IT기반보호단 암호응용팀

암호, 그 중요성은 계속된다

모든 분야가 그러하겠지만, 정보보호 분야 역시 다양한 기술들이 접목돼 있다. 그중 암호 기술은 '암호=정보보호'라는 등식이 성립될 만큼 정보보호 제품 및 서비스의 근간을 이뤄왔고, 또 불과 몇 년전까지만 해도 암호학자가 정보보호 전문가로 대표되기도 했다. 물론 암호 이외의 다양한 기술들이 정보보호에 접목되고 있는 현 시점에서도 암호기술의 중요성은 여전히 유효하다. 다만 많은 사람들이 가장 기본적인 것을 간과하듯, 정보보호 기술 도처에 있는 암호 혹은 암호와 관련된 기술의 중요성을 미처 생각하지 못할 뿐이다.

글 · 사진 정보보호뉴스 취재팀

한국정보보호진흥원이 처음 설립된 이후 몇 년동안 암호기술을 연구하고, 관련 정책을 수립 및 적용하기 위해 투입된 인력 및 부서의 규모는 상당히 컸다. 비록 현재 암호응용팀의 규모가 축소되고 또, 이들이 KISA 내에서 유일하게 '암호'라는 단어를 사용하는 팀으로 남아있지만, 이런 변화가 정보보호 분야에서 암호의 비중을 평가하는 잣대로 사용될 수 없다는 사실은 분명하다.

IT와 암호의 접점

"기초학문이라는 것이 있듯, 암호는 정보보호의 기초이자 근간입니다. 기반기술이기에 특정 기업이나 시장에서 개발하는 것은 쉽지 않죠. 암호기술에 대한 연구 및 개발뿐만 아니라 그 기술을 각 기업이 응용할 수 있도록 가교역할을 하는 것이 현재 암호응용팀에게 주어진 임무라고 봐요." IT기반보호단 암호응용팀 전길수 팀장의 말이다.

사실 전 팀장의 말을 빌리지 않더라도, 정보보호 분야에서 암호기술은 참으로 많은 분야에서 응용된다. 단지 응용되는 비중의 차이일 뿐, 암호화 통신을 비롯해 시스템, 네트워크 보안제품에 적용된 암호기술의 중요성은 매우 크다. "겉으로 드러나지 않는 분야이기에 일반인들에게 암호는 비중이 낮은 것으로 간주되곤 해요. 실제로 견고하고 효과적인 암호 알고리즘이 개발된다고 해도 이 사실을 중요하게 생각하는 사용자는 거의 없잖아요. 하지만 암호기술이 정보보호의 근간을 이루고 있다는 사실만은 변함이 없어요"라는 전 팀장은 최근에는 본래의 순수 암호연구에서 벗어나 암호기술이 적용될 수 있는 다양한 응용분야로의 접근을 시도하고 있다고 설명한다.

암호가 우리의 곁으로 왔다

올해 초 발간한 '안전한 패스워드를 위한 가이드라인'처럼 암호응용팀은 암호기술이 응용될 수 있는 분야를 발굴하고, 해당 분야에 어떻게 적용되어야 할 것인지를 제시하는 등 암호기술이 실생활에서 쉽게 활용할 수 있도록 노력하고 있다. 이런 역할은 암호기술 자체를 위한 연구에서 한걸음 발전된 것임은 분명하다. "지금까지 해왔던 암호 기반 기술개발이나 국제표준 추진 등의 활동 이외에도 암호와 관련된 인증 서비스 분야는 매우 흥미있는 분야입니다." 전 팀장은 그런 의미에서 최근 아이디 관리 서비스에 대한 연구가 활발하게 이뤄지고 있다고 한다. 인터넷 활용의 증가로 많은 사용자들이 수많은 웹사이트에 아이디를 등록하고 자신의 개인정보를 제공하고 있지만, 이로 인해 한 사용자가 많은 아이디를 관리해야 하는 불편이 발생하게 된다. 여기에 개인정보 오남용 피해가 급증함에 따라 최근 많은 아이디에 대한 통합관리 요구가 제기되고 있다. 암호응용팀도 이런 불편함을 암호기술로 해결하기 위해 연구하고 있는 것이다.

"해킹, 피싱 등 악의적인 목적으로 아이디와 패스워드를 수집하는 경우가 늘어나면서, 신뢰할 수 있는 사이트에 아이디와 패스워드, 그리고 개인정보를 저장시키고 이를 여러 웹서비스 업체가 이용할 수 있도록 하는 오픈 아이디는 향후 G-PIN, i-PIN 그리고 공인인증서와 결합해 보다 강력한 인증이 요구되는 분야로까지 확대가 가능하다고 봅니다"라는 전 팀장은 기술적인 적용이 용이하고, 별도의 비용이 발생하지 않는 오픈 아이디를 비롯한 아이디 관리 서비스에 대한 관심은 더욱 커질 것이라고 전망했다. "사이버 공간에서는 자신을 식별할 수 있는 인증정보들이 반드시 필요해요. 문제는 그 정보를 어떻게 숨기고, 제어하고 또 통제할 것이냐 하는 것이죠. 가령 사용자들에게 패스워드를 8자리 이상으로만 쓰게 한다면 안전성은 강화되겠지만, 현실적으로 사용자들이 많은 불편함을 느끼겠죠. 결국, 서로 모순된 관계에 있는 보안성과 편의성을 어떻게 만족시킬 것이냐가 암호응용 기술이 풀어나가야 할 과제라고 봐요"라고 전 팀장은 암호기술의 응용분야의 한 예를 소개한다.

서두에 언급했듯, 암호기술은 보안서버를 비롯해, 보안관리, 데이터 송수신, 접근제어 등 다양한 정보보호 분야에 적용되고 있다. 하지만 100% 완전하지 않다는 것이 정보보호의 숙명이듯, 암호도 완벽할 수는 없다. 그런 의미에서 어쩌면 IT 발전에 가장 민감한 것이 암호기술이고, 지속적인 연구를 통해 변화에 빠르게 대응해야 하는 것 역시 암호기술이다. 기초 암호기술의 연구와 이에 대한 활용분야의 발굴 및 지원이 활발하게 이뤄질 수 있는 가교역할. 그것이 바로 암호응용팀에 거는 우리들의 기대다. S

"일반인들에게는 낯설겠지만, 암호기술은 새로운 기술변화에 민감하게 반응하고, 또 대응하고 있어요. 이뿐만 아니에요. 암호기술을 통해 보다 안전하고 편리하게 서비스를 이용할 수 있도록 다양한 응용분야도 개발해야 해요." IT기반보호단 암호응용팀 전길수 팀장은 암호기술의 지속적인 개발과 응용분야의 발굴은 암호응용팀의 중요한 몫이라고 설명한다.