크리니티 시큐어
CRINITY SECURE

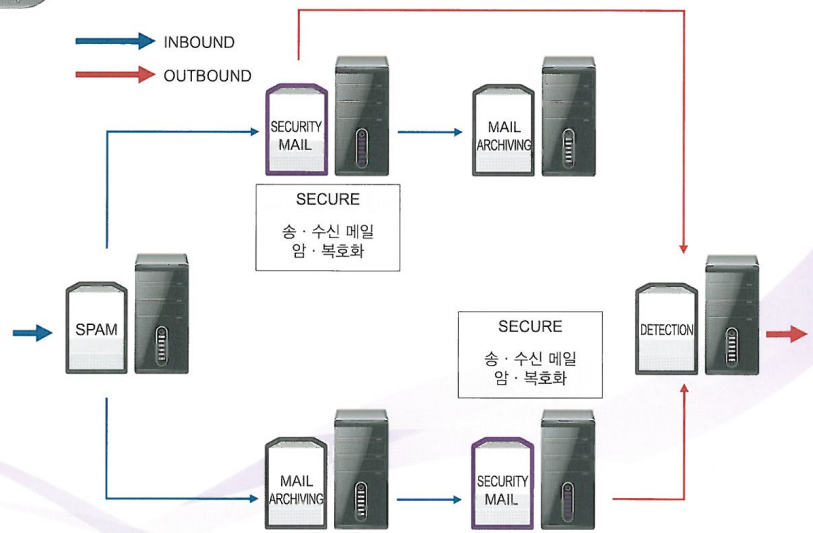
국정원 가이드라인 준수한 보안메일 솔루션

국정원의 '상용이메일 차단 가이드라인'을 준수한 보안메일 솔루션인 크리니티 시큐어는 사용자 정보 암호화(MD5) 저장, 웹구간 보안통신(SSL) 적용, ARIA 암호화모듈 탑재와 100% Java Based 설계로 다양한 보안모듈(웹구간 암호화, 본문 암호화, 키보드 보안 등)과의 연동을 통해 보안성을 강화한 메일 시스템을 제공합니다.

Key Features

◎ 국가정보원 '공공기관 상용이메일 차단 가이드라인'을 준수하는 보안메일 솔루션
◎ 100% Java Based 솔루션으로 다양한 보안모듈 및 기존 인프라와의 유연한 연동지원
◎ 사용자 정보 암호화(MD5), 웹구간 통신 암호화(SSL), ARIA 암호 및 GPKI, NPKI 인증 모듈 기본적용
◎ 보안모듈(본문 암호화, 웹구간 암호화, 키보드 보안) 적용을 통한 고객사 맞춤형 보안환경 구성
◎ 크리니티 메시징의 웹 2.0 Ajax 인터페이스 적용으로 사용자 편의성과 송수신 보안성 강화 동시 제공
◎ 고용노동부, 국방부, 한국은행, 국민연금공단, 포천시청 등 검증된 고객사 보유

Architecture



CRINITY SOLUTION SUITE
TOTAL MESSAGING SOLUTION PROVIDER

Benefits

◎ 인증서를 통한 사용자 인증 : 인증서(GPKI or NPKI)를 통해 메일 송수신 대상의 본인 여부 증명 가능
◎ 전자서명을 통한 데이터 무결성 확보 : 인터넷 상에서 전달된 메일의 내용이 위 · 변조되지 않은 데이터임을 확인 가능
◎ 데이터 암호화를 통한 기밀성 확보 : 네트워크 상에서 전달되는 사용자의 신상정보, 각종 사용 내역 등 중요 데이터의 도청 가능성 완전 봉쇄
◎ 전자서명을 통한 부인방지 수행 : 수신 확인 메시지에 대해 암호화 및 전자서명 기능을 제공하여 수신 메일에 대한 부인 방지 기능 제공

Major Functions

인증서를 이용한 암 · 복호화	■인증서(GPKI or NPKI)를 통한 암호화 혹은 개인 인증서를 통한 전자서명을 사용하여 자동 등록 가능 ■등록된 수신자들의 인증서(공개키 정보)를 이용하여 메일을 암호화해서 전송 ■수신자는 공개키 정보(주민등록번호 뒷자리, 아이디 등)를 이용하여 메일 복호화
인증서 방식의 로그인	■웹 프로토콜을 기반으로 SSL 사용자와 웹 서버간에 설치되어 보안서비스 제공 ■웹메일에 인증서를 이용하여 개인정보 유출 및 위 · 변조 방지하여 보안성 강화
키로깅 방지 기능(옵션)	■키보드를 통해 입력되는 아이디, 패스워드 정보를 드라이버 레벨에서 암호화 처리 ■정보유출도구의 공격에 의해 중요 정보가 유출되는 것을 근본적으로 차단
보안메일 발송	■발신인이 메일을 보낼 때 암호 입력 -> 수신자는 발신인이 입력한 암호를 입력해야 메일 보기 가능

Paradigm

공공기관	■행정업무용, 공문서 발송, 민원서류 접수, 정책관련 의사결정, 대민 서비스 등
금융기관	■송금, 계좌이체, 세금납부 등의 개인 Privacy 관련 문서, 내부 금융정보 유통, 고객관리용 발송메일 등
기 업	■Project 관리문서, 내부의사결정, 인사규정, 개발연구자료, 도면, 세금계산서 유통 등
대 학 교	■교수 및 연구실의 연구논문자료, 학사행정자료, 교수 및 학생 신상자료 등

Requirements

H/W	■최소 : CPU Xeon 3.0 Dual, Memory 2GB 이상, HDD 500G 이상 ■권장 : CPU Xeon 3.0 Quad, Memory 4GB 이상, HDD 500G 이상
OS	■Linux (Redhat 계열), Unix(Solaris, HP-UX, AIX)
DBMS	■MySQL, Oracle
WAS	■Websphere, JBoss, Weblogic, Jeus, Tomcat

구입 문의
E-Mail. sales@crinity.com
Tel. 070-7018-9251~3

제휴 문의
E-Mail. news@crinity.com
Tel. 070-7018-9257