2012년 금융IT 정보보호동향 예측 분석

유정각*, 태인규**

* 금융결제원 금융정보보호부 보안기술분석팀 과장(E-mail: kagi@kftc.or.kr)
** 금융결제원 금융정보보호부 보안기술분석팀 계장(E-mail: graylynx@kftc.or.kr)

〈요 약〉

2011년 초 발표된 금융결제원의 금융ISAC 기술보고서 '2011년 금융IT 정보보호 동향 예측 분석'에서는 2011년의 주요 정보보호 이슈로서 목표대상이 명확한 조직적 공격, 스마트폰 등 모바일 관련 위협, 악성 프로그램 위협, 데이터 유출 등을 예측한 바 있다. 실제로 지난 한 해 동안 이 같은 정보보호 이슈들은 분산서비스거부(Distributed Denial of Service, DDoS) 공격, 개인정보와 산업기밀 유출, 전산 시스템 장애 등 다양한 침해사고로 거의 모든 산업 분야에서 현실화되어 나타났다. 특히 핵티비즘(hacktivism)에 바탕을 둔 공격이 증가하는가 하면 국내외 유수의 기업들이 대규모 데이터 유출로 곤혹을 치르기도 했다.

이에 본고에서는 여러 기관에서 발표한 2012년 정보보호동향 예측 자료를 토대로 2012년 정보보호동향을 예측하고 금융IT 관련 주요 이슈를 전망함으로써 금융기관의 선제적 대응방안 마련을 통한 보안성 및 안전성 향상에 기여하고자 한다.

2012년에는 전년도와 마찬가지로 APT(Advanced Persistent Threat)로 대표되는 '목표대상이 명확한 조직적 공격'이 1위의 정보보호 이슈로 예측되었으며, 최근의 모바일 트렌드를 감안한 모바일 관련 위협, 고도화된 악성 프로그램의 위협이 그 뒤를 이었다. 이는 2011년도와 동일한 양상으로 전반적인 공격 트렌드가 APT 및 모바일 기기로 이동하고 있음을 방증한다고 볼 수 있다. 이 외에도 데이터 유출, 소셜 네트워크 서비스 위협, 사회적 이슈와 결합된 소셜 엔지니어링을 통한 공격, 클라우드 컴퓨팅 보안, 사이버 범죄 조직의 체계화 · 은닉화, 보안관제의 변화, HTML5 보안 등이 2012년 고려해야 할 Top 10 이슈로 선정되었다.

특히 2012년 정보보호 이슈와 관련하여, 국내 금융IT 부문에서는 'IT컴플라이언스 요구사항 변화', '스마트폰 뱅킹 서비스 위협 증가', '내부정보 유출방지 강화'가 주목받을 것으로 예상된다. 각종 관련 법률의 제 · 개정이나 금융 감독당국의 IT보안 검사 강화 움직임을 감안할 때 금융기관이 이 같은 컴플라이언스 요구에 부응하여야 할 것이며, 최근 빠르게 증가하고 있는 스마트폰 뱅킹 서비스에 대해서도 다양한 형태의 공격 시도가 본격화될 수 있는 바 이에 대한 사전적 대응이 필요할 것이다.

아울러 그동안 금융IT 서비스가 빠르게 변화하고 발전하면서 주요 보안 이슈에만 편중하여 대응하여 왔다면, 2012년은 경영진의 지원과 관심을 바탕으로 현재의 보안 대책을 전반적으로 재검토하여 효율성을 높이고, 안전성을 향상시킬 수 있도록 재구성하는 작업이 필요한 시점이라 할 수 있겠다.

Ⅰ. 개요

1. 배경 및 목적

정보보호업계에서는 한 해를 정리하고 다음 해를 준비하는 차원에서 매년 동향 예측 보고서를 발표한다. 이와 관련하여 금융결제원 금융ISAC은 업계의 동향 예측자료들을 수집 · 분석하여 공통적으로 언급된 이슈들을 뽑아, TOP 10 이슈를 도출하고 금융IT 분야에서 예상되는 이슈를 정리해 왔다.

2011년은 분산 서비스거부(Distributed Denial of Service, DDoS) 공격, 개인정보와 산업기밀 유출, 전산 시스템 장애 등 다양한 침해사고가 발생하였을 뿐만 아니라 수천만 건의 개인정보가 유출되는 등 사고의 피해 및 규모가 거대해졌다. 또한 정부와 공공기관, 정보보호업계, 금융회사, 게임회사, 언론사 등 거의 모든 영역의 산업분야에서 침해사고가 발생하였고, 핵티비즘(hacktivism)[1]에 바탕을 둔 공격자의 활동도 적극적으로 변화함에 따라 정보보호에 대한 관심이 급증한 한 해였다.

본고를 통해 발생가능한 위협들의 보안 리스크를 평가하여 선제적인 대응방안을 마련함으로써, 금융기관의 보안성과 안전성 향상에 기여할 수 있을 것으로 기대한다.

2. 범위

본고에서는 지난 2011년에 발생한 다양한 보안이슈 사항을 정리하고, 여러 기관에서 발표한 2012년 정보보호동향 예측을 토대로 전반적인 시장 전망을 정리한다. 또한 이러한 전망과 금융IT 분야의 주요 이슈사항을 종합하여 금융IT 측면에서 정보보호동향을 예측해본다.

제II장에서는 금융결제원 금융ISAC 기술보고서 '2011년 금융IT 정보보호동향 예측 분석'에서 선정한 '2011 정보보호동향 예측 TOP 10'과 실제 현실화된 대표사례를 비교 · 분석하여 지난 2011년의 주요 이슈들을 정리한다. 제III장에서는 국내외 정보보호업체, 관련 기관 및 언론 등 총 21개 기관에서 발표한 '2012 정보보호동향 예측 자료'를 분석하고, 2012년의 핫이슈가 될 것으로 예상되는 '2012 정보보호동향 예측 TOP 10' 및 '금융IT 관련 주요 이슈'를 선정한다. 마지막으로 제IV장에서는 3년간의 '정보보호동향 예측 TOP 10'을 비교 · 분석하고 결론을 맺는다.

1) 해킹(hacking)과 행동주의(activism)를 합성한 단어로 정치 · 사회적 목적을 가진 사이버 공격 행위를 지칭한다.

II. 2011년 주요 이슈

2011년은 대형 침해사고가 잇달아 발생하면서 정보보호 업계를 긴장시킨 한 해였다. 특히, 금융권에서는 DDoS 공격, 주요 시스템 파괴, 고객정보 유출 사고 등이 발생하였고, 최근에는 스마트폰 뱅킹 서비스에 대한 보안위협도 빠르게 증가하는 등 정보보호의 중요성이 대두되고 있다. 이에 '2011년 금융IT 정보보호동향 예측 분석' 보고서에서 선정한 '2011 정보보호동향 예측 TOP 10'을 기준으로 2011년 발생한 침해사고 및 보안이슈를 정리하였다(표1 참조).

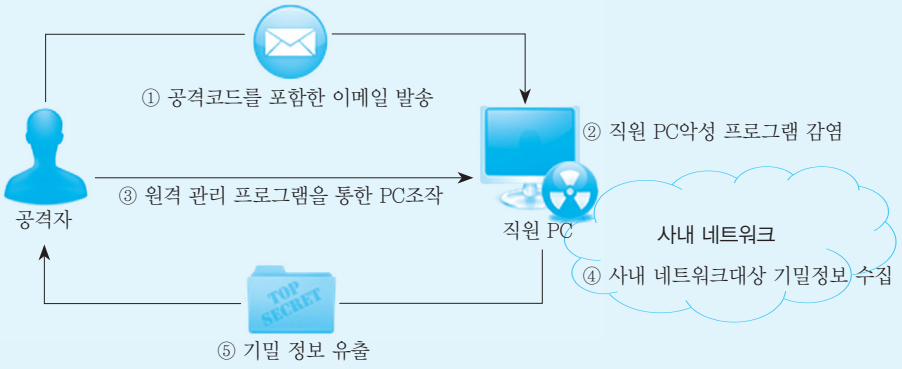
〈표1〉 2011 정보보호동향 예측 TOP 10 및 대표사례

순위	2011 정보보호동향 예측 TOP 10	대표사례
1	목표대상이 명확한 조직적 공격	– RSA, 농협, SK커뮤니케이션즈 등의 침해사고 – Night Dragon, The Nitro 등의 공격행위 – 어노니머스, 룰즈섹 등 핵티비스트 활동
2	스마트폰 등 모바일 관련 위협	– 안드로이드 대상 악성 프로그램 급증 – 스마트폰 터치스크린 키로깅
3	악성 프로그램 위협	– 자바, 플래시, PDF 리더, 한컴 오피스 제로데이 악용 – 유출된 인증서로 전자서명 된 악성 프로그램 유포
4	소셜 네트워크 서비스 위협	– SNS를 통한 악성 프로그램 유포 – 개인정보 유출
5	데이터 유출	– 산업비밀, 금융, 개인정보 유출 – 내부자 정보 유출
6	클라우드 컴퓨팅 보안	– 아마존 클라우드 서비스 장애 – 클라우드 서비스를 이용한 정보 유출
7	운영체제 관련 위협	– 맥OS 대상 악성 프로그램 증가 – 운영체제 보호기법 우회
8	소셜 엔지니어링	– 보이스 피싱과 연계된 웹사이트 피싱 공격
9	사이버범죄에 대한 대응 및 국제공조 강화	– 3.4 DDoS 공격 분석 국제 공조 – 국제 사이버 범죄조직 추적
10	전자금융보안	– 인터넷뱅킹 트로이목마 악성 프로그램 유행 – 제우스 소스코드 유출 및 변종 등장

APT(Advanced Persistent Threat)로 대표되는 '목표대상이 명확한 조직적 공격'의 사례는 RSA의 OTP(One Time Password) 토큰 관련 기밀정보 유출, 농협의 주요 시스템 파괴, SK커뮤니케이션즈 대량 고객정보유출 등의 사고를 꼽을 수 있다. APT는 주로 정부나 기업을 대상으로 산업기밀이나 군사기밀, 고객정보 등의 정보를 탈취하는 공격으

로, 2005년에는 주당 1건 정도 발견되었으나 2011년에는 매일 80여건이 탐지되는 등 크게 급증한 것으로 조사되었다.[2] 특이한 사례로는 2010년 이란의 원자력발전소를 공격해 주목받았던 스턱스넷(Stuxnet)의 제작자가 유포한 것으로 추정되는 듀큐(Duqu)라는 악성 프로그램이 발견되었으나, 아직까지 명확한 대상이나 피해상황은 밝혀지지 않고 있다.[3] 또한 〈그림1〉에서와 같이 RSA를 공격하여 OTP 토큰정보를 유출하고, 방위산업 업체인 록히드 마틴(Lockheed Martin)을 공격한 사건을 분석 중에 국내 통신업체를 포함한 총 760여개의 세계적으로 유명한 기업들을 대상으로 공격이 진행되었음이 알려지기도 했다.[4]

〈그림1〉 RSA에 대한 조직적 공격 사례



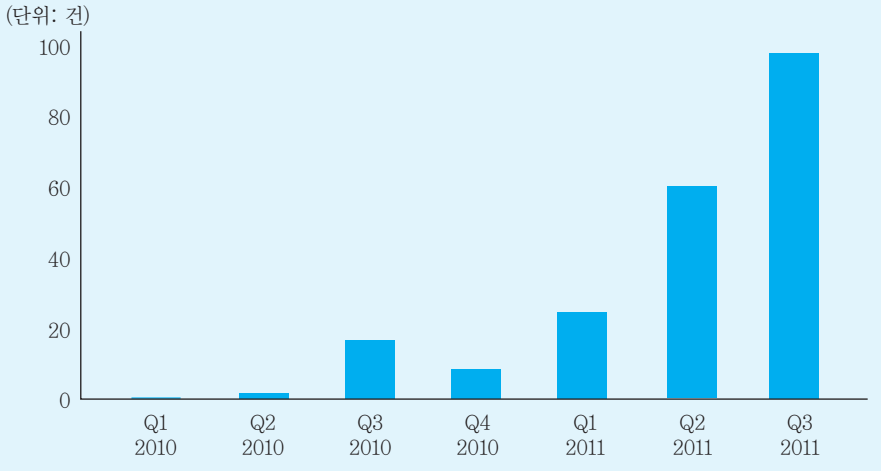
한편, 어노니머스(Anonymous), 룰즈섹(LulzSec) 등 핵티비즘을 표방한 공격자에 의한 침해사고가 상당수 발생하였다.[5] 사고 이후 CEO가 사임한 미국 보안회사인 HBGary를 비롯하여 FBI, CIA 등의 정부기관, 소니(Sony) 그룹의 다양한 계열사 등이 공격당했고, 특히 소니 PSN(PlayStation Network)의 경우 1억 명의 고객정보가 유출되고, 2개월간 서비스를 제공하지 못하는 등 큰 타격을 입은 것으로 조사되었다. 연말에는 민간전략정보분석 기업을 공격해 획득한 신용카드 정보를 이용하여 전자 프런티어 재단(Electronic Frontier Foundation)과 적십자사에 기부한 영수증을 공개하기도 하였다.[6]

또한 스마트폰의 보급이 전세계적으로 크게 증가하면서 '스마트폰 등 모바일 관련 위

2) Intelligence Report: November 2011, Symantec.
3) W32.Duqu: The Precursor to the Next Stuxnet, Symmantec(2011.10.).
4) Who Else Was Hit by the RSA Attackers?, Krebs on Security(2011.10.).
5) 2011 is the Year of the Hacktivist, Verizon Report Suggests, WIRED(2011.12.).
6) Antisec Hits Private Intel Firm; Million of Docs Allegedly Lifted, WIRED(2011.12.).

협'이 주목받고 있다. 이러한 추세와 더불어 스마트폰을 대상으로 한 악성 프로그램도 증가하였는데, 특히 앱의 배포 및 설치가 자유로운 안드로이드(Android) 운영체제 환경을 대상으로 급증하고 있다(그림2 참조).[7] 초창기 스마트폰 악성 프로그램은 단순히 정보 유출이나 부정 문자메시지 발송 등의 낮은 수준으로 구현되었으나, 최근에는 자동 루팅(rooting) 및 원격 명령수행을 통한 봇넷(Botnet) 구축까지 가능한 수준으로 발전하였다.[8] 또한 스마트폰 환경에서 동작하는 키보드 로깅 프로그램이 상용제품 및 개념증명(Proof of Concept) 코드로 공개되면서 스마트폰의 정보 유출 위협이 점차 현실화되고 있는 상황이다.[9][10] 스마트폰 뱅킹 서비스 측면에서는 중대한 보안이슈가 발견되지 않았으나, 스마트폰 뱅킹 앱의 변형된 환경(탈옥, 루팅) 탐지 기능을 우회할 수 있는 도구[11][12]들이 블랙마켓에서 유통되고 있어 지속적인 모니터링이 요구된다.

〈그림2〉 안드로이드 환경에서 악성 프로그램 발견 빈도



'악성 프로그램 위협' 측면에서는 양적인 증가와 더불어 공격 대상 및 방법에서의 변화가 감지되었다. 우선 윈도우 환경뿐만 아니라 맥OS 대상 악성 프로그램[13]이 증가하였으며, 앞서 언급한 바와 같이 스마트폰 대상, 특히 안드로이드 환경에서 동작하는 악성 프

7) Threats Report: Third Quarter 2011, McAfee.
8) 안드로이드 기반 악성 앱 동향, 금융ISAC 기술노트, TN-2011-4(2011. 3.).
9) 탈옥된 iOS 환경의 키로거 관련, 금융ISAC 기술노트, TN-2011-5(2011. 4.).
10) 가상키보드 키로깅 등 스마트폰 뱅킹 해킹 관련, 금융ISAC 기술노트, TN-2011-13(2011.11.).
11) kBankTweak(http://www.myrepospace.com/profile/kBankTweak).
12) HideJB(http://devbug.me/category/프로그래밍/HideJB).
13) Crimekit for MacOSX launched, CSIS(2011. 5. 2.).

로그램이 급증하였다. 공격 방법으로는 운영체제의 취약점보다 널리 사용되는 응용프로그램의 취약점이 많이 이용되었는데, 국내에서 주로 사용되는 한글 워드프로세서를 포함하여 자바, 어도비 플래시 플레이어, PDF 리더의 제로데이(0-day)[14] 취약점이 다수 발견되었다. 또한 악성 프로그램이 윈도우 드라이버 파일 형태로 유포될 때 도난당한 인증서로 서명되어 운영체제의 경고 없이 악성 프로그램이 설치되기도 하였다(그림3 참조). 악성 프로그램의 유포경로는 타겟팅된 스팸 메일을 통해 관심이 있을 법한 이슈에 악성 프로그램을 첨부하는 형태나 유명 웹 사이트를 침해한 후 악성 프로그램을 유포하는 방식이 주로 이용되었다. 특히, 국내에서는 주말에 주요 언론사 및 커뮤니티의 홈페이지에 게시되는 광고서버나, 소셜 댓글 등을 제공하는 서버를 침해하여 악성 프로그램을 유포하는 사례가 매우 빈번히 발견되고 있어 각별한 주의가 요구된다.[15]

〈그림3〉 Duqu 악성 프로그램 유포에 이용된 인증서

2011년은 세계적으로 대규모 '데이터 유출' 사고가 자주 발생한 해로, 유출된 정보의 양이 소니의 경우 최대 1억 명을 넘어서고, 국내에서는 SK커뮤니케이션즈 3,500만 명, 넥슨 1,300만 명에 달하는 등 피해 규모가 매우 크다고 할 수 있다(표2 참조).[16] 데이터 유

14) 취약점 정보가 알려졌으나 취약점에 대한 패치가 제공되지 않은 상태이다.
15) 성탄연휴 이틀간, 최소 20만대 PC 악성코드에 감염!, 데일리시큐(2011.12.26.).
16) Ten Big Breaches In 2011, Dark Reading(2011.11.29.).

출은 타겟팅된 공격으로 발생한 경우도 있으며, 내부 직원의 고의로 인한 유출 사고도 다수 발생하였다. 유출된 정보에는 보통 암호화된 비밀번호가 포함되어 있어 전 국가적으로 비밀번호 변경 캠페인이 활발하게 진행되었다. 다만 비밀번호를 변경하더라도 유출된 개인정보를 이용해 비밀번호 찾기가 가능할 수 있어 주의가 요구된다.

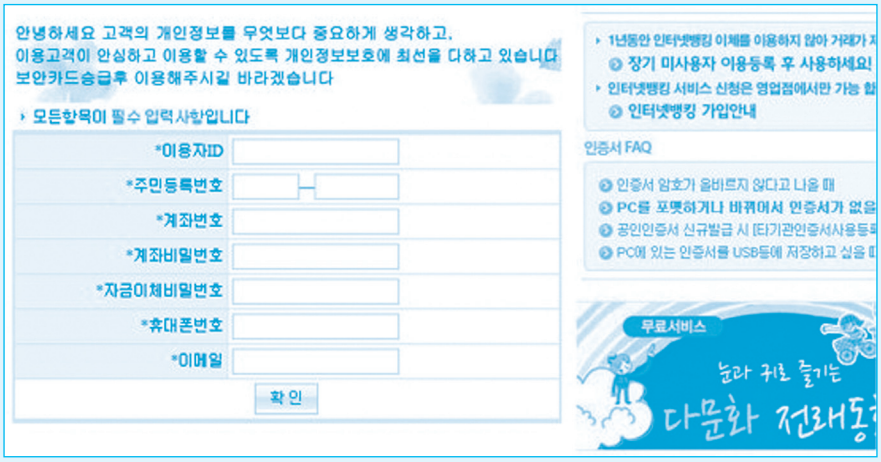
〈표2〉 2011년 발생한 대규모 데이터 유출 사고

피해기업	시기	유출내용
코모도 (Comodo)	2011. 3	– 인증서 발급기관인 코모도사의 RA 시스템 침해 – 구글, 야후 등에 대한 서버 인증서 부정 발급
EMC RSA	2011. 3	– 직원에게 악성 이메일 발송을 통한 RAT 감염 후 정보유출 – OTP 토큰인 SecurID 제품의 기밀정보 유출(추정)
엡실론 (Epsilon)	2011. 3	– 마켓팅 대행업체인 엡실론의 메일발송 서버 침해 – 수백만 명의 고객정보 유출
워드프레스 (WordPress)	2011. 4	– 운영서버의 관리자 권한 침해 – 공개되지 않은 소스코드 유출
소니 PSN (PlayStation Network)	2011. 4	– 소니 플레이스테이션 온라인 게임 관련 서버 침입 – 1개월 이상의 서비스 장애 유발 및 1억 명의 고객정보(1,200만 명의 신용카드 정보 포함) 유출
씨티은행	2011. 5	– 홈페이지 고객정보 조회 페이지에 취약점 존재 – 신용카드 고객정보(36만 명) 유출
SK 커뮤니케이션즈	2011. 7	– 알툴즈 업데이트 서버를 이용한 직원 PC의 RAT 감염 – 고객정보(3,500만 건) 유출
트라이케어 (TRICARE)	2011. 9	– 위탁업체 사이언스 애플리케이션 인터내셔널에서 백업 테이프 도난 – 개인정보 및 진료기록 등 고객정보(490만 건) 유출
페이스북 (FaceBook)	2011.11	– 자동 친구 요청을 통해 수천명의 인맥 형성(연구목적) – 250GB 용량의 개인정보 획득
스팀 (Steam)	2011.11	– 게임 유통업체의 포럼 사이트 침해 – 고객정보(3,500만 명) 유출

다음으로 유명 웹사이트와 동일한 모양의 피싱(Phishing) 사이트를 만들고 보이스피싱으로 방문을 유도하는 '소셜 엔지니어링'을 통한 피해도 증가하였다. 금융사고가 발생하였으니 계좌잠금 조치가 필요하다거나, 보안등급 승급 등을 미끼로 계좌번호, 계좌비밀번호, 공인인증서 비밀번호, 보안카드 일련번호 등 계좌이체나 카드론 대출 등에 필요한 정보를 입력하도록 유도하였는데, 대검찰청, 금융위원회 e-금융민원센터, 한국정보보호진흥원, 은행 등을 모방한 피싱 사이트가 발견된 바 있다(그림4 참조).[17)18)]

17) 가짜 대검찰청 홈페이지를 이용한 개인정보 수집 주의, 울지않는벌새(2011. 9. 7.).
18) 가짜 e-금융민원센터를 이용한 보이스피싱 주의, 울지않는벌새(2011.11.16.).

〈그림4〉 사칭 홈페이지를 통한 정보 입력 유도



'사이버범죄에 대한 대응 및 국제공조 강화' 측면에서는 3월에 발생한 DDoS 공격의 수사과정을 통해 관련 내용을 파악할 수 있다. 해당 DDoS 공격의 경우 총 746대의 C&C(Command and Control) 서버가 세계 각국에 흩어져 있었으나, 경찰청은 41개국에 국제 공조수사를 요청하여 서버 6대의 하드디스크 이미지를 제공 받은 것으로 알려졌다. 해당 이미지 분석을 통해 C&C 서버의 역할과 계층구조 등을 파악할 수 있었으며, 일부 국가에서는 FTP를 통해 이미지 파일을 보내주는 등 적극적으로 협조하기도 하였다.[19] 이렇듯 사이버 범죄행위는 해외의 공격자에 의한 사고뿐만 아니라 해외에 위치하는 중간 경유지를 이용하는 경우가 많기 때문에 국제공조 강화는 지속되어야 한다.

'전자금융보안'과 관련해서는 뱅킹 트로이목마(Trojan)의 대표적인 악성 프로그램인 제우스의 소스코드가 인터넷에 유출되면서 다양한 경로를 통해 변종이 전파되었다.[20] 국내 인터넷뱅킹 서비스를 대상으로 한 악성 프로그램이 발견되기도 했으나, 초보적인 수준으로 별다른 피해는 알려지지 않았다. 또한 국정감사에서 원격관리도구(Remote Administration Tool, RAT)를 이용한 화면해킹 시연이나 웹 인젝션(Web Injection) 기술이 이슈가 되기도 했다.[21][22] 한편, 해외에서는 휴대전화 문자메시지로 전송되는 일회용 비밀번호(mobile Transaction Authentication Number, mTAN)를 가로채는 기능을

19) 국제 사이버범죄 대응 심포지엄 2011 행사동향, 금융ISAC 기술동향, TT-2011-6(2011. 7.).
20) Zeus 소스코드 유출에 따른 국내 인터넷뱅킹 영향, 금융ISAC 기술노트, TN-2011-6(2011. 6.).
21) 국정감사 화면해킹 시연 관련, 금융ISAC 기술노트, TN-2011-11(2011. 9.).
22) 웹 인젝션 공격기법 분석, 금융ISAC 기술노트, TN-2011-10(2011. 9.).

가진 스마트폰 대상 악성 프로그램이 발견된 바 있다.[23]

이러한 이슈들 외에도 인터넷 보안 프로토콜 표준인 TLS/SSL 프로토콜과 관련한 위협이 다수 발생하였는데, 서버의 인증서를 발급하는 인증기관(Certificate Authority)인 코모도(Comodo)와 디지노타(Diginotar) 등의 주요 시스템이 공격자로부터 침해당해 구글, 야후 등 유명 사이트에 대한 인증서가 공격에 이용되기도 했다. 또한 프로토콜이 가진 취약점을 이용하여 통신 내용의 기밀성을 침해할 수 있는 공격도구(Browser Exploit Against SSL/TLS, BEAST)[24]가 발표되었고, 통신 세션을 생성할 때 서버의 부하가 가중되는 특징을 악용한 공격도구(THC-SSL-DOS)[25]도 공개되었다. 최근 구글, 페이스북, 트위터 등에서 도감청 등을 피하기 위하여 TLS/SSL을 적용할 수 있도록 하고, TLS/SSL을 서버 차원에서 강제할 수 있는 HSTS(HTTP Strict Transport Security) 기능도 표준화 작업 중에 있는 등 TLS/SSL의 이용이 증가할 것으로 예상되므로 지속적인 정보수집이 요구된다.

Ⅲ. 2012년 동향예측

1. 예측자료 분석결과

가. 분석 개요

맥아피(McAfee), 웹센스(WebSense), 안철수연구소 등 국내외 정보보호 업체, 언론 및 관련 기관에서 발표한 총 21건의 '2012년 정보보호동향 예측 자료'를 토대로 전반적인 보안업계의 예측을 분석하였다. 각 자료에서 예측된 총 141건의 이슈에 대해 공통점을 찾아 분류하고, 2012년의 핫이슈가 될 것으로 주목되는 '2012 정보보호동향 예측 분석 TOP 10'을 선정하였다.

2012년 정보보호동향 예측자료는 〈표3〉에서와 같이 크게 공격 트렌드, 플랫폼 보안, 악성 프로그램, 서비스 보안, 대응 트렌드, 정책 이슈의 6가지 부문으로 분류할 수 있었으며, 이 중 '공격 트렌드'에 대한 예측이 42%로 가장 많았고, '플랫폼 보안'에 대한 예측은 26%, '악성 프로그램'에 대한 예측은 14%, '서비스 보안'에 대한 예측은 11%로 그 뒤를 이었다(그림5 참조).

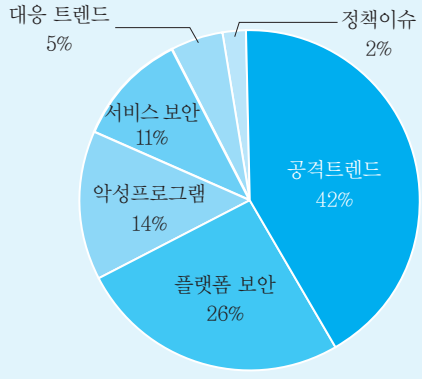
23) Trojan:SymbOS/Spitmo.A, F-Secure(2011. 4.).
24) Juliano Rizzo, BEAST: Surprising crypto attack against HTTPS(2011. 9.).
25) TLS/SSL 서비스 거부 공격 도구 분석, 금융ISAC 기술노트, TN-2011-14(2011.11.).

〈표3〉 2012 정보보호동향 예측 분류

(단위: 건)

부문	세부 내용	건수
공격 트렌드	APT, 조직적 사이버 범죄, 데이터 유출, CaaS 등	59
플랫폼 보안	스마트폰 등 모바일 관련, 클라우드 컴퓨팅, 윈도우8, 맥OS 등	37
악성 프로그램	복잡한 악성 프로그램 위협 증가, 인증서 사용, 봇넷 등	20
서비스 보안	소셜 네트워크 서비스 위협, 전자금융보안, 웹 보안 등	16
대응 트렌드	보안관제 기술 변화, 보안시장의 성장 등	7
정책이슈	IT컴플라이언스 등	2
합 계		141

〈그림5〉 2012 정보보호동향 예측 분류 비율



'공격 트렌드' 부문에서는 APT와 같은 목표대상이 명확한 조직적 공격, 데이터 유출, 핵티비즘 등의 공격행위, 사이버 범죄조직의 CaaS(Crime as a Service) 등의 주제들이 선정되었다. '플랫폼 보안' 부문에서는 스마트폰 등 모바일 관련 위협, 클라우드 컴퓨팅 보안, 윈도우8 및 맥OS 등 운영체제 관련 위협 등에 대한 전망이 있었으며, '악성 프로그램' 부문에서는 악성 프로그램의 고도화 · 자동화, 봇넷, 공격 툴킷의 증가 등이 예측되었다. '서비스 보안' 부문에서는 소셜 네트워크 서비스 위협에 관한 언급이 가장 많았으며, 전자금융보안 및 HTML5 보안에 관한 예측도 있었다. '대응 트렌드'에서는 보안관제 기술의 변화를 다루었고, '정책이슈' 부문에서는 IT컴플라이언스가 주로 언급되었다.

2012년 정보보호동향 예측자료 분석결과를 토대로 선정된 '2012 정보보호동향 예측 TOP 10'은 〈표4〉와 같다.

〈표4〉 2012 정보보호동향 예측 TOP 10

(단위: 건)

순위	2012 정보보호동향 예측 TOP 10	건수
1	목표대상이 명확한 조직적 공격	33
2	스마트폰 등 모바일 관련 위협	31
3	악성 프로그램 위협	20
4	데이터 유출	14
5	소셜 네트워크 서비스 위협	10
6	소셜 엔지니어링	7
7	클라우드 컴퓨팅 보안	6
8	사이버범죄 조직화	5
9	보안관제의 변화	4
10	HTML5 보안	3

1위는 APT로 대표되는 사이버워(Cyber War) 및 SCADA(Supervisory Control And Data Acquisition) 시스템을 타켓으로 한 '목표대상이 명확한 조직적 공격'에 대한 예측이고, 2위는 스마트폰과 태블릿 등 모바일 기기의 사용이 늘어남에 따른 '모바일 관련 위협'에 대한 예측이다. 3위는 수법이 더욱 고도화되고 다양한 유형의 위협이 혼합되어 있는 '악성 프로그램 위협'이 증가할 것이라는 예측이고, 4위는 개인 및 금융정보, 산업 기밀 등 '데이터 유출' 위협에 대한 예측이다. 5위는 트위터나 페이스북과 같은 소셜 네트워크 서비스의 이용이 많아짐에 따라 이에 따른 위협이 증가할 것이라는 예측이다.

6위는 선거나 런던 올림픽 등의 사회적 이슈와 결합된 소셜 엔지니어링을 통한 공격이 증가할 것이란 예측이고, 7위는 최근 도입이 증가하고 있는 클라우드 컴퓨팅 관련 보안 이슈가 많아질 것이라는 예측이다. 8위는 사이버 범죄 조직이 체계화, 은닉화 되어 CaaS를 제공할 것이라는 예측이고, 9위는 TLS/SSL 프로토콜 증가와 빅데이터에 대한 보안관제 기술의 변화에 대한 예측이며, 10위는 상업적 이용이 증가하고 있는 HTML5의 보안성과 관련된 예측이다.

나. 주요 이슈

1) 목표대상이 명확한 조직적 공격

'목표대상이 명확한 조직적 공격'과 관련된 이슈는 2010년부터 정보보호동향 예측 1위

를 연속으로 차지하고 있다. 실제 APT에 의한 침해사고가 지속적으로 발생하고 있고, 전세계적으로 사이버워와 관련하여 국가차원에서 조직적인 움직임이 표면화되는 만큼 2012년에도 APT에 의한 침해사고는 계속 발생할 것으로 예상된다.

또한 올해는 미국과 우리나라의 대통령 선거와 같은 사회적으로 관심이 큰 이슈가 있어 핵티비즘을 표방한 정치적 의도의 공격행위가 증가하리라 예상된다. 지난해 핵티비즘으로 인한 침해사고와 관련하여 유출된 데이터를 포함한 공격의 내용이 인터넷에 구체적으로 발표됨으로써 피해 대상이 큰 타격을 입은 바 있으므로 더욱 주의해야 할 것으로 보인다.

한편, 2010년에 발견된 대표적인 APT 악성 프로그램인 스턱스넷과 같이 전력, 원자력, 수도 등 사회 기반시설을 관리하는 SCADA 시스템 대상 공격 역시 계속될 것으로 예측되고 있다. SCADA 시스템에 대한 공격은 IT 측면에서의 침해 및 데이터 유출 문제가 아닌 사회적인 혼란과 물리적 · 인적 피해로 연계될 수 있어 대비가 필요하다.

2) 스마트폰 등 모바일 관련 위협

스마트폰, 태블릿 등의 모바일 기기 이용자가 늘어남에 따라 모바일 애플리케이션에 대한 공격이 집중될 것으로 예측된다. 단순한 정보 유출 수준이 아닌 모바일 기기 운영체제 환경에서 전파되는 웜(worm)의 등장이나 봇넷의 출현이 예상된다. 모바일 환경은 기기의 종류가 다양하고 실시간으로 취약점 패치가 제공되지 않아 상당수의 모바일 기기가 제로데이 취약점에 노출되어 있을 것으로 판단된다. 특히, 안드로이드 기기의 경우 펌웨어 업데이트의 제한으로 인해 취약점 패치에 상당 기간이 소요되며, 블랙마켓을 통한 악성 앱의 유포가 수월하여 상대적으로 위험도가 더 높다고 할 수 있다.

모바일 기기에 백신 등의 보안 솔루션을 설치하더라도 플랫폼의 특성상 권한이 제한되기 때문에 악성 프로그램의 탐지 및 차단에도 한계가 있다. 또한, 보안 관리자에 의해 관리되지 않는 모바일 단말에 업무 데이터가 저장되는 사례가 갈수록 증가하고 있어, 이로 인한 데이터 유출 사고가 발생할 것으로 예측되고 있다. 특히, 직원의 개인기기(Bring Your Own Device, BYOD)에 대한 적극적인 통제절차를 검토할 필요가 있다. 그리고 개인의 위치 정보가 쉽게 노출될 수 있는 위협에 대해서도 경고하고 있으며, TV나 냉장고 등 기존의 전자 제품이 인터넷에 연결되면서 새로운 위협 요소로 등장하리라 예상되고 있다.

3) 악성 프로그램 위협

악성 프로그램은 매년 양적으로 급증할 뿐만 아니라 유포 방식에 있어서도 정상적인 인증서로 서명되거나, 디스크의 부팅 영역에 감염되는 부트킷(Bootkit)을 이용하는 등 질적으로도 고도화되고 있다. 또한 가짜 백신(Scareware)과 같이 정상적인 프로그램으로 위장한 악성 프로그램도 지속적으로 증가할 것으로 예측되고 있다.

한편, 악성 프로그램을 유포할 때 운영체제 수준의 취약점을 공격벡터로 사용하는 것이 가장 위협적이나, 최근에는 운영체제 취약점이 존재하더라도 코드 실행이 어렵도록 여러 보안 기술이 적용되어 있어 공격코드 작성이 어려워지고 있다. 따라서 일반적으로 사용자가 많은 자바, 플래시 플레이어, PDF 리더, 오피스 프로그램의 취약점을 이용한 공격시도가 증가하고 있다. 소셜 엔지니어링을 통해 타겟팅된 공격을 수행할 때도 이러한 응용프로그램의 취약점을 이용할 가능성이 높을 것으로 판단된다.

대형 봇넷의 경우, 국제적으로 여러 기관이 공조하여 폐쇄하고 있어 사이버 범죄조직에서는 소규모 봇넷을 다수 구축하여 관리할 가능성이 높아지고 있다. 또한 블랙마켓에서 감염 PC의 수만큼 대금을 지불하는 PPI(Pay-Per-Install) 서비스를 이용하거나 공격툴킷(Exploit Toolkit)을 이용해 더욱 쉽게 봇넷 구축이 가능해질 것으로 예상된다.

온라인결제나 인터넷뱅킹 및 스마트폰 뱅킹 등의 전자금융 서비스와 관련해서는 트로이목마형 악성 프로그램이 계속 증가할 것이고, 유출된 제우스 소스코드를 이용한 변종 및 스마트폰 대상 악성 프로그램이 증가할 것으로 보인다.

4) 데이터 유출

데이터 유출은 사이버 공격행위의 최종 목적 중 하나로서, 유출한 데이터를 블랙마켓에 매매하여 현금화하거나, 정부기관 및 기업의 중요 데이터를 인터넷에 공개하는 핵티비즘으로 이용될 수 있다. 따라서 홈페이지에 대한 공격을 포함하여 중요 정보에 접근할 수 있을 것으로 예상되는 임직원을 대상으로 한 타겟팅된 공격이 증가할 것으로 예상된다. 상대적으로 보안관리 능력이 떨어지는 중소 규모의 기업은 쉽게 공격당할 수 있으므로 꼭 필요한 데이터만을 수집하고 불필요한 데이터는 상시적으로 파기하는 등의 대비가 요구된다.

한편, 외부에서의 공격으로 인한 데이터 유출 외에도 중요 데이터에 접근 권한을 가진 내부 직원에 의한 고의적 · 비고의적 사고도 증가할 것으로 예측되고 있다. 특히, 모바일 오피스 등 모바일 단말을 통한 업무를 시작하기 전에 추가적인 보안 대책을 마련해야 한다.

2. 금융IT 관련 주요이슈

가. IT컴플라이언스 요구사항 변화

전자금융거래법 및 전자금융감독규정 전면개정 및 시행, 개인정보보호법 시행, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 개정 등 금융IT보안과 관련된 컴플라이언스 측면에서 변화가 크게 나타나고 있다(표5 참조).

〈표5〉 금융IT 보안관련 법률 주요 제 · 개정내용

법명	시행일	제 · 개정내용
개인정보보호법	2011. 9.30	– 개인정보 보호 범위의 확대(종이문서 포함) – 이용자 고유식별정보 처리 제한 – 개인정보 유출 통지 및 신고제 도입 – 개인정보 영향평가 의무 수행(공공기관)
전자금융거래법 전자금융감독규정	2012. 5.15 2011.10.10	– 정보보호최고책임자(CSO) 지정 의무화 – 전자금융기반시설에 대한 취약점 분석 · 평가 의무화 – 정보기술 및 보안 분야의 관련 인프라 확보 권고 – IT 세부 보안기준을 감독규정으로 상향조정
정보통신망 이용촉진 및 정보보호 등에 관한 법률	2012. 7	– 개인정보보호법에 명시된 주요내용 포함 – 임원급의 정보보호 최고책임자(CSO) 지정 – 정보보호 관리체계(ISMS) 인증제도 일원화 (정보보호 안전진단제도 폐지)

금융위원회에는 금융IT보안을 총괄하는 전자금융팀이 신설되었고, 금융감독원은 IT보안 검사를 대폭 강화할 것으로 예고하고 있다. 따라서 금융회사에서는 이러한 변화에 따른 자사의 보안 규정, 예산, 인력 등에 대해 조정이 필요한 상황이다.

나. 스마트폰 뱅킹 서비스 위협 증가

스마트폰 뱅킹 서비스의 가입자 수는 2011년 3분기 기준 812만 명으로, 곧 천만 명을 넘어설 것으로 기대되고 있다. 하지만 이와 함께 스마트폰에 대한 보안 위협의 증가와 공격 기법의 현실화로 인해 스마트폰 뱅킹 서비스를 대상으로 하는 악성 프로그램이 대거 출현할 것으로 예상된다. 따라서 스마트폰 뱅킹 서비스를 제공하는 금융회사는 이용 고객에게 악성 프로그램에 대한 주의사항을 지속적으로 안내하고 보안위협에 선제적으로 대

응해 나가는 자세가 필요하다.

현재 스마트폰 뱅킹 서비스에 대한 보안 기능은 운영체제 변형 탐지, 백신 설치(가능한 플랫폼만), 가상 키보드 입력으로 구분되어진다. 그러나 운영체제 변형 탐지의 경우 리버스 엔지니어링을 통해 무력화 될 수 있고, 일반 앱의 권한으로 동작하는 백신의 역할은 PC에 비하여 제한적이며, 가상 키보드의 경우에도 키로깅이 가능할 수 있다. 따라서 새로운 보안 기술에 대하여 연구하고, 관련 위협에 대해 지속적인 모니터링을 수행해야 하겠다.

한편, 스마트폰 뿐만 아니라 태블릿PC, 스마트TV 등 다양한 모바일 기기에서 별도의 뱅킹 서비스를 제공하여 관리의 복잡성이 증가할 것으로 예상되고 있다. 따라서 장기적으로는 하나의 서비스 플랫폼을 통해 모든 단말을 대상으로 전자금융 서비스가 가능할 수 있도록 준비할 필요가 있다.

다. 내부정보 유출방지 강화

금융회사는 주민등록번호와 같은 개인의 식별 정보 뿐만 아니라 신용, 자산 등 실생활에 밀접한 개인정보를 다루고 있어 공격자들의 타깃으로 빈번하게 선택되는 편이다. 더불어 해외에서는 경제위기 등의 이유로 핵티비즘 그룹이 금융회사를 대상으로 직접 공격을 수행하겠다고 선전포고한 사례도 찾아볼 수 있다. 또한, 내부정보 유출로 인해 피해가 발생할 경우 감독당국으로부터 경영진의 문책은 물론 유출된 고객의 집단 소송에 의한 경제적인 타격도 클 것으로 판단된다. 따라서 금융회사는 개인 및 금융정보를 최우선적인 보호 대상으로 취급하고, 처리 시스템에 대한 기술적 · 관리적 보호조치를 수행하여야 한다.

내부정보 유출방지를 위해서는 네트워크 접근통제 및 내부정보 유출방지 솔루션을 기본으로 운영하고, 데이터베이스에 대한 접근권한을 최소화하며, 데이터 암호화를 통해 유출 가능성을 최소화할 수 있다. 아울러 논리적 또는 물리적으로 네트워크를 분리하여 업무 데이터의 외부 유출 경로를 차단할 수 있다. 내부정보 유출방지 정책을 세울 때는 외부 공격자로부터 침해사고로 인한 위협 뿐만 아니라 내부에서 권한을 가진 직원의 오용에 관한 부분도 반드시 고려하여야 한다.

더불어 하나의 시스템(네트워크 구간)이 침해되더라도 주변의 시스템(네트워크 구간)으로의 추가 공격행위를 차단할 수 있는 봉쇄(containment) 개념의 보안 대책을 검토할 수 있다. 그리고 기존의 침입차단 및 탐지 이벤트를 종합 분석하는 통합보안관리시스템(Enterprise Security Management)을 확장하여 응용프로그램에서 발생되는 이벤트나 다른 보안 솔루션의 이벤트까지 축적하여 분석할 수 있는 시스템에 대해서도 장기적으로

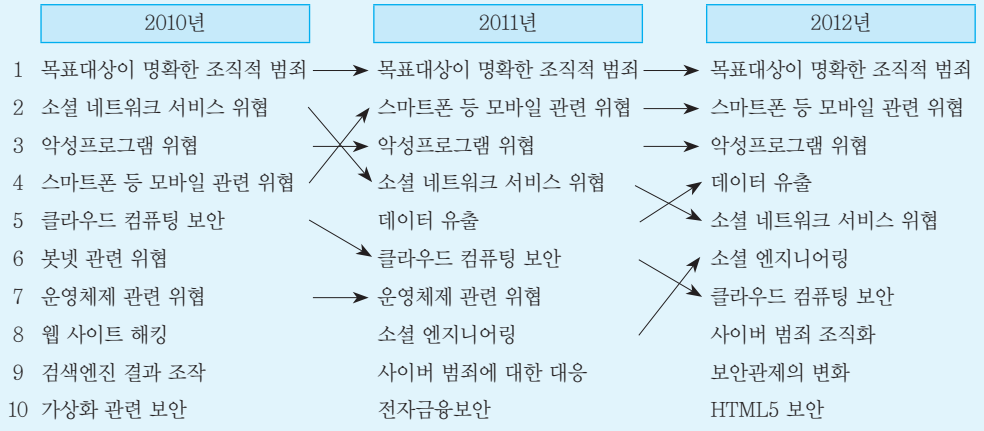
고민할 필요가 있다.

Ⅳ. 결론

본고에서는 지난해 선정된 '2011 정보보호동향 예측 TOP 10'과 비교하여 실제 한 해 동안 발생한 주요 이슈들을 비교 · 정리하고, 국내외 정보보호 업체, 관련기관 및 언론 등에서 발표한 총 141건의 '2012 정보보호동향 예측 자료'를 분석하여 '주요 부문별 예측 분류 비율' 및 '2012 정보보호동향 예측 TOP 10'을 선정하였다.

2010년부터 선정한 정보보호동향 예측 TOP 10의 추이를 살펴보면 상위권의 순위는 큰 변화가 없는데 반해 하위권에서만 일부 항목이 변경되고 있음을 알 수 있다(그림6 참조).

〈그림6〉 정보보호동향 예측 TOP 10 추이



특히 '목표대상이 명확한 조직적 범죄'의 경우 3년 연속 1위로 선정되고, '스마트폰 등 모바일 관련 위협'은 2년 연속 2위로 선정되는 등 전반적인 공격 트렌드가 APT 및 모바일 기기로 이동하고 있음을 확인할 수 있다. 결국 이러한 형태의 악성 프로그램이 개발되어지고, 소셜 엔지니어링과 소셜 네트워크 서비스를 통해 유포되며, 침해사고 결과 데이터가 유출되는 형태로 보안위협이 현실화되고 있는 것이다.

보안위협으로 선정된 각각의 항목은 현실에 복합적으로 영향을 끼치게 되며, 사소한 부분일지라도 취약한 포인트가 있다면 그 부분으로부터 공격이 시작되기 때문에 어떠한 영역도 소홀히 해서는 안된다. 즉, 중요한 시스템이라면 계층적인 보호를 통해 복수의 보호

기술을 적용하여 안전하게 관리하여야 하고, 중요도가 낮은 시스템이라 할지라도 보호기법을 적용하지 않는 상태로 운영하여서는 안된다.

지난해는 국내외의 굵직한 침해 사고가 자주 발생했던 만큼, 여론이나 관계기관의 관심이 급증하고 관련 법률 및 규정의 제 · 개정을 포함한 다양한 보호조치가 논의된 한 해였다. 따라서 올해에는 감독 및 규제기관에서 각 금융회사들이 어떻게 보호조치를 적용하고, 보안위협에 대응하고 있는지 집중적인 점검을 진행할 것으로 예상되고 있다.

최근 들어 금융IT 서비스가 빠르게 변화하고 발전하면서 주요 보안 이슈에만 편중하여 대응하여 왔다면, 2012년은 경영진의 지원과 관심을 바탕으로 현재의 보안 대책을 전반적으로 재검토하여 효율성을 높이고, 안전성을 향상시킬 수 있도록 재구성하는 작업이 필요한 시점이라 할 수 있겠다.

〈참 고 문 헌〉

[1] Adam Powers, The Future of Security: Top Five Predictions for 2012, Tangled Web Blog, 2011.12.

[2] Booz Allen Reports Top Ten Cyber Security Trends for Financial Services in 2012, Booz Allen Hamilton, 2011.11.

[3] Chris Wysopal, Which of the 10 Big Breaches in 2011 Were Application Security Related?, Veracode, 2011.12.

[4] David Coursey, Best Read: Brandt's Top 5 Malware Threats in 2012, Forbes, 2011.12.

[5] Derek Brown, 2011: The Year in Review, Tipping Point, 2011.12.

[6] Five Security Predictions for 2012, ThreatPost, 2011.12.

[7] Five predictions for security in 2012, CNET, 2011.12.

[8] Josh Shaul, A Look Back at the Top Breaches of 2011_Team Shatter Exclusive, Team Shatter, 2011.12.

[9] Kaspersky Lab, Targeted Attacks, Cyber Warfare, Mobile Threats: What to Expect in 2012, Kaspersky, 2011.12.

[10] Luis Corrons, 2012 Security Trends, PandaLabs, 2011.12.

[11] McAfee Labs, 2012 McAfee Threat Predictions: A look at the latest threats that could affect consumers this coming year, McAfee, 2011.12.

[12] Mel Morris, Top 7 cybersecurity predictions for 2012, Webroot, 2011.11.

[13] Michael Sutton, 2012 Security Predictions, Zscaler, 2011.12.

[14] M86 Security Labs: Threat Predictions 2012, M86 Security, 2011.

[15] Rick Popko, Top 8 Security Predictions for 2012, Fortinet, 2011.12.

[16] Robert David Graham, Predictions for 2012, Errata Security, 2012. 1.

[17] Top 11 Data Breaches of 2011, Imperva, 2011.11.

[18] Sara Yin, Top 5 Security Predictions for 2012, Security Watch, 2011.12.

[19] Sinead O'Connor, Trends 2012, G Data, 2011.12.

[20] Social Media Abuse, Mobile Malware Headline 2011 Top Internet Security Trends, Dark Reading, 2011.12.

[21] Ten Big Breaches In 2011, Dark Reading, 2011.11.

[22] The Day Before Zero, 2012 Security Predictions, Damballa, 2011.12.

[23] Threatpost Top Security News Stories of 2011, Threatpost, 2011.12.
[24] Top 9 Data Security Trends for 2012, Imperva, 2011.12.
[25] Trend Micro, 12 for 2012: What Will The New Year Bring?, Malware blog, 2011.12.
[26] WatchGuard Technologies, 2012 Security Predictions, WatchGuard, 2011.12.
[27] Websense Security Labs, 2012 Cyber Security Predictions from the Websense Security Labs, WebSense, 2011.11.
[28] Websense, 2011 predictions score A−, 2012 predictions coming soon…, 2011.11.
[29] 2011년 10대 보안 위협 트렌드 발표, 안철수연구소, 2011.12.
[30] 2012년 예상 7대 보안 위협 트렌드 발표, 안철수연구소, 2012. 1.