J-TOPS

software*system*solution inSOUL SISOUL

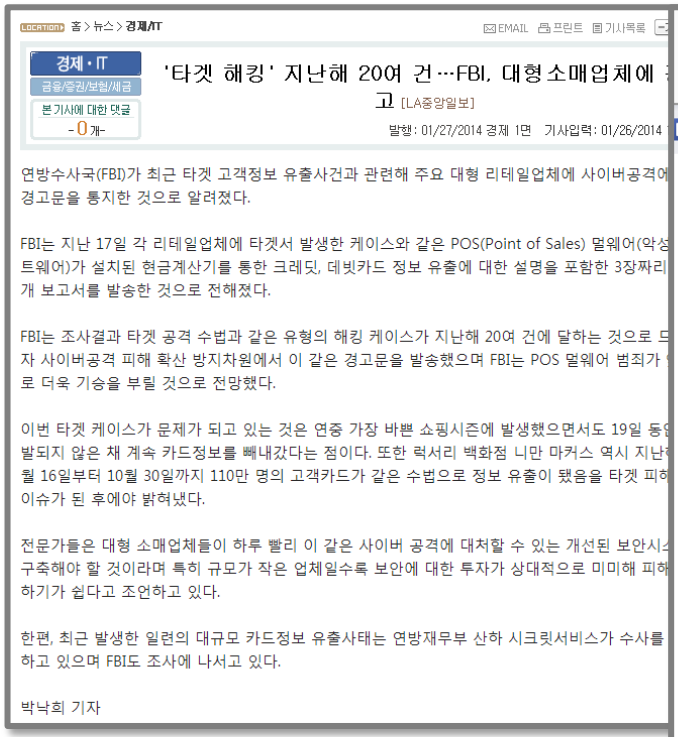
보안통제가 내장된 POS !!!

"단말 통제강화를 통한 POS를 통한 내부/외부 해킹 방지"

1. 보안통제가 내장된 POS의 필요성

1.1 제안배경

POS 단말기는 인터넷을 통한 개인신용카드의 모든 정보를 저장하고 있어, 의도치 않은 악성코드 감염, 내부 사용자 또는 외부 유지보수 인력에 의한 백도어 설치 등에 의해 국내는 물론 해외로 카드번호, 유효기간, 비밀번호 등이 유출될 가능성이 높은 실정이다.



LOCATION 홈 > 뉴스 > 경제/IT

경제 · IT

금융/증권/보험/세금

본기사에 대한 댓글 -0개-

'타겟 해킹' 지난해 20여 건…FBI, 대형 소매업체에 주…
고 [LA중앙일보]

발행: 01/27/2014 경제 1면 기사입력: 01/26/2014

연방수사국(FBI)가 최근 타겟 고객정보 유출사건과 관련해 주요 대형 리테일업체에 사이버공격에
경고문을 통지한 것으로 알려졌다.

FBI는 지난 17일 각 리테일업체에 타겟서 발생한 케이스와 같은 POS(Point of Sales) 멀웨어(악성
트웨어)가 설치된 현금계산기를 통한 크레딧, 데빗카드 정보 유출에 대한 설명을 포함한 3장짜리
개 보고서를 발송한 것으로 전해졌다.

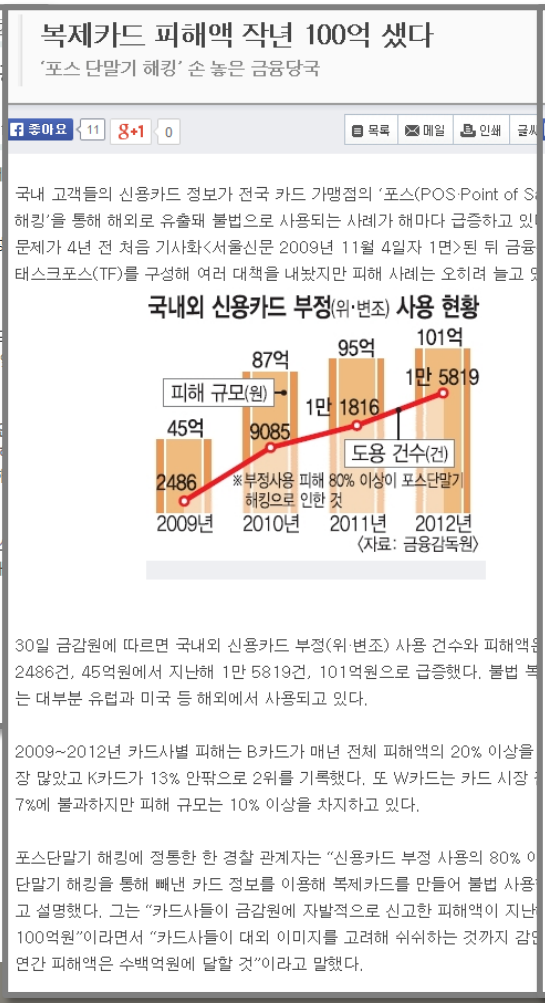
FBI는 조사결과 타겟 공격 수법과 같은 유형의 해킹 케이스가 지난해 20여 건에 달하는 것으로 드
자 사이버공격 피해 확산 방지차원에서 이 같은 경고문을 발송했으며 FBI는 POS 멀웨어 범죄가
로 더욱 기승을 부릴 것으로 전망했다.

이번 타겟 케이스가 문제가 되고 있는 것은 연중 가장 바쁜 쇼핑시즌에 발생했으면서도 19일 동안
발되지 않은 채 계속 카드정보를 빼내갔다는 점이다. 또한 럭셔리 백화점 니만 마커스 역시 지난
월 16일부터 10월 30일까지 110만 명의 고객카드가 같은 수법으로 정보 유출이 됐음을 타겟 피해
이슈가 된 후에야 밝혀냈다.

전문가들은 대형 소매업체들이 하루 빨리 이 같은 사이버 공격에 대처할 수 있는 개선된 보안시스
구축해야 할 것이라며 특히 규모가 작은 업체일수록 보안에 대한 투자가 상대적으로 미미해 피해
하기가 쉽다고 조언하고 있다.

한편, 최근 발생한 일련의 대규모 카드정보 유출사태는 연방재무부 산하 시크릿서비스가 수사를
하고 있으며 FBI도 조사에 나서고 있다.

박낙희 기자



복제카드 피해액 작년 100억 샜다

'포스 단말기 해킹' 손 놓은 금융당국

좋아요 11 +1 0 목록 메일 인쇄

국내 고객들의 신용카드 정보가 전국 카드 가맹점의 '포스(POS·Point of S
해킹'을 통해 해외로 유출돼 불법으로 사용되는 사례가 해마다 급증하고 있
문제가 4년 전 처음 기사화<서울신문 2009년 11월 4일자 1면>된 뒤 금융
태스크포스(TF)를 구성해 여러 대책을 내놨지만 피해 사례는 오히려 늘고 있

국내외 신용카드 부정(위·변조) 사용 현황

〈자료: 금융감독원〉

30일 금감원에 따르면 국내외 신용카드 부정(위·변조) 사용 건수와 피해액은
2486건, 45억원에서 지난해 1만 5819건, 101억원으로 급증했다. 불법 복
는 대부분 유럽과 미국 등 해외에서 사용되고 있다.

2009~2012년 카드사별 피해는 B카드가 매년 전체 피해액의 20% 이상을
장 많았고 K카드가 13% 안팎으로 2위를 기록했다. 또 W카드는 카드 시장
7%에 불과하지만 피해 규모는 10% 이상을 차지하고 있다.

포스단말기 해킹에 정통한 한 경찰 관계자는 "신용카드 부정 사용의 80% 이
단말기 해킹을 통해 빼낸 카드 정보를 이용해 복제카드를 만들어 불법 사용
고 설명했다. 그는 "카드사들이 금감원에 자발적으로 신고한 피해액이 지난
100억원"이라면서 "카드사들이 대외 이미지를 고려해 쉬쉬하는 것까지 감안
연간 피해액은 수백억원에 달할 것"이라고 말했다.

[서울신문 탐사보도] 카드 '포스단말기' 위험

긁는순간 정보 해외유출… 불법복제돼 마구 사용

좋아요 0 +1 0 목록 메일 인쇄 글씨크기

국내 고객 신용카드 정보가 전국 카드가맹점의 '포스단말기'를 통해 해외로 유출돼 복제된 뒤 불법 사용되고 있는 것으로 확인됐다. 8월 초부터 이 같은 움직임이 포착됐으며, 이후 수사 당국은 유출 경위와 피해 규모 등 실태파악에 들어갔다. 소프트웨어 보안전문 업체인 안철수연구소는 백신 개발 및 해법 찾기에 돌입했다. 하지만 해당 카드사들이 고객의 정보 유출을 은폐하고, 피해 규모를 축소하고 있어 정확한 규모 파악은 잘 안 되고 있다.

포스단말기는 백화점·할인점·편의점·프랜차이즈 업소 등 중·대형 가맹점에 설치돼 있다.

카드사별 사고 발생 현황 ※2009년 8월9~9월21일

카드사	불법복제 사용건수(건)	카드 사용액(억)	사용국가
신한	27	5600만	미국, 이탈리아, 스페인
롯데	17	3340만	그리스
국민	9	700만	미국, 이탈리아
현대	40	1400만	미국, 이탈리아
BC	11	4900만	미국, 이탈리아
외환	4	800만	그리스
삼성	미공개	1억 미만	이탈리아

(자료: 7개 카드사)

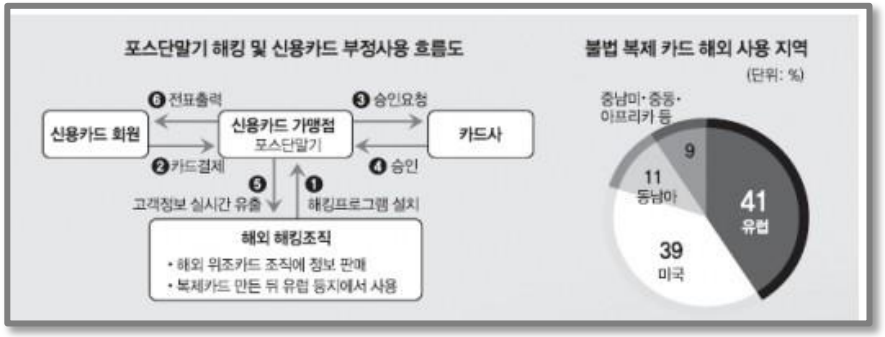
포스(POS: Point of Sale) 단말기는 단순히 거래 내역만 저장되는 다른 카드단말기와 달리 카드번호·유효기간 등 모든 신용카드 정보가 저장되는 단말기다. 이 단말기는 하드와 소프트웨어로 이뤄진 일반 PC와 같다고 보면된다. 이 때문에 포스단말기는 범죄조직들의 해킹 표적이 되고 있다. 전문가들은 포스단말기를 이용한 카드 복제는 기존의 단순 카드 복제와는 다른 신종 수법으로 이를 방치할 경우 금융피해가 눈덩이처럼 불어날 수 있다며 적극적인 대응에 나서야 한다고 말한다.

3일 수사당국과 카드사 등에 따르면 신한·국민·삼성·현대·롯데·BC·외환카드 등 7개 카드사의 고객 정보가 카드를 긁는 순간 실시간으로 빠져나가고 있는 것으로 파악되고 있다.

8월9일부터 9월21일까지 전국 카드가맹점의 '포스단말기'가 해킹돼 7개 카드사의 ▲카드번호 ▲유효기간 ▲PVV(카드 비밀번호 암호화값) ▲CVV(신용인증값) 등 고객들의 신용카드정보가 국외로 유출됐다. 이 기간 동안 7개 카드사들의 카드정보 3000건(명)이 새나갔으며 이 중 6개 카드사(삼성카드는 미공개) 108건이 미국·이탈리아·그리스·스페인 등지에서 불법 복제돼 3억여원의 카드사용액이 발생했다(표 참조).

1.2 주요 해킹 기법

1. 해킹을 통해 심은 악성코드 Keylogger에 의해 취득한 정보를 지정한 e-mail, FTP경로로 실시간 또는 지정된 시간에 전송



2. 포스 단말에 접근권한이 있는 내부관리자 또는 외부 유지보수 인력에 의한 정보 취득, USB등을 통한 유출
   1) 내부정보 즉, POS 접속 패스워드 및 정보처리 절차를 알고 있어 언제라도 마음만 먹으면 정보취득 가능

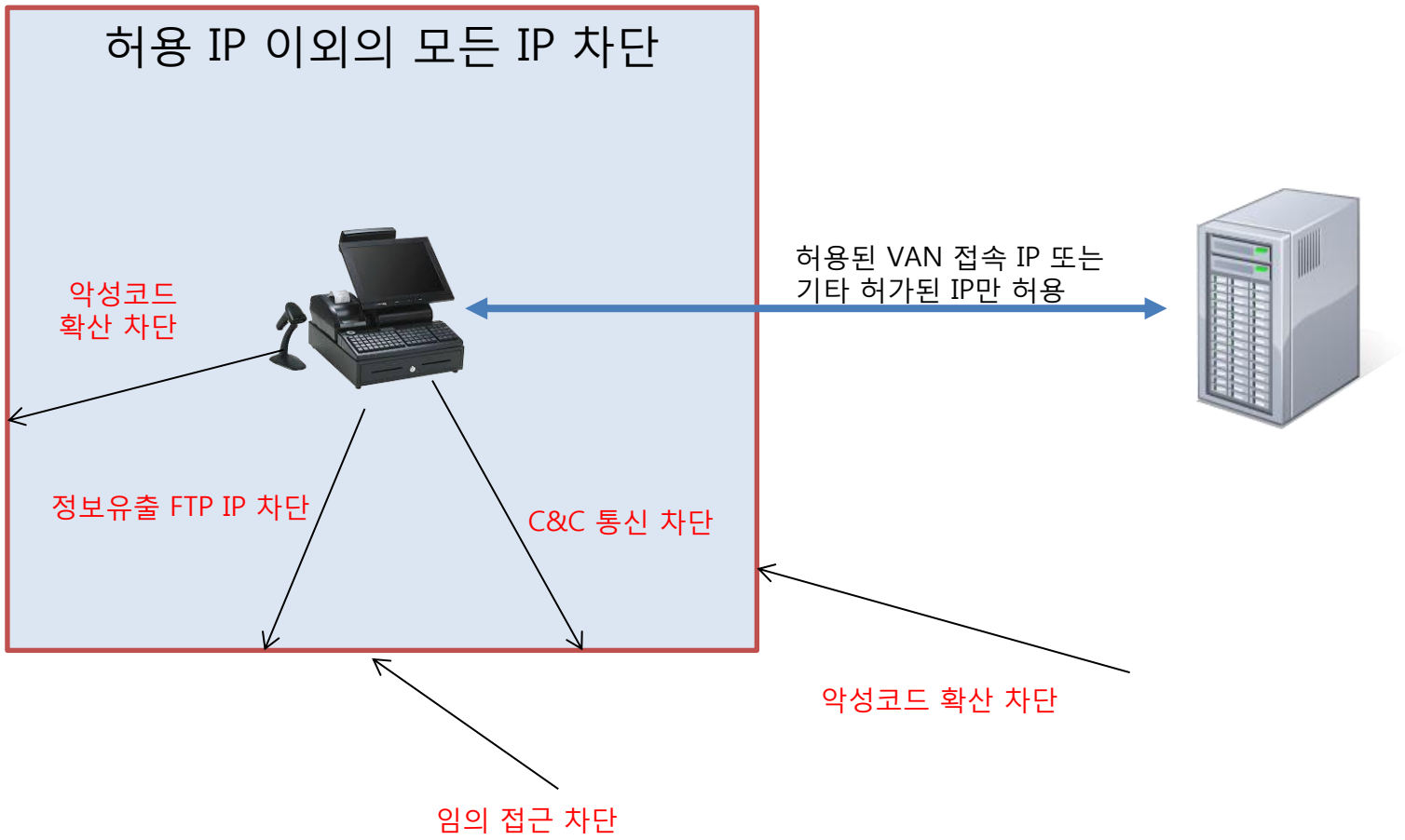
1.3 기존의 POS 단말기 해킹 차단 방안

- 카드 소유자 정보 및 민감정보 암호화
- 카드 소유자 정보에 대한 물리적 접근통제
- Virus 백신 SW설치 및 정기 업데이트
- Data 보호를 위한 네트워크 침입차단시스템 설치 및 유지관리
- 보안 시스템/프로세스 정기적 테스트 등

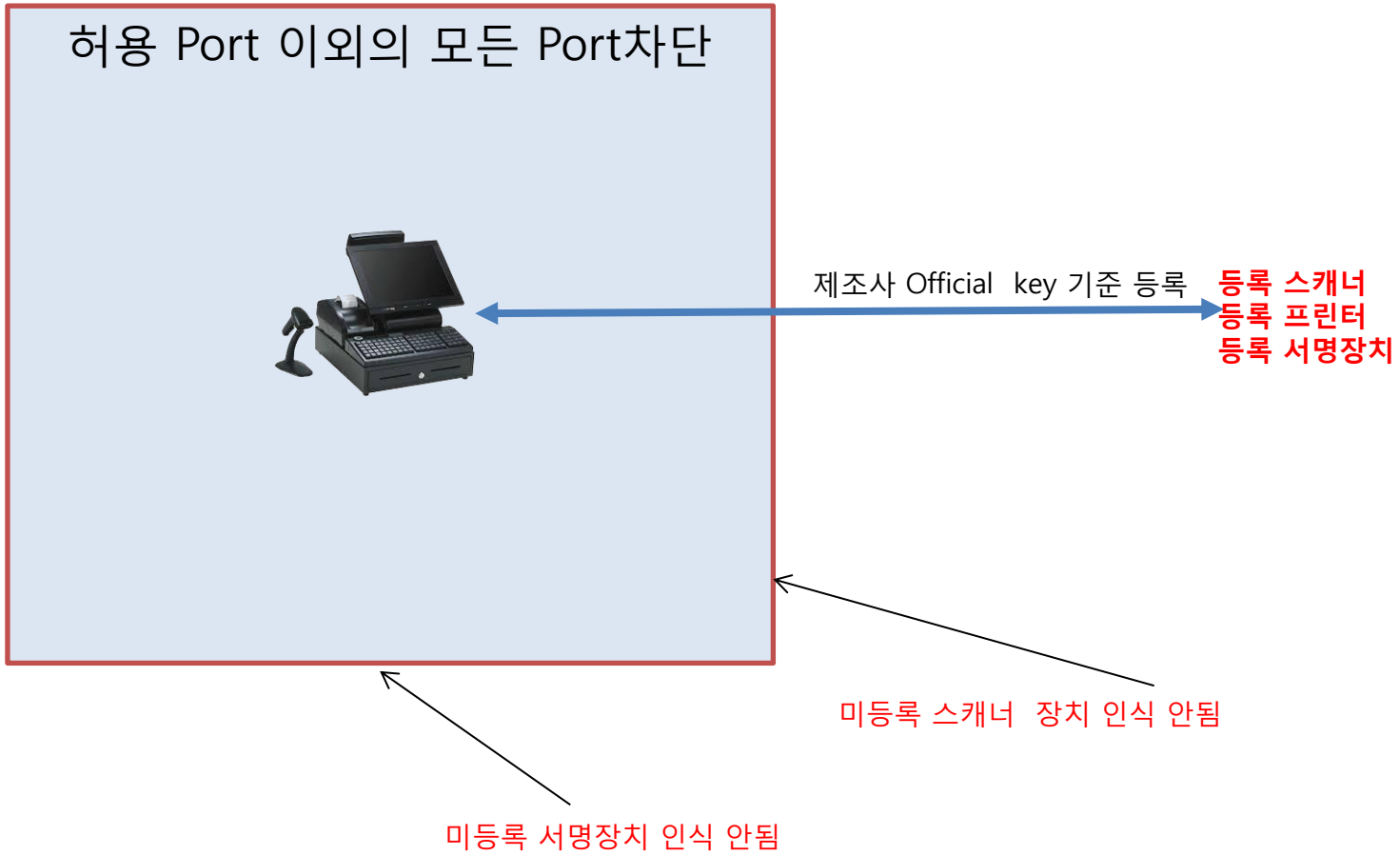
2.1 J-TOPS제공 주요 보안 기법

1. **IP 통제** : POS 단말기와 연결이 허락된 IP(본사 메인서버, PC서버등)외에 In/Out-bound 접속 차단으로 정보의 외부 유출 및 감염확산 방지
2. **Port 통제** : 스캐너, 전자서명장치, 프린터에 대한 기기 인증 및 등록 기기외 접속 차단으로 위/변조 외부 기기에 의한 정보 유출 차단
3. **Storage 통제** : USB, 네트워크 스토리지 등 정보 유출 차단
4. **Process 통제** : 주로 Embedded Windows를 사용하는 PC Process 중 등록된 White list process를 제외한 의심 process 실행 차단
5. **프로그램 통제** : 자동실행 악성코드에 의한 FTP, e-mail 등 등록된 White list 프로그램 외 임의 실행 프로그램 실행 차단
6. **내부/외부 사용자 통제** : 직접 접속이 가능한 권한 사용자에 대한 사전 등록 및 통제정책에 의한 변심 정보유출 방지
7. **POS 사용 모니터링** : 운용중인 POS에 대한 정의된 위협을 본사 또는 거점에서 24시간 모니터링하고 위협 발생시 원격에서 POS를 종료함으로 정보유출 또는 악성코드 확산 방지

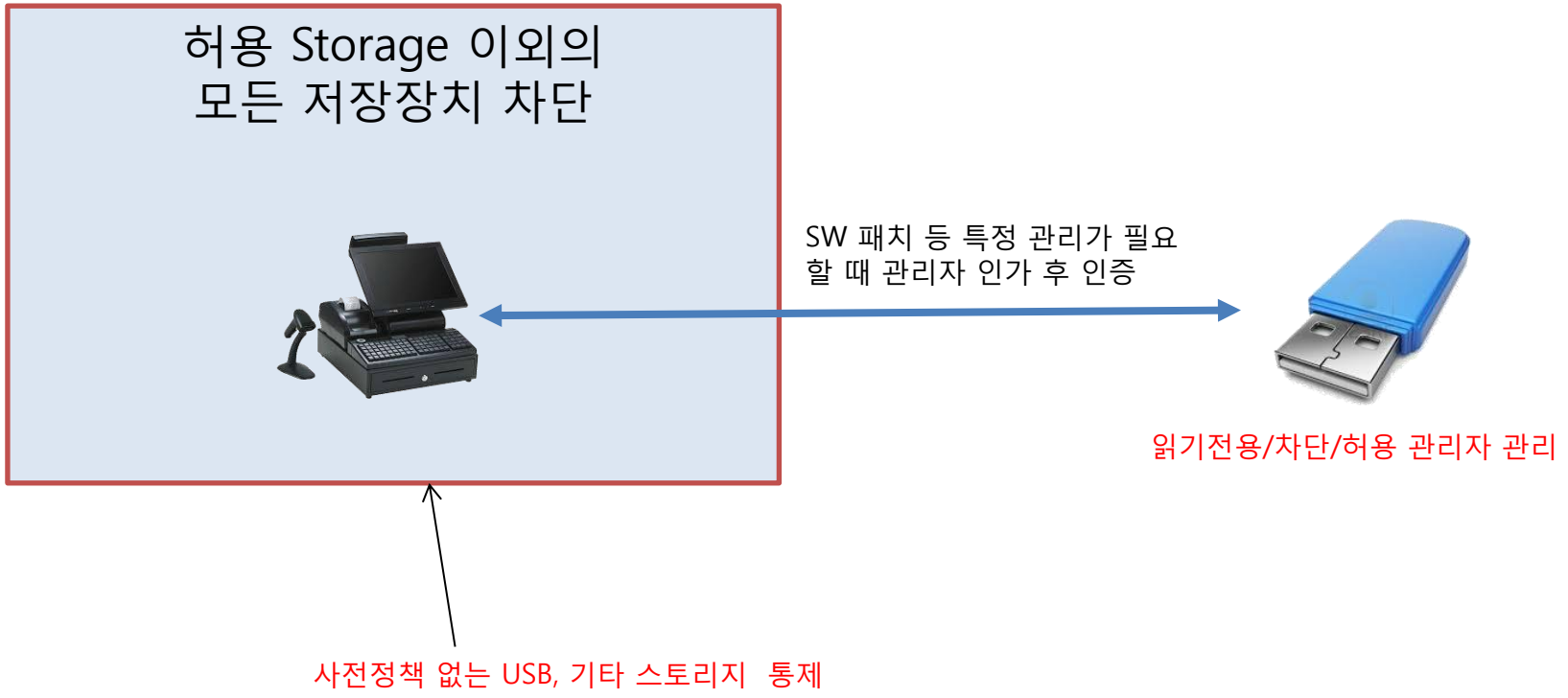
2.1.1 POS 단말기 자체 IP 통제



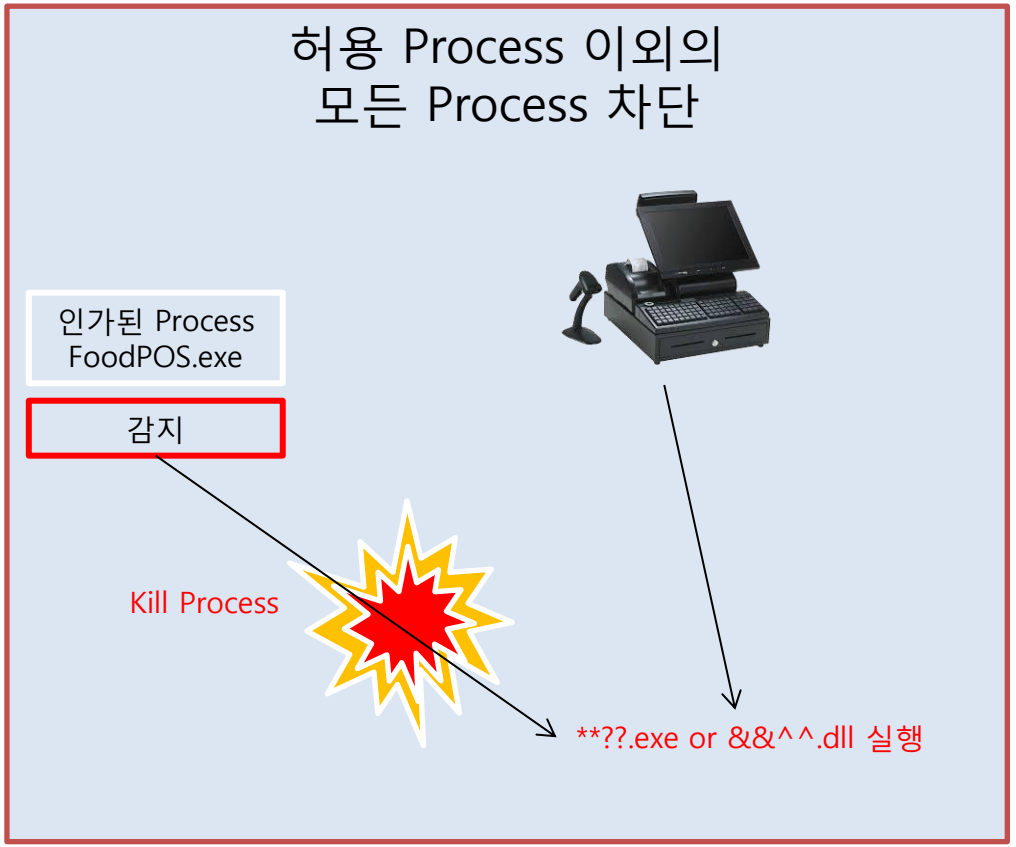
2.1.2 POS 단말기 Port통제



2.1.3 POS 단말기 Storage 통제

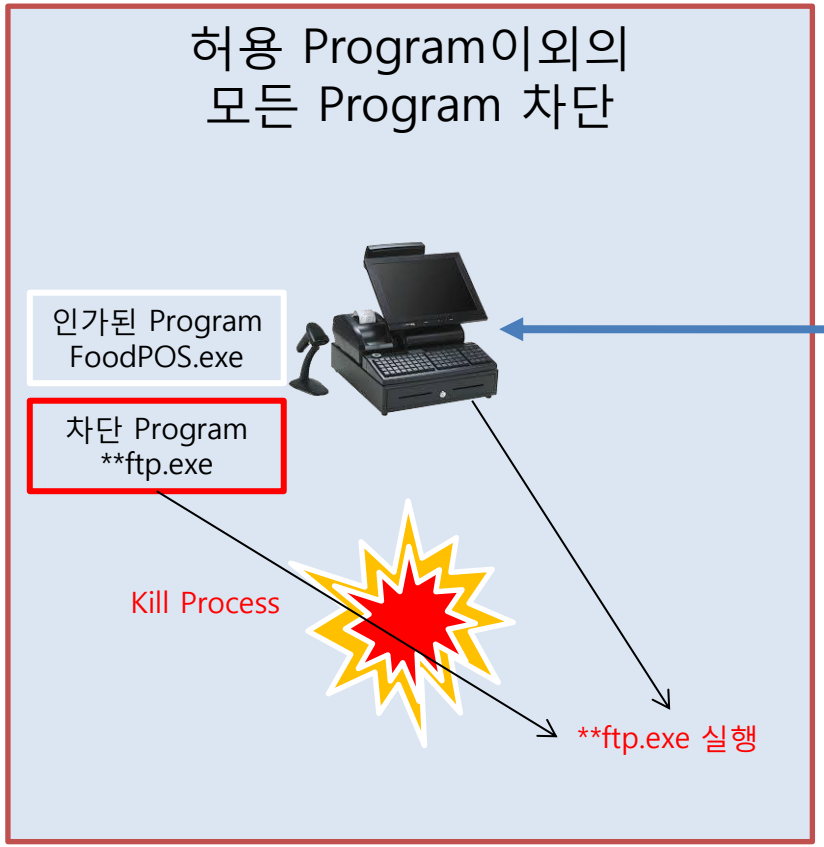


2.1.4 POS 단말기 Process 통제



의심 프로세스 발견시
실행 중지

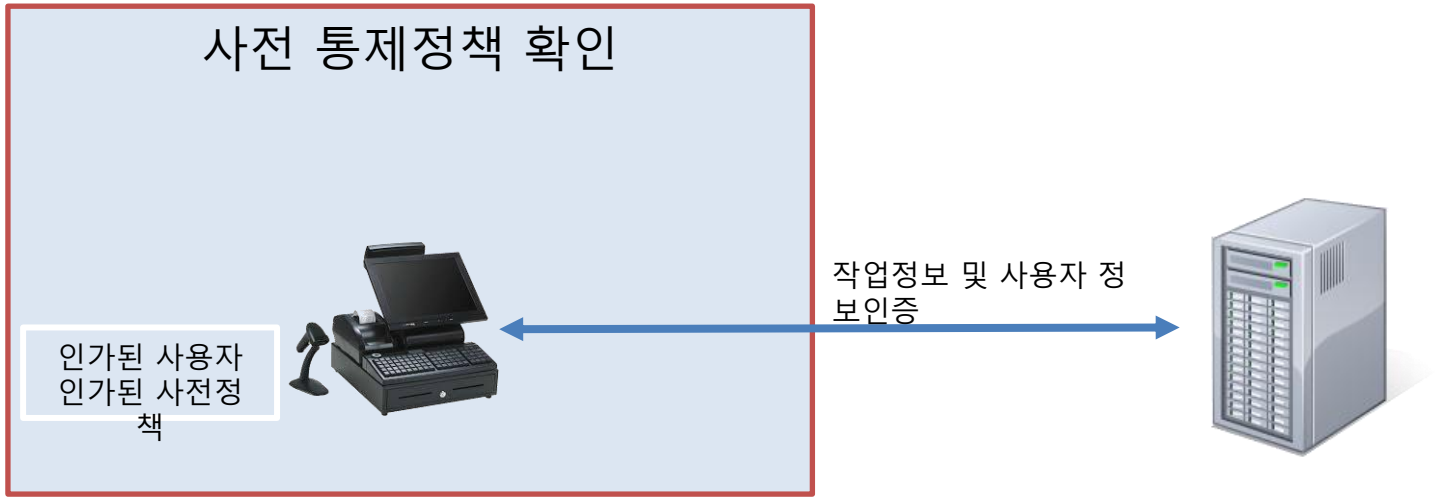
2.1.5 POS 단말기 Program통제



인가된 FoodPOS.exe

외부로 정보유출 시도
하는 process 차단

2.1.6 POS 단말기 권한 사용자 통제



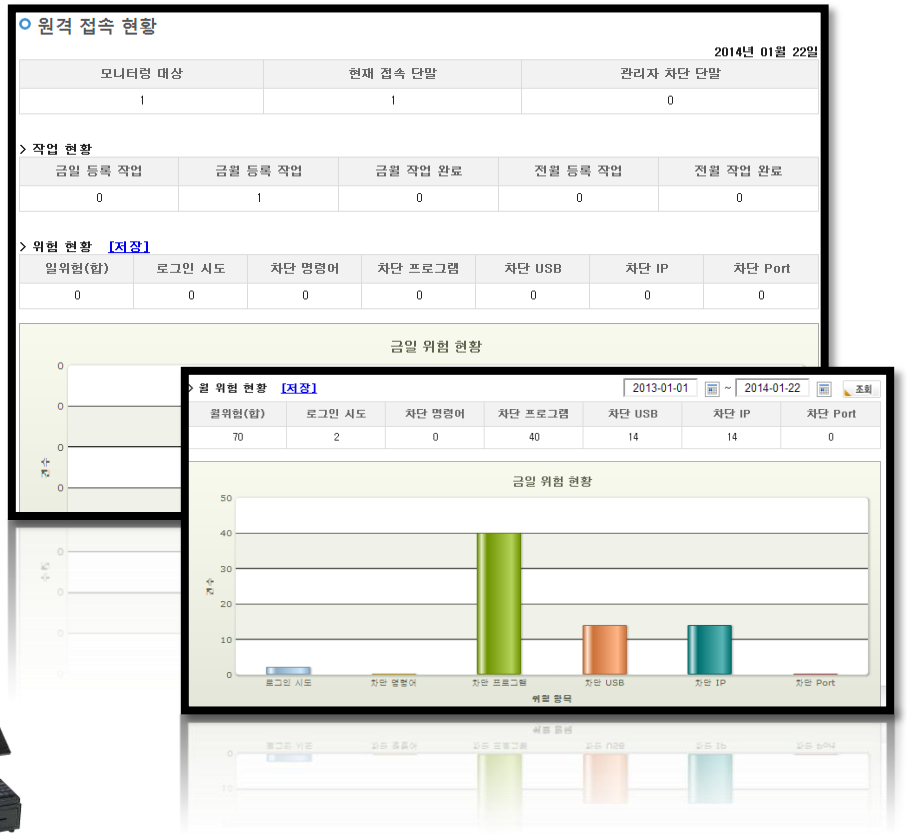
사전통제정책설정

- ✓ 설정관리자
- ✓ 작업시간
- ✓ 작업자
- ✓ 사용IP에서
- ✓ 개방할 IP는
- ✓ 차단할 명령어는?
- ✓ 차단할 프로그램은?
- ✓ 허용할 포트는?
- ✓ 허용할 매체는?

사전 정보 입력

2.1.7 POS 단말기 사용 모니터링

대기중 차단/확인중 사용/작업중



작업현황 및 통계

THANK YOU