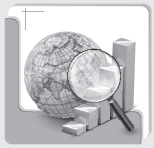
개인정보 분쟁조정 사례



1 개인정보분쟁조정위원회, 해킹으로 인하여 개인정보를 유출당한 정보통신서비스제공자에 대하여 손해배상 결정(2014. 11. 10.)

개요

■ 개인정보분쟁조정위원회는「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제28조 제1항을 위반하여 개인정보의 분실 · 도난 · 누출 · 변조 또는 훼손을 방지하기 위하여 규정된 기술적 · 관리적 조치를 다하지 아니한 정보통신서비스제공자에 대하여 정신적 피해에 관한 손해배상 결정을 하였다.

사실관계

■ 피신청인은 2011. 3. 성명불상의 해커에 의하여 전산시스템에 저장중이던 신청인의 개인정보를 유출당하였고, 피신청인은 2014. 7. 신청인을 포함한 고객 개인정보가 유출되었다는 사실을 인지하고, 신청인에게 이를 통지하였다.

– 이에 신청인은 해킹으로 인하여 개인정보가 유출된 피신청인에 대하여 정신적 손해배상을 요구하는 분쟁조정을 신청하였다.

조정결정 내용

■ 피신청인의 기술적 · 관리적 조치 의무

–「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법') 제28조 제1항 및 같은 법 시행령 제15조 제1항 내지 제5항은 정보통신서비스 제공자등이 개인정보를 취급할

때에는 개인정보의 분실 · 도난 · 누출 · 변조 또는 훼손을 방지하기 위하여 적합한 기술적 · 관리적 조치를 해야 함을 규정하고 있으며, 제6항은 방송통신위원회로 하여금 개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하도록 규정하고 있다.이에 따른 「舊, 개인정보의 기술적 · 관리적 보호조치 기준」(2012. 8. 23. 방송통신위원회 고시 제2012-50호로 개정되기 전의 것) 제4조 제8항은 정보통신서비스 제공자등은 취급중인 개인정보가 인터넷 홈페이지 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터에 조치를 취하여야 함을 규정하고 있고, 같은 고시 제7조는 정보통신서비스 제공자등은 운영체제 제작업체에서 업데이트 공지가 있는 경우에는 응용프로그램과 정합성을 고려하여 최신 소프트웨어로 갱신 · 점검해야 함을 규정하고 있어, 피신청인은 정보통신서비스제공자로서 위 법령 및 고시가 규정하는 기술적 · 관리적 보호조치를 준수해야 할 의무가 있다고 할 것이다.

■ 피신청인의 법위반 여부 판단

– 2011. 3. 발생된 피신청인의 고객 개인정보유출사고와 관련하여, 이 사건 사고는 당시 피신청인이 운영중이던 서버 운영체제인 Windows 2003의 IIS(Internet Information Service) 버전 6.0이 가지고 있던 고유 취약점으로 인하여 발생되었던 것으로 파악된다.

– 그러나 피신청인이 주장하는 해당 취약점은 이미 이 사건이 발생하기 이전인 2009. 12. 공식적으로 알려진 것으로서, 피신청인으로서는 해당 취약점이 발표된 이후부터 이 사건 발생 직전까지의 기간동안 취급중인 개인정보가 인터넷 홈페이지 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 ① 서버에 파일 업로드를 허용하지 아니하도록 조치하는 방법, ② 파일 업로드를 해야하는 서버일 경우라도 서버에서 업로드된 파일에 스크립트 실행 권한을 부여하지 않는 방법, 또는 ③ 파일 스크립트 실행 권한을 부여해야 하는 서버의 경우라면 권한 설정을 새로이 점검하는 방법 등을 통하여 본 취약점을 충분히 보완할 수 있었음이 인정되고,가사, 피신청인이 위 취약점 보완방법에 따른 조치를 별도로 취하지 아니하였다고 하더라도, 이 사건 발생 이전에 서버 운영체제를 응용프로그램과의 정합성을 고려한 최신 소프트웨어로 갱신 · 점검을 위하여 업데이트만 하였더라도 이 사건 사고를 사전에 방지할 수 있었을 개연성이 충분히 존재하였음에도 피신청인은 위와 같은 조치들을 소홀히 한 과실이 있다고 판단된다.

– 그러므로 피신청인은 개인정보의 분실 · 도난 · 누출 · 변조 또는 훼손을 방지하기 위하여 규정된 기술적 · 관리적 조치를 다하지 아니함으로써 신청인의 개인정보를 외부에 유출하여, 「정보통신망법」 제28조 제1항을 위반하였다고 판단된다.

관련 법령

【정보통신망 이용촉진 및 정보보호 등에 관한 법률】

제28조(개인정보의 보호조치) ① 정보통신서비스 제공자등이 개인정보를 취급할 때에는 개인정보의 분실 · 도난 · 누출 · 변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적 · 관리적 조치를 하여야 한다.

1. 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립 · 시행
2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치 · 운영
3. 접속기록의 위조 · 변조 방지를 위한 조치
4. 개인정보를 안전하게 저장 · 전송할 수 있는 암호화기술 등을 이용한 보안조치
5. 백신 소프트웨어의 설치 · 운영 등 컴퓨터바이러스에 의한 침해 방지조치
6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치

② 정보통신서비스 제공자등은 이용자의 개인정보를 취급하는 자를 최소한으로 제한하여야 한다.

【정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령】

제15조(개인정보의 보호조치) ① ~ ⑤ (생략)

⑥ 방송통신위원회는 제1항부터 제5항까지의 규정에 따른 사항과 법 제28조제1항제6호에 따른 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하여야 한다.

【舊, 개인정보의 기술적 · 관리적 보호조치 기준】

제4조(접근통제) ① ~ ⑦ (생략)

⑧ 정보통신서비스 제공자등은 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터에 조치를 취하여야 한다.

제7조(악성프로그램 방지) 정보통신서비스 제공자등은 백신소프트웨어를 월 1회이상 주기적으로 갱신 · 점검하고, 악성 프로그램관련 경보가 발령된 경우 및 백신소프트웨어 또는 운영체제 제작업체에서 업데이트 공지가 있는 경우에는 응용프로그램과 정합성을 고려하여 최신 소프트웨어로 갱신 · 점검하여야 한다.