情報保護學會論文誌
第19卷 第3號, 2009. 6

개인정보관리를 위한 메시지 트리 기반의 모바일 알람 시스템 구축*

장 은 영,† 김 형 종,‡ 황 준
서울여자대학교 컴퓨터학과

Development of Mobile Alarm System using Message Tree for Personal Information Management*

Eun-young Jang,† Hyung-Jong Kim,‡ Jun Hwang
Division of Computer, Seoul Women's University

요 약

최근 개인 정보 유출 사고가 빈번히 발생하고 있으나, 개인들은 이러한 정보의 유출에 대해 언론의 보도를 통해서 알게 되는 것일 일반적이다. 개인정보의 소유권에 대해 고려해 볼 때, 이러한 현상은 이치에 맞지 않는 것이라고 할 수 있다. 본 논문에서는 이러한 문제의 해결책으로 모바일 알람 시스템을 제안한다. 모바일 알람 시스템은 사용자의 개인정보 활용에 대한 알람정보를 모바일 문자로 보내고, 문자 수신자는 모바일 대응 프로그램을 통해 알람정보에 따른 동의 및 거부의견을 전달하여 본인이 개인정보 관리에 직접적으로 관여 할 수 있도록 하는 시스템이다. 본 연구에서는 모바일 기기의 제한된 인터페이스를 고려하여 "개인정보 유출 알람 메시지 트리"를 구성하였다. 개인정보 유출 알람 메시지 트리는 전송된 메시지에 대한 단순응대를 통해 개인정보 통제의 모든 대응 방법 수행을 체계적으로 할 수 있도록 한다. 본 논문의 기여도는 모바일 알람 시스템의 알람 메시지 트리 설계를 통해 인터페이스가 한정되어 있는 모바일환경에서 실시간 개인정보 관리 시스템의 구조제안에 있다.

ABSTRACT

When a private information security incident occurs, the people who own the information are not acknowledged about their information leakage until those affairs appear in public media. This research aims at developing a mobile alarm system for acknowledging suspicious events to the information owners. The mobile alarm system was designed considering the limited user interface of mobile terminal and concept of "personal information leakage message tree" is deployed. The message tree contains every possible situation about personal information leakage and the leaves of the tree has several choices that the information owner can select. This message tree concept enables each information owner to manager his or her information leakage situation by just pushing a few buttons of mobile device. The contribution of this paper is in design of a comprehensive alarm message tree and development of mobile alarm system containing the message tree concept.

Keywords: Mobile Alarm, Personal information leakage, Message Tree

I. 서 론

정보통신기술이 발전하고 인터넷이 확산되어 유비쿼터스 사회가 되면서 여러 분야에서 개인정보의 활용이 증가 하였다. 따라서 정보의 가치는 점점 높아졌고 많은 개인 정보를 보유한 기업의 가치는 상승하였다.

접수일(2009년 1월 18일), 수정일(2009년 5월 11일), 게재확정일(2009년 6월 5일)
* 본 연구는 서울시 산학연 협력사업(NT070103) 지원으로 수행하였습니다.
† 주저자, elishajey@gmail.com
‡ 교신저자, hkim@swu.ac.kr

그러나 개인정보보호에 대한 인식수준이 낮고, 다양한 유무선 기기에 대한 해킹, 바이러스, 공격의 기술이 발전하면서 다양한 경로를 통한 정보유출 피해자가 속출했다. 현재는 이를 막기 위해 정보유출방지 프로그램인 백신, 방화벽, 데이터베이스 보안 솔루션 등을 이용해 개인정보 유출을 최소화 하고 있다. 게다가 승인된 정보 활용에 관한 문제도 야기되고 있는데, 사용자들은 회원 가입 시 기업에서 요구한 정보기입사항에 개인정보의 중요성을 인식하지 못하고 무분별하게 정보를 기입하여 정보 유출이 발생하고 있다. 또한 기업들은 정보소유자의 동의 없이 이러한 개인정보를 사용하고 관리하며 자기업간은 무분별하게 개인정보를 공유하고 있다. 이로써 사용자는 자신의 정보에 대한 사용출처를 알 수 없는 상황이다. 현재 정부에서는 법적으로 이 문제에 대 시정명령이나 과태료 부과, 형사고발 조치는 하고 있다. 그러나 위반 기업이 있다 하더라도 사용자에게 위반 사실을 알리지 않고, 가벼운 벌금으로 순간만 모면하는 상황이 지속되고 있다.[1] 또한 전자상거래의 보편화로 인해 개인정보는 더욱 쉽게 모니터링 되고 유출, 침해되고 있다. 이러한 상황에 대해 사용자나 공공기관은 개인정보보호의 최소한의 규정을 원하고 있다. 설문결과, 모든 사용자는 자신의 정보 활용에 대해 반드시 통지, 확인을 받아야 한다고 답하였다[1].

이러한 문제점의 해결을 위해 본 논문에서는 보안이 보장되는 개인정보 관리를 하는 정보관리 시스템의 주변 보안 시스템인 알람시스템을 설계하였으며 사용자의 개인정보 활용에 대한 알람의 요구를 만족시키기 위해서 모바일 알람 메시지를 제안하였다. 본 논문에서는 사용자가 개인정보를 모바일을 통해 1차로 직접 관리할 수 있는 보안이 보장된 개인정보 유출 대응 시스템을 제안한다.

II. 관련연구

정보기술의 발전으로 전자상거래가 증가하면서 정보 활용의 범위가 증대되어 개인정보에 대한 공격이 늘어나고 있다. 개인정보의 침해 및 유출은 유형별 증감은 있지만 꾸준히 많이 발생하고 있으며, 일반 사용자 정보의 중요성 인식이 높아짐에 따라 침해신고도 증가하고 있다. 개인정보 침해, 유출 신고 현황은 주민번호 등 타인정보의 훼손, 침해, 도용이 가장 많은 비중을 차지하며, 그 다음으로 이용자 동의 없는 개인정보수집과 동의철회·열람 또는 정정 요구 등 불응, 고지·명시한 범위를 초과한 목적 외 이용 또는 제 3자 제공유형 순으로 많은 비중을 차지한다. 정보통신망법 규정외의 침해 유형은 신고사항에 대한 변동사항이 많으나 높은 발생률을 보이고 있다. 사건 발생의 증가는 기본적으로 해킹 및 바이러스의 증가에 인한 피해와 보이스 피싱 등 많은 불법광고, 유령 사이트 등으로 인한 피해가 속출하면서 피해가 늘어난 것으로 보인다.[2]

현재, 개인정보의 침해 및 유출을 감소시키기 위해 다양한 알람서비스 및 시스템이 도입되고 있다. 참고[3]에서 제안한 시스템은 수행 시 특정 패턴과 비교하여 비정상이라고 판단되는 수행 발견 시 시스템에서 알람이 발생한다. 이벤트 호출내역으로 정의된 패턴과 알람의 비교로 인해 다양한 공격에 대한 침입 탐지가 가능하다. 참고[4]에서 제안하는 시스템은 같은 로컬 영역의 침입탐지 시스템의 관리 시스템 간에 알람을 주고받는데 로컬 정책과 정보로 침입을 구분하여 정의된 알람상황에 대응을 하거나 시스템 수행을 한다. 이메일을 통한 침입 알람 시스템은 개인 PC에 침입탐지 프로그램을 설치하면, 침입탐지 시스템에 의해 사용자의 네트워크 통신이 모니터링 되고 위험도 평가지수에 따라 침입에 대한 대응이 이루어진다[9]. 침입탐지를 위한 모바일 관리 프로그램은 무선 단말기를 이용하여 침입탐지를 감지하고 신속하고 적절한 대응을 가능하게 한다[10]. 이로써 관리자는 이동환경에서도 침입탐지 시스템을 효율적으로 관리 할 수 있다.

본 논문에서는 개인정보 침해 및 유출 사고를 방지하기 위해 경제협력개발기구(Organization for Economic Cooperation and Development) 개인정보보호 8대원칙을 기반으로 개인정보 유출 대응 시스템을 구축하였다. 참고[3]과 참고[4]의 정보보호에 대한 알람은 정보관리 시스템에서 발생하는 알람으로 비정상적인 행위를 발견하면 해당하는 행위의 진행을 차단하는 것이다. 본 논문에서는 사용자의 행위를 비정상, 정상과 비정상 의심 행위로 구분하고, 비정상 의심 행위에 대해 사용자가 비정상이나 정상으로 판단한다. 이러한 행위 분류는 보안이 강화된 시스템에서 정상 행위가 비정상으로 판단되는 것을 줄이는 효과가 있다. 이로 인해 관리목록이 감소하고, 관련 서비스가

1) 장광영. "유비쿼터스 사회의 개인정보 보호에 관한 연구," 보안뉴스, 2008.06.25

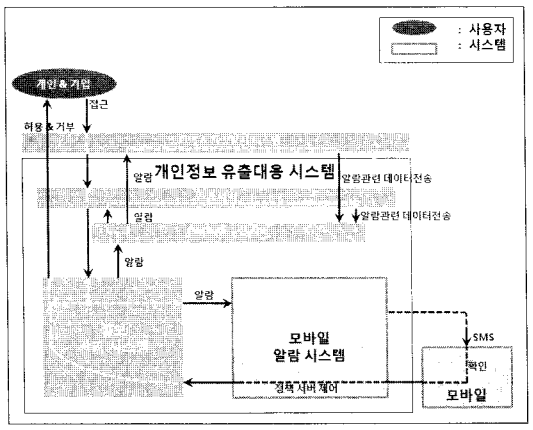
2) KISA(한국정보보호진흥원)-개인정보 침해 신고 현황

효율적으로 제공된다. 또한 참고[9]의 이메일을 이용한 침입 알람 시스템은 비 이동성으로 인하여 사용자가 실시간으로 알람 정보를 확인하는 것이 불가능하다. 본 논문에서는 이동성이 확보되는 모바일 알람메시지로 사용자가 실시간으로 알람상황을 파악할 수 있게 한다. 모바일 대응 프로그램은 참고[10]의 모바일 침입탐지 시스템의 관리 시스템의 단점을 보완하여 사용자가 자신의 개인정보를 관리한다. 즉, 본 논문에서는 제안하는 모바일 알람 메시지 트리를 기반으로 구축된 모바일 알람시스템은 이동성이 지원되는 알람메시지 전송을 가능하게하고 사용자가 정보관리에 참여할 수 있게 한다.

III. 개인정보 유출 대응 시스템

본 논문에서 제안하는 개인정보 유출 대응 시스템은 네트워크상에서 교환되는 모든 개인정보를 효과적이고 체계적으로 보호하기 위한 시스템이다. 정보관리 시스템에는 성명, 주민번호를 기본으로 거주지, 학력, 의료 정보 등의 개인을 식별 할 수 있는 정보가 저장되는데 이 정보는 정보 소유자가 각 정보의 특성과 목적에 따라 정보관리 시스템에 저장 여부와 공개등급을 지정한 것이어야 한다. 또한 정보관리 시스템에 저장되는 정보는 반드시 사용자의 참여를 통한 정확하고 완전한 최신 정보여야 한다.

3.1 개인정보 유출 대응 시스템 구조 및 역할



[그림 1] 개인정보 유출 대응 시스템

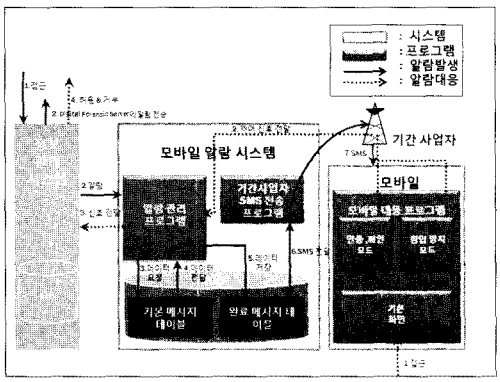
정보 관리 시스템은 한 곳에 모든 개인정보가 보관이 되는 구조이므로, 높은 보안성이 요구된다. 그러므로 주변의 보안서버와 모바일 알람 시스템으로 정보관리 시스템을 보호하고, 신뢰할 수 있는 관리자가 지속적으로 관리를 해야 한다. 본 논문에서 제안하는 개인정보 유출 대응 시스템은 관리자의 적절한 조치 및 주변 보안 시스템의 보안성 강화, 정보 소유자의 실시간 대응으로 인해 정보 오남용을 막고 지속적인 정보 소유자와의 커뮤니케이션으로 정보의 정확성을 보장하여 개인정보의 보안과 정보의 부정확성에 대한 문제점을 개선한다. [그림 1]의 개인정보 유출 대응 시스템의 구조는 방화벽, 침입탐지 시스템, 로그 데이터 수집 서버, 인증서버와 모바일 알람시스템으로 구성되었다.

- 방화벽 - 네트워크 접근 행동에 따라 공격자로 판단되는 접근을 필터링한다.
- 침입탐지 시스템 - 네트워크 패킷의 정보를 분석하여 공격자 여부를 판단하여 접근을 막는다.
- 인증 서버 - 본인 확인과정을 통하여 공격자를 차단한다.
- 모바일 알람시스템 - 정책 위반되는 행위와 인증 과정 및 정보소유자의 동의가 필요한 서비스를 위해 모바일에 알람메시지를 보냄으로써 사용자의 동의나 거부를 받아 정보유출을 막는다.
- 로그데이터 수집서버 - 알람발생 시 방화벽, 침입탐지시스템, 정보관리 시스템에 정보를 요청하여 로그데이터 수집 서버에 정보를 저장한다.
- 관리자 - 정보소유자의 모바일대응에 따르거나 정보가 유출된 상황에 대해 조치를 해야 할 책임과 개인정보관리의 안정성을 확보할 책임을 갖는다.

전체적인 시스템의 구동은 [그림 1]과 같다. 개인 혹은 기업 사용자가 개인정보 활용을 목적으로 한 접근과 통신은 정보관리 시스템을 통해서만 가능하며 반드시 방화벽, 침입탐지 시스템, 인증 서버를 거친 후 가능하다. 또한 사용자의 정보 활용은 정보소유자의 정보공개등급, 정보의 정확성과 개인정보보호 정책에 맞는 행위일 경우에 허가된다. 비정상적인 행위와 통신, 정보의 부족, 부정확, 공개등급 불가 사항일 시 개인정보 활용은 거부되며 사건에 대한 알람이 발생한다. 이 알람은 방화벽, 침입탐지시스템, 인증서버로 전달되어 각 시스템에서 로그데이터 수집 서버로 사건 관련 정보를 전달한다. 사용자가 인지해야하는 알람상황은 모바일 알람시스템으로 전달되는데, 이 알람정보는 무선 통신 중계 기간사업자를 통해 정보소유자의

모바일 알람메시지로 전달된다. 또한 사용자의 알람메시지에 대한 사용자의 개인정보 활용 등에 대한 허용 및 거부의 결정의사가 실시간으로 정보관리 시스템으로 전달된다.

3.2 개인정보 유출 대응을 위한 모바일알람 시스템



〔그림 2〕 알람 전달 및 모바일 알람 대응 신호 전달과정

기존 알람 서비스들은 알람프로그램 설치 후 비정상적인 접근에 대해 실시간으로 팝업창으로 알려주거나 개인정보보안 사이트나 이메일을 통해 정보유출과 자신의 정보 활용에 대해 확인할 수 있다. 그러나 이동환경에서 개인정보 유출에 대한 탐지가 어렵거나 개인정보 관리의 기본적인 상황을 즉시 알기 어렵다. 이러한 이유와 모바일 기기의 보편화로 사용자들은 모바일을 통해 알람메시지를 받길 원하고 있다[2]. 본 논문에서는 알람서비스의 문제점과 사용자들의 요구사항들을 해결하기위해 정보관리시스템에서 알람상황 발생 시 모바일 알람 시스템에서 알람 발생상황의 세부내용을 알려주는 상세 알람메시지를 제공한다.

모바일 알람시스템에서 모바일 알람메시지를 전달하는 구조는 〔그림 2〕와 같다. 알람발생 상황에 해당하는 비정상행위나 개인 정보 관리에 문제가 발생 했을 때, 정보관리 시스템은 알람을 알람메시지의 종류, 사용자의 정보, 알람정보, 발생시간으로 구성하여 모바일 알람시스템으로 전달한다. 알람관리 프로그램은 3.3장에서 언급하는 개인정보 유출 알람 메시지 분류에 따라 메시지 내용이 정의된 데이터베이스(Data Base)의 기본 메시지 테이블에서 메시지의 세부내용을 가져와 정보 관리 시스템에서 전달된 사용자 정보를 포함하여 완료메시지로 테이블에 저장한다. 완료메시지의 데이터형식은 기간사업자 SMS전송 프로그램이 사용자의 모바일로 전달 가능한 데이터 형식을 따른다. 알람메시지는 완 메시지의 저장과 동시에 실시간으로 작동하는 기간사업자 SMS전송 프로그램에 의해 WAP(Wireless Application Protocol) PUSH 송신과정을 거쳐 단방향 SMS(Short Message Service)로 사용자에게 전달된다. 모바일 알람 시스템을 통한 메시지 전달 시 알람 관리 프로그램에서는 시스템에 전달되는 알람 관련 정보를 감시할 수 있으며, 기간사업자 SMS전송 모니터링 프로그램을 통해 알람메시지 전달 과정을 감시 할 수 있으므로 메시지 전달에 안전성이 확보된다.

현재 양방향 서비스의 모바일 알람서비스는 URL(Uniform Resource Locater)메시지의 전달로 상용화되어있다. 이 서비스는 이동환경에서 탐지가능하며 양방향 서비스로 메시지의 내용에 대해 사용자가 의사를 결정할 수 있는 메시지이다. 그러나 이 서비스는 개인정보 유출 대응 시스템의 정보관리 시스템에서 관리하는 개인 정보의 중요성에 비해 인증 및 부인방지를 보장하지 않는 낮은 보안성을 갖고 있으므로 본 논문에서 제안하는 개인정보 보안이 강화된 침입 대응 프로그램에 해당되지 않는다. 이러한 URL메시지의 문제점을 보안하기 위해서 본 논문에서 제안하는 모바일 대응프로그램은 Java 모바일 프로그램의 플랫폼으로 J2ME(Java2 platform Micro Edition)의 CLDC(Connected Limited Device Configuration) / MIDP(Mobile Information Device Profile)[3]에서 제공하는 장비내외 등의 보안검증으로 바이러스와 악성코드로부터 보호되며, 통신은 인증, 암호화, 데이터의 무결성, 모바일 시스템의 안정성이 확립된 WAP 통신[4]을 이용한다. 또한 개인정보 유출대응 시스템에 가입 시 등록한 아이디와 비밀번호와 모바일 인증을 통한 서비스로 타인의 모바일 대응 프로그램 사용을 방지 할 수 있다.

이러한 모바일 대응 프로그램은 개인정보보호 시스템에서 제공하는 모바일서비스를 동의한 사용자를 위한

3) MIDP의 보안모듈은 모바일 어플리케이션을 클래스파일 검증 기를 통해 위험한 어플리케이션의 수행이 이루어지지 않게 하여 모바일시스템의 안정성을 확보한다. CLDC와 MIDP에서 공통으로 제공하는 보안검증은 사전검증, 장비 내 검증이 있다. CLDC에서는 어플리케이션 레벨 보안이 지원되는데 이것은 모래 상자 보안 모델이라고 한다. 그러나 J2ME의 CLDC/MIDP는 데이터 보안을 지원하지 않고, 악성 코드로부터 보호하는 것이 목적이다.

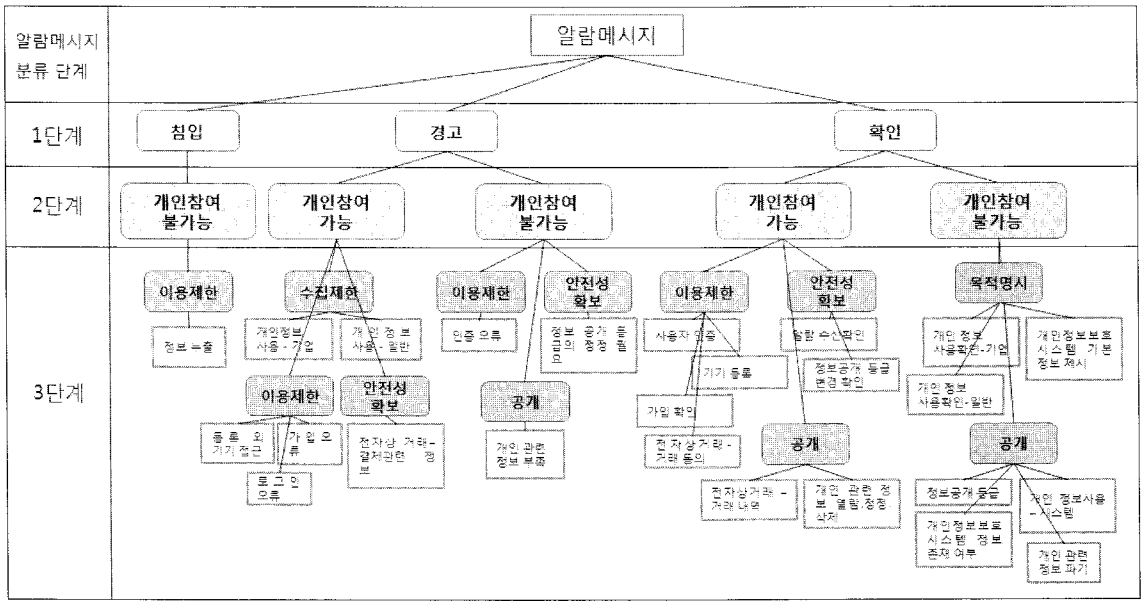
4) WAP통신의 무선G/W는 서비스 공급자 위치에 설치된 G/W여야 보안성을 확보 할 수 있다[2].

것으로 [그림 2]와 같이 메인 화면과 동의 및 침입방지 서브 모드로 구성된다. 3.3장의 알람메시지 구분에서 개인정보 유출이 의심되는 상황 중 모바일을 통해 개인정보의 관리가 가능한 상황은 정상상황임을 인증하여 개인정보 활용에 동의하거나 개인정보 침입을 방지하기 위해 정보 활용을 거부하는 상황으로 분류된다. 모바일 대응 프로그램의 서브모드는 동의 및 확인모드와 침입방지 모드로 구분하여 사용자가 선택한 모드에 따라 정보관리 시스템에 전달되는 사용자의 개인정보 활용에 대한 의견의 타입을 다르게 한다. 이러한 모드의 구분은 정보관리 시스템으로 전달되는 정보 소유자의 의견은 위험의 운선순위에 따라 관리하기 위함이다.

3.3 개인정보 유출 알람 메시지 트리

개인정보 유출 대응 시스템의 정보관리 시스템에서 발생하는 알람은 로그데이터 수집 서버에 사건관련 정보를 수집하기 위해 발생하며 주변 보안 시스템에 알람 정보를 전달하기위해 발생한다. 그러나 모바일 알람 시스템에서 발생하는 알람은 사용자가 직접 실시간으로 본인 정보를 확인하고 관리하는 것을 목적으로 발생한다. 알람메시지는 [그림 3]과 같이 3단계의 트리구조로 나뉜다. 알람메시지는 관련연구에서 언급한 개인정보 침해 유형별 현황과 사례를 분석하고 정의하였으며 [표 1]과 같이 개인정보보호 8대원칙과 연관하여 분류하였다. 또한 사용자와 관리자 관점을 적용하여 어떻게 관리되는 것이 개인정보보호정책에 적법하며 효율적으로 관리 될 수 있는 지를 고려하여 분류하였다. 모든 사건은 개인정보보호원칙 중 몇 가지의 원칙을 위배하여 개인정보가 침해된 상황이므로 사건과 개인정보보호 원칙간의 상호관계가 성립된다. 그러므로 본 시스템은 개인정보보호 원칙을 위배하는 사건 기반의 알람을 발생시키고 알람 관련 정보를 개인정보보호 원칙을 기반으로 제어한다. [그림 3]의 개인정보 유출 알람 메시지 트리 분류와 개인정보보호적용원칙의 상세 내용은 [표 1]과 같다.

1단계는 사용자의 개인정보 요청 접근행위에 따라 '위험도'에 따라 정상(확인)/비정상(침입, 경고)로 분류된다. 위험도에 따라 접근을 분류하는 것은 비정상적인 접근을 막아 '정보 활용을 차단'하기 위해서이며, 비정상으로 의심되는 행위와 정상 행위를 따로 분류하고 다음 단계를 거쳐 정보 활용이 가능한 상황인지 알람이 필요한 상황인지를 결정하기 위해서이다. 여기서 말하는 비정상 행위는 데이터가 유출되어 개인정보보호원칙 중 '데이터의 안전성 확보'의 원칙이 위배된 상황이다. 비정상으로 의심되는 행위는 데이터의 안전성 확보가 확실하지 않은 상황이며, 정상 행위는 데이터의 안전성이 확보된 상황이다. 위험도에 따라 관리의 우선순위는 침입, 경고, 확인의 순서로 정해져 가장 위험한 알람상황을 최우선 순위로 관리된다.



[그림 3] 개인정보 유출 알람 메시지 트리

〔표 1〕 개인정보 유출 알람메시지 트리의 OECD 적용 항목

분류	분류 단계 정의	OECD 적용원칙		상세 구분 및 메시지 타입 정의
1단계	정보 유출 상황을 위험도에 따라 관리	안전성 확보	침입	정보 관리 시스템의 개인정보가 유출
			경고	개인 정보부족, 정보등급이 위험
			확인	정보 소유자에게 동의를 구하거나 관련정보를 통지
2단계	사용자의 의견반영으로 개인정보관리	개인 참여	개인참여 가능	사용자가 True/False형식으로 개인정보 편리에 참여 가능
			개인참여 불가능	알람서비스가 통보 형식
3단계	상세한 메시지 분류로 제한적 환경의 모바일로 개인정보 유출에 대응 가능	수집제한		기업과 개인의 개인정보 사용에 제한
		목적명시		개인정보 사용의 목적을 명시
		이용제한		개인정보 사용을 제한
		안전성 확보		높은 등급의 정보사용의 안전을 확보
		공개		개인정보 관리의 기본정보를 공개

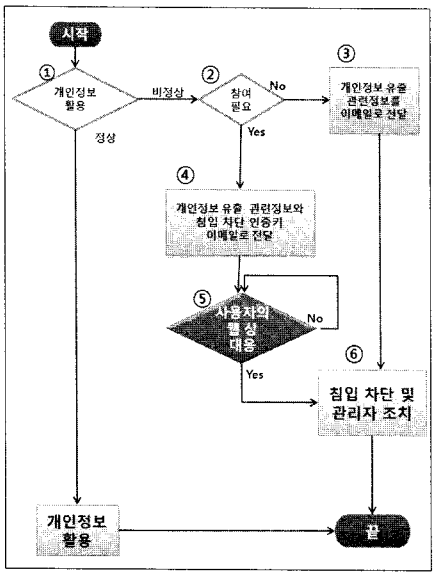
2단계는 개인정보관리를 '정보소유자가 관리 가능' 한지 여부로 분류되었는데, 개인정보에 대한 침입상황은 개인 참여가 불가능하며 즉시 관리자가 조치를 취해야 하는 위험 상황으로 분류된다. 이 단계는 개인정보보호원칙의 단계 중 모바일을 이용한 '개인 참여의 원칙' 적용 여부로 분류된다. 개인 참여 불가능한 상황은 개인정보관리의 관련정보를 정확히 표현할 수 있지만, 대응이 필요 없고 사용자가 동의한 정보제공 상황에 대해 통지하는 경우로 1단계의 경고노드의 개인 참여 불가능 노드에 해당한다. 이 알람메시지는 다른 기기를 이용하여 개인정보유출에 대한 대응을 촉구한다. 다음은 개인정보관리의 관련정보를 모바일 환경에서 모두 표현할 수 없는 경우이다. 이 경우는 1단계의 확인노드에 해당하는 개인 참여 불가능 노드로 사용자의 알권리를 보장해 주기위해 개인정보와 관련된 정보를 간단히 하여 모바일로 공개하는 경우이다. 개인 참여 가능노드는 모바일 환경에서 개인정보관리의 알람 정보를 정확히 표현할 수 있고 정보관리에 대해 True/False의 사용자의 의견을 수렴할 수 있는 경우이다. 이 상황은 간편한 모바일 대응이 가능한 상황도 포함되지만, 모바일 결제나 사용자의 개인정보가 유출될 수 있는 위험한 상황이 필수로 포함한다. 그 이유는 위협적인 정보침해 및 유출, 정보 오남용은 정보 손실 가치가 크므로 실시간으로 방지해야하기 때문이다. 확인 노드의 개인 참여 가능 노드는 개인정보가 유출된 상황은 아니지만 개인정보 유출의 시발점이 될 수 있기 때문에 사용자 동의가 필요하다. 경고 노드의 개인 참여 가능 노드는 사용자에게 개인정보 '사용에 대해 허가'를 받거나 사용자의 실수로 발생한 경고상황을 사용자가 확인함으로서 잘못 판단된 비정상으로 의심되는 상황을 '비정상상황에서 제외'시키기 위해 지원된다. 이로 인해 정보관리시스템에서 높은 보안성을 위해 비정상으로 의심되는 행위를 비정상으로 분류할 때 생기는 정상 접근이 비정상으로 포함될 경우에 발생할 수 있는 원활하지 못한 서비스 제공으로 인한 회사의 금전적 손실을 줄일 수 있다. 게다가 원활한 서비스 제공을 위해 의심되는 비정상상황을 정상상황으로 분류할 때 발생하는 정보관리시스템의 보안성 감소가 해결될 수 있다. 그러므로 개인정보관리에 대한 사용자 참여의견 반영은 개인정보를 활용하려는 접근이 비정상 상황으로 분류될 때 잃는 편의성 감소와 정상상황으로 분류 때는 잃는 보안성 감소의 트레이드오프(trade off)를 줄일 수 있게 된다.

3단계는 정보표현이 제한된 모바일환경으로 '세부적인 정보 제공'을 하기위한 분류 단계이다. 상세적인 정보제공으로 사용자는 PC등의 다른 기기를 이용하지 않아도 높은 보안성을 요구하는 정보 외의 개인정보관리에 대한 정보를 실시간으로 상세하게 제공받을 수 있다. 관련연구의 개인정보 침해유형의 실제 사건을 분석한 결과, 내부 공격자나 모든 권한을 획득한 공격자에 의한 사건을 제외하고 침입자에 의한 사건은 관리자가 보장해야하는 정보정확성과 책임의 원칙을 제외한 나머지 6개의 원칙을 위배한 것이 나타났다. 이 분석에 따르면 정보정확성의 원칙은 개인정보를 관리하는 시스템의 정보저장 데이터베이스에서 지켜야 할 사항으로 모든 메시지에 해당되는 사항이므로 메시

지 분류에 해당되지 않으며, 책임의 원칙은 회사나 관리자가 지켜야 할 사항으로 사용자가 전달받는 알람메시지의 내용에 해당되지 않는다. 나머지 6개의 원칙 중 모든 사건이 정보보호 원칙 중 중복하여 위배되는 안전성확보와 개인 참여 원칙을 제외한 '수집제한, 목적명시, 이용제한, 공개의 원칙'이 각 사건별로 대입된다. 그러나 개인정보 중 보안등급이 높은 정보에 해당하는 전자 결제 정보와 개인정보 관리 등급은 다시 한 번 '안전성확보의 원칙'을 대입하였는데, 그 이유는 정보 중 가치가 높은 전자상거래정보 및 사용자 인증에 대한 정보를 신속하게 제공하고 정보 위협 시 다른 상황과 분리하여 관리하기 위해서이다.

위와 같은 3단계 알람메시지 분류로 생성되는 알람메시지는 개인정보 관리가 개인정보보호법과 원칙을 따르는 것을 증명하고 사용자의 알권리를 만족시킨다. 또한, 사용자가 개입된 정보관리로 개인정보 유출에 효과적으로 대응하고 관리하여 개인정보 관리에 대한 적법성과 효율성이 높아지게 된다.

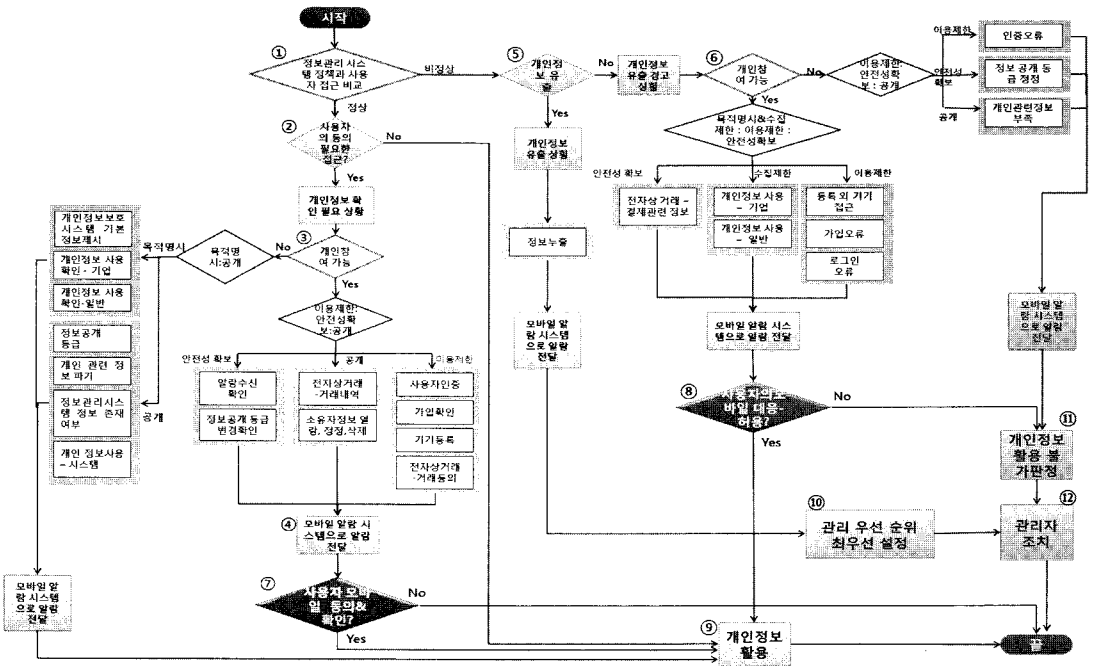
3.4 모바일 알람 시스템 알고리즘



〔그림 4〕 기존 알람 시스템

기존 알람 시스템은 〔그림 4〕와 같이 알람메시지를 전달하고 침입에 대응한다[9]. ①개인정보에 대한 접근이 정상일 경우는 개인정보를 정상적으로 활용한다. 그러나 개인정보에 대한 접근이 비정상일 경우 중 ②개인의 참여가 필요하지 않는 경우는 ③이메일로 개인정보 유출에 대한 관련정보를 통지한다. 이때 이메일은 알람과 관련된 내용을 확인 가능하다. 비정상적인 개인정보 활용 중 ②개인의 참여가 요구되는 상황은 ④사용자가 개인정보 유출 관련정보와 침입 차단 인증키를 메일로 전달받게 된다. ⑤사용자는 침입 차단 인증키를 이용하여 웹을 통해 침입에 대응할 수 있다. 그러나 실시간 대응이 어렵기 때문에 대응이 없을 경우 더 이상의 관리가 진행되지 않으므로 ⑥관리자의 조치가 유보될 수 있다. 기존 시스템은 정확한 유출상황 내용을 사용자에게 통지하지만, 이동성을 지원하지 않는 알람(메일)으로 웹에서 확인해야하기 때문에 불편하다. 즉, 사용자는 통지내용을 실시간으로 확인하기 어렵기 때문에 개인정보 관리에 사용자의 의견을 적절히 반영하기 어려우며 사용자의 대응에 따라 비효율적인 관리 대기시간이 생긴다. 게다가 각각의 정보관리에 대한 분류가 없으므로 관리자는 시스템에서 지정한 알람의 위험도에만 의존하여 정보를 일괄적으로 관리해야 한다.

본 논문에서는 기존 알람시스템의 비효율성을 개선하고 사용자의 높아진 개인정보보호의 관심에 부합하기 위해 시간과 장소의 제약이 없이 사용자가 직접 개인정보관리에 참여 가능한 시스템을 설계하고 구현하였다. 알람시스템은 알람메시지를 구성하는 단계와 동일하게 구성된다. 〔그림 5〕와 같이 ①사용자의 접근을 정보관리 시스템의 정책과 비교하여 정상여부를 판단하고 ⑤정보가 유출된 비정상 상황이면 침입알람이 발생한다. ⑤정보가 유출되지 않았지만, 정보유출이 의심되는 상황은 경고 알람이 발생한다. 다음 단계로 ⑥경고형의 모바일 알람 메시지는 사용자의 확인이 필요한 상황과 참여가 필요한 상황으로 나뉜다. 모바일 참여가 가능한 알람 발생 시 사용자가 거부의견을 전달하면 의심되는 상황을 막았으므로 시스템의 보안성이 높아지며, 동의의견을 전달하면 서비스 제공이 정상적으로 이루어지므로 편의성을 해치지 않는다. ②정보관리 시스템에서 사용자의 접근이 정상으로 판단되고 사용자의 동의가 필요 접근이라면 확인&동의 알람이 발생하는데 이 알람은 사용자에게 정보를 제공해야하는 법적인 의무로 발생하는 알람이다. 다음 단계는 ③모바일 참여가능여부에 따라 나뉘는데, 참여 가능한 알람은 사용자 인증을 통해 보안성을 높이기 위함이다. ④정보 관리 시스템이 알람을 모바일 알람시스템에 전달하면 무선데이터를 전송하는 기간사업자를 통해 사용자에게 모바일메시지로 전달된다. 참여 가능한 알람메시지가 통보되면 사용자는 모바일 대응 프로그램을

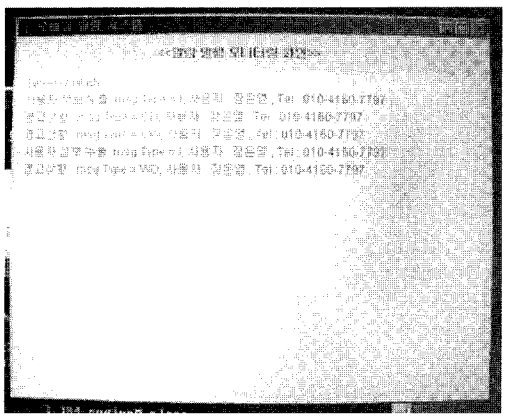


〔그림 5〕 알람 결정 및 모바일 대응으로 인한 정보 관리 결정

통해 동의 및 확인 의견을 전달할 수 있다. ⑦⑧사용자가 참여 가능한 메시지 수신 시 거부의견을 전달할 경우와 동의 및 확인 의견이 3분 안에 전달하지 않을 경우, 사용자의 의견은 거부로 판단된다. ②사용자의 접근이 정상접근으로 판단된 ③사용자 동의 필요하지 않은 접근과 사용자의 동의는 필요하지만 사용자의 참여 불가능 한 메시지 전달 상황, 그리고 ⑦사용자의 참여가 가능한 상황 모바일을 통해 허용의견을 전달 될 경우 ⑨정보의 활용, 확인, 수정사항이 허용된다. ⑤정보가 유출되어 알람메시지가 전송된 상황과 정보 유출이 의심되는 경고 상황에서 사용자의 참여 가능한 메시지가 전달되었지만 ⑧사용자의 동의 및 확인 의견이 없는 경우와 ⑥경고 상황에 참여 불가능한 메시지가 전달되었을 경우 ⑪개인정보 활용은 불가능 하다. 이러한 알람발생 위험 상황이 사용자의 정보가 유출된 ⑩과 같이 긴급 상황으로 정보를 우선으로 관리하고 정보가 ⑫유출된 상황을 최우선으로 관리하여 알람발생을 위험상황에 따라 우선순위로 체계적인 관리를 한다.

본 시스템은 사용자의 참여를 통해 의견을 수렴하여 개인정보를 활용하고 알람을 우선순위에 따라 관리를 한다. 알람메시지 트리는 사건으로 인한 개인정보 침해 및 유출을 기반으로 정의되었기 때문에, 시스템에서 발생하는 알람메시지는 사건을 방지하기위해 시스템에서 발생할 수 있는 모든 상황을 포함해야한다. 그러므로 〔그림 5〕의 알람결정 및 모바일 대응으로 인한 정보관리결정은 〔그림 3〕의 메시지가 생성되는 알람메시지 트리의 결정단계와 같아야 한다.

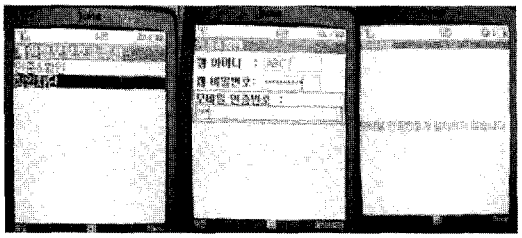
IV. 시스템 구현



〔그림 6〕 모바일 알람관리 프로그램

모바일 알람시스템에는 데이터베이스와 〔그림 6〕의 모바일 알람관리 프로그램과 기간사업자에서 제공한

SMS전달 프로그램이 실시간으로 작동되고 있다. 정보관리 시스템에서 모바일 알람시스템으로 알람메시지를 전달하면 알람관리 프로그램에 의해 메시지의 내용과 메시지 전달에 필요한 정보 사항, 사용자의 정보가 완료메시지로 저장된다. 실시간 작동하고 있는 SMS전송프로그램은 완료메시지가 저장된 후 즉시 사용자에게 모바일 알람메시지를 전달한다. 관리자는 모바일 알람관리 프로그램을 통해 알람메시지 전달 정보를 모니터링 할 수 있다.



〔그림 7〕 모바일 대응 프로그램

〔그림 7〕의 모바일 대응프로그램을 이용해 사용자는 개인정보 유출 위험상황과 동의가 요구되는 상황에 의견을 전달 할 수 있다. 참여 가능한 알람 메시지일 경우, 메시지의 세부내용에 따라 서브 모드에 접근하여 사용자의 동의 및 확인 의견과 거부 의견 전달이 가능한데, 정보 관리 시스템의 아이디와 비밀번호, 인증서버에서 발급한 모바일 인증번호를 입력하여 인증번호 일치 시 의견을 전달할 수 있다. 이 의견은 모바일 알람 시스템의 모바일 알람관리 프로그램을 통해 전달되어 정보관리 시스템의 알람 상황에 대응할 수 있다. 침입차단의 거부의견은 정보 활용을 제한하며, 정보관리 시스템의 의견수용 제한 시간 내에 동의 및 확인 의견을 전달하지 않을 경우, 개인 정보 활용은 거부된다. 정보 유출 상황 시 사용자의 모바일대응 프로그램을 통한 의사전달은 사용자가 직접 정보관리 시스템을 우선적인 관리를 가능하게 하며, 그 의사에 따른 관리자의 관리가 이루어지게 된다.

V. 결 론

본 논문에서 제안한 시스템은 기간사업자의 무선통신 송신방식을 따르므로 보안성과 신뢰성이 확보된 무선 WAP 게이트웨이를 보장할 수 없다. 즉, 무선 네트워크 장치의 보안에 위협을 주는 신호방해 공작, 배터리 소진공격, Dos(Denial Of Service)공격 탐지를 보장 할 수 없다. 하지만 무선네트워크 장치의 단점 중 장치분실 및 도난, 비정상적인 접근은 모바일 인증과 인증 서버를 통한 사용자인증으로 보완 가능하며, IP Spoofing, 악성코드는 자바프로그램과 WAP 통신 보안모듈로 대응 가능하다. 신원·위치노출의 익명은 WAP 통신의 WTLS의 암호화 기술로 보장하였다. 그러므로 본 논문에서 제안한 개인정보유출 대응 시스템은 기존 시스템의 단점을 보안하여 1차로 개인정보보호 시스템의 보안성이 강화된 개인정보 관리를 하고, 2차로는 알람메시지 통지, 3차로는 모바일 대응 프로그램을 이용한 정보소유자의 개인 참여를 가능하게 하며 4차로 관리자의 로그데이터 수집 시 저장된 알람발생사건 분석과 조치, 개인정보보호시스템의 전반적 관리로 개인정보의 보안을 철저하게 하며 효과적인 관리를 보장 한다. 그러므로 본 논문의 모바일 알람시스템은 보편화된 모바일 무선 네트워크 환경에 맞는 알람 메시지 통보와 모바일 대응프로그램으로 개인정보를 사용자와 신뢰 할 수 있는 관리자가 협력하여 개인정보를 관리하는 환경을 보장하는 보안성이 강화된 정보관리 시스템이라고 할 수 있다.

향후에는 본 논문에서 언급한 알람시스템의 정의를 기반으로 모바일 알람 시스템을 모델링하여 정형화하고 시뮬레이션을 통해 시스템의 효율성과 보안성을 증명할 것이다. 또한, 개인정보보호 정책시스템을 분석하여 알람시스템과 정보관리 시스템의 호환성을 고려하여 독립적인 알람시스템 구성을 모색하고 시스템 간 주고받는 신호를 정의할 것이다.

참 고 문 헌

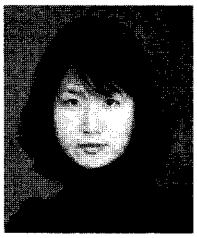
〔1〕 J. Burkhadrdt, T. Schaeck, S. Happer, K. Rindtorff, and T. Schaeck, Pervasive computing: Technology and Architecture of mobile internet applications, Addison-Wesley Longman Publishing Co, Jan. 2001.

〔2〕 B. LEE, Users' Perspective on Regulation to Protect Privacy on the Web, The International Information and Library Review, pp. 379-402, Sep. 2000.

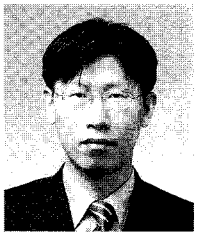
〔3〕 R. Sekar and P. Uppuluri, "Synthesizing Fast Intrusion Prevention/Detection Systems from High-Level Specifications," Proceedings of the 3rd USENIX

Windows NT Symposium, pp. 12-15, July 1999.
[4] L.H. Overby, "Selectively responding to intrusions by computers evaluating," Patent Application Publication, Mar. 2005.
[5] 장혜진, "자바 무선 보안," 정보과학회지, 20(4), pp. 66-72, 2002년 4월.
[6] 김형교, 강민구, 강성철, 정준현, "휴대단말 및 개인정보의 정보보호 동향," 인터넷정보학회지, 2(3), pp. 73-93, 2001년 9월.
[7] 강성철, "개인정보보호 실태와 정책방향," 인터넷정보학회지, 1(2), pp. 54-58, 2000년 12월.
[8] 김행욱, 정숙희, 강홍식, "WAP기반의 무선 단말기를 이용한 효과적인 IDS 관리/제어 시스템 구현," 한국정보보호과학회 2002 가을 학술발표논문집, 29(2), pp. 643-645, 2002년 10월.
[9] 장재혁, 정현철, 최용락, "E-Mail을 이용한 실시간 침입대응시스템," 한국인터넷정보학회 2001 추계학술발표대회 논문집, 2(2), pp. 281-285, 2001년 11월.
[10] 김기수, "유비쿼터스 네트워크에서 안전한 개인정보보호를 위한 프라이버시 보호 방안," 한국정보과학회 2007 가을 학술발표 논문집, 34(2), pp. 132-135, 2007년 10월.
[11] 송유진, "유비쿼터스 환경에서 개인정보보호의 기술동향," 정보보호학회지, 16(3), pp. 75-86, 2006년 6월.

〈著者紹介〉



장 은 영 (Eun-young Jang) 학생회원
2008년: 서울여자대학교 정보통신공학부 멀티미디어통신공학과(공학사)
2009년~현재: 서울여자대학교 일반대학원 컴퓨터학과 석박사통합과정
〈관심분야〉 정보보호, 네트워크 보안, 취약점 분석 및 모델링



김 형 종 (Hyung Jong Kim) 종신회원
1996년: 성균관대학교 정보 공학과(공학사)
1998년: 성균관대학교 정보 공학과(공학석사)
2001년: 성균관대학교 전기전자 및 컴퓨터공학과(공학박사)
2001년~2007년: 한국정보보호진흥원 수석연구원
2004년~2006년: Carnegie Mellon University, USA Visiting Researcher
2007년~현재: 서울여자대학교 컴퓨터학부 조교수
〈관심분야〉 취약점 분석 및 모델링, 이산사건 시뮬레이션 방법론, 침입감내기술

황 준 (Jun Hwang) 정회원
1985년: 중앙대학교 컴퓨터공학과 졸업(학사)
1987년: 중앙대학교 대학원 컴퓨터공학과 졸업(석사)
1991년: 중앙대학교 대학원 컴퓨터공학과 졸업(박사)
1992년~현재: 서울여자대학교 정보미디어대학 미디어학부 교수
〈관심분야〉 IPTV, Convergence Computing, Digital Broadcasting, 개인정보보호