(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년10월28일
(11) 등록번호 10-2164338
(24) 등록일자 2020년10월05일

(51) 국제특허분류(Int. Cl.)
*H04L 12/58* (2006.01) *G06Q 50/32* (2012.01)
*H04L 29/06* (2006.01)
(52) CPC특허분류
*H04L 51/30* (2013.01)
*G06Q 50/32* (2013.01)
(21) 출원번호 10-2020-0016274
(22) 출원일자 2020년02월11일
심사청구일자 2020년02월11일
(56) 선행기술조사문헌
JP2009017348 A*
*(뒷면에 계속)*

(73) 특허권자
**(주)리투인소프트웨어**
서울특별시 강남구 언주로113길 7, 3층(논현동, 논현237빌딩)
(72) 발명자
**김한주**
서울특별시 강남구 삼성로149길 3-6 5층 (청담동)
(74) 대리인
**김현수**

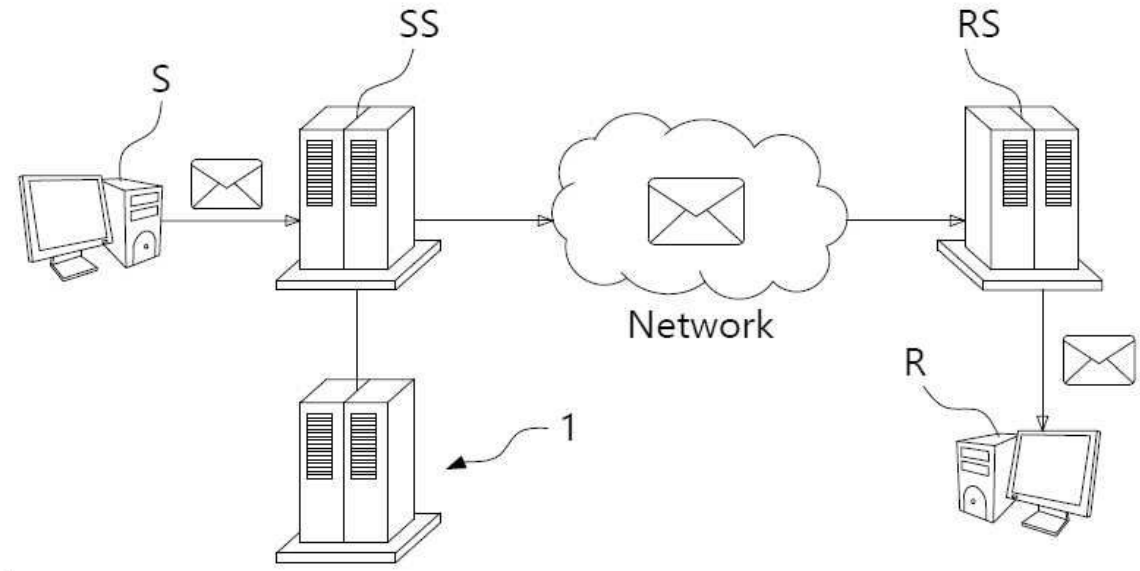
전체 청구항 수 : 총 21 항 심사관 : 안동진

(54) 발명의 명칭 **발송자 사칭을 방지하기 위한 전자메일 보안 시스템 및 그 방법**

## (57) 요 약

본 발명은 발송자 사칭을 방지하기 위한 전자메일 보안 시스템 및 그 방법에 관한 것으로, 더욱 상세하게는, 발송처를 위조하는 메일을 수신측이 아닌 발신측의 의지로 막을 수 있도록 하며, 발송측의 기존 메일시스템과 보안 시스템의 변경을 가하지 않아도 되고, 수신측의 메일 환경을 변경하지 않아도 메일 공격을 차단할 수 있도록 하는, 발송자 사칭을 방지하기 위한 전자메일 보안 시스템 및 그 방법에 관한 것이다.

*대 표 도* - 도1



(52) CPC특허분류
*H04L 51/08* (2013.01)
*H04L 51/18* (2013.01)
*H04L 63/0428* (2013.01)

(56) 선행기술조사문헌
KR101847381 B1*
KR1020050002712 A*
KR1020070074315 A*
KR1020120134980 A*
*는 심사관에 의하여 인용된 문헌

# 명 세 서

## 청구범위

### 청구항 1

발신 대상 전자메일을 수신하는 메일수신부와,

발신 대상 전자메일을 구성하는 데이터에서 전자메일 수신측이 수신한 메일로부터 확인 가능한 항목의 특정 값을 추출하는 사인생성정보추출부와,

추출된 특정 값으로 사인정보를 생성하는 사인정보생성부와,

생성된 사인정보를 발신 대상 전자메일에 부가하는 사인정보부가부와,

사인정보가 부가된 발신 대상 전자메일을 전송하는 메일전송부를 포함하며,

상기 사인정보는, 이미지 또는 텍스트 형식이고,

상기 사인정보부가부는, 상기 사인정보생성부가 생성한 이미지 또는 텍스트 형식의 사인정보를 발신 대상 전자메일의 본문에 삽입하는 사인정보삽입모듈을 포함하여,

수신측의 메일 환경을 변경하지 않아도 전자메일 수신측에서 수신된 전자메일의 정보가 사인정보와 일치하는지 여부를 확인해 위험 메일을 파악할 수 있도록 하는, 발송자 사칭을 방지하기 위한 전자메일 보안 시스템.

### 청구항 2

제1항에 있어서,

상기 사인정보생성부는, 이미지 형식으로 사인정보를 생성하는 이미지생성모듈을 포함하는 것을 특징으로 하는, 발송자 사칭을 방지하기 위한 전자메일 보안 시스템.

### 청구항 3

제1항에 있어서,

상기 사인정보생성부는, 텍스트 형식으로 사인정보를 생성하는 텍스트생성모듈을 포함하는 것을 특징으로 하는, 발송자 사칭을 방지하기 위한 전자메일 보안 시스템.

### 청구항 4

삭제

### 청구항 5

제1항에 있어서,

상기 사인정보생성부는, 웹페이지 형식으로 사인정보를 생성하는 웹페이지생성모듈을 포함하는 것을 특징으로 하는, 발송자 사칭을 방지하기 위한 전자메일 보안 시스템.

### 청구항 6

제5항에 있어서,

상기 웹페이지생성모듈은, 상기 사인생성정보추출부에 의해 추출된 특정 값을 암호화하여 암호값을 생성하는 웹페이지암호값생성모듈과, 상기 암호값을 사용하여 발송 도메인 확인용 URL을 생성하는 발송도메인확인URL생성모듈을 포함하는 것을 특징으로 하는, 발송자 사칭을 방지하기 위한 전자메일 보안 시스템.

### 청구항 7

제6항에 있어서,

상기 사인정보부가부는, 상기 사인정보삽입모듈에 의해 발신 대상 전자메일의 본문에 삽입된 이미지 또는 텍스트 형식의 사인정보에 상기 웹페이지생성모듈에 의해 생성된 상기 발송 도메인 확인용 URL을 삽입하는 발송도메인확인URL삽입모듈을 포함하는 것을 특징으로 하는, 발송자 사칭을 방지하기 위한 전자메일 보안 시스템.

**청구항 8**

제1항에 있어서,

상기 사인정보생성부는, 호출 이미지 형식으로 사인정보를 생성하는 호출이미지생성모듈을 포함하는 것을 특징으로 하는, 발송자 사칭을 방지하기 위한 전자메일 보안 시스템.

**청구항 9**

제8항에 있어서,

상기 호출이미지생성모듈은, 상기 사인생성정보추출부에 의해 추출된 특정 값을 암호화하여 암호값을 생성하는 호출이미지암호값생성모듈과, 상기 암호값을 사용하여 사인 이미지 요청용 URL을 생성하는 사인이미지요청URL생성모듈을 포함하는 것을 특징으로 하는, 발송자 사칭을 방지하기 위한 전자메일 보안 시스템.

**청구항 10**

제9항에 있어서,

상기 사인정보부가부는, 상기 호출이미지생성모듈이 생성한 상기 사인 이미지 요청용 URL을 발신 대상 전자메일의 본문에 삽입하는 사인이미지요청URL삽입모듈을 포함하는 것을 특징으로 하는, 발송자 사칭을 방지하기 위한 전자메일 보안 시스템.

**청구항 11**

제10항에 있어서,

상기 사인정보생성부는, 웹페이지 형식으로 사인정보를 생성하는 웹페이지생성모듈을 포함하는 것을 특징으로 하는, 발송자 사칭을 방지하기 위한 전자메일 보안 시스템.

**청구항 12**

제11항에 있어서,

상기 웹페이지생성모듈은, 상기 사인생성정보추출부에 의해 추출된 특정 값을 암호화하여 암호값을 생성하는 웹페이지암호값생성모듈과, 상기 암호값을 사용하여 발송 도메인 확인용 URL을 생성하는 발송도메인확인URL생성모듈을 포함하는 것을 특징으로 하는, 발송자 사칭을 방지하기 위한 전자메일 보안 시스템.

**청구항 13**

제12항에 있어서,

상기 사인정보부가부는, 상기 사인이미지요청URL삽입모듈에 의해 발신 대상 전자메일의 본문에 삽입된 사인 이미지 요청용 URL에 의해 호출되는 이미지 형식의 사인정보에 상기 웹페이지생성모듈에 의해 생성된 상기 발송 도메인 확인용 URL을 삽입하는 발송도메인확인URL삽입모듈을 포함하는 것을 특징으로 하는, 발송자 사칭을 방지하기 위한 전자메일 보안 시스템.

**청구항 14**

제1항에 있어서,

상기 사인생성정보추출부는, 발신 대상 전자메일의 발송시각을 추출하는 발송시각추출모듈과, 발신 대상 전자메일의 발신주소를 추출하는 발신주소추출모듈과, 발신 대상 전자메일의 수신주소를 추출하는 수신주소추출모듈과, 발신 대상 전자메일의 참조주소를 추출하는 참조주소추출모듈과, 발신 대상 전자메일의 메일제목을 추출하는 메일제목추출모듈을 포함하는 것을 특징으로 하는, 발송자 사칭을 방지하기 위한 전자메일 보안 시스템.

**청구항 15**

제14항에 있어서,

상기 사인정보생성부는, 상기 메일제목추출모듈로부터 전달받은 메일제목의 일부분을 블라인드 처리하는 변환처리모듈을 추가로 포함하는 것을 특징으로 하는, 발송자 사칭을 방지하기 위한 전자메일 보안 시스템.

**청구항 16**

메일수신부가 발신 대상 전자메일을 수신하는 메일수신단계와,

상기 메일수신단계 이후에, 사인생성정보추출부가 발신 대상 전자메일을 구성하는 데이터에서 전자메일 수신측이 수신한 메일로부터 확인 가능한 항목의 특정 값을 추출하는 사인생성정보추출단계와,

상기 사인생성정보추출단계 이후에, 이미지생성모듈이 추출된 특정 값으로 이미지 형식의 사인정보를 생성하는 이미지생성단계와,

상기 사인생성정보추출단계 이후에, 웹페이지생성모듈이 웹페이지 형식으로 사인정보를 생성하는 웹페이지생성단계와,

상기 이미지생성단계 및 상기 웹페이지생성단계 이후에, 사인정보삽입모듈이 상기 이미지생성모듈이 생성한 이미지 형식의 사인정보를 발신 대상 전자메일의 본문에 삽입하는 사인정보삽입단계와,

상기 사인정보삽입단계 이후에, 발송도메인확인URL삽입모듈이 상기 사인정보삽입모듈에 의해 발신 대상 전자메일의 본문에 삽입된 이미지 형식의 사인정보에 상기 웹페이지생성모듈에 의해 생성된 발송 도메인 확인용 URL을 삽입하는 발송도메인확인URL삽입단계와,

상기 발송도메인확인URL삽입단계 이후에, 메일전송부가 사인정보가 부가된 발신 대상 전자메일을 전송하는 메일전송단계를 포함하여,

수신측의 메일 환경을 변경하지 않아도 전자메일 수신측에서 수신된 전자메일의 정보가 사인정보와 일치하는지 여부를 확인해 위험 메일을 파악할 수 있도록 하는, 발송자 사칭을 방지하기 위한 전자메일 보안 방법.

**청구항 17**

메일수신부가 발신 대상 전자메일을 수신하는 메일수신단계와,

상기 메일수신단계 이후에, 사인생성정보추출부가 발신 대상 전자메일을 구성하는 데이터에서 전자메일 수신측이 수신한 메일로부터 확인 가능한 항목의 특정 값을 추출하는 사인생성정보추출단계와,

상기 사인생성정보추출단계 이후에, 텍스트생성모듈이 추출된 특정 값으로 텍스트 형식의 사인정보를 생성하는 텍스트생성단계와,

상기 사인생성정보추출단계 이후에, 웹페이지생성모듈이 웹페이지 형식으로 사인정보를 생성하는 웹페이지생성단계와,

상기 텍스트생성단계 및 상기 웹페이지생성단계 이후에, 사인정보삽입모듈이 상기 텍스트생성모듈이 생성한 텍스트 형식의 사인정보를 발신 대상 전자메일의 본문에 삽입하는 사인정보삽입단계와,

상기 사인정보삽입단계 이후에, 발송도메인확인URL삽입모듈이 상기 사인정보삽입모듈에 의해 발신 대상 전자메일의 본문에 삽입된 텍스트 형식의 사인정보에 상기 웹페이지생성모듈에 의해 생성된 발송 도메인 확인용 URL을 삽입하는 발송도메인확인URL삽입단계와,

상기 발송도메인확인URL삽입단계 이후에, 메일전송부가 사인정보가 부가된 발신 대상 전자메일을 전송하는 메일전송단계를 포함하여,

수신측의 메일 환경을 변경하지 않아도 전자메일 수신측에서 수신된 전자메일의 정보가 사인정보와 일치하는지 여부를 확인해 위험 메일을 파악할 수 있도록 하는, 발송자 사칭을 방지하기 위한 전자메일 보안 방법.

**청구항 18**

메일수신부가 발신 대상 전자메일을 수신하는 메일수신단계와,

상기 메일수신단계 이후에, 사인생성정보추출부가 발신 대상 전자메일을 구성하는 데이터에서 전자메일 수신측이 수신한 메일로부터 확인 가능한 항목의 특정 값을 추출하는 사인생성정보추출단계와,

상기 사인생성정보추출단계 이후에, 호출이미지생성모듈이 추출된 특정 값으로 호출 이미지 형식의 사인정보를 생성하는 호출이미지생성단계와,

상기 사인생성정보추출단계 이후에, 웹페이지생성모듈이 웹페이지 형식으로 사인정보를 생성하는 웹페이지생성단계와,

상기 호출이미지생성단계 및 상기 웹페이지생성단계 이후에, 사인이미지요청URL삽입모듈이 상기 호출이미지생성모듈이 생성한 호출 이미지 형식의 사인정보를 발신 대상 전자메일의 본문에 삽입하는 사인이미지요청URL삽입단계와,

상기 사인이미지요청URL삽입단계 이후에, 발송도메인확인URL삽입모듈이 상기 사인이미지요청URL삽입모듈에 의해 발신 대상 전자메일의 본문에 삽입된 사인 이미지 요청용 URL에 의해 호출되는 이미지 형식의 사인정보에 상기 웹페이지생성모듈에 의해 생성된 발송 도메인 확인용 URL을 삽입하는 발송도메인확인URL삽입단계와,

상기 발송도메인확인URL삽입단계 이후에, 메일전송부가 사인정보가 부가된 발신 대상 전자메일을 전송하는 메일전송단계를 포함하여,

수신측의 메일 환경을 변경하지 않아도 전자메일 수신측에서 수신된 전자메일의 정보가 사인정보와 일치하는지 여부를 확인해 위험 메일을 파악할 수 있도록 하는, 발송자 사칭을 방지하기 위한 전자메일 보안 방법.

**청구항 19**

제18항에 있어서,

상기 호출이미지생성단계는, 호출이미지암호값생성모듈이 상기 사인생성정보추출부에 의해 추출된 특정 값을 암호화하여 암호값을 생성하는 호출이미지암호값생성단계와, 상기 호출이미지암호값생성단계 이후에, 사인이미지요청URL생성모듈이 상기 암호값을 사용하여 사인 이미지 요청용 URL을 생성하는 사인이미지요청URL생성단계를 포함하는 것을 특징으로 하는, 발송자 사칭을 방지하기 위한 전자메일 보안 방법.

**청구항 20**

제16항 내지 제18항 중 어느 한 항에 있어서,

상기 웹페이지생성단계는, 웹페이지암호값생성모듈이 상기 사인생성정보추출부에 의해 추출된 특정 값을 암호화하여 암호값을 생성하는 웹페이지암호값생성단계와, 상기 웹페이지암호값생성단계 이후에, 발송도메인확인URL생성모듈이 상기 암호값을 사용하여 발송 도메인 확인용 URL을 생성하는 발송도메인확인URL생성단계를 포함하는 것을 특징으로 하는, 발송자 사칭을 방지하기 위한 전자메일 보안 방법.

**청구항 21**

제16항 내지 제18항 중 어느 한 항에 있어서,

상기 사인생성정보추출단계는, 발송시각추출모듈이 발신 대상 전자메일의 발송시각을 추출하는 발송시각추출단계와, 발신주소추출모듈이 발신 대상 전자메일의 발신주소를 추출하는 발신주소추출단계와, 수신주소추출모듈이 발신 대상 전자메일의 수신주소를 추출하는 수신주소추출단계와, 참조주소추출모듈이 발신 대상 전자메일의 참조주소를 추출하는 참조주소추출단계와, 메일제목추출모듈이 발신 대상 전자메일의 메일제목을 추출하는 메일제목추출단계를 포함하는 것을 특징으로 하는, 발송자 사칭을 방지하기 위한 전자메일 보안 방법.

**청구항 22**

제21항에 있어서,

상기 전자메일 보안 방법은, 상기 메일제목추출단계 이후에, 변환처리모듈이 상기 메일제목추출모듈로부터 전달받은 메일제목의 일부분을 블라인드 처리하는 변환처리단계를 추가로 포함하는 것을 특징으로 하는, 발송자 사칭을 방지하기 위한 전자메일 보안 방법.

## *발명의 설명*

## 기 술 분 야

[0001] 본 발명은 발송자 사칭을 방지하기 위한 전자메일 보안 시스템 및 그 방법에 관한 것으로, 더욱 상세하게는, 발송처를 위조하는 메일을 수신측이 아닌 발신측의 의지로 막을 수 있도록 하며, 발송측의 기존 메일시스템과 보안시스템의 변경을 가하지 않아도 되고, 수신측의 메일 환경을 변경하지 않아도 메일 공격을 차단할 수 있도록 하는, 발송자 사칭을 방지하기 위한 전자메일 보안 시스템 및 그 방법에 관한 것이다.

## 배 경 기 술

[0002] 글로벌 인터넷 기반의 전자 메일을 사용하는 경우에는, 메일 시스템이 전세계 인터넷망에 연결되어 헤아릴 수 없을 만큼 많은 메일 시스템들과 통신을 하게 되면서, 각종 위험에 쉽게 노출될 수밖에 없다. 프로그램을 이용하여 불특정 다수의 사용자 메일 시스템에 스팸(Spam) 메일을 보내어 음란물 사이트, 도박 사이트, 불법 사이트 등의 광고를 하거나, 메일에 사용자 정보를 탈취하는 악성링크, 첨부파일 등을 삽입해 공격하는 패턴 등을 그 예로 들 수 있다.

[0003] 이러한 문제를 해결하기 위해, 메일 사용자의 개입이 없더라도, 서버 시스템에서 안전한 메일과 위험한 메일을 자동으로 구분할 수 있도록 하는 기술이 개발 되었으며, 그 대표적인 기술이, 발신측 DNS(Domain Name Server) 기반의 SPF(Sender Policy Framework)와, DKIM(Domain Keys Identified Mail)와, DMARC(Domain-based Message Authentication)이다.

[0004] SPF는, 메일 서버 등록제라고 불리는 것으로, 대다수 스팸 발송자가 자신의 신원을 감추기 위하여 발송자 주소나 전송 경로를 허위로 표기하거나 변경하는 경우가 많다는데 착안하여, 메일 서버 정보를 사전에 DNS에 공개 등록함으로써 수신자로 하여금 이메일에 표시된 발송자 정보가 실제 메일 서버의 정보와 일치하는지를 확인할 수 있도록 하는 인증기술을 말한다. SPF를 이용한 이메일 인증절차를 구체적으로 설명하면, 발신자측에서는 자신의 메일 서버 정보와 정책을 나타내는 SPF 레코드를 발신측 도메인 네임 서버(DNS)에 등록하고, 수신자측에서는 이메일 수신시 발신자의 DNS에 등록된 SPF 레코드를 확인하여 해당 이메일에 표시된 발송 IP와 대조하고 그 결과값에 따라 수신 여부를 결정하게 된다. 상기 SPF는 타 인증기술에 비해 적용이 용이하고 호환성이 좋으며 오픈소스를 기반으로 하므로 전 세계적으로 폭넓은 지지기반을 확보하고 있으나, 메일 서버나 스팸차단솔루션에는 SPF 확인 기능이 설치되어 있어야 하는 한계가 있다.

[0005] DKIM은, 도메인 키 인증 메일이라고도 하며, 공개키/비밀키를 기반으로 하는 이메일 인증 방식으로, 디지털 서명을 메일 헤더(Header)에 삽입하여 발신자가 위조되지 않았는지를 수신자 측에서 검증할 수 있도록 하는 인증기술을 말한다. 구체적으로 발신측에서는 DKIM 복호화에 사용될 공개키를 DNS에 등록을 하고 수신측으로 메일을 발송하면, 수신측에서는 메일 수신시 DKIM Header를 검사하고, 발신측 도메인에 DKIM 공개키를 DNS에 질의하여 DKIM-Signature 항목을 복호화 후, 메일 내 컨텐츠가 해시정보와 일치하는지 여부를 확인해, 해시값이 일치하면 통과시키고, 해시값이 불일치하면 스팸으로 차단하게 된다.

[0006] DMARC는, 상기 메일서버 등록제(SPF)와 도메인 키 인증메일(DKIM)을 활용하여 정당한 발신자인지 구분하는 인증기술로, 의심되는 이메일을 처리후 리포팅을 보고 받을 수 있게 한 메일 인증 방식을 말한다. 즉, 발신측에서 DNS에 DMARC 정책을 사전에 게시하고 수신측으로 메일을 발송하게 되면, 수신측에서는 SPF/DKIM을 검사하고, SPF/DKIM 검증 실패시 발신측에서 사전에 게시한 DMARC 정책을 조회한 뒤, None(통과), Quarantine(스팸차단), Reject(메일거부) 옵션에 따라 메일을 처리하게 된다.

[0007] 하지만, 상기 SPF, DKIM, DMARC는 아래와 같은 문제점이 지적되고 있다.

[0008] 우선, SPF, DKIM, DMARC로 수신측이 스팸 메일을 차단하려고 할 경우, 발신 도메인이 SPF, DKIM, DMARC 정보를 제공하지 않는 경우에는 메일 차단이 이루어지겠지만, 반대로, SPF, DKIM, DMARC 정보를 제공할 경우에는 메일이 차단되지 않게 된다. 즉, 악성 메일이라도 SPF, DKIM, DMARC 정보만 있다면 수신측 메일 보안 시스템을 그대로 통과해 버릴 수 있게 되는 것이다. 상기 SPF, DKIM, DMARC는 누구나 사용이 가능하며 크게 어렵지도 않은바, 결국 위험한 메일이라도 SPF, DKIM, DMARC 관리가 된 다른 도메인의 메일은 메일 보안 시스템을 통과할 수 있는 출입증을 가지게 된다는 점에서 심각한 문제가 있다.

[0009] 또한, SPF, DKIM, DMARC는 어디까지나 시스템 관리적 관점에서의 기술적인 장치로, 시스템 상에서 확인된 정보를 메일 사용자에게 메일 보기 화면에 부가정보로 표시할 뿐이다. 하지만, 일반적인 메일 사용자는 이러한 부가정보 보다는 메일의 내용에만 집중하기 때문에 위험한 메일임에도 불구하고, 이름이나 제목, 메일 내용만 읽고

메일을 받아드릴 수 있게 된다.

[0010] 게다가, SPF, DKIM, DMARC는 발신측의 정보에 기반하지만, 수신측에 의존적이라는 문제도 있다. 수신측이 해당 기술을 활용하지 않거나 의도된 화이트리스트나 부가적인 필터들에 의해 의도치 않은 허점을 발생시킬 경우, 발신측을 가장한 메일은 원 발신측의 의사와는 상관없이 수신측 사용자에게 받아들여질 수 있다.

[0011] 뿐만 아니라, SPF, DKIM, DMARC를 설정하지 않은 메일이 모두 위험한 메일이라고 단정할 수도 없는 노릇이다.

[0012] 발신측의 메일 중 위조된 위험 메일을 구분하기 위한 방법으로, 송수신이 필요하다고 분류된 메일 서버와 1:1 보안통신을 하고, 별도의 메일 열람 환경을 사용하는 방법이 있는데, 이 방법은 비용 측면에서 매우 불리하고 폐쇄적이라는 치명적인 약점을 가지고 있다.

[0013] 결국 글로벌 인터넷 상에서의 메일 사용에는 완전하고 범용적인 안전을 보장하는 기술적인 방법은 없고, 폭주하는 스패머(Spammer)를 구분하는 데이터베이스나 이미 확인된 시그니처 기반의 패턴을 분석하는 방법만 있을 뿐이다.

[0014] 만일 모든 정부기관이 DKIM를 도입한다고 가정했을 때, 정부기관과 거래하는 모든 민간기업은 DKIM이 확인되는 메일만 통과하는 시스템으로 추가 투자를 할 수밖에 없어, 예상치 못한 많은 비용의 지출을 겪게 될 것이다.

[0015] 또한, DKIM 기술은 도메인 키가 없는 메일을 차단하는 수준에 그치는바, DKIM 없이 메일 폭탄을 터뜨리는 낮은 수준의 스패머(Spammer) 공격은 차단할 수 있을지언정, DKIM을 활용한 높은 수준의 공격을 차단하지 못하게 된다. 결국, DKIM이 있는 공격에서는 이러한 DKIM이 메일 보안 시스템을 무력화시키는 통과 출입증으로 작용할 수도 있다.

[0016] 이에 관련 업계에서는 스패머가 DKIM 보다 훨씬 많은 비용을 지불해야만 송신측 사칭이 가능하며, RSA(Rivest, Shamir, Adleman) 공개키를 공개하지 않는 방식으로 송신측을 확인할 수 있고, 도입되는 기술이 송수신측의 기존 메일 서버나 보안 시스템에 추가적인 투자를 요구하지 않으며, 인터넷에 연결되어 있는 사용자의 다양한 단말, 메일 프로그램을 그대로 사용할 수 있고, 메일을 열람하는 사용자가 쉽게 신뢰하는 송신측이 맞는지를 확인할 수 있도록 하는 새로운 메일 시스템의 도입을 요구하고 있는 실정이다.

## *선행기술문헌*

### *특허문헌*

[0017] (특허문헌 0001) 한국공개특허공보 제10-2016-0018218호 (2016.02.17.)

## *발명의 내용*

### *해결하려는 과제*

[0018] 본 발명은 상기와 같은 문제점을 해결하고자 안출된 것으로,

[0019] 본 발명의 목적은, 발송처를 위조하는 메일을 수신측이 아닌 발신측의 의지로 막을 수 있도록 하는 것이다.

[0020] 본 발명의 다른 목적은, 보내는 주소를 사칭한 메일 공격과, 제목 또는 내용을 도용한 메일 공격과, 보내는 주소를 유사하게 변조한 메일 공격과, 인벨럽(envelope)의 보낸주소와 메일 헤더(header)의 보낸주소 불일치를 허용하는 수신측 메일 서버에 대한 메일 공격과, 보낸 이름을 도용하여 메일 수신자를 사칭한 메일 공격 등으로부터 수신측을 보호하는 것이다.

[0021] 본 발명의 또 다른 목적은, 발송처를 위조하는 대량 스팸 메일의 경우, 일치하는 사인정보를 발송 메일마다 생성해야만 하고, 동일한 정보의 사인정보 생성이 가능한 경우에도 사용자 클릭시 발송측 도메인으로 접속되어야만 하며, URL 접속시 열람한 메일의 정보와 일치하는 확인페이지가 출력되어야만 하는바, 발송자 사칭 메일을 원천적으로 차단하는 전자메일 보안 시스템을 제공하는 것이다.

[0022] 본 발명의 또 다른 목적은, 발송측의 기존 메일시스템과 보안시스템의 변경을 가하지 않아도 되는 전자메일 보안 시스템을 제공하는 것이다.

[0023] 본 발명의 또 다른 목적은, 수신측의 메일 환경을 변경하지 않아도 메일 공격을 차단할 수 있도록 하는 전자메

일 보안 시스템을 제공하는 것이다.

[0024] 본 발명의 또 다른 목적은, 공격자가 다른 메일에 정상적으로 삽입된 사인 이미지 요청용 URL, 사인정보 또는 발송 도메인 확인용 URL을 다른 메일에 재사용할 경우, 메일 제목, 발신 주소 및 수신 주소까지 동일하게 사용하여 메일을 보내야 하며, 특히 발송 시각까지 동일하게 해야 하는바, 한 개의 사인 이미지 요청용 URL 또는 사인정보 등으로는 다수의 수신 주소로 대량 발송을 할 수 없게 됨으로써, 공격자의 자동화 공격을 무력화 시키는 전자메일 보안 시스템을 제공하는 것이다.

[0025] 본 발명의 또 다른 목적은, 공격자가 사인 이미지 요청용 URL 또는 사인정보를 제3의 위조서버 URL로 공격하는 경우, 메일을 열람하는 열람자가 해당 URL을 클릭했을 때, 정상적으로 발송된 정보가 표시되지 않거나 열람하는 메일과는 다른 값들이 표시되도록 함으로써, 발송자 사칭 메일을 용이하게 검출할 수 있도록 하는, 전자메일 보안 시스템을 제공하는 것이다.

[0026] 본 발명의 또 다른 목적은, 공격자가 발송 도메인 확인용 URL(K)를 위조한 URL(K')로 공격하는 경우, 메일을 열람하는 열람자가 URL(K')를 클릭 했을 때에는, 발송측 서버 도메인이 아닌 위조한 도메인 URL(K')로 연결될 수 밖에 없고, 또한, 공격자가 발송자를 사칭하기 위해서는 URL(K')가 정상적인 URL(K)와 유사하게 표시되도록 하는 시스템까지 구축해야 하는바, 공격 시도를 애초에 단념하게 하는 것이다.

[0027] 본 발명의 또 다른 목적은, 수신측 메일 서버가 정상적인 발송 도메인 확인용 URL(K)를 제공하는 동일한 시스템인 경우 OCR 기술로 URL(S') 또는 사인정보를 인식하고, URL(K')를 검증할 수 있도록 하는 것이다.

[0028] 본 발명의 또 다른 목적은, 공격자가 발송 도메인 확인용 URL(K)를 무작위로 탐색공격하는 경우, URL(K)에 사용하는 암호값은 일련의 값이 아니며, 무작위한 값이므로, 존재하지 않는 K값의 URL(K)를 요청하는 IP를 차단할 수 있는 전자메일 보안 시스템을 제공하는 것이다.

[0029] 본 발명의 또 다른 목적은, 공격자가 네트워크상에서 하이재킹(Hijacking)을 하여 사인 이미지 요청용 URL(S)와 발송 도메인 확인용 URL(K)를 지연없이 사용하는 경우에는 수신자가 동일한 메일제목, 동일한 발신주소, 동일한 발송시각을 가지는 중복되는 메일을 수신하게 되고, 지연되는 경우에는 수신자가 발송시각이 차이 나는 메일을 수신하게 되므로, 발송자 사칭 메일임을 용이하게 알 수 있도록 하는 것이다.

[0030] 본 발명의 또 다른 목적은, 공격자가 K값을 공격하여 암호화 함수를 알아내는 경우, RSA와 달리 암호화/복호화가 모두 발송측 서버에서만 이루어지므로 암호를 해독할 수 없도록 하는 것이다.

## *과제의 해결 수단*

[0031] 본 발명은 앞서 본 목적을 달성하기 위해서 다음과 같은 구성을 가진 실시예에 의해서 구현된다.

[0032] 본 발명의 일 실시예에 따르면, 본 발명은, 발신 대상 전자메일을 수신하는 메일수신부와, 발신 대상 전자메일을 구성하는 데이터에서 특정 값을 추출하는 사인생성정보추출부와, 추출된 특정 값으로 사인정보를 생성하는 사인정보생성부와, 생성된 사인정보를 발신 대상 전자메일에 부가하는 사인정보부가부와, 사인정보가 부가된 발신 대상 전자메일을 전송하는 메일전송부를 포함하여, 전자메일 수신측에서 수신된 전자메일의 정보가 사인정보와 일치하는지 여부를 확인해 위험 메일을 파악할 수 있도록 한다.

[0033] 본 발명의 다른 실시예에 따르면, 본 발명은, 상기 사인정보생성부는, 이미지 형식으로 사인정보를 생성하는 이미지생성모듈을 포함하는 것을 특징으로 한다.

[0034] 본 발명의 또 다른 실시예에 따르면, 본 발명은, 상기 사인정보생성부는, 텍스트 형식으로 사인정보를 생성하는 텍스트생성모듈을 포함하는 것을 특징으로 한다.

[0035] 본 발명의 또 다른 실시예에 따르면, 본 발명은, 상기 사인정보부가부는, 상기 사인정보생성부가 생성한 이미지 또는 텍스트 형식의 사인정보를 발신 대상 전자메일의 본문에 삽입하는 사인정보삽입모듈을 포함하는 것을 특징으로 한다.

[0036] 본 발명의 또 다른 실시예에 따르면, 본 발명은, 상기 사인정보생성부는, 웹페이지 형식으로 사인정보를 생성하는 웹페이지생성모듈을 포함하는 것을 특징으로 한다.

[0037] 본 발명의 또 다른 실시예에 따르면, 본 발명은, 상기 웹페이지생성모듈은, 상기 사인생성정보추출부에 의해 추출된 특정 값을 암호화하여 암호값을 생성하는 웹페이지암호값생성모듈과, 상기 암호값을 사용하여 발송 도메인 확인용 URL을 생성하는 발송도메인확인URL생성모듈을 포함하는 것을 특징으로 한다.

[0038] 본 발명의 또 다른 실시예에 따르면, 본 발명은, 상기 사인정보부가부는, 상기 사인정보삽입모듈에 의해 발신 대상 전자메일의 본문에 삽입된 이미지 또는 텍스트 형식의 사인정보에 상기 웹페이지생성모듈에 의해 생성된 상기 발송 도메인 확인용 URL을 삽입하는 발송도메인확인URL삽입모듈을 포함하는 것을 특징으로 한다.

[0039] 본 발명의 또 다른 실시예에 따르면, 본 발명은, 상기 사인정보생성부는, 호출 이미지 형식으로 사인정보를 생성하는 호출이미지생성모듈을 포함하는 것을 특징으로 한다.

[0040] 본 발명의 또 다른 실시예에 따르면, 본 발명은, 상기 호출이미지생성모듈은, 상기 사인생성정보추출부에 의해 추출된 특정 값을 암호화하여 암호값을 생성하는 호출이미지암호값생성모듈과, 상기 암호값을 사용하여 사인 이미지 요청용 URL을 생성하는 사인이미지요청URL생성모듈을 포함하는 것을 특징으로 한다.

[0041] 본 발명의 또 다른 실시예에 따르면, 본 발명은, 상기 사인정보부가부는, 상기 호출이미지생성모듈이 생성한 상기 사인 이미지 요청용 URL을 발신 대상 전자메일의 본문에 삽입하는 사인이미지요청URL삽입모듈을 포함하는 것을 특징으로 한다.

[0042] 본 발명의 또 다른 실시예에 따르면, 본 발명은, 상기 사인정보생성부는, 웹페이지 형식으로 사인정보를 생성하는 웹페이지생성모듈을 포함하는 것을 특징으로 한다.

[0043] 본 발명의 또 다른 실시예에 따르면, 본 발명은, 상기 웹페이지생성모듈은, 상기 사인생성정보추출부에 의해 추출된 특정 값을 암호화하여 암호값을 생성하는 웹페이지암호값생성모듈과, 상기 암호값을 사용하여 발송 도메인 확인용 URL을 생성하는 발송도메인확인URL생성모듈을 포함하는 것을 특징으로 한다.

[0044] 본 발명의 또 다른 실시예에 따르면, 본 발명은, 상기 사인정보부가부는, 상기 사인이미지요청URL삽입모듈에 의해 발신 대상 전자메일의 본문에 삽입된 사인 이미지 요청용 URL에 의해 호출되는 이미지 형식의 사인정보에 상기 웹페이지생성모듈에 의해 생성된 상기 발송 도메인 확인용 URL을 삽입하는 발송도메인확인URL삽입모듈을 포함하는 것을 특징으로 한다.

[0045] 본 발명의 또 다른 실시예에 따르면, 본 발명은, 상기 사인생성정보추출부는, 발신 대상 전자메일의 발송시각을 추출하는 발송시각추출모듈과, 발신 대상 전자메일의 발신주소를 추출하는 발신주소추출모듈과, 발신 대상 전자메일의 수신주소를 추출하는 수신주소추출모듈과, 발신 대상 전자메일의 참조주소를 추출하는 참조주소추출모듈과, 발신 대상 전자메일의 메일제목을 추출하는 메일제목추출모듈을 포함하는 것을 특징으로 한다.

[0046] 본 발명의 또 다른 실시예에 따르면, 본 발명은, 상기 사인정보생성부는, 상기 메일제목추출모듈로부터 전달받은 메일제목의 일부분을 블라인드 처리하는 변환처리모듈을 추가로 포함하는 것을 특징으로 한다.

[0047] 본 발명의 또 다른 실시예에 따르면, 본 발명은, 메일수신부가 발신 대상 전자메일을 수신하는 메일수신단계와, 상기 메일수신단계 이후에, 사인생성정보추출부가 발신 대상 전자메일을 구성하는 데이터에서 특정 값을 추출하는 사인생성정보추출단계와, 상기 사인생성정보추출단계 이후에, 이미지생성모듈이 추출된 특정 값으로 이미지 형식의 사인정보를 생성하는 이미지생성단계와, 상기 사인생성정보추출단계 이후에, 웹페이지생성모듈이 웹페이지 형식으로 사인정보를 생성하는 웹페이지생성단계와, 상기 이미지생성단계 및 상기 웹페이지생성단계 이후에, 사인정보삽입모듈이 상기 이미지생성모듈이 생성한 이미지 형식의 사인정보를 발신 대상 전자메일의 본문에 삽입하는 사인정보삽입단계와, 상기 사인정보삽입단계 이후에, 발송도메인확인URL삽입모듈이 상기 사인정보삽입모듈에 의해 발신 대상 전자메일의 본문에 삽입된 이미지 형식의 사인정보에 상기 웹페이지생성모듈에 의해 생성된 발송 도메인 확인용 URL을 삽입하는 발송도메인확인URL삽입단계와, 상기 발송도메인확인URL삽입단계 이후에, 메일전송부가 사인정보가 부가된 발신 대상 전자메일을 전송하는 메일전송단계를 포함하여, 전자메일 수신측에서 수신된 전자메일의 정보가 사인정보와 일치하는지 여부를 확인해 위험 메일을 파악할 수 있도록 한다.

[0048] 본 발명의 또 다른 실시예에 따르면, 본 발명은, 메일수신부가 발신 대상 전자메일을 수신하는 메일수신단계와, 상기 메일수신단계 이후에, 사인생성정보추출부가 발신 대상 전자메일을 구성하는 데이터에서 특정 값을 추출하는 사인생성정보추출단계와, 상기 사인생성정보추출단계 이후에, 텍스트생성모듈이 추출된 특정 값으로 텍스트 형식의 사인정보를 생성하는 텍스트생성단계와, 상기 사인생성정보추출단계 이후에, 웹페이지생성모듈이 웹페이지 형식으로 사인정보를 생성하는 웹페이지생성단계와, 상기 텍스트생성단계 및 상기 웹페이지생성단계 이후에, 사인정보삽입모듈이 상기 텍스트생성모듈이 생성한 텍스트 형식의 사인정보를 발신 대상 전자메일의 본문에 삽입하는 사인정보삽입단계와, 상기 사인정보삽입단계 이후에, 발송도메인확인URL삽입모듈이 상기 사인정보삽입모듈에 의해 발신 대상 전자메일의 본문에 삽입된 텍스트 형식의 사인정보에 상기 웹페이지생성모듈에 의해 생성된 발송 도메인 확인용 URL을 삽입하는 발송도메인확인URL삽입단계와, 상기 발송도메인확인URL삽입단계 이후에,

메일전송부가 사인정보가 부가된 발신 대상 전자메일을 전송하는 메일전송단계를 포함하여, 전자메일 수신측에서 수신된 전자메일의 정보가 사인정보와 일치하는지 여부를 확인해 위험 메일을 파악할 수 있도록 한다.

[0049] 본 발명의 또 다른 실시예에 따르면, 본 발명은, 메일수신부가 발신 대상 전자메일을 수신하는 메일수신단계와, 상기 메일수신단계 이후에, 사인생성정보추출부가 발신 대상 전자메일을 구성하는 데이터에서 특정 값을 추출하는 사인생성정보추출단계와, 상기 사인생성정보추출단계 이후에, 호출이미지생성모듈이 추출된 특정 값으로 호출 이미지 형식의 사인정보를 생성하는 호출이미지생성단계와, 상기 사인생성정보추출단계 이후에, 웹페이지생성모듈이 웹페이지 형식으로 사인정보를 생성하는 웹페이지생성단계와, 상기 호출이미지생성단계 및 상기 웹페이지생성단계 이후에, 사인이미지요청URL삽입모듈이 상기 호출이미지생성모듈이 생성한 호출 이미지 형식의 사인정보를 발신 대상 전자메일의 본문에 삽입하는 사인이미지요청URL삽입단계와, 상기 사인이미지요청URL삽입단계 이후에, 발송도메인확인URL삽입모듈이 상기 사인이미지요청URL삽입모듈에 의해 발신 대상 전자메일의 본문에 삽입된 사인 이미지 요청용 URL에 의해 호출되는 이미지 형식의 사인정보에 상기 웹페이지생성모듈에 의해 생성된 발송 도메인 확인용 URL을 삽입하는 발송도메인확인URL삽입단계와, 상기 발송도메인확인URL삽입단계 이후에, 메일전송부가 사인정보가 부가된 발신 대상 전자메일을 전송하는 메일전송단계를 포함하여, 전자메일 수신측에서 수신된 전자메일의 정보가 사인정보와 일치하는지 여부를 확인해 위험 메일을 파악할 수 있도록 한다.

[0050] 본 발명의 또 다른 실시예에 따르면, 본 발명은, 상기 호출이미지생성단계는, 호출이미지암호값생성모듈이 상기 사인생성정보추출부에 의해 추출된 특정 값을 암호화하여 암호값을 생성하는 호출이미지암호값생성단계와, 상기 호출이미지암호값생성단계 이후에, 사인이미지요청URL생성모듈이 상기 암호값을 사용하여 사인 이미지 요청용 URL을 생성하는 사인이미지요청URL생성단계를 포함하는 것을 특징으로 한다.

[0051] 본 발명의 또 다른 실시예에 따르면, 본 발명은, 상기 웹페이지생성단계는, 웹페이지암호값생성모듈이 상기 사인생성정보추출부에 의해 추출된 특정 값을 암호화하여 암호값을 생성하는 웹페이지암호값생성단계와, 상기 웹페이지암호값생성단계 이후에, 발송도메인확인URL생성모듈이 상기 암호값을 사용하여 발송 도메인 확인용 URL을 생성하는 발송도메인확인URL생성단계를 포함하는 것을 특징으로 한다.

[0052] 본 발명의 또 다른 실시예에 따르면, 본 발명은, 상기 사인생성정보추출단계는, 발송시각추출모듈이 발신 대상 전자메일의 발송시각을 추출하는 발송시각추출단계와, 발신주소추출모듈이 발신 대상 전자메일의 발신주소를 추출하는 발신주소추출단계와, 수신주소추출모듈이 발신 대상 전자메일의 수신주소를 추출하는 수신주소추출단계와, 참조주소추출모듈이 발신 대상 전자메일의 참조주소를 추출하는 참조주소추출단계와, 메일제목추출모듈이 발신 대상 전자메일의 메일제목을 추출하는 메일제목추출단계를 포함하는 것을 특징으로 한다.

[0053] 본 발명의 또 다른 실시예에 따르면, 본 발명은, 상기 메일제목추출단계 이후에, 변환처리모듈이 상기 메일제목추출모듈로부터 전달받은 메일제목의 일부분을 블라인드 처리하는 변환처리단계를 추가로 포함하는 것을 특징으로 한다.

## *발명의 효과*

[0054] 본 발명은 앞서 본 실시예와 하기에 설명할 구성과 결합, 사용관계에 의해 다음과 같은 효과를 얻을 수 있다.

[0055] 본 발명은, 발송처를 위조하는 메일을 수신측이 아닌 발신측의 의지로 막을 수 있도록 하는 효과를 가진다.

[0056] 본 발명은, 보내는 주소를 사칭한 메일 공격과, 제목 또는 내용을 도용한 메일 공격과, 보내는 주소를 유사하게 변조한 메일 공격과, 인벨럽(envelope)의 보낸주소와 메일 헤더(header)의 보낸주소 불일치를 허용하는 수신측 메일 서버에 대한 메일 공격과, 보낸 이름을 도용하여 메일 수신자를 사칭한 메일 공격 등으로부터 수신측을 보호하는 효과를 도출한다.

[0057] 본 발명은, 발송처를 위조하는 대량 스팸 메일의 경우, 일치하는 사인정보를 발송 메일마다 생성해야만 하고, 동일한 정보의 사인정보 생성이 가능한 경우에도 사용자 클릭시 발송측 도메인으로 접속되어야만 하며, URL 접속시 열람한 메일의 정보와 일치하는 확인페이지가 출력되어야만 하는바, 발송자 사칭 메일을 원천적으로 차단하는 전자메일 보안 시스템을 제공하는 효과가 있다.

[0058] 본 발명은, 발송측의 기존 메일시스템과 보안시스템의 변경을 가하지 않아도 되는 전자메일 보안 시스템을 제공하는 효과를 가진다.

[0059] 본 발명은, 수신측의 메일 환경을 변경하지 않아도 메일 공격을 차단할 수 있도록 하는 전자메일 보안 시스템을 제공하는 효과를 가진다.

[0060] 본 발명은, 공격자가 다른 메일에 정상적으로 삽입된 사인 이미지 요청용 URL, 사인정보 또는 발송 도메인 확인용 URL을 다른 메일에 재사용할 경우, 메일 제목, 발신 주소 및 수신 주소까지 동일하게 사용하여 메일을 보내야 하며, 특히 발송 시각까지 동일하게 해야 하는바, 한 개의 사인 이미지 요청용 URL 또는 사인정보 등으로는 다수의 수신 주소로 대량 발송을 할 수 없게 됨으로써, 공격자의 자동화 공격을 무력화 시키는 전자메일 보안 시스템을 제공하는 효과를 도출한다.

[0061] 본 발명은, 공격자가 사인 이미지 요청용 URL 또는 사인정보를 제3의 위조서버 URL로 공격하는 경우, 메일을 열람하는 열람자가 해당 URL을 클릭했을 때, 정상적으로 발송된 정보가 표시되지 않거나 열람하는 메일과는 다른 값들이 표시되도록 함으로써, 발송자 사칭 메일을 용이하게 검출할 수 있도록 하는, 전자메일 보안 시스템을 제공하는 효과가 있다.

[0062] 본 발명은, 공격자가 발송 도메인 확인용 URL(K)를 위조한 URL(K')로 공격하는 경우, 메일을 열람하는 열람자가 URL(K')를 클릭 했을 때에는, 발송측 서버 도메인이 아닌 위조한 도메인 URL(K')로 연결될 수밖에 없고, 또한, 공격자가 발송자를 사칭하기 위해서는 URL(K')가 정상적인 URL(K)와 유사하게 표시되도록 하는 시스템까지 구축해야 하는바, 공격 시도를 애초에 단념하게 하는 효과를 가진다.

[0063] 본 발명은, 수신측 메일 서버가 정상적인 발송 도메인 확인용 URL(K)를 제공하는 동일한 시스템인 경우 OCR 기술로 URL(S') 또는 사인정보를 인식하고, URL(K')를 검증할 수 있도록 하는 효과를 도출한다.

[0064] 본 발명은, 공격자가 발송 도메인 확인용 URL(K)를 무작위로 탐색공격하는 경우, URL(K)에 사용하는 암호값은 일련의 값이 아니며, 무작위한 값이므로, 존재하지 않는 K값의 URL(K)를 요청하는 IP를 차단할 수 있는 전자메일 보안 시스템을 제공하는 효과가 있다.

[0065] 본 발명은, 공격자가 네트워크상에서 하이재킹(Hijacking)을 하여 사인 이미지 요청용 URL(S)와 발송 도메인 확인용 URL(K)를 지연없이 사용하는 경우에는 수신자가 동일한 메일제목, 동일한 발신주소, 동일한 발송시각을 가지는 중복되는 메일을 수신하게 되고, 지연되는 경우에는 수신자가 발송시각이 차이 나는 메일을 수신하게 되므로, 발송자 사칭 메일임을 용이하게 알 수 있도록 하는 효과를 가진다.

[0066] 본 발명은, 공격자가 K값을 공격하여 암호화 함수를 알아내는 경우, RSA와 달리 암호화/복호화가 모두 발송측 서버에서만 이루어지므로 암호를 해독할 수 없도록 하는 효과를 도출한다.

## *도면의 간단한 설명*

[0067] 도 1은 본 발명의 발송자 사칭을 방지하기 위한 전자메일 보안 시스템에 관한 개념도.

도 2는 도 1의 블럭도.

도 3은 사인생성정보추출부를 도시한 도면.

도 4는 사인정보생성부를 도시한 도면.

도 5는 사인정보의 일 실시예를 도시한 도면.

도 6은 사인정보의 다른 실시예를 도시한 도면.

도 7은 호출이미지생성모듈을 도시한 도면.

도 8은 웹페이지생성모듈을 도시한 도면.

도 9는 사인정보부가부를 도시한 도면.

도 10은 사인정보의 또 다른 실시예를 도시한 도면.

도 11는 본 발명의 일 실시예에 따른, 발송자 사칭을 방지하기 위한 전자메일 보안 방법에 관한 도면.

도 12는 본 발명의 다른 실시예에 따른, 발송자 사칭을 방지하기 위한 전자메일 보안 방법에 관한 도면.

도 13은 본 발명의 또 다른 실시예에 따른, 발송자 사칭을 방지하기 위한 전자메일 보안 방법에 관한 도면.

도 14는 본 발명의 또 다른 실시예에 따른, 발송자 사칭을 방지하기 위한 전자메일 보안 방법에 관한 도면.

도 15는 본 발명의 사용상태도.

도 16은 본 발명의 사용상태도.

도 17은 본 발명이 구현된 화면의 일 예를 도시한 도면.

## *발명을 실시하기 위한 구체적인 내용*

[0068] 이하에서는 본 발명에 따른 발송자 사칭을 방지하기 위한 전자메일 보안 시스템 및 그 방법의 바람직한 실시 예들을 첨부된 도면을 참고하여 상세히 설명한다. 하기에서 본 발명을 설명함에 있어 공지의 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하도록 한다. 특별한 정의가 없는 한 본 명세서의 모든 용어는 본 발명이 속하는 기술분야의 통상의 지식을 가진 기술자가 이해하는 당해 용어의 일반적 의미와 동일하고 만약 본 명세서에서 사용된 용어의 의미와 충돌하는 경우에는 본 명세서에서 사용된 정의에 따른다.

[0070] 본 발명인 발송자 사칭을 방지하기 위한 전자메일 보안 시스템(1)은, 전자메일 수신측에서 수신된 전자메일의 정보가 사인(Sign)정보와 일치하는지 여부를 확인해 위험 메일을 파악할 수 있도록 하는 것으로, 발송처를 위조하는 메일을 수신측이 아닌 발신측의 의지로 막을 수 있도록 하며, 발송측의 기존 메일시스템과 보안시스템의 변경을 가하지 않아도 되고, 수신측의 메일 환경을 변경하지 않아도 메일 공격을 차단하는 특징이 있다. 일반적인 메일 사인은 고정적으로 사용되며 메일을 작성하는 사용자가 발송 메일에만 해당되는 정보를 상시 기입하지는 못한다는 점에 착안하여, 발송하는 메일에만 해당되는 추가적인 정보를 자동으로 메일사인에 구성하여 보내면 수신자에게 발송메일의 신뢰도를 제공할 수 있게 된다.

[0071] 도 1은 본 발명의 발송자 사칭을 방지하기 위한 전자메일 보안 시스템(1)에 관한 개념도이고, 도 2는 도 1의 블럭도로, 도 1 및 도 2를 참고하면, 기존에는 발신측 단말(S)에서 발신측 서버(SS)로 메일이 전송되면, 네트워크를 통해 해당 메일이 수신측 서버(RS)로 수신이 되어 수신측 단말(S)로 전해지게 되었다. 이러한 구조에서는 발송자 사칭 공격 메일의 전송이 용이하였는바, 본 발명은 발신측에 전자메일 보안 시스템(1)을 추가 구성하여 발송자 사칭 메일 공격을 차단하고자 한다. 이러한 상기 발송자 사칭을 방지하기 위한 전자메일 보안 시스템(1)은, 메일수신부(10), 사인생성정보추출부(20), 사인정보생성부(30), 사인정보부가부(40), 메일전송부(50)를 포함한다.

[0072] 상기 메일수신부(10)는, 발신 대상 전자메일을 수신하는 구성으로, 발신측에서 수신측에 보내고자 하는 메일에 사인정보가 부가될 수 있도록, 특정 메일을 중간에서 수신하는 구성으로 볼 수 있다. 바람직하게는 상기 메일수신부(10)는 기존의 발신측 메일서버에 연결될 수 있다.

[0073] 상기 사인생성정보추출부(20)는, 발신 대상 전자메일을 구성하는 데이터에서 특정 값을 추출하는 구성으로, 상기 메일수신부(10)와 연결되어 상기 메일수신부(10)에 수신된 메일의 헤더(Header) 등을 포함한 메일을 구성하는 데이터에서 특정 값들을 추출하는 것을 말한다. 예를 들어, 발신 대상 전자메일에는, 발송시각, 발신주소, 수신주소, 참조주소, 메일제목, 메일내용 등이 포함될 수 있다.

[0074] 도 3은 사인생성정보추출부(20)를 도시한 도면으로, 도 3을 참고하여 설명하면, 이러한 상기 사인생성정보추출부(20)는, 발송시각추출모듈(21), 발신주소추출모듈(23), 수신주소추출모듈(25), 참조주소추출모듈(27), 메일제목추출모듈(29)을 포함한다.

[0075] 상기 발송시각추출모듈(21)은, 발신 대상 전자메일의 발송시각을 추출하는 구성을 말한다. 전술한 바와 같이, 발신 대상 전자메일을 구성하는 데이터에는 특정 값들이 존재하는데, 상기 발송시각추출모듈(21)은 이러한 특정 값 중에서도 메일이 발송된 시각을 추출하는 구성이다.

[0076] 상기 발신주소추출모듈(23)은, 발신 대상 전자메일의 발신주소를 추출하는 구성으로, 바람직하게는 복수의 정보를 포함하고 있는 메일을 구성하는 데이터에서 발송자의 주소를 추출하는 것으로 볼 수 있다.

[0077] 상기 수신주소추출모듈(25)은, 발신 대상 전자메일의 수신주소를 추출하는 구성으로, 상기 수신주소추출모듈(25)은 메일을 구성하는 데이터에서 발신측이 지정한 수신측의 주소를 추출한다.

[0078] 상기 참조주소추출모듈(27)은, 발신 대상 전자메일의 참조주소를 추출하는 구성으로, 메일을 보낼 때 참조한 주소들을 추출하게 된다.

[0079] 상기 메일제목추출모듈(29)은, 발신 대상 전자메일의 메일제목을 추출하는 구성을 말한다. 상기 메일제목추출모듈(29)에 의해 추출된 특정 값은 후술할 변환처리모듈(39)에 의해 변환 과정을 거칠 수 있다.

[0080] 그 밖에 상기 사인생성정보추출부(20)에는 발신 대상 전자메일에서 메일내용의 문자열 길이를 추출할 수 있는 본문길이추출모듈 등이 추가 구성될 수 있다.

[0081] 상기 사인정보생성부(30)는, 추출된 특정 값으로 사인정보를 생성하는 구성을 말한다. 즉, 상기 사인정보생성부(30)는 상기 사인생성정보추출부(20)와 연결이 되어, 상기 사인생성정보추출부(20)에 의해 추출된 특정 값을 사용해 추출된 특정 값들이 표시된 이미지나, 텍스트, 호출이미지 등의 형식으로 사인정보를 생성하게 된다.

[0082] 도 4는 사인정보생성부(30)를 도시한 도면으로, 도 4를 참고하면, 이러한 사인정보생성부(30)는, 이미지생성모듈(31), 텍스트생성모듈(33), 호출이미지생성모듈(35), 웹페이지생성모듈(37), 변환처리모듈(39)을 포함한다.

[0083] 상기 이미지생성모듈(31)은, 이미지(image) 형식으로 사인정보를 생성하는 구성을 말한다. 도 5는 사인정보의 일 실시예를 도시한 도면으로, 도 5를 참고하면, 이미지 형식의 사인정보에는 도 5에 도시된 바와 같이, 발송시각, 발신주소, 수신주소, 참조주소, 메일제목, 본문길이 등이 포함될 수 있다. 상기 이미지생성모듈(31)에 의해 생성된 이미지는 후술할 사인정보삽입모듈(41)에 의해 메일 본문에 삽입될 수 있으며, 수신측에서는 수신된 메일을 열었을 때, 메일 본문에서 상기 이미지를 확인할 수 있게 된다.

[0084] 상기 텍스트생성모듈(33)은, 텍스트(text) 형식으로 사인정보를 생성하는 구성을 가리킨다. 상기 이미지생성모듈(31)이 상기 사인생성정보추출부(20)가 추출한 특정 값을 이미지 형식으로 나타내는 것이었다면, 상기 텍스트생성모듈(33)은 이미지 대신, 수신측이 열람하게 될 메일 본문에 특정 값을 텍스트 형식으로 나타내는 구성이다. 사인정보를 이미지 형식으로 구현했을 때에는, 다양한 원인에 의해 수신측에서 해당 이미지가 깨져 안보일 수도 있는바, 텍스트 형식의 사인정보를 메일 본문에 부가함으로써, 이러한 문제를 방지할 수 있다.

[0085] 상기 호출이미지생성모듈(35)은, 호출 이미지 형식으로 사인정보를 생성하는 구성을 말한다. 호출 이미지 형식이란, 직접적으로 메일 본문에 이미지를 삽입하는 것이 아니라, 수신측에서 수신한 메일을 열었을 때 자동으로 발송측 서버로 사인 이미지 요청용 URL(URL(S))이 요청되고, 발송측 서버가 URL(S)에서 획득한 암호화값을 복호화하여 해당 메일에만 이미지 형식의 사인정보를 제공할 수 있는 형식을 말한다.

[0086] 상기 이미지생성모듈(31)에 의해 생성된 이미지 형식의 사인정보에 의할 경우 메일 본문에 삽입된 이미지가 변경되지 않지만, 상기 호출이미지생성모듈(35)에 의해 생성된 호출 이미지 형식의 사인정보에 의할 경우 발송측 서버로 이미지를 요청할 때마다 이미지가 변경될 수 있다.

[0087] 도 6은 사인정보의 다른 실시예를 도시한 도면으로, 도 6을 참고하면, 도 6의 사인정보에는 현재시각이 표시되는데, 상기 이미지생성모듈(31)에 의한 이미지 형식의 사인정보는 현재시각의 업데이트가 불가능한 반면, 상기 호출이미지생성모듈(35)에 의한 이미지 형식의 사인정보는 현재시각의 업데이트가 가능해 진다.

[0088] 도 7은 호출이미지생성모듈(35)을 도시한 도면으로, 도 7을 참고하면, 이러한 상기 호출이미지생성모듈(35)은, 호출이미지암호값생성모듈(351), 사인이미지요청URL생성모듈(353)을 포함한다.

[0089] 상기 호출이미지암호값생성모듈(351)은, 상기 사인생성정보추출부(20)에 의해 추출된 특정 값을 암호화하여 암호값을 생성하는 구성을 말한다. 전술한 바와 같이, 상기 호출이미지생성모듈(35)에 의해서는 발신 대상 전자메일의 본문에 URL(S)가 부가되어, 수신측에서 메일을 열었을 때 자동으로 발신측 서버로의 URL(S) 요청이 있게 되는데, 이러한 URL(S)의 요청이 우회 접속이 아닌, 적법한 접속을 통해서만 가능하도록 상기 호출이미지암호값생성모듈(351)을 통해 상기 암호값을 생성하게 된다.

[0090] 상기 사인이미지요청URL생성모듈(353)은, 상기 호출이미지암호값생성모듈(351)이 생성한 암호값을 사용하여 사인 이미지 요청용 URL(URL(S))을 생성하는 구성을 말한다. 상기 사인이미지요청URL생성모듈(353)에 의해 생성된 URL(S)는 후술할 사인이미지요청URL삽입모듈(43)에 의해 발신 대상 전자메일 본문에 삽입될 수 있다.

[0091] 상기 웹페이지생성모듈(37)은, 웹페이지 형식으로 사인정보를 생성하는 구성을 말한다. 웹페이지 형식이란, 직접적으로 메일 본문에 어떠한 사인정보를 삽입한 것이 아니라, 수신측에서 수신한 메일을 열었을 때 메일 본문에 발송 도메인 확인용 URL(URL(K))이 존재하고, 메일 수신자측에서 해당 URL(K)을 클릭 했을 때, 발송측 서버로 URL(K)가 요청되고, 발송측 서버가 URL(K)에서 획득한 암호화값을 복호화하여 사인정보를 가지고 있는 웹페이지가 출력되도록 하는 것을 의미한다.

[0092] 도 8은 웹페이지생성모듈(37)을 도시한 도면으로, 도 8을 참고하면, 상기 웹페이지생성모듈(37)은, 웹페이지암호값생성모듈(371), 발송도메인확인URL생성모듈(373)을 포함한다.

[0093] 상기 웹페이지암호값생성모듈(371)은, 상기 사인생성정보추출부(20)에 의해 추출된 특정 값을 암호화하여 암호

값을 생성하는 구성을 말한다. 상기 웹페이지생성모듈(37)에 의해서는 발신 대상 전자메일의 본문에 발송 도메인 확인용 URL(URL(K))이 부가되어, 수신측에서 메일을 열어 해당 URL(K)를 클릭 했을 때 발신측 서버로의 URL(K) 요청이 있게 되는데, 이러한 URL(K)의 요청이 적법한 접속을 통해서만 가능하도록 상기 웹페이지암호값생성모듈(371)은 특정 값을 암호화한다.

[0094] 상기 발송도메인확인URL생성모듈(373)은, 상기 웹페이지암호값생성모듈(371)이 생성한 암호값을 사용하여 발송 도메인 확인용 URL(URL(K))을 생성하는 구성을 말한다. 상기 발송 도메인 확인용 URL은 발송 도메인으로 접속하는 확인용 링크만이 아니라, 공공기관에서 제공하는 공용도메인을 통해서 확인하는 링크를 모두 포함하는 광의의 개념이다. 상기 발송도메인확인URL생성모듈(373)에 의해 생성된 URL(K)는 후술할 발송도메인확인URL삽입모듈(45)에 의해 발신 대상 전자메일 본문에 삽입될 수 있다. 상기 URL(K)를 통해 발송 메일에 대한 정보를 웹페이지 상에서 구현할 수 있고, 문자가 전송되도록 하여 문자에 발송 메일에 대한 정보가 포함되도록 할 수도 있으며, 채팅 앱 등을 통해 발송 메일에 대한 정보가 고지되도록 할 수도 있다.

[0095] 상기 변환처리모듈(39)은, 상기 사인생성정보추출부(20)의 상기 메일제목추출모듈(29)로부터 전달받은 메일제목의 일부분을 블라인드 처리하는 구성을 말한다. 도 5 및 도 6을 참고하면, 상기 사인생성정보추출부(20)에 의해 발신 대상 전자메일을 구성하는 데이터로부터 발송시각, 발신주소, 수신주소, 참조주소, 메일제목, 본문길이가 추출되었다고 가정했을 때, 상기 이미지생성모듈(31), 상기 텍스트생성모듈(33) 또는 상기 호출이미지생성모듈(35)에 의해 추출된 특정 헤드값이 사인정보로 만들어지게 될 경우, 해당 이미지 사인정보 등에는 발신 대상 전자메일의 원래 메일제목이 그대로 노출되게 된다.

[0096] 메일제목은 메일의 전체 내용을 가늠해 볼 수 있도록 하는 대표적인 단어나 문구로 형성되는바, 이러한 메일제목만으로도 얼마든지 메일에 어떠한 내용이 적혀있을지 추정이 가능하다. 따라서, 메일제목 노출에 의한 정보유출의 염려를 막기 위해 상기 변환처리모듈(39)는 도 5 및 도 6에 도시된 바와 같이, 메일제목의 일부분을 '*' 등의 표현을 통해 가릴 수 있다. 블라인드 되는 부분을 지정하는 방식과 관련하여 일정한 음절을 기준으로 하거나, 앞에서부터 몇 번째 문자들을 기준으로 하거나, 랜덤하게 선정하는 등의 다양한 방식이 적용될 수 있다. 다만, 수신자측에서 받은 메일의 정보를 사인정보와 비교해 발송자 사칭 메일 여부를 확인해 볼 수 있도록 메일제목 전체를 블라인드 처리하는 것은 제외됨이 바람직하다.

[0097] 상기 사인정보부가부(40)는, 생성된 사인정보를 발신 대상 전자메일에 부가하는 구성을 말한다. 즉, 상기 사인정보생성부(30)에 의해 생성된 이미지, 텍스트, URL 형식의 사인정보 등을 메일에 첨부하는 것을 말한다. 상기 사인정보부가부(40)에 의해 최초의 발신 대상 전자메일에는 없었던 사인정보가 추가되고, 수신측에서는 전자메일을 열람할 때, 추가된 사인정보를 확인할 수 있게 된다.

[0098] 도 9는 사인정보부가부를 도시한 도면으로, 도 9를 참고하면, 이러한 상기 사인정보부가부(40)는, 사인정보삽입모듈(41), 사인이미지요청URL삽입모듈(43), 발송도메인확인URL삽입모듈(45)을 포함한다.

[0099] 상기 사인정보삽입모듈(41)은, 상기 사인정보생성부(30)가 생성한 이미지 또는 텍스트 형식의 사인정보를 발신 대상 전자메일의 본문에 삽입하는 구성을 말한다. 즉, 상기 사인정보삽입모듈(41)은, 상기 사인정보생성부(30) 중에서 상기 이미지생성모듈(31) 및 상기 텍스트생성모듈(33)과 연결되어, 상기 이미지생성모듈(31)이 생성한 이미지 형식의 사인정보를 받거나, 상기 텍스트생성모듈(33)이 생성한 텍스트 형식의 사인정보를 받아, 이를 전자메일의 본문에 첨가시키는 기능을 한다. 이로써, 후술할 메일전송부(50)에 의해 수신측으로 전송되는 메일 내에는 변경이 불가능한 이미지 형식의 사인정보 및/또는 텍스트 형식의 사인정보가 추가된다. 웹 문서를 작성하는 언어인 HTML(Hyper Text Markup Language)을 예로 들면, 상기 사인정보삽입모듈(41)에 의해 전자메일에 이미지 형식의 사인정보(IMG)를 삽입하는 동작은 <img src="cid:IMG"> 와 같이 표현될 수 있다.

[0100] 상기 사인이미지요청URL삽입모듈(43)은, 상기 호출이미지생성모듈(35)이 생성한 상기 사인 이미지 요청용 URL(URL(S)을 발신 대상 전자메일의 본문에 삽입하는 구성을 말한다. 전술한 바와 같이, 상기 호출이미지생성모듈(35)에 의해서는 갱신이 가능한 이미지 사인정보가 제공될 수 있는바, 상기 호출이미지생성모듈(35)에 의해 생성된 URL(S)는 상기 사인이미지요청URL삽입모듈(43)을 통해 메일 본문에 부가될 수 있다. HTML로 표현하면, 상기 사인정보삽입모듈(41)의 동작은 <img src="URL(S)"> 일 수 있다.

[0101] 상기 발송도메인확인URL삽입모듈(45)은, 상기 사인정보삽입모듈(41)에 의해 발신 대상 전자메일의 본문에 삽입된 이미지(IMG) 또는 텍스트 형식의 사인정보에 상기 웹페이지생성모듈(37)에 의해 생성된 상기 발송 도메인 확인용 URL(URL(K))을 삽입하는 구성을 말한다. 이러한 상기 발송도메인확인URL삽입모듈(45)의 동작은 HTML로 <a href="URL(K)"><img src="cid:IMG"></a>와 같이 표현될 수 있다.

[0102] 또한, 상기 발송도메인확인URL삽입모듈(45)은, 상기 사인이미지요청URL삽입모듈(43)에 의해 발신 대상 전자메일의 본문에 삽입된 사인 이미지 요청용 URL(URL(S))에 의해 호출되는 이미지 형식의 사인정보에 상기 웹페이지생성모듈(37)에 의해 생성된 상기 발송 도메인 확인용 URL(URL(K))을 삽입할 수도 있으며, 이는 HTML로 <a href="URL(K)"><img src="URL(S)"></a>와 같이 표현된다.

[0103] 도 10은 사인정보의 또 다른 실시예를 도시한 도면으로, 도 10을 참고하면, 상기 발송도메인확인URL삽입모듈(45)에 의해, 수신자측에서 수신한 메일을 열람할 경우 메일의 본문에는 도 10에 도시된 바와 같이 클릭을 유도하는 표현이 나타날 수 있고, 메일 수신자측에서는 1차적으로 메일 본문에 보이는 사인정보의 특정 값을 메일정보와 비교하고, 2차적으로 URL(K)를 클릭해 URL(K)를 호출하면, 발송측 서버는 URL(K)에서 획득한 암호화 값을 복호화 하여 웹페이지를 출력하게 된다.

[0104] 웹브라우저를 통해 나타난 웹페이지 상에는 접속주소가 나타나고, 현재시각, 발송시각, 발신주소, 수신주소, 참조주소, 메일제목, 본문길이, 발송사 로고, 부가적인 사인정보 등이 표현될 수 있다. 수신측에서는 이러한 사인정보를 수신한 메일 정보와 비교하게 된다.

[0105] 상기 메일전송부(50)는, 사인정보가 부가된 발신 대상 전자메일을 전송하는 구성을 말한다. 상기 사인생성정보추출부(20)에 의해 특정 값이 추출되고, 이를 통해 상기 사인정보생성부(30)가 사인정보를 생성하면, 상기 사인정보부가부(40)가 이를 메인 본문에 첨부하게 되는바, 해당 작업까지 완료가 되면, 상기 메일전송부(50)가 상기 사인정보부가부(40)로부터 사인정보가 첨가된 메일을 전달받아 인터넷망 등을 통해 수신측 서버로 메일을 전송하게 된다.

[0107] 이하에서는 발송자 사칭을 방지하기 위한 전자메일 보안 방법(S1)에 관해 설명하도록 하겠다.

[0108] 상기 발송자 사칭을 방지하기 위한 전자메일 보안 방법(S1)은, 전자메일 수신측에서 수신된 전자메일의 정보가 사인정보와 일치하는지 여부를 확인해 위험 메일을 파악할 수 있도록 하는 것으로, 발송처를 위조하는 메일을 수신측이 아닌 발신측의 의지로 막을 수 있도록 하며, 발송측의 기존 메일시스템과 보안시스템의 변경을 가하지 않아도 되고, 수신측의 메일 환경을 변경하지 않아도 메일 공격을 차단할 수 있도록 하는 방법에 관한 것이다.

[0109] 도 11은 본 발명의 일 실시예에 따른, 발송자 사칭을 방지하기 위한 전자메일 보안 방법(S1)에 관한 도면으로, 도 11을 참고하면, 이러한 상기 발송자 사칭을 방지하기 위한 전자메일 보안 방법(S1)은, 메일수신단계(S10)와, 사인생성정보추출단계(S20)와, 사인정보생성단계(S30)와, 사인정보부가단계(S40)와, 메일전송단계(S50)를 포함한다.

[0110] 상기 메일수신단계(S10)는, 메일수신부(10)가 발신 대상 전자메일을 수신하는 단계를 말한다. 상기 메일수신단계(S10)를 통해 발신측 서버에서 수신측 서버로 보내고자 하는 발신 메일이 전자메일 보안 시스템(1)에 수신될 수 있게 된다.

[0111] 상기 사인생성정보추출단계(S20)는, 상기 메일수신단계(S10) 이후에, 사인생성정보추출부(20)가 발신 대상 전자메일을 구성하는 데이터에서 특정 값을 추출하는 단계를 말한다. 상기 특정 값에는 발송시각, 발신주소, 수신주소, 참조주소, 메일제목, 메일내용 등이 포함될 수 있다. 도 11을 참고하면, 이러한 상기 사인생성정보추출단계(S20)는, 발송시각추출단계(S21), 발신주소추출단계(S23), 수신주소추출단계(S25), 참조주소추출단계(S27), 메일제목추출단계(S29)를 포함한다.

[0112] 상기 발송시각추출단계(S21)는, 발송시각추출모듈(21)이 발신 대상 전자메일의 발송시각을 추출하는 단계를 말한다. 발신 대상 전자메일을 구성하는 데이터에는 특정 값들이 존재하는데, 상기 발송시각추출모듈(21)은 이러한 특정 값 중에서도 메일이 발송된 시각을 추출한다.

[0113] 상기 발신주소추출단계(S23)는, 발신주소추출모듈(23)이 발신 대상 전자메일의 발신주소를 추출하는 단계를 말한다. 상기 발신주소추출모듈(23)은 복수의 정보를 포함하고 있는 메일을 구성하는 데이터에서 발송자의 주소를 추출하게 된다.

[0114] 상기 수신주소추출단계(S25)는, 수신주소추출모듈(25)이 발신 대상 전자메일의 수신주소를 추출하는 단계를 말한다. 즉, 메일을 구성하는 데이터에서 해당 메일을 받을 것으로 예정된 수신자측의 메일 주소가 추출된다.

[0115] 상기 참조주소추출단계(S27)는, 참조주소추출모듈(27)이 발신 대상 전자메일의 참조주소를 추출하는 단계를 말한다. 상기 참조주소추출모듈(27)은 발신주소 및 수신주소 이외에 해당 메일을 참조하는 것으로 된 참조메일주소를 추출한다.

[0116] 상기 메일제목추출단계(S29)는, 메일제목추출모듈(29)이 발신 대상 전자메일의 메일제목을 추출하는 단계를 말한다. 추출된 메일제목은 변환처리모듈(39)에 의해 일부의 문자 등이 블라인드 처리되어 정보 유출의 위험이 방지될 수 있다.

[0117] 상기 사인정보생성단계(S30)는, 상기 사인생성정보추출단계(S20) 이후에, 사인정보생성부(30)가 추출된 특정 값으로 사인정보를 생성하는 단계를 말한다. 상기 사인정보는 이미지, 텍스트, URL 등의 형태로 구현될 수 있다.

[0118] 이러한 상기 사인정보생성단계(S30)는, 이미지생성단계(S31), 텍스트생성단계(S33), 호출이미지생성단계(S35), 웹페이지생성단계(S37), 변환처리단계(S39)를 포함한다.

[0119] 상기 이미지생성단계(S31)는, 이미지생성모듈(31)이 추출된 특정 값으로 이미지 형식의 사인정보를 생성하는 단계를 말한다. 이미지 형식의 사인정보의 경우 변경이 불가능한 바, 해당 이미지에 기록된 사인정보를 본 수신측에서는 사인정보에 대한 높은 신뢰를 형성할 수 있다.

[0120] 상기 텍스트생성단계(S33)는, 텍스트생성모듈(33)이 추출된 특정 값으로 텍스트 형식의 사인정보를 생성하는 단계를 말한다. 이미지 형식의 사인정보의 경우, 다양한 원인에 의해 이미지가 깨지거나 보이지 않아 수신측에서 확인이 불가할 수 있는바, 이러한 경우 텍스트 형식의 사인정보 부가가 대안이 될 수 있다.

[0121] 상기 호출이미지생성단계(S35)는, 호출이미지생성모듈(35)이 추출된 특정 값으로 호출 이미지 형식의 사인정보를 생성하는 단계를 말한다. 호출 이미지 형식은 이미지 형식으로 사인정보를 제공하는 것이기는 하지만, 직접적으로 메일 본문에 이미지를 삽입하는 것이 아니라, 수신측에서 수신한 메일을 열었을 때 자동으로 발송측 서버로 사인 이미지 요청용 URL(URL(S))이 요청되고, 발송측 서버가 URL(S)에서 획득한 암호화값을 복호화하여 해당 메일에만 이미지 형식의 사인정보를 제공하게 되는바, 현재시각과 같은 정보를 URL(S) 요청시마다 갱신할 수 있다는 이점이 생긴다.

[0122] 이러한 상기 호출이미지생성단계(S35)는, 호출이미지암호값생성단계(S351), 사인이미지요청URL생성단계(S353)를 포함한다.

[0123] 상기 호출이미지암호값생성단계(S351)는, 호출이미지암호값생성모듈(351)이 상기 사인생성정보추출부(20)에 의해 추출된 특정 값을 암호화하여 암호값을 생성하는 단계를 말한다. 상기 호출이미지생성모듈(35)에 의해서는 발신 대상 전자메일의 본문에 URL(S)가 부가되어, 수신측에서 메일을 열었을 때 자동으로 발신측 서버로의 URL(S) 요청이 있게 되는데, 이러한 URL(S)의 요청이 우회 접속이 아닌, 적법한 접속을 통해서만 가능하도록 상기 호출이미지암호값생성모듈(351)을 통해 상기 암호값을 생성하게 된다. 생성된 암호값은, 수신측에서 URL(S) 접속 시도시 발송측 서버에서 복호화가 이루어질 수 있다.

[0124] 상기 사인이미지요청URL생성단계(S353)는, 상기 호출이미지암호값생성단계(S351) 이후에, 사인이미지요청URL생성모듈(353)이 상기 암호값을 사용하여 사인 이미지 요청용 URL을 생성하는 단계를 말한다. 상기 사인이미지요청URL생성모듈(353)에 의해 생성된 URL(S)는 사인이미지요청URL삽입모듈(43)에 의해 발신 대상 전자메일 본문에 삽입되어, 수신자 측으로 전송되고, 수신자측에서 메일을 열었을 때 자동으로 URL(S) 접속이 시도될 수 있다.

[0125] 상기 웹페이지생성단계(S37)는, 웹페이지생성모듈(37)이 웹페이지 형식으로 사인정보를 생성하는 단계를 말한다. 웹페이지 형식이란, 수신측에서 수신한 메일을 열었을 때 메일 본문에 발송 도메인 확인용 URL(URL(K))이 존재하고, 메일 수신자측에서 해당 URL(K)을 클릭 했을 때, 발송측 서버로 URL(K)가 요청되며, 발송측 서버가 URL(K)에서 획득한 암호화값을 복호화하여 사인정보를 가지고 있는 웹페이지가 출력되는 형식을 말한다.

[0126] 이러한 상기 웹페이지생성단계(S37)는, 웹페이지암호값생성단계(S371)와, 발송도메인확인URL생성단계(S373)를 포함한다.

[0127] 상기 웹페이지암호값생성단계(S371)는, 웹페이지암호값생성모듈(371)이 상기 사인생성정보추출부(20)에 의해 추출된 특정 값을 암호화하여 암호값을 생성하는 단계를 말한다. 특정 값은 암호화 되는바, 적법한 권한이 없는 자가 우회 접속등을 시도할 때 해당 웹페이지가 보이지 않도록 할 수 있다.

[0128] 상기 발송도메인확인URL생성단계(S373)는, 상기 웹페이지암호값생성단계(S371) 이후에, 발송도메인확인URL생성모듈(373)이 상기 암호값을 사용하여 발송 도메인 확인용 URL(URL(K))을 생성하는 단계를 말한다. 상기 발송도메인확인URL생성모듈(373)에 의해 생성된 URL(K)는 발송도메인확인URL삽입모듈(45)에 의해 발신 대상 전자메일 본문에 삽입된다.

[0129] 상기 변환처리단계(S39)는, 상기 메일제목추출단계(S29) 이후에, 변환처리모듈(39)이 상기 메일제목추출모듈

(29)로부터 전달받은 메일제목의 일부분을 블라인드 처리하는 단계를 말한다. 메일제목은 메일의 전체 내용을 가늠해 볼 수 있도록 하는 대표적인 단어나 문구로 형성되는바, 이러한 메일제목만으로도 얼마든지 메일에 어떠한 내용이 적혀있을지 추정이 가능하므로, 메일제목 노출에 의한 정보 유출의 염려를 막기 위해 상기 변환처리단계(S39)에서는 메일제목의 일부분을 '*' 등으로 블라인드 처리할 수 있다.

[0130] 상기 사인정보부가단계(S40)는, 상기 사인정보생성단계(S30) 이후에, 사인정보부가부(40)가 생성된 사인정보를 발신 대상 전자메일에 부가하는 단계를 말한다. 상기 사인정보부가단계(S41)에 의해 상기 사인정보생성단계(S30)에서 생성된 이미지, 텍스트, URL 형식의 사인정보 등이 메일 본문에 첨부될 수 있다.

[0131] 이러한 상기 사인정보부가단계(S40)는, 사인정보삽입단계(S41), 사인이미지요청URL삽입단계(S43), 발송도메인확인URL삽입단계(S45)를 포함한다.

[0132] 상기 사인정보삽입단계(S41)는, 사인정보삽입모듈(41)이 상기 사인정보생성부(30)가 생성한 이미지 또는 텍스트 형식의 사인정보를 발신 대상 전자메일의 본문에 삽입하는 단계를 말한다. HTML을 예로 들어, 전자메일에 이미지 형식의 사인정보(IMG)를 삽입하는 동작은 <img src="cid:IMG"> 와 같이 표현될 수 있다.

[0133] 상기 사인이미지요청URL삽입단계(S43)는, 사인이미지요청URL삽입모듈(41)이 상기 호출이미지생성모듈(35)이 생성한 상기 사인 이미지 요청용 URL(URL(S))을 발신 대상 전자메일의 본문에 삽입하는 단계를 말한다. 상기 사인이미지요청URL삽입단계(S43)는 HTML로 <img src="URL(S)">와 같이 표현된다.

[0134] 상기 발송도메인확인URL삽입단계(S45)는, 발송도메인확인URL삽입모듈(45)이, 상기 사인정보삽입모듈(41)에 의해 발신 대상 전자메일의 본문에 삽입된 이미지(IMG) 또는 텍스트 형식의 사인정보에 상기 웹페이지생성모듈(37)에 의해 생성된 상기 발송 도메인 확인용 URL(URL(K))을 삽입하거나, 상기 사인이미지요청URL삽입모듈(43)에 의해 발신 대상 전자메일의 본문에 삽입된 사인 이미지 요청용 URL(URL(S))에 의해 호출되는 이미지 형식의 사인정보에 상기 웹페이지생성모듈(37)에 의해 생성된 상기 발송 도메인 확인용 URL(URL(K))을 삽입하는 단계를 말한다. HTML에 의하면, 전자의 경우는 <a href="URL(K)"><img src="cid:IMG"></a>, 후자의 경우 <a href="URL(K)"><img src="URL(S)"></a>일 수 있다.

[0135] 상기 메일전송단계(S50)는, 상기 사인정보부가단계(S40) 이후에, 메일전송부(50)가 사인정보가 부가된 발신 대상 전자메일을 전송하는 단계를 말한다. 이로써 수신자 측에서는 메일을 열람할 때 사인정보를 함께 확인할 수 있게 된다.

[0137] 이하에서는, 전술한 각 단계 중, 이미지 형식으로 사인정보를 생성해 생성된 이미지 형식의 사인정보에 발송 도메인 확인용 URL을 삽입하는 과정과, 텍스트 형식으로 사인정보를 생성해 생성된 텍스트 형식의 사인정보에 발송 도메인 확인용 URL을 삽입한 과정과, 호출 이미지 형식으로 사인정보를 생성해 생성된 호출 이미지 형식의 사인정보에 발송 도메인 확인용 URL을 삽입하는 과정을 각각 분리해 각 단계의 선후 관계를 주목하면서 서술하도록 하겠다.

[0138] 도 12는 본 발명의 일 실시예에 따른, 발송자 사칭을 방지하기 위한 전자메일 보안 방법(S1)에 관한 도면으로, 도 12를 참고하여 설명하면, 본 실시예는 이미지 형식으로 사인정보를 생성해, 생성된 이미지 형식의 사인정보에 발송 도메인 확인용 URL을 삽입한 것을 특징으로 한다.

[0139] 구체적으로, 메일수신부(10)가 발신 대상 전자메일을 수신하는 메일수신단계(S10)와, 상기 메일수신단계(S10) 이후에, 사인생성정보추출부(20)가 발신 대상 전자메일을 구성하는 데이터에서 특정 값을 추출하는 사인생성정보추출단계(S20)가 진행된다.

[0140] 상기 사인생성정보추출단계(S20) 이후에는, 이미지생성모듈(31)이 추출된 특정 값으로 이미지 형식의 사인정보를 생성하는 이미지생성단계(S31)가 이루어진다.

[0141] 또한, 상기 사인생성정보추출단계(S20) 이후에는, 웹페이지생성모듈(37)이 웹페이지 형식으로 사인정보를 생성하는 웹페이지생성단계(S37)가 진행된다.

[0142] 상기 이미지생성단계(S31) 및 상기 웹페이지생성단계(S37) 이후에는, 사인정보삽입모듈(41)이 상기 이미지생성모듈(31)이 생성한 이미지 형식의 사인정보를 발신 대상 전자메일의 본문에 삽입하는 사인정보삽입단계(S41)가 진행되고, 상기 사인정보삽입단계(S41) 이후에는, 발송도메인확인URL삽입모듈(45)이 상기 사인정보삽입모듈(41)에 의해 발신 대상 전자메일의 본문에 삽입된 이미지 형식의 사인정보에 상기 웹페이지생성모듈(37)에 의해 생성된 발송 도메인 확인용 URL을 삽입하는 발송도메인확인URL삽입단계(S45)가 진행되며, 상기 발송도메인확인URL삽입단계(S45) 이후에는, 메일전송부(50)가 사인정보가 부가된 발신 대상 전자메일을 전송하는 메일전송단계

(S50)가 진행된다.

[0143] 도 13은 본 발명의 다른 실시예에 따른, 발송자 사칭을 방지하기 위한 전자메일 보안 방법(S1)에 관한 도면으로, 도 13을 참고하여 설명하면, 본 실시예는 텍스트 형식으로 사인정보를 생성해, 생성된 텍스트 형식의 사인정보에 발송 도메인 확인용 URL을 삽입한 것을 특징으로 한다.

[0144] 그 과정을 살펴보면, 우선 메일수신부(10)가 발신 대상 전자메일을 수신하는 메일수신단계(S10)와, 상기 메일수신단계(S10) 이후에, 사인생성정보추출부(20)가 발신 대상 전자메일을 구성하는 데이터에서 특정 값을 추출하는 사인생성정보추출단계(S20)가 차례로 진행된다.

[0145] 상기 사인생성정보추출단계(S20) 이후에는, 텍스트생성모듈(33)이 추출된 특정 값으로 텍스트 형식의 사인정보를 생성하는 텍스트생성단계(S33) 계속된다.

[0146] 바람직하게는 상기 텍스트생성단계(S33)와 별도로, 상기 사인생성정보추출단계(S20) 이후에, 웹페이지생성모듈(37)이 웹페이지 형식으로 사인정보를 생성하는 웹페이지생성단계(S37)가 진행된다.

[0147] 상기 텍스트생성단계(S33) 및 상기 웹페이지생성단계(S37) 이후에는, 사인정보삽입모듈(41)이 상기 텍스트생성모듈(33)이 생성한 텍스트 형식의 사인정보를 발신 대상 전자메일의 본문에 삽입하는 사인정보삽입단계(S41)와, 상기 사인정보삽입단계(S41) 이후에, 발송도메인확인URL삽입모듈(45)이 상기 사인정보삽입모듈(41)에 의해 발신 대상 전자메일의 본문에 삽입된 텍스트 형식의 사인정보에 상기 웹페이지생성모듈(37)에 의해 생성된 발송 도메인 확인용 URL을 삽입하는 발송도메인확인URL삽입단계(S45)와, 상기 발송도메인확인URL삽입단계(S45) 이후에, 메일전송부(50)가 사인정보가 부가된 발신 대상 전자메일을 전송하는 메일전송단계(S50)가 차례로 진행될 수 있다.

[0148] 도 14는 본 발명의 또 다른 실시예에 따른, 발송자 사칭을 방지하기 위한 전자메일 보안 방법(S1)에 관한 도면으로, 도 14를 참고하여 설명하면, 본 실시예는 호출 이미지 형식으로 사인정보를 생성해, 생성된 호출 이미지 형식의 사인정보에 발송 도메인 확인용 URL을 삽입한 것을 특징으로 한다.

[0149] 이에 대한 구체적인 과정을 설명하면, 앞서 설명한 예들과 유사하게 먼저, 메일수신부(10)가 발신 대상 전자메일을 수신하는 메일수신단계(S10)가 진행되고, 상기 메일수신단계(S10) 이후에, 사인생성정보추출부(20)가 발신 대상 전자메일에서 특정 값을 추출하는 사인생성정보추출단계(S20)가 이루어진다.

[0150] 상기 사인생성정보추출단계(S20) 이후에는, 호출이미지생성모듈(35)이 추출된 특정 값으로 호출 이미지 형식의 사인정보를 생성하는 호출이미지생성단계(S35)가 이루어지며, 이와 별도로, 상기 사인생성정보추출단계(S20) 이후에, 웹페이지생성모듈(37)이 웹페이지 형식으로 사인정보를 생성하는 웹페이지생성단계(S37)가 진행될 수 있다.

[0151] 상기 호출이미지생성단계(S35) 및 상기 웹페이지생성단계(S37) 이후에는, 사인이미지요청URL삽입모듈(43)이 상기 호출이미지생성모듈(35)이 생성한 호출 이미지 형식의 사인정보를 발신 대상 전자메일의 본문에 삽입하는 사인이미지요청URL삽입단계(S43)가 진행되고, 상기 사인이미지요청URL삽입단계(S43) 이후에, 발송도메인확인URL삽입모듈(45)이 상기 사인이미지요청URL삽입모듈(43)에 의해 발신 대상 전자메일의 본문에 삽입된 사인 이미지 요청용 URL에 의해 호출되는 이미지 형식의 사인정보에 상기 웹페이지생성모듈(37)에 의해 생성된 발송 도메인 확인용 URL을 삽입하는 발송도메인확인URL삽입단계(S45)가 진행되며, 상기 발송도메인확인URL삽입단계(S45) 이후에, 메일전송부(50)가 사인정보가 부가된 발신 대상 전자메일을 전송하는 메일전송단계(S50)가 이루어질 수 있다.

[0152] 도 15 및 도 16은 본 발명의 사용상태도이고, 도 17은 본 발명이 구현된 화면의 일 예를 도시한 도면으로, 도 15 내지 도 17을 참고하면, 본 발명의 전자메일 보안 시스템(1)에 의해 수신자 측이 받은 메일에는 사인정보가 포함되어, 수신자가 메일을 열었을 때, 도 15에 도시된 바와 같이, 메일 내용의 하단에 사인정보가 표시될 수 있다. 수신자측은 수신한 메일 정보를 불러와 해당 메일의 정보를 사인정보와 비교해 봄으로써, 해당 메일이 발송자를 사칭한 메일인지 여부를 확인할 수 있게 된다. 또한, 메일 본문에는 도 15에 도시된 바와 같이, URL(K)의 클릭을 유도하는 표현이 나타날 수 있고, 수신자가 이를 클릭 등을 할 경우, 도 16에 도시된 바와 같이 웹페이지가 나타나게 되며서, 해당 웹페이지를 통해 사인정보를 확인할 수 있다. 추가적으로, 상기 발신 도메인 확인 URL을 통해 스마트폰으로 문자가 전송되도록 하거나, 채팅앱으로 발송 메일에 대한 정보를 고지해 줄 수도 있다.

[0153] 결국, 수신자측에서는 1차적으로 메일 본문에 보이는 사인정보의 특정 값을 메일 정보와 비교하고, 2차적으로

URL(K)를 클릭해 URL(K)를 호출하면, 발송측 서버는 URL(K)에서 획득한 암호화 값을 복호화 하여 웹페이지를 출력하게 되고, 웹브라우저를 통해 나타난 웹페이지 상에는 접속주소와 함께, 현재시각, 발송시각, 발신주소, 수신주소, 참조주소, 메일제목, 본문길이, 발송사 로고, 부가적인 사인정보 등이 표현될 수 있는바, 수신측에서는 이러한 사인정보를 수신한 메일 정보와 비교함으로써 위험 메일인지 여부를 판단할 수 있게 된다. 스패머가 발송처를 위조하는 메일을 보내려고 할 경우 사인정보와 메일상의 정보가 일치하지 않게 되며, 특히 대량 스팸 메일의 경우 일치하는 사인정보를 발송 메일마다 생성해야만 하고, 동일한 정보의 사인정보 생성이 가능한 경우에도 사용자 클릭시 발송측 도메인으로 접속되어야만 하며, URL 접속시 열람한 메일의 정보와 일치하는 확인페이지가 출력되어야만 하는바, 발송자 사칭 메일은 원천적으로 차단된다.

[0155] 이상의 상세한 설명은 본 발명을 예시하는 것이다. 또한, 전술한 내용은 본 발명의 바람직한 실시 형태를 나타내어 설명하는 것이며, 본 발명은 다양한 다른 조합, 변경 및 환경에서 사용할 수 있다. 즉 본 명세서에 개시된 발명의 개념의 범위, 저술한 개시 내용과 균등한 범위 및/또는 당업계의 기술 또는 지식의 범위내에서 변경 또는 수정이 가능하다. 저술한 실시예는 본 발명의 기술적 사상을 구현하기 위한 최선의 상태를 설명하는 것이며, 본 발명의 구체적인 적용 분야 및 용도에서 요구되는 다양한 변경도 가능하다. 따라서 이상의 발명의 상세한 설명은 개시된 실시 상태로 본 발명을 제한하려는 의도가 아니다. 또한 첨부된 청구범위는 다른 실시 상태도 포함하는 것으로 해석되어야 한다.

## *부호의 설명*

[0156] 1: 발송자 사칭을 방지하기 위한 전자메일 보안 시스템

10: 메일수신부

20: 사인생성정보추출부

21: 발송시각추출모듈

23: 발신주소추출모듈

25: 수신주소추출모듈

27: 참조주소추출모듈

29: 메일제목추출모듈

30: 사인정보생성부

31: 이미지생성모듈

33: 텍스트생성모듈

35: 호출이미지생성모듈

351: 호출이미지암호값생성모듈

353: 사인이미지요청URL생성모듈

37: 웹페이지생성모듈

371: 웹페이지암호값생성모듈

373: 발송도메인확인URL생성모듈

39: 변환처리모듈

40: 사인정보부가부

41: 사인정보삽입모듈

43: 사인이미지요청URL삽입모듈

45: 발송도메인확인URL삽입모듈

50: 메일전송부

S1: 발송자 사칭을 방지하기 위한 전자메일 보안 방법

S10: 메일수신단계

S20: 사인생성정보추출단계

S21: 발송시각추출단계

S23: 발신주소추출단계

S25: 수신주소추출단계

S27: 참조주소추출단계

S29: 메일제목추출단계

S30: 사인정보생성단계

S31: 이미지생성단계

S33: 텍스트생성단계

S35: 호출이미지생성단계

S351: 호출이미지암호값생성단계

S353: 사인이미지요청URL생성단계

S37: 웹페이지생성단계

S371: 웹페이지암호값생성단계

S373: 발송도메인확인URL생성단계

S39: 변환처리단계

S40: 사인정보부가단계

S41: 사인정보삽입단계

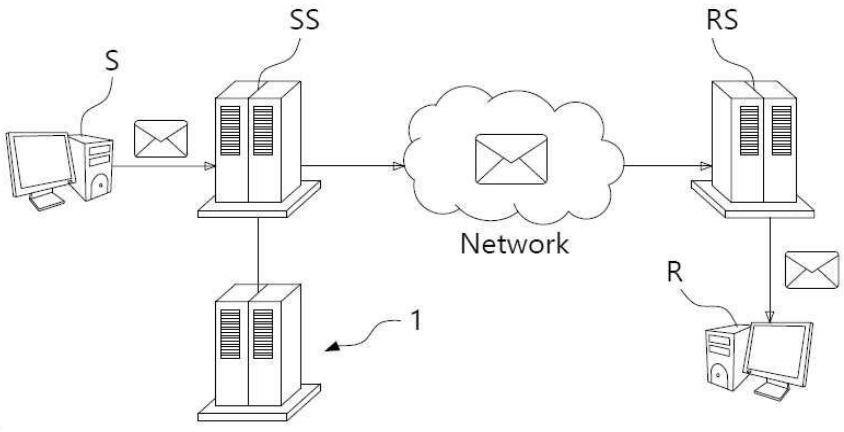
S43: 사인이미지요청URL삽입단계

S45: 발송도메인확인URL삽입단계

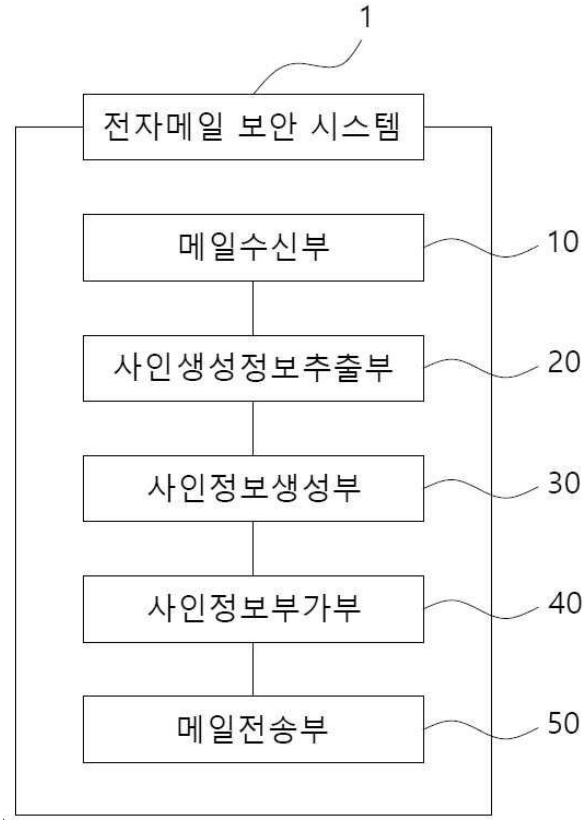
S50: 메일전송단계

## 도면

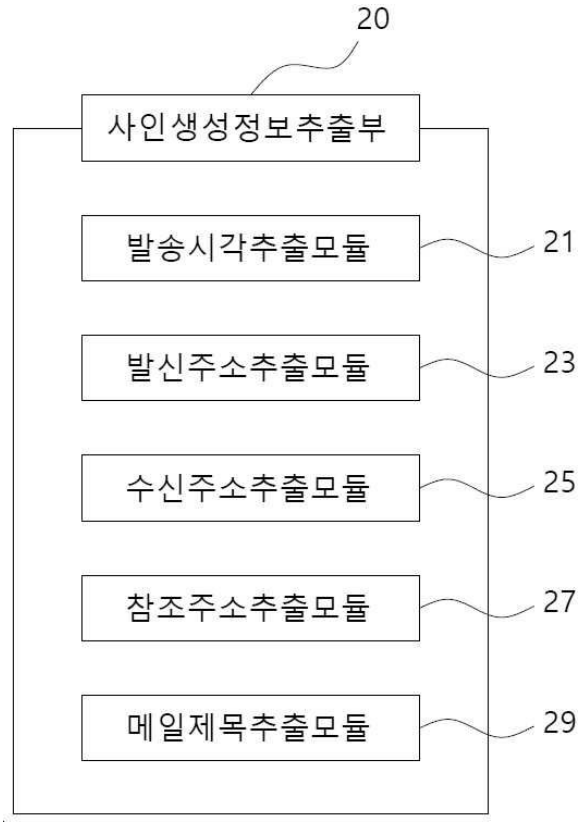
### 도면1



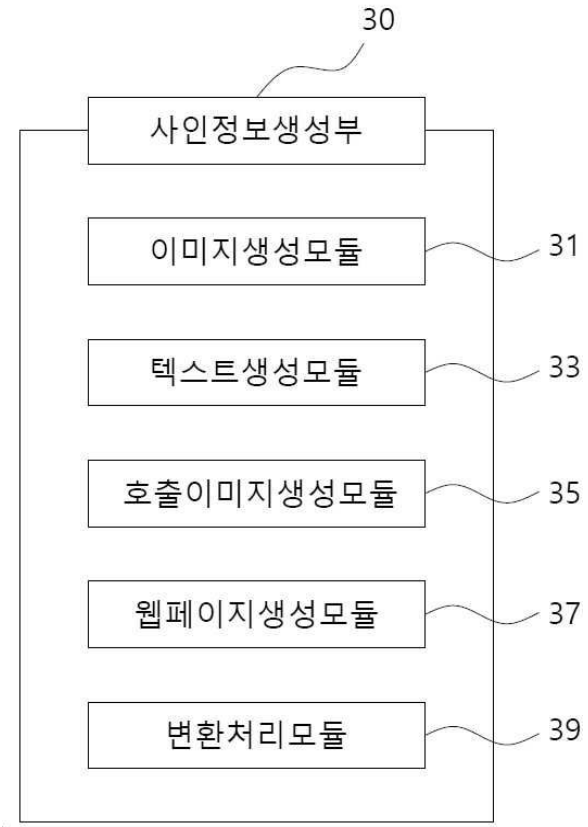
도면2


1
전자메일 보안 시스템
메일수신부
10
사인생성정보추출부
20
사인정보생성부
30
사인정보부가부
40
메일전송부
50

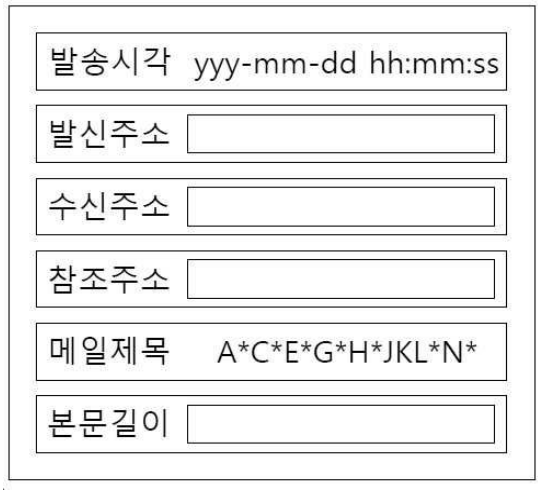
도면3


20
사인생성정보추출부
발송시각추출모듈
21
발신주소추출모듈
23
수신주소추출모듈
25
참조주소추출모듈
27
메일제목추출모듈
29

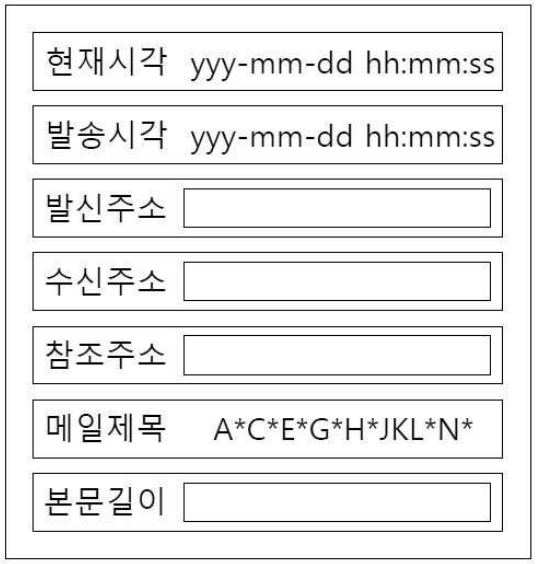
도면4


30
사인정보생성부
이미지생성모듈
31
텍스트생성모듈
33
호출이미지생성모듈
35
웹페이지생성모듈
37
변환처리모듈
39

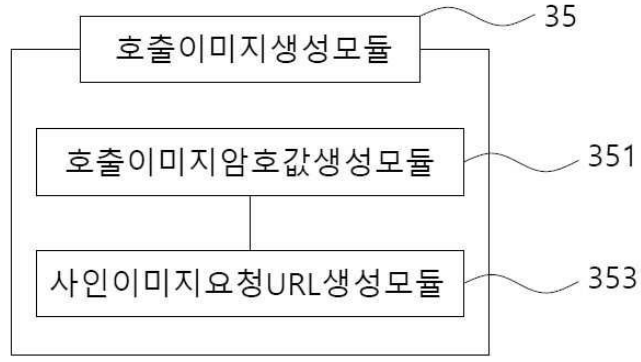
도면5


발송시각 yyy-mm-dd hh:mm:ss
발신주소
수신주소
참조주소
메일제목 A*C*E*G*H*JKL*N*
본문길이

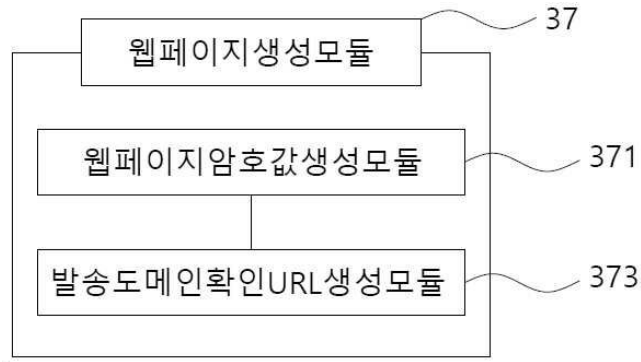
도면6


현재시각 yyy-mm-dd hh:mm:ss
발송시각 yyy-mm-dd hh:mm:ss
발신주소
수신주소
참조주소
메일제목 A*C*E*G*H*JKL*N*
본문길이

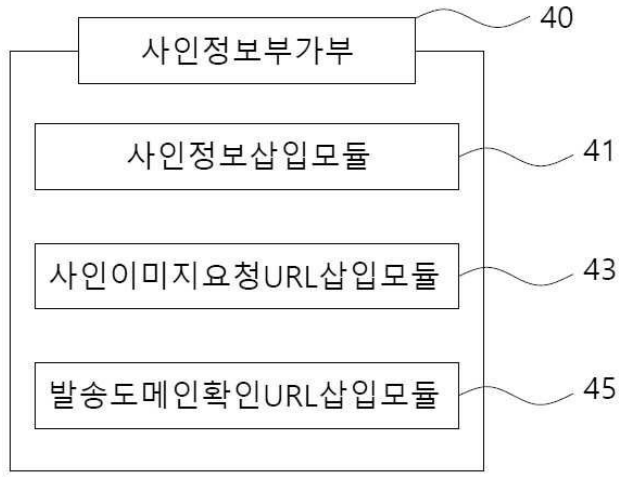
도면7


35
호출이미지생성모듈
351
호출이미지암호값생성모듈
353
사인이미지요청URL생성모듈

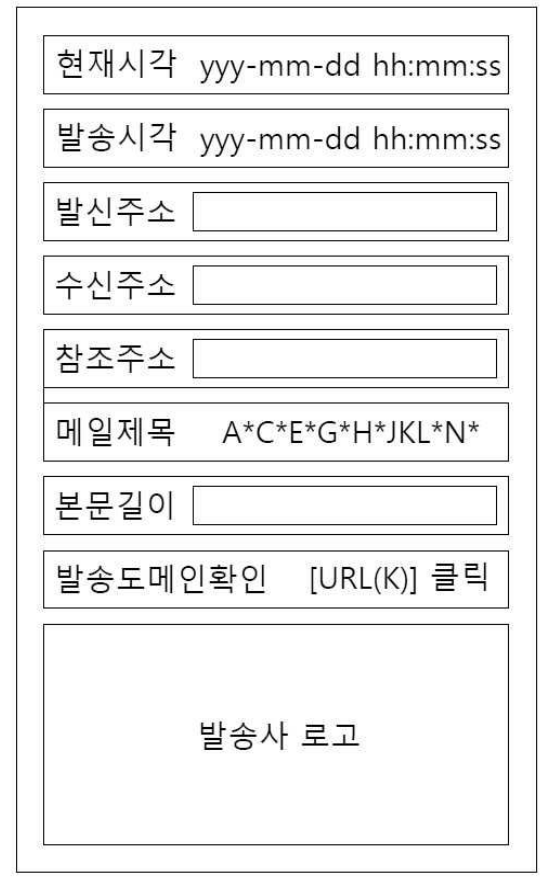
도면8


37
웹페이지생성모듈
371
웹페이지암호값생성모듈
373
발송도메인확인URL생성모듈

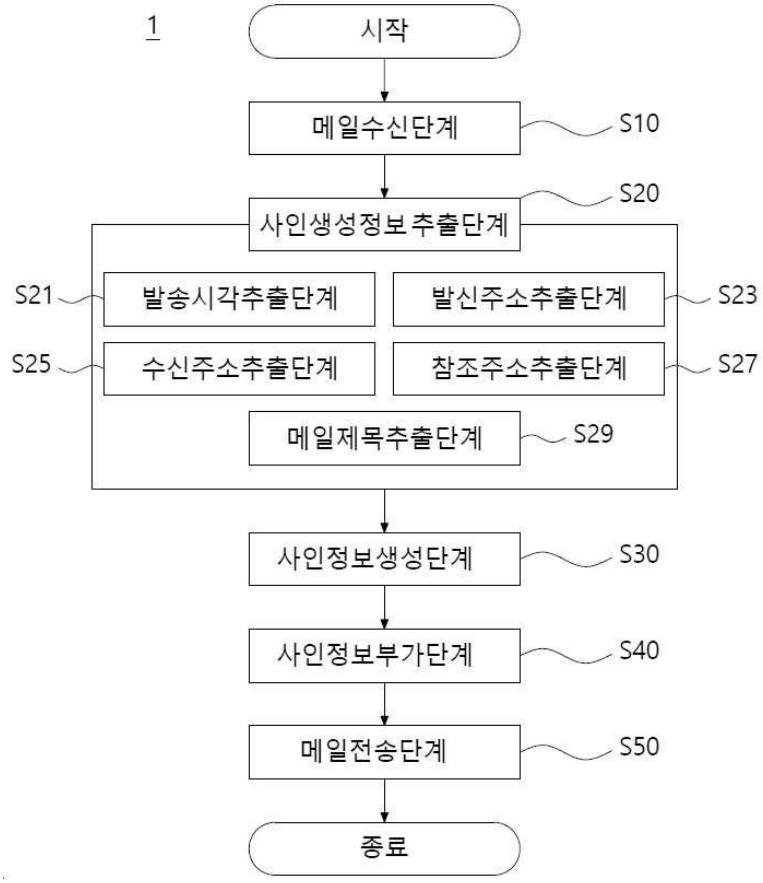
도면9


사인정보부가부
40
사인정보삽입모듈
41
사인이미지요청URL삽입모듈
43
발송도메인확인URL삽입모듈
45

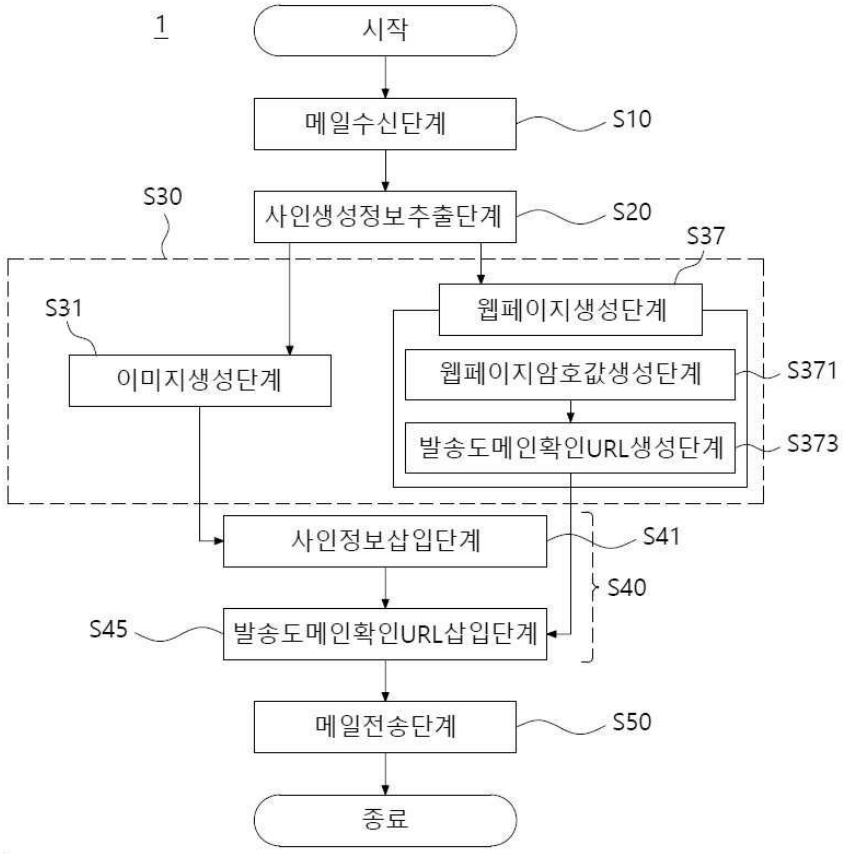
도면10


현재시각 yyy-mm-dd hh:mm:ss
발송시각 yyy-mm-dd hh:mm:ss
발신주소
수신주소
참조주소
메일제목 A*C*E*G*H*JKL*N*
본문길이
발송도메인확인 [URL(K)] 클릭
발송사 로고

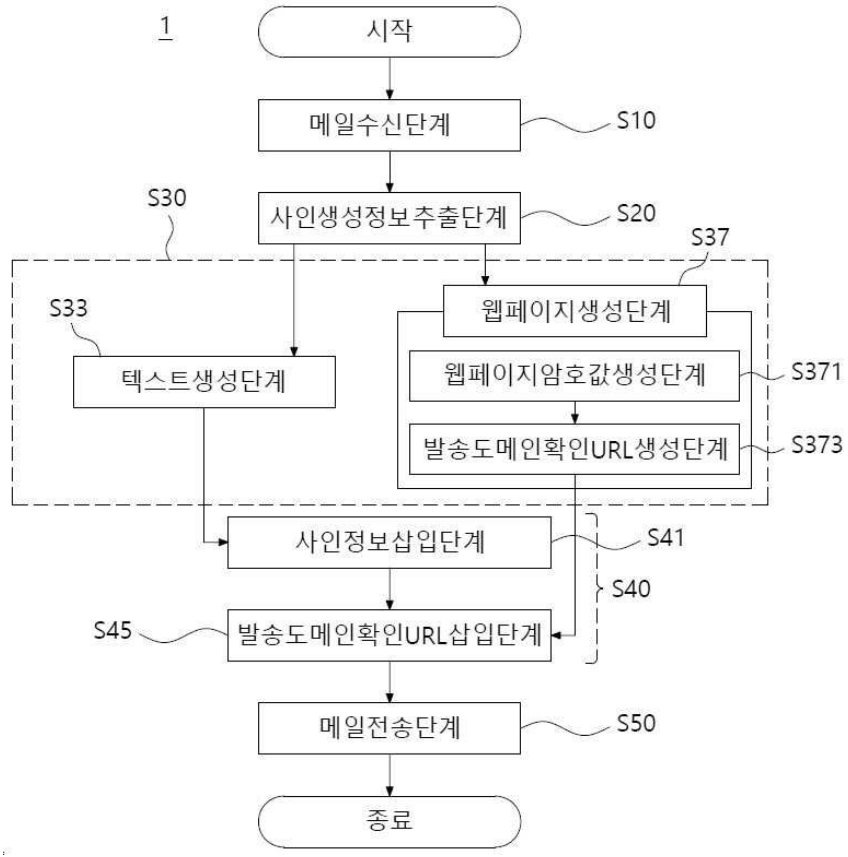
도면11


1
시작
메일수신단계
S10
사인생성정보추출단계
S20
S21
발송시각추출단계
발신주소추출단계
S23
S25
수신주소추출단계
참조주소추출단계
S27
메일제목추출단계
S29
사인정보생성단계
S30
사인정보부가단계
S40
메일전송단계
S50
종료

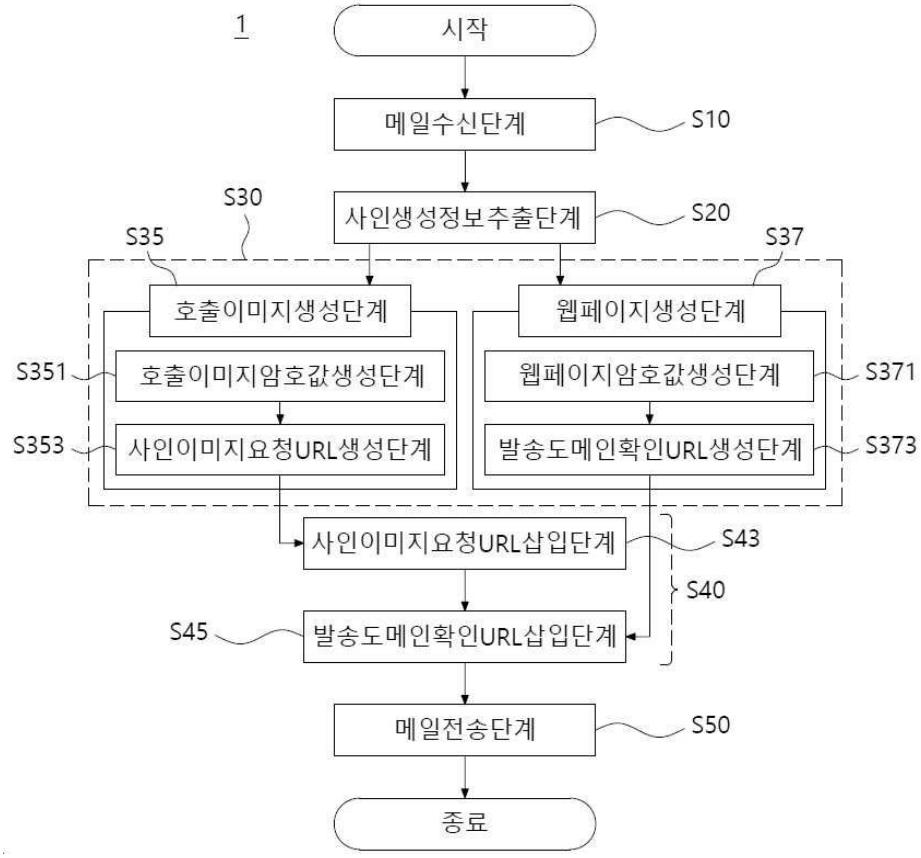
도면12


1
시작
메일수신단계
S10
S30
사인생성정보추출단계
S20
S37
S31
웹페이지생성단계
이미지생성단계
웹페이지암호값생성단계
S371
발송도메인확인URL생성단계
S373
사인정보삽입단계
S41
S40
S45
발송도메인확인URL삽입단계
메일전송단계
S50
종료

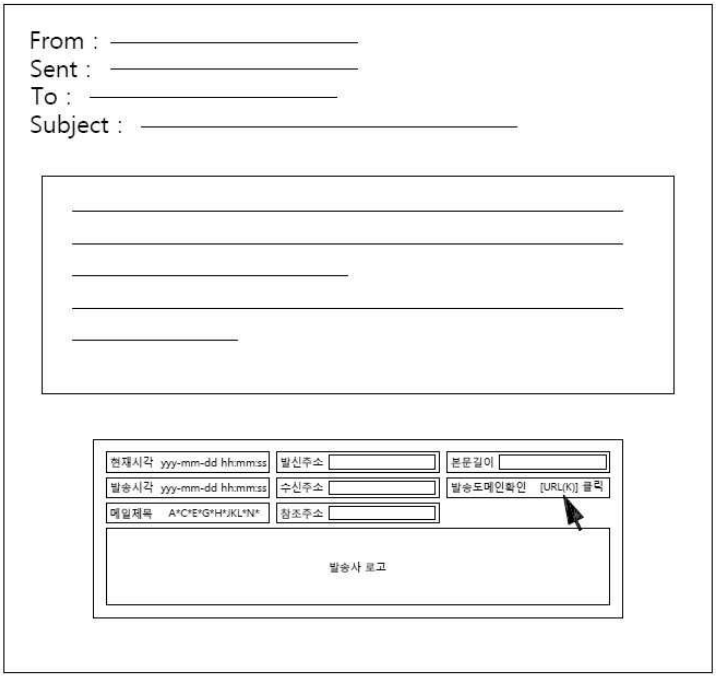
도면13


1
시작
메일수신단계
S10
S30
사인생성정보추출단계
S20
S37
웹페이지생성단계
S33
텍스트생성단계
웹페이지암호값생성단계
S371
발송도메인확인URL생성단계
S373
사인정보삽입단계
S41
S40
S45
발송도메인확인URL삽입단계
메일전송단계
S50
종료

도면14


1
시작
메일수신단계
S10
S30
사인생성정보추출단계
S20
S35
S37
호출이미지생성단계
웹페이지생성단계
S351
호출이미지암호값생성단계
웹페이지암호값생성단계
S371
S353
사인이미지요청URL생성단계
발송도메인확인URL생성단계
S373
사인이미지요청URL삽입단계
S43
S40
S45
발송도메인확인URL삽입단계
메일전송단계
S50
종료

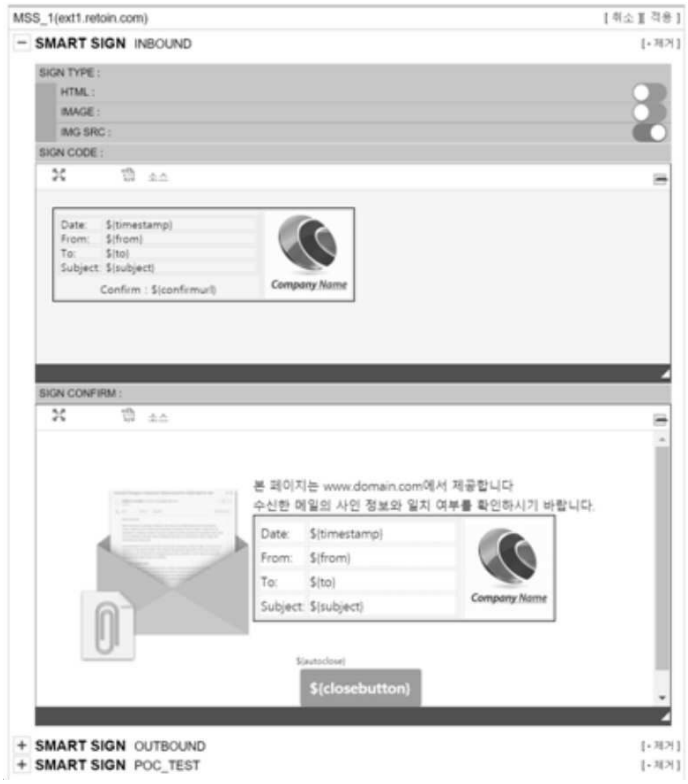
도면15


From :
Sent :
To :
Subject :
현재시각 yyy-mm-dd hh:mm:ss
발신주소
본문길이
발송시각 yyy-mm-dd hh:mm:ss
수신주소
발송도메인확인 [URL(K)] 클릭
메일제목 A*C*E*G*H*JKL*N*
참조주소
발송사 로고

도면16


https://
현재시각 yyy-mm-dd hh:mm:ss
발송시각 yyy-mm-dd hh:mm:ss
발신주소
수신주소
참조주소
메일제목 A*C*E*G*H*JKL*N*
본문길이
발송사 로고

도면17


MSS_1(ext1.retoin.com)
[ 취소 ][ 적용 ]
SMART SIGN INBOUND
[- 제거 ]
SIGN TYPE :
HTML :
IMAGE :
IMG SRC :
SIGN CODE :
Date: $(timestamp)
From: $(from)
To: $(to)
Subject: $(subject)
Confirm : $(confirmurl)
Company Name
SIGN CONFIRM :
본 페이지는 www.domain.com에서 제공합니다
수신한 메일의 사인 정보와 일치 여부를 확인하시기 바랍니다.
Date: $(timestamp)
From: $(from)
To: $(to)
Subject: $(subject)
Company Name
$(autoclose)
$(closebutton)
SMART SIGN OUTBOUND
[- 제거 ]
SMART SIGN POC_TEST
[- 제거 ]