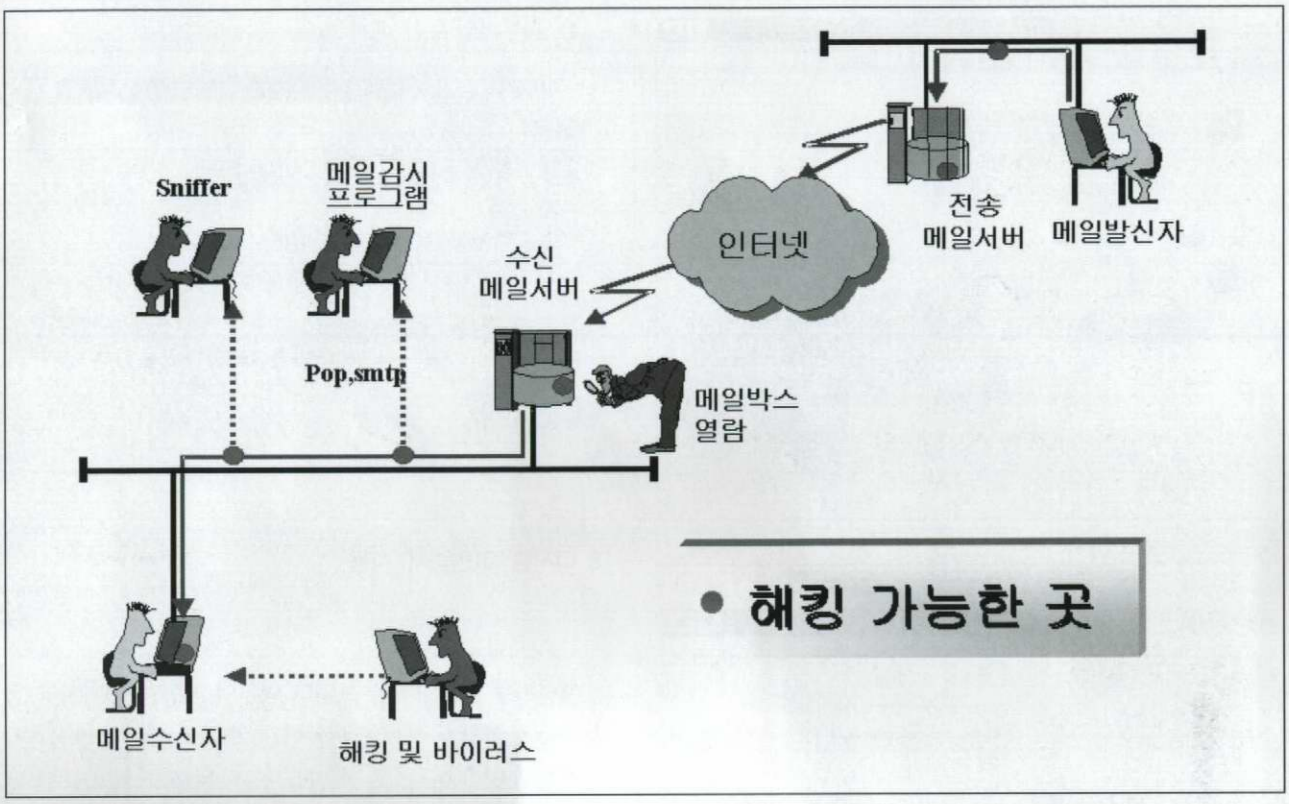
전자우편의 동작원리와 보안 및 스팸메일의 불법성

개인정보 불법 수집 및 판매 등 방지책 필요

김연수 연구원
한국정보보호진흥원
개인정보분쟁조정위원회

이 장에서는 E-mail의 원리와 다양한 기능 그리고 보안과의 관계를 알아보고자 한다. 우리가 가장 즐겨하면서도 정작 보안부분은 취약한 것이 바로 E-mail이다. 이메일의 원리에 대해서 살펴보고 취약한 보안부분을 점검해보는 것도 자신의 개인정보와 바이러스 및 각종 불법 메일을 방지하는 한 방법일 수 있다. 또한 다양한 유형의 바이러스형 메일의 특징을 알아보고 감염방지와 보안 등에 대한 유익한 정보가 되었으면 한다.

-편집자 주-



(지난호에 이어서)

제 4 절 이메일 해킹과 보안

I 이메일 해킹 경로

메일 발신자가 메일을 전송하면 '전송 메일 서버'로 메일이 보내지고 인터넷(네트워크)을 통하여 상대방의 '수신 메일 서버'에 도착해 모니터로 나타나게 되는데 일련의 과정에서 해커가 침입할 수 있는 방법은 각 단계 및 전송 과정의 거의 모든 곳에서 가능하다.

II 메일 보안

1. 술적 관리적 이메일 보안체계 수립

1) 내 외부 전송 이메일 통제

용량이 큰 파일에는 중요정보가 저장되었을 가능성이 크기 때문에 원천적으로 서버에서 전송제한을 하게 되는데 내부 소속원간 또는 내부 네트워크에서 외부로 전송되는 이메일의 용량과 내용을 제한하는 방법으로 보통 이메일의 용량이 5MB - 100MB 정도의 일정한 한도를 넘는 경우 전송을 금지하거나 상급자에게 전송되어 상급자가 기밀성을 판단하게 한다.

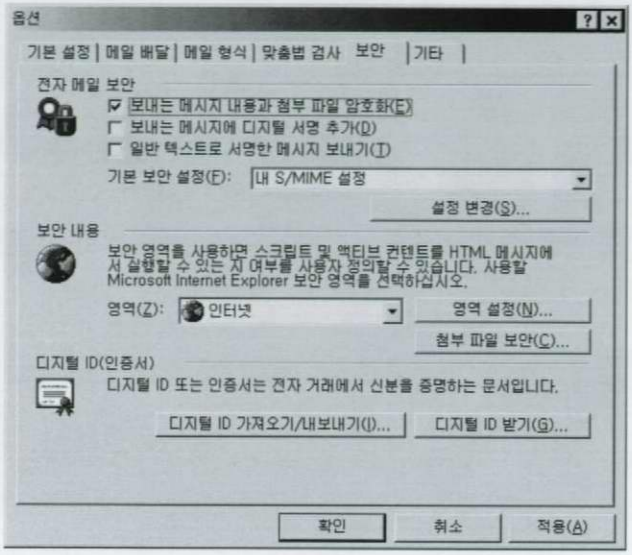
2) 옵션에 따른 이메일 열람 제한

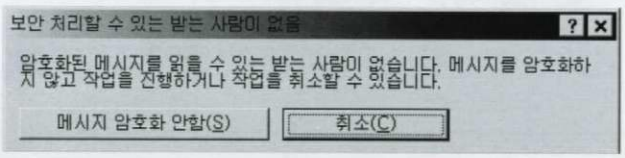
전수신되는 이메일의 '제목'란에 특정 용어를 사용하여 분류를 설정할 수 있다. 이렇게 분류된 이메일은 지정된 수신자만 볼 수 있게 하거나 일정 시간이 경과하면 자동적으로파기되게 할 수도 있고 회신이나 인쇄 등을 제한할 수도 있다.

2. 아웃룩 익스프레스의 보안 설정

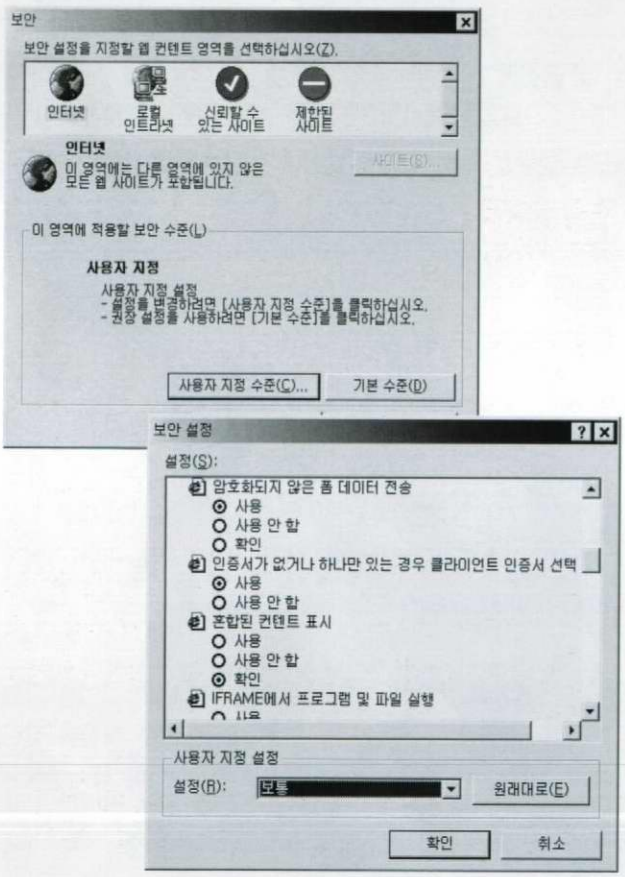
1) 아웃룩에서 보내는 메일의 첨부파일을 암호화하여 보내는 방법을 소개하기로 한다. 아웃룩2000의 '도구—옵션'의 '보안'을 클릭한다. 나타난 창에서 '보내는 메시지 내용과 첨부 파일 암호화'에 체크한다. 이때 기본적으로 내 시스템에는 디지털 ID(인증서)가 있어야 한다.

2) 이메일을 작성하고 '보내기' 버튼을 클릭하면 상대방이 디지털 서명(인증서)를 가지고 있지 않은 경우 다음과 같은 메시지가 나타난다. 이때에는 '취소'를 누르면 상대방에게 이메일을 전송할 수 없고,' 메시지 암호화 안함'을 선택하면 암호화하지 않은 상태로 전송된다.

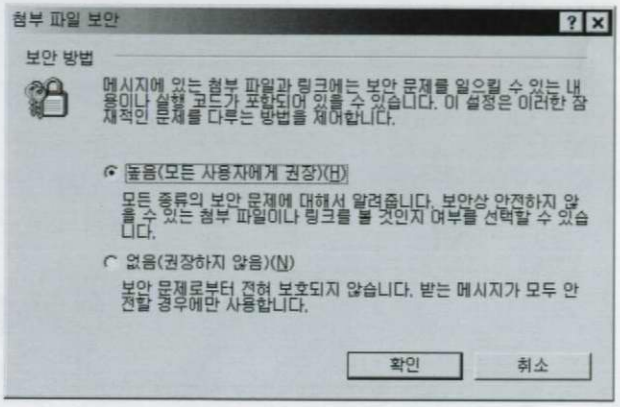




3) 다음의 예제는 보안수준을 높이는 것으로 '사용자 지정 수준' 에서 '보안설정' 의 각 옵션을 지정할 수 있다.



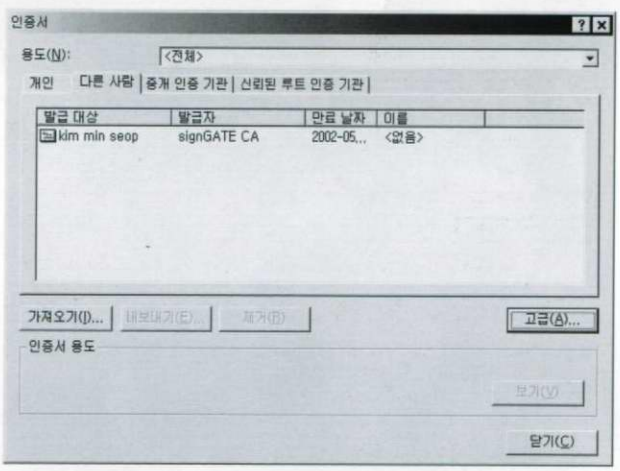
4) '첨부파일 보안' 에서 '높음' 을 선택한다.



3. 디지털 ID(인증서) 사용

1) 디지털 ID 기능

메시지를 암호화하여 보내면 임의의 사람이 메시지와 첨부파일을 읽고자 하여도 해독이 불가하기 때문에 발신자가 지정한 사람이 아니고는 메일을 읽을 수 없다. 디지털 ID는 인터넷에서 이용자의 신원을 확인할 수 있는 수단이다. 즉 디지털 ID 발급업체를 통하여 메일 발신자의 신원을 입증받고 신뢰할 수 있게 된다. 그러나 메시지에 보안을 설정하기 위해서는 디지털 ID을 사용해야 하고 암호화된 이메일 메시지를 보내려면 발신자의 연락처 목록에 수신자의 디지털 ID 복사본이 있어야 합니다.



2) 디지털 ID 구성 : 공개키, 디지털 서명, 개인키

디지털 ID는 공개키, 디지털 서명, 개인키로 구성되는데 메일을 작성하여 메시지에 디지털 서명을 하면 공개키와 디지털 서명이 추가되고 이러한 디지털 서명과 공개키를 조합하여 인증서라는 것이 성립된다. 메일을 받는 사람은 키를

사용해 암호를 해독하여 메시지를 읽을 수 있다. 디지털 서명은 타인에 의한 메시지 변조를 방지할 수 있고 수신자는 발신자가 누구인지 그 신분을 명확히 확인할 수 있게 된다.

일부 메일 서버의 경우에 네트워크 관리자가 디지털 ID를 발급할 수도 있다. 디지털 ID의 일부분은 바꿀 수 없는 개인키이며 보통 이용자 컴퓨터에 저장되어 있다. 이 개인키를 다른 컴퓨터로 내보내거나 가져오는 방법으로 컴퓨터 사이에서 보안 이메일의 보안 설정을 할 수 있다.

3) 디지털 ID 인증서 발급업체

디지털 ID는 독립적인 인증기관에서 발급하기 때문에 인증기관에 디지털 ID를 신청하고 자신의 신분을 증명하여 디지털 ID를 발급받게 된다. 아웃룩(Microsoft Outlook)에는 보안 이메일 메시지를 주고 받을 수 있도록 하고 사용 권한이 없는 사용자로부터 정보를 보호하는 기능이 있다. 디지털 ID를 발급받을 수 있는 보증서 발급업체는 다음과 같다.(http://officeupdate.microsoft.com/korea/outlook/outlook2000/highencrypt/certpage.htm?&helplcid=1042)

- Verisign Inc

(https://digitalid.verisign.com/cgi-bin/OEenroll.exe?name=&email=)

Verising은 마이크로소프트사가 선호하는 디지털 ID 공급업체로서 아웃룩 사용자들은 시험 디지털 ID를 무료로 받을 수 있다. VeriSign 서비스에는 SSL용 IIS(Internet Information Server - 인터넷 정보 서버) 및 Internet Explorer 클라이언트 보증서, Outlook Express와 Outlook 98, Outlook 2000용 S/MIME 보증서, 은행용 128 비트 암호화를 위한 SGC 보증서, Active-X 응용 프로그램에 전자 서명을 위한 인증 코드 보증서와 시간 스탬프 서비스 등이 있다.

- Golbalsign

(http://www.globalsign.net/digital_certificate/index.cfm)

Golbalsign은 CA(Certification Authority)로서 개인키를 발급하여 디지털 보증서에 서명하고 관리한다.

- British Telecommunications

(http://www.ignite.com/application-services/products/verisign/)

British Telecommunications는 웹 사이트와 인트라넷을 보유한 회사의 보안 서버 보증서와 Outlook Express와 Outlook 98용 개인 디지털 보증서를 제공한다. 이 보증서는 VeriSign Global Trust Network에서 발급되어 인트라넷이나 엑스트라넷, 인터넷 응용 프로그램을 통해 글로벌로 상호 이용할 수 있다.

- Thawte Certification

(http://www.thawte.com/certs/personal/contents.html)

Thawte Certification은 이메일 서명과 암호화를 위한 무료 개인 보증서를 제공한다. Thawte는 글로벌 CA로서 이미 전 세계 인터넷 전자 상거래 서버의 30%를 공인하였다고 한다.

- 라이코스 코리아

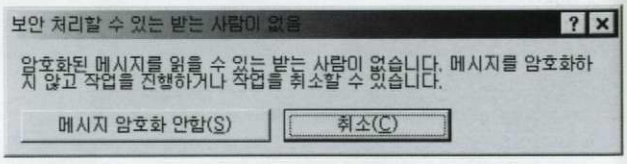
(http://www.lycos.co.kr)

라이코스 코리아가 제공하는 인증서는 회원에 한하여 수신자의 이메일 주소가 xxx@lycos.co.kr인 경우에 보안 메일을 전송할 수 있다.

4) 디지털 ID 사용 원리

갑이 을에게 중요한 이메일을 보내기 위하여 디지털 서명으로 전송하는 과정을 설명하기로 한다.

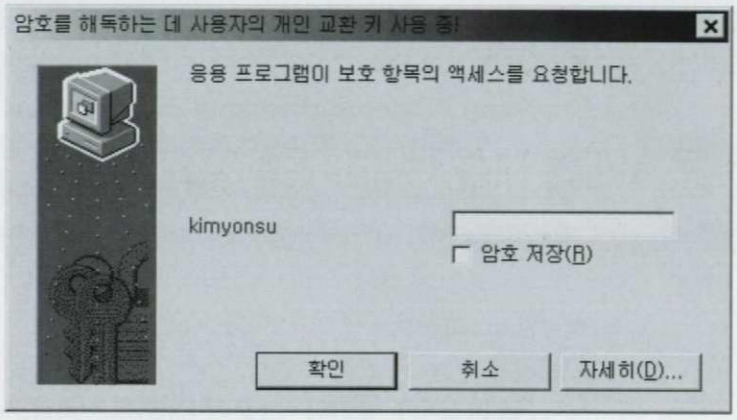
- 작성된 메일을 암호화하여 보내려면 연락처 목록이나 주소록에 을(수신자)의 디지털 ID 복사본이 저장되어 있어야 하므로 을에게 디지털 서명된 메일(디지털 ID를 첨부한 이메일)을 보내달라고 요청한다. 만일 을에게 인증서가 없거나 보내오지 않으면 수신자인 을의 인증서를 갑의 주소록 목록에서 등록할 수 없어 암호화하여 메일을 보낼 수 없게 된다(암호화되지 않은 상태로 보낼 수는 있다).

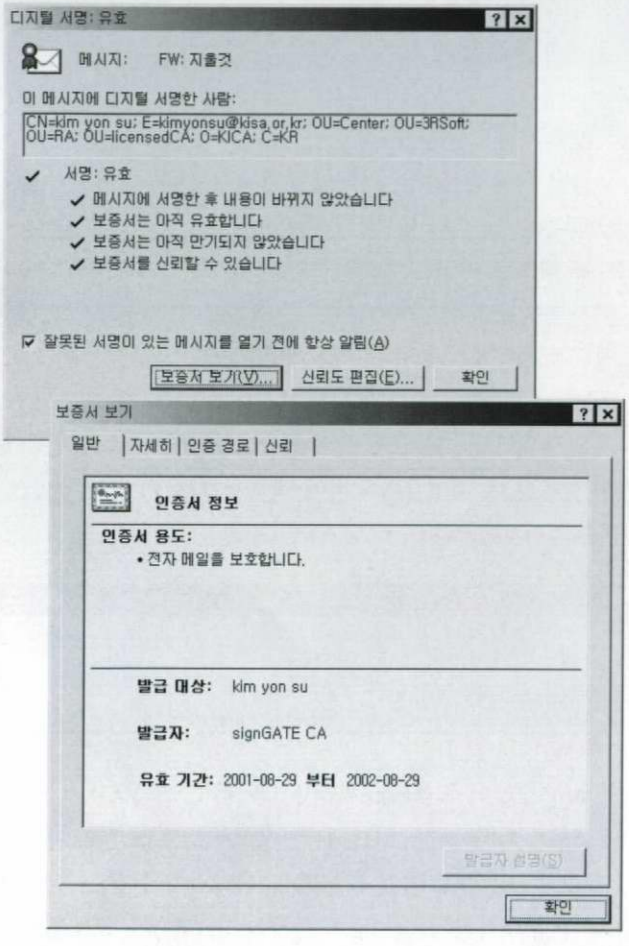


- 을로부터 메일이 도착하면 디지털 ID가 첨부된 메시지를 열고, '보낸 사람' 필드에서 이름을 마우스 오른쪽 단추로 클릭한 다음 바로 가기 메뉴에서 '연락처에 추가'를 클릭한다. 연락처 목록에 그 사람의 항목이 있으면 '이 주소 겹쳐쓰기'를 클릭한다.

이제 받는 사람의 연락처 항목에 디지털 ID가 저장되어 있으므로 암호화된 전자 메일 메시지를 그 사람에게 보낼 수 있다. 연락처에 대한 인증서를 보려면 메시지 수신자의 이름을 두 번 클릭한 다음 인증서 탭을 클릭한다.

- 을은 갑의 메일을 수신하고 (자신의 인증 암호를 기입한 후- 옵션에서 설정한 경우에 한함) 읽으면 된다. 미리보기 창에서는 갑의 메일의 메시지 내용이 나타나지 않으므로 메시지를 활성화 해야 한다.





III 기타

첨부파일에 암호를 설정하여 보내는 방법이 있다. 예컨대 한글 문서에 문서암호를 설정해서 보내면 타인이 중간에 가로챌지라도 문서의 암호를 해독하지 않는 한 문서내용을 볼 수 없게 된다.

디지털서명(인증서)이 대중화되어 있지 않기 때문에 수신자가 디지털서명을 보유하지 않은 상태에서 전송자만 디지털서명으로 암호화해서 보낼 수가 없기 때문에 첨부문서 암호화 방식은 유용하고 편리한 방법이다.

그 외에도 대다수가 첨부문서로 컴퓨터바이러스 등이 유포되고 해킹툴을 통하여 정보유출을 시도하는 경우가 많기 때문에 V3, 바이로봇 등의 백신 프로그램을 실시간으로 작동시켜 수신되는 첨부파일을 검색케 하는 것도 좋은 방법이다.

(다음호에 계속)