





정보 기술 접근성 리포트

# 가상 키보드 접근성



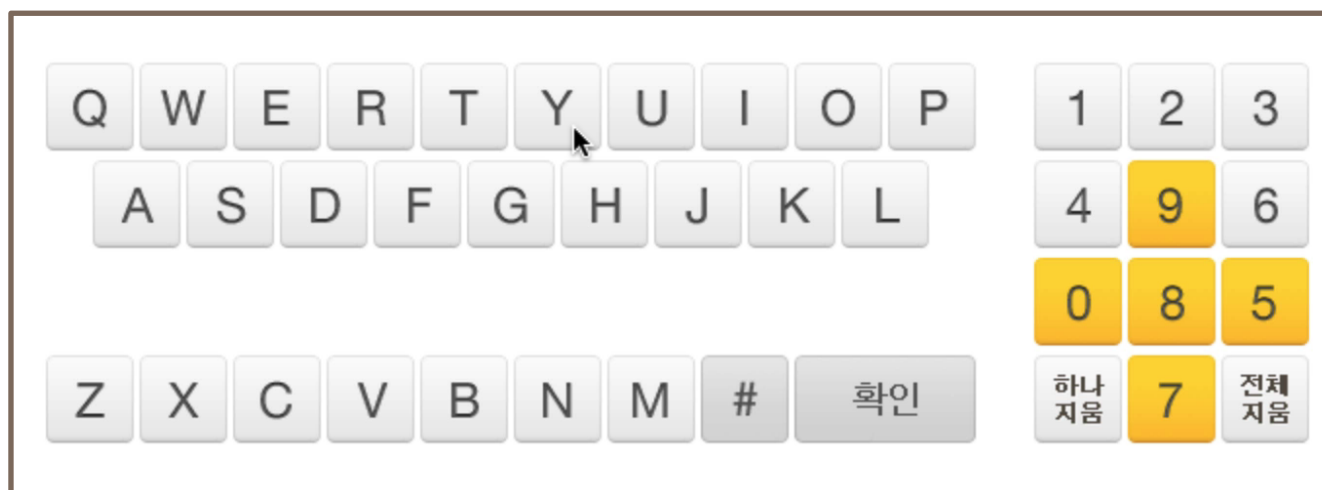
야무





# 가상 키보드란 ?

물리적인 키보드가 아니라 화면에 가상으로 나타나는 키보드입니다.  
가상 키보드를 사용하는 이유는 **개인 정보를 보호하기 위해서** 입니다.





주민등록번호, 은행 계좌의 비밀번호 등과 같이 개인정보를 물리적인 키보드로 입력할 경우  
**해킹프로그램이 사용자가 키보드로 입력하는 키 값을 탈취하여 개인정보를 빼낼 수 있는**  
위험을 미연에 방지하고자 하는 목적을 가지고 있습니다.







## 가상 키보드, 데스크탑 웹 환경

공인인증서 로그인

아이디 로그인(개인고객)

KB튼튼간편인증

아이디

YAMOO9

로그인

사용자암호

.

KB국민은행

QWERTYUIOP

ASDFGHJKL

KB 마우스 입력기

ZXCVBNM#확인

123

496

085

하나  
지움7전체  
지움

회원가입

버튼을 이용하여 주시기 바랍니다.



## 가상 키보드, 모바일 앱 환경

KB 국민은행

지훈(Jee Hoon)

은행개인 | yesign 만료일

영문/숫자/특수문자 조합(10자리 이상)

확인

1234567890

qwertyuiop

asdfghjkl

↑zxcvbnm↵

#+=영어SPACE재배열

아이디 로그인

설정

공인인증서 | 아이디 | 비밀번호 | 지문

특수기호

닫기

이용자 아이디 입력

로그인

이용자 비밀번호 입력

공인인증서가 없는 고객은 조회거래만 가능합니다.

123

🌐

🗣

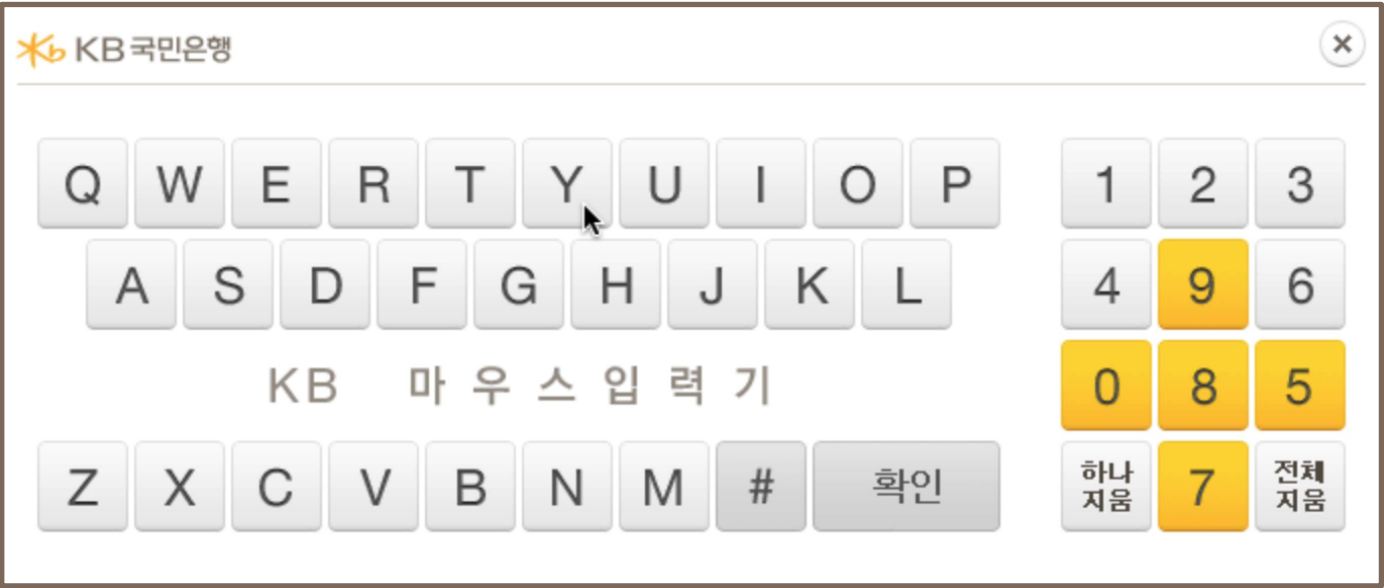
간격

다음문장

Accessibility Open Academy

Internet Accessibility Technology Conference 2017





가상 키보드 자판을 살펴보면 **QWERTY 유형**과 **ABC 유형**이 있습니다.  
QWERTY 혹은 ABC 자판 배열은 **일반적인 키보드와 자판이 동일**하기 때문에  
**사용자가 쉽게 적응하여 빠르게 입력 가능** 합니다.

그러나 **입력 값의 좌표**와 사용하고 있는 **자판의 배열** 또한 **가로채기 쉬워**  
**사용자가 입력한 정보가 손쉽게 유출될 수 있다**는 단점이 있습니다.



입력 정보 유출 문제를 해결하기 위해 무작위 키 배열을 사용하는 방식도 등장했지만, 무작위 키 배열의 경우 사용자가 사용하는데 매우 불편하다는 치명적인 단점 때문에 **최근에는 이를 응용하여, 무작위로 여백을 삽입하는 방식을 사용하고 있습니다.**

이 방식은 **기존 QWERTY 자판에 임의의 무작위 여백을 삽입 함으로써 전체적인 배열은 유지하고, 입력 좌표를 통한 입력 키에 대한 유추를 어렵게 만든 방식입니다.**



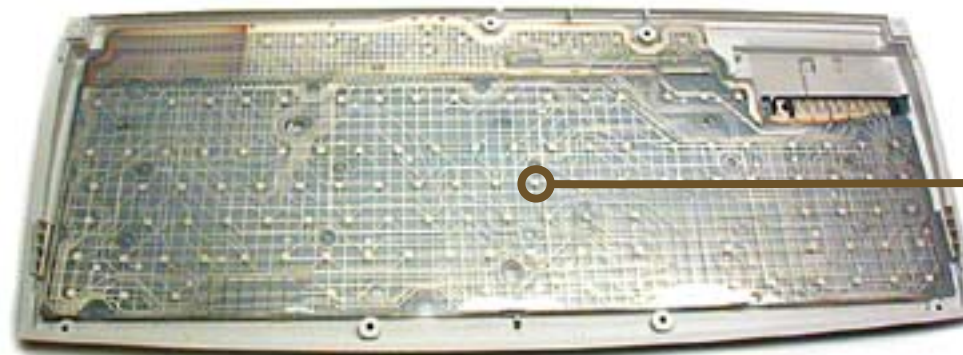


# 가상 키보드 & 보안





일반적으로 **키보드에 키를 입력**하면 키보드에 **연결된 마이크로 프로세서**가  
키 정보를 컴퓨터에 연결하는 케이블을 통해 신호를 보냅니다.







키보드를 통해 **입력된 데이터가 운영체제에 도달**하면 키보드 장치 드라이버에서  
문자, 숫자 및 기호에 대한 **키보드 "스캔 코드"의 변환을 처리**하게 되는데  
이를 **키로거**Keylogger 가 가로칩니다.





해커가 사용자 계정 정보를 가로채기 위해  
사용자의 **입력을 기록하는 악성 코드인 키로거를 사용하여,**  
**키 입력이 이루어지게 되면 운영체제를 통해 정보를 빼내갈 수 있습니다.**





# 키로거 유형

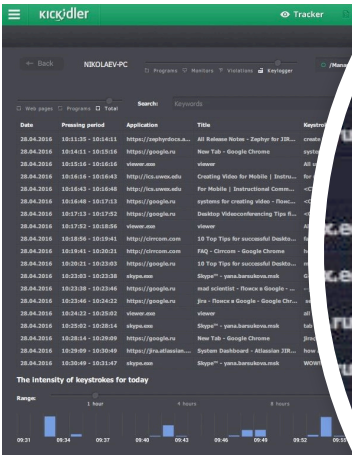
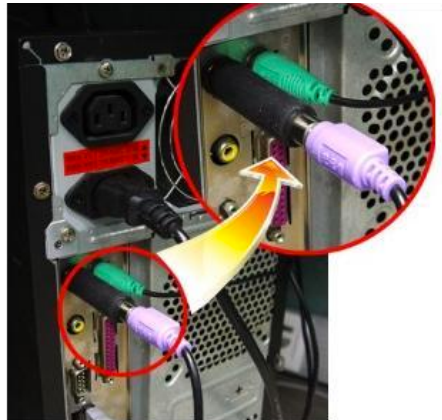
하드웨어 유형

소프트웨어 유형

PS/2 Keylogger

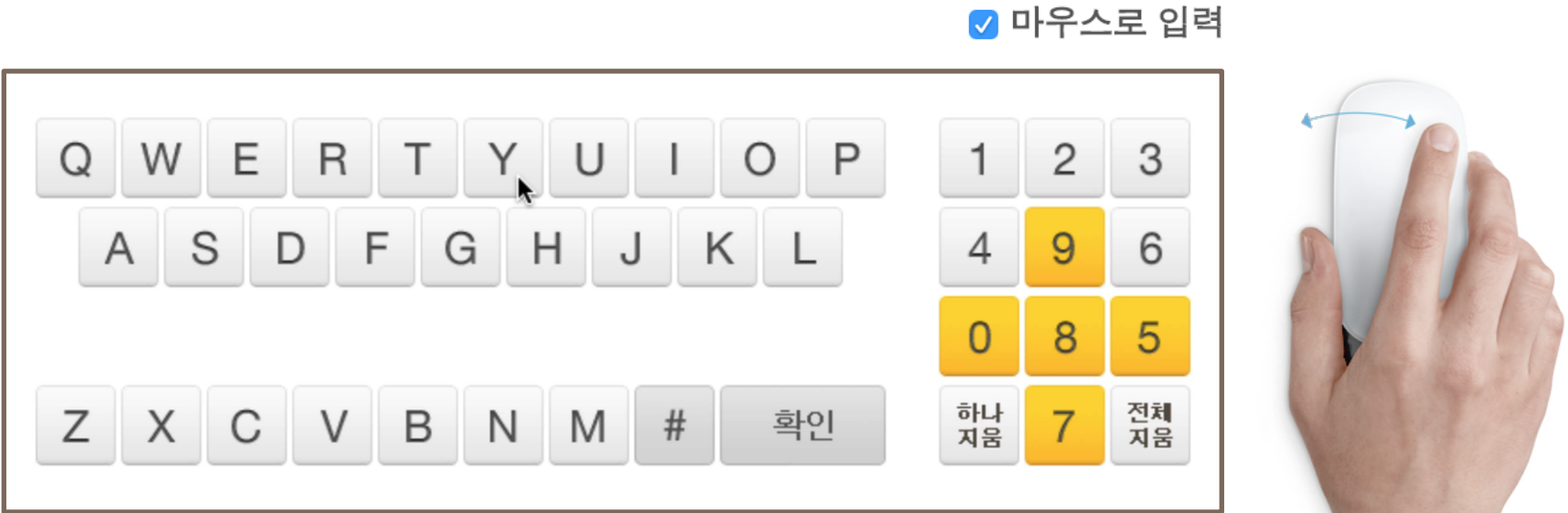


USB Keylogger



Title	Keystrokes
All Release Notes - Zephyr for JIR...	create test↵
New Tab - Google Chrome	systems for v--creating video↵
viewer	All users
Creating Video for Mobile   Instru...	for mobilre--↵
For Mobile   Instructional Comm...	<CTRL + C>
systems for creating video - Поиск...	<CTRL + V> find↵
Desktop Videoconferencing Tips fi...	<CTRL + C><CTRL + V>↵
viewer	All users
10 Top Tips for successful Desko...	faq↵
FAQ - Cirrcom - Google Chrome	how can i contact you↵
10 Top Tips for successful Desko...	mad s
- yana.barsukova.msk	G--Hoe--w is yout--
- Поиск в Google - ...	+jira
Google Chr...	gan



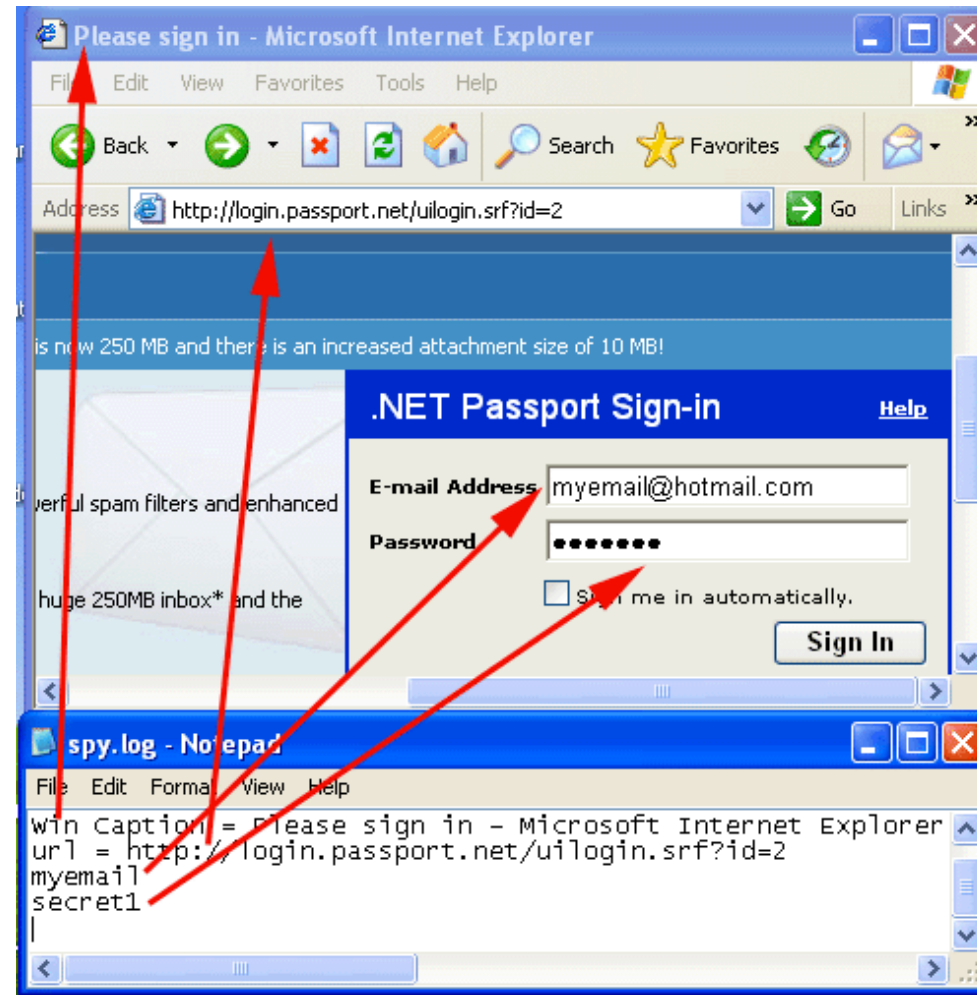


개인의 '정보를 보호하기 위해' 등장한 **가상 키보드**는 일부 해킹 시도는 무력화 할 수 있지만,  
**모든 해킹 시도에서 안전하다고 보장할 수는 없습니다.**





마우스를 사용하면 가상 키보드를 통해 사용자가 입력한 키 정보를 감출 수 있지만,  
키로거는 모든 마우스 클릭에 대해 클릭 한 위치와 순서를 정확히 보여주는 이미지를 캡처 할 수 있습니다.



키로깅의 이와 같은 접근 방식은 마우스 인터랙션에 따른 키보드 레이아웃 화면을 획득 함으로  
일반적인 보안 기술을 회피할 수 있고, 키보드 배치 방식에 관계 없이 보고 있는 내용과 클릭 한 위치를 기록합니다.



# LiveSlides web content

To view

**Download the add-in.**

[liveslides.com/download](https://liveslides.com/download)

**Start the presentation.**



고객님의 안전한 서비스 이용을 위해서 아래와 같은 보안프로그램 설치가 필요합니다.

전체설치 버튼을 클릭하시면 인터넷뱅킹 이용에 필요한 보안프로그램을 자동으로 설치합니다.  
아래 설치현황에 설치가 모두 완료된 경우 버튼 또는 홈페이지 버튼을 클릭하여 이동합니다.



보안 필수 프로그램

프로그램명	내용	설치현황	설치관리
 통합설치관리 (Veraport)	인터넷뱅킹 관련 설치프로그램을 통합하여 관리하기 위한 프로그램입니다. <a href="#">자세히 보기</a>	미설치	<a href="#">다운로드</a>
 공인인증서 보안 (XecureWeb)	공인인증서 전자서명을 지원해주는 프로그램입니다. <a href="#">자세히 보기</a>	미확인	<a href="#">다운로드</a>
 키보드 보안 (TouchEnkey)	키보드로 입력되는 중요데이터 암호화 및 위/변조 방지 프로그램입니다. <a href="#">자세히 보기</a>	미확인	<a href="#">다운로드</a>
 개인PC방화벽 (Netizen)	실시간 해킹차단 및 바이러스 검색 치료프로그램입니다. <a href="#">자세히 보기</a>	미확인	<a href="#">다운로드</a>
 보안로그 (IPinside)	보안로그 수집 프로그램입니다. <a href="#">자세히 보기</a>	미확인	<a href="#">다운로드</a>

• 통합설치 프로그램에 의한 자동설치가 어려우실 경우, 보안프로그램 안내 메뉴에서 개별 수동 설치하실 수 있습니다. [바로가기](#)





## 가상키보드 90% 이상 해킹 성공



단독보도 | 가상키보드 보안성 실험 결과

금융사 35곳 중 31곳  
위택스, 공공 I-PIN  
RCS 공격에 뚫렸다

더 스쿠프 The SCOOP 가 발표한 자료에 따르면 원격조정시스템 RCS 해킹 툴을 이용해  
국내 금융회사 35곳(저축은행 제외), 위택스(지방세 인터넷 납부시스템), 공공 I-PIN에 설치된  
가상 키보드 보안 능력을 검증한 결과, RCS에 의한 해킹 성공률이 무려 90%에 육박했습니다.





가상 키보드 + 보안 프로그램의 보안은  
100% 안전을 보장하지 못합니다!





# 가상 키보드 & 법적 근거





**"가상 키보드의 보안능력이 약하다"**는 지적은 이미 수년 전부터 제기 되어 왔습니다.  
그렇다면 보안이 취약한 가상 키보드 및 보안 프로그램 설치를  
기업에서 아직까지 고집하고 있는 이유는 무엇 일까요?





**"가상 키보드의 보안능력이 약하다"**는 지적은 이미 수년 전부터 제기 되어 왔습니다.  
그렇다면 보안이 취약한 가상 키보드 및 보안 프로그램 설치를  
기업에서 아직까지 고집하고 있는 이유는 무엇 일까요?







세상을 바로 읽는 진실의 힘  
**팩트체크**  
F A C T C H E C K

행정규칙

본문 제정·개정이유 연혁 관련법령 첨부파일 법령체계도 법령비 법령주소복사 법령용어 화면내검색 새창

**제5절 전자금융업무**

☐ 제29조(전자금융거래 시 준수사항) ①금융기관 또는 전자금융업자는 다음의 경우를 제외하고는 전자자금이체 시 일회용 비밀번호(보안카드를 포함한다)를 적용하여야 한다. <개정 2009.7.24>

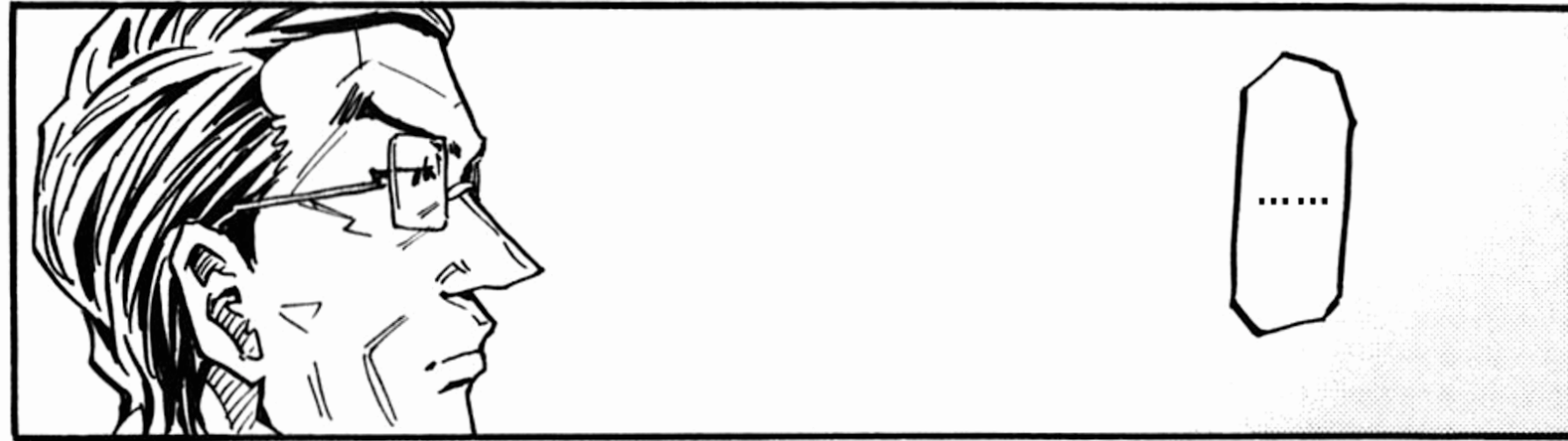
3. 이용자PC에서의 정보유출을 방지하기 위해 이용자의 접속 시 우선적으로 이용자PC에 개인용 침입차단시스템, 키보드해킹방지 프로그램 등의 보안프로그램을 설치할 것(다만, 고객의 책임으로 본인이 동의하는 경우에는 보안프로그램 해제 가능)

해당 규정은 2010년 8월 12일의 시행세칙 이고,  
2012년 5월 29일 시행세칙이 개정 되면서 관련 내용은 폐지되었습니다.  
결국 기업은 이미 폐지된 내용을 설치 근거로 내세우고 있는 것입니다.





전자금융감독규정 시행세칙의 개정을 시작으로 금융감독원에서  
**자율 보안을 선언**하였기 때문에 **가상키보드를 꼭 써야 할 이유는 없습니다.**



자율 보안 이지만...  
보안 가상 키보드 프로그램을  
설치하도록 제공하지 않으면  
취약점으로 진단 하겠네.




다만, 금융보안원 보안 취약점 진단에서  
**보안 가상 키보드 프로그램을 설치하도록  
제공하지 않으면 취약점으로 진단**을 하기  
때문에 시행세칙에서 제외 되었다 하더라도,  
**현실적으로는 설치를 하도록 유도할 수 밖에  
없다는 후문도 있습니다.**



# 가상 키보드 & 접근성





  
  
 표시  
  
  
[로그인에 어려움이 있으신가요?](#)

카드 연결  

MasterCard

카드 번호

만료 MM/YY

CSC(3자리)

Gireum 3(sam)-dong Seongbuk-gu, Seoul, not applied(n/a) 136-809

저장

**가상 키보드**는 사용자 입력 값을 받아야 하는 입력서식 중에서도 **보안이 필요한 콘텐츠 유형에 사용** 되고 있습니다.  
이러한 입력양식은 특별한 분야에서 제한적으로 사용 되는 것이 아니라 **금융, 결제 등의 분야에서 널리 사용** 되고 있고,  
그 유형으로는 사용자 **로그인, 카드번호 입력, 각종 비밀번호 입력** 등을 들 수 있습니다.  
웹을 활용하는 사용자라면 누구나 쉽게 접할 수 있는 유형입니다.





• • • • •  
접근할 수 없는 암호입력 키패드



## 암호입력 키패드의 인식 및 키보드 접근

— 간편결제 서비스에서 제공하는 암호입력 화면 사례 —

SmilePay

결제금액 26,900원

KB국민카드

일시불

☒ KB 포인트리 사용

비밀번호 재설정 >

보안키보드 작동중

3	0	5	8
1	4		6
2	7	9	←

네이버페이 비밀번호

김\*\*\*\*\*님이 접속중

비밀번호를 입력하세요.

비밀번호를 잊어버리셨나요?  
비밀번호 재설정을 위해서는 본인인증이 필요합니다.

비밀번호 재설정

2	5	1	9
4	7	6	8
0			3
전체삭제		←	

RocketPay

로켓페이 비밀번호 설정

로켓페이 이용을 위한  
비밀번호를 설정해주세요.

보안 키보드 작동중

9	0	3	6
1	2		8
4	7		5
←		입력완료	

11Pay - Chrome

11Pay 결제

안전한 결제를 위해  
결제 비밀번호를 입력해주세요.

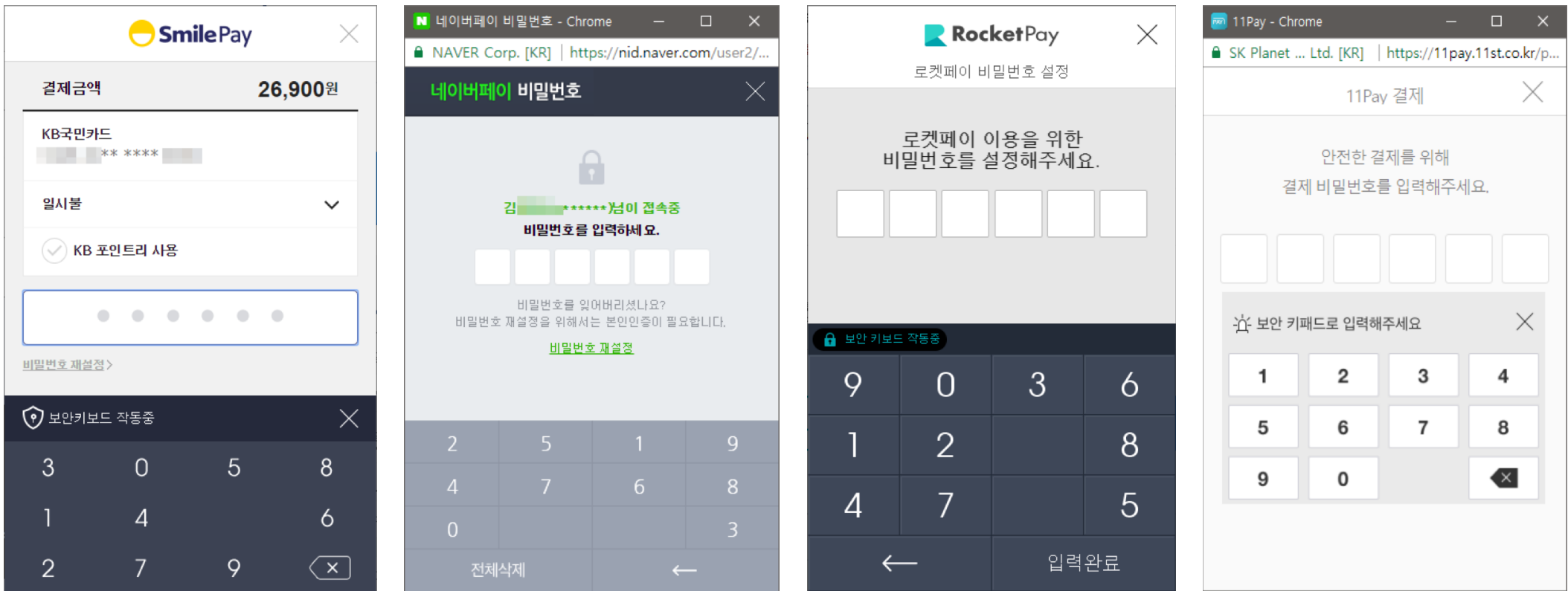
보안 키패드로 입력해주세요

1	2	3	4
5	6	7	8
9	0		←



## 암호입력 키패드의 인식 및 키보드 접근

— 간편결제 서비스에서 제공하는 암호입력 화면 사례 —

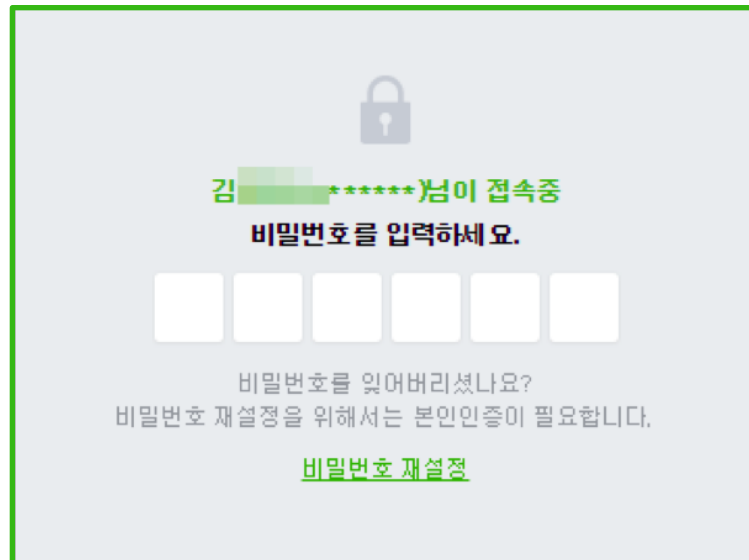


시각장애인이 아닌 사용자의 경우 암호입력 키패드를 사용할 수 있지만,  
스크린리더 사용자의 경우, 암호입력 키패드를 인식할 수 없는 등의 문제가 발생합니다.



Nvaccess

스크린리더 재연절차



NVDA 음성 출력 뷰어

헤딩 레벨 2  
비밀번호를 입력하세요.  
비밀번호를 잊어버리셨나요?  
빈줄  
비밀번호 재설정을 위해서는 본인인증이 필요합니다.  
링크  
비밀번호 재설정  
테이블 5 행, 0 열  
1행 1열  
클릭가능  
전체삭제  
3열  
클릭가능  
2행 1열  
클릭가능  
2열  
3열  
클릭가능  
4열  
클릭가능  
3행 1열  
클릭가능  
2열  
클릭가능  
3열  
클릭가능  
네이버페이 비밀번호 - Internet Explorer  
바탕 화면

음성으로 들리는 내용 중  
가장 심각한 이슈는  
가상 키패드 숫자를 전혀  
인식할 수 없다는 것입니다.

☐ NVDA 시작시 음성 출력 뷰어 실행 (S)



markup.html — Example - @yamoo9

markup.html x

```
<td>
  <a class="key" onclick="doClick('0')">
    <span class="number key1_1"></span>
  </a>
</td>
```

가상 키패드 버튼이 링크로 구현 되어 있지만, 링크에는 기능을 알 수 있는 링크 텍스트가 전혀 제공되지 않은 상태입니다.

스크린리더로 들을 수 있는 텍스트 정보가 전혀 없기 때문에 가상 키패드에 접근 하더라도 키패드 기능을 인식할 방법이 없습니다.





markup.html — Example - @yamoo9

markup.html x

```
<td class="rocketpay-keypad-td">
  <a class="rocketpay-keypad-key" href="#" data-key="E17qphjHIM">
    <span class="rocketpay-keypad-position-2"></span>
  </a>
</td>
```

다른 간편결제 서비스의 암호 입력 키패드 마크업 이지만 이전 사례와 크게 다르지 않습니다.  
이 또한 키패드 영역에 키를 구분할 수 있는 텍스트 정보를 전혀 제공하지 않은 상태입니다.


스크린리더를 통해 키패드 내용을 듣고 입력해야 하는 시각장애인은 키패드 정보를 음성으로 인식할 수 없어 암호를 입력하는 것이 불가능하므로 연결된 서비스의 이용이 불가능한 문제를 발생 시킵니다.



markup.html — Example - @yamoo9


markup.html ✕

```
<td>
  <a class="key" onclick="doClick('0')">
    <span class="number key1_2"></span>
  </a>
</td>
```

 RocketPay

로켓페이 비밀번호 설정

로켓페이 이용을 위한  
비밀번호를 설정해주세요.



시각장애인을 위한 정보만 누락된 것은 아닙니다.

키보드만 사용가능한 사용자가 키보드로 초점을 이동하여 보안 키패드에 접근하는 것 또한 불가능합니다.

암호를 입력 하는 키패드를 a 요소로 구성하고 href 속성을 정의하지 않은 상태입니다. 결과는 키보드로 링크에 접근할 수 없어 키패드 입력이 불가능합니다.



```
style.css — Example - @yamoo9

markup.html x style.css x

<button
  id="tnn3qbpvfy"
  alt="Virtual Keyboard"
  class="nfilter_keypad_button"
  ondragstart="return false;"
  onmousedown="return false;"
  onmouseup="javascript:nFilterOnKeyClick(this)"
  ondoubleclick="return false;"
  ontouchstart="javascript:nFilterOnTouchstart()"
  ontouchend="javascript:nFilterOnTouchend(this)">
</button>

.nfilter_keypad_button {
  ...
  outline: none;
  ...
}
```

키패드를 구성하는 버튼에 `outline: none` 스타일을 사용하고 있어 키보드로 접근하더라도 어떤 키패드에 접근했는지 알 수가 없는 상태입니다.



김 [redacted] \*\*\*\*\*님이 접속중

비밀번호를 입력하세요.

\* \*

키패드를 입력할 때 현재 몇 글자가 입력 되었는지 확인하는 것은  
매우 중요한 과정이며 반드시 필요한 정보입니다.



김\*\*\*\*\*님이 접속중

비밀번호를 입력하세요.

Two green boxes with asterisks and four white boxes for password input.

“비밀번호를 입력하세요”와 “비밀번호를 잊어버리셨나요?” 사이  
입력해야 할 개수와 현재 입력된 개수를 알 수 있는 박스 영역이 존재하지만,

NVDA 음성 출력 뷰어

비밀번호를 입력하세요.  
비밀번호를 잊어버리셨나요?  
빈줄  
비밀번호 재설정을 위해서는 본인인증이 필요합니다.  
링크

암호 글자 수에 대한 정보가 표시되는 영역에서 음성으로는 아무런 정보도 인지되지 않습니다.  
사용자가 **입력해야 하는 입력 양식이 있다는 것**을 알 수 없고, **총 몇 글자를 입력해야 하고**  
**현재 몇 글자까지 입력 되었는지 구분할 수 있는 정보가 전혀 없습니다.**





```
markup.html — Example - @yamoo9
markup.html x

<h2 class="h2 center">비밀번호를 입력하세요</h2>
<div class="password center">
  <span class="charactor on" id="key_1"></span>
  <span class="character" id="key_2"></span>
  <span class="character" id="key_3"></span>
  <span class="character" id="key_4"></span>
  <span class="character" id="key_5"></span>
  <span class="character" id="key_6"></span>
</div>
```

글자수를 확인할 수 있는 텍스트 정보를 제공하고 있지 않습니다.  
IR(Image Replacement) 기법을 사용하여 글자수를 구분하는  
배경 이미지를 제공하면서 그와 동등한 수준의 대체텍스트를 제공  
하지 않아 스크린리더로는 어떤 정보도 인식할 수 없는 것입니다.



markup.html — Example - @yamoo9

markup.html x

```
<button type="button" class="bt_scu active" id="scu1" name="keyPadPassword">
  <span id="b0" class="spr active">*</span>
  <span id="b1" class="spr active">*</span>
  <span id="b2" class="spr">*</span>
  <span id="b3" class="spr">*</span>
  <span id="b4" class="spr">*</span>
  <span id="b5" class="spr">*</span>
</button>
```

다른 간편결제 서비스 마크업을 살펴보면

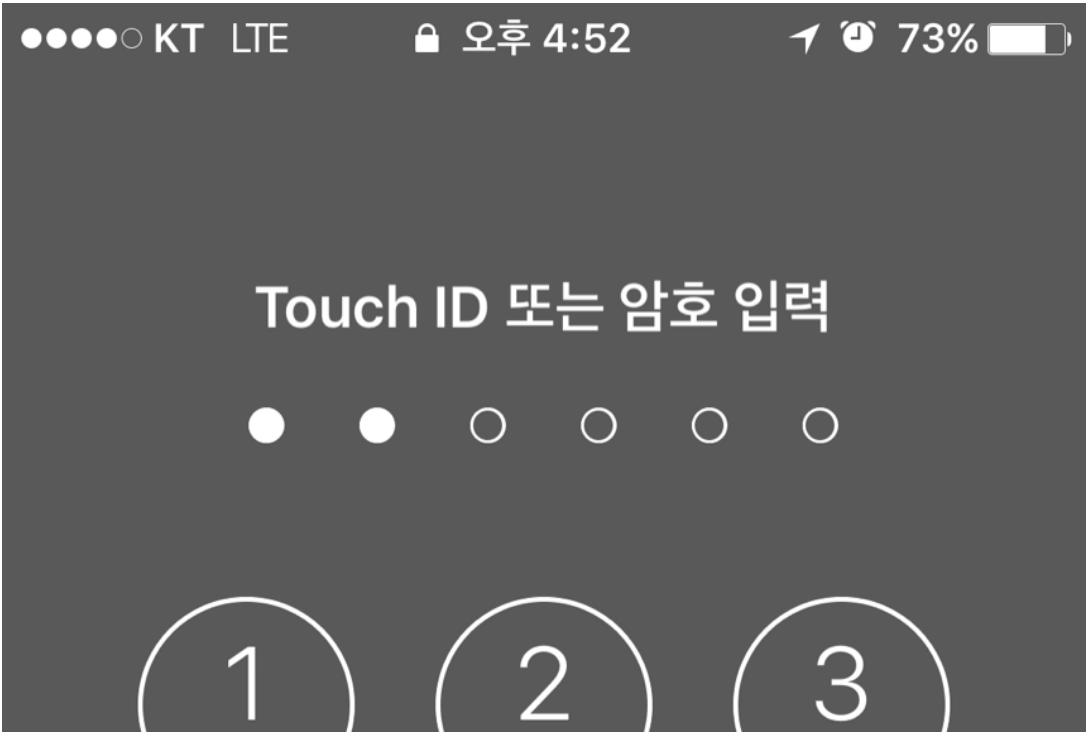
해당 글자수 영역에 \*를 제공하여 글자수가 몇 개인지 확인은 가능하지만 현재 입력된 글자수와 입력되지 않은 글자수를 구분할 수는 없습니다.

서로 다른 class를 사용하여 시각적으로 입력 된 글자수를 구분하고 있지만 동등한 수준의 대체텍스트를 제공하고 있다고 볼 수 없습니다.

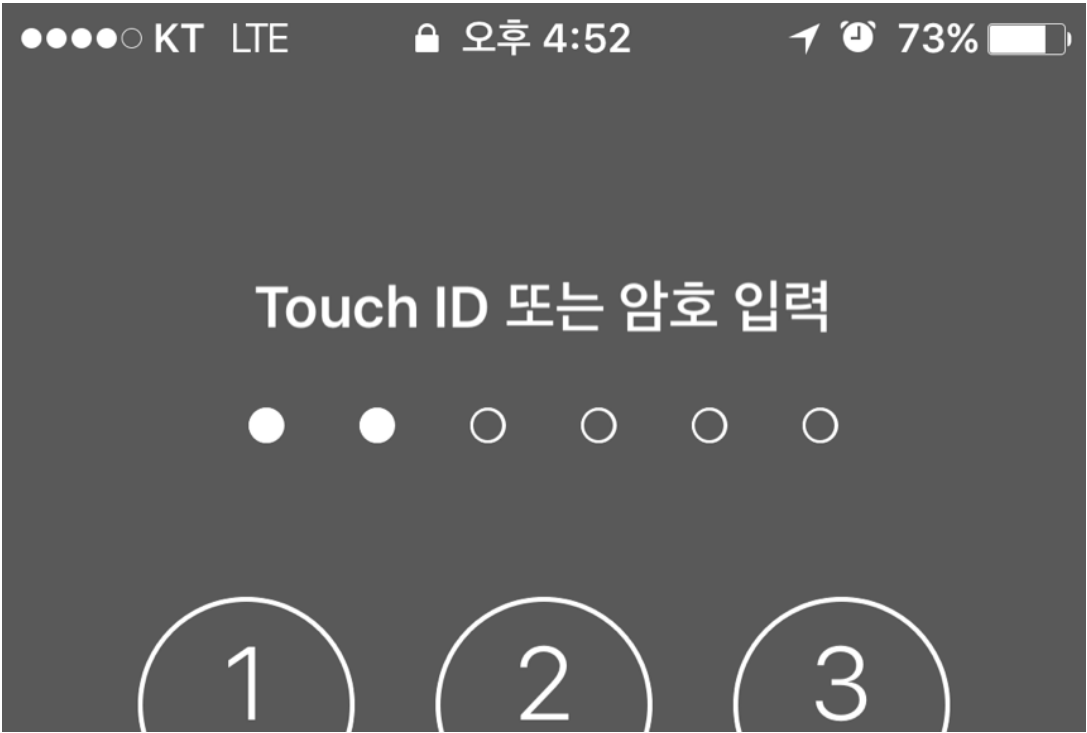


암호 키패드에 대체텍스트를 제공하지 않고, 키보드 초점의 접근을 막았으며, 현재 입력된 글자수를 확인할 수 없는 문제는  
간편 결제 서비스에서 모두 동일하게 나타나고 있어 장애인이 동일 유형의 서비스에 접근하는 것이 불가능한 상태입니다.

뿐만 아니라, 해당 간편결제 서비스들은 추가 적립 등의 혜택을 함께 제공하고 있어 서비스 접근성 뿐만 아니라  
사용자의 금전적인 손해까지 발생하고 있는 상황입니다.



**모바일 OS 암호입력 필드 제공 방법을 참고하면  
점으로 표시된 입력 글자수 표시 영역을 음성으로 확인했을 때  
“암호필드 6개 중 2개의 값 입력됨”과 같은 형태로  
음성이 출력되고 있습니다.**

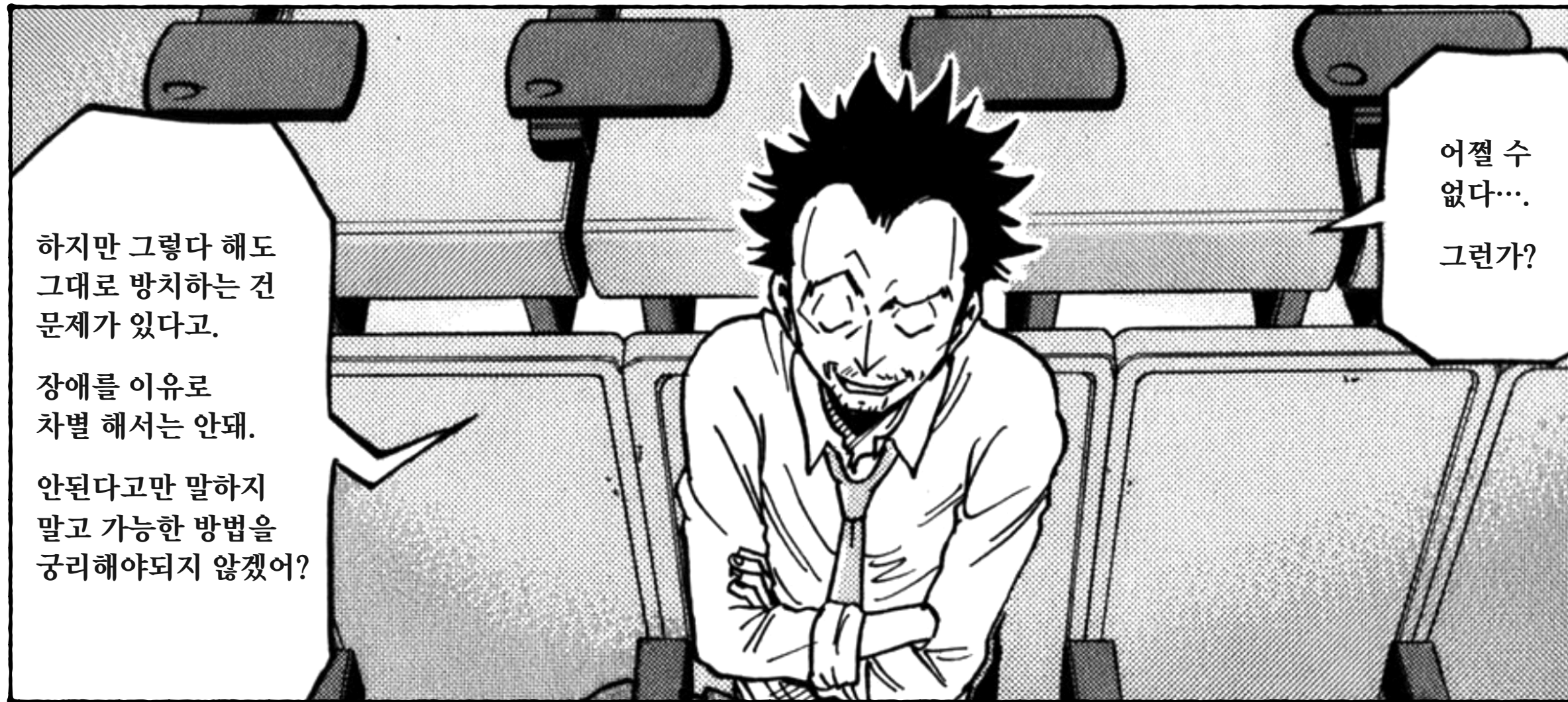


웹 서비스에서도 유사한 형태로 간결하고 명확하게  
현재 글자수와 전체 글자수 정보를 인식할 수 있도록  
하여 접근성을 보장해야 합니다.





**웹에서 제공하는 가상 키패드는 기계적인 방식으로 접근하는 것을 차단하는 형태로 구현되어 있습니다.**  
하지만 스크린리더 사용자는 보조기술을 통해 콘텐츠에 접근해야 하기 때문에, 사용자를 위한  
**접근성을 제공하는 것이 현실적으로 불가능한 상태입니다.**



기술적으로 불가능하다고 해서 장애인이 보안 키패드를 이용할 수 없는 이슈를 그대로 방치한다면  
**장애가 있는 사용자는 해당 서비스를 전혀 이용할 수 없는 상태로 방치하는 것과 다르지 않습니다.**

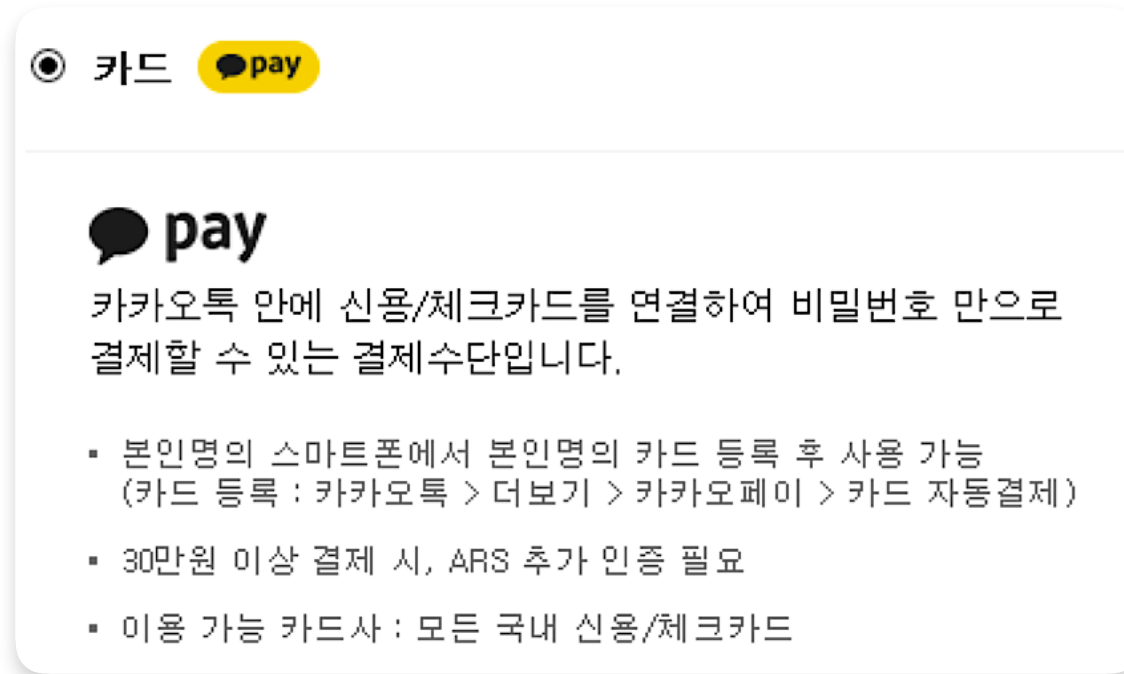
**결국 장애를 이유로 서비스를 사용할 권리를 박탈하고 차별하는 행위로  
이는 장애인차별금지법의 취지에 반하는 것이 됩니다.**







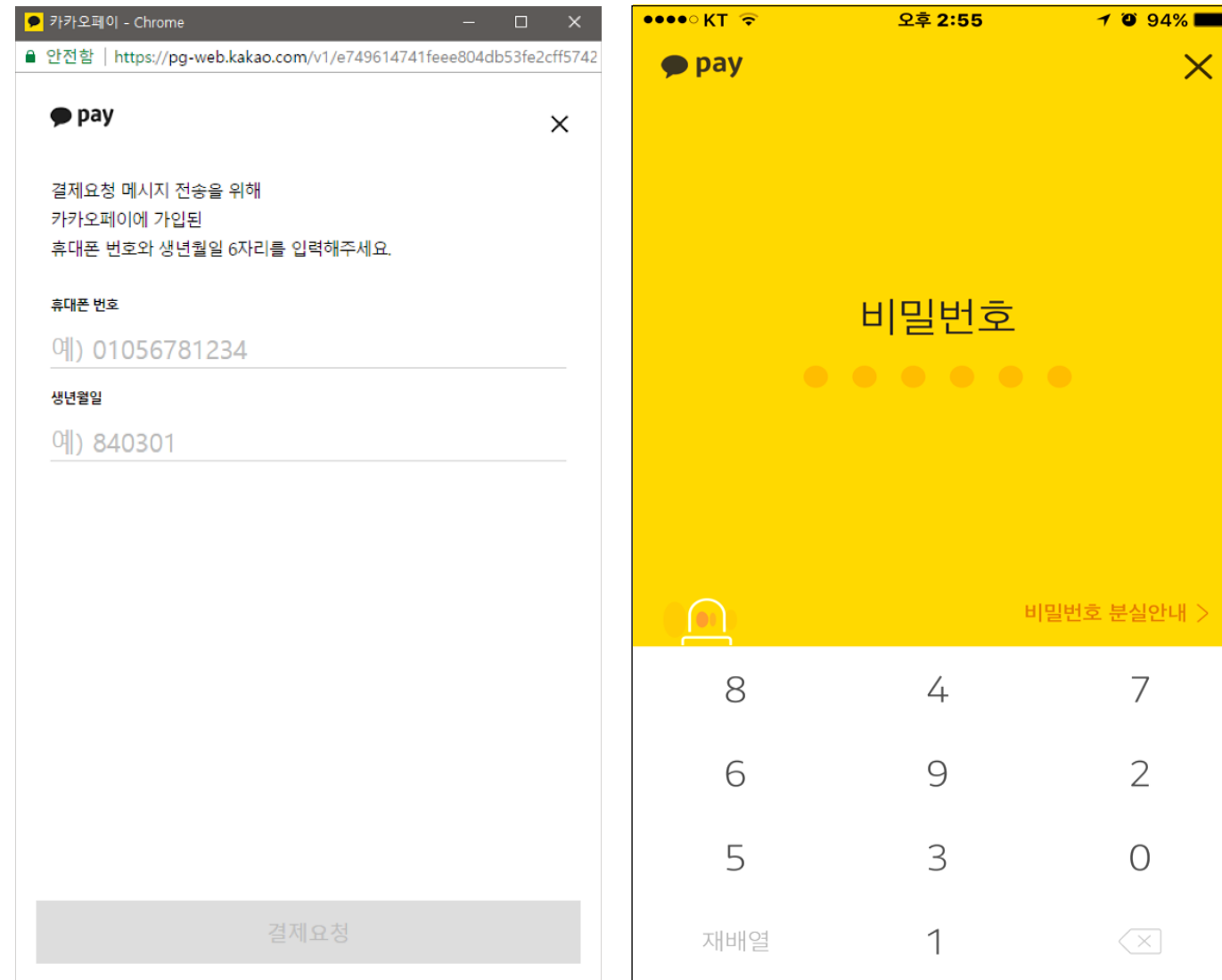
• • • • • • • • • •  
모바일 애플리케이션을 이용한 대체수단



보안 키패드를 대체할 수 있는 보안 수단이 가상키보드 + 보안 프로그램 뿐 일까요?

PC와 모바일에서 결제 서비스를 제공하는 간편결제 서비스 사례를 살펴보면  
또 다른 **대체 수단 사용이 가능함을 확인** 할 수 있습니다.



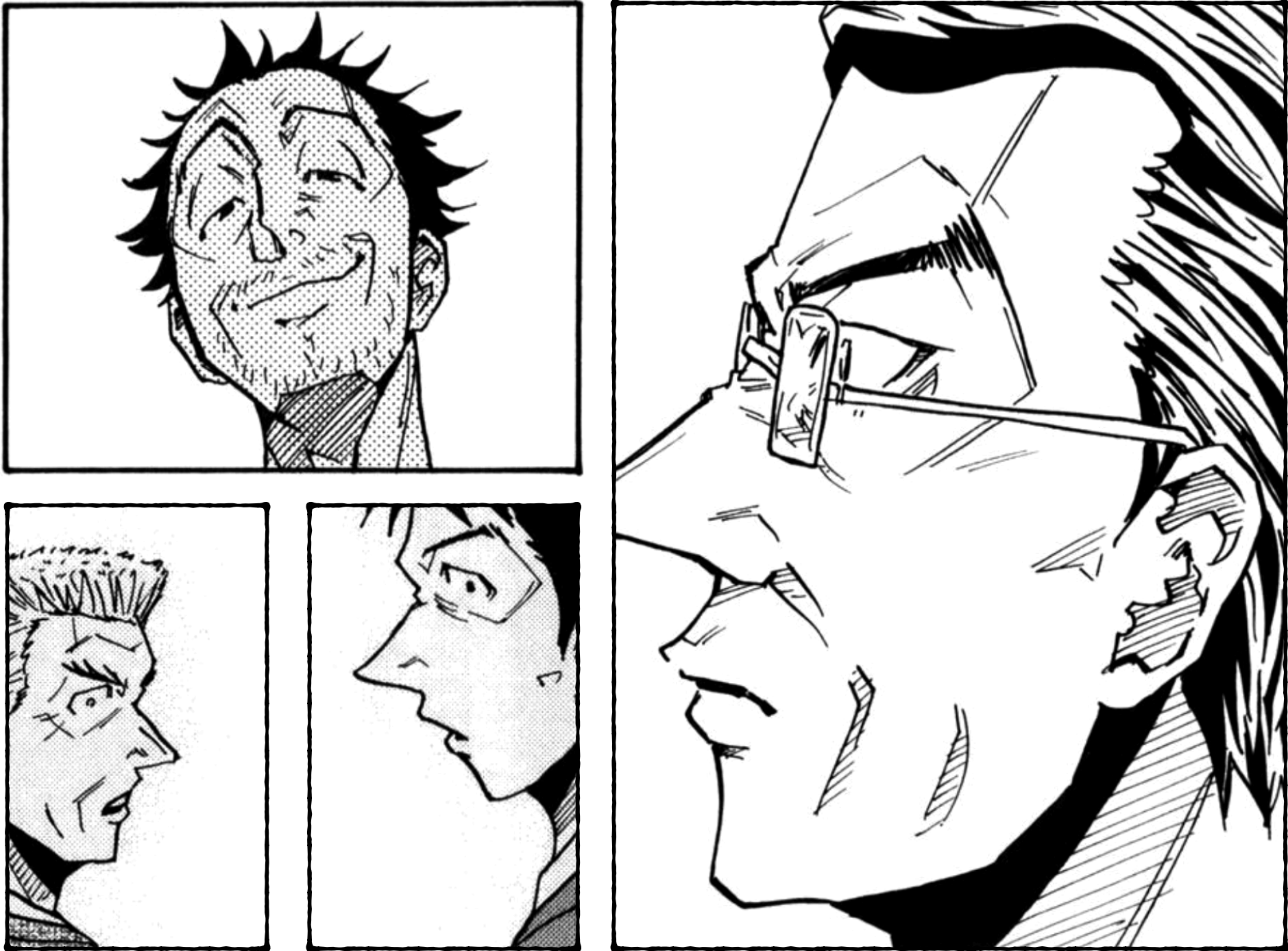


암호입력 화면 대신, 휴대폰 번호, 생년월일 입력 화면이 나타나고, 결제요청 하면  
**모바일 애플리케이션의 결제수단과 연동을 통해 결제 가능** 합니다.

웹과 달리 앱 환경에서는 키보드 정보를 읽어주는데 보안과 관련된 기술적 이슈가 없습니다.

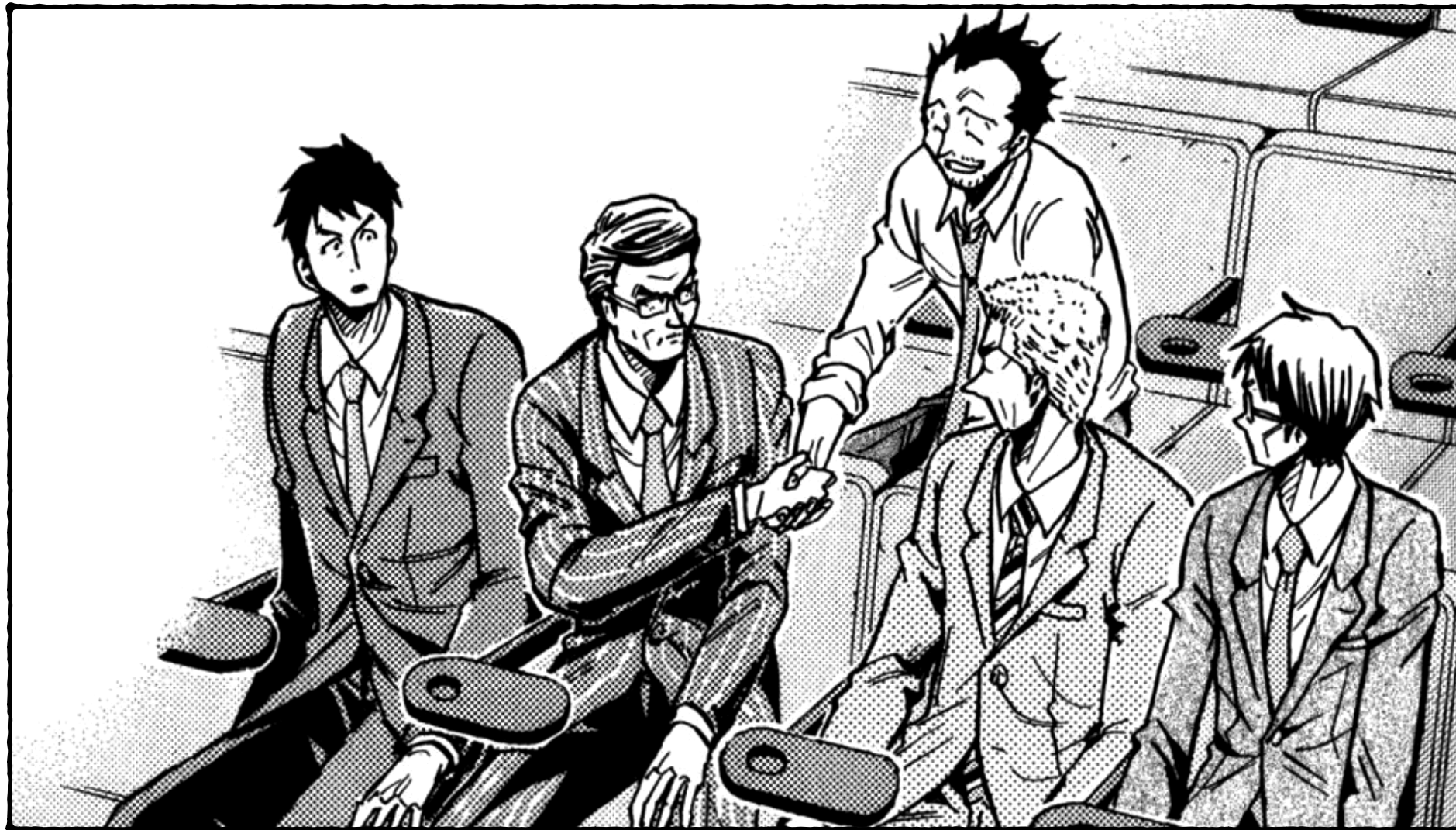












함께 제공되는 또 다른 인증수단은 특히 **장애인의 접근성을**  
**보장하는 수단으로 선택되어야 합니다.**

**보안 정책과 인증수단 제공을 다변화하여 장애가 있는 사용자도**  
**서비스 이용에 문제가 없도록 하는 것이 가장 적절한 개선방안이 될 것입니다.**



# 정보 기술 접근성 리포트 2017







▶ CAPTCHA (캡차)
▼ 가상 키보드(보안 키보드)
가상 키보드란?
가상 키보드와 보안
가상 키보드 제공의 국내 법적 근거
▼ 가상 키보드 제공 사례 분석
접근할 수 없는 암호입력 키패드
대체수단을 함께 제공하는 키패드
모바일 애플리케이션을 이용한 대체수단
HTML로 구현된 가상 키보드
보안 키보드 대체 수단
지연이체 대체 수단
1회용 액세스 토큰 대체 수단
가상 키보드에 대한 제언
보안키보드의 보안
▶ 미디어 플레이어
참고자료



입력하기까지 제한 시간도 없고, SMS를 전송 받을 휴대폰만 있다면 모두 어려움 없이 사용이 가능하다.

지연이체 대체 수단

이 방법은 착오 송금 또는 금융 사기를 막기 위한 것으로 은행계좌에 있는 돈을 찾거나 보낼 때 일정 시간 '지연' 시켜 처리한다. 이 때 지연 시간이 금융 사기범들에게 넘어가는 돈을 지키는 역할을 한다.

국내 모든 금융기관에서는 2015년 10월 16일부터 "지연이체" 제도를 도입 시행하고 있다. 다만 신청자에 한해 이 서비스를 이용할 수 있고 기본적으로 지연이체가 사용되고 있지 않다.  
반면 중국에서는 급증하는 전화 금융사기(보이스 피싱) 방지를 목적으로 현금 자동 입출금기(ATM)를 이용한 송금 때 24시간 후에 이체되도록 하는 방안을 대다수 금융기관에 도입(2016년 12월)하였다. 은행 간 계좌 이체는 실시간 또는 길어야 2시간 이내 이루어 졌는데 기존의 제도를 대폭 조정한 것이다.



중국뿐 아니라 해외에서도 지연이체 방법을 사용하고 있는데 미국, 일본, 홍콩, 독일 사례를 살펴 보면 나라 별 금융기관마다 조금씩 다르긴 하지만 금융 사기 문제를 해결하기 위한 방책으로 지연 이체 처리하는 것을 알 수 있다.

구분	주요내용
----	------

클라이언트는 사용자 계정 정보(ID/Password)와 current\_time 변수 정보(서버의 데이터베이스, 클라이언트 스토리지에 모두 저장)를 API를 통해 서버에 토큰을 요청하면, 서버는 클라이언트의 입력을 해석하고 해시 토큰(예: 58f52c075aca5d3e07869598c4d66648)을 생성하고 이를 서버 측 데이터베이스에 저장하고, 클라이언트에 응답으로 전송한다.



클라이언트는 서버로부터 전송 받은 토큰을 클라이언트 스토리지(예: sessionStorage. 세션 스토리지는 세션이 만료되면 파괴 된다)에 저장하고, 토큰 + 인증 요청 과정에서 보낸 current\_time 변수를 사용하여 새 해시 토큰(main\_token이라고 한다)을 생성한다.

서버 또한 동일한 알고리즘을 사용하여 작업을 수행하고 클라이언트와 일치하는 토큰을 만든다.



클라이언트가 서버 API를 통해 요청(Request) 할 때마다 생성된 메인 토큰(main\_token)을 서버에 보내면, 서버는 서버에서 생성된 메인 토큰과 클라이언트가 보낸 메인 토큰을 비교한다. 각 토큰이 일치하면 데이터 리소스에 접근 가능한 사용자임을 인증한다.



# LiveSlides web content

To view

**Download the add-in.**

[liveslides.com/download](https://liveslides.com/download)

**Start the presentation.**



# 리/포/트/작/성/에 힘/쓰는/사/람/들



조은

apes0123@gmail.com



김데레사

seulbinim@gmail.com



한정기

hanjeonggi@gmail.com



야무

yamoo9@naver.com



지성봉

publisher@publisher.name



김혜일

haeppa@gmail.com

모두에게 열려있는 자유로운 웹 세상

IAT 컨퍼런스 2017



/감/사/합/니/다/