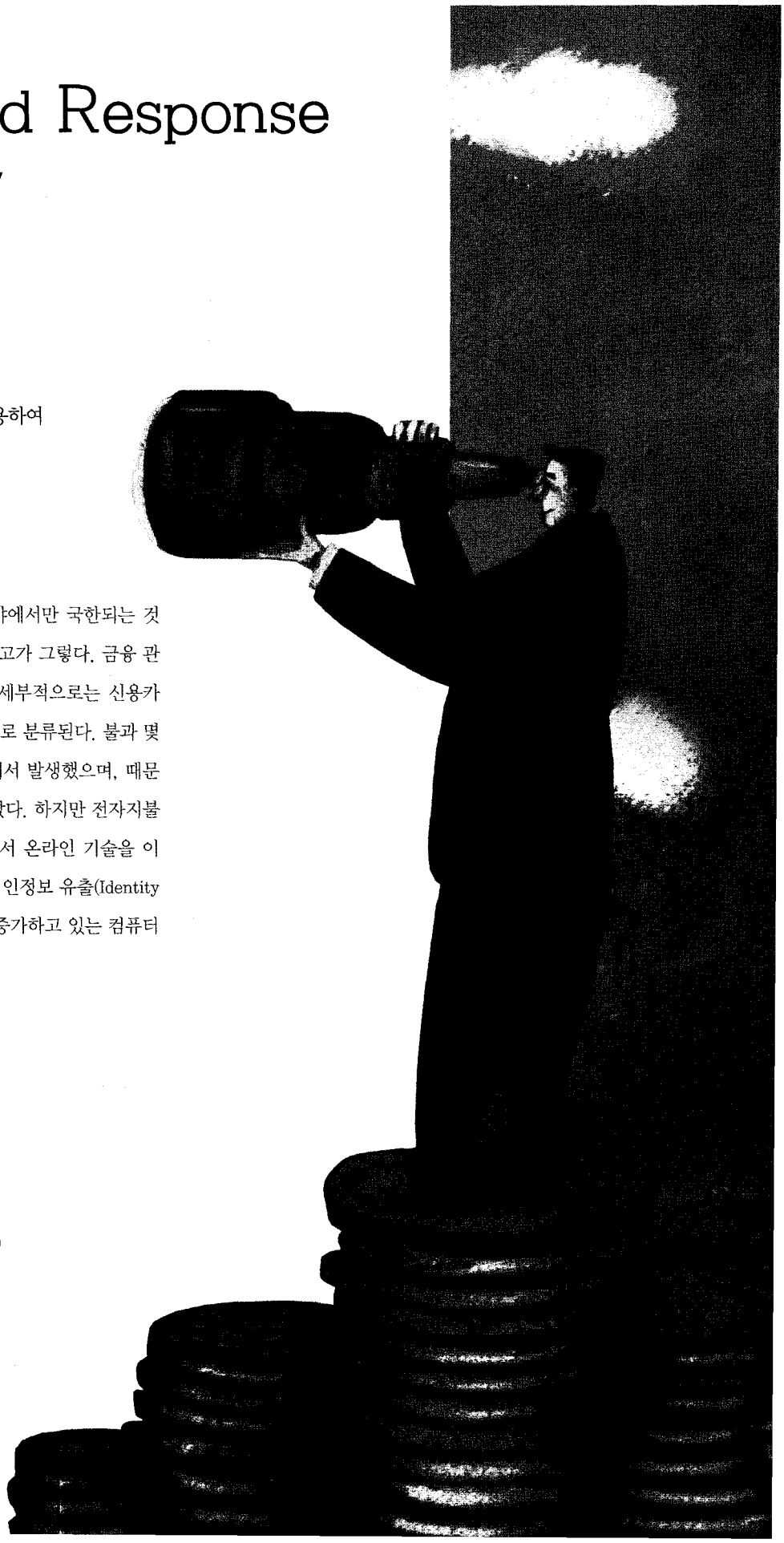
Online Fraud Response
- Beyond Security



"최근의 공격자들은 정보를 훔치고 이를 이용하여
금전적 이익을 얻는 것이
주요 목적이며, 이를 위해 기술적 방법과
非기술적 방법을 이용한다."

보안 사고는 컴퓨터 및 인터넷과 관련한 분야에서만 국한되는 것은 아니다. 대표적으로 신용카드 정보유출 사고가 그렇다. 금융 관련 사고는 일반적으로 'Fraud'라고 불리며, 세부적으로는 신용카드 위조, 명의도용, 도난분실 등의 사고유형으로 분류된다. 불과 몇 년전까지만 해도 Fraud는 주로 오프라인 상에서 발생했으며, 때문에 정보보호 전문가의 능력이 요구되지는 않았다. 하지만 전자지불 및 전자금융이 발전하고 그 규모가 확대되면서 온라인 기술을 이용한 Fraud가 증가하고 있다. 최근 몇 년간 개인정보 유출(Identity Theft)과 신용카드 관련 사고는 가장 빠르게 증가하고 있는 컴퓨터 범죄 중 하나로 분류되고 있다.

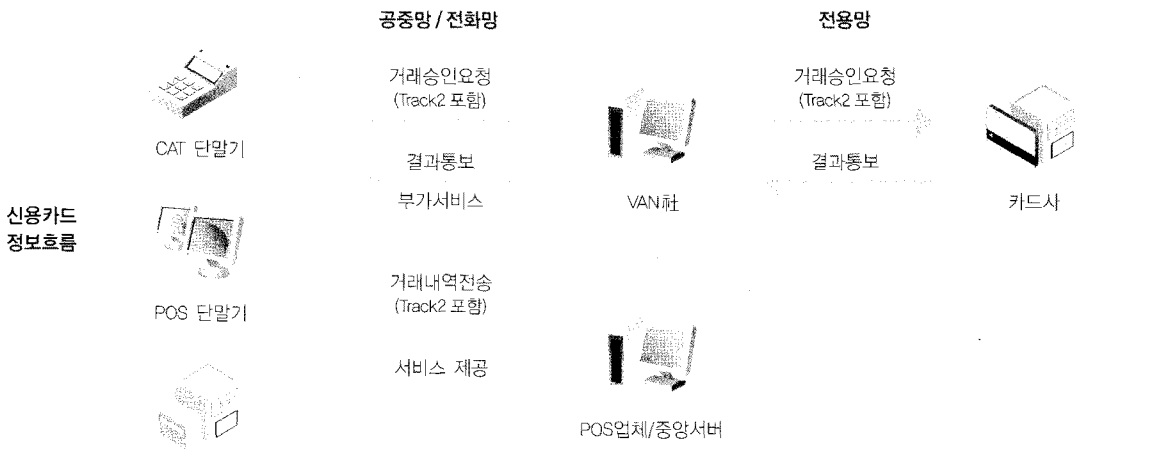
글 **이현우** | 前 신한카드 과장_ talltree2@naver.com

신용카드는 이미 오래 전부터 해킹 대상의 한 분야였고, Carding(신용카드 정보 해킹 행위, 부정사용 행위), Cardable(신용카드 정보를 획득할 수 있는 기업 전산망, 전자상거래 사이트, 현금화 가능 사이트), Carder(신용카드 정보만을 전문적으로 유출하는 공격자) 등의 용어가 사용되고 있다. 조직화된 범죄자들은 인터넷 상에서 자신들만의 통신 채널을 통해 정보를 상호 교환하면서 신용카드 정보가 저장된 전상망을 해킹, 정보를 유출하고 이를 다양한 경로를 통해 현금화한다.

■ 신용카드 정보유출 현황

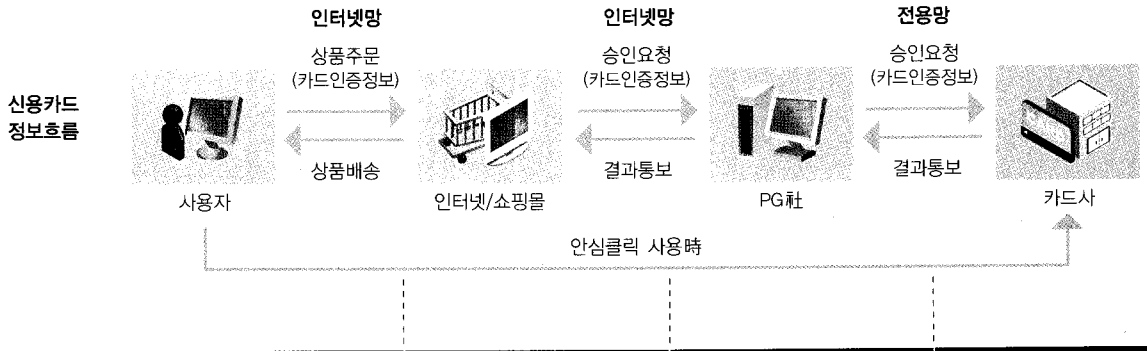
신용카드 위조 및 부정사용에 필요한 정보는 오프라인 거래와 온라인 거래로 구분해 살펴볼 수 있다. 오프라인 거래에서는 신용카드 뒷면 마그네틱에 저장된 정보가 필요하며, 온라인 거래에서는 카드번호, 유효기간, CVC(Card Validation Code) 등의 정보가 필요하다. 따라서 신용카드 정보유출 사고는 이 같은 정보를 획득하는 것에서 출발한다.

신용카드 정보유출 기법은 카드정보의 흐름에 따라 그 기법이 지속적으로 발전 및 변화하고 있는데, 고전적인 오프라인 기법으로는 사용자가 가맹점에서 카드 결제 시 위장 취업자가 신용카드 리더기(Skimmer)를 이용해 카드정보를 복사하는 방법이 있다. 그리고 신용카드 정보를 다루는 기업 전산망을 해킹해 대량의 정보를 빼내거나, Crimeware(범죄를 목적으로 하는 악성 프로그램)를 이용해 사용자 PC에서 정보를 획득하는 방법도 있다. 여기서 한걸음 더 나아가 최근에는 불법 정보획득을 위해 '사람을 해킹'하는 피싱(Phishing), 전화사기 등이 성행하고 있다.



정보 유출처	가맹점	네트워크	카드정보처리업체	네트워크	카드사
정보 유출기법	– 위장취업자에 의한 Skimming – POS에 저장된 Track2 정보유출 – 인터넷에 연결된 POS 해킹	– 와이어 태핑 – 네트워크 도청	– VAN사에 저장된 Track2 정보 유출 – POS관리업체에 저장된 Track2 정보유출(내부자/해킹)	– 네트워크 도청	– 카드사 정보유출 (내부자/해킹)

그림 1 · 오프라인 거래에서의 카드정보 흐름과 정보유출 기법



정보 유출처	사용자	인터넷/쇼핑몰	PG사	카드사
정보 유출기법	- PC를 해킹하여 KEY 입력 유출(악성프로그램) - 위조된 카드사 홈페이지로 유인, 카드정보 유출 (피싱, 파밍 등)	- 네트워크 도청 - 인터넷 쇼핑몰에 저장된 카드정보 유출 (내부자/해킹)	- PG사에 저장된 카드정보 유출 (내부자/해킹)	- 카드사 정보유출 (내부자/해킹)

그림 2 · 온라인 거래에서의 카드정보 흐름과 정보유출 기법

신용카드 정보를 획득한 공격자의 다음 단계는 해당 정보를 이용해 현금화하는 것이다. 기존 오프라인 방법으로는 유출된 정보로 위조 카드를 제작해 상점에서 상품을 구매한 후 되파는 방법이 주로 이뤄졌다. 그런데 최근에는 신용카드 정보, 즉 데이터를 정보 수집상이나 부정 사용자에게 판매하거나, 전자상거래 사이트에서의 고가 상품 구매 또는 인터넷 지급수단 및 자금 이체 서비스를 이용한 현금화 수법들이 증가하고 있다. 특히 사이버 머니, 온라인 자금이체 서비스는 향후 범죄자들의 주요 현금화 기법으로 부상할 것으로 예상된다.

■■ 정보유출 사고 전망

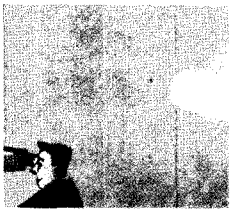
이처럼 신용카드 정보유출 사고의 이면에는 온라인 상의 해킹 기법의 변화와 연계돼 있고, 향후 정보유출 사고는 정보통신 기술 및 서비스의 변화에 따라 지속적으로 변화해 나갈 것이다.

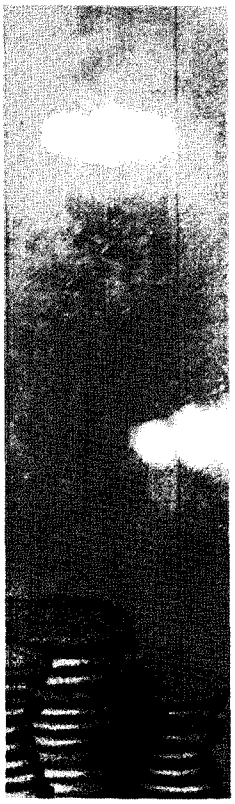
대표적으로 신용카드와 관련된 전산 인프라에 대한 집중적인 공격이 발생할 수 있다. 2004년 이후 중국에서 국내 온라인 게임 사이트를 집중적으로 공격해, 게임 아이템 및 게임 머니를 유출해 현금화하는 사고가 많이 발생하고 있는데, 국내에서 이 같은 현금화 방법을 규제하면서 점차 이 같은 공격은 줄어들 것으로 예상된다. 대신 공격자들은 또 다른 공격 대상을 찾을 것이며 신용카드가 그 대상이 될 가능성이 높다. 단지 공격의 대상이 되느냐 마느냐의 문제만 남아 있다.

이 같은 정보유출 사고에 대해 각 금융기관은 지금까지 내부 시스템과 네트워크만을 보호하는데 집중해 왔다. 하지만, 신용카드 정보가 유출될 수 있는 범위는 카드회사 이외에 VAN사, PG사, POS 업체, 전자상거래 업체, 가맹점 단말기, 온라인 사용자 단계로 확대되고 있다. 따라서 보호해야 할 대상도 확대될 수밖에 없다. VISA에서 시행하고 있는 PCI DSS(지불카드 협회 정보보안 표준) 프로그램은 신용카드 인프라 전반에 대한 보안 준수사항을 규정하는 대표적인 사례다.

한편, Fraud 탐지 및 모니터링에 대해서는 주로 오프라인에서 발생하는 부정 거래를 모니터링하는 방식이었는데, 향후에는 온라인 거래에 대한 모니터링을 보다 강화할 필요가 있다. 그러나 현재 온라인 거래에 대해서는 부정사용을 탐지하기 위한 모니터링 요소(Factor)가 오프라인 거래에 비해서 매우 부족한 상태이다. 따라서 전자상거래 업체 및 PG업체와 협력하여 온라인 거래를 보다 세밀하게 분석하고 모니터링하기 위한 기반을 구축해야 한다. 또한, 사고 대응 및 사후처리 부분에 있어서도 온라인 금융 사고를 분석하고 대응할 수 있는 보안 전문인력을 양성해야 한다. 그리고 무엇보다 온라인 사고의 책임 및 책임 규명을 위한 명확한 절차 및 기준이 필요한 시점이다.

■ 사용자 인식제고, 우선되어야





그렇다면 이와 같은 신용카드 Fraud, 더 나아가 금융사고를 예방하기 위한 방법에는 무엇이 있을까. Fraud에 대비한 금융기관의 관리적 대응방안으로는 사용자 인식, 금융기관의 역할, 그리고 법/제도적인 측면으로 구분해 살펴볼 수 있다. 먼저 온라인 Fraud에 대한 광범위한 사용자 홍보 및 인식 교육이 필요하다. 온라인을 이용한 서비스 및 거래가 지속적으로 증가하는 반면, 이와 관련된 사고에 대한 사용자 인식이 매우 부족한 상태이다. 특히, 최근에는 피싱(Phishing), 비싱(Vishing) 등 일반 사용자를 속여 정보를 유출하는 사회공학(Social Engineering) 기법이 증가하고 있는데, 이는 기술적 방법만으로 예방할 수 없는 공격이며, 금융기관 종사자를 포함한 사용자를 대상으로 한 인식교육을 통해 해소할 수 있다. 관리적 대응방안 뿐만 아니라, 금융기관은 각 기관의 신용카드 정보가 전송되고 처리되는 모든 부분에 대한 기술적 대응수단을 적용해 정보유출 개연성을 최소화시켜야 한다. 이를 위해서는 VAN사, PG사 등 각 금융기관 공통의 관심 대상이 되는 업체들이 있는데, 가능한 전 금융기관이 공통의 기준을 수립하여 일원화된 관리를 시행하는 것이 효과적이다. 공통의 관심사로는 아래와 같은 사항이 될 수 있을 것이다.

- POS, ATM, 전자 금융 거래를 위한 소프트웨어 등에 대한 개발 및 관리 기준 수립
- 신용카드 정보 및 금융 정보 처리 업체에 대한 IT 보안 기준 수립
- 사용자 대상 보안 인식 교육
- 온라인 금융사고 신고 접수 및 처리

최근 대부분의 보안사고는 Fraud로 연결되고 있으며, 이에 대한 예방 및 대응과 관련된 업무는 지속적으로 증가할 것이다. 지금까지 신용카드 Fraud 현황을 통해 컴퓨터 보안사고가 어떻게 오프라인 상의 Fraud에 영향을 미치는지 설명한 것처럼, 향후에는 온라인과 오프라인의 사기는 연계될 가능성이 높다. 문제는 이런 현상은 비단 금융권의 문제만이 아니라, 산업별로 다양한 방식으로 나타날 수 있다는 점이다. 지금은 산업별 정보보안의 특성을 이해하고, 정보유출 사고가 어떠한 위험을 줄 수 있는가에 대한 이해가 필요한 시점이다. **S**