(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
G06F 15/00 (2006.01)
G06F 15/16 (2006.01)

(45) 공고일자 2007년07월06일
(11) 등록번호 10-0736540
(24) 등록일자 2007년06월29일

(21) 출원번호 10-2006-0016262
(22) 출원일자 2006년02월20일
심사청구일자 2006년02월20일

(65) 공개번호
(43) 공개일자

(73) 특허권자 에스케이 텔레콤주식회사
서울 중구 을지로2가 11번지

(72) 발명자 조영문
서울 관악구 봉천10동 886-6번지 202호

박선호
서울 금천구 시흥2동 벽산아파트 519동 1803호

이기혁
서울 마포구 공덕1동 삼성래미안2차아파트 108동 1003호

박종희
서울 마포구 신공덕동 155번지 삼성래미안아파트 103동 802호

이상훈
서울 강동구 상일동 주공5단지아파트 524동 407호

(74) 대리인 남상선

(56) 선행기술조사문헌
JP 2004-302764

심사관 : 여원현

전체 청구항 수 : 총 17 항

(54) 웹 서버 위/변조 감시장치 및 그 방법

(57) 요약

웹 서버의 위/변조를 실시간으로 감시하는 웹 서버 위/변조 감시장치가 개시된다. 이를 위하여, 상기 웹 서버의 구조 및 컴포넌트에 대한 정보를 수집하는 정보수집모듈; 사전 정의된 기준정보와 주기적으로 수집된 정보의 비교를 통해 상기 웹 서버의 위/변조 발생여부를 실시간 검사하는 분석모듈; 및 상기 분석모듈의 검사결과, 상기 웹 서버에 위/변조 발생시 관리자에게 통보하는 대응모듈을 포함하는 웹 서버 위/변조 감시 장치를 제공함으로써, 해킹, 침해사고 및 운영자 미숙으로 인한 홈페이지 중단의 가능성을 축소할 수 있으며, 그 중단시간을 최소화 할 수 있고, 신속한 복구를 통해 대 고객 이미지의 훼손을 방지할 수 있다.

대표도

도 2

특허청구의 범위

청구항 1.

적어도 하나의 웹 서버 위/변조 감시 장치에 있어서,

상기 웹 서버의 구조 및 컴포넌트에 대한 정보를 수집하는 정보수집모듈;

사전 정의된 기준정보와 주기적으로 수집된 정보의 비교를 통해 상기 웹 서버의 위/변조 발생여부를 실시간 검사하는 분석모듈; 및

상기 분석모듈의 검사결과, 상기 웹 서버에 위/변조 발생시 관리자에게 통보하는 대응모듈을 포함하는 것을 특징으로 하는 웹 서버 위/변조 감시 장치.

청구항 2.

제1항에 있어서, 상기 분석모듈은,

대량의 점검대상 및 상세 분석수행 시, 멀티-쓰레드(Multi-thread) 방식의 스캐닝 및 해쉬값을 조회를 통해 실시간 검사를 수행하는 것을 특징으로 하는 웹 서버 위/변조 감시 장치.

청구항 3.

제1항에 있어서, 상기 정보수집모듈은,

상기 웹 서버에서 제공되는 웹 페이지의 링크 연결구조를 분석하고, 상기 웹 서버의 컴포턴트를 분석하는 웹 페이지 수집부;

상기 웹 페이지수집부가 수집한 수집정보에 대하여, 상기 분석모듈에서 수행될 비교대상이 없거나, 자동으로 변경되는 웹 페이지, 또는 컴포넌트를 탐색하여 필터링을 수행하는 페이지내용 필터부; 및

상기 웹 페이지 수집부에서 추출한 정보들 가운데, 상기 페이지내용 필터부에서 필터링된 수집정보를 해쉬(Hash) 알고리즘을 이용하여 축약하는 해쉬부를 포함하는 것을 특징으로 하는 웹 서버 위/변조 감시 장치.

청구항 4.

제1항에 있어서, 상기 분석모듈은,

상기 웹 서버에 대하여 사전에 추출된 해쉬값과 주기적으로 수집된 웹 페이지의 해쉬값 비교를 통해 상기 웹 서버의 위/변조를 판단하는 해쉬값 비교기; 및

상기 웹 서버가 해킹되고, 2차적인 해킹을 위하여 삽입되는 코드를 분석하여 웹 페이지에 위/변조가 발생하였는지를 판단하는 해킹코드 분석기를 포함하는 것을 특징으로 하는 웹 서버 위/변조 감시 장치.

청구항 5.

제4항에 있어서, 상기 해쉬값 비교기는,

상기 비교에 대한 범위 지정이 가능하도록 하기 위하여, 분석범위에 따른 해쉬값을 미리 저장하는 것을 특징으로 하는 웹 서버 위/변조 감시 장치.

청구항 6.

제4항에 있어서,

사전에 상기 웹 서버의 웹 페이지에 은닉코드를 삽입한 후, 상기 은닉코드를 비교 분석함으로써 위/변조를 점검하는 은닉코드 분석기를 더 포함하는 것을 특징으로 하는 웹 서버 위/변조 감시 장치.

청구항 7.

제6항에 있어서, 상기 은닉코드 분석기는,

CGI(Common Interface Gateway)를 호출함으로써 생성되며, 시간 및 일자에 따라 변경되는 것을 특징으로 하는 웹 서버 위/변조 감시 장치.

청구항 8.

제1항에 있어서, 상기 대응모듈은,

상기 웹 서버에 위/변조 발생시 관리자에게 SMS로 통보하는 SMS전송부;

상기 웹 서버의 변경내역에 대한 통보를 통하여 정상적인 변경인지를 확인하는 메일발송부; 및

미리 복구모듈을 작성한 후, 상기 위/변조된 웹 서버의 복구지시를 수신하면, 상기 복구모듈을 실행시키는 URL호출부를 포함하는 것을 특징으로 하는 웹 서버 위/변조 감시 장치.

청구항 9.

제1항에 있어서,

상기 웹 서버 각각의 웹 페이지 구성 및 컴포넌트 정보를 미리 저장하고, 그 비교 방법을 미리 기록하는 구성DB를 더 포함하는 것을 특징으로 하는 웹 서버 위/변조 감시 장치.

청구항 10.

제1항 또는 제9항에 있어서,

해킹 시 사용되는 스크립트 및 피싱에 사용되는 URL 및 그 방법을 DB화하여 저장해두는 해킹코드DB를 더 포함하는 것을 특징으로 하는 웹 서버 위/변조 감시 장치.

청구항 11.

웹 서버 위/변조 감시 방법에 있어서,

(A) 적어도 하나의 감시대상 웹 서버에 대한 컨텐츠를 수집하는 단계;

(B) 상기 수집한 컨텐츠를 해쉬 알고리즘을 통해 축약하는 단계;

(C) 상기 축약된 컨텐츠를 사전에 추출된 상기 컨텐츠의 해쉬값과 비교하는 단계; 및

(D) 상술한 비교결과를 통해 상기 웹 서버에 위/변조가 발생된 것으로 판단되면, 관리서버에 통보하는 단계를 포함하는 것을 특징으로 하는 웹 서버 위/변조 감시 방법.

청구항 12.

제11항에 있어서, 상기 (C) 단계는,

상기 웹 서버가 해킹된 경우, 2차적인 해킹을 위하여 삽입한 코드를 분석하여 상기 웹 서버의 위/변조를 판단하는 단계를 더 포함하는 것을 특징으로 하는 웹 서버 위/변조 감시 방법.

청구항 13.

제11항에 있어서, 상기 (D) 단계는,

상기 관리서버로부터 복구지시를 수신하면, 상기 관리서버에 대한 인증을 거친 후, 상기 웹 서버에 대한 복구를 수행하는 단계를 더 포함하는 것을 특징으로 하는 웹 서버 위/변조 감시 방법.

청구항 14.

웹 서버 위/변조 감시 방법에 있어서,

(A) 적어도 하나의 감시대상 웹 서버에 은닉코드를 삽입하는 단계;

(B) 상기 웹 서버에 대한 컨텐츠를 수집하는 단계;

(C) 상기 수집된 컨텐츠에서 은닉코드를 추출하여 원본 은닉코드와 비교하는 단계; 및

(D) 상술한 비교결과를 통해 상기 웹 서버에 위/변조가 발생된 것으로 판단되면, 관리서버에 통보하는 단계를 포함하는 것을 특징으로 하는 웹 서버 위/변조 감시 방법.

청구항 15.

제14항에 있어서, 상기 (C) 단계는,

상기 웹 서버가 해킹된 경우, 2차적인 해킹을 위하여 삽입한 코드를 분석하여 상기 웹 서버의 위/변조를 판단하는 단계를 더 포함하는 것을 특징으로 하는 웹 서버 위/변조 감시 방법.

청구항 16.

제14항에 있어서, 상기 (D) 단계는,

상기 관리서버로부터 복구지시를 수신하면, 상기 관리서버에 대한 인증을 거친 후, 상기 웹 서버에 대한 복구를 수행하는 단계를 더 포함하는 것을 특징으로 하는 웹 서버 위/변조 감시 방법.

청구항 17.

제 14항에 있어서, 상기 은닉코드는,

CGI(Common Interface Gateway)를 호출함으로써 생성되며, 시간 및 일자에 따라 변경되는 것을 특징으로 하는 웹 서버 위/변조 감시 방법.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 위/변조(defacement) 감시장치에 관한 것으로, 보다 상세하게는 웹 서버의 위/변조를 실시간으로 감시하는 웹 서버 위/변조 감시장치에 관한 것이다.

종래의 웹 서버 위/변조 감시장치의 경우에는 에이전트 방식(즉, 감시대상 웹 서버에 에이전트를 설치)이 주로 이용되었다. 즉, 상기 에이전트 방식은, 접근자의 웹 브라우저에 자동 다운로드 되는 기능을 가진 자바 애플릿을 이용하여 에이전트를 만들고, 에이전트 내에 소켓을 이용한 통신의 원리를 첨가하여 에이전트 서버 내에 접근자의 정보를 전달한다. 이러한 에이전트로부터 받은 접근자 정보와 불법 침입자의 웹 서버 접근으로부터 발생되는 HTTP 헤더의 정보를 비교하여 자신의 위치를 은닉한 불법침입자의 원천 위치를 파악하여 추적할 수 있고, 중간경로의 위치를 파악할 수 있다. 또한 에이전트로부터 받은 정보를 자료실, 게시판에 사용하여 부정한 글이나 자료를 올린 사용자의 추적자료로 사용할 수 있으며, 중간 경유지를 이용하여 자기정보를 은닉하는 사람은 사용하지 못하도록 할 수 있다. 아울러, 웹 기반 채팅에서 채팅에 접근 할 수 없는 사용자가 프락시 주소를 반복하여 하나의 채팅방에 계속 다른 접근자로 위장하여 들어갈 수 있는 문제점을 에이전트의 정보를 이용하여 접근자의 원천 위치를 파악 할 수 있었다.

그러나, 상술한 에이전트 방식은 웹 서버의 가용성에 큰 영향을 끼치는 문제점이 있어왔다. 또한, 상술한 방식을 실용화한 제품 자체에는 그 성능 때문에 시장 창출에 실패하여 현재 마땅한 대안이 없는 상태이다.

발명이 이루고자 하는 기술적 과제

따라서, 본 발명의 목적은, 관리대상 웹 서버에 탐지용 에이전트를 설치하지 않고서도 오프라인 상에서 실시간으로 감시할 수 있는 웹 서버 위/변조 감시장치를 제공하는 데 있다.

발명의 구성

상기 목적을 달성하기 위하여, 본 발명의 일 실시예에 따른 웹 서버 위/변조 감시 장치는, 상기 웹 서버의 구조 및 컴포넌트에 대한 정보를 수집하는 정보수집모듈; 사전 정의된 기준정보와 주기적으로 수집된 정보의 비교를 통해 상기 웹 서버의 위/변조 발생여부를 실시간 검사하는 분석모듈; 및 상기 분석모듈의 검사결과, 상기 웹 서버에 위/변조 발생시 관리자에게 통보하는 대응모듈을 포함하는 것을 특징으로 한다.

여기서, 상기 정보수집모듈은, 상기 웹 서버에서 제공되는 웹 페이지의 링크 연결구조를 분석하고, 상기 웹 서버의 컴포넌트를 분석하는 웹 페이지 수집부; 상기 웹 페이지수집부가 수집한 수집정보에 대하여, 상기 분석모듈에서 수행될 비교대상이 없거나, 자동으로 변경되는 웹 페이지, 또는 컴포넌트를 탐색하여 필터링을 수행하는 페이지내용 필터부; 및 상기 웹 페이지 수집부에서 추출한 정보들 가운데, 상기 페이지내용 필터부에서 필터링된 수집정보를 해쉬(Hash) 알고리즘을 이용하여 축약하는 해쉬부를 포함하는 것을 특징으로 한다.

또한, 상기 분석모듈은, 상기 웹 서버에 대하여 사전에 추출된 해쉬값과 주기적으로 수집된 웹 페이지의 해쉬값 비교를 통해 상기 웹 서버의 위/변조를 판단하는 해쉬값 비교기; 및 상기 웹 서버가 해킹되고, 2차적인 해킹을 위하여 삽입되는 코드를 분석하여 웹 페이지에 위/변조가 발생하였는지를 판단하는 해킹코드 분석기를 포함하는 것을 특징으로 한다.

그리고, 상기 대응모듈은, 상기 웹 서버에 위/변조 발생시 관리자에게 SMS로 통보하는 SMS전송부; 상기 웹 서버의 변경내역에 대한 통보를 통하여 정상적인 변경인지를 확인하는 메일발송부; 및 미리 복구모듈을 작성한 후, 상기 위/변조된 웹 서버의 복구지시를 수신하면, 상기 복구모듈을 실행시키는 URL호출부를 포함하는 것을 특징으로 한다.

바람직하게는, 상기 웹 서버 각각의 웹 페이지 구성 및 컴포넌트 정보를 미리 저장하고, 그 비교 방법을 미리 기록하는 구성DB를 더 포함하는 것을 특징으로 한다.

바람직하게는, 제1항 또는 제9항에 있어서, 해킹 시 사용되는 스크립트 및 피싱에 사용되는 URL 및 그 방법을 DB화하여 저장해두는 해킹코드DB를 더 포함하는 것을 특징으로 한다.

한편, 본 발명의 일 실시에에 따른 웹 서버 위/변조 감시 방법은, (A) 적어도 하나의 감시대상 웹 서버에 대한 컨텐츠를 수집하는 단계; (B) 상기 수집한 컨텐츠를 해쉬 알고리즘을 통해 축약하는 단계; (C) 상기 축약된 컨텐츠를 사전에 추출된 상기 컨텐츠의 해쉬값과 비교하는 단계; 및 (D) 상술한 비교결과를 통해 상기 웹 서버에 위/변조가 발생된 것으로 판단되면, 관리서버에 통보하는 단계를 포함하는 것을 특징으로 한다.

여기서, 상기 (C) 단계는, 상기 웹 서버가 해킹된 경우, 2차적인 해킹을 위하여 삽입한 코드를 분석하여 상기 웹 서버의 위/변조를 판단하는 단계를 더 포함하는 것을 특징으로 한다.

또한, 상기 (D) 단계는, 상기 관리서버로부터 복구지시를 수신하면, 상기 관리서버에 대한 인증을 거친 후, 상기 웹 서버에 대한 복구를 수행하는 단계를 더 포함하는 것을 특징으로 한다.

또 다른 한편, 본 발명의 다른 실시예에 따른 웹 서버 위/변조 감시 방법은, (A) 적어도 하나의 감시대상 웹 서버에 은닉코드를 삽입하는 단계; (B) 상기 웹 서버에 대한 컨텐츠를 수집하는 단계; (C) 상기 수집된 컨텐츠에서 은닉코드를 추출하여 원본 은닉코드와 비교하는 단계; 및 (D) 상술한 비교결과를 통해 상기 웹 서버에 위/변조가 발생된 것으로 판단되면, 관리서버에 통보하는 단계를 포함하는 것을 특징으로 한다.

이하에서는, 첨부도면 및 바람직한 실시예를 참조하여 본 발명을 상세히 설명한다. 도면상에서 동일 또는 유사한 구성요소에 대하여는 동일한 참조번호를 부여하였다.

도1은 본 발명의 바람직한 실시예에 따른 웹 서버 위/변조 감시 시스템을 나타내는 구성도이다.

도1에 도시한 바와 같이, 상기 시스템은, 관리자에 의해 운용되며 로그분석과 핫 라인을 지원하는 관리장치(300); 상기 관리장치(300)와 접속되어 감시대상 웹 서버에 위/변조 발생시 복구처리를 수행하는 복구장치(400); 웹 서버 위/변조 감시장치(200); 및 적어도 하나의 감시대상 웹 서버(100)를 포함한다.

웹 서버 위/변조 감시장치(Web Deface Checker; 이하 WDC, 200)는 웹 페이지 정보를 수집하고, 상기 수집된 웹 페이지의 위/변조를 분석하여 해당 위/변조 발생시 SMS, Mail 및/또는 URL호출 등과 같은 연동기능을 이용하여 관리장치(300)로 통보한다.

이를 위하여, WDC는 감시대상 웹 서버(100)의 구조 및 상기 웹 서버(100)로부터 제공되는 컴포넌트에 대한 분석을 통해 상기 웹 서버(100)의 정보를 수집하고, 사전 정의된 기준정보와 주기적으로 수집된 정보의 비교를 통해 위/변조 여부를 분석하며, 상기 분석결과 웹 서버(100) 위/변조 발생시, 관리자에게 다양한 방식으로 통보한다.

이하, 웹 서버 위/변조 감시 방법을 설명한다.

먼저, 주기적인 웹 서버(100) 검사를 통해 웹 서버(100) 위/변조 여부를 체크하고, 웹 서버(100) 위/변조 발생 그 즉시 백업파일(Backup file)을 이용한 웹 페이지 복구를 수행한다. 이때, 상기 복구여부는 정책적 고려사항으로써, 웹 서버(100) 환경이나 관리자의 선택 사항이다. 또한, 상기 웹 서버(100) 검사는, 웹 서비스의 사용량이 많은 시간에는 점검주기를 길게 하고, 해킹이 주로 발생되는 야간에는 점검주기를 짧게 한다.

이후, 웹 서버(100) 위/변조가 발생한 서버에 대한 정보 및 변조발생 사실을 관리자에게 통지하고, 상기 관리자의 대응지시에 따른다.

도2는 본 발명의 바람직한 실시예에 따른 웹 서버 위/변조 감시 장치를 나타내는 구성도이다.

도2에 도시한 바와 같이, 상기 감시장치(200)는, 정보수집모듈(210); 분석모듈(220); 대응모듈(230); 구성DB(240); 해킹코드DB(250) 및 로그DB(260)를 포함한다.

정보수집모듈(210)은, 감시대상 웹 서버(100)의 구조 및 컴포넌트에 대한 정보를 수집하며, 웹 페이지 수집부(211); 페이지내용 필터부(212); 및 해싱부(213)를 포함한다.

웹 페이지 수집부(211)는 감시대상 웹 서버(100)에서 제공되는 웹 페이지의 링크 연결구조 등과 같은 상기 웹 서버(100)의 구조를 분석하고, 상기 웹 서버(100)에서 제공되는 액티브X, 자바모듈(Java module), 자바 스크립트(Java Script), 이미지, 인클루드 파일(Include File) 등과 같은 컴포턴트를 분석한다.

페이지내용 필터부(212)는 상술한 웹 페이지수집부(211)의 주요 수집정보에 있어서, 비교대상이 없거나, 자동으로 변경되는 웹 페이지, 또는 컴포넌트에 대해서 예외적으로 처리한다.

그리고, 해싱부(213)는 감시대상 웹 서버(100)에서 추출된 컨텐츠들을 해쉬(Hash) 알고리즘을 이용하여 축약한다.

분석모듈(220)은, 사전 정의된 기준정보와 주기적으로 수집된 정보의 비골르 통해 감시대상 웹 서버(100)의 위/변조 발생 여부를 파악하고, 대량의 점검대상 및 상세 분석수행 시, 최적의 성능을 확보하기 위하여 멀티쓰레드(Multi-thread)방식의 스캐닝 및 해쉬값을 조회하여 실시간 검사가 가능하며, 해쉬값 비교기(221); 은닉코드 분석기(222); 및 해킹코드 분석기(223)를 포함한다.

해쉬값 비교기(221)는 감시대상 웹 서버(100)에 대하여 사전에 추출된 해쉬값과 주기적으로 수집된 웹 페이지의 해쉬값을 비교한다. 특히, 상기 분석에 대한 범위 지정이 가능하도록 하기 위하여, 분석범위(웹페이지 깊이(Depth))에 따른 해쉬값을 저장한다.

은닉코드 분석기(222)는 상기 해쉬값 비교를 통하여, 위/변조를 점검하는 과정은 상기 웹 서버 위/변조 감시장치(200) 내부적으로 매우 복잡하기 때문에, 속도 및 성능의 최적화를 위하여, 사전에 웹 페이지에 은닉코드를 삽입한 후, 이를 수집하여 분석함으로써, 위/변조를 점검할 수 있다. 이러한 은닉코드는 CGI(Common Interface Gateway)를 호출함으로써 생성되며, 시간/일자에 따라 변경된다.

해킹코드 분석기(223)는 감시대상 웹 서버(100)가 해킹되고, 2차적인 해킹을 위하여 삽입되는 코드를 분석하여 웹 페이지에 위/변조가 발생하였는지를 판단한다. 이때, 2차적인 해킹은 사용자 ID/패스워드 분실, 피싱 등과 같은 경우를 의미한다.

대응모듈(230)은, 감시대상 웹 서버(100)에 위/변조 발생시 SMS/메일/URL호출 등과 같은 연동기능을 통해 관리자에게 통보하며, SMS 전송부(231); 메일발송부(232); 및 URL호출부(233)를 포함한다.

SMS전송부(231)는 감시대상 웹 서버(100)에 위/변조 발생시 관리자에게 SMS로 통보하며, 메일발송부(232)는 SMS와는 별도로, 상기 웹 서버(100) 위/변조의 내역(즉, 웹 서버의 변경내역)에 대한 통보를 통하여 정상적인 변경인지를 확인할 수 있게 한다.

URL호출부(233)는 감시대상 웹 서버(100)의 관리자가 복구기능을 요청하였을 경우, 복구 기능을 CGI(Common Interface Gateway)로 구현하여, 상기 웹 서버 위/변조 감시장치(200)에서는 해당 CGI를 요청함으로써 복구를 수행한다. 이때, 복구를 수행하기에 앞서 해당 관리자에 대한 인증을 반드시 거친다.

구성DB(240)는 감시대상 웹 서버(100) 각각의 웹 페이지 구성 및 컴포넌트 정보를 미리 저장하고, 그 비교 방법을 기록해 둠으로써, 상기 정보수집모듈(210)의 웹 페이지 필터링 및 비교절차를 간소화 한다.

해킹코드DB(250)는 최근 해킹 동향 분석을 통하여, 해킹 시 사용되는 스크립트 및 피싱에 사용되는 URL 및 그 방법을 DB화하여 저장하며, 상기 분석모듈(220)과 연동한다.

로그 DB(260)는 감시대상 웹 서버(100)의 각 고객의 로그 내역을 저장하며, 상기 WDC(200)의 각 구성부와 연동한다.

이와 같이, 구성된 본 발명의 바람직한 실시예에 따른 웹 서버 위/변조 감지장치의 동작을 설명한다.

먼저, 적어도 하나 이상의 감시대상 웹 서버(100)에 대한 정보를 수집한다(S310). 이때, 상기 웹 서버(100)에서 제공되는 웹 페이지의 링크 연결구조 분석을 통해 웹 서버(100)의 구조를 분석하고 액티브X, 자바모듈, 자바스크립트, 이미지, 인클루드파일 등과 같은 컴포넌트를 분석한다. 이때, 비교대상이 없거나 자동으로 변경되는 페이지 또는 컴포넌트는 제외 처리한다.

이어, 수집한 각각의 컨텐츠(즉, 웹 페이지 또는 컴포넌트)를 해쉬 알고리즘을 통해 축약한 후, 사전에 추출된 상기 컨텐츠의 해쉬값과 비교한다(S320). 이때, 수집한 컨텐츠들에 대한 분석범위를 미리 설정하도록 한다. 예컨대, 해당 웹 페이지의 깊이(Depth)를 그 예로 들 수 있다.

이와 더불어, 감시대상 웹 서버(100)가 해킹된 경우, 2차적인 해킹을 위하여 삽입한 코드를 분석하여 웹 페이지의 위/변조가 발생하였는지를 점검한다(S330).

상술한 비교결과, 감시대상 웹 서버(100)에 위/변조가 발생되면, 관리자에게 통보하고, 복구가 필요할 경우에는 관리자에 대한 인증을 거친 후, 해당 웹 서버(100)에 대한 복구를 수행한다(S340). 이때, SMS를 통해 관리자에 통보할 수 있으며, 상기 웹 서버(100)에 대한 정상적인 변경인 경우에는 상기 변경에 대한 내역을 이메일을 통해 관리자에게 전송함으로써, 정상적인 변경인지 여부를 확인 받도록 한다. 또한, 감시대상 웹 서버(100)에 복구가 필요한 경우에는 복구장치에 요청하여 상기 웹 서버(100)가 제공하는 웹 페이지를 복구할 수 있도록 한다.

한편, 상기 단계 320의 경우, 해쉬값 비교를 통해 위/변조를 체크하므로, 그 과정이 매우 복잡하고 상기 감시장치(200)에 상당한 부하를 준다. 이에 따라, 상기 단계 310 이전에, 감시대상 웹 서버(100)가 제공하는 웹 페이지에 특정 은닉코드를 삽입하여 상기 단계 320에서 이를 분석함으로써, 웹 서버(100)의 위/변조를 감시할 수 있다. 이러한 은닉코드는, 전술한 바와 같이, CGI(Common Interface Gateway)를 호출함으로써 생성되며, 상기 은닉코드는 시간/일자에 따라 변경된다.

이와 같이 본 발명이 구성/동작 함으로써, 오프라인 브라우저 기술을 활용하여, 넌 에이전트(Non-Agent) 방식의 웹 페이지 위/변조 탐지를 수행하고, 감시 대상 웹사이트의 구조 및 컨텐츠 분석 시, 상기 감시장치의 가용성에 대한 영향도를 최소화할 수 있는 특징이 있다.

또한, 본 발명은 대량의 점검대상 및 상세 분석수행 시, 최적의 성능을 확보하기 위하여, 멀티쓰레드(Multi-thread)방식의 스캐닝 및 해쉬값을 조회함으로써, 실시간 검사가 가능한 특징이 있다.

또한, 본 발명은 최근 해킹 동향 분석을 통하여, 해킹 시 사용되는 스크립트 및 피싱에 사용되는 URL 및 그 방법을 DB화함으로써, 다양한 위/변조 검증기능을 제공할 수 있는 특징이 있다.

또한, 본 발명은, 웹 서비스의 사용량이 많은 시간에는 점검주기를 길게 하고, 해킹이 주로 발생되는 야간에는 점검주기를 짧게 함으로서, 웹 서버(100)에 대한 영향도를 최소화하는 특징이 있다.

또한, 본 발명에 따르면, 점검 깊이(Depth)에 대한 조정을 통해 최적 점검속도를 유지시킬 수 있는 특징이 있다.

또한, 본 발명에 따르면, 사전에 삽입되어 주기적으로 변경되는 은닉코드를 분석함으로써, 빠른 위/변조 점검을 수행할 수 있는 특징이 있다.

그리고, 본 발명에 따르면, 인증이 필요한 웹 페이지에 대한 점검을 수행하기 위하여, 감시대상 웹 서버(100)에 ID/패스워드, 인증서 등과 같은 인증방식을 지원하고, 인증 시 소요되는 시간 및 서버 부하를 최소화하는 특징이 있다.

지금까지 본 발명을 바람직한 실시예를 참조하여 상세히 설명하였지만, 당업자는 본 발명의 사상 및 범위를 벗어나지 않고 다양한 변형 또는 수정이 가능하다는 것을 알 것이다.

발명의 효과

이상 설명한 바와 같이, 본 발명에 따르면, 해킹, 침해사고 및 운영자 미숙으로 인한 홈페이지 중단의 가능성을 축소할 수 있으며, 그 중단시간을 최소화 할 수 있고, 신속한 복구를 통해 대 고객 이미지의 훼손을 방지할 수 있는 효과가 있다.

또한, 넌 에이전트(Non-Agent) 방식의 웹 서버 위/변조 감시를 통해 관리장치의 가용성을 보장할 수 있는 효과가 있다.

도면의 간단한 설명

도1은 본 발명의 바람직한 실시예에 따른 웹 서버 위/변조 감시 시스템을 나타내는 구성도.

도2는 본 발명의 바람직한 실시예에 따른 웹 서버 위/변조 감시 장치를 나타내는 구성도.

도3은 본 발명의 바람직한 실시예에 따른 웹 서버 위/변조 감시 방법을 나타내는 순서도.

* 도면의 주요부분에 대한 부호설명*

200: 감시장치

210: 정보수집모듈

220: 분석모듈

230: 대응모듈

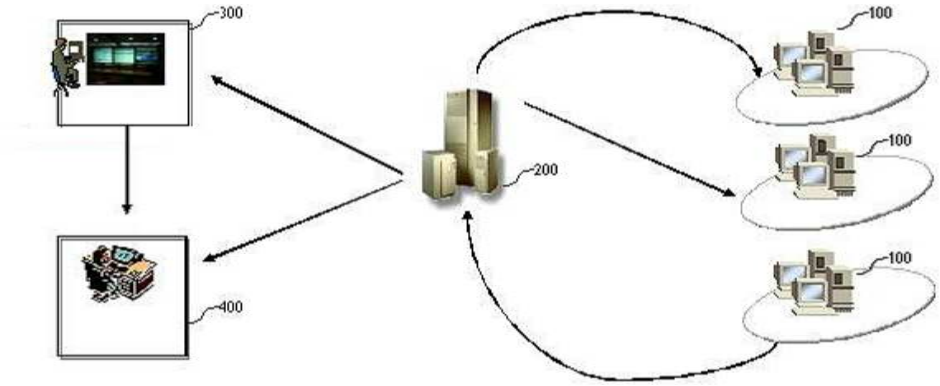
240: 구성DB

250: 해킹코드DB

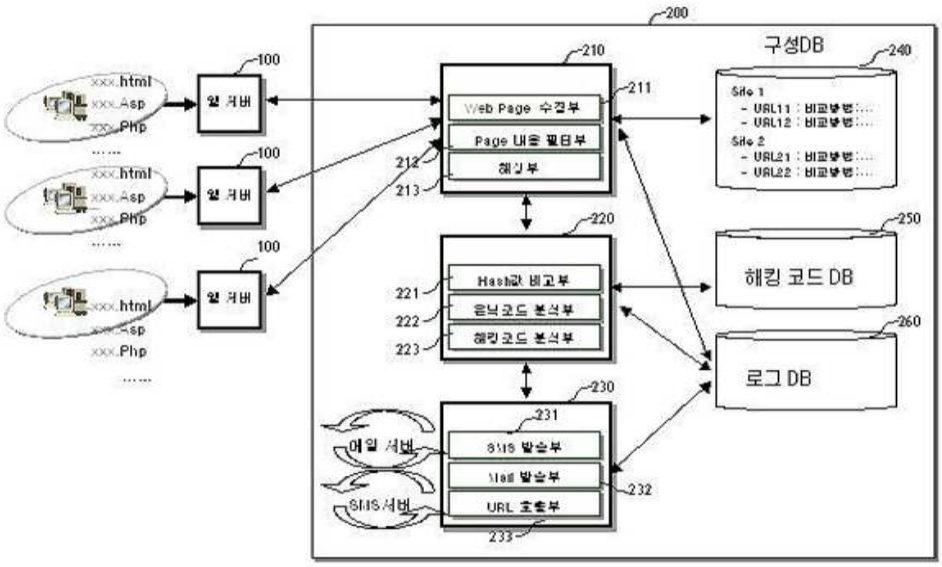
260: 로그DB

도면

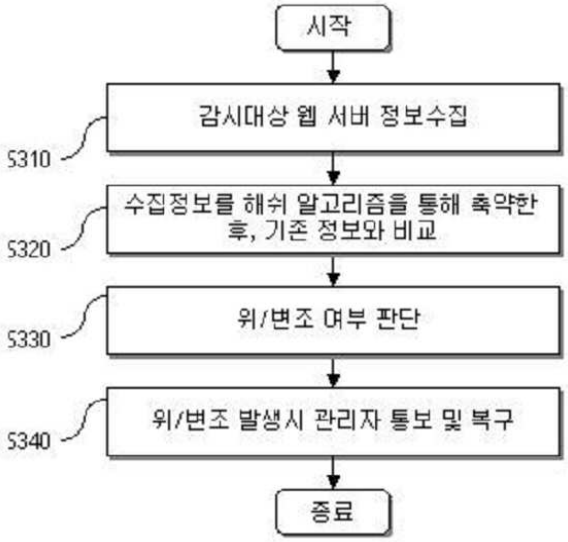
도면1


300
100
200
100
100
400

도면2


200
구성DB
240
210
211
Web Page 수정부
Page 내용 필터부
해킹부
212
213
220
221
222
223
Hash값 비교부
음악코드 분석부
해킹코드 분석부
250
해킹 코드 DB
260
로그 DB
230
231
SMS 발송부
Mail 발송부
URL 호출부
232
233
이메일 서버
SMS서버
100
웹 서버
xxx.html
xxx.Asp
xxx.Php

도면3


시작
감시대상 웹 서버 정보수집
S310
수집정보를 해쉬 알고리즘을 통해 축약한 후, 기존 정보와 비교
S320
위/변조 여부 판단
S330
위/변조 발생시 관리자 통보 및 복구
S340
종료