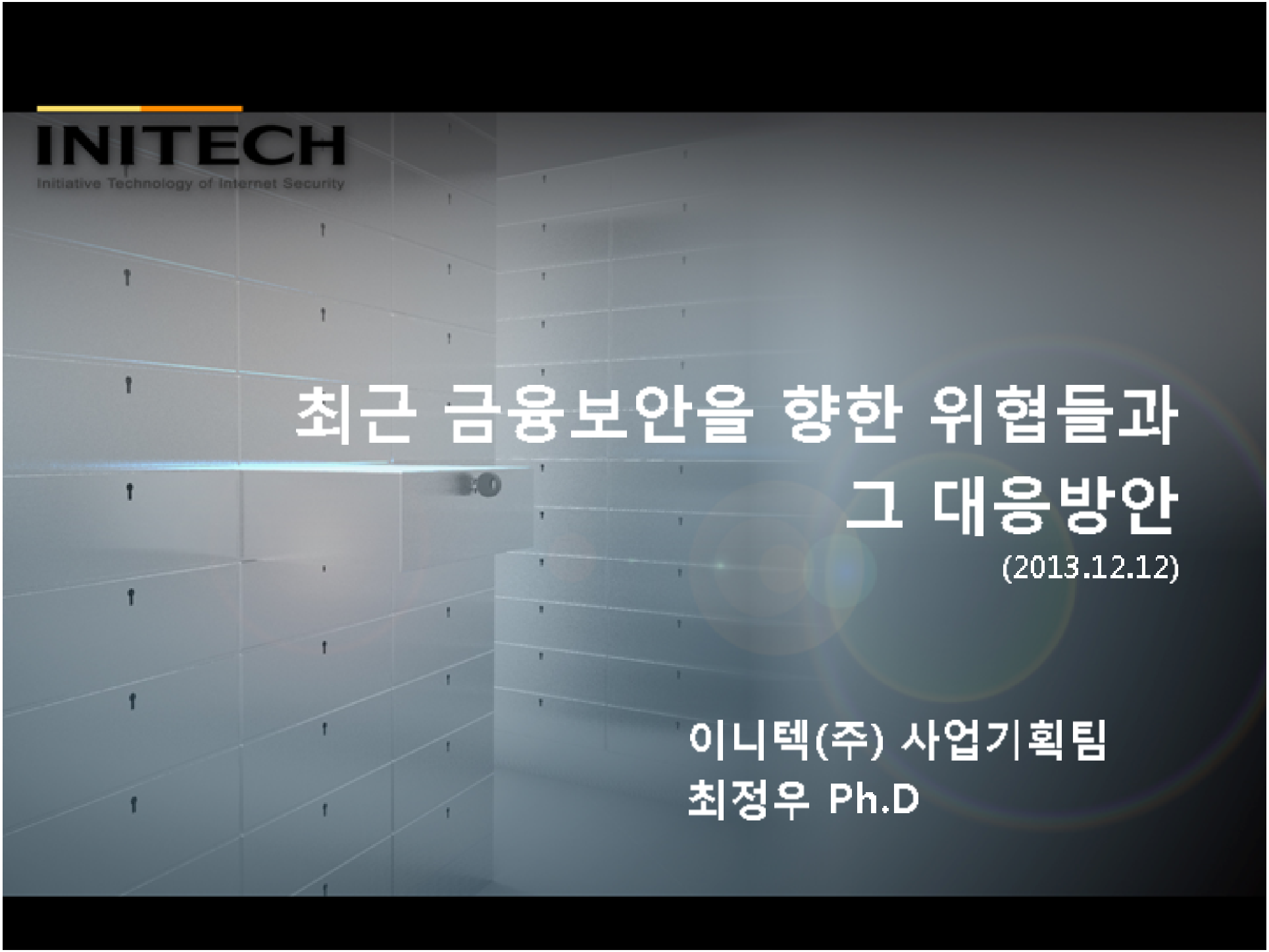
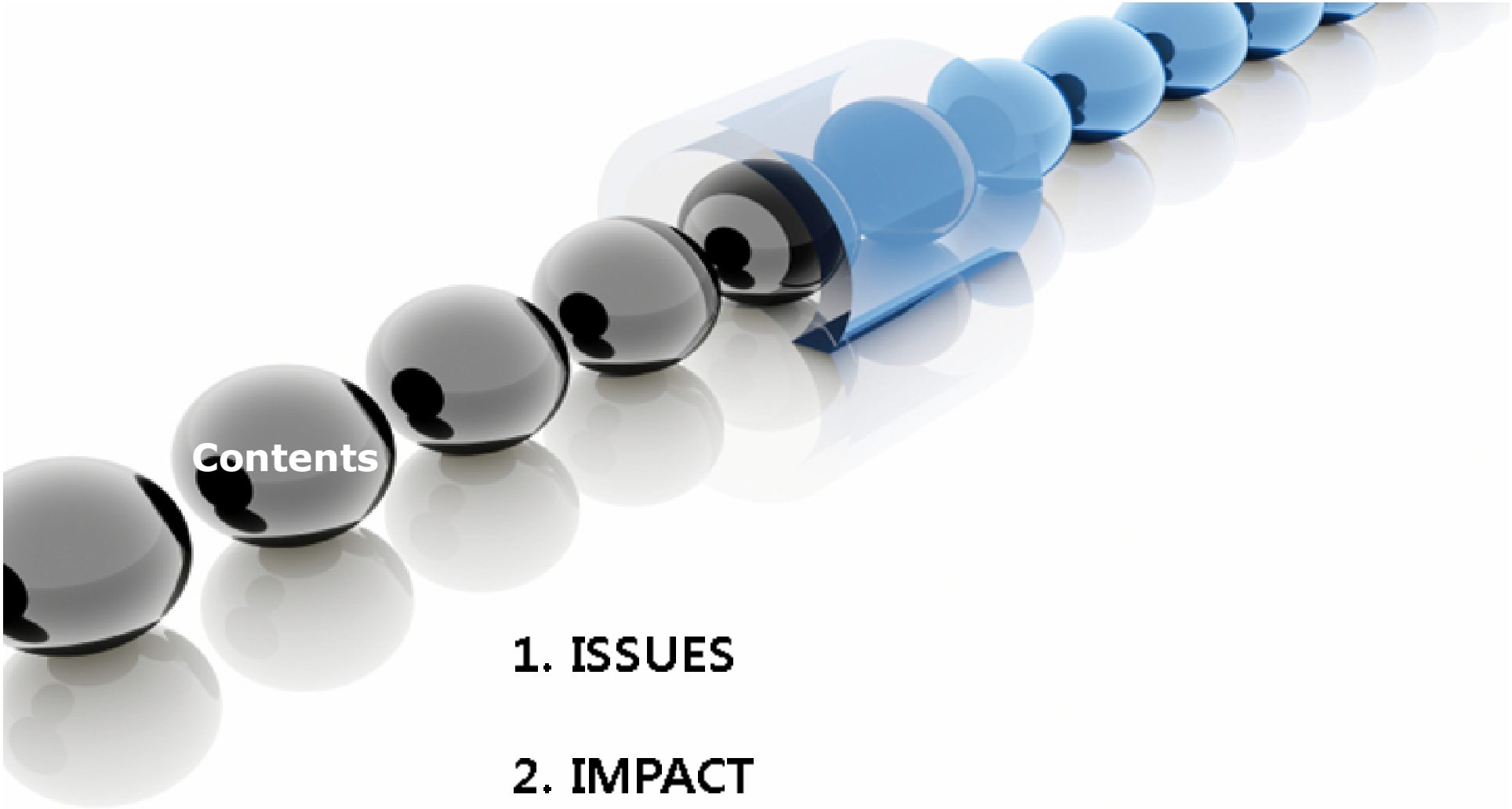


최근 금융보안을 향한 위협들과 그 대응방안

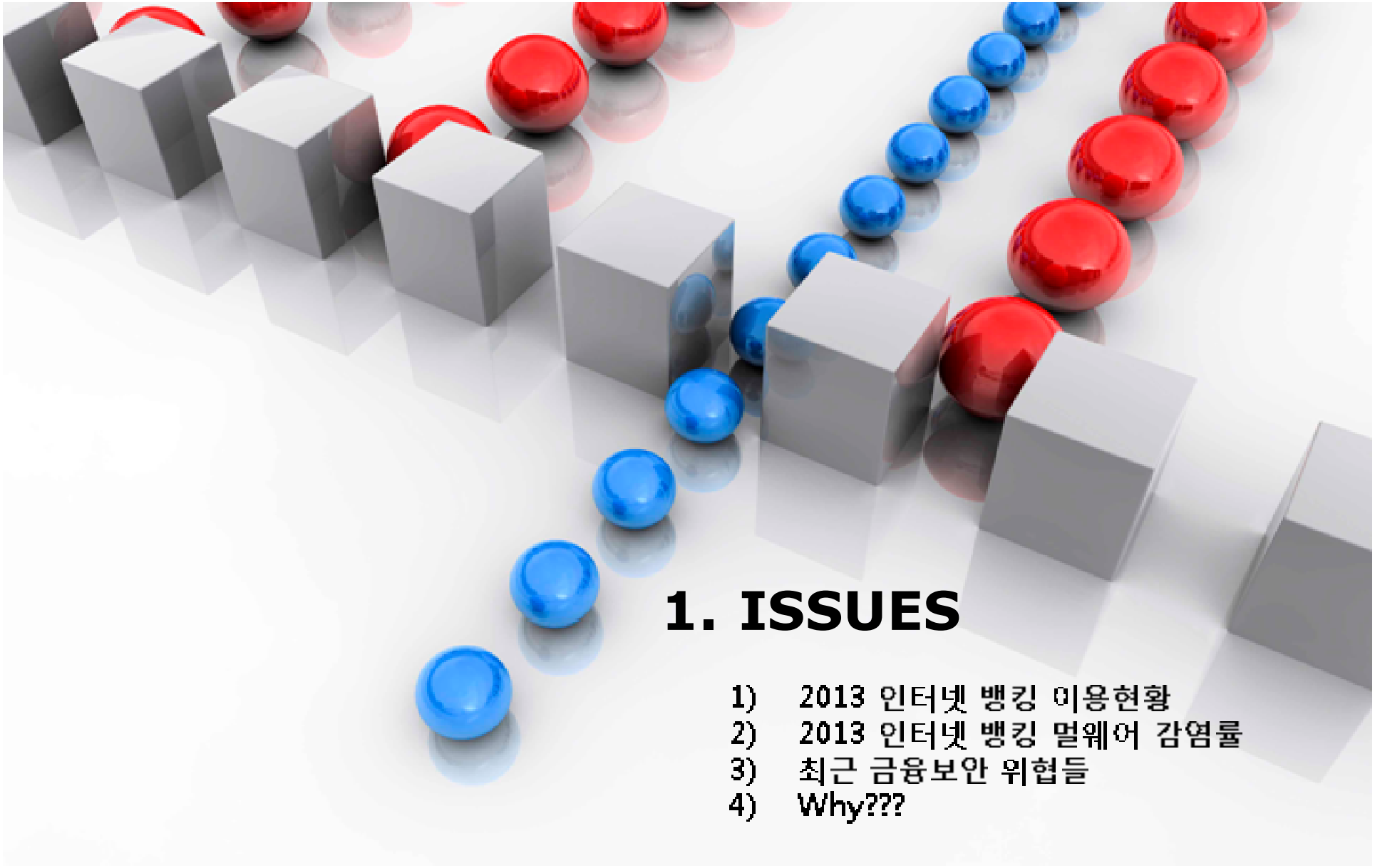
(2013.12.12)

이니텍(주) 사업기획팀
최정우 Ph.D



Contents

1. ISSUES
2. IMPACT
3. MARCKET TREND
4. ACTION



1. ISSUES

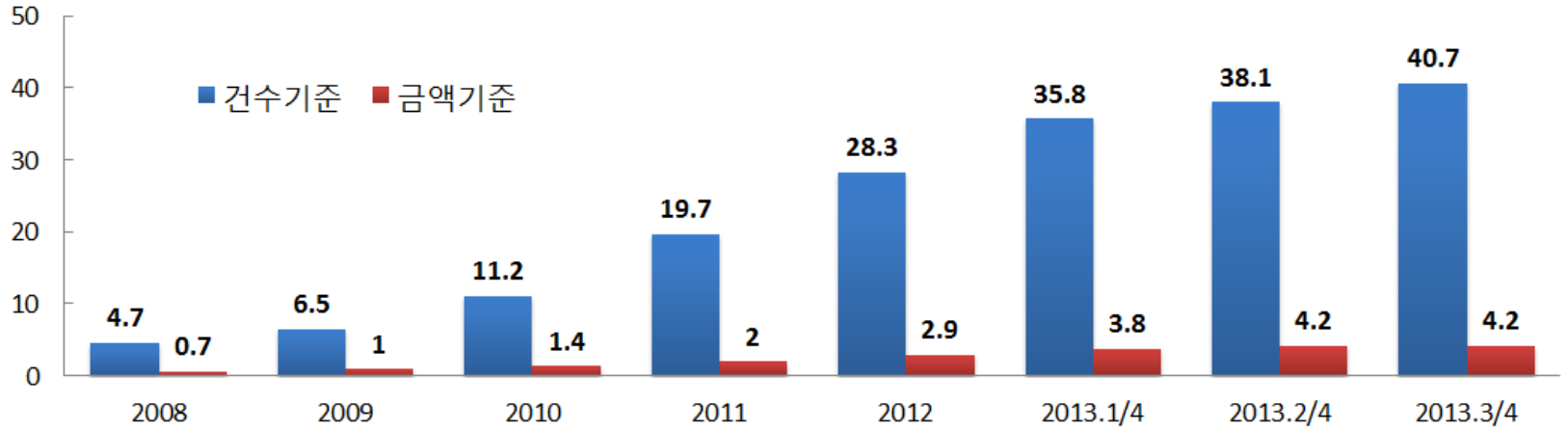
1) 2013 인터넷 뱅킹 이용현황
2) 2013 인터넷 뱅킹 멀웨어 감염률
3) 최근 금융보안 위협들
4) Why???

1) 2013 인터넷 뱅킹 이용 현황

2013년 3/4분기중 인터넷뱅킹(모바일뱅킹 포함) 이용건수(금액)는
일평균 5,476만건(33조 4,790억원)으로 전분기대비 1.4%(0.4%) 증가

전체 인터넷뱅킹 이용실적 중 모바일뱅킹 비중(건수 기준)은 40.7%로 계속 높아지고 있으나,
금액기준으로는 전분기와 동일한 4.2% 수준을 유지함

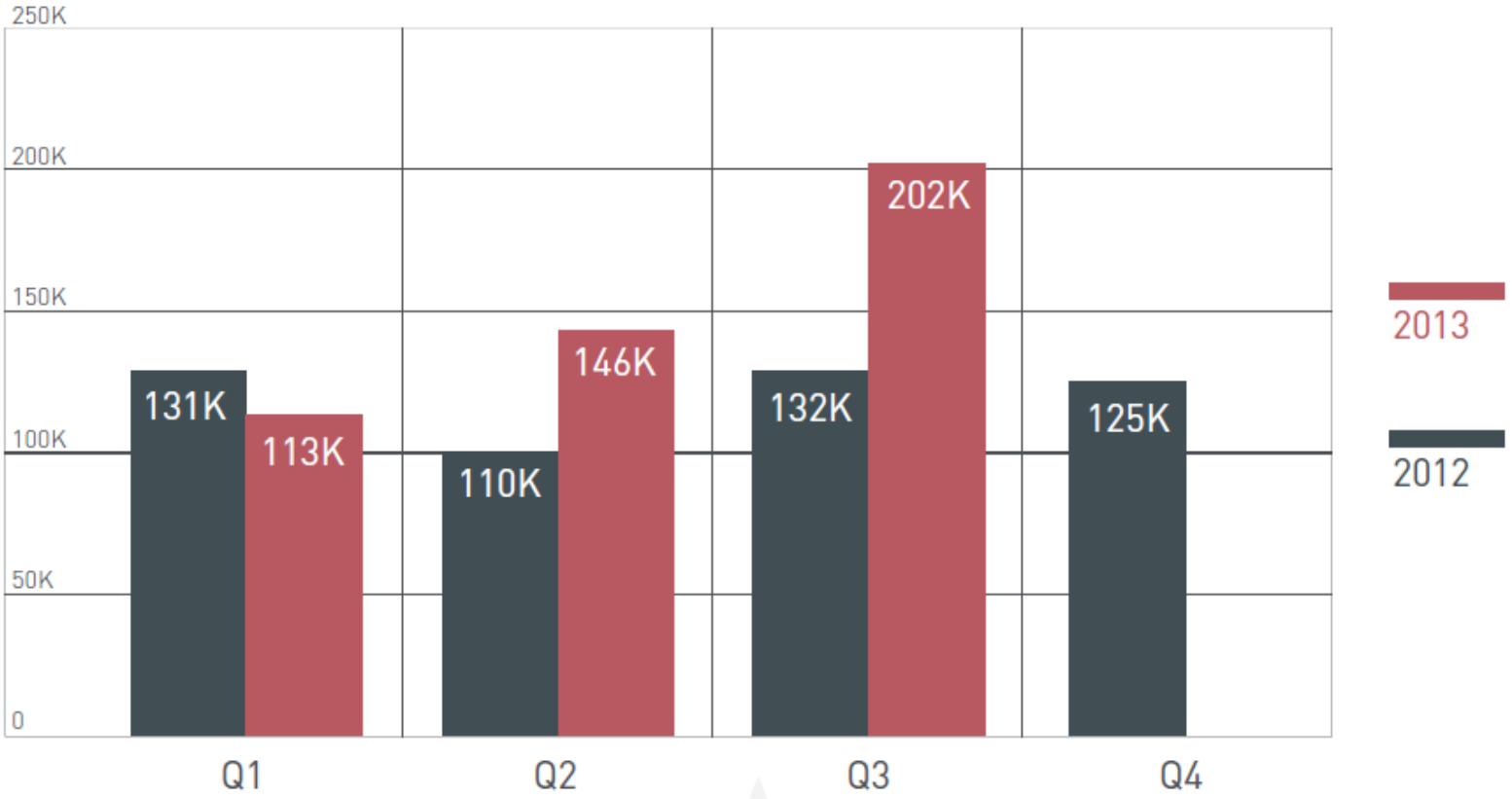
■ 모바일뱅킹의 경우 이용자 대부분이 계좌잔고 조회(전체 이용건수의 91%)와
소액 자금이체서비스(1건당 평균 70만원)를 이용



[Source : 한국은행 (2013년 11월 14일 공보 2013-11-10호)]

INITECH

2) 2013 인터넷 뱅킹 멀웨어 감염률

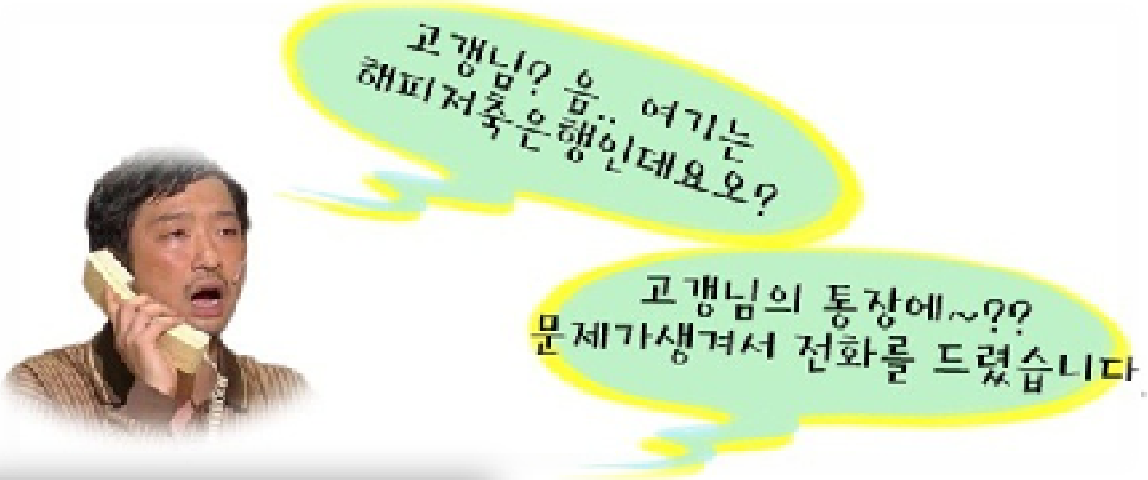


이번 분기에 탐지된 온라인 뱅킹 멀웨어의 수는 200,000건 이상이었으며 이는 2002년 이후 가장 높은 기록입니다.

[Source : TrendLabs 3Q 2013 보안 보고서]

INITECH

3) 최근 금융보안 위협들 – (1) 보이스 피싱 (Voice Phishing)



INITECH


PHISHING
SCAMS
BEWARE
OF
PHISHING

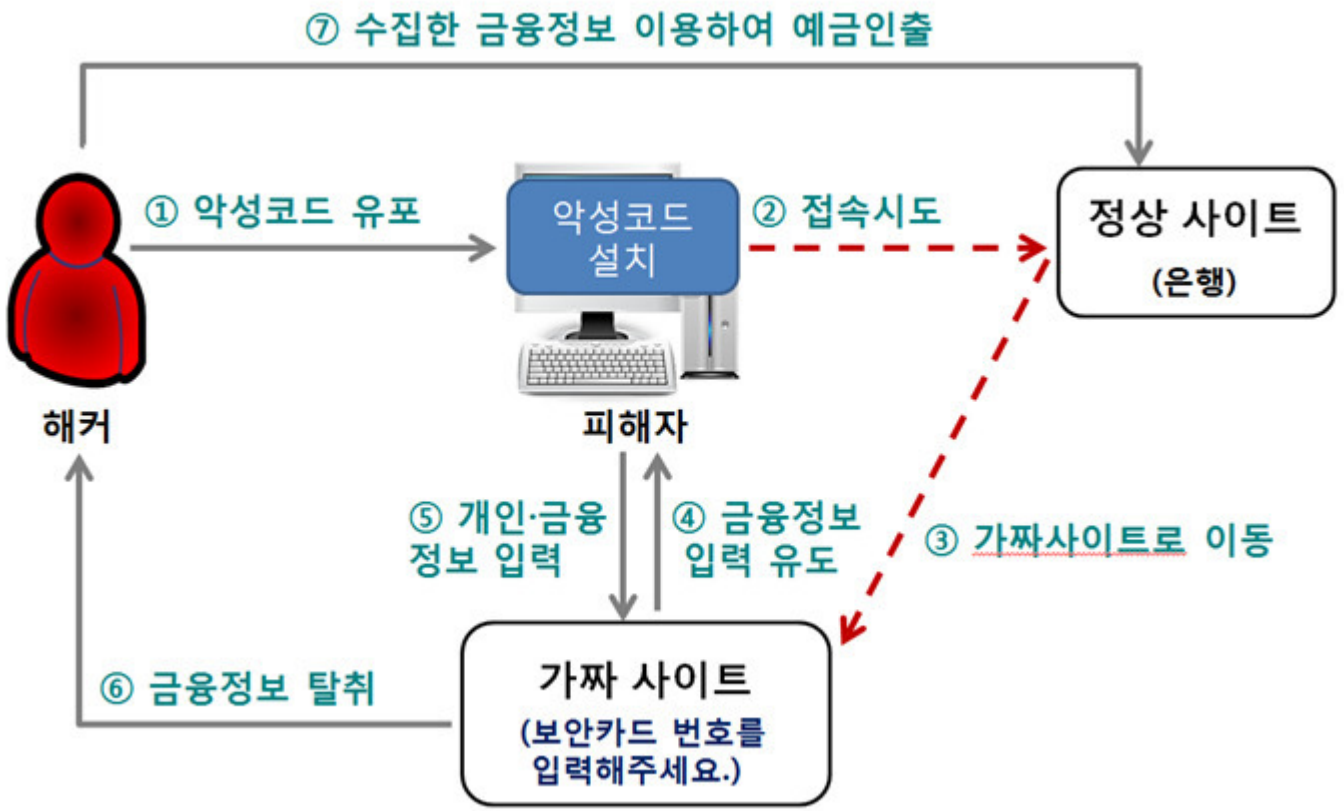
3) 최근 금융보안 위협들 – (3) 스미싱(Smishing)

[Source : Wikitree]

단축URL = 스미싱의 수단?

악성코드 유포수단으로 사용

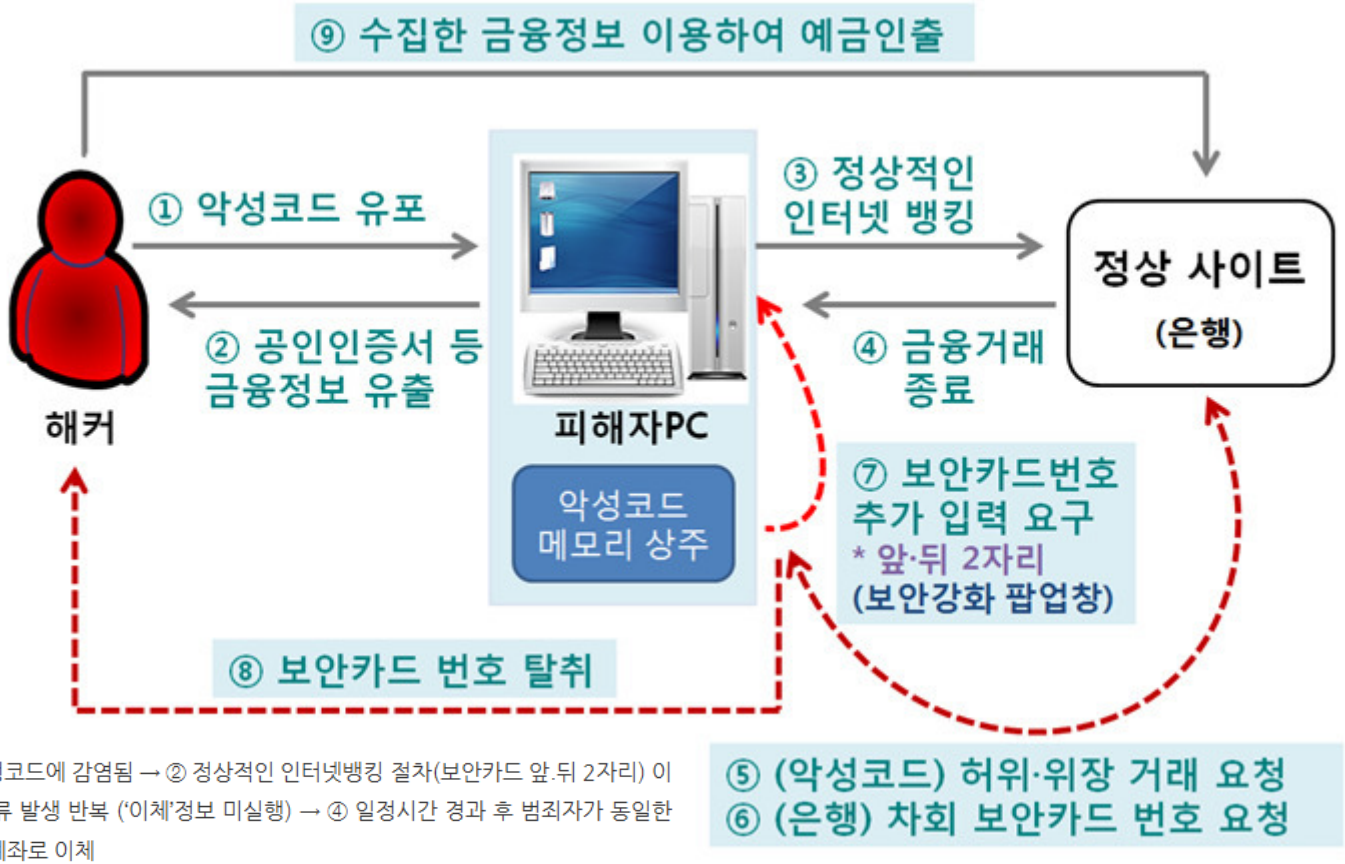
3) 최근 금융보안 위협들 – (4) 파밍(Pharming)



[Source : 경찰청]

INITECH

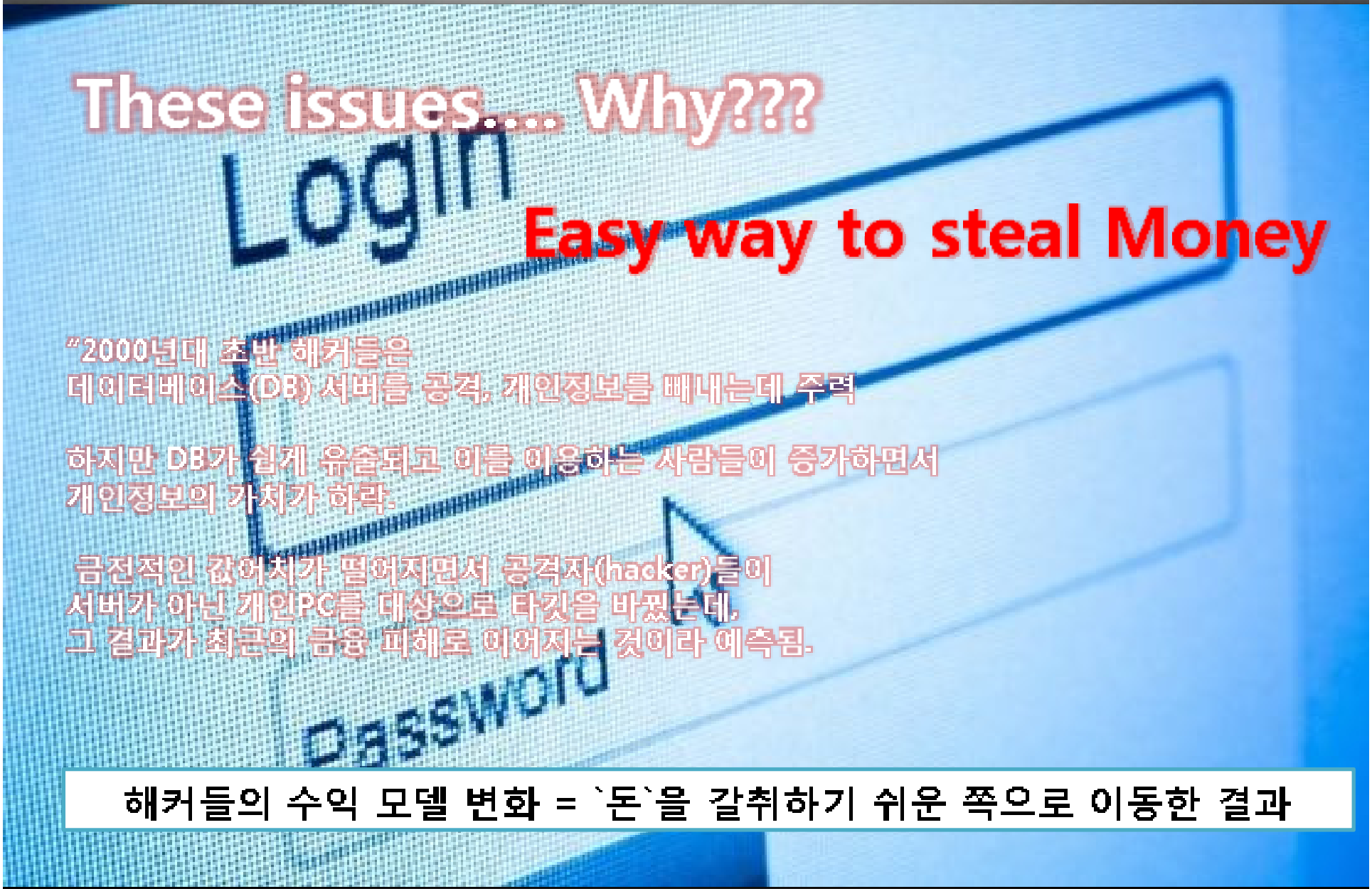
3) 최근 금융보안 위협들 – (5) 메모리 해킹 (memory hacking)



(기존) ① 사용자PC가 악성코드에 감염됨 → ② 정상적인 인터넷뱅킹 절차(보안카드 앞.뒤 2자리) 이행 후 '이체' 클릭 → ③ 오류 발생 반복 ('이체'정보 미실행) → ④ 일정시간 경과 후 범죄자가 동일한 보안카드 번호 입력, 범행계좌로 이체

(신종) ① 사용자PC가 악성코드에 감염됨 → ② 금융정보 유출 → ③ 정상적으로 인터넷뱅킹 종료 → ④ 사용자PC 메모리에 상주한 악성코드가 은행을 상대로 허위.위장 거래 요청 → ⑤ 은행사이트에서는 정상 요청으로 오인하고 다시 보안카드번호 요청 → ⑥ 악성코드 작동으로 피해자 PC상에서 보안카드번호 입력 요구(보안강화 팝업창) → ⑦ 보안카드 번호 탈취 후 거래 중단 → ⑧ 수집한 금융정보를 이용하여 예금 부당 인출

INITECH



These issues... Why???

Easy way to steal Money

"2000년대 초반 해커들은
데이터베이스(DB) 서버를 공격, 개인정보를 빼내는데 주력

하지만 DB가 쉽게 유출되고 이를 이용하는 사람들이 증가하면서
개인정보의 가치가 하락.

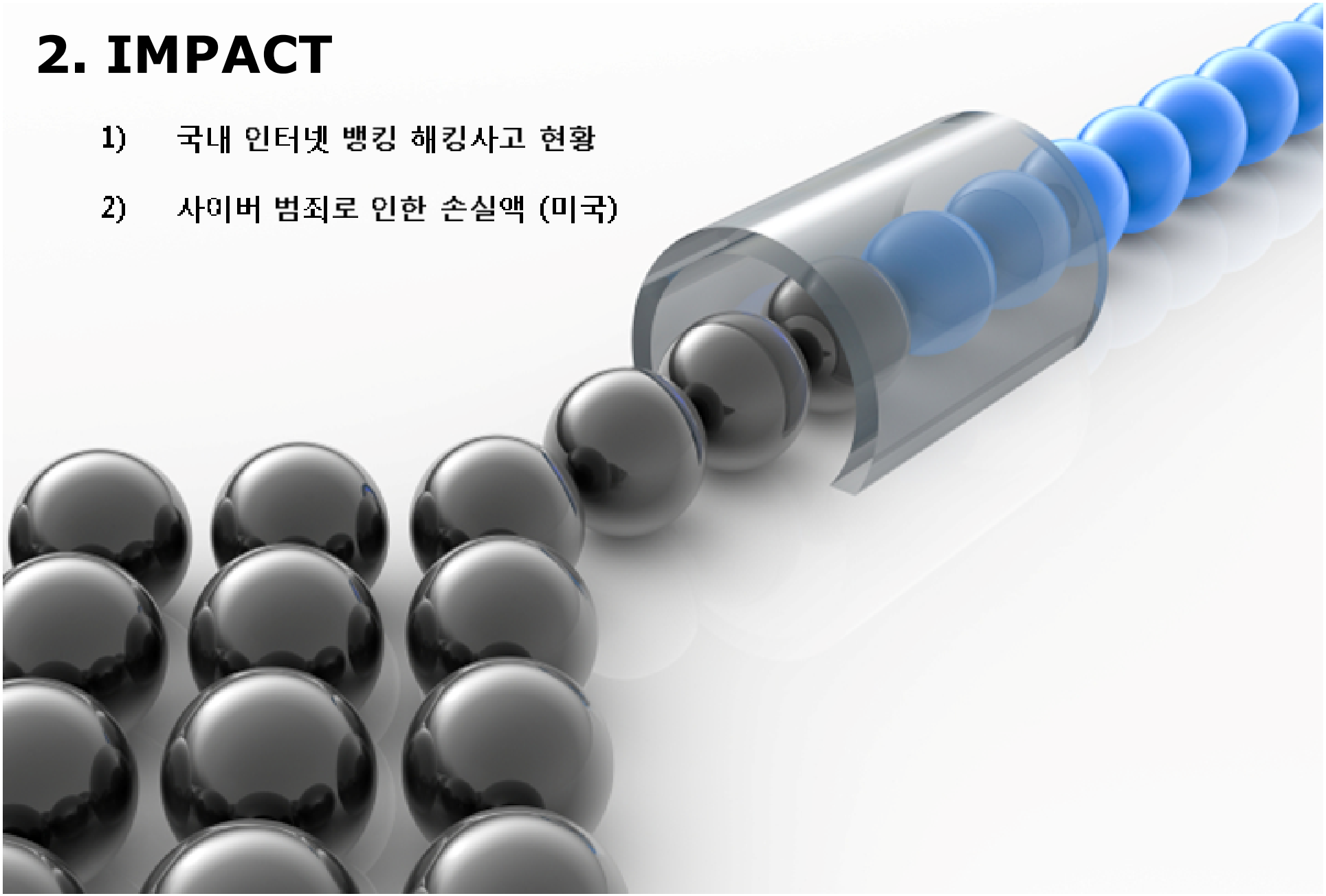
금전적인 값어치가 떨어지면서 공격자(hacker)들이
서버가 아닌 개인PC를 대상으로 타깃을 바꿨는데,
그 결과가 최근의 금융 피해로 이어지는 것이라 예측됨.

해커들의 수익 모델 변화 = `돈`을 갈취하기 쉬운 쪽으로 이동한 결과

2. IMPACT

1) 국내 인터넷 뱅킹 해킹사고 현황

2) 사이버 범죄로 인한 손실액 (미국)



1) 국내 인터넷 뱅킹 해킹사고 현황

[Source : Visual Dive, 금융감독원 '인터넷뱅킹 해킹사고 현황']

INITECH

미국 국제전략문제연구소(CSIS : *Center for Strategic and International Studies*) 曰...

사이버 범죄로 미국 경제가
매년 1000억 달러(약 111조원) 정도에 달하는 손실을 본다는 분석

추산된 사이버 범죄 피해액은
50만8000명의 일자리가 사라지는 것과 같은 규모

그렇다면 한국은 ? ? ?

INITECH

3. MARKET TREND

1) 해외 금융보안 사례

2) 국내 금융보안 사례

문답식 로그인 인증을 통한 추가적인 정보 요구

미국의2개 은행에서는 인터넷뱅킹 로그인 시 문답식 형태로 개인정보를 추가적으로 요구하고 있으며, 접속된 이용자PC에 대한 지속적인 모니터링을 통해 이용자PC 정보 또한 로그인 인증시 활용.

OTP 단말기에 추가 정보 입력을 통한 OTP 번호 생성

영국, 네덜란드, 호주 등의 일부 은행에서 제공하는OTP 단말기는 인터넷뱅킹 웹페이지 상에서 제공하는 난수값, 카드정보, 이체대상 정보 등을 추가적으로 입력해야만 OTP 번호를 생성

[Source : 금융보안연구원, '해외 인터넷뱅킹 보안현황 조사보고서' 2010]

국가	은행	인증매체	암호화 방식	비고
미국	Bank of America (BOA)	o 문답식로그인 인증 o SMS OTP o 카드 OTP	EV SSL	평가판백신 제공
	Citi Bank	o 이메일을 통한 Secure Authorization Code	SSL	
	US Bank	o 문답식로그인 인증	SSL	
영국	Barclays Bank	o 스마트카드 리더기 OTP	SSL	무료 백신 제공
영국	Royal Bank of Scotland	o 스마트카드 리더기 OTP	SSL	무료 개인방화벽제공
	Lloyds TSB Bank	o 전화인증	SSL	
네덜란드	ABN-AMRO Bank	◦ 인터넷뱅킹 전용 단말기	SSL	
	SNS Bank	◦ 토큰 OTP	SSL	
	RABO Bank	◦ 토큰 OTP	SSL	
호주	Bank of Queensland (BOQ)	o 토큰 OTP	SSL	계좌번호 및 이체금액을 추가 입력
	Commonwealth Bank	o 토큰 OTP(기업고객)	SSL	
	ANZ Bank	o 토큰 OTP(기업고객)	SSL	
싱가포르	DBS Bank	o 토큰 OTP	SSL	
	United Overseas Bank (UOB)	o 토큰 OTP o SMS OTP	EV SSL	
	OCBC Bank	o 마우스입력기 o 토큰 OTP o SMS OTP o Mobile OTP	SSL	
중국	공상은행	o USB키 인증서 o 보안카드 o SMS 인증	SSL	바이러스 백신 키보드보안프로그램 CAPTCHA 제공
	건설은행	o USB키 인증서 o 보안카드 o SMS OTP	SSL	마우스입력기 (가상키보드) CAPTCHA 제공
	중국은행	o OTP o 개인인증서	SSL	키보드보안프로그램 제공
말레이시아	RHB Bank	o 보안카드 + SMS OTP	SSL	마우스입력기 (가상키보드) 제공
	Maybank	o SMS OTP o ATM OTP o Telebanking OTP	SSL	
	AmBank	o SMS OTP o Telebanking OTP	SSL	

Bank of America

SiteKey

사이트의 위조 여부를 고객들이 쉽게 식별할 수 있도록 워터마크를 삽입하는 기술로 피싱 피해 방지

온라인뱅킹에 나타날 수 있는 각종 사이버 위협 정보도 함께 제공

HSBC

Security Device (OTP)

매번 i-bank 접속시마다 장치에서 발생되는 6digit 번호를 입력해야만 사용이 가능한 방식

INITECH

Banking & Payments ASIA

RHB launches improved security token device

22 November 2012 by BPA Editorial

[Source : timetric.com]

INITECH

Visa trials PIN payment card to fight online fraud

Banks build one-time generator into plastic

By John Leyden, 10th November 2008

The next-generation cards feature a numeric keypad on the back of a plastic card. Customers enter their PIN code to generate a one-time password. This code, displayed on a card's display panel, is then used to authenticate online purchases.

[Source : www.theregister.co.uk]

INITECH

Banking security on a USB stick

IBM Research has developed a USB device that protects online bank transactions by creating a protected channel directly to the bank's server.

IBM Research's Zone Trusted Information Channel is a USB that makes online banking safer.
(Credit: IBM Research)

[Source : cnet.com]

INITECH

무선 데이터 보안, VPN 제품군

Guard My IP
Protect your online identity

INITECH


How secure is your bank online?
We've put the customer-facing security of ten banks to the test – how does yours perform?
Top
Natwest/RBS 76%
The Co-operative Bank 72%
HSBC 72%
Bottom
Smile 68%
Halifax 67%
Santander 47%
Which?

The Telegraph http://www.telegraph.co.uk
By Jessica Winch 20 Sep 2013

Which? www.which.net/

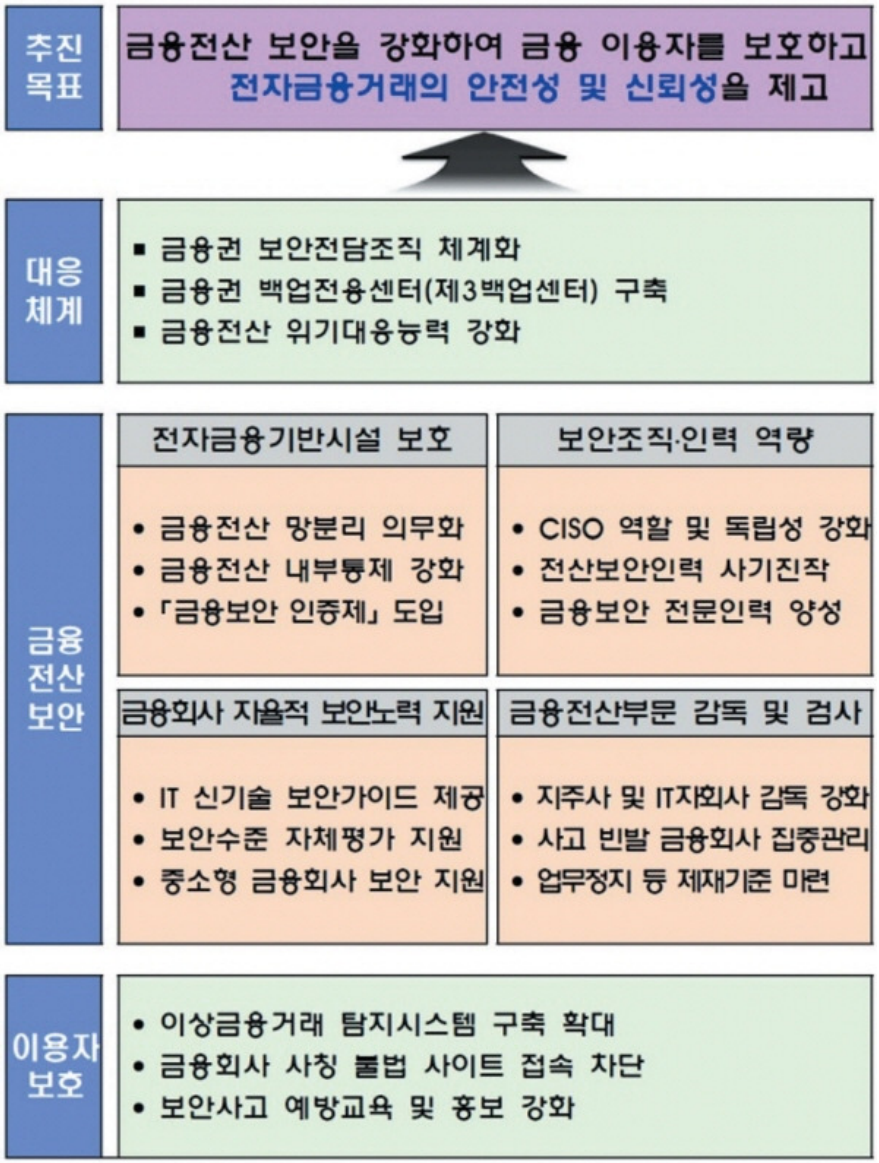
Santander has 'worst online banking security'

NatWest/RBS	**76%**
The Co-operative Bank	72%
HSBC	72%
Barclays	71%
Norwich & Peterborough BS	70%
Lloyds TSB	69%
Nationwide	69%
Smile	68%
Halifax	67%
Santander Abbey	47%

The banks were scored on
-login security,
-logout security,
-transferring money,
-changing account details,
-navigation and the encryption used to protect information as it's transmitted across the internet.

Source: Which?

The group surveyed 1,475 members in July and
two thirds of respondents said they would only access their bank account from a **home computer.**
Fewer than one in ten used their **smart phone** to visit their bank's online service.
Six in ten people believe mobile banking is **not secure enough.**



금융전산 보안 강화 종합대책

(2013년 7월 10일)

금융위, 금융전산 위기대응 체계 강화 및 전자금융기반시설 보안 강화 추구

이상금융거래 탐지시스템 구축도 확대된다. 현재 카드사에 서 운영 중인 이상거래탐지시스템을 은행이나 증권사에도 확 대 구축하고, 자체 탐지한 이상금융거래 정보를 전 금융권과 공유하는 체계를 구축한다. 국내 금융회사를 사칭하는 해외 불법사이트로 접속되는 것을 차단하기 위해 인터넷 사업자의 불법 및 유해사이트 차단 시스템이 활용되며, 영업점에서 유 의사항이 담긴 홍보자료 배포와 보안사고 예방법 설명 화면 노 출 등 이용자 교육도 강화된다.

금융위원회
FINANCIAL SERVICES COMMISSION

INITECH

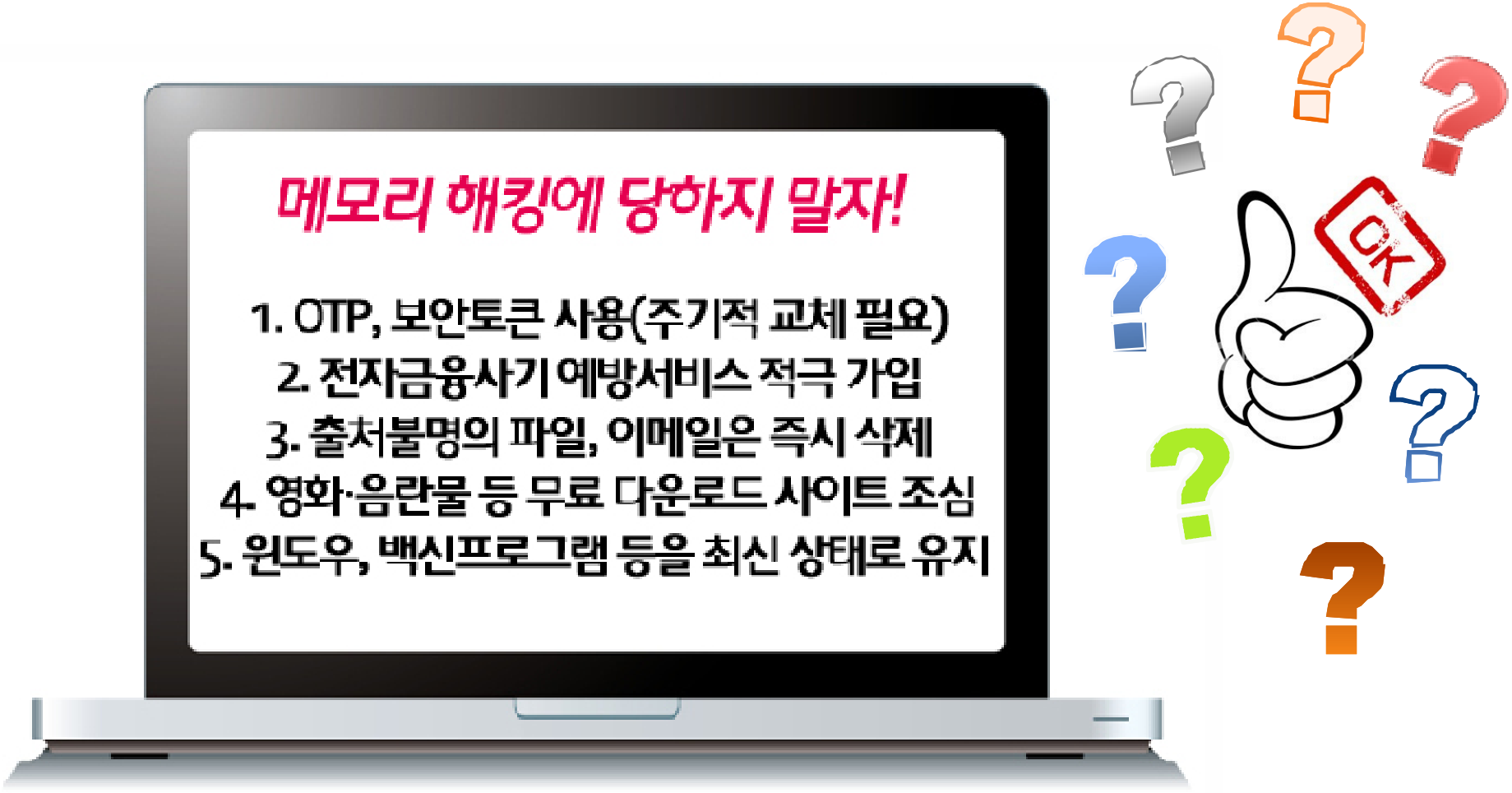
금융위와 미래부 등 범부처 대책협의회의 '신·변종 전기통신금융사기 피해방지 종합대책' (2013년 12월 3일)

- 보안기능을 강화한 메모리해킹 대응방안
- 해킹에 이용된 계좌 지급정지제도를 강화, 제2금융권까지 적용대상을 확대
- 입금계좌지정제를 개선, 사전에 지정한 입금계좌로는 기존대로 거래를 진행하고, 미지정 입금계좌로는 소액이체만 가능토록

"신변종 사기는 계속해서 나오고 있다"며 "새로운 사기수법이 나오면 그때그때 신속히 대응할 수 있는 대책을 내놓고 발표하겠다"는 입장

금융위원회
FINANCIAL SERVICES COMMISSION

미래창조과학부


메모리 해킹에 당하지 말자!
1. OTP, 보안토큰 사용(주기적 교체 필요)
2. 전자금융사기 예방서비스 적극 가입
3. 출처불명의 파일, 이메일은 즉시 삭제
4. 영화·음란물 등 무료 다운로드 사이트 조심
5. 윈도우, 백신프로그램 등을 최신 상태로 유지
OK

[Source : 경찰청]

PC 지정과 스마트폰 이용한 투팩터 인증으로 대응해야... ?

거래연동 OTP를 금융권에서 도입해야... ?

금융거래 전용 브라우저... ?

INITECH

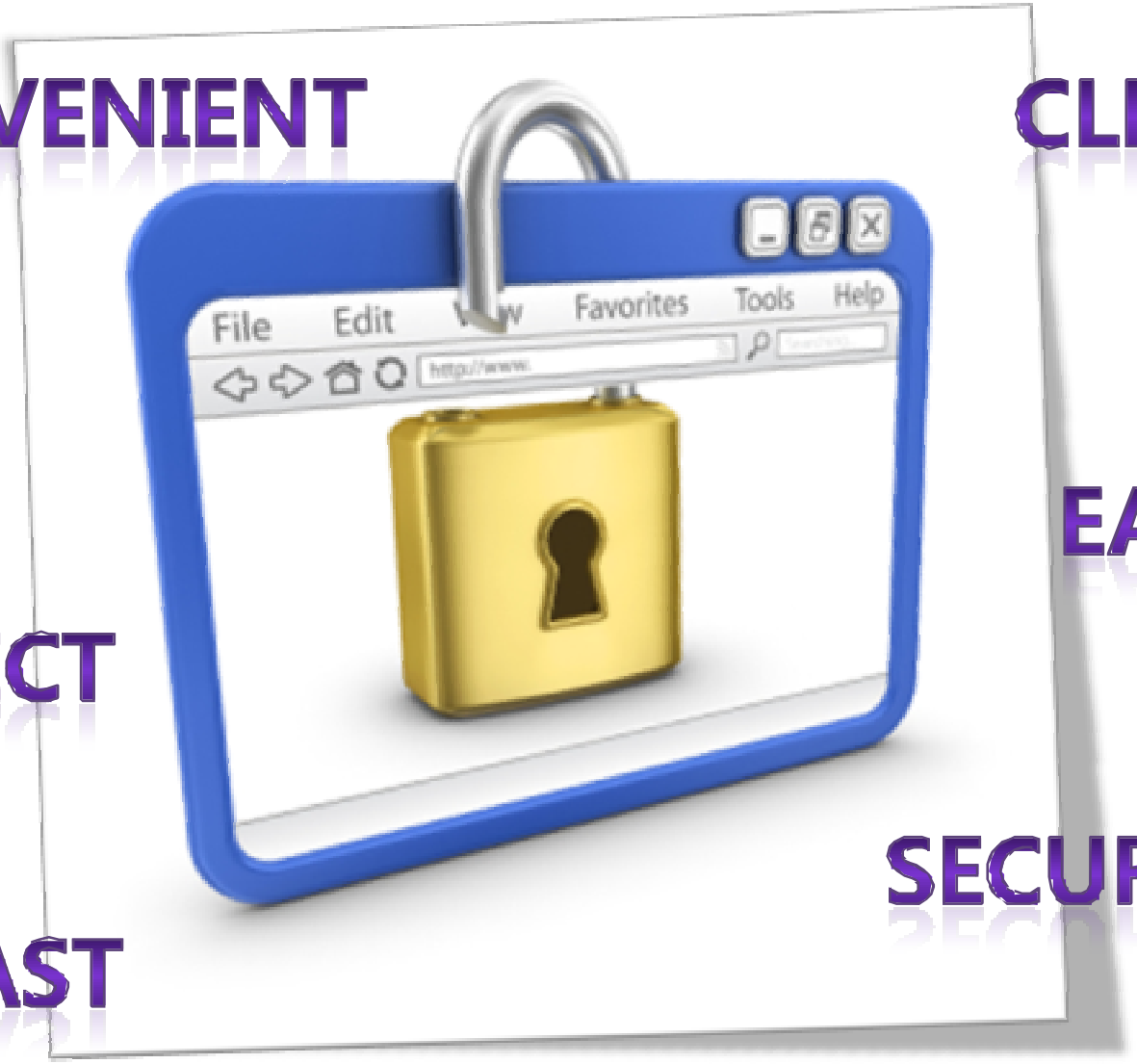
국내 전자금융 거래 편리성은 하락?

고객 편의성 측면 보다는
해당 보안을 강화하고
전자금융거래 체계 자체를 재정비?

INITECH

CONVENIENT

CLEAN



EASY

PROTECT

SECURE

FAST

INITECH

4. ACTION

1) 이니텍의 대응방안
   (1) 웹 위변조, 메모리해킹 방지 솔루션
   (2) 파밍방지 서비스
   (3) 클린 브라우저 솔루션

2) 앞으로의 고민...

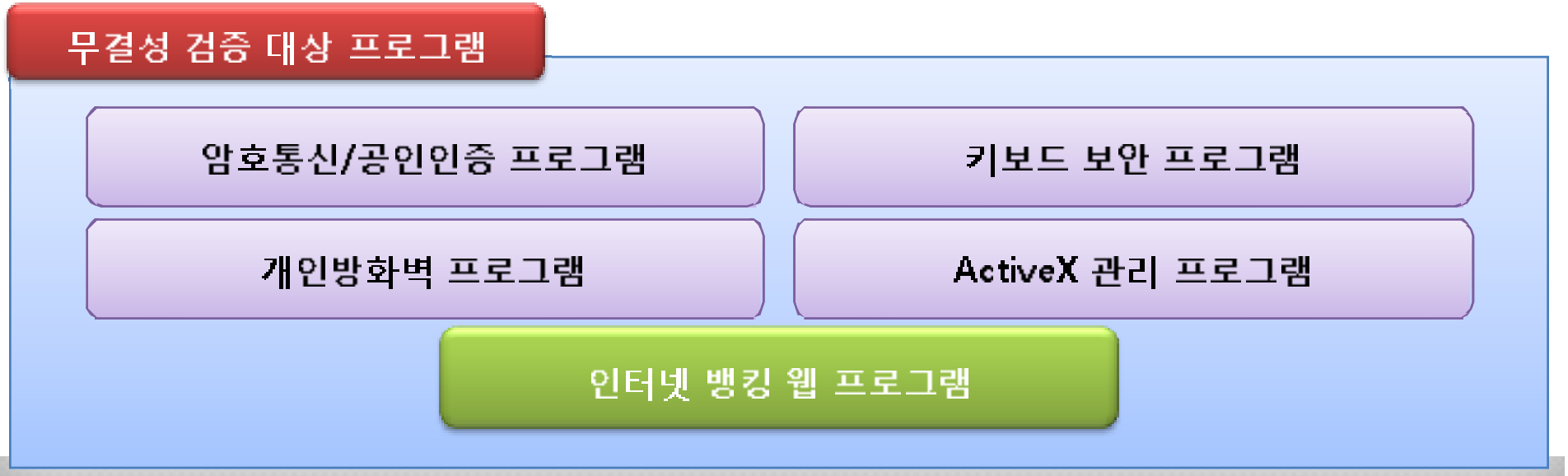

1. 웹 위변조, 메모리해킹 방지 솔루션
2. 파밍방지 서비스
3. 클린 브라우저 솔루션

금융회사 정보기술(IT)부문 보호업무 모범 규준(2011.11)

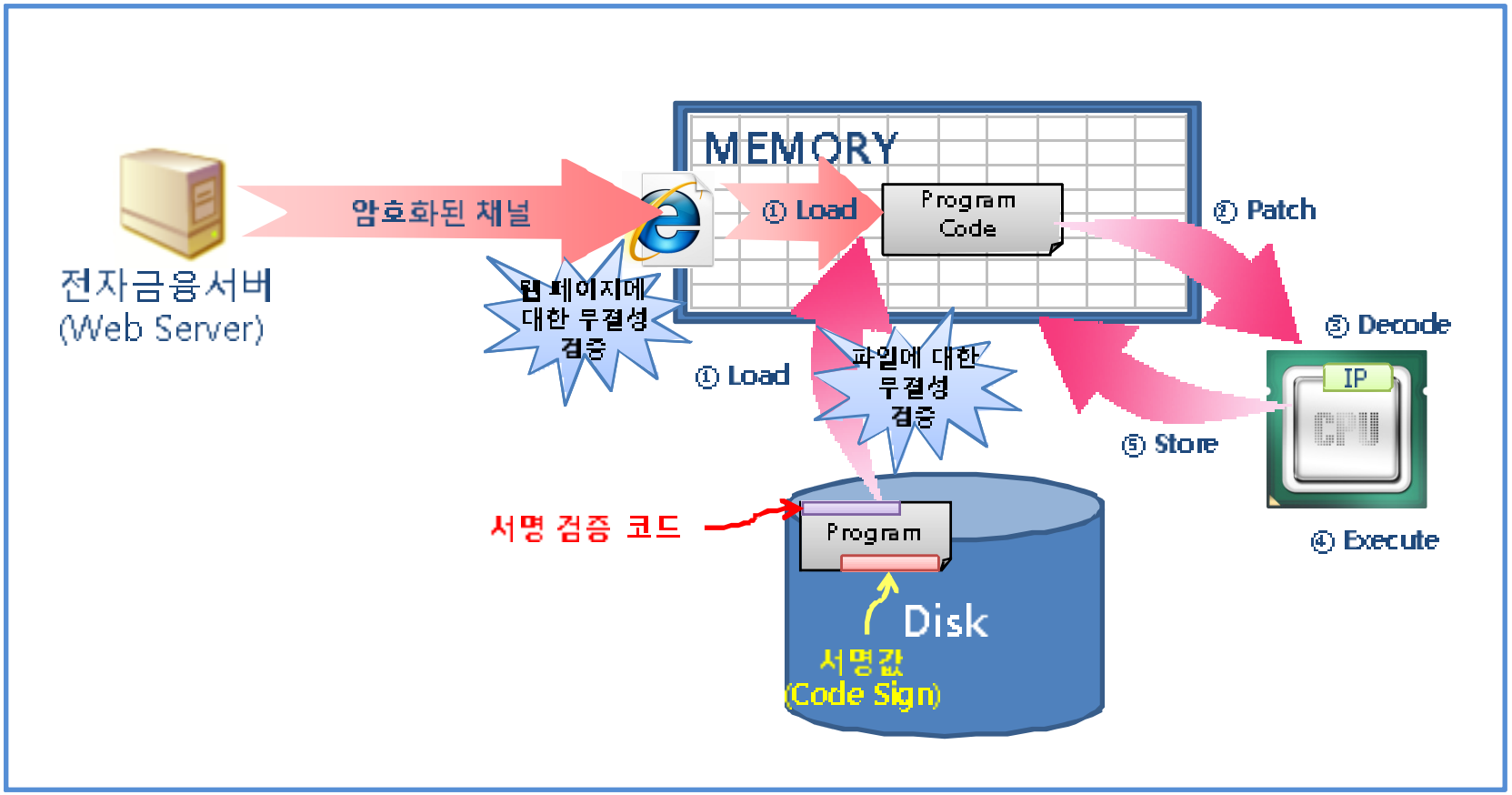
⑧ (전자금융거래프로그램검증) 금융회사 등은 악성코드를 이용한 전자금융사고에 대비하여 전자금융거래에서 이용자에게 제공하거나 거래를 처리하기 위한 **전자금융거래프로그램(거래전문포함)의 위, 변조 여부 등 무결성을 검증할 수 있는 방법을 제공**하여야 한다.

☞ 전자금융거래프로그램 검증 방법(예시) : 금융회사 등이 배포한 프로그램과 PC, 스마트폰 등 이용자 전자적 장치에서 구동되는 프로그램의 파일크기, 해쉬 결과 확인 등을 통해 프로그램 무결성 검증 실시

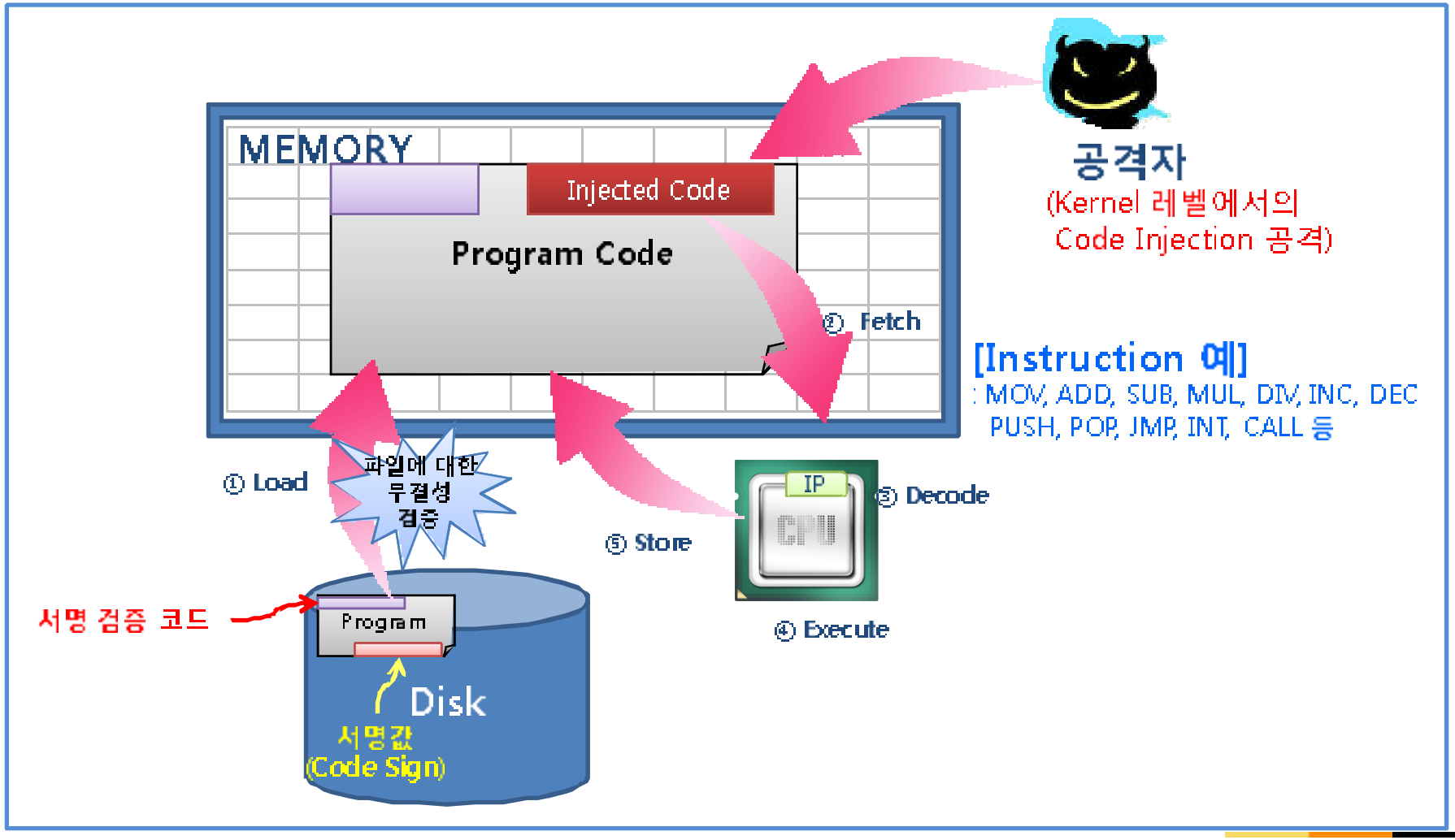
➔ 인터넷 뱅킹을 위해 사용되는 모든 프로그램의 무결성을 보증해야 함.



전자금융거래프로그램의 무결성 검증 방법



메모리 해킹 (?)

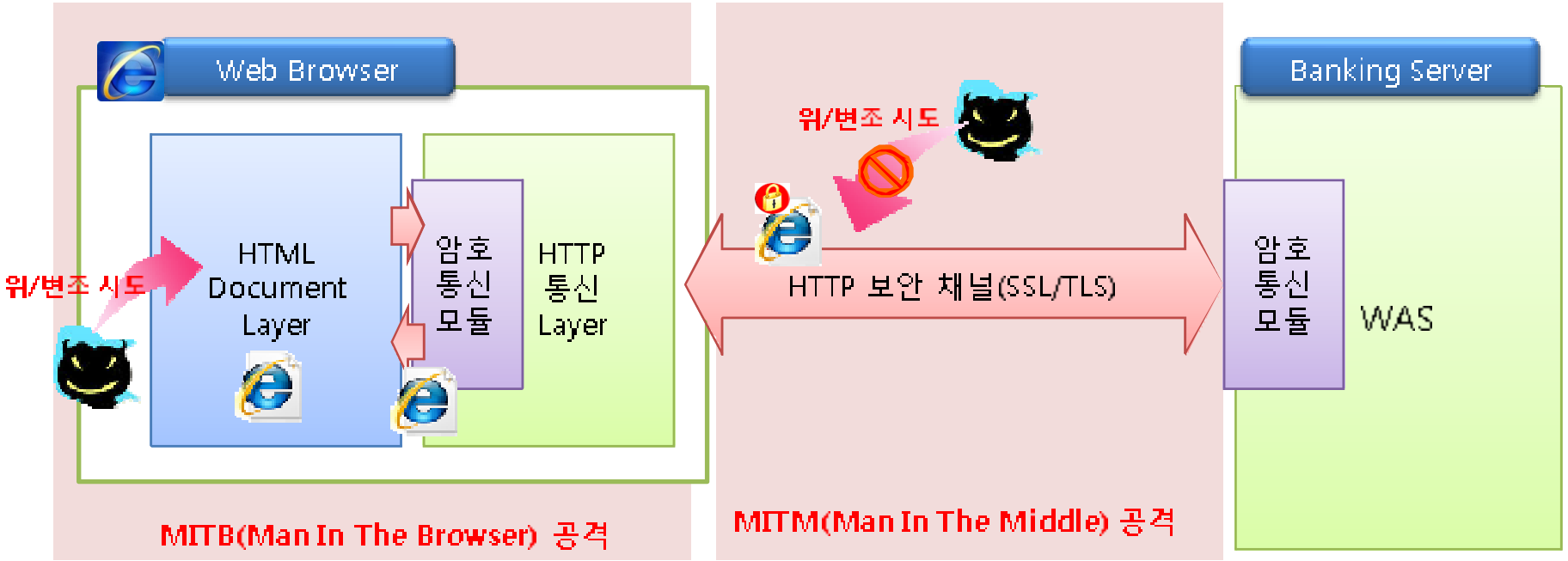

MEMORY
Injected Code
Program Code
② Fetch
공격자
(Kernel 레벨에서의
Code Injection 공격)
[Instruction 예]
: MOV, ADD, SUB, MUL, DIV, INC, DEC
PUSH, POP, JMP, INT, CALL 등
① Load
파일에 대한
무결성
검증
③ Decode
IP
CPU
⑤ Store
④ Execute
서명 검증 코드
Program
Disk
서명값
(Code Sign)

MITB(Man-in-the-browser) 공격과 Web Injection

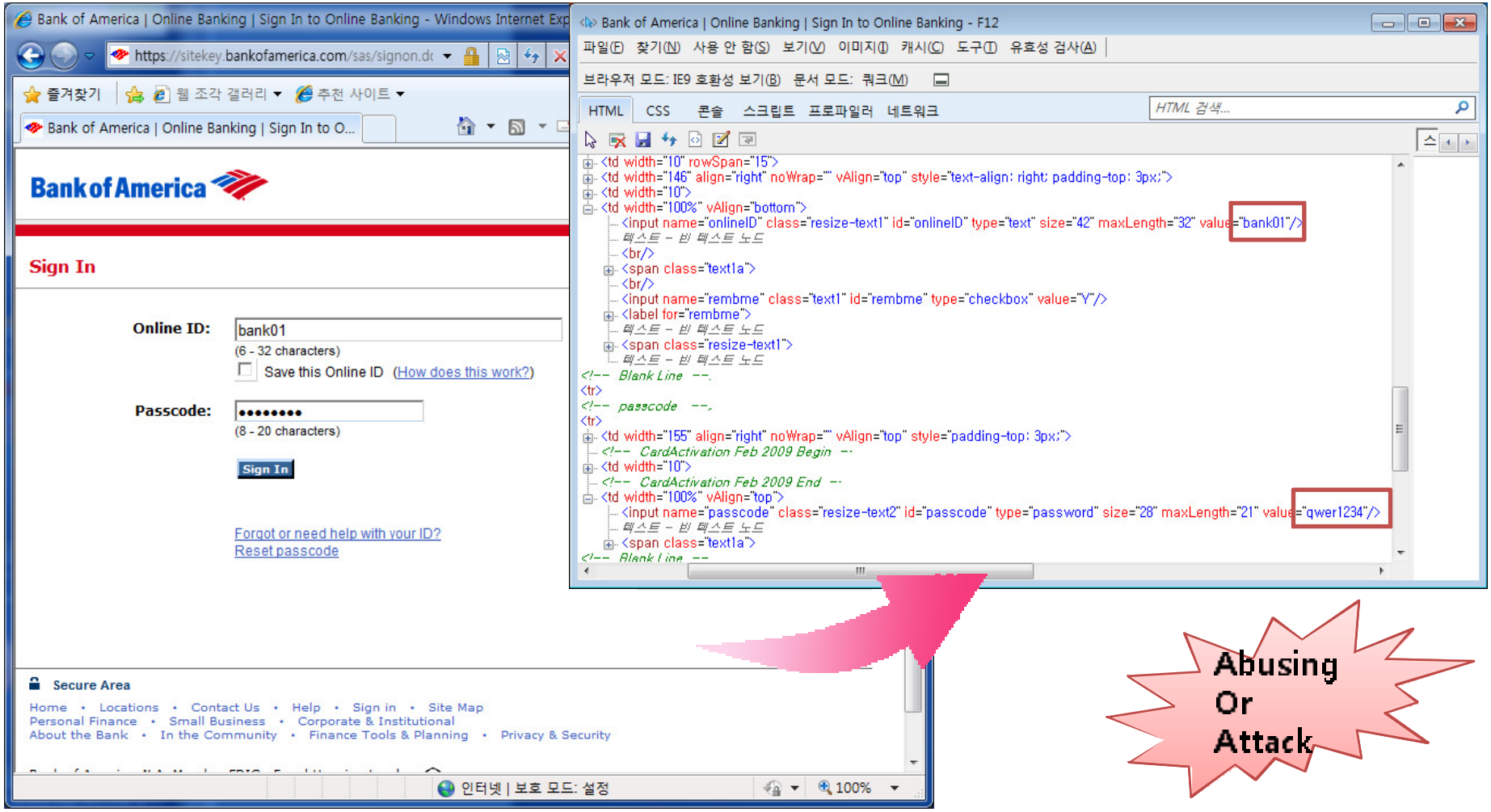
: MITB 공격은 웹 브라우저 내에 악성 프로그램이 설치된 상태에서 이루어지며, 악성 프로그램은 메모리에 로딩된 웹 페이지의 내용을 도청하거나 위/변조 할 수 있다.

이는 통신구간에서 이루어지는 MITM 과 관계가 없으며, SSL/TLS 로 통신구간이 암호화되어 있더라도 MITB 의 위협이 존재한다.

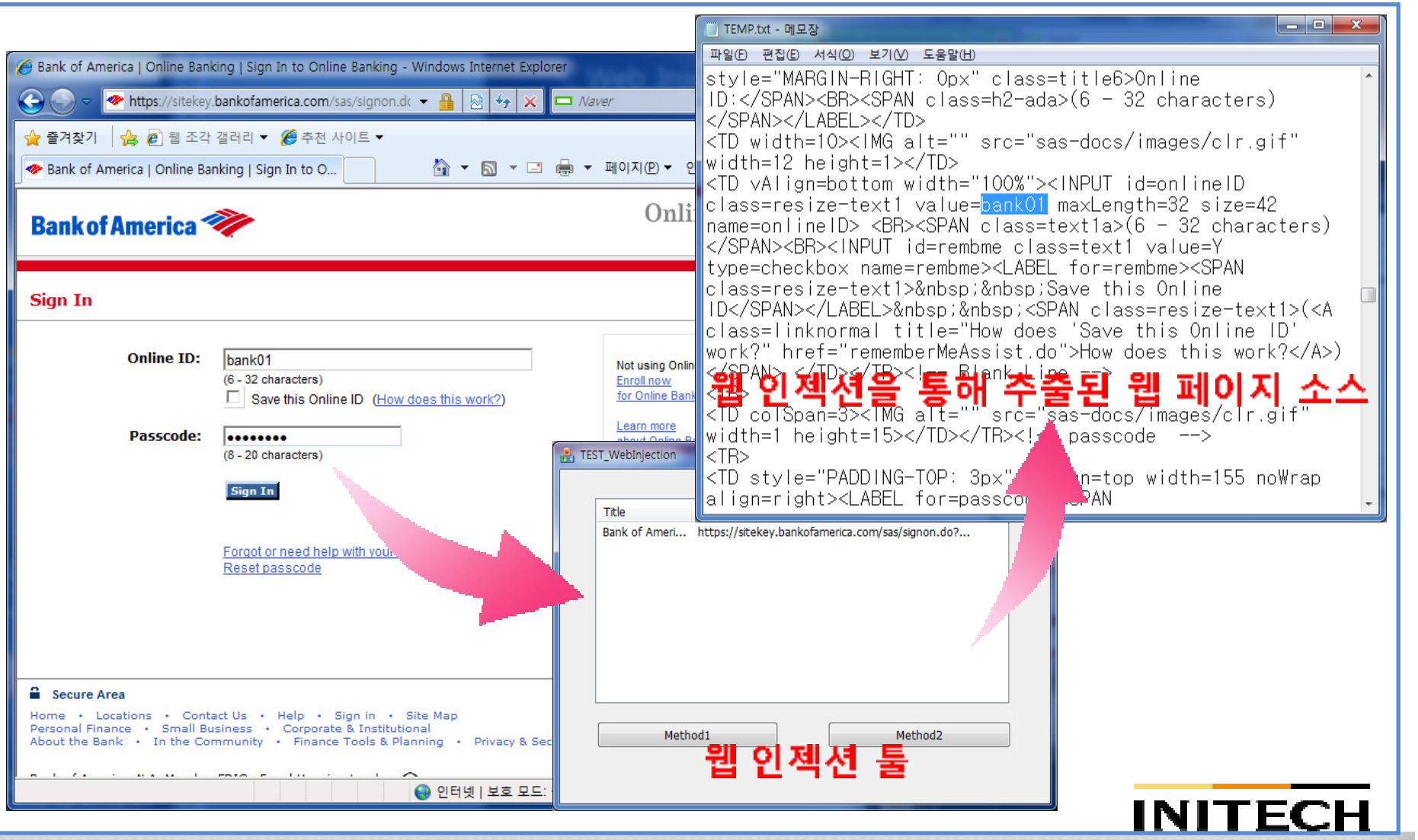
MITB 를 통해 웹 페이지를 위/변조하는 공격을 Web Injection 이라고 한다.



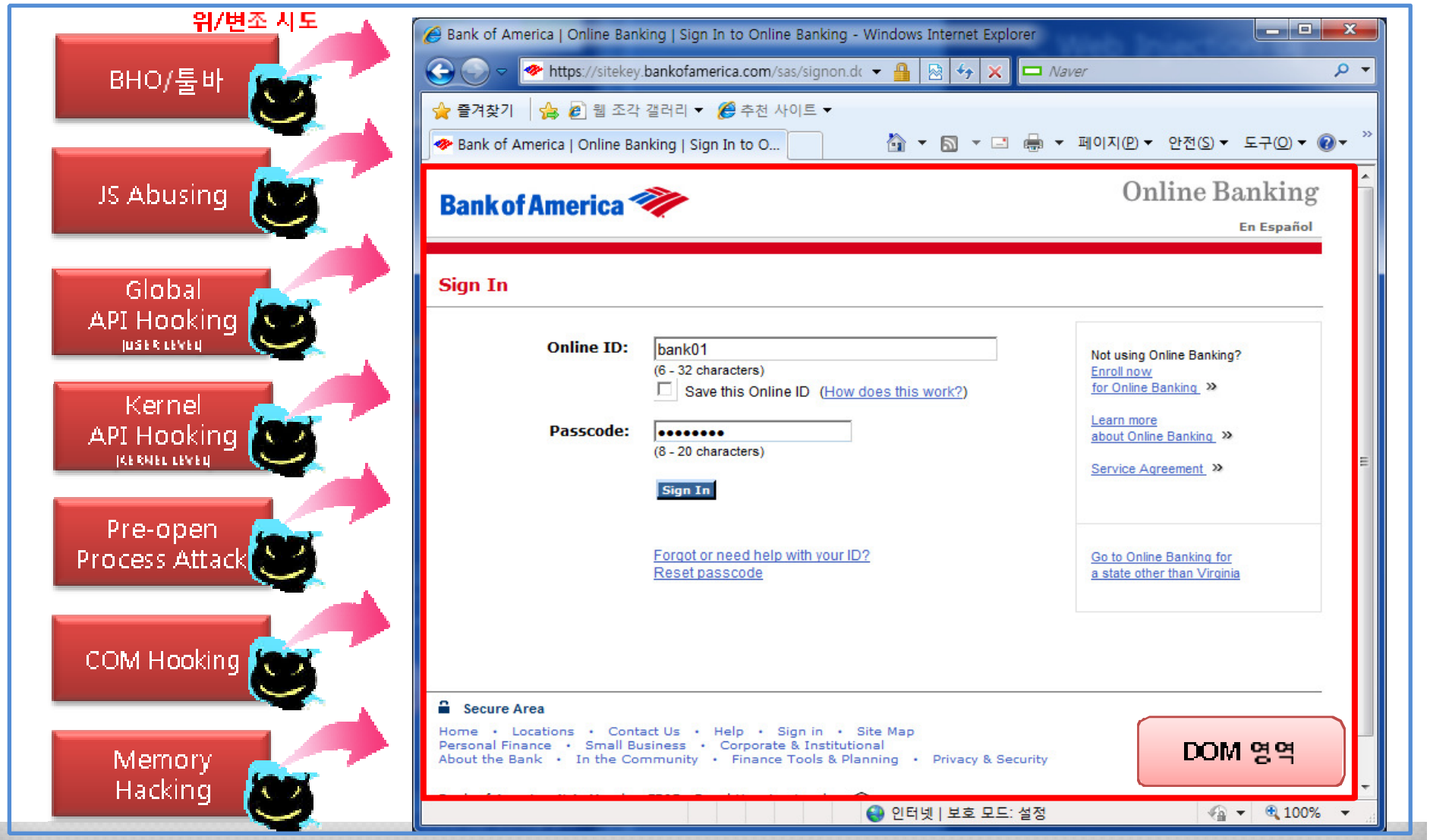
디버깅 인터페이스를 통한 로딩된 DOM 내부 접근(Web Injection 가능)



PC 상에서의 후킹을 통한 Web Injection 상황



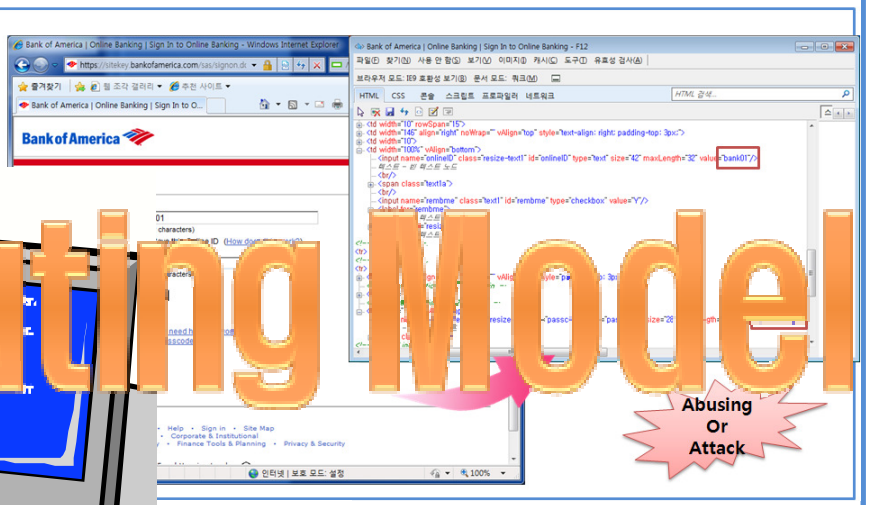
웹 브라우저 내 로딩된 DOM 객체를 변조하는 Web Injection 공격의 유형



MITB 공격(메모리 해킹, Web Injection) 등을 근본적으로 차단하는 방법은?

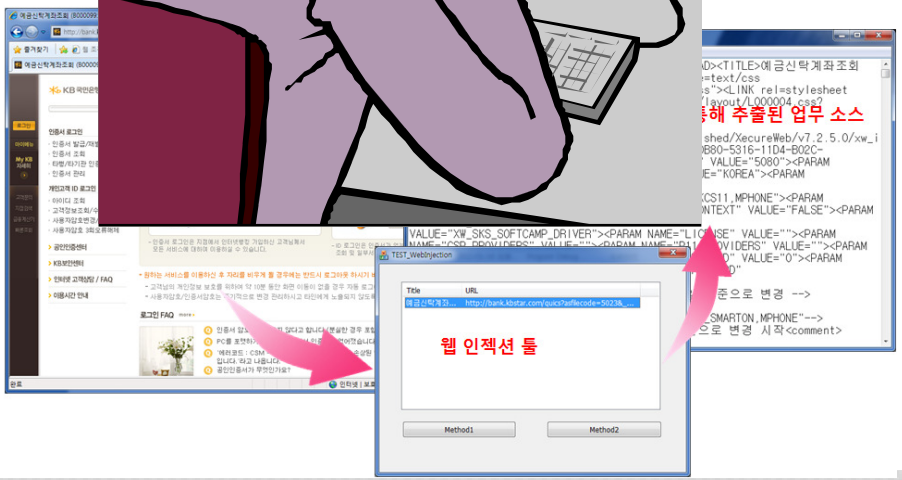
4. 메모리 해킹(?)

5. 디버깅 인터페이스를 통한 로딩된 DOM 내부 접근



Trust Computing Model

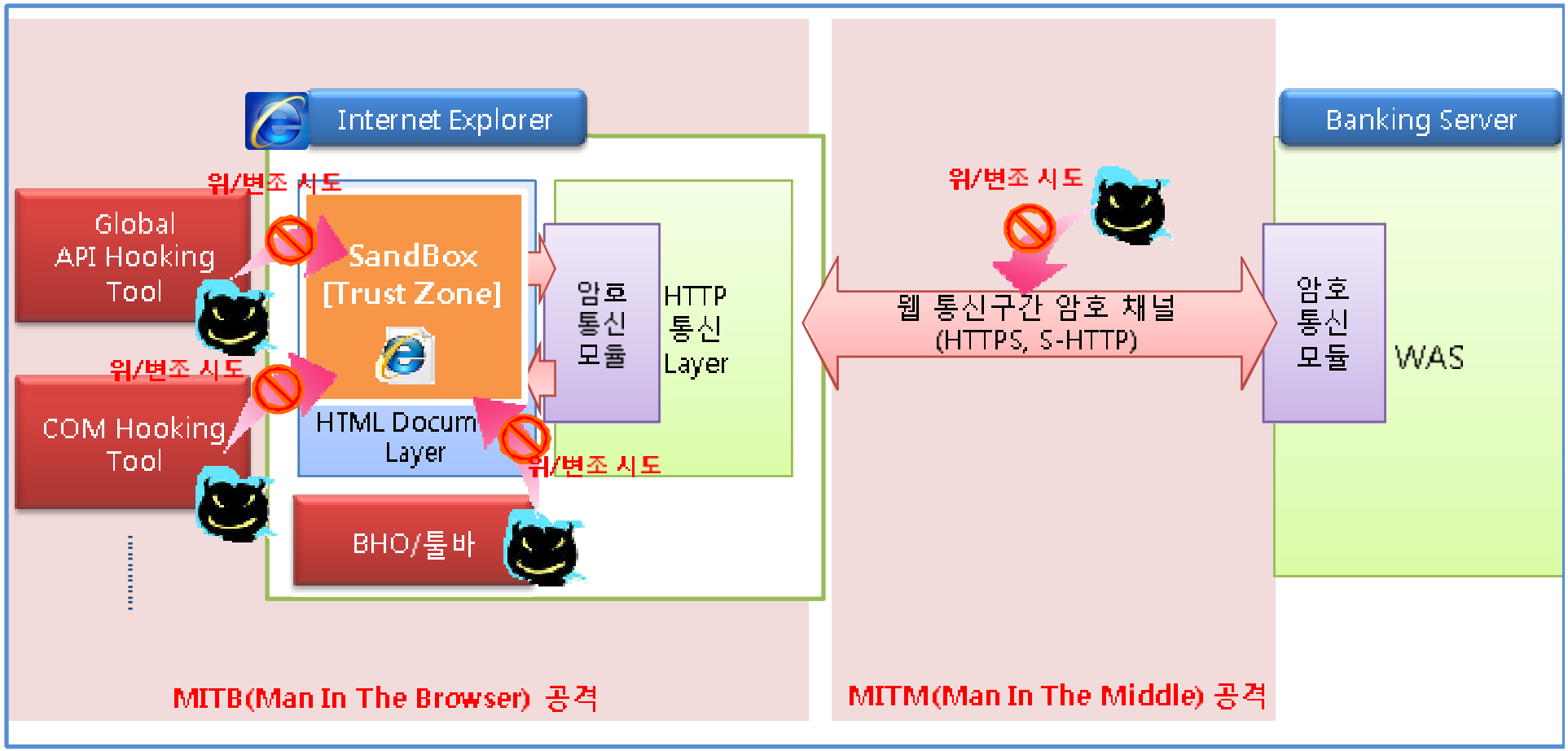
5. PC 상0



INITECH

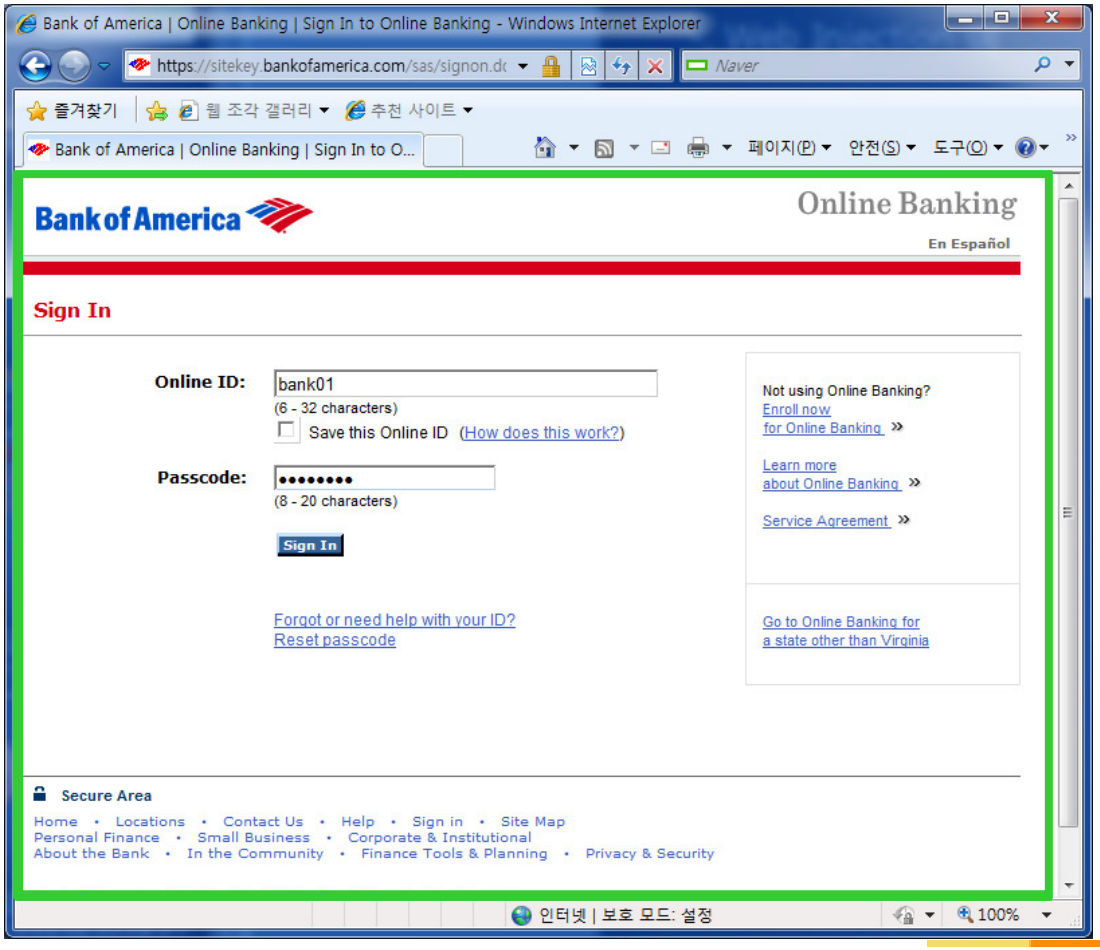
INISAFE SandBox™ 란?

: MITB(메모리 해킹, Web Injection) 공격 등을 차단하는 보안 솔루션.



INISAFE SandBox™ 의 보안 기능

: 웹 브라우저 내에 구성된 보안 영역(SandBox) 에서 인터넷 뱅킹 실행.



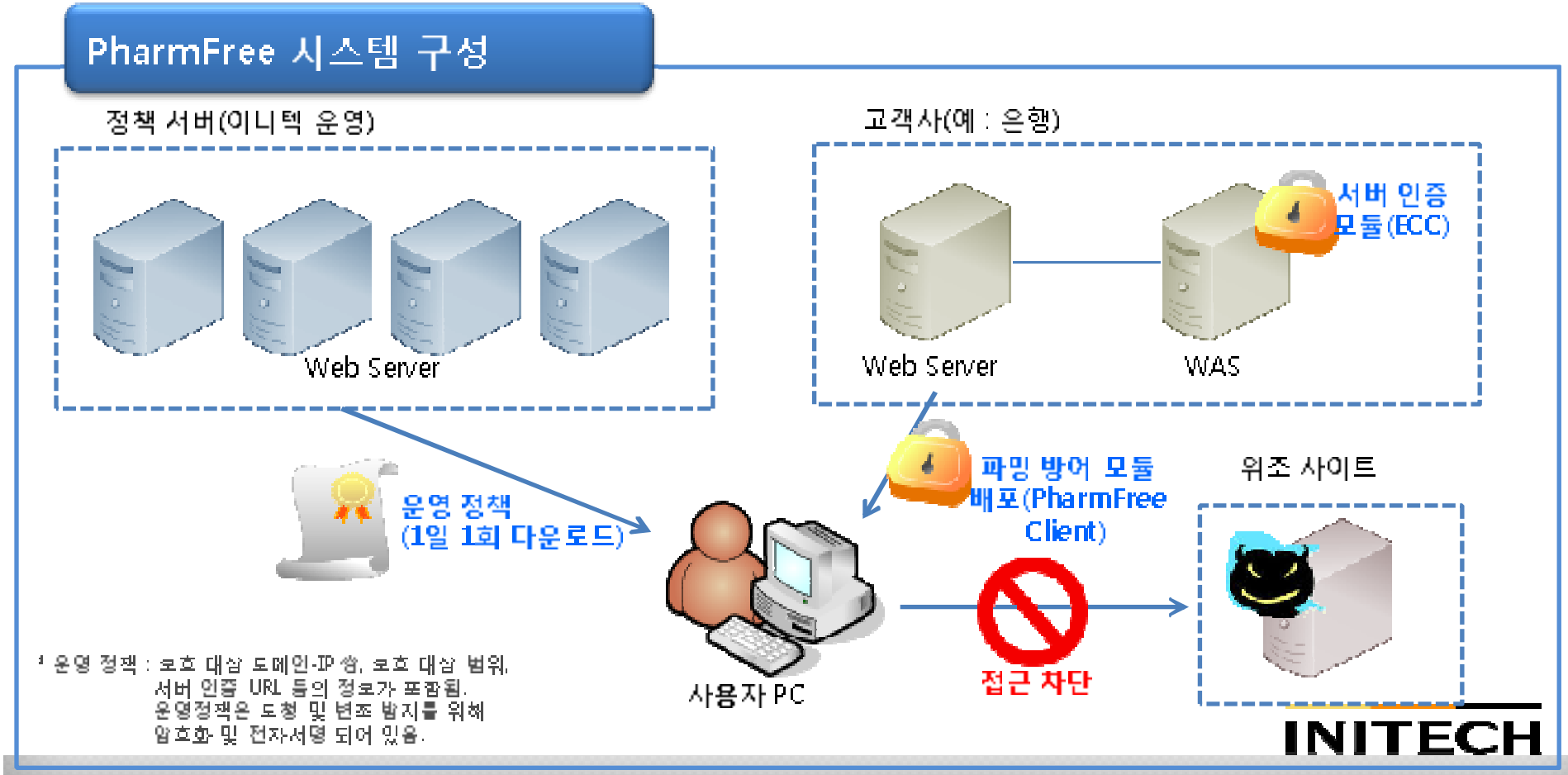
INITECH

INIService PharmFree™란?

- 클라이언트 프로그램이 백신처럼 PC 에 설치되어 서비스 형태로 상시 구동되며,
  정책 서버를 통해 보호 대상 도메인과 보호 범위를 수신 받아 파밍 공격을 탐지하고, 차단
- 멀티 브라우저와 CS 프로그램 까지도 지원
- 클라이언트 프로그램에 무력화 방지 기술이 적용되어 파밍 보안 서비스의 연속성을 보장

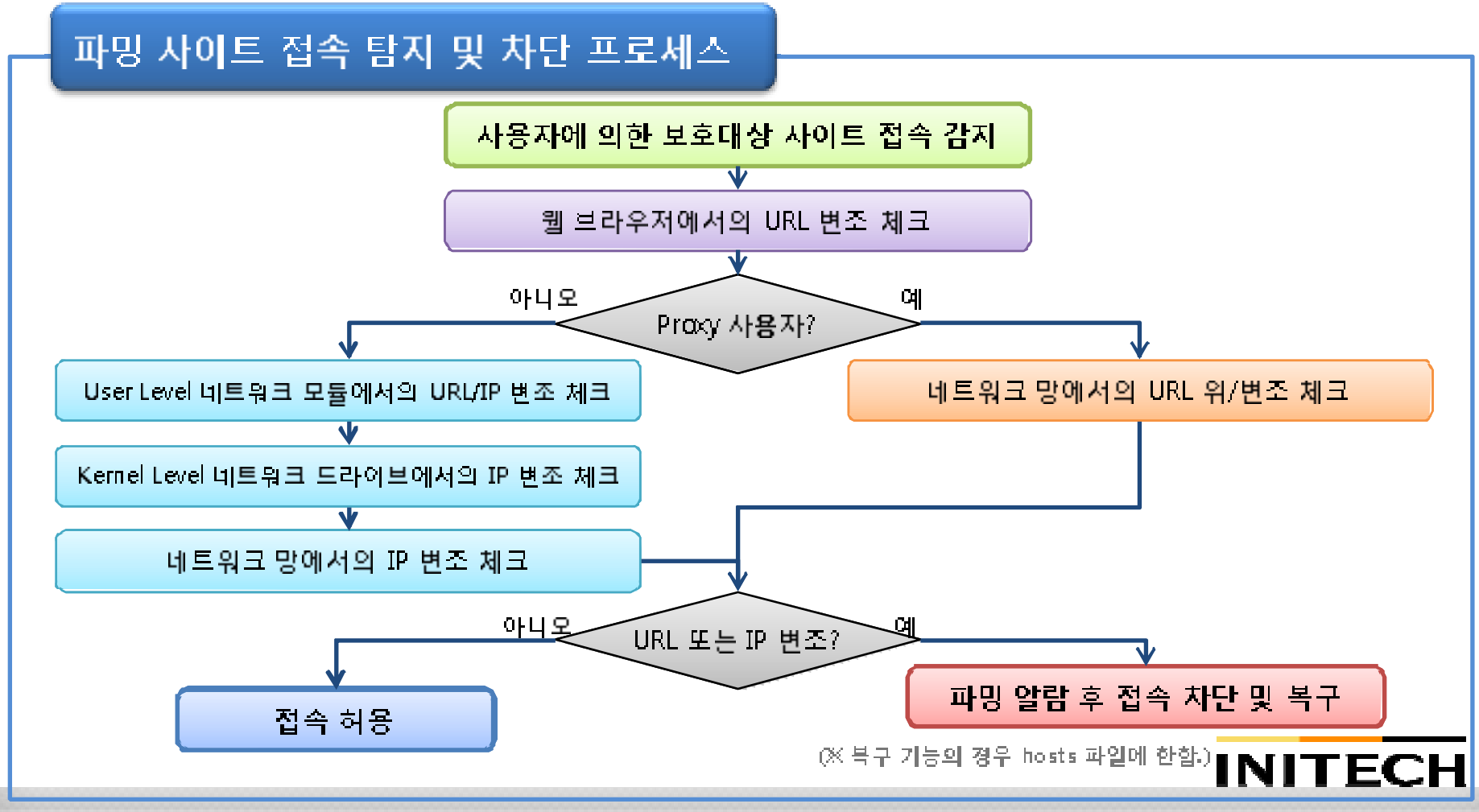
INIService PharmFree™의 시스템 구성

- 고객사 서버와 정책 서버, 파밍 방어를 위한 클라이언트 모듈로 구성
- 고객사 서버에는 서버 인증을 위해 팜프리 서버 인증(ECC) 모듈이 설치



INIService PharmFree™ 흐름도

아래와 같은 프로세스를 통해 파밍 사이트 접속을 탐지하고 차단.

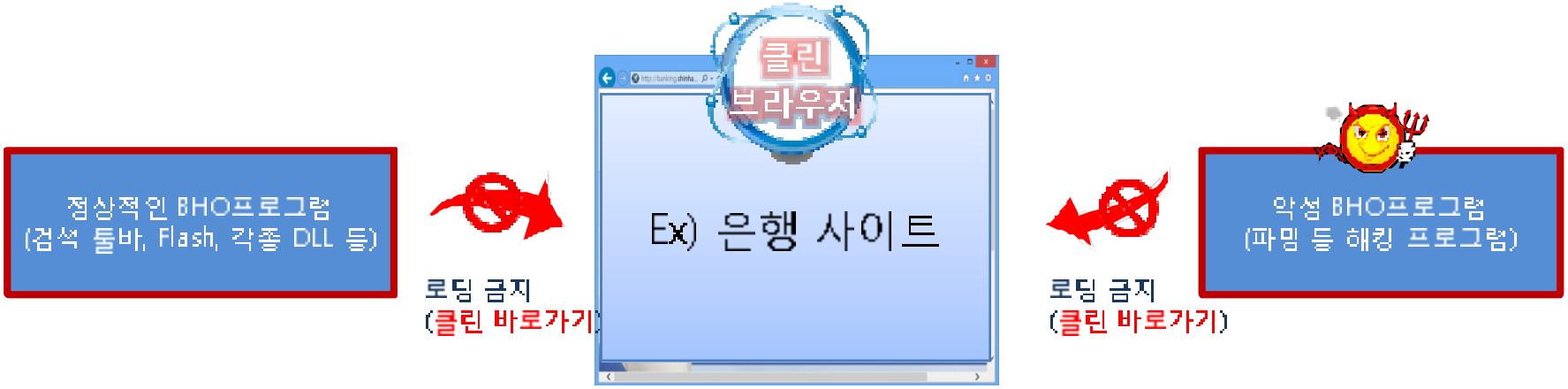


클린 브라우저 란?

Internet Explorer 브라우저의 BHO기능 및 DLL을 사용하여 수동 및 자동으로 설치된 프로그램

(툴바, 검색, 악성프로그램 등)을 브라우저 초기 로딩시 사전에 차단(클린 바로가기)하여

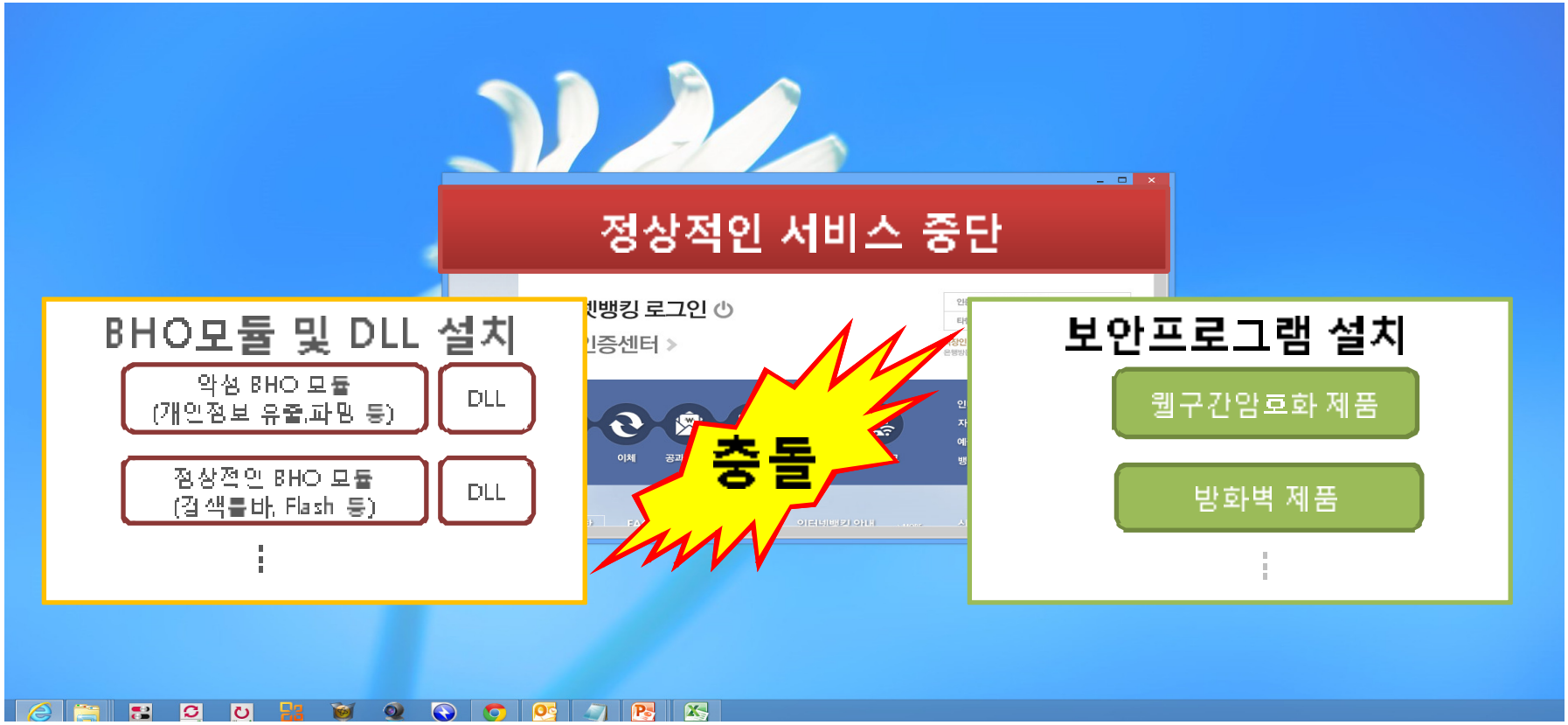
느린 속도와 툴바 및 DLL 등을 없앤 깨끗한 심플 브라우저



※ BHO(Browser Helper Object): 웹브라우저의 기능을 확장시켜주는 것으로
웹 브라우저가 자체적으로 제공하지 못하는 기능을 지원하는 플러그인과 같은 개념

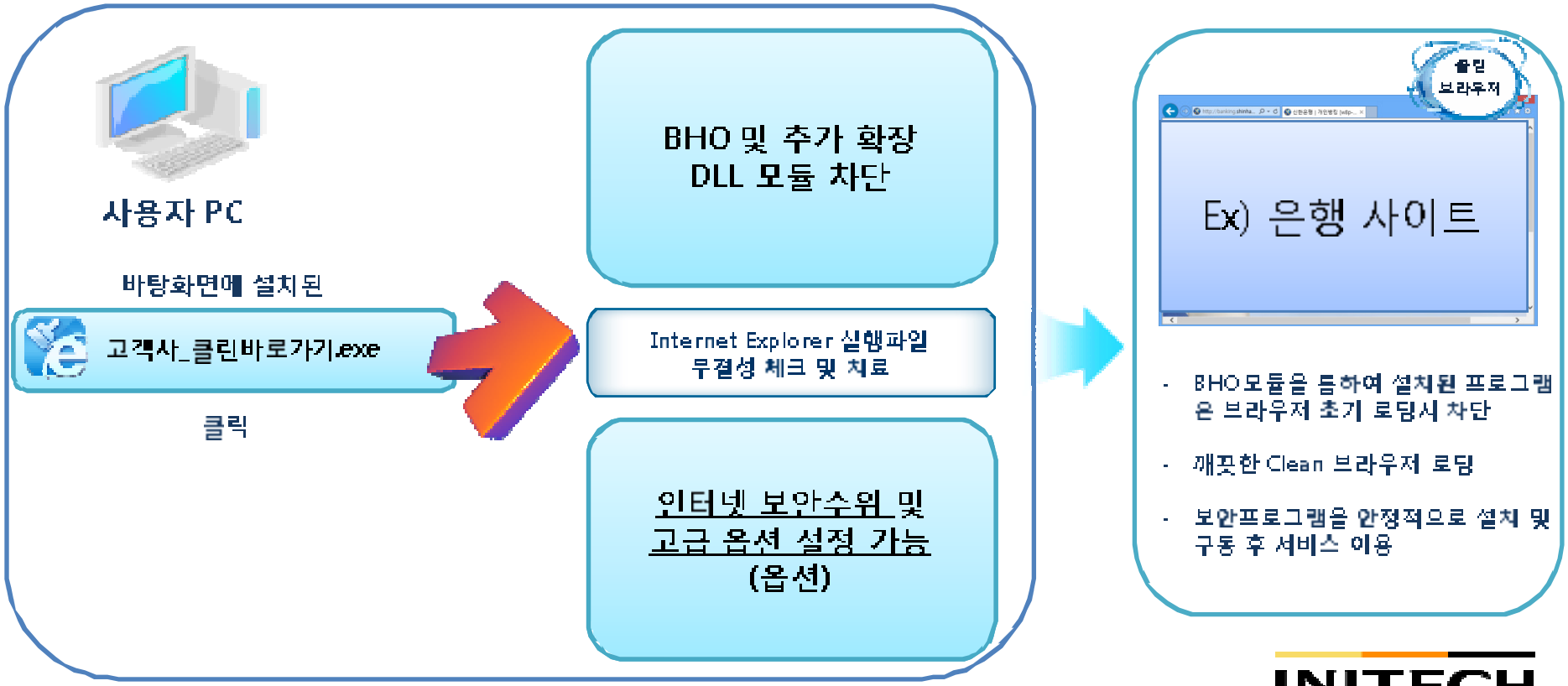
프로그램 충돌로 인한 사이트 접속 중단

BHO모듈 및 DLL을 통하여 설치되었던 프로그램과
안전한 접속 및 금융거래를 위해 필요한 보안프로그램과 충돌로 인하여
서비스가 중지되는 현상이 발생할 수 있음



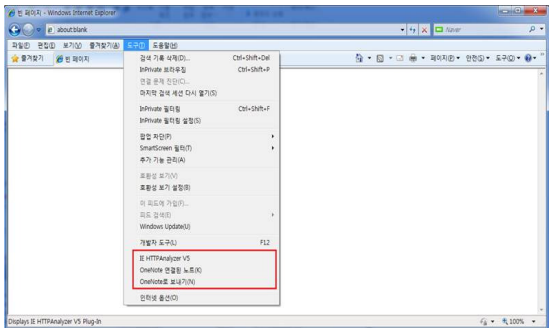
BHO모듈 및 툴바 차단 프로세스

사이트 접속 시 클린바로가기 접속프로그램을 통하여 사전에 설치되었던 프로그램들을 사전에 차단 후 브라우저 로딩이 되면서 안정적으로 서비스가능

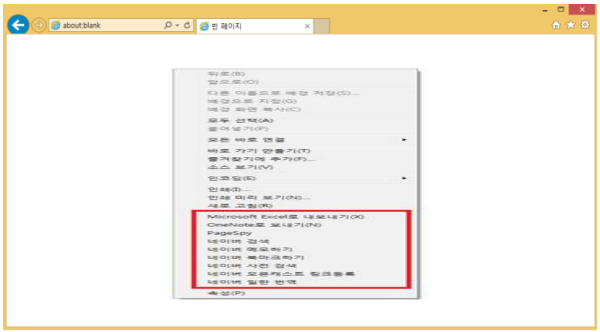


INITECH

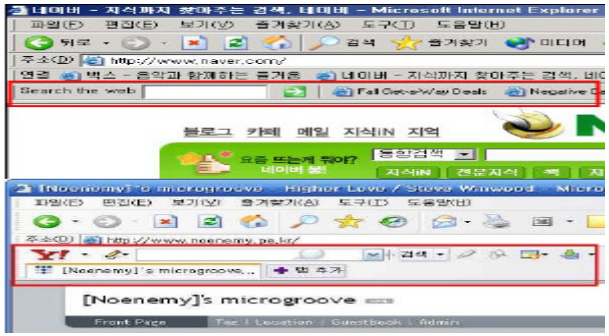
BHO 및 DLL에 의해 설치된 기능 차단 (주요 차단기능)



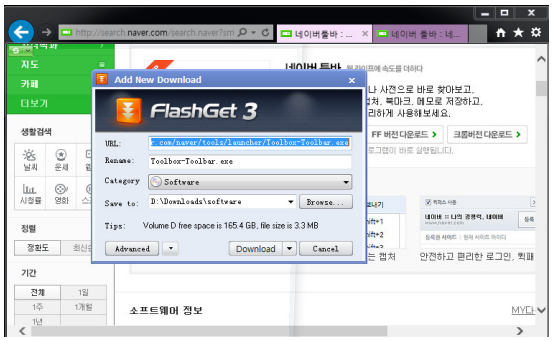
<도구 또는 도움말 확장메뉴 차단>



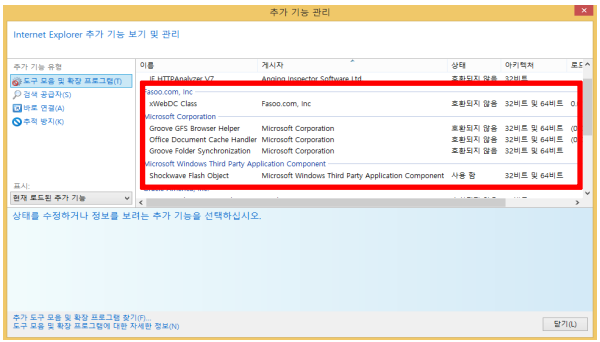
<오른쪽 마우스 클릭 시 추가 설치된 메뉴 차단>



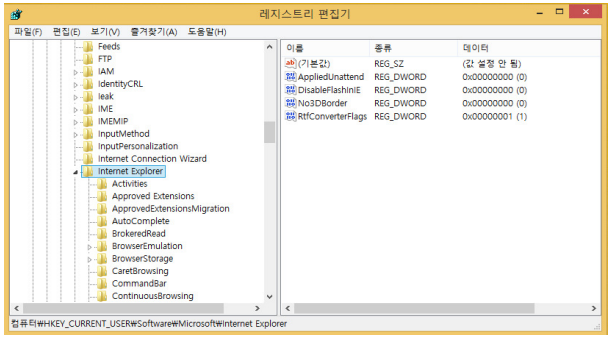
<IE상단의 툴바 및 툴바 버튼 차단>



<Custom 다운로드 관리자 차단>



<브라우저 확장 DLL 차단>



<각종 레지스트리 조작을 통한 DLL Injection 차단>

INISafe 클린 바로가기™

기대효과

사용자 측면

- 클린 바로가기 접속프로그램을 통해 사이트 접속 시 안정성 및 기업의 신뢰성 확보
- 사이트 접속 시 툴바 및 BHO모듈을 초기해 차단해 안정적인 서비스 접속
- 다양한 악성프로그램들과 충돌로 인하여 불필요한 콜센터 지원 요청 최소화

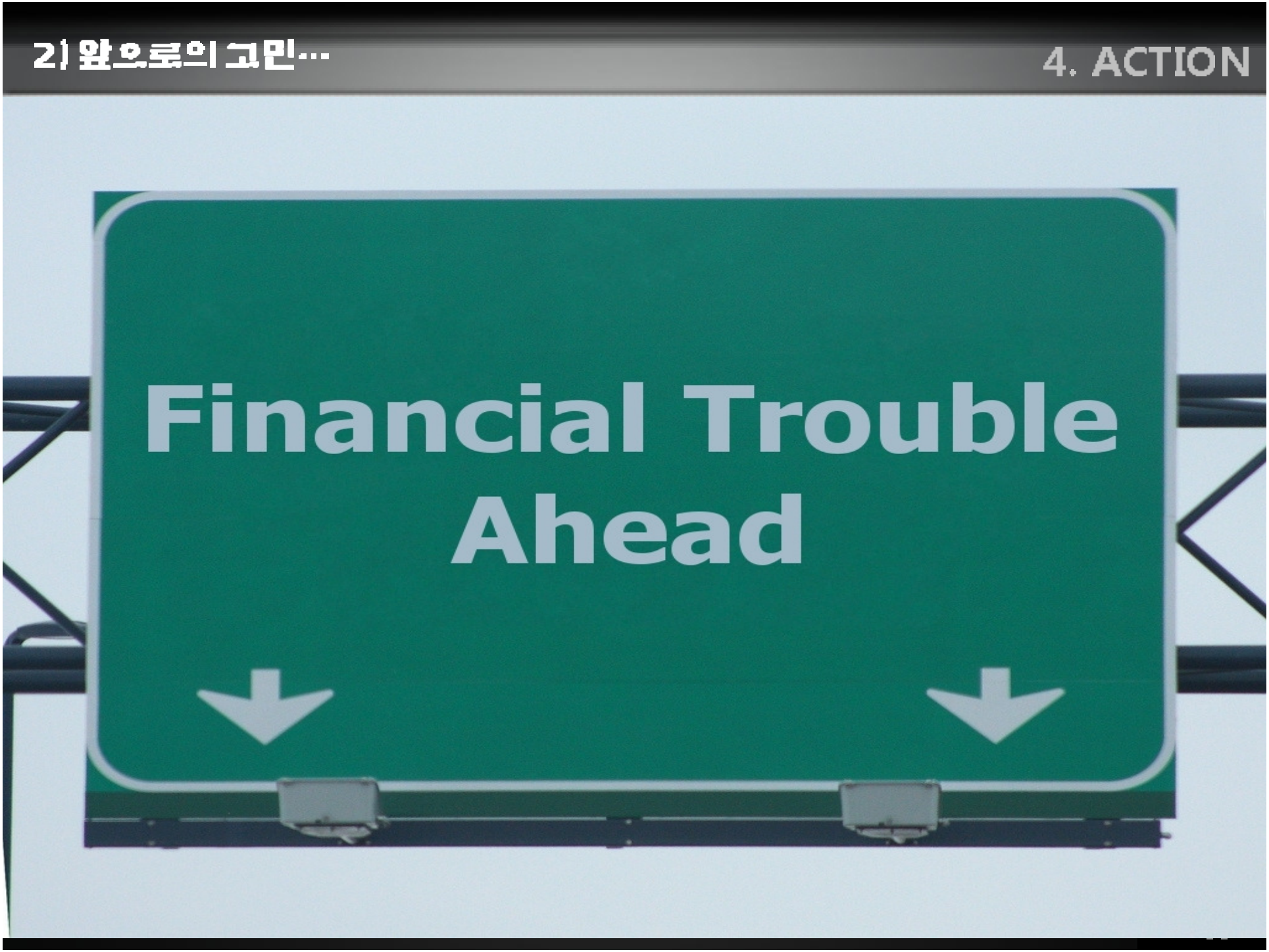
관리자 및 운영자 측면

- 악성프로그램들과 충돌로 인해 반복되는 장애문제 해결에 대한 인력,시간,금전적인 부분 감소
- 서버모듈은 없으며, 사용자에게 접속프로그램을 배포하여 따로 관리가 필요 없음

보안적 측면

- BHO를 이용하여 특정사이트 주소가 입력될 때마다 공격자가 지정한 파밍 사이트로 연결되지 않도록 사전에 BHO, 툴바 접속 차단

INITECH


Financial Trouble
Ahead


T
Y
U
I
F
Yes
May be
No
K
V
B
N
M
<
,


감사합니다.
INITECH
이니텍㈜
최정우
보안사업부문/사업기획팀
숭실대학교
산업·정보시스템공학과 겸임교수
차장 / 공학박사
152-050 서울 구로구 구로동 222-14
에이스하이엔드타워 2차 10~11층
E-Mail :
Jeongwoo.choi@initech.com
INITECH