V-PAD

사용자 입력보호를 위한 가상 키패드 솔루션

보안된 가상 키패드를 활용한 사용자 입력 데이터 보호 시스템 입니다.

V-Pad ?

브이패드(V-Pad) 란?

오픈 웹 환경을 위한 산업표준기술(플래시)과 표준 웹 기술만을 이용하여 제작된 사용자단 개인정보 보호 솔루션으로, 사용자 PC에 보안 에이전트 설치없이 웹 접속만으로 아이디, 암호, 기타 시스템 접근에 필요한 중요 정보 입력에 대한 해킹(키로그, 화면캡쳐 등)을 원천차단하고, 쉽고 직관적인 사용자 인터페이스를 통하여 별도의 교육 없이 웹 접속만으로 사용할 수 있습니다.

관련 특허 보유

사용자 컴퓨터에 키스트로크 해킹 보안 프로그램 설치가 필요 없는 변조된 일회성 인증 데이터 생성 방식을 이용한 정보 보안 방법 및 장치 (등록번호: 제 10-0838488호)

국정원 국가용 암호제품 등록

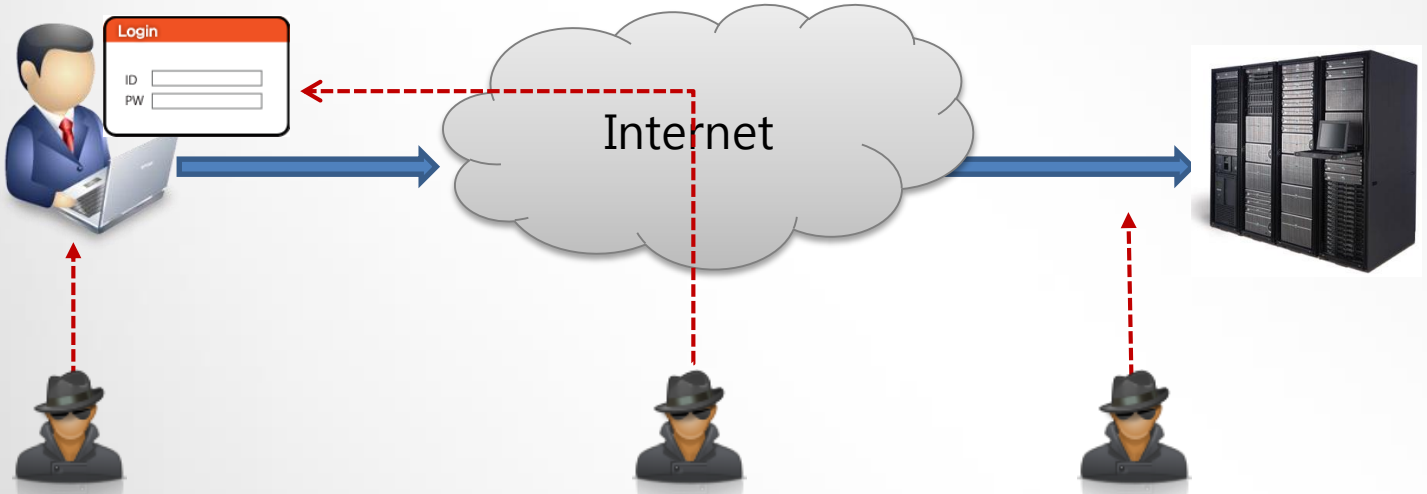
굿소프트웨어(GS) 인증제품

나라장터 등록제품

사회적협동조합

사이버 상의 위협 증가 (종합)

**최근 인터넷관련 범죄가 증가하고, 해킹방식이 워낙 다양해 100% 막을 수 없는게 현실이다.
여러 분야에서 본인 인증강화를 위한 다각적인 보안대책을 강구하고 있다.
특히 사용자 Password의 보안 취약성은 개인정보 유출은 법죄에 악용될 수 있으며,
금전적인 피해로 확대되어 큰 피해를 입힐 수 있습니다.**



키보드 입력정보 해킹

아이디, 암호 입력단계에서
키-로거와 같은 해킹 툴을
활용한 가로채기

메모리 해킹 위협

메모리에 침투하여 조작 후
사용자 모르게 인출

해킹툴을 이용한 정보 탈취

스파이웨어, 백-도어 및
기타 악성코드로 인한 고도화된
해킹 기술에 따른
사용자 아이디, 암호가 쉽게 유출

서버 전송구간

입력된 아이디, 암호가 서버로
전달될 때, BHO유형, 스니핑
(Sniffing)툴을 통한 가로채기

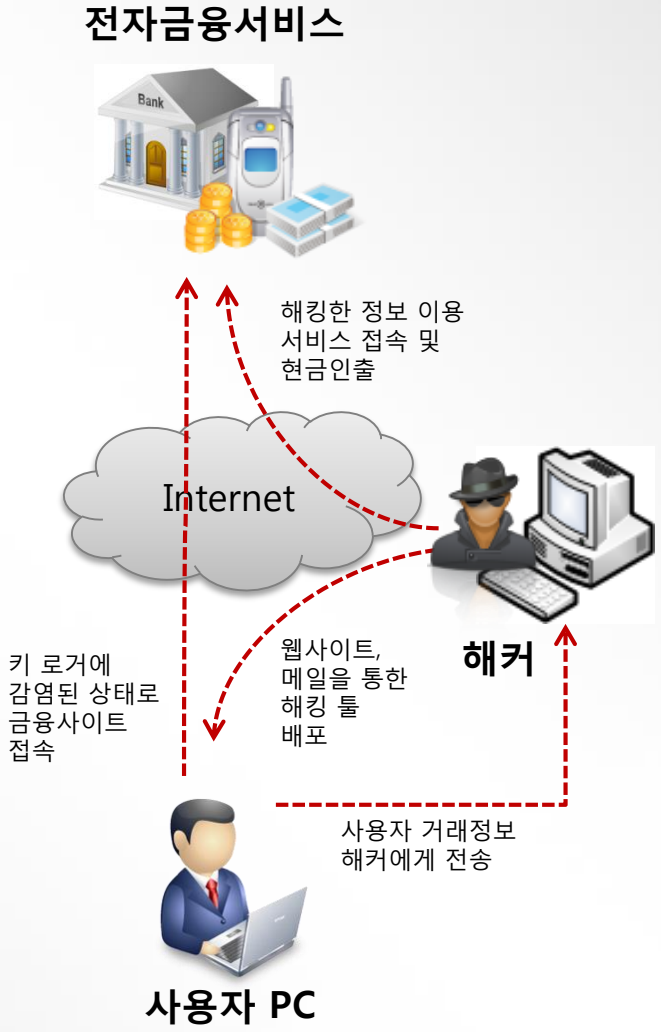
사이버 상의 위협 증가 – 사례1

인터넷 뱅킹 해킹 유형

인터넷 뱅킹 해킹을 통한 현금 인출사고 발생

개인PC에 피싱, 파밍, 스니핑, 키 로깅 등 다양한 해킹툴을 이용하여 ID/PW, 계좌 비밀번호, 보안카드 번호 등 고객정보를 획득하여 해당 인터넷 뱅킹 서비스에 접속 후 현금서비스 및 이체

5000만원 이상 이체시 일회용 비밀번호 생성기(OTP)나 보안토큰을 사용하도록 하였으나, 이를 피해 5000만원 이하의 금액 인출사고가 잇따랐다.



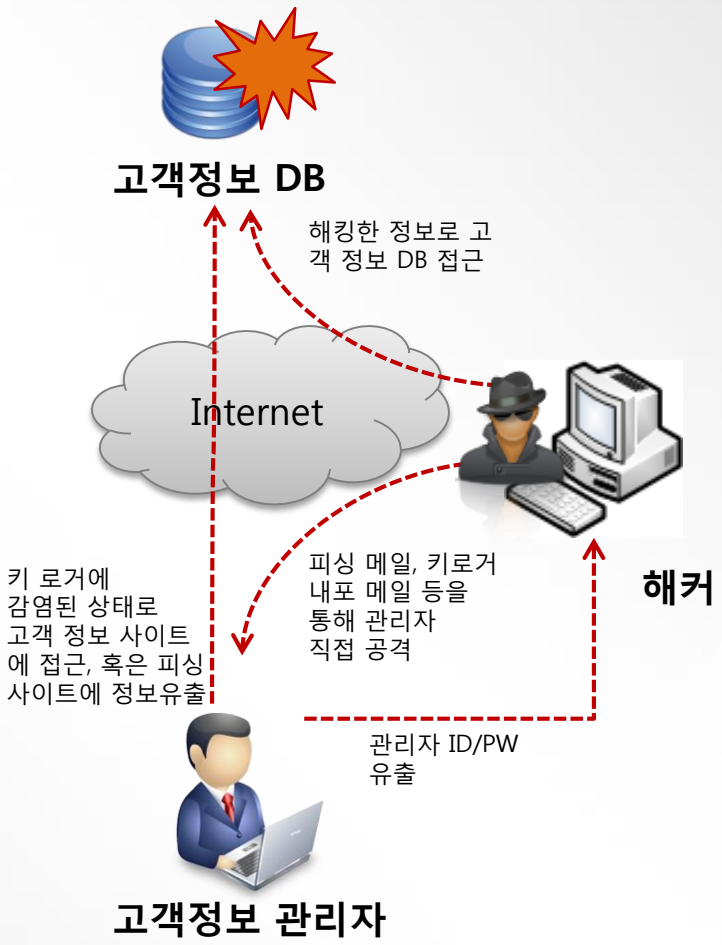
사이버 상의 위협 증가 – 사례2

고객정보 관리자 공격 유형

**잇단 해킹에 의한 고객정보 유출사고,
내부자 계정유출이 주범**

지금까지 발생한 고객 정보유출사건을 살펴보면 내부자 계정유출로 인한 제2차 피해라는 공통점이 있으며 해커들은 개인정보를 유출하기 위한 첫 단계로 고객DB 접근이 가능한 내부관리자 혹은 사이트 운영자의 계정을 노림.

일단 관리자의계정을 알기만 하면 정보 접근이 허가된 사용자로 분류돼 고객정보를 마음대로 가져 올 수 있음



사이버 상의 위협 증가 – 사례3

온라인 서비스 해킹 사고 유형

훔친 ID와 PW를 이용하여 사이버머니를 탈취하거나 개인정보를 빼내 금전적 피해사고 발생

인터넷쇼핑몰, 온라인 게임 등 일반 온라인 서비스에서 가장 많이 발생하고 있는 계정 도용패턴으로, 해커는 보안이 가장 취약한 사용자PC에 해킹툴을 설치하고, 여기서 얻어낸 정보로 온라인 서비스에 접속을 시도함. 2차 인증 수단이 없는 온라인 서비스에서 가장 간단하면서도 위협적인 계정 도용 패턴임

온라인 게임사이트

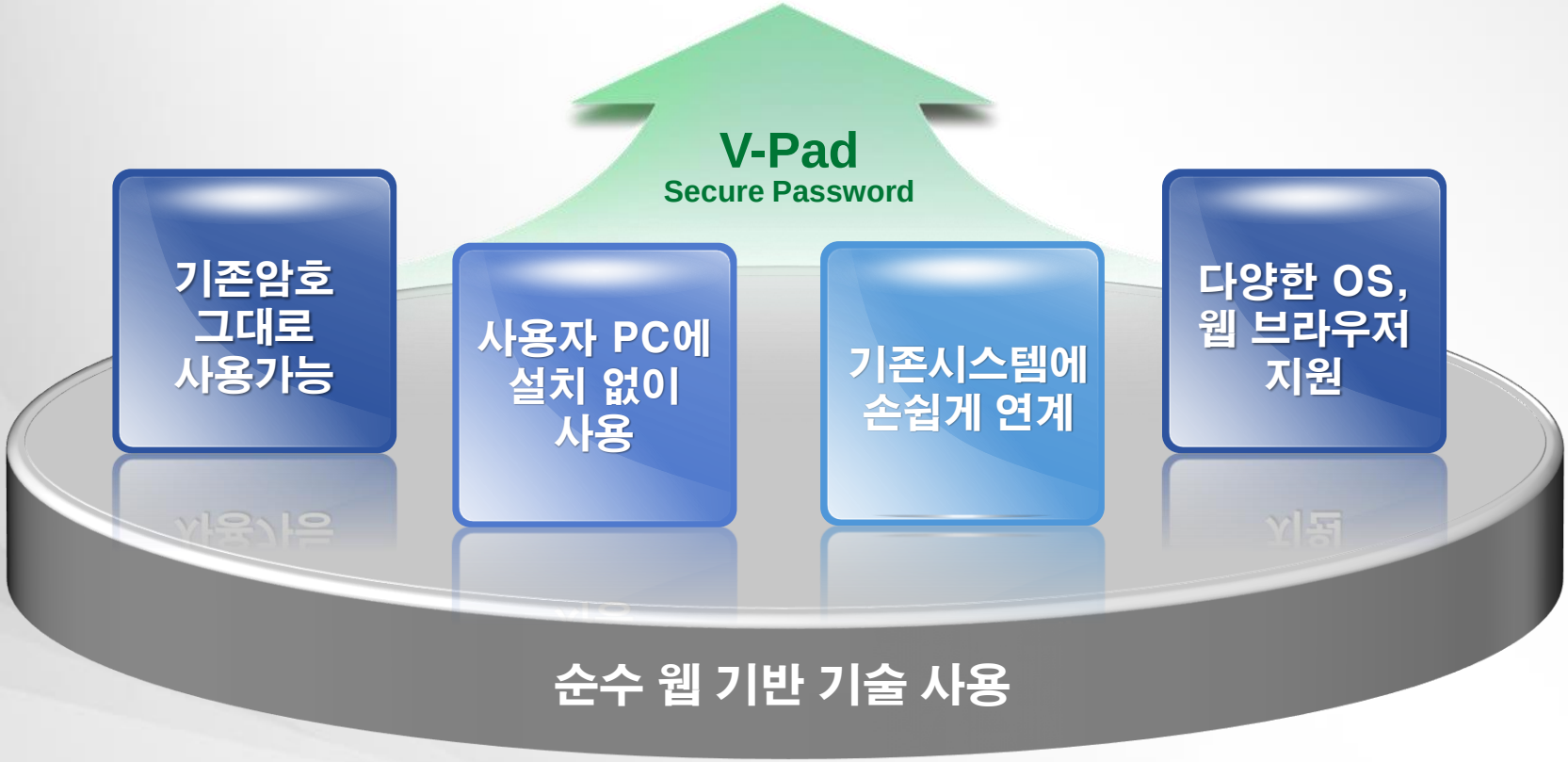
사용자 PC

기존 인증체계와 해결과제

구분	사용자 PC 해킹	고정 Password 취약점 이용	서버 전송구간 해킹
위협	■ 아이디, 암호 키 입력 정보 해킹 ■ 스크린 캡쳐를 통한 가상 키 패드 입력 정보 해킹 ■ 메모리 해킹	스파이웨어, 백-도어 및 기타 악성코드로 인한 고도화된 해킹 기술에 따른 사용자 아이디, 암호가 쉽게 유출	입력된 아이디, 암호가 서버로 전달될 때, BHO유형, 스니핑(Sniffing)툴을 통한 가로채기
기존 인증 보안 사례	사용자가 입력하는 키보드 정보 해킹을 방지하기 위한 방화벽, 키보드 보안 프로그램 등 사용자 PC에서 매번 다수의 보안 프로그램 다운로드가 필요함	알려진 악성코드 제거 및 OTP를 활용한 고정 Password 해킹 피해 최소화 (OTP발생기, 토큰 사용)	사용자 PC에서 서버 전송구간 암호화를 통한 정보유출 방지 (ECC, ECDH)
해결과제	**<서비스 제공 자 측면 >** ■ 프로그램 다운로드를 위한 네트워크 사용 증가 ■ OS, 인터넷 브라우저 종류에 따른 지원 여부 및 유지보수 어려움 **<사용자 측면 >** 사이트마다 다른 보안프로그램 설치 유도	**<서비스 제공 자 측면 >** ■ 보안카드 보안 취약점에 대한 불안 ■ OTP 인증 사용자 콜 응대 ■ OTP 인증 서버 관리 **<사용자 측면 >** OTP발생기 구입 비용발생 매번 다른 암호를 입력 해야 하는 불편함	**<서비스 제공 자 측면 >** 서버전송 정보 보안을 위한 별도의 네트워크 보안솔루션 도입 필요에 따른 비용 발생

V-Pad 특징

순수웹환경으로 제작된 사용자단 개인정보보호 솔루션으로,
사용자 컴퓨터에 별도의 설치 없이 간단히 웹 접속하여 사용할 수 있습니다.
이 시스템은 키로거, 악성코드 등에 의한 불법 해킹 을 막는
직관적인 인터페이스를 가진 솔루션 입니다.



V-Pad 특징 -1

순수 웹기반 기술

순수 웹 환경에서 제작된 사용자단 개인정보 보호 솔루션

기존 시스템의 변경 없이 고객사의 웹 서버에 설치하여 사용할 수 있으며, 순수 웹 기반 시스템이므로 사용자 PC단에는 설치되지 않습니다.

기존 암호 그대로 보안 강화

순수 웹 환경에서 제작된 사용자단 개인정보 보호 솔루션

사용자가 사용하는 암호를 그대로 사용 가능
마우스를 이용한 키 값을 생성하므로 키보드 해킹으로부터 안전합니다.
마우스 위치를 가상화 하므로 마우스 해킹에 대해서 안전합니다.
키패드가 캡쳐되더라도 복수개의 가상 마우스를 사용하므로 해킹에 안전합니다. 매번 키 교환을 통한 암호키를 생성하고 입력된 암호 문자열을 해당 키로 암호화 하므로 패킷 스니핑에 안전하며 암호화 된 값은 서버단까지 그대로 전달됩니다.

다양한 스킨 적용 가능

Open 웹 환경에 적합한 디자인 변경가능
고객의 요구에 맞는 다양한 일회용 비밀번호 입력기를 제공하며, 일회용 비밀 번호 입력기 커스터마이징이 가능합니다.

다양한 데스크탑 환경 모두 지원

Windows: IE, FireFox, Safari, Chrome, Opera
Mac: FireFox, Safari, Chrome, Opera
Linux: FireFox, Chrome

완벽한 E2E 지원

사용자 입력부터 서버까지 복호화 구간 제거(E2E)

세션마다 암호 키 교환을 통한 암호 전달(ECC, ECDH) 암호 키 유출 불가

유저 프랜들리 인터페이스 지원

Adobe Flash 기반

화려한 멀티미디어 기능을 이용한 유저 프랜들리 패드 지원
가상키패드 커스터마이징을 통한 사용자 만족 증대

클라이언트 장애 최소화

사용자 데스크톱 환경에 클라이언트 모듈 설치없이 산업 표준인 플래시와 웹 표준 준수를 통하여 사용자 오류 최소화
가상키패드 UI(사용자 인터페이스)와 암호화 모듈 일체형

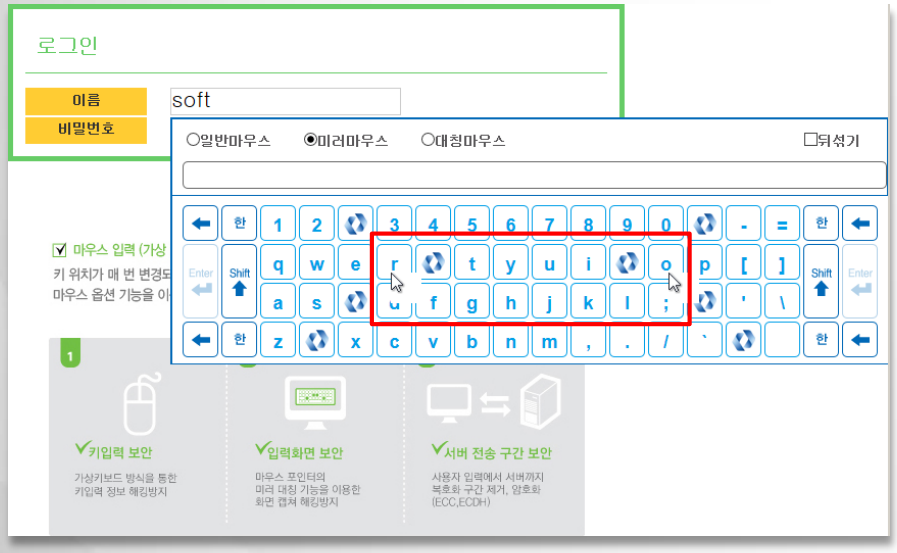
V-Pad 특징 -2

마우스 옵션 기능

1)일반 마우스 , 2)미러 마우스, 3)대칭 마우스

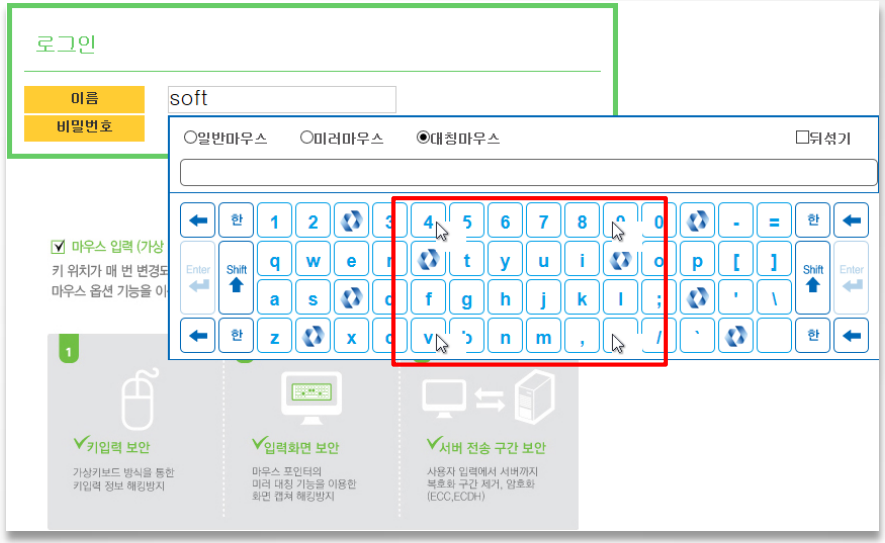
해킹에 의해 스크린 캡쳐 시 마우스 옵션을 이용하여 사용자의 입력 정보 알 수 없습니다.

미러 마우스



2개의 마우스를 화면에 보여 주며, 어떠한 문자를 입력 하는지 알 수 없도록 화면에 보여 줍니다.

대칭 마우스



4개의 마우스를 화면에 보여 주며, 어떠한 문자를 입력 하는지 알 수 없도록 화면에 보여 줌. 미러마우스 보다 한층 강화 된 마우스 기능을 화면에 보여 줍니다.

*일반 마우스 옵션은 마우스 커서가 1개 보여지는 일반적인 형태 입니다.

기존 보안 취약점 해결 방안

기존 취약점	해결효과
BHO공격	인터넷익스플로러의 BHO(Browser Helper Object)제어, 변조어 상관없이 독립적인 기능을 수행하고, 서버&클라이언트 동기화로 DOM(Document Object Model)영역의 입력정보 탈취, 변경, 재사용을 보안
메모리해킹 공격	윈도우 OS메시지 처리,메모리 덤프 기술을 이용하여 메모리에 적제된 입력 정보 해킹 -E2E(종단간 암호화)에 따라 실시간 입력정보 암호로 메모리 적제 및 자동 Destory 되어 안전
키보드 입력 정보 공격	외부 화면에 출력되지[않는 VI가상보드를 이용하여 입력 상태 및 정보 확인 불가능 새로운 키[로그 프로그램 및 변종 해킹프로그램에 의한 입력정보 유출에서 안전
DLL 인젝션 공격	동작중인 보안프로그램 내부에 해킹모듈 침투로부터 차단. (보안프로그램 자체보호)
리버스 엔지니어링	보안프로그램 실행 전 설치 된 파일에 대하여 Binary상태에서 분석 및 취약점 발견에 대하여 보안 프로그램보호 (보안프로그램 자체보호)
원격 해킹 공격	VI기술을 적용한 보안 영역을 원격 해킹프로그램으로부터 안전하게 차단

시스템 구성도 및 구성장치

시스템 구성도

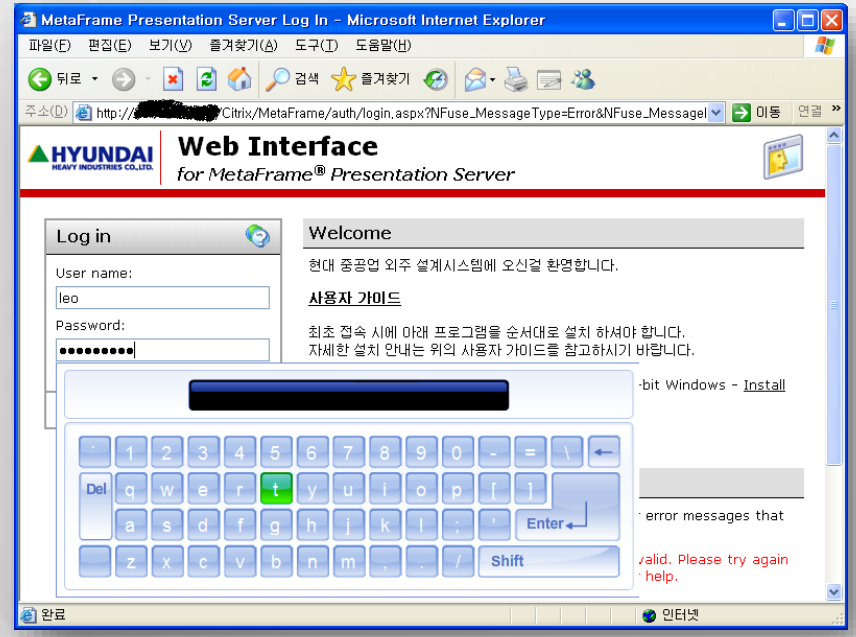
구성장치

구축사례 (D증권)

웹트레이딩 / 계좌번호입력

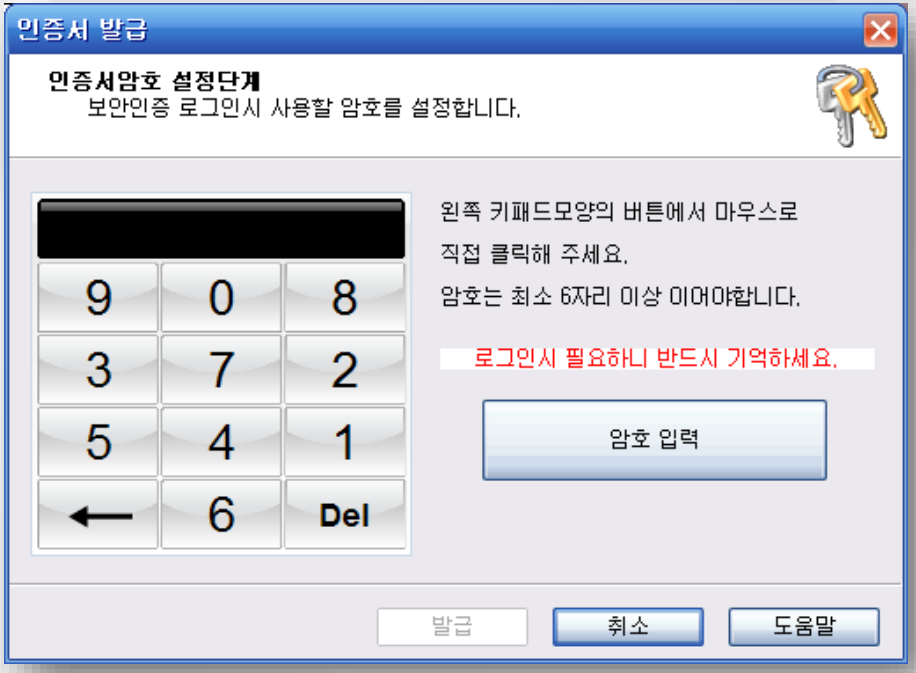
웹트레이딩 / 주민번호,계좌번호입력

구축사례 (H중공업)

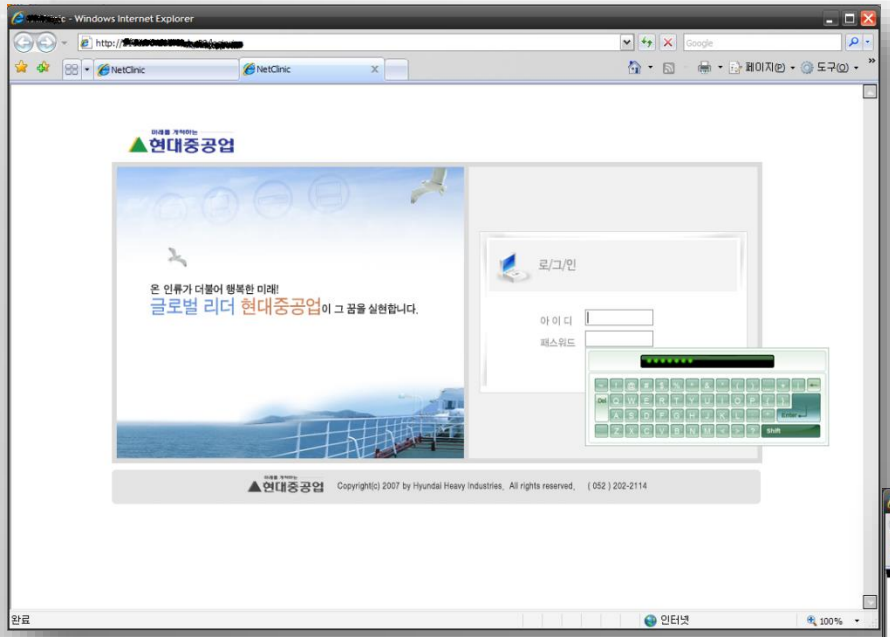


설계시스템 / 암호입력

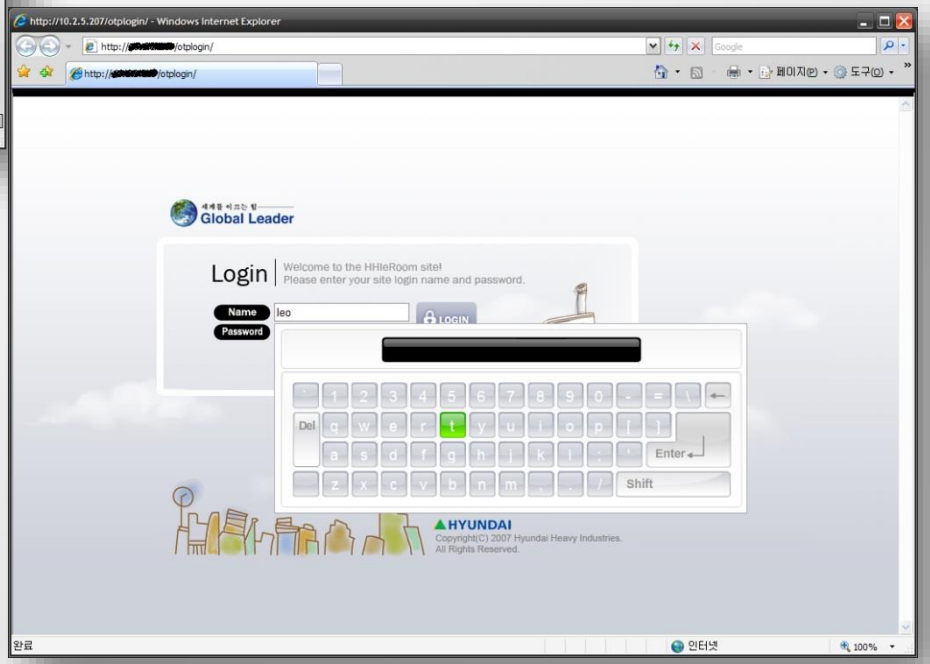
사용자 인증 / 인증서암호설정



구축사례 (H중공업)



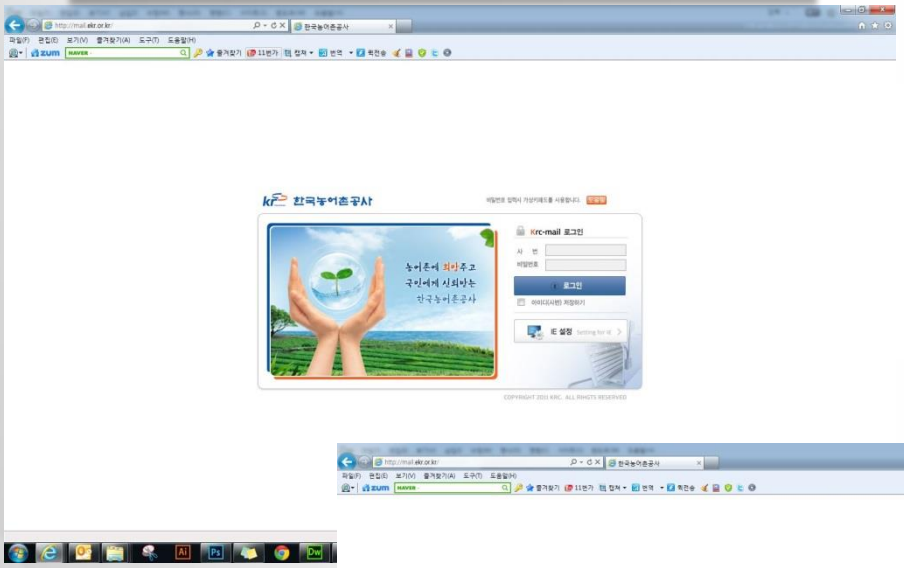
원격지원/아이디,암호입력



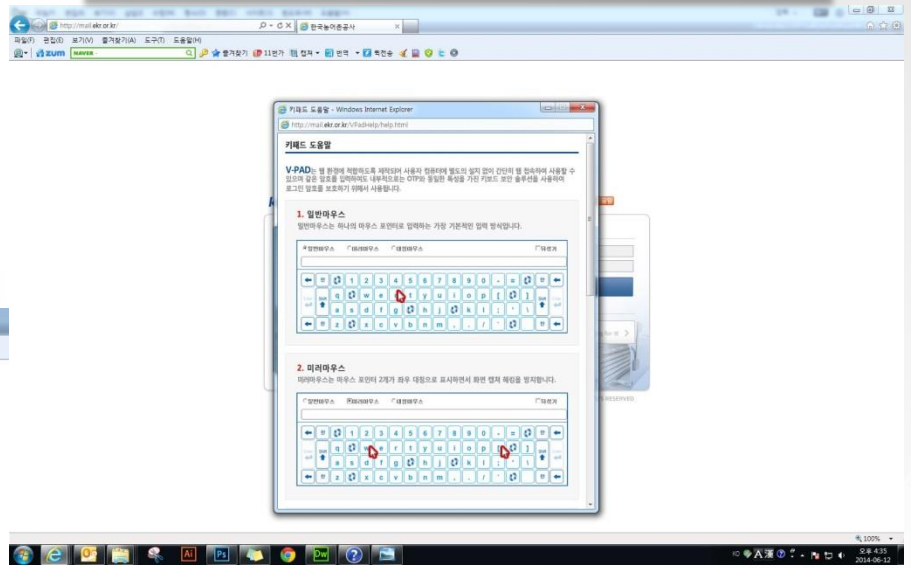
문서관리시스템/아이디,암호입력

구축사례 (농어촌공사)

외부 접속 메일시스템 메인

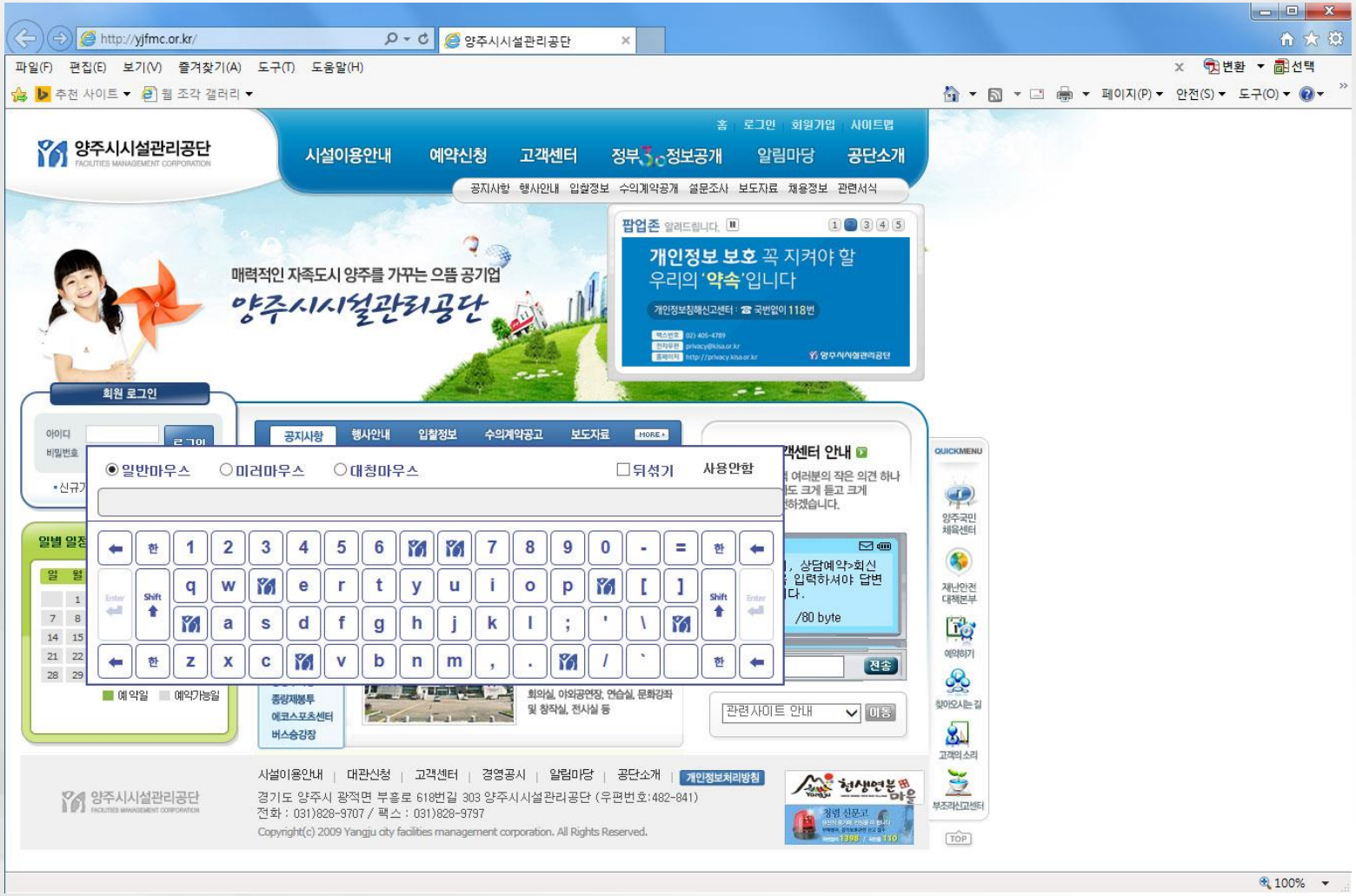


V-pad 사용 도움말



패스워드 입력 시 V-pad 사용

구축사례 (양주시시설관리공단)



세부규격

Web Browser

· Internet Explorer · Google Chrome · Mozilla Firefox · Apple Safari · Opera	· Google Chrome · Mozilla Firefox · Apple Safari · Opera	· Google Chrome · Mozilla Firefox · Opera

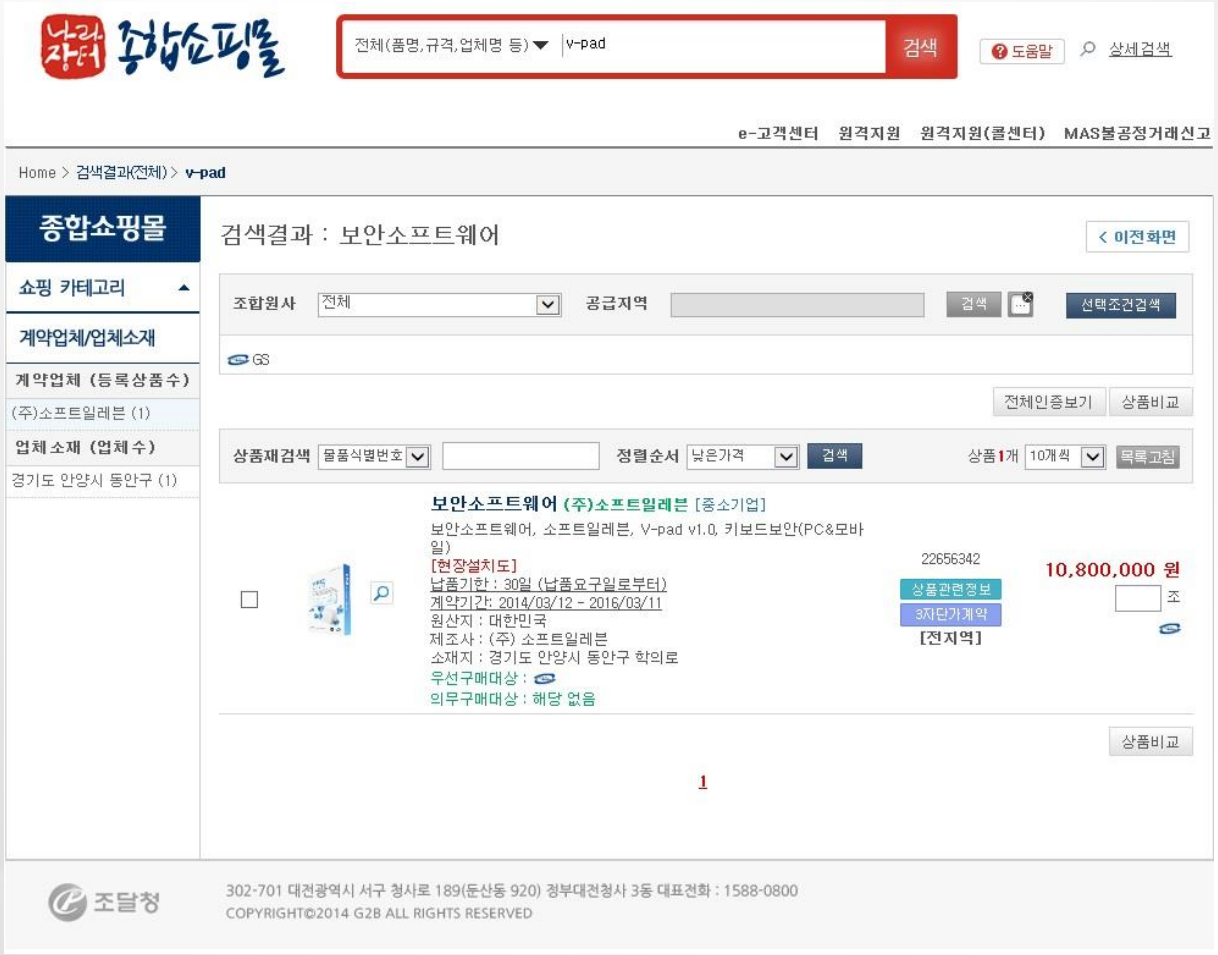
OS

MS-Windows XP, Vista, 7, 2003, 2008	Mac OS X	Linux

- **데모 사이트 안내**

1) URL : http://www.easykeytec.co.kr/demo.php

나라장터 종합쇼핑몰



>> 링크

감사합니다

㈜와이드라인 주소 : 서울특별시 구로구 디지털로27길 36,6층 603-1호(구로동, 이스페이스)
TEL : 02-2038-0150 FAX : 02-2038-0852