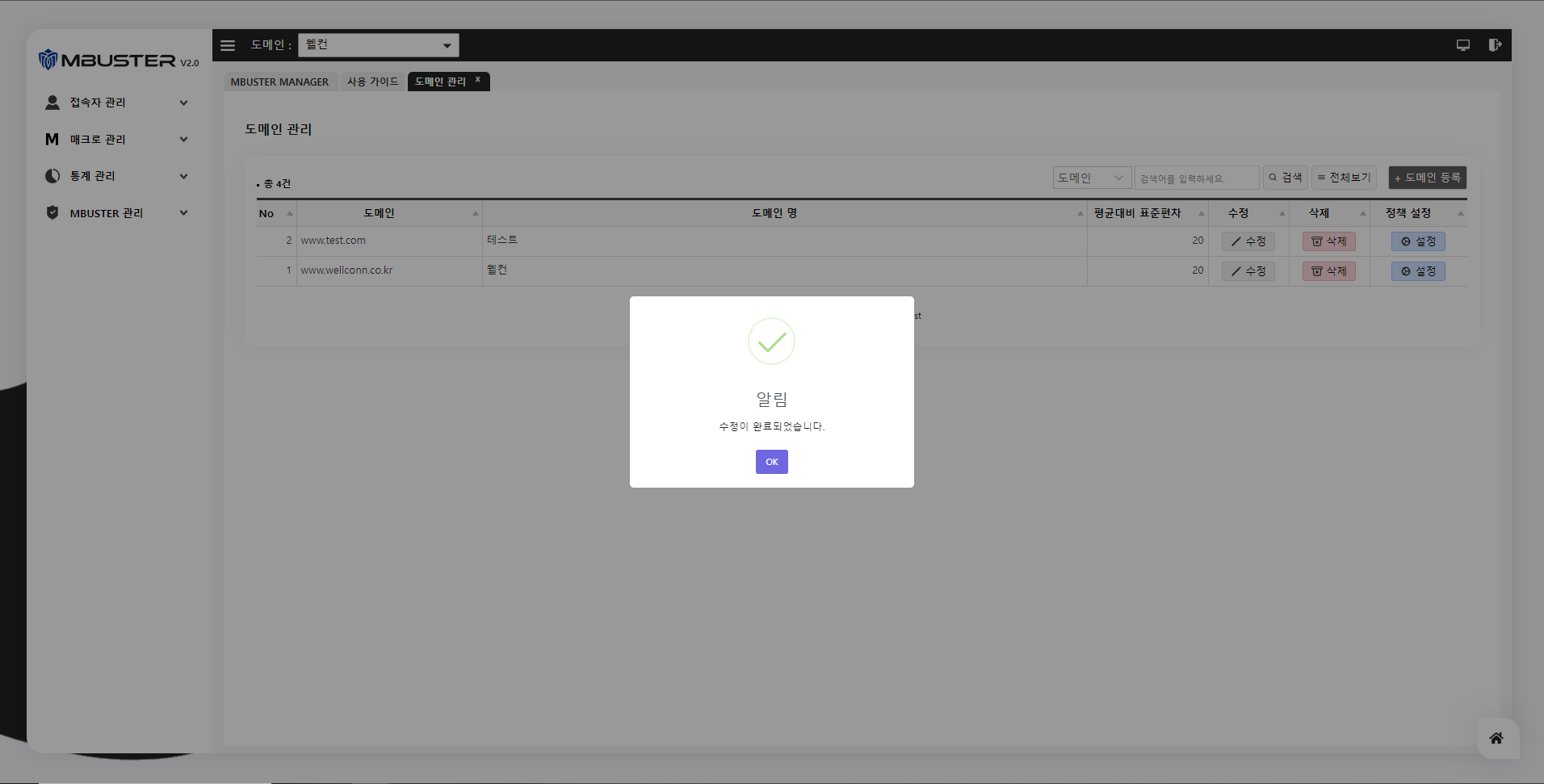
<도메인 관리>

|  |  |
| --- | --- |
| **항목** | **설명** |
| **도메인 검색** | 리스트 내 도메인 검색 기능 |
| **No** | 리스트 순번 |
| **도메인** | 적용 대상 사이트 도메인 |
| **도메인명** | 도메인 별칭 |
| **평균대비 표준편차** | 통계기반 차단 접속 횟수 기준치에 사용될 계산값 |
| **수정** | 도메인 수정을 할 수 있는 버튼 |
| **삭제** | 도메인 삭제를 할 수 있는 버튼 |
| **정책 설정** | 해당 도메인에 대해 정책 설정을 할 수 있는 페이지로 이동 |

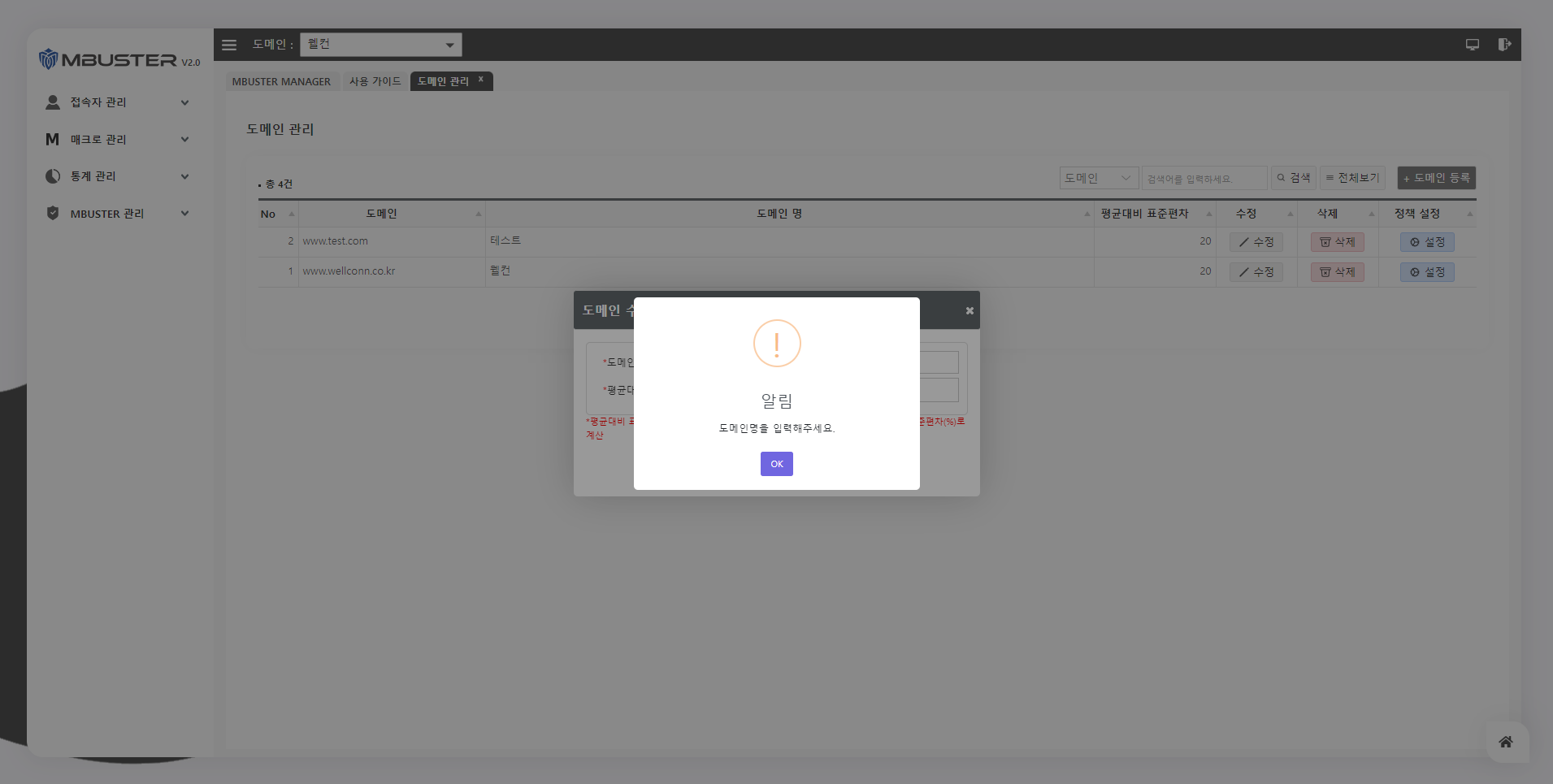


<도메인 수정>

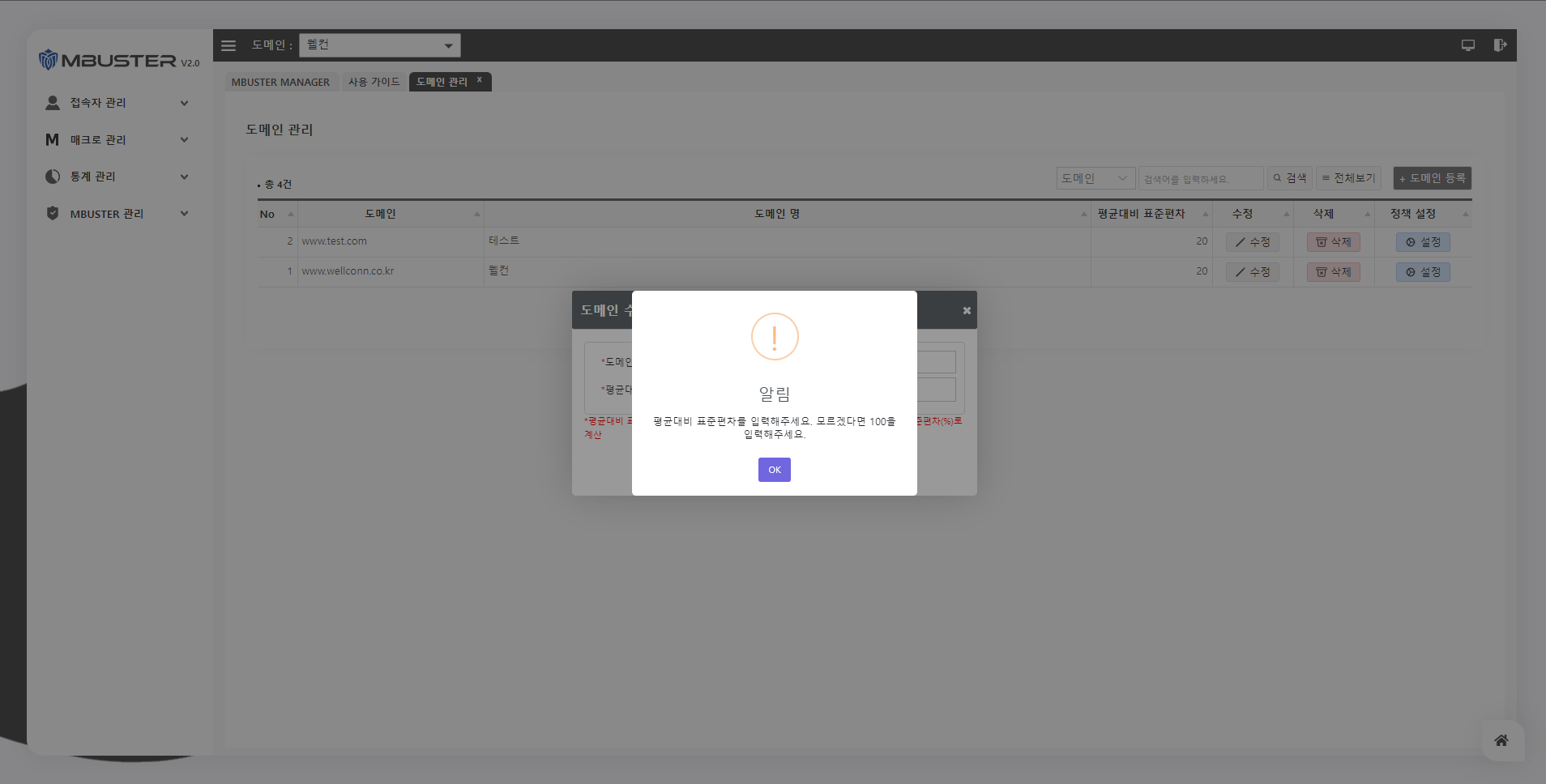
|  |  |
| --- | --- |
| **항목** | **설명** |
| **도메인 명** | 도메인 별칭. 한글, 영어 등 문자와 숫자 입력 가능합니다.  사용 가능한 특수문자 : ~!@#$%^\*()\_-=  미입력시 알림창 발생합니다. |
| **평균대비 표준편차** | 통계기반 차단 접속 횟수 기준치에 사용될 계산값.  숫자만 입력할 수 있습니다.  미입력시 알림창 발생합니다. |



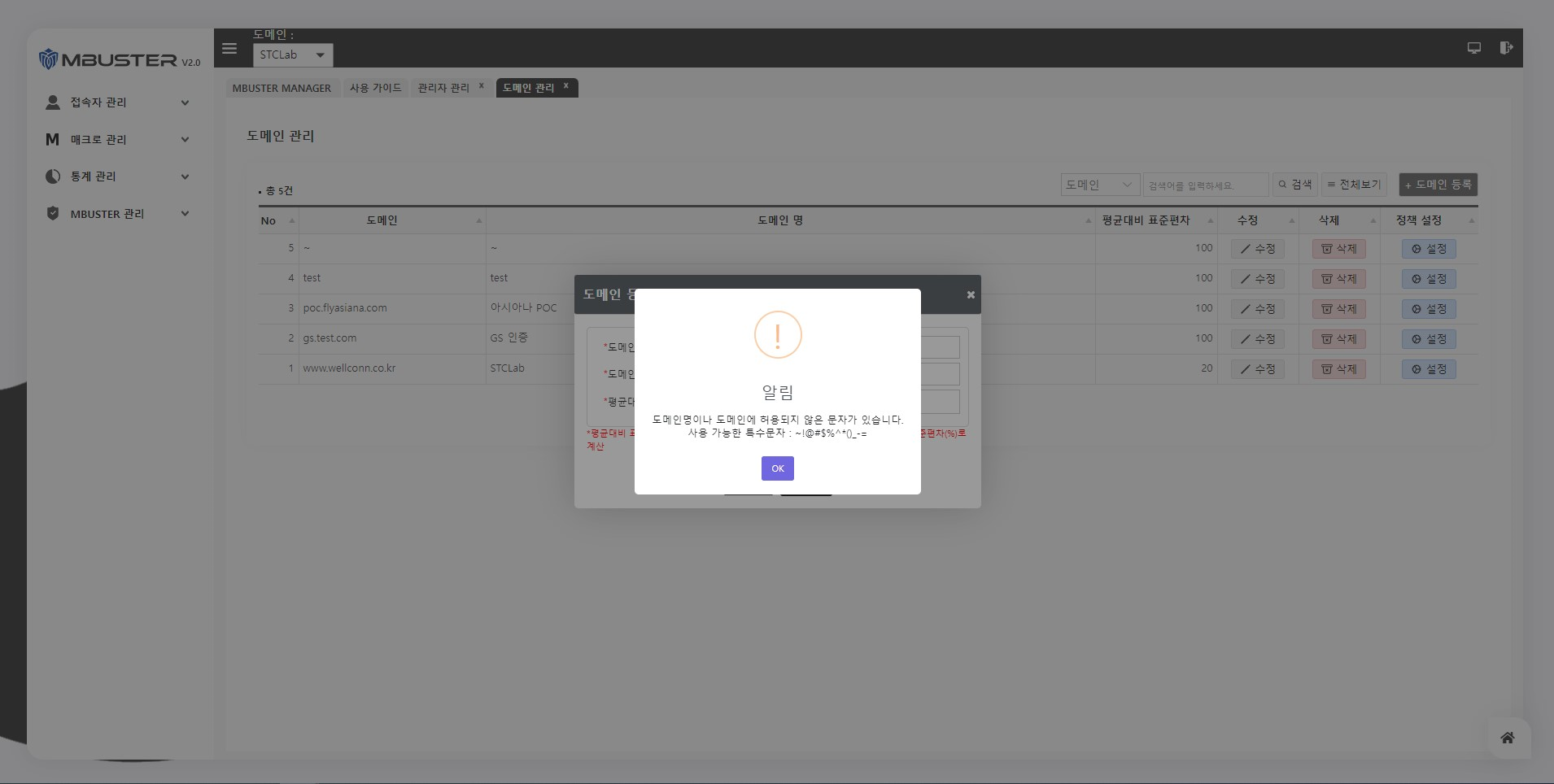
<도메인 수정 성공 알림>

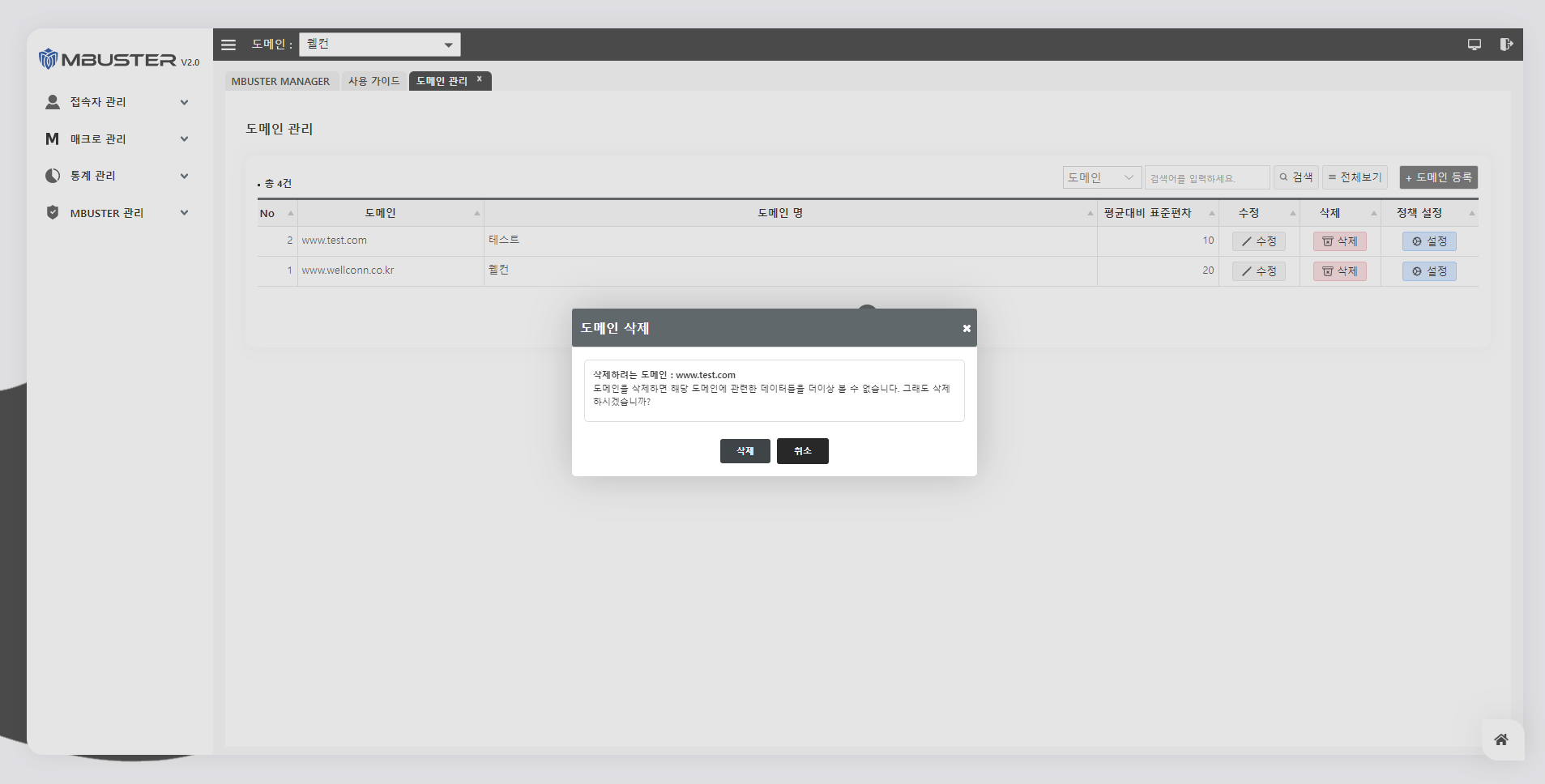


<도메인명 미입력시 알림>

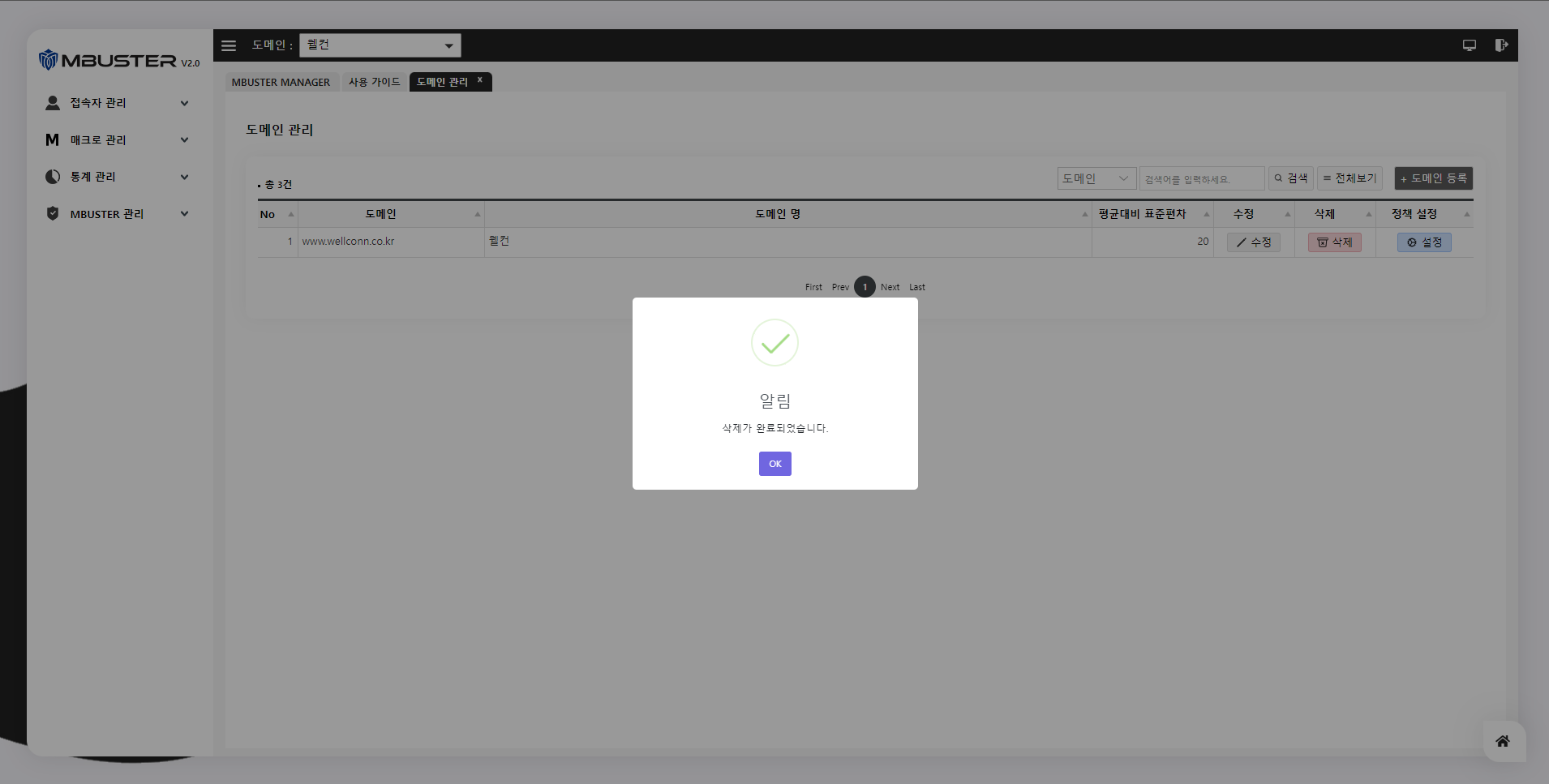


<평균대비 표준편차 미입력시 알림>

<사용 불가 문자 입력시 알림>



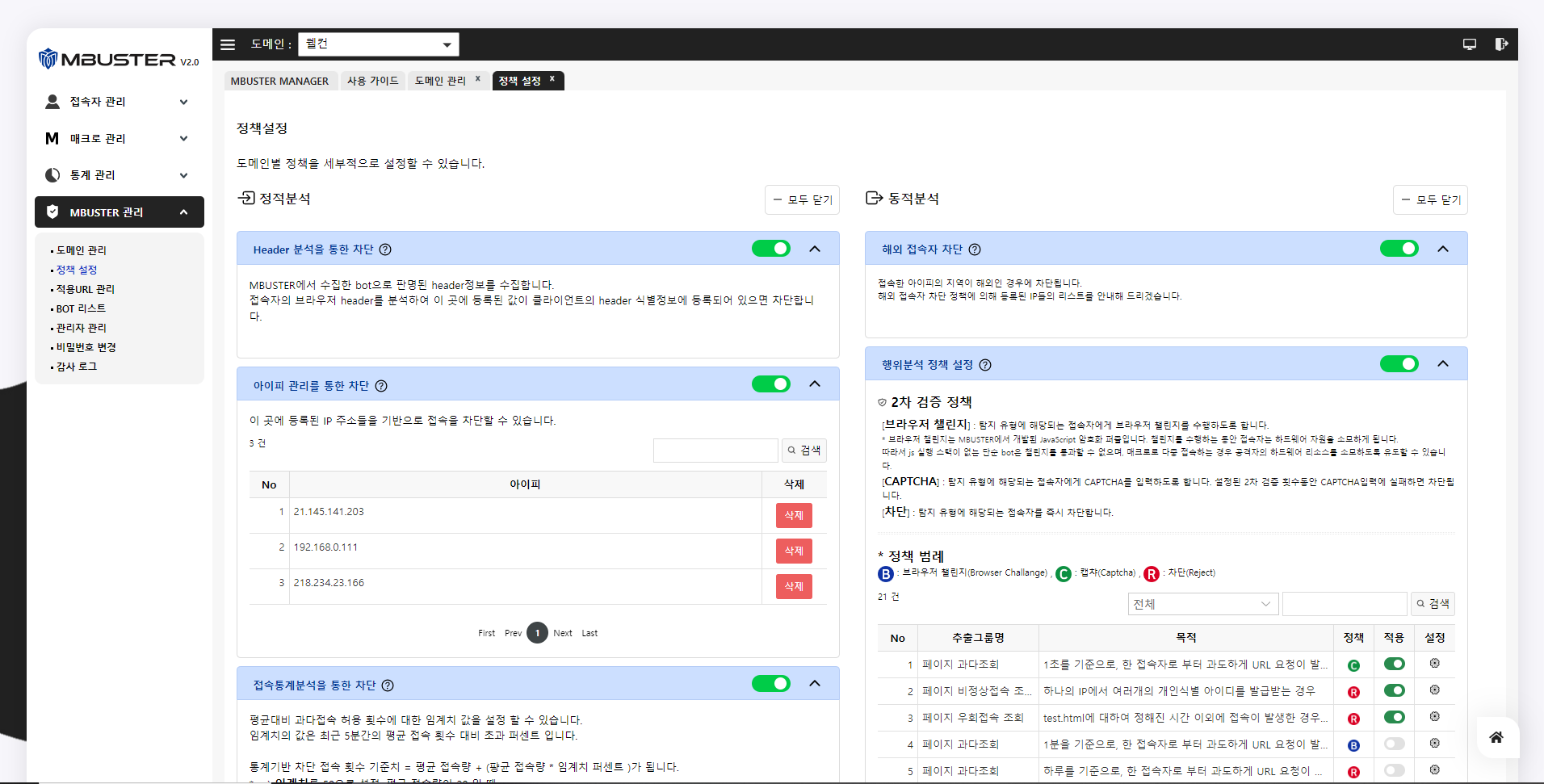
<도메인 삭제 확인 팝업>



<도메인 삭제 성공 알림>

**8.3 정책 설정**

정책 설정은 선택된 도메인에 대하여 각 매크로 차단 정책을 ON/OFF 시키고, 행위분석 조건에 대해 임계치 및 2차 검증 정책을 설정할 수 있는 페이지입니다.



<정책 설정>

\* 분석 정책별 토글 스위치: 정적/동적 분석의 다섯가지 정책을 켜고 끌 수 있습니다.

단, 행위분석 정책 설정이 ON 되어있더라도 각 행위분석 하위 설정이 OFF 되어있는 경우

정책이 동작하지 않습니다.

\* 행위분석 정책별 토글 스위치: 각 행위분석 별로 정책을 켜고 끌 수 있습니다.

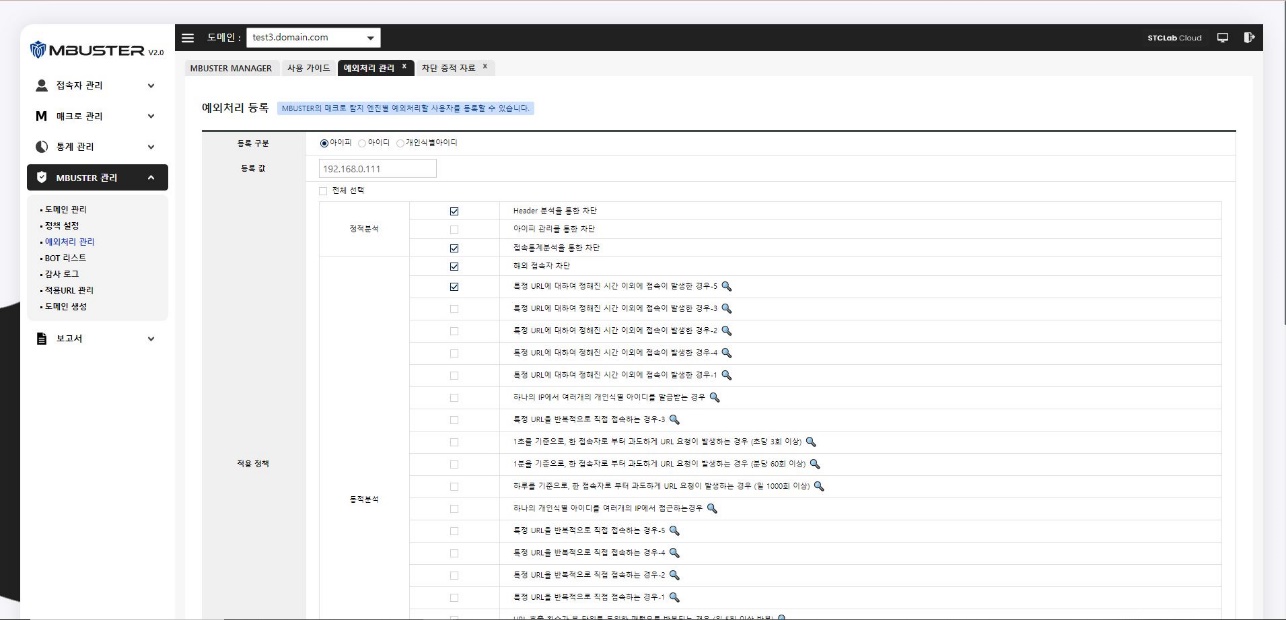
단, 행위분석 정책 설정이 OFF 되어있는 경우 각 행위분석 하위 설정이 ON 이더라도 정책이 동작하지 않습니다.

|  |  |
| --- | --- |
| **항목** | **설명** |
| **Header 분석을 통한 차단** | 웹 사이트에 접속하는 사용자의 요청 헤더값을 분석하여 매크로를 차단할지 여부를 설정합니다. 정적분석에 해당합니다. |
| **아이피 관리를 통한 차단** | MBUSTER가 관리하는 BOT　IP 및 차단 설정된 IP에 대해 차단할지 여부를 설정합니다. 정적분석에 해당합니다. |
| **접속통계분석을 통한 차단** | 접속통계분석을 통해 사용자를 차단할지 여부를 설정합니다. 평균대비 과다접속 허용 횟수에 대한 임계치 값을 설정 할 수 있습니다. 임계치의 값은 평균 접속 횟수 대비 초과 퍼센트입니다. 정적분석에 해당합니다. |
| **해외 접속자 차단** | 접속한 아이피의 지역이 해외인 경우에 차단할지 여부를 설정합니다. 동적분석에 해당합니다.  \* 해외접속자로 차단된 경우, 해당사용자가 국내에서 접속을 다시 하더라도 차단상태, 개인식별아이디를 해제하여야 정상적으로 접속가능합니다. |
| **행위분석 정책 설정** | 행위분석에 따라 사용자를 차단할지 여부를 설정합니다.  [페이지 과다조회]  특정 URL을 과다하게 요청하는 경우,  특정 시간을 기준으로 한 접속자로부터 과도하게 URL 요청이 발생 할 경우.  [페이지 반복조회]  URL 호출 횟수가 분 단위로 동일한 패턴으로 반복되는 경우.  [페이지 우회접속 조회]  특정페이지에 대하여 정해진 시간 이외에 접속이 발생한 경우.  [페이지 비정상접속 조회]  특정 URL을 반복적으로 직접 접속하는 경우.  하나의 개인식별 아이디를 여러개의 IP에서 접근하는 경우.  하나의 IP에서 여러개의 개인식별 아이디를 발급받는 경우.  \* [페이지 비정상접속 조회 정책] 중‘하나의 IP에서 여러개의 개인식별 아이디를 발급받는 경우’의 예외사항: MBUSTER의 행위분석은 IP 단위가 아닌 개인 식별 아이디 단위(단말별)로 관리하는 것을 원칙으로 합니다. 하나의 IP에서 여러 개의 단말을 통해 들어오는 경우, 해당 IP는 비정상 행위의 원천지 아이피로 간주하여 개인식별 단위가 아닌 IP 자체를 차단합니다. 이러한 차단의 경우 일반 관리자의 해지가 불가능 하며, 엔지니어에게 기술지원 요청을 통해 해지해야 합니다. |

|  |  |
| --- | --- |
| **항목** | **설명** |
| **행위분석 정책 설정** | |  |  | | --- | --- | | No | 리스트 순번 | | 매크로 탐지 | 행위분석 조건 | | 임계치 | 해당 행위 분석 유형에서 접속자의 행위 유형을 감지하기 위한 임계값. 숫자만 입력가능합니다. | | 2차 검증 정책 | [브라우저 챌린지] : 탐지 유형에 해당되는 접속자에게 브라우저 챌린지를 수행하도록 합니다.  \* 브라우저 챌린지는 MBUSTER에서 개발된 JavaScript 암호화 퍼즐입니다. 챌린지를 수행하는 동안 접속자는 하드웨어 자원을 소모하게 됩니다.  따라서 js 실행 스택이 없는 단순 bot은 챌린지를 통과할 수 없으며, 매크로로 다중 접속하는 경우 공격자의 하드웨어 리소스를 소모하도록 유도할 수 있습니다.  [CAPTCHA] : 탐지 유형에 해당되는 접속자에게 CAPTCHA를 입력하도록 합니다. 설정된 2차 검증 횟수동안 CAPTCHA입력에 실패하면 차단됩니다.  [차단] : 탐지 유형에 해당되는 접속자를 즉시 차단합니다. | | 2차 검증 횟수 | 2차 검증을 몇 번 진행할지 설정합니다. 설정값을 초과할 경우 매크로로 간주되어 차단됩니다. | | 대상 URL | 감지할 URL을 지정 할 수 있습니다. | | 시작,종료시간 | [페이지 우회접속 조회]에서 시작시간과 종료시간을 지정후 이외의 시간에 접속시 정책을 적용 할 수 있습니다 | |

\* 행위분석 정책 설정의 경우 수집된 로그 기반으로 분석하여 등록되는 정책으로 실시간이 아닌 배치작업으로 진행됩니다.

**8.4 예외처리 관리**

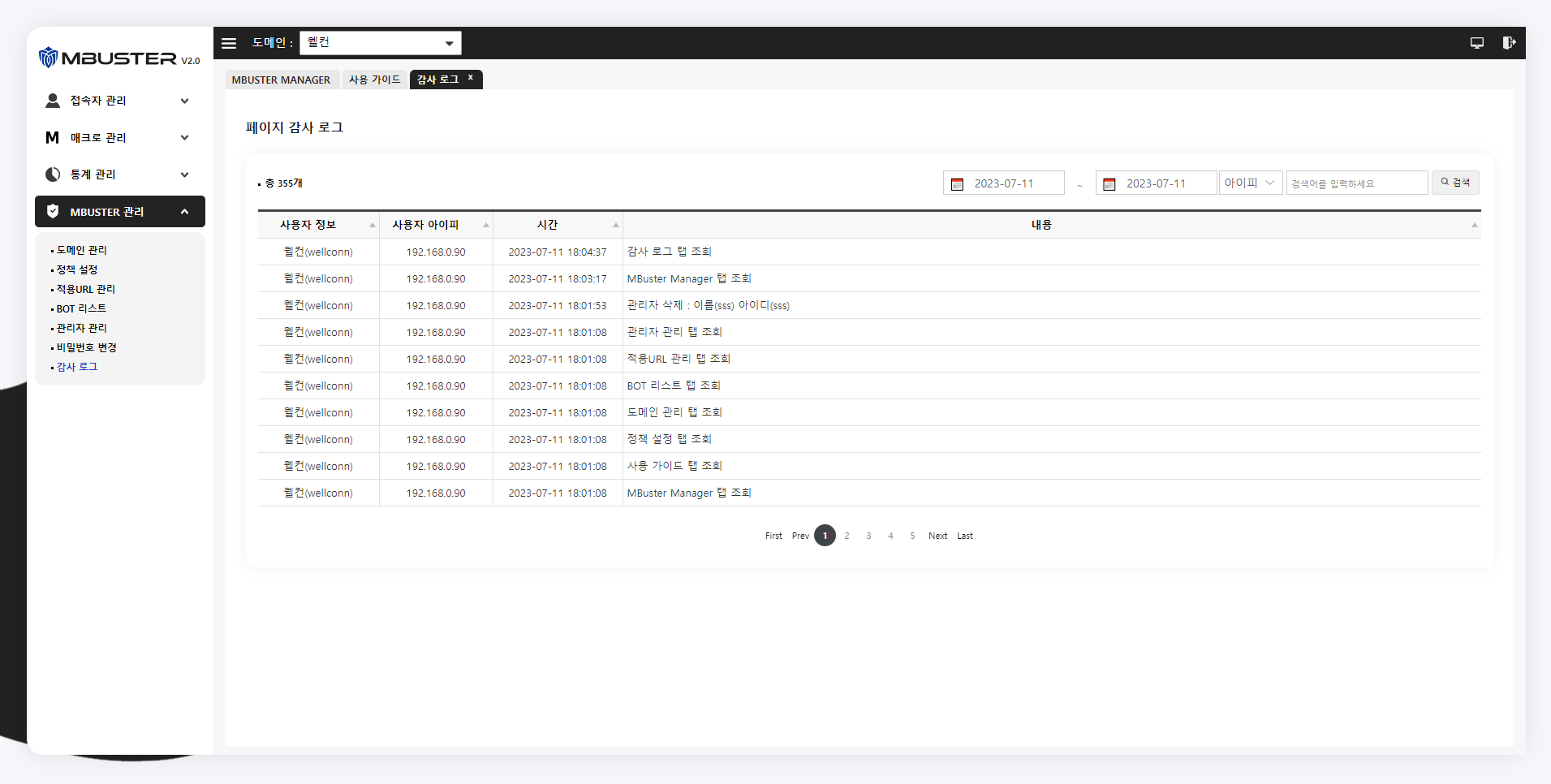
예외처리 관리는 MBUSTER가 매크로로 판단하더라도 예외사항을 적용하여 특정 유저를 차단하지 않도록 설정하는 페이지입니다.

<예외 처리 관리 >

|  |  |
| --- | --- |
| **항목** | **설명** |
| 둥록 구분 | 예외처리를 적용할 값의 유형을 선택합니다. 아이피/아이디/개인식별아이디 중 선택할 수 있습니다., |
| 등록 값 | 예외처리를 적용할 값을 입력합니다.  ex) 아이피일 경우: 234.23.13.254  아이디일 경우: user123 개인식별아이디일 경우: 234.23.13.254\_T\_20554\_WC |
| **적용 정책** | 어떤 정책에 유저의 예외처리를 적용할 것인지 선택합니다.  다중 선택할 수 있으며, 모든 정책에서 해당 유저를 차단하고 싶지 않을 경우 전체 선택을 통해 예외처리를 적용할 수 있습니다. |

**8.5 감사로그**

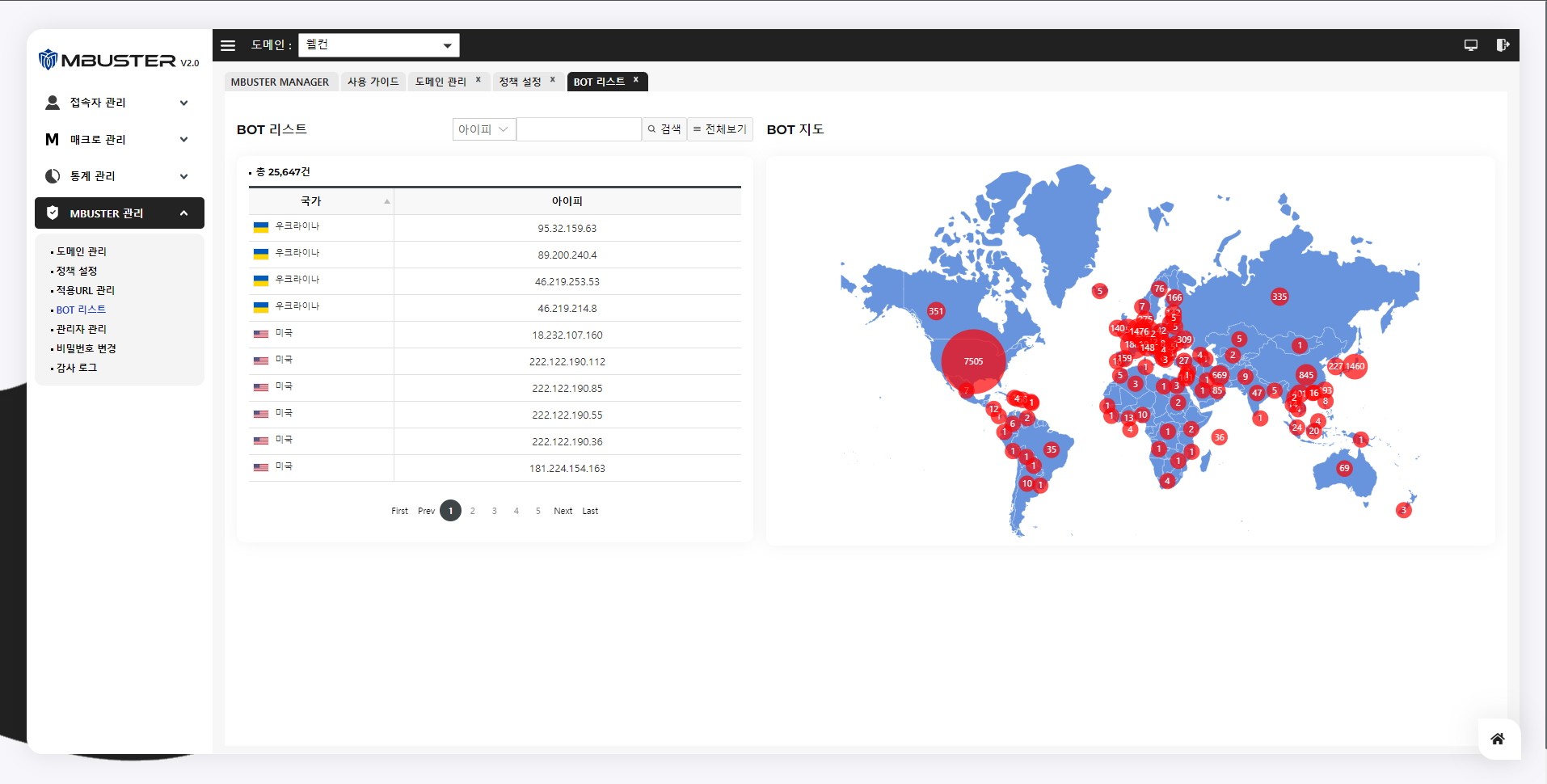
MBUSTER에 접근하여 이용한 메뉴에 대한 감사로그를 기록합니다

<감사로그>

|  |  |
| --- | --- |
| **항목** | **설명** |
| **기간 검색** | 조회하고자 하는 기간을 선택합니다. |
| **검색** | 아이피/아이디/이름/내용에 따라 입력한 검색어로 검색합니다. |
| **사용자 정보** | 행위자를 보여줍니다. |
| **사용자 아이피** | 행위자의 아이피를 보여줍니다. |
| **시간** | 행위자가 메뉴 접근 등의 행동을 한 시간을 보여줍니다. |
| **내용** | 행위자가 행한 행동을 보여줍니다. |

**8.6 BOT 리스트**

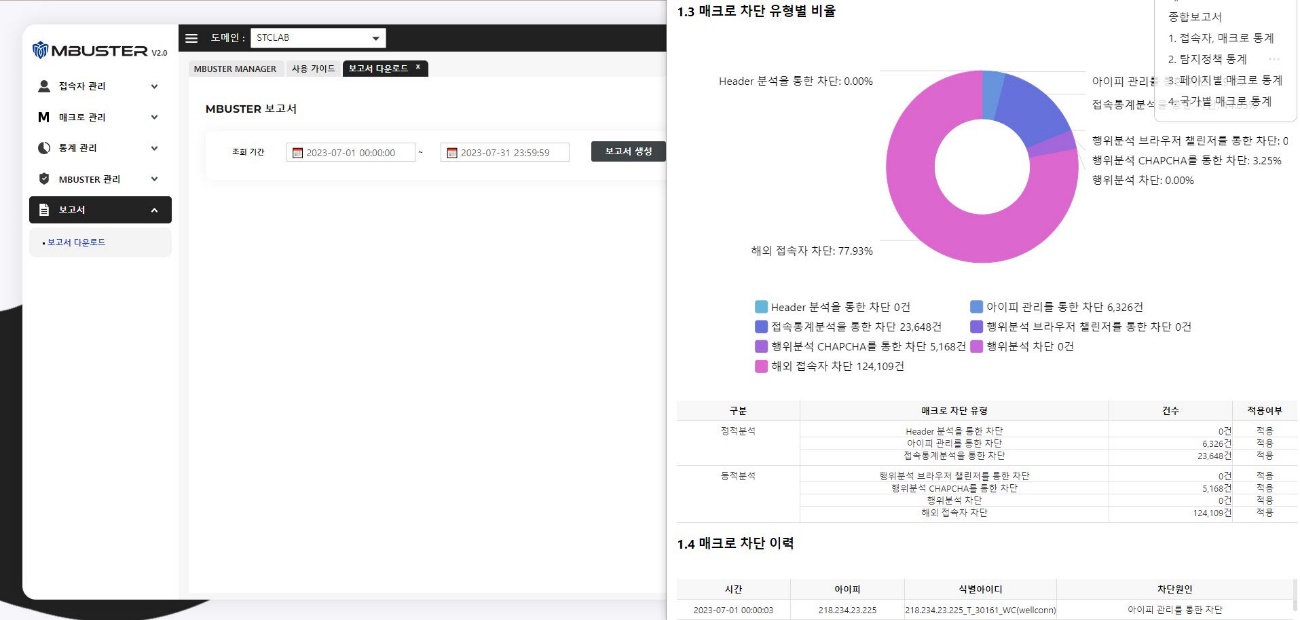
BOT 리스트는 MBUSTER가 관리하고 있는 유해한 BOT 정보를 보여주는 페이지입니다.



<BOT 리스트>

|  |  |
| --- | --- |
| **항목** | **설명** |
| **도메인** | 조회하고자 하는 도메인을 선택합니다. |
| **기간 검색** | 조회하고자 하는 기간을 선택합니다. |
| **아이피 검색** | 검색한 아이피를 기준으로 리스트와 차트를 조회할 수 있습니다. |
| **BOT 리스트** | BOT 리스트를 국가 정보와 함께 보여줍니다.   |  |  | | --- | --- | | 국가 | BOT의 국가 정보 | | 아이피 | BOT의 아이피 | |
| **BOT 차트** | BOT의 국가 정보를 보여줍니다. |

**9. 보고서**

지정한 일자 및 시간에 따른 보고서를 조회하고 엑셀로 다운받을 수 있습니다.

<BOT 리스트>

|  |  |
| --- | --- |
| **항목** | **설명** |
| **조회 기간** | 보고서를 조회하고자 하는 기간을 선택합니다. |

**10. 데이터 저장 및 복구**

MBUSTER V2.0을 통하여 수집된 접속 로그에 대하여 일 단위로 백업을 진행하고, 해당 부분에 대하여 복구가 필요한 경우 엔지니어 방문을 통한 복구를 진행합니다. 데이터 보관 기간은 설정 파일에 설정된 기간에 따라 달라지며, 자동으로 데이터 저장 및 삭제가 이루어집니다.

**11. 기술지원 문의**

온라인상이나 설명서로도 문제를 해결할 수 없을 시에는 ㈜에스티씨랩의 기술 지원 센터로 연락하시기 바랍니다.

• 전화번호 : 02) 3453-1424

**12. MBUSTER MANAGER 가이드**

MBUSTER MANAGER에는 챗봇 기능이 탑재되어 있습니다. 이 기능을 사용하여 매크로 차단과 관련된 질문에 대한 답변을 얻을 수 있습니다. 아래는 채팅 질의문 내에서 사용되는 parameter들로, 이들을 활용하여 답변 내용을 구성할 수 있습니다:

**1. 날짜 검색**

사용자는 원하는 답변의 기준이 되는 날짜를 지정할 수 있습니다.

날짜 parameter 구성은 다음과 같이 입력해야 합니다.

- "*시작일*부터 *종료일*까지" 형식으로 명시해야 하며, 날짜는 YYYY-MM-DD 형식으로 입력해야 합니다.

잘못된 예시:“2023년 6월 16일부터 2023년 6월 20일까지 매크로 리스트 보여줘”

올바른 예시: "2023-06-16부터 2023-06-20까지 매크로 리스트 보여줘”

- 날짜와 관련된 단어를 입력할 수 있습니다.

다음을 제외한 단어들은 명확하게 날짜로 인식하지 못합니다.

|  |
| --- |
| 오늘, 금일, 어제, 작일, 전날, 그제, 그저께, 한 달 전, 지난달, 올해, 작년, 재작년, 금주, 이번 주,  이번 달, 이번 연도, 지난주 |

- 사용예시 : “어제 매크로 리스트 보여줘”

**2. 아이피 검색**

사용자는 아이피 주소를 검색하거나 MBUSTER에서 브라우저별로 발행하는 개인 식별키를 찾을 수 있습니다.

- 아이피 주소 예시: "123.123.123.123“

- 개인 식별키 예시: "123.123.123.123\_T\_760919\_WC"

**13. 용어 정의**

본 용어 정의의 목적은 사용자 취급설명서를 읽는 사용자로 하여금 도움을 얻도록 하기 위함이다.

**매크로 –** 매크로란 사용자의 반복적인 작업을 자동화하기 위한 일련의 명령어나 스크립트를 말한다. 예를 들어 엑셀에서 반복적으로 수행하는 작업이 있는 경우 이 작업을 매크로로 녹화하고 실행하면, 동일한 작업을 매크로를 실행함으로써 한번에 처리할 수 있다. 매크로는 자동화된 작업 수행 뿐만 아니라, 사용자의 입력을 자동으로 처리하거나, 문서의 자동 생성 등 다양한 용도로 사용될 수 있다. 매크로는 업무 효율성을 높이는 데 매우 유용한 도구이지만, 악용될 경우 보안상의 위협이 될 수 있다.

**접속자 –** 매크로로 판단되지 않은 정상 접속을 한 사용자를 의미한다.

**차단 –** 관리하는 대상 도메인에 사용자가 접속하지 못하도록 접근을 차단함을 의미한다.

**정적분석 -** 정적 분석은 접속자의 정보를 통해 접속자를 정적(static)으로 분석하는 과정을 말한다. 이는 주로 접속자의 정보를 신속하고 효과적으로 분석하고 대응하는 데에 사용된다. 특히 매크로에 대한 즉각적인 대응이 가능하여 선제적으로 차단하는 데에 매우 유용하다.

**동적분석 -** 동적 분석은 접속자의 정보를 활용하여 접속자를 동적(dynamic)으로 분석하는 과정을 말한다. 이를 통해 접속자들의 행적을 분석하여 이상행위로 탐지되는 경우 매크로로 간주하여 차단한다. MBuster에서는 사이트에 접속하는 각 접속 단말마다 별도의 식별키를 발급하여 관리하기 때문에 동적 분석을 활용하면 악성 트래픽을 발생시키는 매크로를 효과적으로 차단하고 관리하는 데에 유용하다.

**캡챠(CAPTCHA) –** 문자와 숫자를 혼합한 도전 과제, 사진에서 객체를 식별하는 도전 과제 등을 통해 인간의 논리적 판단력을 이용하여 매크로 사용 여부를 판단한다.

**Header –** 사용자가 웹사이트에 접속할 때 요청하는 값으로, 클라이언트 프로그램 정보, 쿠키 정보 등을 담고 있다.

**브라우저 챌린지 –** 사용자의 브라우저가 자동화된 스크립트를 실행할 때 발생하는 특정한 행위를 감지하여 매크로 사용 여부를 판단하는 방식이다.

**URL –** 우리가 원하는 정보를 인터넷에서 찾기 위해서는 그 정보가 어디에 위치해 있는지를 아는 것이 중요합니다. 이때 정보가 들어있는 웹페이지의 위치를 나타내는 주소입니다.

**도메인 -** 숫자로 이루어진 인터넷상의 컴퓨터 주소를 알기 쉬운 영문으로 표현한 것을 말한다.

**아이피 –** 사용자가 웹서버와 통신을 할 때, 송신자와 수신자를 구별하기 위한 고유의 주소를 뜻한다.

**행위자 –** 관리자UI에 로그인하여 어떠한 행동을 한 사람을 말한다.

**행위분석 –** 사용자의 행동 패턴을 분석하여 매크로인지 판단한다.

**SHA256 –** 암호화된 문자열을 다시 원래의 문자열로 복호화할 수 없는 단방향 암호화 방식이다.

**SALT –** SALT는 임의의 난수 값을 의미한다. 비밀번호를 저장할 때 각 사용자마다 고유한 SALT 값을 생성하고, 이 SALT 값을 원본 비밀번호와 함께 해시 함수에 입력한다. 이렇게 함으로써 동일한 비밀번호를 사용하더라도 SALT 값이 다르기 때문에 해시 결과가 서로 다르게 나온다.

**모달 –** 모달은 화면에서 특정 작업을 수행하기 위해 나타나는 작은 창이나 팝업을 말한다.